ManageEngine
Log360

User Guide



CONTENTS

1. What is Log360 . . . . . **1**

2. What's new **2**

3. Licenses & Editions **4**

4. Get started **8**

5. Setting up Log360 . . . . . **11**

5.1. Prerequisites **11**

5.1.1. System requirements 11

5.1.2. Port requirements 18

5.1.3. Increasing Product Memory 46

5.2. Installation **47**

5.2.1. Installation and uninstallation 47

5.2.2. Starting and stopping the product 68

5.2.3. Accessing the product 72

5.3. Essential configurations **73**

5.3.1. Reverse proxy **73**

5.3.1.1. Overview 73

5.3.1.2. Managing reverse proxy 75

5.4. Components of Log360 . . . . . **81**

5.4.1. Overview 81

5.4.2. Downloading and installing components 83

5.4.3. Integrating the components 88

5.4.4. Navigating across components 92

5.4.5. Additional configurations 95

6. Scalability **97**

6.1. Log processor **97**

6.1.1. Overview 97

6.1.2. Configuring Log Processors 100

6.1.3. Managing Log Processors 116

6.1.4. Troubleshooting tips 137

7. Data source configuration **140**

7.1. Windows Infrastructure **140**

7.1.1. Overview 140

7.1.2. Working 141

7.1.3. Prerequisites for adding Windows devices 143

7.1.4. Add Windows devices 150

7.1.5. Add AWS EC2 Windows instance 153

7.1.6. Configuring out-of-the-box reports 157

7.2. Syslog Devices **160**

7.2.1. Overview 160

7.3. Linux and Unix Systems **165**

7.3.1. UNIX device 165

7.3.2. Mac OS device . . . 166
7.4. Database . . . 167
7.4.1. SQL Servers . . . 167
7.4.2. MySQL Servers . . . 168
7.4.3. Oracle . . . 169
7.5. Endpoint Security Solutions . . . 170
7.5.1. FireEye devices . . . 170
7.5.2. Malwarebytes devices . . . 171
7.5.3. McAfee devices . . . 172
7.5.4. Symantec DLP devices . . . 174
7.5.5. Symantec Endpoint Protection devices . . . 175
7.5.6. Trend Micro - Deep Security . . . 176
7.6. Network devices . . . 178
7.6.1. HP-UX/Solaris/AIX device . . . 178
7.6.2. Arista Switches . . . 179
7.6.3. Cisco Switches . . . 180
7.6.4. Cisco Firepower devices . . . 181
7.6.5. Sonicwall devices . . . 183
7.6.6. Juniper devices . . . 184
7.6.7. PaloAlto devices . . . 185
7.6.8. Cisco devices . . . 187
7.6.9. Fortinet devices . . . 188
7.6.10. CheckPoint devices . . . 189
7.6.11. NetScreen devices . . . 190
7.6.12. Watchguard devices . . . 191
7.6.13. Sophos and Cyberoam devices . . . 192
7.6.14. Barracuda devices . . . 193
7.6.15. Huawei Firewall devices . . . 195
7.6.16. Meraki devices . . . 196
7.6.17. pfSense devices . . . 197
7.6.18. H3C devices . . . 198
7.6.19. StormShield devices . . . 199
7.6.20. F5 devices . . . 200
7.6.21. Forcepoint devices . . . 202
7.6.22. Dell devices . . . 203
7.6.23. Topsec devices . . . 204
7.6.24. Sangfor devices . . . 206
7.6.25. Stackato devices . . . 209
7.6.26. Scaler NSS devices . . . 210
7.7. General applications . . . 211
7.7.1. CEF devices . . . 211
7.7.2. Printer server . . . 212
7.7.3. Terminal server . . . 214
7.7.4. Sysmon application . . . 215

7.7.5. Syslog application . . . 217
7.8. ManageEngine applications . . . 219
7.9. Other Devices . . . 227
7.9.1. Adding other devices . . . 227
7.9.2. IBM AS400 devices . . . 228
7.9.3. File Integrity Monitoring . . . 232
7.10. Import Logs . . . 239
7.10.1. Import Log Files . . . 239
7.11. Hypervisors . . . 255
7.11.1. On a VMware . . . 255
7.11.2. Adding vCenter Microsoft Hyper V . . . 256
7.12. Vulnerability Scanners . . . 257
7.12.1. Nessus and reports . . . 257
7.12.2. Nmap . . . 260
7.12.3. Nexpose . . . 261
7.12.4. OpenVAS . . . 262
7.12.5. Qualys . . . 263
7.13. Web Servers . . . 264
7.13.1. IIS servers . . . 264
7.14. Cloud sources . . . 270
7.14.1. M365 . . . 270
7.14.1.1. Overview . . . 270
7.14.1.2. Adding data source . . . 272
7.14.2. Troubleshooting . . . 275
7.14.3. AWS . . . 277
8. Working with Log360 . . . 288
8.1. User interface . . . 288
8.1.1. Tabs . . . 288
8.1.2. Log receiver . . . 295
8.1.3. Notification center . . . 298
8.1.4. Global search . . . 299
8.2. Dashboard . . . 301
8.2.1. Overview . . . 301
8.2.2. Predefined tabs and widgets . . . 308
8.2.3. Customize dashboard views . . . 322
8.3. Reports . . . 343
8.3.1. Overview . . . 343
8.3.2. Managing Predefined Reports . . . 345
8.3.3. Schedule Reports . . . 347
8.3.4. Create Custom Reports . . . 349
8.3.5. Managing Report Views . . . 357
8.3.6. Mark report as favourite . . . 360
8.3.7. Report Export and Customization . . . 362
8.4. Compliance . . . 368

8.4.1. Overview . . . 368
8.4.2. Configuring custom compliance reports . . . 373
8.4.3. Managing compliance regulations . . . 377
8.4.4. Scheduling compliance reports . . . 381
8.4.5. Managing compliance schedulers . . . 387
8.4.6. Viewing and managing compliance reports . . . 391
8.4.6.1. Risk posture . . . 398
8.4.6.1.1. Overview . . . 398
8.4.6.1.2. Risk analysis . . . 400
8.4.6.1.3. Active Directory . . . 406
8.4.6.1.4. SQL server . . . 423
8.5. Search . . . 451
8.5.1. Log search/ Forensic search . . . 451
8.5.2. How to Extract New Fields . . . 456
8.5.3. How to Search Logs . . . 460
8.5.4. How to Tag Fields . . . 467
8.6. Alerts . . . 472
8.6.1. Overview . . . 472
8.6.2. Create Alert Profile . . . 475
8.6.3. Manage Alert Profiles . . . 486
8.6.4. Alert notification & remediation . . . 495
9. Settings . . . 500
9.1. Admin Settings . . . 500
9.1.1. Administration Settings . . . 500
9.1.2. Device Group Management . . . 501
9.1.3. Archive . . . 504
9.1.4. Privacy settings . . . 525
9.1.5. Profiles . . . 527
9.1.6. Custom log parsing . . . 529
9.1.7. Retention settings . . . 537
9.1.8. Log collection filter . . . 539
9.1.9. Log collection alerts . . . 542
9.1.10. Tags . . . 543
9.1.11. Auto Update . . . 544
9.1.12. Agent adminstration and settings . . . 545
9.1.12.1. Overview . . . 545
9.1.12.2. Agent installation . . . 547
9.1.12.3. Managing agents . . . 561
9.1.12.4. Agent settings . . . 566
9.1.13. Centralized technician management . . . 569
9.1.13.1. Overview . . . 569
9.1.13.2. Adding technicians . . . 573
9.1.13.3. Managing technicians . . . 587
9.1.13.4. Creating and managing roles . . . 602

9.2. Product Settings **612**
9.2.1. Overview 612
9.2.2. Security Hardening 613
9.3. Logon Settings **615**
9.3.1. General 615
9.3.2. Two-factor Authentication 620
9.3.3. Single Sign-On 636
9.3.4. Smartcard Authentication 650
9.3.5. Allow/restrict IP addresses 657
9.3.6. Working Hour Settings 664
9.3.7. Reset Account Settings 665
9.3.8. Domains & Workgroups 667
9.3.9. Report Profiles 673
9.3.10. NTLMv2 SSO configuration 674
9.4. API Settings **675**
9.4.1. API Settings 675
9.4.2. Get log sources 678
9.4.3. Get log fields 680
9.4.4. Get log types 682
9.4.5. Asynchronous Search 684
9.4.6. Jobs Endpoint 686
9.4.7. Jobs Result endpoint 690
9.4.8. Get alert profiles 692
9.4.9. Synchronous alerts 694
9.4.10. Asynchronous alerts 698
9.4.11. Synchronous Search 701
9.5. System Settings **705**
9.5.1. System Settings 705
9.5.2. Connection Settings 706
9.5.3. Notification Settings 721
9.5.4. Listener Ports **732**
9.5.4.1. Syslog 732
9.5.4.2. SNMP Traps 742
9.5.5. Re-branding 748
9.5.6. System diagnostics 751
9.5.7. System Info 752
9.5.8. Service account permissions 755
9.5.9. System Utilization 760
9.5.10. SSL Certitiation Tool **763**
9.5.10.1. SSL configuration for Log360 763
9.5.10.2. What is SSL 766
9.5.10.3. Server Settings 768
9.5.11. Deploy and Manage Log Collection Agents 777
9.5.12. Install EventLog Analyzer as a service 791

9.6. Configurations . . . **793**
9.6.1. Device Management . . . 793
9.6.2. Configure External ManageEngine Applications . . . 802
9.6.3. Device Auto Allocation . . . **804**
9.6.3.1. Overview . . . 804
9.6.3.2. Configuring Auto Allocation . . . 808
9.6.3.3. Configuring Auto Allocation Policies . . . 811
9.6.3.4. Check Unallocated Device Status . . . 817
9.6.3.5. Sync Settings . . . 820
9.6.4. Manage Applications . . . 823
9.6.5. Application . . . 825
9.6.6. Adding custom threat sources . . . 826
10. Threat intelligence & data analytics . . . **833**
10.1. Threat detection . . . **833**
10.1.1. Security Dashboard . . . **833**
10.1.1.1. Overview . . . 833
10.1.1.2. Security dashboard widgets . . . 839
10.1.2. Rule management . . . **853**
10.1.2.1. Overview . . . 853
10.1.2.2. Understanding rules . . . 858
10.1.2.3. Creating custom rules . . . 878
10.1.2.4. Managing rules . . . 886
10.1.2.5. Query grammar . . . 905
10.1.2.6. Scheduled detection reports . . . 926
10.1.3. AD Object Filter . . . **931**
10.1.3.1. Object filtering for Active Directory for rule fine tuning . . . 931
10.1.3.2. Accessing and applying object filtering . . . 936
10.1.4. Rule library . . . **958**
10.1.4.1. Overview . . . 958
10.1.4.2. Installing Rules . . . 961
10.1.4.3. Configuring auto-install settings . . . 967
10.1.4.4. Configuring Rule Update Settings . . . 970
10.1.5. Advanced threat analytics . . . **978**
10.1.5.1. Overview . . . 978
10.1.5.2. Log360 Cloud Threat Analytics . . . 982
10.1.5.3. VirusTotal . . . 986
10.1.5.4. Constella Intelligence . . . 994
10.1.5.5. Threat Whitelisting . . . 998
10.1.5.6. Threat Import . . . 1004
10.1.5.7. Switching threat stores . . . 1006
10.1.5.8. MITRE ATT&CK TTP(S) Framework Integration . . . 1008
10.1.6. VM Management . . . 1010
10.1.7. Manage Vulnerability Data . . . 1012
10.2. Threat investigation . . . **1014**

10.2.1. Overview . . . 1014
10.2.2. Zia Insights . . . 1016
10.2.2.1. Overview . . . 1016
10.2.2.2. Using Zia Insights . . . 1019
10.2.2.3. Setting up Zia Insights . . . 1025
10.2.2.4. Invoking Zia Insights . . . 1038
10.2.3. Incident workbench . . . 1044
10.2.3.1. Overview . . . 1044
10.2.3.2. Access . . . 1046
10.2.3.3. User Analytics . . . 1051
10.2.3.4. Process Analytics . . . 1055
10.2.3.5. Advanced Threat Analytics . . . 1060
10.2.3.6. Incident Building . . . 1064
10.3. Threat response . . . 1068
10.3.1. Incident management . . . 1068
10.3.1.1. Create and assign workflow profiles . . . 1068
10.3.2. Playbook management . . . 1080
10.3.2.1. Overview . . . 1080
10.3.2.2. Prerequisites . . . 1089
10.3.2.3. Create a playbook . . . 1099
10.3.2.4. Managing playbooks . . . 1112
10.3.2.5. Update playbook credentials . . . 1116
10.3.3. Ticketing tools configuration . . . 1128
11. General Settings . . . 1149
11.1. Database Settings . . . 1149
11.1.1. Auto Backup . . . 1149
11.1.2. Migration . . . 1152
11.1.3. Overview . . . 1158
11.2. Database Access . . . 1159
11.3. Log Level Settings . . . 1160
11.4. Log Forwarder . . . 1161
11.5. Product Settings . . . 1165
12. Integrations . . . 1176
12.1. Extensions . . . 1176
12.1.1. Installing Extensions . . . 1176
12.1.2. Compliance Extensions . . . 1184
12.1.3. Veeam . . . 1186
12.1.4. Dropbox . . . 1199
13. Search Engine . . . 1207
13.1. Elastic Search . . . 1207
14. Developer Space . . . 1210
14.1. Custom widgets . . . 1210
15. Migration . . . 1226
15.1. Migrate data from PostgreSQL to MS SQL database . . . 1226

15.2. Migrating to a Different Directory in the Same Server 1230
15.3. MySQL to MSSQL Migration 1231
15.4. Migrating inbuilt PostgreSQL to a common PGSQL database 1234
15.5. Scalability migration guide 1236
16. MSSP edition **1238**
16.1. Overview 1238
16.2. Customer management 1242
16.3. License management 1253
16.4. Technician management 1261
16.5. Reverse proxy 1270
16.6. Auto-upgrade 1273
17. FAQ and troubleshooting **1280**
17.1. Troubleshooting Tips 1280
17.2. Frequently Asked Questions 1312
18. Technical Support **1319**
18.1. Overview 1319
18.2. Create SIF offline 1320
18.3. Contact Support 1323

1. What is Log360?

Last updated on: September 12, 2025

Log360 is a unified security information and event management (SIEM) solution from ManageEngine. It is designed to help enterprises secure their IT environment, meet compliance mandates, and gain visibility into potential threats. By combining log management, Active Directory auditing, cloud security, user behavior analytics, and more into a single platform, it empowers security teams to detect, investigate, and respond to threats faster.

The product offers:

- Security event management: Collect, analyze, and monitor logs from servers, applications, firewalls, databases, and endpoints.
- Threat detection, investigation, and response (TDIR): Detect anomalies and insider threats using machine learning and user/entity behavior analytics (UEBA).
- Active Directory auditing: Track changes and monitor logons to prevent unauthorized access.
- Cloud security monitoring: Gain visibility into cloud platforms like Microsoft 365, AWS, and Azure.
- Compliance reporting: Generate out-of-the-box reports to meet global compliance mandates like GDPR, HIPAA, PCI DSS, SOX, NIS2, DORA, and more.

In short, Log360 provides end-to-end visibility across on-premises, cloud, and hybrid environments, making it an integral part of a modern security operations center (SOC).

Why Log360?

Choosing Log360 helps enterprises achieve both security efficiency and compliance readiness. Here's why organizations prefer Log360:

1. Comprehensive security coverage Log360 combines multiple security solutions into one platform—covering log management, Active Directory auditing, cloud monitoring, data access governance, and privileged access management.
2. Faster threat detection and response With built-in analytics and UEBA, Log360 detects unusual user activities, insider threats, ransomware, and data exfiltration attempts in real time.
3. Simplified compliance Log360 provides prebuilt compliance reports and alerting mechanisms, helping organizations stay compliant with international and industry-specific regulations.
4. Centralized visibility Security teams can monitor their entire IT infrastructure—on-premises, cloud, and hybrid—from a single console, reducing complexity.
5. Scalability and flexibility Designed for organizations of all sizes, Log360 scales easily with business growth while offering flexible deployment options (on-premises or cloud).
6. Cost-effective SIEM By consolidating multiple tools, Log360 reduces the need for separate point solutions, making it a cost-efficient option for enterprises.

2. What's new in Log360

Last updated on: September 12, 2025

New features

Re-engineered detection architecture

- Centralized detection console: Manage detection rules across MITRE, UEBA, correlation, and threat intelligence engines from a single unified interface.
- Security analytics dashboard: Monitor rule coverage, alert trends, detection health, and top threats in one place.
- Multi-mode rule creation: Build standard, anomaly, and advanced rules to cover a wide range of security scenarios.
- Object-level filtering: Scope detection rules by users, groups, and OUs to cut down false positives and alert fatigue.
- Tuning insights: Optimize rule performance through insights into hit frequencies, alert volumes, and suppression opportunities.
- Cloud-delivered content: 2,000+ prebuilt rules mapped to MITRE ATT&CK®, anomaly detections, correlation logic, and threat intelligence use cases.
- Correlation engine: Perform complex, flexible aggregated queries for sophisticated attack pattern detection.

Microsoft 365 support

- New log source: Collect logs from Microsoft 365 environments natively.
- Predefined reports: 200+ built-in reports for Entra ID, Exchange Online, Sharepoint, OneDrive, and Teams.
- Security rules: 51 pre-defined Microsoft 365 detection rules.
- Object filter support: Apply identity-based filters to predefined rules to reduce noise.

Scalable architecture

- The solution will now support multi-tier or n-tier architecture where the log processors will handle specific capabilities of product easing the scalability and improving performance metrics.
- Horizontal scaling: Add log processor nodes to handle increased workloads with improved resilience and performance.
- High availability: Prevent single points of failure with role-based distribution across correlation, search, and alerting engines.
- Secure collection: Supports agent-based syslog collection with https encryption for secure data transfer.

Playbook recommendations

- Intelligent playbook suggestions based on event type and past executions.

Enhancements

- Rule notifications : Configure alert profiles to send notifications to all admins or specific recipients.
- RSA SecurID REST API support: Adds rest api-based integration for RSA SecureID (recommended over sdk-based integration).
- Reverse proxy enhancement: Now enabled only when at least one component is integrated.
- Faster alert processing: Optimized the alert engine’s criteria-matching logic to handle high log volumes more efficiently.
- LDAP SSL: Included as a part of the solution's security hardening score calculation.
- Login page customization: Option to hide the “forgot password” link.
- Product notifications: Alerts for the solution's startup, AMS expiry, and version upgrades.
- SSL settings: New dedicated tab in connection settings for easier configuration.
- Compliance reports: Added support for NIS2 and FADP compliance frameworks.

UI changes

- Integration settings: Reorganized under a dedicated advanced configuration tab for easier navigation.
- Session activity reports: Now integrated within the reports module for unified reporting.
- Browser title & Favicon rebranding: Customize product appearance to match your organization.

3. License Details

Last updated on: September 12, 2025

Eventlog Analyzer

License Details

Unlike some of our competitors, who charge based on log volume processed, ManageEngine EventLog Analyzer offers a simple licensing model. Licensing is based on the license model and the number of log sources. The product has just one edition, Professional edition. The license models are, Perpetual (Standard) and Annual Subscription Model (ASM).
The solution is licensed based on the number of log sources, endpoints and cloud accounts.

Available Editions

Professional:

The Professional edition is designed for businesses of all sizes, whether operating from a single site or across multiple geographical locations. It enables monitoring from 10 to unlimited hosts and applications, while supporting high log reception rates that scale with your infrastructure.

Advantages of ManageEngine Licensing

Licensing is simple, cost-conscious, and based on the number of devices or applications to be monitored. There are no restrictions on deployment models, allowing you to scale seamlessly as your monitoring needs grow.

License Models

Perpetual model

In this model, the licensing is perpetual and a nominal amount is charged as Annual Maintenance and Support (AMS) fee to provide the maintenance, support, and updates.

Annual Subscription model

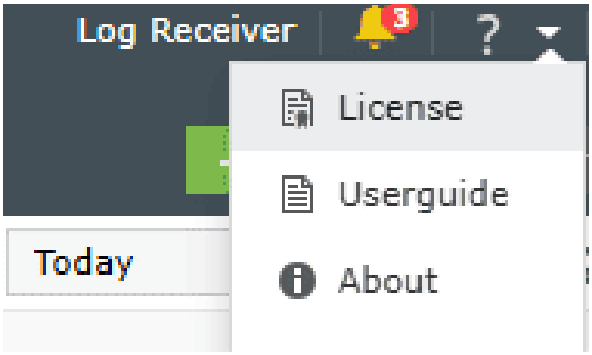
In this model, the license is valid for one year and after that the license expires. To continue the license should be renewed every year. Annual Maintenance and Support (AMS) fee is included in the subscription price and not charged separately.

How to choose the license

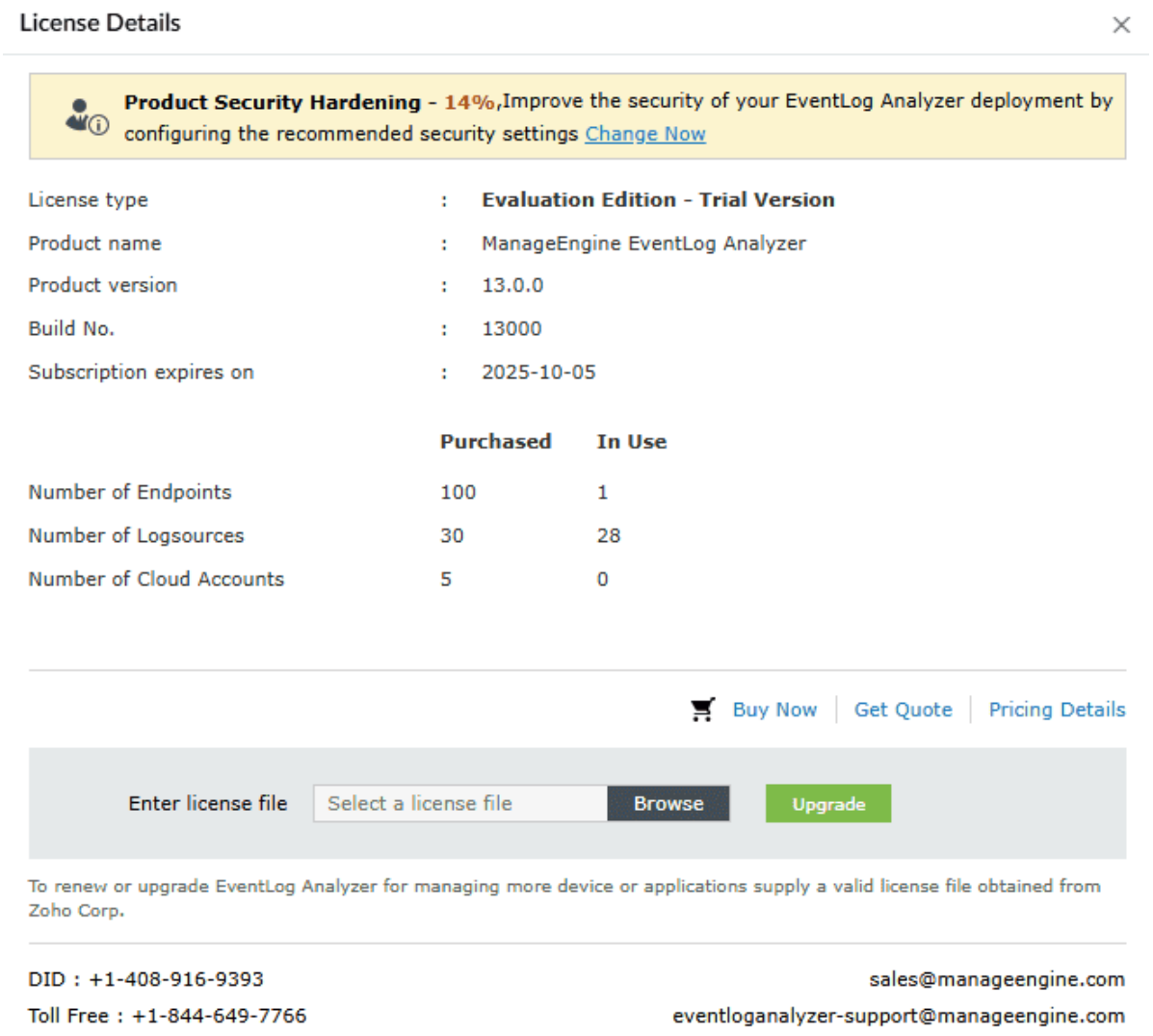
- Decide upon the number of log sources, endpoints and cloud accounts to be monitored.
- Choose Perpetual model for a license with no expiry and choose Annual Subscription Model for low entry cost.

Steps to apply the license

- Click on the ? icon on the top right corner of the UI and select License.



- The License Details pop-up appears.
- Browse for the required license file and click on Upgrade.



Upgrade from evaluator to purchased license

- Before upgrading the current license, ensure that you save the new license file from ZOHO Corp. on the machine in which EventLog Analyzer is installed.
- After you log in to EventLog Analyzer, click the Upgrade License link present in the top-right corner of the UI.
- Browse for the new license file and select it.

- Click Upgrade to apply the new license file.

> Note
>
> The new license will be applied with immediate effect. You do not have to shutdown and restart the server after the license is applied.

Display license details

The License window that opens up displays the license information for the current EventLog Analyzer installation. It displays the following information:

- Type of license applied - Free or Professional
- Number of days remaining for the license to expire
- Number of devices currently configured
- Maximum number of devices that you are allowed to manage

Log360

Licensing

Log360 can be downloaded and used for a 30-day trial period, with full access to all the components along with technical support . Once the 30-day trial ends, you have to purchase and apply the license to continue enjoying the full benefits of the product.
The product comes in a single edition viz., Professional edition.
The solution is licensed based on the number of Domain controllers, log sources, File servers, endpoints, and cloud accounts .
After the purchase, you can apply the license file to the product using the License link available in the top right corner of the Log360 Web portal.

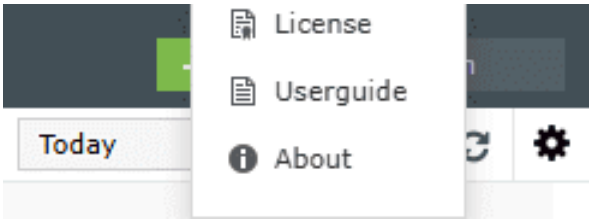
> Note
>
> With Log360, it is always pay only for what you use. You can choose to buy the license only for the component that you need.

To get a customized price quote for Log360, Click here.
Contact our support team log360-support@manageengine.com for any further queries.

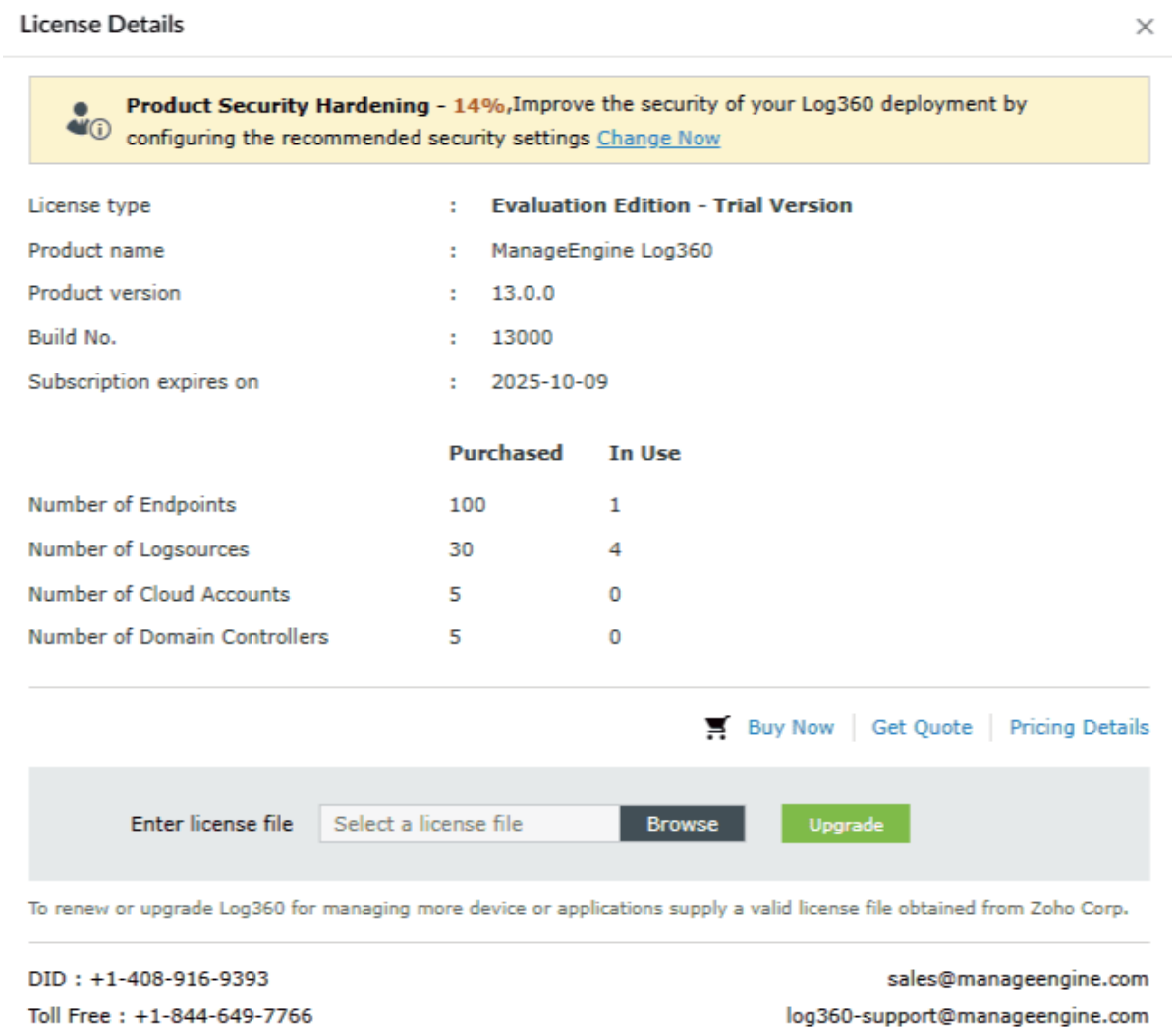
Applying License:

- Click the License link available in the top right corner of the Log360 client. This opens the License details window.





- Use the Browse button to select the license file received from ManageEngine.



- Click on the Apply button to apply the license.

4. Get Started

Last updated on: September 12, 2025

In this page

Home

Reports

Compliance

Search

Correlation

Alerts

Settings

LogMe

Support

+Add

EventLog Analyzer is a comprehensive log management solution for SIEM and compliance. Here are some points to help you get started once you've installed EventLog Analyzer.

Home

The Home tab provides dashboards that allow you to gain a high-level overview of important security events in the network. You can view the severity levels of events, trends in logs, network traffic, and security threats that have been flagged.

Reports

The Reports tab displays audit reports. EventLog Analyzer provides over 1000 pre-built reports for a wide range of devices, networking equipment, and applications. You can view, add, manage, schedule, and filter reports from the reports tab. To learn more about EventLog Analyzer's reports, click here (attach link here).

Compliance

EventLog Analyzer simplifies IT compliance and regulatory audit(s). The Compliance tab in the UI helps you export comprehensive compliance reports in any format, tweak the existing report templates, and create new compliance reports. Click here to learn more about compliance reports.

Search

Search

The Search tab allows you to search through your logs and extract relevant information about a security incident. The click-based search engine makes it easy to drill-down to the root cause of an incident. The search results can then be saved as a report for auditors.

Correlation

EventLog Analyzer's real-time correlation engine helps you detect and mitigate security threats at an early stage. You can leverage the predefined rules that address a wide range of use cases and set custom rules based on the requirements of your organization. Click here (attach link here) to learn more about correlation feature in EventLog Analyzer.

Alerts

The Alerts tab in the UI helps you view all alerts that have been triggered in your network. You can leverage the built-in alert profiles and configure custom alerting criteria as per your requirements. Furthermore, critical capabilities for incident response such as ticketing tool integrations and response workflows can be configured here.

Settings

The Settings tab can be used to access the configuration settings (attach link here), admin settings (attach link here) and system settings (attach link here).

LogMe

The LogMe tab in the UI displays the different log sources supported by EventLog Analyzer and describes how to configure them for auditing.

Support

The Support tab allows you to get in touch with our technical support team and gives you access to resources that help you learn more about the solution. You can also request for a new feature and create support logs from this tab.

+Add

The +Add button in the UI is a shortcut that helps you add log sources for auditing and configure alerts, reports and log filters without having to use the settings tab.
Just getting started? Download our quick start guide to see how to install EventLog Analyzer, add devices, import logs etc.

5.1.1. System Requirements

Last updated on: September 12, 2025

In this page

Hardware Requirements

General Recommendations

VM infrastructure

CPU & RAM

Disk

Web browsers

Databases

Windows Agent Requirements

Operating systems

Installation server

This section lists the minimum system requirements for installing and working with EventLog Analyzer.

Hardware Requirements

Log management solutions are resource-intensive and selecting the right hardware plays a major role in ensuring optimal performance.
The following table denotes the suggested hardware requirements based on the type of flow.

	Low Flow	Normal Flow	High Flow
Processor cores	6	12	24
RAM	16 GB	32 GB	48 GB *
IOPS	150	750	1500 *
Disk space	1.2 TB	3 TB *	4 TB *
Network card capacity	1 GB/s	1 GB/s	10 GB/s
CPU Architecture	64-bit	64-bit	64-bit

	Low Flow	Normal Flow	High Flow

Note

- The above-mentioned values are approximate. It is recommended to run a test environment similar to the production environment with the setup details mentioned in the above table. Based on the exact flow and data size, the system requirements can be fine-tuned. Click here to access the Tuning Guide.
- For higher IOPS, we can use RAID or SSD.
- The specified RAM for High flow is designed to handle real-time log processing and search operations for up to 2TB of data.
- For searches spanning multiple days (>2TB of data), the required RAM can be calculated as: (Index Data Size in GB / 60) + 16 GB.

Use the following table to determine the type of flow for your instance.

Log type	Size (in Bytes)	Category	Log Units		
Low Flow (EPS)	Normal Flow (EPS)	High Flow (EPS)			
Windows	900	Windows	300	1500	3000
Linux, HP, pfSense, Juniper	150	Type 1 Syslogs	2000	10000	20000
Cisco. Sonicwall, Huaweii, Netscreen, Meraki, H3C	300	Type 2 Syslogs	1500	6000	12000
Barracuda, Fortinet, Checkpoint	450	Type 3 Syslogs	1200	4000	7000
Palo Alto, Sophos, F5, Firepower, and other syslogs	600	Type 4 Syslogs	800	2500	5000

Note

- A single-installation server can handle either a maximum of 3000 Windows logs or any of the high flow values mentioned for each log type in the above table.
- For log types which are not mentioned in the above table, choose the appropriate category based on the log size. For example, in the case of SQL Server logs when the byte size is 900 bytes, and EPS is 3000, it should be considered as High Flow.
- If the combined flow exceeds the capacity of a single node, or if log storage requirements are greater than 2TB, it is recommended to add an additional Log Processor node.
    - Each additional Log Processor contributes both EPS handling capacity and storage capacity, ensuring performance and scalability.
    - An additional Log Processor node can handle either up to 3000 Windows EPS or the high-flow EPS for a single log type listed in the table.

    Technical Distribution Scenarios

    - Windows EPS Scaling
        - Maximum supported per node: 3000 EPS.
        - If total flow = 4500 EPS, the flow is split across nodes:
            - Node 1: ~2250 EPS.
            - Node 2: ~2250 EPS.
    - Syslog EPS Scaling (Type 1 Syslogs)
        - Maximum supported per node: 10,000 EPS.
        - If total flow = 15,000 EPS, the flow is split across nodes:
            - Node 1: ~7500 EPS.
            - Node 2: ~7500 EPS.
    - Storage-Based Scaling
        - Maximum supported per node: 2TB of log storage.
        - If storage requirement = 5TB, logs are distributed across nodes:
            - Node 1: ~1.7TB.
            - Node 2: ~1.7TB.
            - Node 3: ~1.6TB.

    General Recommendation:
    If your EPS or storage requirement exceeds the capacity of available nodes, additional Log Processor nodes must be added. The number of nodes required depends on your environment's EPS rate and storage growth, and can be scaled horizontally as needed.
- It is recommended to choose the next higher band if advanced threat analytics and a large number of correlation rules have been used.

General Recommendations

VM infrastructure

- Allocate 100 percent RAM/CPU to the virtual machine running EventLog Analyzer. Sharing memory/CPU with other virtual machines on the same host may result in RAM/CPU starvation and may negatively impact EventLog Analyzer's performance.
- Employ thick provisioning, as thin provisioning increases I/O latency. In case of VMware, Select Thick provisioned, eagerly zeroed as lazily zeroed is lower in performance.
- Enabling VM snapshots is not recommended as the host duplicates data in multiple blocks by increasing reads and writes, resulting in increased IO latency and degraded performance.

CPU & RAM:

- Server CPU utilization should always be maintained below 85% to ensure optimal performance.
- 50% of server RAM should be kept free for off-heap utilization of Elasticsearch for optimal performance.

Disk:

- Disk latency greatly affects the performance of EventLog Analyzer. Direct-attached storage (DAS) is recommended on par with the throughout of an SSD with near-zero latency and high throughput. An enterprise storage area network (SAN) can be faster than SSD.

Web browsers:

EventLog Analyzer has been tested to support the following browsers and versions with at least a 1280x1024 display resolution:

- Microsoft Edge
- Firefox 4 and later
- Chrome 8 and later

Databases:

EventLog Analyzer can use the following databases as its back-end database.
Bundled with the product

- PostgreSQL

External databases

- Microsoft SQL 2012 & above

Please note the hardware requirements needed to configure the MS SQL database for EventLog Analyzer:

RAM	CPU	IOPS	Disk space
8GB	6	300-500	300-500 GB

Windows Agent Requirements

Windows Agent Requirements

For the Windows agent to run properly, ensure the following requirements are fulfilled.
The below table denotes the suggested hardware requirements based on the type of flow.

	Low Flow (300)	Normal Flow (1500)	High Flow (3000)
Processor Cores	4	6	12
RAM	8 GB	12GB	16 GB
Free Disk Space *	20 GB	20 GB	20 GB
CPU Architecture	32/64 bit	32/64 bit	32/64 bit

The Free Disk Space must be at least 1 GB greater than the configured maximum size of the data directory in the Agent settings if offline log collection is configured.

> **Note**
>
> To prevent high RAM utilization in the agent-installed device, ensure that the total size of the evtx logs is equivalent to 20 minutes of log data. This can be calculated by the time difference at which the first and last log entries were made (timestamps can be found in Evtx channel).
> To modify log size, open Event Viewer > right click on the required channel > Log Properties and then modify Maximum Log Size.

Operating systems

EventLog Analyzer can be installed in machines running the following operating systems and versions:
Versions requirements for Evaluation

- Windows 8 & above (or) Windows Server 2012
- Ubuntu 14 & above/ CentOS 7 & above/ Red Hat 7 & above/ Opensuse 15 & above

Version requirements for Production

- Windows Server 2022/ 2019/ 2016/ 2012 R2/ 2012
- Ubuntu 14 & above/ Red Hat version 7 & above/ CentOS 7 & above

Eventlog Analyzer on Windows v/s Linux
The below table lists all the differences of the Eventlog Analyzer instance when installed in Windows and Linux.

Feature	Windows	Linux
Domain and workgroup	Available	N/A

Feature	Windows	Linux
discovery		
Device discovery	Available	N/A
Windows devices and Windows application log collection	Agentless, agent-based and third party syslog forwarders supported	Agent-based and third party syslog forwarders supported
Auto Push and Upgrade Windows agent	Available	N/A
IIS Sites discovery and configuration	Available	N/A Note: IIS log collection is supported via import
SQL Server as back-end database	Available	N/A
MS SQL discovery and configuration	Available	N/A Note: MS SQL log collection is supported via Windows agent
MySQL discovery and configuration	Available	MySQL discovery is supported only for Linux devices. MySQL log collection from Windows machines can be done via import.
Workflow	All actions are available	Windows environment-related actions, such as process actions, service actions, AD actions, and Windows actions, are not available.
AD user login	Available	N/A
Smart Card Login & Configuration	Available	N/A

Installation server

- SIEM solutions are resource-intensive. It is recommended to provide a dedicated server for their optimal performance.
- Eventlog Analyzer uses Elasticsearch. Elasticsearch process is expected to utilize off-heap memory for

- EventLog Analyzer uses Elasticsearch. Elasticsearch process is expected to utilize off-heap memory for better performance. Off-heap memory is maintained by the operating system and will free up when necessary.

5.1.2. Prerequisites

Last updated on: September 12, 2025

In this page

Overview

Prerequisites for Log360

Ports required for EventLog Analyzer

Primary Ports

Log Collection

Agent orchestration

Importing logs

Discovery

Incident Workflow Management

Distributed communication Setup

Advanced threat analytics

Overview

This page outlines the prerequisites and setup requirements including ports, log processors, log collection, agent orchestration, discovery, workflow actions, distributed communication, antivirus exceptions, and threat analytics.
Before starting EventLog Analyzer in your environment, ensure that the following are taken care of.

Prerequisites for Log360

Prerequisites applicable for Log360

Before starting Log360 in your environment, ensure that the following are taken care of.

Ports required for Log360

The following port has to be open in Log360 for Elasticsearch.

Port Number	Port Usage
9322 (TCP)	Communication with Elasticsearch server

Ports required for ADAudit Plus

The following ports need to be opened for event collection:

Port Number(s)	Port Usage
389	Communication with LDAP protocol

Port Number(s)	Port Usage
135	Communication with RPC
445,135	Communication with NetBIOS Session Service

The following ports are needed to access ADAudit Plus:

Port Number	Port Usage
8081	HTTP
8444	HTTPS

Ports required for EventLog Analyzer

EventLog Analyzer requires the below mentioned ports to be opened on the server:

Port Number(s)	Port Usage
8095 (TCP)	Web server port
513, 514 (UDP)	Syslog listener port
514 (TCP)	Syslog listener port
33335 (TCP)	PostgreSQL/MS SQL database port

Agentless log collection:

The below mentioned ports need to be opened on the server and the remote host machine for agentless log collection to be enabled.

EventLog Analyzer uses the following ports for WMI, RPC, and DCOM.

Port Number(s)	Port Usage
135, 445, 139 (TCP)	WMI, DCOM, RPC
49152-65534 (TCP)	WMI, DCOM, RPC

Agent-based Log collection:

EventLog Analyzer uses the following ports for local agent to server UDP communication.

Port Number(s)	Port Usage
5000, 5001, 5002 (UDP)	UDP ports for EventLog Analyzer local agent-server communication

EventLog Analyzer uses the following ports for remote agent to server TCP communication:

Port Number	Port Usage

Port Number	Port Usage
8095 (TCP)	TCP port for EventLog Analyzer remote agent-server communication

For IBM AS/400

The below mentioned ports need to be opened on the server and the remote host machine.

Port Number(s)	Port Usage
446-449, 8470-8476, 9470-9476 (TCP)	Keep the mentioned ports opened for access to IBM AS/400 machines

Ports required for M365 Manager Plus

The following ports need to be opened for event collection:

Port Number	Port Usage
80 (TCP) (HTTP)	Communication with Exchange and Microsoft Online
443 (TCP) (HTTPS)	Communication with Exchange and Microsoft Online (SSL)

The following ports are needed to access M365 Manager Plus:

Port Number	Port Usage
8365 (TCP) (HTTP)	Default product port
9365 (TCP) (HTTPS)	Default product port (SSL)

Ports required for Exchange Reporter Plus

The following ports need to be opened for the product to communicate with Exchange Servers:

Port Number	Port Usage
135 (TCP)	RPC
5985 (TCP)	Windows PowerShell Default psSession
5986 (TCP) (HTTPS)	Windows PowerShell Default psSession SSL
80 (TCP)	PowerShell
443 (TCP) (HTTPS)	PowerShell SSL

The following ports need to be opened for the product to communicate with Active Directory:

Port Number	Port Usage
389 (TCP)	LDAP
636 (TCP) (HTTPS)	LDAP SSL
3268 (TCP)	LDAP GC
3269 (TCP) (HTTPS)	LDAP GC SSL
53 (TCP)	DNS
88 (TCP)	Kerberos
139 (TCP)	NetBIOS

The following ports are needed for Exchange Reporter Plus:

Port Number	Port Usage
8181	HTTPS
3309	ERP product database

Ports required for ADManager Plus

The following ports are required for ADManager Plus:

Port Number	Port Usage
33306	Communication with database
31000	Java wrapper service
22	Secure Shell (SSH)
8080/8443	Web server
2000	Email
389/639	LDAP/LDAPS

80 Port Number	Exchange server Port Usage
80,443	G Suite, Microsoft365
3268	LDAP search for Global Catalog (GC)

Ports required for Cloud Security Plus

The following ports are needed to access Cloud Security Plus:

Port Number	Port Usage
8055	HTTP
8056	HTTPS
514	Default Syslog listener
25	Default mail server SMTP
33355	PostgreSQL/MS SQL database
80, 443	Clouds and their data source
9300-9400 (any one TCP port) 9200-9300 (any one HTTP port)	Elastic Search

Using Log360 with Antivirus Applications

To ensure unhindered functioning of Log360, you need to add the following files to the exception list of your Antivirus application:

Path	Need for whitelisting	Impact if not whitelisted
<ME>/elasticsearch/ES/data	Elasticsearch indexed data is stored	Reports would be affected if the data is deleted.
<ME>/elasticsearch/ES/repo	Elasticsearch index snapshot is taken at this location.	Snapshots and Elasticsearch archival feature will fail if the files at this location are deleted.
<ME>/elasticsearch/ES/archive	Elasticsearch archives are stored here.	Data will not be available if the files located here are deleted.
<Log360_Home>/bin	All binaries are included here. Some Antivirus applications might block them as false positive.	Product might not function.

Path	Need for whitelisting	Impact if not whitelisted
<Log360_Home>/pgsql/bin	Postgres binaries are included here. Might be detected as false positive by Antivirus applications.	Product might not start.
<Log360_Home>/lib/native	All binaries are included here. Some Antivirus applications might block them as false positive.	Product might not function.
<Log360_Home>/tools	All tools binaries are included here. Some Antivirus applications might block them as false positive.	Some tools might not work if the files are removed by Antivirus applications.

Ports required for Log360 UEBA

Web Server Port

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
HTTP/8096 (configurable)	UEBA Server	• UEBA Technician Machine.	Ports Usage: • The ports will by default be used for communication between the admin server and browser. • The port can be customized by the user. The acceptable range for the value is between 1024-65535.

Elasticsearch

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
TCP/9230 (configurable)	UEBA Search Engine Management Node [UEBA Node]	• UEBA Server	Ports Usage: • The Elasticsearch server in UEBA uses this port. • The port can be customized by the user. The acceptable range for the value is between 9230-9290.

Database

PORT	Additional Rights and Permissions
TCP/33337	Ports Usage: • Utilization of PostgressSQL/MSSQL database port in order to connect to the PostgreSQL database in UEBA. • Firewall port need not be opened since the internal port is bound to localhost.

Redis Cache

PORT	Additional Rights and Permissions
TCP/8179	Ports Usage: • Utilization of the port in order to connect to the Redis database in UEBA. • The acceptable range for the value is between 8179-8189.

SSL Configured Server

PORT	Additional Rights and Permissions
SSL/8446	Ports Usage: • Utilization of SSL to enhance the security between server and the client through HTTPS. • The port can be customized by the user. The acceptable range for the value is between 1024-65535.

ActiveMQ

PORT	Additional Rights and Permissions
TCP/61616	Ports Usage: • Fetches the real time events from integrated products. • The acceptable range for the value is between 61616-61626.

Ports used by PAM360

The below table lists the set of all ports used by PAM360 for remote access:

Port Name	Port Number	Direction
PostgreSQL port	3456	Outbound
Web client port	8282	Inbound
SSH port	22	Outbound
Telnet port	23	Outbound
LDAP without SSL port	389	Outbound
LDAP with SSL port	636	Outbound
SMTP port	25	Outbound
MS SQL port	1433	Outbound

Port Name Oracle port	Port Number 1521	Direction Outbound
Sybase ASE port	5000	Outbound
Password Verification port	135, 139, 445	Outbound
Auto Logon Spark View Gateway port	8283	Inbound
RDP	3389	Outbound
SSH API	6622	Inbound
REST API	8282	Inbound
Private CA-OCSP Responder Server port	8080	Inbound

What are the ports required for EventLog Analyzer?

1. Primary Ports

Web Server Port

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
HTTPS/8095 (configurable)	EventLog Analyzer Server	• EventLog Analyzer Technician Machine. • EventLog Analyzer Agent Machine.	Ports Usage: • The ports will by default be used for communication between the admin server and managed server, as well as between the agent and server. • The port can be customized by the user. The acceptable range for the value is between 1024–65535.

Log Processors

When Log360 is configured with multiple Log Processors in a scalable setup, the following ports are required in addition to the primary ports:

PORT	INBOUND	OUTBOUND	USAGE

PORT	INBOUND	OUTBOUND	USAGE
TCP/9092, 9093	EventLog Analyzer Server and Log Processor	EventLog Analyzer Server and Log Processor	Log Queue Engine communication
TCP/7800	EventLog Analyzer Server and Log Processor	EventLog Analyzer Server and Log Processor	Cluster communication between Log Processor and the main server

Elasticsearch

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
TCP/9300-9400 (configurable)	EventLog Analyzer Search Engine Management Node [SEM Node]	EventLog Analyzer Server	Ports Usage: • The Elasticsearch server in EventLog Analyzer uses this port. EventLog Analyzer Server and SEM can coexist on the same server. • The port can be customized by the user. The acceptable range for the value is between 1024–65535.

Redis Port

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
TCP/8179-8189	EventLog Analyzer Server and Log Processor	EventLog Analyzer Server and Log Processor	Ports Usage: • Utilization of Redis port in order to connect to the Redis in EventLog Analyzer. • Firewall port need not be opened since the internal port is bound to localhost.

Internal Communication

PORT	INBOUND And OUTBOUND	Additional Rights and Permissions
UDP/5000 (configurable)	EventLog Analyzer Server	Ports Usage: • These UDP ports are used internally by EventLog Analyzer for agent-to-server communication. • The port can be customized by the user. The acceptable range for the value is between 1024–65535. • Internal port bound to localhost, firewall port need not be opened.

Database

PORT	Additional Rights and Permissions

PORT	Additional Rights and Permissions
TCP/33335	Ports Usage: • Utilization of PostgreSQL/MySQL database port in order to connect to the PostgreSQL/MySQL database in EventLog Analyzer. • Firewall port need not be opened since the internal port is bound to localhost.

2. Log Collection

Windows Log Collection

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Event Log Readers • Distributed COM Users User Permissions: For root\cimv2 in WMI Properties: • Enable Account • Remote Enable • Read Security. Firewall Permissions: • Predefined Rule: Windows Management Instrumentation (WMI)
TCP/139	Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	Windows Device	EventLog Analyzer Server	SMB RPC/NP	
Dynamic ranges of RPC ports - TCP/49152 to 65,535	Windows Device	EventLog Analyzer Server	RPC randomly allocates high TCP ports for Windows Server 2008 and later versions, as well as for Windows Vista and subsequent versions	

Note

- It is not necessary to open outbound ports on the EventLog Analyzer agent machine and inbound ports on the EventLog Analyzer server.
- For Windows 2000, Windows XP, and Windows Server 2003, dynamic RPC ports range from 1025 to 5000.
- To enhance security across a broad spectrum of open ports, it is advisable to include the Server IP address within the firewall's scope. This ensures that only authorized traffic from the designated server is permitted through the firewall. Moreover, predefined rules with process and service filters, such as WMI,RPC,HTTP/HTTPS,Remote Event Log Management can further bolster security by allowing only specific processes or services to communicate through the

designated ports. If the Server IP undergoes any changes, it is imperative to promptly update the corresponding firewall rule accordingly.

Syslog Collection

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
UDP/514 (configurable)	EventLog Analyzer Server	Target Device	Syslog	User Permissions: • The port is customizable by the user.
UDP/513 (configurable)	EventLog Analyzer Server	Target Device	Syslog	
TLS/513 (configurable)	EventLog Analyzer Server	Target Device	Syslog	
TCP/514 (configurable)	EventLog Analyzer Server	Target Device	Syslog	

SSH Communication

PERMISSION	USAGES
Ensure that the algorithm mentioned below is present in the sshd_config file. File Location: /etc/ssh/sshd_config Key exchange (KEX): diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1, diffie-hellman-group14-sha256 , diffie-hellman-group15-sha512, diffie-hellman-group16-sha512, diffie-hellman-group17-sha512, diffie-hellman-group18-sha512 , ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp52 Ciphers: aes128cbc, aes128ctr, aes192cbc, aes192ctr, aes256cbc, aes256ctr, arcfour128, arcfour256, blowfishcbc, tripledescbc MAC: hmacmd5, hmacmd596, hmacsha1, hmacsha196, hmacsha256, hmacsha512 *This will be Required for all Linux Communications.	• Linux Agent Installation • Linux Agent Management & Communication • Configuring Automatic SysLog Forwarding • Linux MYSQL Server Discovery

Configure Automatic SysLog Forwarding

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/22	Linux	EventLog	SSH	User Rights: Service restart rights for 'rsyslog' or 'syslog' service. User Permissions:

PORTS	Device INBOUND	Analyzer Server OUTBOUND	SERVICE	Additional Rights and Permissions
				• "rw" permission should be enabled to files (/etc/rsyslog.conf or /etc/syslog.conf). • Permissions for SSH Communication

AS400 Log Collection

PORTS	INBOUND	OUTBOUND
TCP/446-449	AS400 Server	EventLog Analyzer Server
TCP/8470-8476	AS400 Serve	EventLog Analyzer Server
TCP/9470-9476	AS400 Serve	EventLog Analyzer Server

SNMP Trap Collection

PORTS	INBOUND	OUTBOUND	SERVICES	Additional Rights and Permissions
UDP/162 (configurable)	EventLog Analyzer Server	Network Device / Application	SNMP	User Permissions: • User can customize the port.

IIS Log Collection

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	IIS Server	EventLog Analyzer Server	RPC	User Permissions: • Read access to the IIS log folder should be enabled. • Permissions for the system 32/inetsrv should be enabled • Administrator share privileges are required eg : Admin$,c$
TCP/139	IIS Server	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	IIS Server	EventLog Analyzer Server	SMB RPC/NP	

3. Agent orchestration

Windows Agent Log Collection and Communication

PORTS	INBOUND	OUTBOUND	Additional Rights and Permissions

PORTS HTTPS/8094, 8095 (configurable)	EventLog Analyzer Server and Log Processor INBOUND	EventLog Analyzer Agent Machine and Log Processor OUTBOUND	Environment Permission: Additional Rights and Permissions • 8094, 8095 port should be open in both Agent machine and in Server machine.

Note

Communication includes tasks such as agent synchronization and checking agent status.

Windows Agent Installation & Management

Windows Agent Installation Prerequisites

Hardware Requirements: This section gives you information about the hardware requirements for the Log360 agent.
For 32 bit machines

- 1 GHz, 32-bit (x86) Pentium Dual Core processor or equivalent
- 2 GB RAM

For 64 bit machines

- 2.80 GHz, 64-bit (x64) Xeon® LV processor or equivalent
- 2 GB RAM

Operating System Requirements: The Log360 agent can be installed and run on the following operating systems (both 32 Bit and 64 Bit architecture) and versions:

- Windows®
- Windows 7 & above
- Windows Server 2008 & above

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	EventLog Analyzer Agent Machine	EventLog Analyzer Server	RPC	User Permissions: • Read, write and modify permissions to files in \\ <ipaddress>\Admin$\TEMP\EventLogAgent should be enabled. • Access "Remote Registry" service • At least read control should be granted for winreg registry key. (Computer \HKEY_LOCAL _MACHINE\ SYSTEM\ CurrentContro lSet\Control\ SecurePipe Servers\winreg). • Read/Write registry keys - SOFTWARE\\ Wow6432Node \\ZOHO Corp\\EventLog Analyzer\\ (or) SOFTWARE \\ZOHO Corp \\EventLog Analyzer\\.
TCP/139	EventLog Analyzer Agent Machine	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	EventLog Analyzer Agent Machine	EventLog Analyzer Server	SMB RPC/NP	
			RPC randomly allocates high TCP ports for Windows	

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
Dynamic ranges of RPC ports - TCP/49152 to 65,535	EventLog Analyzer Agent Machine	EventLog Analyzer Server	Server 2008 and later versions, as well as for Windows Vista and subsequent versions	• There should be access to remote services.msc

Note

Management involves actions like starting, stopping, or uninstalling the agent software.

Linux Agent Installation

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/22	EventLog Analyzer Agent Machine	EventLog Analyzer Server	SSH	Sudo User Permissions: • "rwx" permission is required for /opt/ManageEngine/ for transferring files. • Permissions for SSH Communication

Linux Agent Management & Communication

PORTS	INBOUND	OUTBOUND	Additional Rights and Permissions
TCP/22	EventLog Analyzer Server	EventLog Analyzer Server	User Permissions: • SFTP permissions to transfer files to /opt/Manage Engine/EventL ogAnalyzer_ Agent and /etc /audisp/plugins.d • Service start/stop/restart permission for auditd. • Permissions for SSH Communication
HTTPS/8094, 8095 (configurable)	EventLog Analyzer Server and Log Processor	EventLog Analyzer Agent Machine and Log Processor	

4. Importing logs

Importing Logs using SMB

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/137	Target Device	EventLog Analyzer Server	NetBIOS name resolution RPC/named pipes (NP)	

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/138	Target Device	EventLog Analyzer Server	NetBIOS datagram	User Permissions: • Network access: Do not allow anonymous not allow anonymous enumeration of SAM accounts and shares. • Sometimes, connecting to different workgroup needs credentials even to view the shared resources.
TCP/139	Target Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	Target Device	EventLog Analyzer Server	SMB RPC/NP	

Importing logs using FTP

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/20	Target Device	EventLog Analyzer Server	FTP/SFTP	User Permissions: • SAuthentication for the FTP server should be enabled.
TCP/21	Target Device	EventLog Analyzer Server	FTP/SFTP	

5. Discovery

Windows Domain Discovery

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/389	Domain Controller	EventLog Analyzer Server	LDAP	User Permissions: • User should have read permission to Active Directory Domain Objects. • Permission to run LDAP query in ADS_ SECURE_AUTHENTICATION mode should be present.

Windows Workgroup Discovery

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	Workgroup Server	EventLog Analyzer Server	RPC	
TCP/139	Workgroup Server	EventLog Analyzer	NetBIOS session	User Permissions: • User should have read permission to Active

PORTS	INBOUND	Server OUTBOUND	RPC/NP SERVICE	Directory Domain Objects Additional Rights and Permissions
TCP/445	Workgroup Server	EventLog Analyzer Server	SMB RPC/NP	• Permission to run WinNT query in ADS_ SECURE_ AUTHENTI CATION mode should be given.
TCP/1024-65535	Workgroup Server	EventLog Analyzer Server	RPC randomly allocated high TCP ports	

Event Source Discovery

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	Target Windows Device	EventLog Analyzer Server	RPC	User Permissions: • The winreg registry key should at the very least be given read control.
TCP/137	Target Windows Device	EventLog Analyzer Server	NetBIOS name resolution RPC/named pipes (NP)	
TCP/138	Target Windows Device	EventLog Analyzer Server	NetBIOS datagram	
TCP/139	Workgroup Server	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	Workgroup Server	EventLog Analyzer Server	SMB RPC/NP	

MSSQL Server Discovery-Windows

PORTS	INBOUND	OUTBOUND	Additional Rights and Permissions
UDP/1434	MSSql Server	EventLog Analyzer Server	User Permissions: • Can be configured to use dynamic TCP ports for communication.
TCP/1433	MSSql Server	EventLog Analyzer Server	

Network Device Discovery

PORTS	INBOUND	OUTBOUND	Additional Rights and Permissions

PORTS	INBOUND	OUTBOUND	Additional Rights and Permissions
UDP/162	Network Devices	EventLog Analyzer Server	Ports Usage:: • Fetches a list of live SNMP-enabled IP devices that responds to the SNMP ping.

IIS Discovery

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/445	IIS Server	EventLog Analyzer Server	SMB RPC/NP	Ports Usage: • The Server Message Block (SMB) protocol uses this port to read the log files.

MYSQL Server Discovery-Windows

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	MySql Server	EventLog Analyzer Server	RPC	User Permissions: • WMI permission is needed to find the MySQL server configuration file using SFTP.
TCP/445	MySql Server	EventLog Analyzer Server	SMB RPC/NP	

MYSQL Server Discovery-Linux

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/22	MySql Server	EventLog Analyzer Server	SMB RPC/NP	User Permissions: • Read permission to the MySQL server configuration file using SFTP. • Permissions for SSH Communication

6. Incident Workflow Management

NETWORK ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND
PING DEVICE	ICMP/No ports	Audited Windows / Linux Device	EventLog Analyzer Server
TRACE ROUTE WINDOWS	ICMP/No ports	Audited Windows Device	EventLog Analyzer Server

BLOCK TRACE ROUTE LINUX	PORT UDP/33434 -33534	INBOUND Audited Linux Device	OUTBOUND EventLog Analyzer Server

WINDOWS ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
LogOff	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • The computer should not include EventLog Analyzer Installed server.
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
Shutdown and Restart	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • The computer should not include EventLog Analyzer Installed server
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and User Permissions:
		Audited	EventLog	NetBIOS	Users Permissions
	TCP/139	Windows Device	Analyzer Server	session RPC/NP	For root\cim v2 In WMI
Execute Windows Script	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • The user should have read,write and modify access to the shared path in the script.
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
Disable USB	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • Remote Registry Service should be running. • Full Control permission to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
ALL SERVICE BLOCK	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users • Administrators User Permissions: For root\cim v2 In WMI Properties:
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
		Audited	EventLog	SMB	

BLOCK	PORT	INBOUND	OUTBOUND	RPC/NP SERVICE	Additional Rights and Permissions
	TCP/445	Windows Device	Analyzer Server	SMB	• Execute Methods • Enable Account
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	• Remote Enable • Read Security
START PROCESS	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
STOP PROCESS	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
	TCP/135	Audited Windows	EventLog Analyzer	RPC	

BLOCK	PORT	Device INBOUND	Server OUTBOUND	SERVICE	Additional Rights and UserGroups: Permissions
		Audited	EventLog	NetBIOS	• Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
TEST PROCESS	TCP/139	Windows Device	Analyzer Server	session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	

LINUX ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
Shutdown and Restart	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: The user should be the root user.
Execute Windows Script	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: Sudo permission for user.
ALL SERVICE BLOCK	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: Sudo permission.
START PROCESS	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: The permission to execute the command should be available for the user whose credentials are provided.
STOP PROCESS	Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: The permission to execute the command should be available for the user whose credentials are provided.
TEST PROCESS	TCP/Specified port.	Audited Linux	EventLog Analyzer	-	-

BLOCK	PORT	Device INBOUND	Server OUTBOUND	SERVICE	Additional Rights and Permissions

NOTIFICATIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
Pop Up WINODWS	TCP/135	Audited Linux Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • "AllowRemoteRPC" should be 1 for HKEY_ LOCAL_MACHINE\ SYSTEM\Current ControlSet\Control\Terminal Server.
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
Pop Up LINUX	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: Sudo permission for user.
Send Email WINDOWS & LINUX	TCP/Port mentioned while config using SMTP server	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: SMTP server should be configured on Event log analyzer server
Send SMS WINDOWS & LINUX	-	-	-	-	Environment Permission: SMS Server should be configured in the product.
Send SNMP Trap WINDOWS & LINUX	UDP/Port specified in workflow block	Audited Windows / Linux Device	EventLog Analyzer Server	-	Environment Permission: The port mentioned in workflow configuration should be open.

Active Directory ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	User Permissions: Additional Rights and Permissions
DELETE AD USER WINDOWS	TCP/389	Audited Domain Controller	EventLog Analyzer Server	LDAP	• The user should have "Delete" Right in the AD to delete other Accounts. • The user to delete should not have "Protect Object from accidental deletion" checked.
DISABLE AD USER WINDOWS	TCP/389	Audited Domain Controller	EventLog Analyzer Server	LDAP	User Permissions: • The User account provided should have "Read","Write ","modify owners" and "modify permissions" permissions enabled.
DISABLE USER COMPUTER WINDOWS & LINUX	TCP/389	Audited Domain Controller	EventLog Analyzer Server	LDAP	User Permission: • The User account provided should have "Read", "Write" , "modify owners" and "modify permissions" permissions enabled.

MISCELLANEOUS ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
WRITE TO FILE WINDOWS	TCP/135	Audited Windows Device	EventLog Analyzer Server	UserGroups: • Distributed COM Users User Rights: • Act as part of the operating system • Log on as a batch job • Log on as a service • Replace a process level token. User Permissions: For root\cim v2 In Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • The user should have read,write and modify access to the shared path.
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	
WRITE TO FILE LINUX	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	Environment Permission: • Sudo permission for user

BLOCK	PORT	Device INBOUND	Server OUTBOUND	Additional Rights and Permissions
HTTP WebHook	-	-	-	Environment Permission: • A "connect" Socket Permission to the host/port combination of the destination URL or a "URL Permission" that permits this request.
FORWARD LOGS	TCP/Specified Port	Audited Windows / Linux Device	EventLog Analyzer Server	-
CSV LOOKUP	TCP/Specified Port	Audited Windows / Linux Device	EventLog Analyzer Server	User Permissions: • Read permission to the specified CSV file.

FIREWALL ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
Cisco ASA deny inbound/Outbound rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: https://www.manageengine.com/products/eventlog/help/threat-intelligence-and-analytics/threat-response/incident-management/playbook-management.html#ciscoCredentials
Fortigate deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: https://www.manageengine.com/products/eventlog/help/threat-intelligence-and-analytics/threat-response/incident-management/playbook-management.html#fortigateCredentials
Palo Alto deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: https://www.manageengine.com/products/eventlog/help/threat-intelligence-and-analytics/threat-response/incident-management/playbook-management.html#paloAltoCredentials
Sophos XG deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: https://www.manageengine.com/products/eventlog/help/threat-intelligence-and-analytics/threat-response/incident-management/playbook-

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
Barracuda deny Access rules	https/8443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: https://www.manageengine.com/products/eventlog/help/threat-intelligence-and-analytics/threat-response/incident-management/playbook-management.html#fortigateCredentials

7. Distributed communication Setup

Distributed

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
HTTP/8095 (configurable)	EventLog Analyzer Managed Server Machine	EventLog Analyzer Admin Server Machine	User Permissions: • Managed server to Admin server communication via default webserver port. • The default port number is 8095. • The port can be customized by the user.
HTTP/8095 (configurable)	EventLog Analyzer Admin Server Machine	EventLog Analyzer Managed Server Machine	User Permissions: • Admin server to Managed server communication via default webserver port • User can customize the port. The value should be between 1024 and 65535.

Centralized Archiving Port

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
SSH/8080 (configurable)	EventLog Analyzer Admin Server Machine	EventLog Analyzer Managed Server Machine	User Permissions: • Managed server transfers the archive files to Admin Server via SSH 8080. • User can customize the port. The value should be between 1024 and 65535.

Using EventLog Analyzer with Antivirus Applications

To ensure unhindered functioning of EventLog Analyzer, you need to add the following files to the exception list of your Antivirus application:

Path	Need for whitelisting	Impact if not whitelisted

Path	Need for whitelisting	Impact if not whitelisted
<ELA_HOME>/ES/data	Elasticsearch indexed data is stored.	All the collected logs will not be available if the data is deleted.
<ELA_HOME>/ES/repo	Elasticsearch index snapshot is taken at this location.	Snapshots and Elasticsearch archival feature will fail if the files at this location are deleted.
<ELA_HOME>/ES/archive	Elasticsearch archives are stored here.	Archived log data will not be available if the files located here are deleted.
<ME>/elasticsearch/ES/data	Elasticsearch indexed data is stored.	Reports would be affected if the data is deleted.
<ME>/elasticsearch/ES/repo	Elasticsearch index snapshot is taken at this location.	Snapshots and Elasticsearch archival feature will fail if the files at this location are deleted.
<ME>/elasticsearch/ES/archive	Elasticsearch archives are stored here.	Data will not be available if the files located here are deleted.
<ELA_HOME>/data/za/threatfeeds	Bundled files containing a list of malicious IPs, domains and URLs that will be used in case there is no internet connectivity will be stored here. These files will be deleted on the first default threat feed synchronization. Whitelisting is required only till first synchronization.	If the files are removed and if there is no internet connectivity, then the list of malicious threat sources will be missed from the dataset.
<ELA_HOME>/data/AlertDump	Formatted logs are stored before processing for alerts. Might be detected as false positive by Antivirus applications.	If the file is quarantined or deleted, related alerts would be missed.
<ELA_HOME>/data/NotificationDump	Formatted logs are stored before processing for notification. Might be detected as false positive by Antivirus applications.	If the file is quarantined or deleted, notification for triggered alerts would be missed.
<ELA_HOME>/bin	All binaries are included here. Some Antivirus applications might block them as false positive.	Product might not function.
<ELA_HOME>/data/imworkflow	Binaries uploaded by users for workflow execution are stored here.	Script Alert workflow might not work as intended.

Path	Need for whitelisting	Impact if not whitelisted
<ELA_HOME>/pgsql/bin	Postgres binaries are included here. Might be detected as false positive by Antivirus applications.	Product might not start.
<ELA_HOME>/lib/native	All binaries are included here. Some Antivirus applications might block them as false positive.	Product might not function.
<ELA_HOME>/archive (If the archive folder is moved to a new location, add the new location)	Antivirus applications might slow down frequent write operations.	Performance issues might occur in the product if the Antivirus applications slow down write operations.
<ELA_HOME>/troubleshooting	All troubleshooting binaries are included here. Some Antivirus applications might block them as false positive.	Some troubleshooting batch files might not work.
<ELA_HOME>/tools	All tools binaries are included here. Some Antivirus applications might block them as false positive.	Some tools might not work if the files are removed by Antivirus applications.
<ELA_HOME>/ES/CachedRecord	Antivirus applications might slow down frequent write operations.	Performance issues might occur in the product if the Antivirus applications slow down write operations.

For Windows agent machine - 64 bit,

Path	Need for whitelisting	Impact if not whitelisted
C:\Program Files (x86)\EventLogAnalyzer_Agent\bin	Agent binaries are stored here.	The Agent might not work if the files are quarantined.
C:\Program Files (x86)\EventLogAnalyzer_Agent\bin\data	Antivirus applications might slow down frequent write operations.	Performance issues might occur in the product if the Antivirus applications slow down write operations.
C:\TEMP\\EventLogAgent	Agent installation files are moved for installation and upgrade.	Agent might not upgrade/not install if the files are quarantined.

For Windows agent machine - 32 bit,

Path	Need for whitelisting	Impact if not whitelisted
C:\Program Files\EventLogAnalyzer_Agent\bin	Agent binaries are stored here.	The Agent might not work if the files are quarantined.

Path	Need for whitelisting	Impact if not whitelisted
C:\Program Files (x86)\EventLogAnalyzer_Agent\bin\data	Antivirus applications might slow down frequent write operations.	Performance issues might occur in the product if the Antivirus applications slow down write operations.
C:\TEMP\\EventLogAgent	Agent installation files are moved for installation and upgrade.	Agent might not upgrade/not install if the files are quarantined.

For Linux agent,

Path	Need for whitelisting	Impact if not whitelisted
/opt/ManageEngine/EventLogAnalyzer_Agent/bin	Agent binaries are stored here.	The Agent might not work if the files are quarantined.
/opt/ManageEngine/EventLogAnalyzer_Agent/bin/data	Antivirus applications might slow down frequent write operations.	Performance issues might occur in the product if the Antivirus applications slow down write operations.

8. Advanced threat analytics

PORT	Additional Rights and Permissions
HTTPS/443	To fetch the "Log360 Cloud Threat Analytics" feeds, the below URLs will be used • https://log360cloud.manageengine.com/ • https://log360feeds.manageengine.com/

Read also

This page elaborated on the setup prerequisites. You can also refer to the guides below for more about system requirements, installation and uninstallation, starting and shutting down, and connecting to the server:

- System Requirements
- Start and Shutdown
- Connect to Server
- Install and Uninstall

5.1.3. Increasing Product Memory

Last updated on: September 12, 2025

Follow these steps to increase the memory allocated to EventLog Analyzer.

1. Go to EventLog Analyzer folder → open file titled "server\conf\wrapper.conf"
2. You can increase the memory allocated by editing the default values of initmemory and maxmemory as shown below.

   # Initial Java Heap Size (in MB)

   wrapper.java.initmemory=1024

   #Maximum Java Heap Size (in MB)

   wrapper.java.maxmemory=1024

```
wrapper.java.additional.36=-XX:CMSInitiatingOccupancyFraction=75
wrapper.java.additional.37=-XX:+PrintCommandLineFlags
wrapper.java.additional.38=-DSSL_PORT=8445
wrapper.java.additional.39=-Dproduct.home=..
wrapper.java.additional.40=-XX:NewRatio=3
wrapper.java.additional.41=-Dmemory_lock=enable
wrapper.java.additional.42=-Dgc_logging=true
wrapper.java.additional.43=-XX:HeapDumpPath=..%WRAPPER_FILE_SEPARATOR%logs%WRAPPER_FILE_SEPARATOR%heapDumps
%WRAPPER_FILE_SEPARATOR%
wrapper.java.additional.44=-XX:+HeapDumpOnOutOfMemoryError
wrapper.java.additional.45=-Djdk.tls.ephemeralDHKeySize=2048
wrapper.java.additional.46=-
DserverFailure.class=com.manageengine.ela.server.performance.debug.startup.ELAServerFailureHandlerImpl
wrapper.java.additional.47=-XX:+CreateMinidumpOnCrash
wrapper.java.additional.48=-XX:ErrorFile=..%WRAPPER_FILE_SEPARATOR%logs%WRAPPER_FILE_SEPARATOR%memDumps
%WRAPPER_FILE_SEPARATOR%hs_err_pid%p.log
wrapper.java.additional.49=-
Djavax.xml.transform.TransformerFactory=com.sun.org.apache.xalan.internal.xsltc.trax.TransformerFactoryImpl

wrapper.jvm.encoding=UTF-8

# Initial Java Heap Size (in MB)
wrapper.java.initmemory=2048

# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=2048

# Application parameters.  Add parameters as needed starting from 1
#wrapper.app.parameter.1=com.adventnet.mfw.Starter
#wrapper.app.parameter.2=-L../lib/AdventNetDeploymentSystem.jar

wrapper.app.parameter.1=com.adventnet.la.tray.ProductStarter
wrapper.app.parameter.2=../server/conf/TrayIconInfo.xml
wrapper.app.parameter.3=EventLogAnalyzer
```

3. Restart the product after memory allocation. The changes will be effective only after the product is restarted.

> **Note**
>
> Memory cannot be increased greater than 1 GB in 32-bit systems.

5.2.1. How to Install and Uninstall EventLog Analyzer

Last updated on: September 12, 2025

In this page

How to install EventLog Analyzer?

How to uninstall EventLog Analyzer?

How to install?

> Note
>
> As soon as EventLog Analyzer is installed on a domain-joined machine, it will automatically discover the device's domain and add the five Windows Server machines that respond first to a broadcast query in the domain. These devices can be deleted by the user, and once deleted, will not be added back automatically.

If you want to install EventLog Analyzer 64 bit version:

- In Windows OS, execute ManageEngine_EventLogAnalyzer_64bit.exe
- In Linux OS, execute ManageEngine_EventLogAnalyzer_64bit.bin

For Linux installation

- Before installing EventLog Analyzer, make the installation file executable by executing the following commands in Unix Terminal or Shell,
- Now, run ManageEngine_EventLogAnalyzer.bin by double clicking or running ./ManageEngine_EventLogAnalyzer.bin in the Terminal or Shell.

Upon starting the installation you will be taken through the following steps:

- Agree to the terms and conditions of the license agreement. You may print it for offline reference.
- Select the folder to install the product. Use the Browse option. The default installation location is C:\ManageEngine\EventLog Analyzer. If the new folder or the default folder does not exist, it will be created and the product will be installed.
- Enter the web server port. The default port number is 8095. Ensure that the default port or the port you have selected is not occupied by some other application.
- Enter the folder name in which the product will be shown in the Program Folder. The default name is ManageEngine EventLog Analyzer.
- Enter your personal details to get assistance.

At the end of the procedure, the wizard displays the ReadMe file and starts the EventLog Analyzer server.
With this the EventLog Analyzer product installation is complete.

How to uninstall?

The procedure to uninstall for both 64 Bit and 32 Bit versions is the same.

Windows:

1. Navigate to the Program folder in which EventLog Analyzer has been installed. By default, this is Start > Programs > ManageEngine

EventLogAnalyzer <version number>.

2. Select the option Uninstall EventLogAnalyzer.
3. You will be asked to confirm your choice, after which EventLog Analyzer is uninstalled.

Linux:

1. Navigate to "<EventLogAnalyzer Home>/_ManageEngine EventLogAnalyzer_installation" directory.
2. Execute the following command in Terminal Shell.
3. You will be asked to confirm your choice, after which EventLog Analyzer is uninstalled.

Before starting EventLog Analyzer in your environment, ensure that the following are taken care of.

What are the ports required for EventLog Analyzer?

1. Primary Ports

Web Server Port

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
HTTP/8095 (configurable)	EventLog Analyzer Server	• EventLog Analyzer Technician Machine. • EventLog Analyzer Agent Machine.	Ports Usage: • The ports will by default be used for communication between the admin server and managed server, as well as between the agent and server. • The port can be customized by the user. The acceptable range for the value is between 1024–65535.

Elasticsearch

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
TCP/9300-9400 (configurable)	EventLog Analyzer Search Engine Management Node [SEM Node]	EventLog Analyzer Server	Ports Usage: • The Elasticsearch server in EventLog Analyzer uses this port. EventLog Analyzer Server and SEM can coexist on the same server. • The port can be customized by the user. The acceptable range for the value is between 1024–65535.

Internal Communication

PORT	INBOUND And OUTBOUND	Additional Rights and Permissions

PORT	INBOUND And OUTBOUND	Ports Usage: • These UDP ports are used internally by EventLog Analyzer for agent-to-server communication.
UDP/5000 (configurable)	EventLog Analyzer Server	• The port can be customized by the user. The acceptable range for the value is between 1024–65535. • Internal port bound to localhost, firewall port need not be opened.

Database

PORT	Additional Rights and Permissions
TCP/33335	Ports Usage: • Utilization of PostgreSQL/MySQL database port in order to connect to the PostgreSQL/MySQL database in EventLog Analyzer. • Firewall port need not be opened since the internal port is bound to localhost.

2. Log Collection

Windows Log Collection

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Event Log Readers • Distributed COM Users User Permissions: For root\cimv2 in WMI Properties: • Enable Account • Remote Enable • Read Security. Firewall Permissions: • Predefined Rule: Windows Management Instrumentation (WMI)
TCP/139	Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	Windows Device	EventLog Analyzer Server	SMB RPC/NP	
Dynamic ranges of RPC ports - TCP/49152 to 65,535	Windows Device	EventLog Analyzer Server	RPC randomly allocates high TCP ports for Windows Server 2008 and later versions, as well as for Windows Vista and subsequent versions	

PORTS	INBOUND	OUTBOUND	SERVICE	(WMI) Additional Rights and Permissions

Note

- It is not necessary to open outbound ports on the EventLog Analyzer agent machine and inbound ports on the EventLog Analyzer server.
- For Windows 2000, Windows XP, and Windows Server 2003, dynamic RPC ports range from 1025 to 5000.
- To enhance security across a broad spectrum of open ports, it is advisable to include the Server IP address within the firewall's scope. This ensures that only authorized traffic from the designated server is permitted through the firewall. Moreover, predefined rules with process and service filters, such as WMI,RPC,HTTP/HTTPS,Remote Event Log Management can further bolster security by allowing only specific processes or services to communicate through the designated ports. If the Server IP undergoes any changes, it is imperative to promptly update the corresponding firewall rule accordingly.

Syslog Collection

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
UDP/514 (configurable)	EventLog Analyzer Server	Target Device	Syslog	User Permissions: • The port is customizable by the user.
UDP/513 (configurable)	EventLog Analyzer Server	Target Device	Syslog	
TLS/513 (configurable)	EventLog Analyzer Server	Target Device	Syslog	
TCP/514 (configurable)	EventLog Analyzer Server	Target Device	Syslog	

SSH Communication

PERMISSION	USAGES
Ensure that the algorithm mentioned below is present in the sshd_config file. File Location: /etc/ssh/sshd_config Key exchange (KEX): diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1, diffie-hellman-group14-sha256 , diffie-hellman-group15-sha512, diffie-hellman-group16-sha512, diffie-hellman-group17-sha512, diffie-hellman-group18-sha512 , ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp52 Ciphers: aes128cbc, aes128ctr, aes192cbc, aes192ctr, aes256cbc, aes256ctr, arcfour128, arcfour256, blowfishcbc, tripledescbc MAC: hmacmd5, hmacmd596, hmacsha1, hmacsha196, hmacsha256, hmacsha512 *This will be Required for all Linux Communications.	• Linux Agent Installation • Linux Agent Management & Communication • Configuring Automatic SysLog Forwarding • Linux MYSQL Server Discovery

Configure Automatic SysLog Forwarding

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/22	Linux Device	EventLog Analyzer Server	SSH	User Rights: Service restart rights for 'rsyslog' or 'syslog' service. User Permissions: • "rw" permission should be enabled to files (/etc/rsyslog.conf or /etc/syslog.conf). • Permissions for SSH Communication

AS400 Log Collection

PORTS	INBOUND	OUTBOUND
TCP/446-449	AS400 Server	EventLog Analyzer Server
TCP/8470-8476	AS400 Serve	EventLog Analyzer Server
TCP/9470-9476	AS400 Serve	EventLog Analyzer Server

SNMP Trap Collection

PORTS	INBOUND	OUTBOUND	SERVICES	Additional Rights and Permissions
UDP/162 (configurable)	EventLog Analyzer Server	Network Device / Application	SNMP	User Permissions: • User can customize the port.

IIS Log Collection

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	IIS Server	EventLog Analyzer Server	RPC	User Permissions: • Read access to the IIS log folder should be enabled. • Permissions for the system 32/inetsrv should be enabled • Administrator share privileges are required eg : Admin$,c$
TCP/139	IIS Server	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	IIS Server	EventLog Analyzer Server	SMB RPC/NP	

3. Agent orchestration

Windows Agent Log Collection and Communication

PORTS	INBOUND	OUTBOUND	Additional Rights and Permissions
HTTP/8095 (configurable)	EventLog Analyzer Server	EventLog Analyzer Agent Machine	Environment Permission: • 8095 port should be open in both Agent machine and in Server machine.

> **Note**
>
> Communication includes tasks such as agent synchronization and checking agent status.

Windows Agent Installation & Management

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	EventLog Analyzer Agent Machine	EventLog Analyzer Server	RPC	User Permissions: • Read, write and modify permissions to files in \\ <ipaddress>\Admin$\TEMP\EventLogAgent should be enabled. • Access "Remote Registry" service • At least read control should be granted for winreg registry key. (Computer \HKEY_LOCAL _MACHINE\ SYSTEM\ CurrentContro lSet\Control\ SecurePipe Servers\winreg). • Read/Write registry keys - SOFTWARE\\ Wow6432Node \\ZOHO Corp\\EventLog Analyzer\\ (or) SOFTWARE \\ZOHO Corp \\EventLog Analyzer\\. • There should be access to remote services.msc
TCP/139	EventLog Analyzer Agent Machine	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	EventLog Analyzer Agent Machine	EventLog Analyzer Server	SMB RPC/NP	
Dynamic ranges of RPC ports - TCP/49152 to 65,535	EventLog Analyzer Agent Machine	EventLog Analyzer Server	RPC randomly allocates high TCP ports for Windows Server 2008 and later versions, as well as for Windows Vista and subsequent versions	

Note

Management involves actions like starting, stopping, or uninstalling the agent software.

Linux Agent Installation

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/22	EventLog Analyzer Agent Machine	EventLog Analyzer Server	SSH	Sudo User Permissions: • "rwx" permission is required for /opt/ManageEngine/ for transferring files. • Permissions for SSH Communication

Linux Agent Management & Communication

PORTS	INBOUND	OUTBOUND	Additional Rights and Permissions
TCP/22	EventLog Analyzer Server	EventLog Analyzer Server	User Permissions: • SFTP permissions to transfer files to /opt/Manage Engine/EventL ogAnalyzer_ Agent and /etc /audisp/plugins.d • Service start/stop/restart permission for auditd. • Permissions for SSH Communication
HTTP/8095 (configurable)	EventLog Analyzer Server	EventLog Analyzer Agent Machine	

4. Importing logs

Importing Logs using SMB

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/137	Target Device	EventLog Analyzer Server	NetBIOS name resolution RPC/named pipes (NP)	User Permissions: • Network access: Do not allow anonymous not allow anonymous enumeration of SAM accounts and shares. • Sometimes, connecting to different workgroup needs credentials even to view the shared resources.
TCP/138	Target Device	EventLog Analyzer Server	NetBIOS datagram	
TCP/139	Target Device	EventLog Analyzer Server	NetBIOS session RPC/NP	

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/445	Target Device	EventLog Analyzer Server	SMB RPC/NP	

Importing logs using FTP

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/20	Target Device	EventLog Analyzer Server	FTP/SFTP	User Permissions: • SAuthentication for the FTP server should be enabled.
TCP/21	Target Device	EventLog Analyzer Server	FTP/SFTP	

5. Discovery

Windows Domain Discovery

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/389	Domain Controller	EventLog Analyzer Server	LDAP	User Permissions: • User should have read permission to Active Directory Domain Objects. • Permission to run LDAP query in ADS_ SECURE_AUTHENTICATION mode should be present.

Windows Workgroup Discovery

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	Workgroup Server	EventLog Analyzer Server	RPC	User Permissions: • User should have read permission to Active Directory Domain Objects. • Permission to run WinNT query in ADS_ SECURE_ AUTHENTI CATION mode should be given.
TCP/139	Workgroup Server	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	Workgroup Server	EventLog Analyzer Server	SMB RPC/NP	
[illegible]	Workgroup	EventLog	RPC randomly	

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/1024-65535	Server	Analyzer Server	allocated high TCP ports	

Event Source Discovery

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	Target Windows Device	EventLog Analyzer Server	RPC	User Permissions: • The winreg registry key should at the very least be given read control.
TCP/137	Target Windows Device	EventLog Analyzer Server	NetBIOS name resolution RPC/named pipes (NP)	
TCP/138	Target Windows Device	EventLog Analyzer Server	NetBIOS datagram	
TCP/139	Workgroup Server	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	Workgroup Server	EventLog Analyzer Server	SMB RPC/NP	

MSSQL Server Discovery-Windows

PORTS	INBOUND	OUTBOUND	Additional Rights and Permissions
UDP/1434	MSSql Server	EventLog Analyzer Server	User Permissions: • Can be configured to use dynamic TCP ports for communication.
TCP/1433	MSSql Server	EventLog Analyzer Server	

Network Device Discovery

PORTS	INBOUND	OUTBOUND	Additional Rights and Permissions
UDP/162	Network Devices	EventLog Analyzer Server	Ports Usage:: • Fetches a list of live SNMP-enabled IP devices that responds to the SNMP ping.

IIS Discovery

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/445	IIS Server	EventLog Analyzer Server	SMB RPC/NP	Ports Usage: • The Server Message Block (SMB) protocol uses this port to read the log files.

MYSQL Server Discovery-Windows

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	MySql Server	EventLog Analyzer Server	RPC	User Permissions: • WMI permission is needed to find the MySQL server configuration file using SFTP.
TCP/445	MySql Server	EventLog Analyzer Server	SMB RPC/NP	

MYSQL Server Discovery-Linux

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/22	MySql Server	EventLog Analyzer Server	SMB RPC/NP	User Permissions: • Read permission to the MySQL server configuration file using SFTP. • Permissions for SSH Communication

6. Incident Workflow Management

NETWORK ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND
PING DEVICE	ICMP/No ports	Audited Windows / Linux Device	EventLog Analyzer Server
TRACE ROUTE WINDOWS	ICMP/No ports	Audited Windows Device	EventLog Analyzer Server
TRACE ROUTE LINUX	UDP/33434 -33534	Audited Linux Device	EventLog Analyzer Server

WINDOWS ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • The computer should not include EventLog Analyzer Installed server.
LogOff	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
Shutdown and Restart	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • The computer should not include EventLog Analyzer Installed server
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
Execute Windows Script	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows	EventLog Analyzer	SMB RPC/NP	

BLOCK	PORT	Device INBOUND	Server OUTBOUND	RPC/NP SERVICE	Additional Rights and Permissions
					Environment Permission: • Read Security
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	• The user should have read,write and modify access to the shared path in the script.
Disable USB	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • Remote Registry Service should be running. • Full Control permission to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
ALL SERVICE BLOCK	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users • Administrators User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	

BLOCK	PORT	INBOUND Audited	OUTBOUND EventLog	SERVICE	Additional Rights and Permissions
START PROCESS	TCP/135	Windows Device	Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
STOP PROCESS	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
TEST PROCESS	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
		Audited	EventLog	SMB	

BLOCK	PORT	INBOUND	OUTBOUND	RPC/NP SERVICE	Additional Rights and Permissions
	TCP/445	Windows Device	Analyzer Server		• Enable Account • Remote Enable
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	• Read Security

LINUX ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
Shutdown and Restart	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: The user should be the root user.
Execute Windows Script	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: Sudo permission for user.
ALL SERVICE BLOCK	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: Sudo permission.
START PROCESS	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: The permission to execute the command should be available for the user whose credentials are provided.
STOP PROCESS	Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: The permission to execute the command should be available for the user whose credentials are provided.
TEST PROCESS	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	-

NOTIFICATIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
		Audited	EventLog		UserGroups:

BLOCK	TCP/135 PORT	Linux INBOUND Device	Analyzer OUTBOUND Server	RPC SERVICE	• Distributed COM Users Additional Rights and Permissions User Permissions
Pop Up WINODWS	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • "AllowRemoteRPC" should be 1 for HKEY_ LOCAL_MACHINE\ SYSTEM\Current ControlSet\Control\Terminal Server.
Pop Up LINUX	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: Sudo permission for user.
Send Email WINDOWS & LINUX	TCP/Port mentioned while config using SMTP server	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: SMTP server should be configured on Event log analyzer server
Send SMS WINDOWS & LINUX	-	-	-	-	Environment Permission: SMS Server should be configured in the product.
Send SNMP Trap WINDOWS & LINUX	UDP/Port specified in workflow block	Audited Windows / Linux Device	EventLog Analyzer Server	-	Environment Permission: The port mentioned in workflow configuration should be open.

AD ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
DELETE AD USER WINDOWS	TCP/389	Audited Domain Controller	EventLog Analyzer Server	LDAP	User Permissions: • The user should have "Delete" Right in the AD to delete other Accounts. • The user to delete should not have "Protect Object from accidental deletion" checked.

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	User Permissions: Additional Rights and Permissions
DISABLE AD USER WINDOWS	TCP/389	Audited Domain Controller	EventLog Analyzer Server	LDAP	• The User account provided should have "Read","Write ","modify owners" and "modify permissions" permissions enabled.
DISABLE USER COMPUTER WINDOWS & LINUX	TCP/389	Audited Domain Controller	EventLog Analyzer Server	LDAP	User Permission: • The User account provided should have "Read", "Write" , "modify owners" and "modify permissions" permissions enabled.

MISCELLANEOUS ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
WRITE TO FILE WINDOWS	TCP/135	Audited Windows Device	EventLog Analyzer Server	UserGroups: • Distributed COM Users User Rights: • Act as part of the operating system • Log on as a batch job • Log on as a service • Replace a process level token. User Permissions: For root\cim v2 In Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • The user should have read,write and modify access to the shared path.
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	
WRITE TO FILE LINUX	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	Environment Permission: • Sudo permission for user
HTTP WebHook	-	-	-	Environment Permission: • A "connect" Socket Permission to the host/port combination of the destination URL or a "URL Permission" that permits this request.

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
FORWARD LOGS	TCP/Specified Port	Audited Windows / Linux Device	EventLog Analyzer Server	-
CSV LOOKUP	TCP/Specified Port	Audited Windows / Linux Device	EventLog Analyzer Server	User Permissions: • Read permission to the specified CSV file.

FIREWALL ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
Cisco ASA deny inbound/Outbound rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: https://www.manageengine.com/products/eventlog/help/threat-intelligence-and-analytics/threat-response/incident-management/playbook-management.html#ciscoCredentials
Fortigate deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: https://www.manageengine.com/products/eventlog/help/threat-intelligence-and-analytics/threat-response/incident-management/playbook-management.html#fortigateCredentials
Palo Alto deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: https://www.manageengine.com/products/eventlog/help/threat-intelligence-and-analytics/threat-response/incident-management/playbook-management.html#paloAltoCredentials
Sophos XG deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: https://www.manageengine.com/products/eventlog/help/threat-intelligence-and-analytics/threat-response/incident-management/playbook-management.html#sophosXGCredentials
Barracuda deny Access rules	https/8443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: https://www.manageengine.com/products/eventlog/help/threat-intelligence-and-analytics/threat-response/incident-management/playbook-

BLOCK	PORT	INBOUND	OUTBOUND	management.html#fortigateCredentials Additional Rights and Permissions

7. Distributed communication Setup

Distributed

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
HTTP/8095 (configurable)	EventLog Analyzer Managed Server Machine	EventLog Analyzer Admin Server Machine	User Permissions: • Managed server to Admin server communication via default webserver port. • The default port number is 8095. • The port can be customized by the user.
HTTP/8095 (configurable)	EventLog Analyzer Admin Server Machine	EventLog Analyzer Managed Server Machine	User Permissions: • Admin server to Managed server communication via default webserver port • User can customize the port. The value should be between 1024 and 65535.

Centralized Archiving Port

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
SSH/8080 (configurable)	EventLog Analyzer Admin Server Machine	EventLog Analyzer Managed Server Machine	User Permissions: • Managed server transfers the archive files to Admin Server via SSH 8080. • User can customize the port. The value should be between 1024 and 65535.

Using EventLog Analyzer with Antivirus Applications

To ensure unhindered functioning of EventLog Analyzer, you need to add the following files to the exception list of your Antivirus application:

Path	Need for whitelisting	Impact if not whitelisted
<ELA_HOME>/ES/data	Elasticsearch indexed data is stored.	All the collected logs will not be available if the data is deleted.
<ELA_HOME>/ES/repo	Elasticsearch index snapshot is taken at this location.	Snapshots and Elasticsearch archival feature will fail if the files at

Path	Need for whitelisting	Impact if not whitelisted
<ELA_HOME>/ES/archive	Elasticsearch archives are stored here.	Archived log data will not be available if the files located here are deleted.
<ME>/elasticsearch/ES/data	Elasticsearch indexed data is stored.	Reports would be affected if the data is deleted.
<ME>/elasticsearch/ES/repo	Elasticsearch index snapshot is taken at this location.	Snapshots and Elasticsearch archival feature will fail if the files at this location are deleted.
<ME>/elasticsearch/ES/archive	Elasticsearch archives are stored here.	Data will not be available if the files located here are deleted.
<ELA_HOME>/data/za/threatfeeds	Bundled files containing a list of malicious IPs, domains and URLs that will be used in case there is no internet connectivity will be stored here. These files will be deleted on the first default threat feed synchronization. Whitelisting is required only till first synchronization.	If the files are removed and if there is no internet connectivity, then the list of malicious threat sources will be missed from the dataset.
<ELA_HOME>/data/AlertDump	Formatted logs are stored before processing for alerts. Might be detected as false positive by Antivirus applications.	If the file is quarantined or deleted, related alerts would be missed.
<ELA_HOME>/data/NotificationDump	Formatted logs are stored before processing for notification. Might be detected as false positive by Antivirus applications.	If the file is quarantined or deleted, notification for triggered alerts would be missed.
<ELA_HOME>/bin	All binaries are included here. Some Antivirus applications might block them as false positive.	Product might not function.
<ELA_HOME>/data/imworkflow	Binaries uploaded by users for workflow execution are stored here.	Script Alert workflow might not work as intended.
<ELA_HOME>/pgsql/bin	Postgres binaries are included here. Might be detected as false positive by Antivirus applications.	Product might not start.
<ELA_HOME>/lib/native	All binaries are included here. Some Antivirus applications might block them as false positive.	Product might not function.

Path	Need for whitelisting	Impact if not whitelisted
<ELA_HOME>/archive (If the archive folder is moved to a new location, add the new location)	Antivirus applications might slow down frequent write operations.	Performance issues might occur in the product if the Antivirus applications slow down write operations.
<ELA_HOME>/troubleshooting	All troubleshooting binaries are included here. Some Antivirus applications might block them as false positive.	Some troubleshooting batch files might not work.
<ELA_HOME>/tools	All tools binaries are included here. Some Antivirus applications might block them as false positive.	Some tools might not work if the files are removed by Antivirus applications.
<ELA_HOME>/ES/CachedRecord	Antivirus applications might slow down frequent write operations.	Performance issues might occur in the product if the Antivirus applications slow down write operations.

For Windows agent machine - 64 bit,

Path	Need for whitelisting	Impact if not whitelisted
C:\Program Files (x86)\EventLogAnalyzer_Agent\bin	Agent binaries are stored here.	The Agent might not work if the files are quarantined.
C:\Program Files (x86)\EventLogAnalyzer_Agent\bin\data	Antivirus applications might slow down frequent write operations.	Performance issues might occur in the product if the Antivirus applications slow down write operations.
C:\TEMP\\EventLogAgent	Agent installation files are moved for installation and upgrade.	Agent might not upgrade/not install if the files are quarantined.

For Windows agent machine - 32 bit,

Path	Need for whitelisting	Impact if not whitelisted
C:\Program Files\EventLogAnalyzer_Agent\bin	Agent binaries are stored here.	The Agent might not work if the files are quarantined.
C:\Program Files (x86)\EventLogAnalyzer_Agent\bin\data	Antivirus applications might slow down frequent write operations.	Performance issues might occur in the product if the Antivirus applications slow down write operations.
C:\TEMP\\EventLogAgent	Agent installation files are moved for installation and upgrade.	Agent might not upgrade/not install if the files are quarantined.

Path	Need for whitelisting	Impact if not whitelisted

For Linux agent,

Path	Need for whitelisting	Impact if not whitelisted
/opt/ManageEngine/EventLogAnalyzer_Agent/bin	Agent binaries are stored here.	The Agent might not work if the files are quarantined.
/opt/ManageEngine/EventLogAnalyzer_Agent/bin/data	Antivirus applications might slow down frequent write operations.	Performance issues might occur in the product if the Antivirus applications slow down write operations.

8. Advanced threat analytics

PORT	Additional Rights and Permissions
HTTPS/443	To fetch the "Log360 Cloud Threat Analytics" feeds, the below URLs will be used • https://log360cloud.manageengine.com/ • https://log360feeds.manageengine.com/

5.2.2. How to Start and Shutdown EventLog Analyzer

Last updated on: September 12, 2025

In this page

How to install EventLog Analyzer?

How to uninstall EventLog Analyzer?

Once you have successfully installed EventLog Analyzer, start the EventLog Analyzer server by following the steps below.

How to start EventLog Analyzer Server/Service

Windows Application:

- Select the desktop shortcut icon for EventLog Analyzer to start the server. (or)
- Select Start > Programs > ManageEngine Log360 <version number> > Log360 to start the server.
- If the server is started and you wish to access it, you can use the tray icon in the task bar to connect to EventLog Analyzer.

Windows Service:

During installation, you would have chosen to install EventLog Analyzer as an application or a service. If you installed it as an application, you can carry out the procedure to convert the software installation to a Windows Service.
Once the software is installed as a service, follow the steps given below to start EventLog Analyzer as a Windows Service:

- Go to the Windows Control Panel > Administrative Tools > Services.
- Right click ManageEngine EventLog Analyzer <version number> and select Start in the menu.
- Alternatively, right click and select Properties. In the General tab, check the Service status is ‘Stopped’ and Start button is in enabled state and other buttons are grayed out. Click the Start button to start the server as a Windows service.

Linux Application:

- For Linux, based on where EventLog Analyzer has been installed, the steps to start the server are as follows.

Installed in	Users who can start	How to Start
		Root user: Navigate to the <Eventlog Analyzer>/bin directory and execute the configureAsService.sh file with root user privileges. Then restart the server using the shutdown.sh and service start commands to

Installed in	Users who can start	How to Start
Top level directories like /opt, /home , /, and others	Root User: Yes Other User: Yes	start using service. Other users: * Open a terminal.* Navigate to the <Eventlog Analyzer>/ES/bin directory, run sudo initES.sh. Alternatively, you can also run initES.sh using root.* Navigate to the <Eventlog Analyzer>/bin directory and execute the run.sh file or start using service.
Home of a user For example, /home/testuser/Eventlog or /home/Admin/Eventlog or any other directory that comes under a user's home directory	User who owns the home directory: Yes Root user: No (Because in redhat & centos a user can't access files of another user since an Elasticsearch user is created when a user is running the application with root. The Elasticsearch user wont be able access their home directory as it's part of another home directory.	Root user: Should not run Other users: * Open a terminal. * Navigate to the <Eventlog Analyzer>/ES/bin</Eventlog> directory, run sudo initES.sh. Alternatively, you can also run initES.sh using root.

- When the respective run.sh file is executed, a command window opens up and displays the startup information of several EventLog Analyzer modules. Once all the modules are successfully started, the following message is displayed:

Server started.
Please connect your client at http://localdevice:8095

- The 8095 port is replaced by the port you have specified as the web server port during installation.

> Note
>
> If the default syslog listener port of EventLog Analyzer is not free then EventLog Analyzer displays "Can't Bind to Port <Port Number>" when logging in to the UI.

Linux Service:

During installation, you would have chosen to install EventLog Analyzer as an application or a service. If you installed it as an application, follow the procedure given below to convert the software installation to a Linux Service. Navigate to the bin folder and execute the following command:

- Once the software is installed as a service, execute the command given below to start Linux Service:
- Check the status of the EventLog Analyzer service by executing the following command (sample output given below):

How to shut down EventLog Analyzer Server/Service

Follow the steps below to shut down the EventLog Analyzer server. Note that once the server is successfully shut down, the PostgreSQL/MySQL database connection is automatically closed, and all the ports used by EventLog Analyzer are freed.

Windows Application:

- Navigate to the Program folder in which EventLog Analyzer has been installed. By default, this is Start > Programs > ManageEngine Log360 <version number>. Select the Shut Down EventLog Analyzer option.
- Alternatively, you can navigate to the <EventLog Analyzer Home>\bin folder and execute the shutdown.bat file. You will be asked to confirm your choice, after which the EventLog Analyzer server is shut down.

Windows Service:

To stop a Windows service, follow the steps given below.

- Go to the Windows Control Panel. Select Administrative Tools > Services.
- Right click ManageEngine EventLog Analyzer <version number>, and select Stop in the menu.
- Alternatively, right click and select Properties. In the General tab of the screen, check the Service status is 'Started' and the Stop button is in enabled state and other buttons are grayed out. Click the Stop button to stop the Windows service.

Linux Application:

- Navigate to the <EventLog Analyzer Home>\bin directory. Execute the shutdown.sh file.
- You will be asked to confirm your choice, after which the EventLog Analyzer server is shut down.

Linux Service:

Execute the commands given below to stop the Linux service (sample outputs are given):

- Stop the service

Stopping ManageEngine EventLog Analyzer <version number>...
Stopped ManageEngine EventLog Analyzer <version number>

- Check the status of the service again:

ManageEngine EventLog Analyzer <version number> is not running.

How to restart EventLog Analyzer Server/Service

1. Stop EventLog Analyzer:
   - For the console application

     Windows
   - Find the EventLog client from the process list.
   - Right click on this and select shutdown. (or)

- Use the Direct Call option.

  Linux:
- Use the Direct Call option.

  Direct Call:
- Go to <EventLog Analyzer Home>\bin.
- Execute the shutdown.bat file.
- Wait till the process completes.

  For the service mode:
- Go to the service console.
- Find the ManageEngine EventLog Analyzer service.
- Click on 'Stop'.

2. Start EventLog Analyzer:
   - For the console application:

     Direct Call:
   - Click on the shortcut icon. (or)
   - Go to <EventLog Analyzer Home>\bin.
   - Execute wrapper.exe ..\server\conf\wrapper.conf

     > **Note**
     >
     > You can also execute run.bat but this is not preferred.

     For the service mode:
   - Go to the service console.
   - Find the ManageEngine EventLog Analyzer service.
   - Click on 'Start'.

5.2.3. Access EventLog Analyzer Server

Last updated on: September 12, 2025

Once the server has successfully started, follow the steps below to access EventLog Analyzer.

- Open a supported web browser. Type the URL address as http://<devicename>:8095 (where <devicename> is the name of the machine in which EventLog Analyzer is running, and 8095 is the default web server port)
- You can also open EventLog Analyzer from the EventLog Analyzer shortcut available in the desktop.
- Log in to EventLog Analyzer using the default username/password combination of admin/admin.
- If you import users from Active Directory or add RADIUS server details, you will find that the options are listed in the Log on to field (below the Password field). In this case, enter the User Name, Password, and select one of the three options in Log on to (Local Authentication or Radius Authentication or Domain Name). Click the Login button to connect to EventLog Analyzer.

EventLog Analyzer provides two external authentication options apart from the local authentication. They are Active Directory and Remote Authentication Dial-in User Service (RADIUS) authentication. The Log on to field will list the following options:

- Local Authentication - If the user details are available in the local EventLog Analyzer server user database.
- Radius Authentication - If the user details are available in a RADIUS server and dummy user entries are available in the local EventLog Analyzer server user database.
- Domain Name(s) - If the user details of a domain are imported from Active Directory into the local EventLog Analyzer server user database.

Once you log in, you can start collecting logs, generating reports and more.

5.3.1.1. Reverse proxy

Last updated on: September 12, 2025

In this page

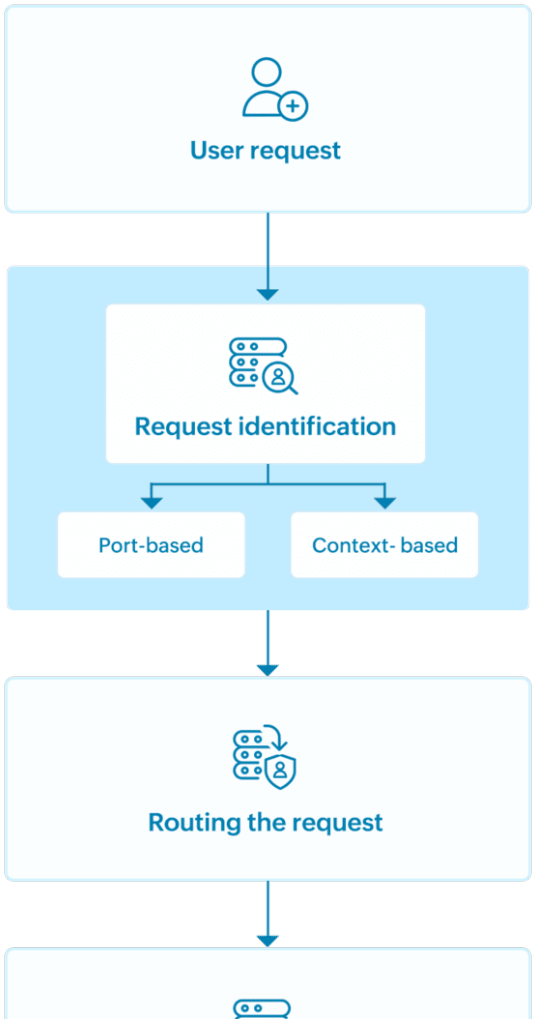
Overview

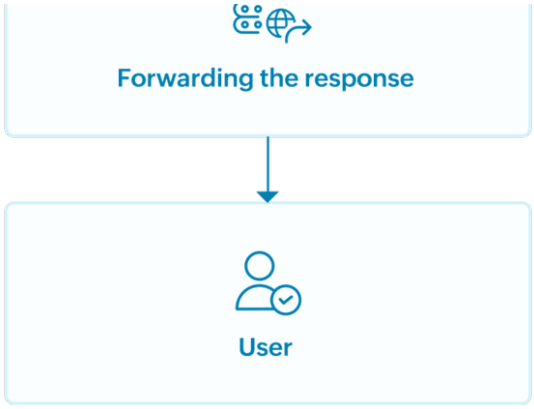
Architecture

Overview

A reverse proxy acts as an intermediary between clients and backend servers. It accepts incoming client requests, forwards them to the appropriate backend servers, and then returns the server's responses to the clients without revealing the identity or details of those backend servers.
ManageEngine Log360 uses a reverse proxy to safeguard internal ports and server details, ensuring secure communication.

Architecture





- User request: Users send requests using an access URL.
- Request identification: The reverse proxy examines the request and determines the target backend server.
  - Port-based: Based on the external port.
  - Context-based: Based on the URL path.
- Routing the request: The reverse proxy forwards the request to the correct backend server.
- Backend processing: Web servers process the request and generate a response.
- Forwarding the response : The reverse proxy returns the response to the user using the original access URL, hiding internal server details.

Log360 supports two types of reverse proxy configurations:

1. Context-based reverse proxy
2. Port-based reverse proxy.

Context-based reverse proxy

In context-based reverse proxy, users access different components using unique paths appended to the same domain.
All user requests are received through a single external port on the reverse proxy server. The proxy then routes the requests internally to the correct backend service based on the URL path.
This setup conceals all internal port numbers and server details, ensuring secure communication.

Port-based reverse proxy

In port-based reverse proxy, users access different components by connecting to different external ports on the same hostname.
Each external port corresponds to a specific server. The reverse proxy listens on these ports and routes requests internally to the requested component.
Despite the use of multiple external ports, internal port numbers and server details remain concealed. The hostname stays consistent across all services, maintaining confidentiality and security.
Read also
This document explained how Log360 uses a reverse proxy to secure communication. To learn how to manage the reverse proxy in Log360, refer to this document:

- Managing reverse proxy

5.3.1.2. Managing reverse proxy

Last updated on: September 12, 2025

In this page

Overview

Enabling context-based reverse proxy

Enabling port-based reverse proxy

Disabling reverse proxy

Overview

This page explains how to configure a reverse proxy in the product console and details the steps to enable and disable it. Reverse proxy can be configured using context-based mode, port-based mode, or both, based on your deployment needs.

Enabling context-based reverse proxy

1. Log into the product console as an administrator.
2. Navigate to the Settings tab.
3. Under System Settings, click Reverse Proxy.

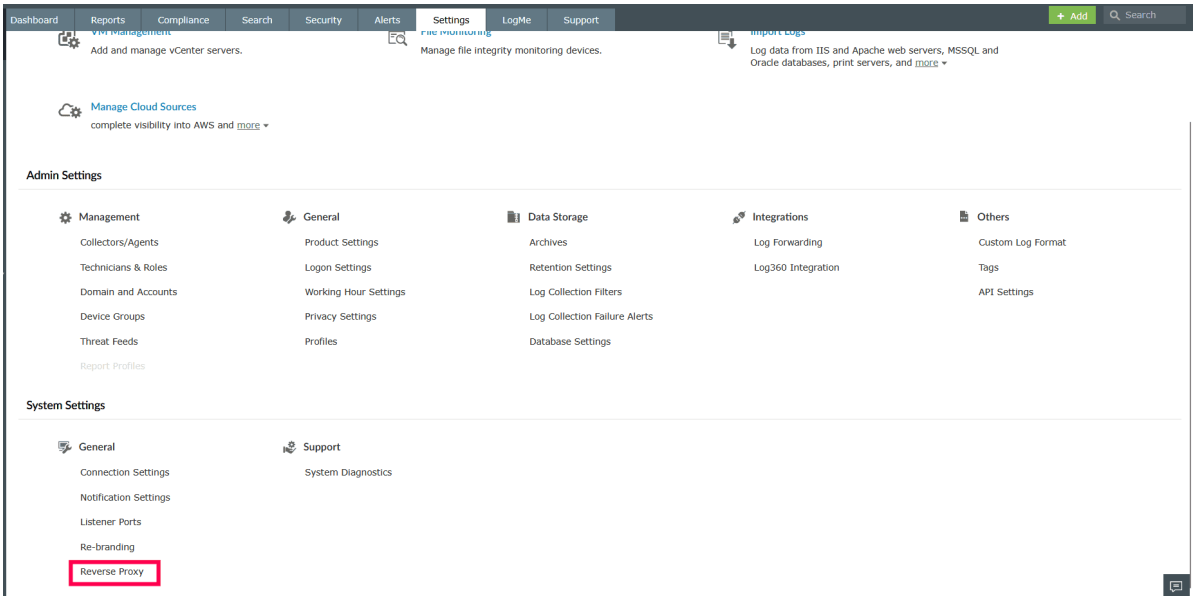


Figure 1: Enabling reverse proxy

4. In the Context-Based tab, select the checkbox Enable Context-Based Reverse Proxy.



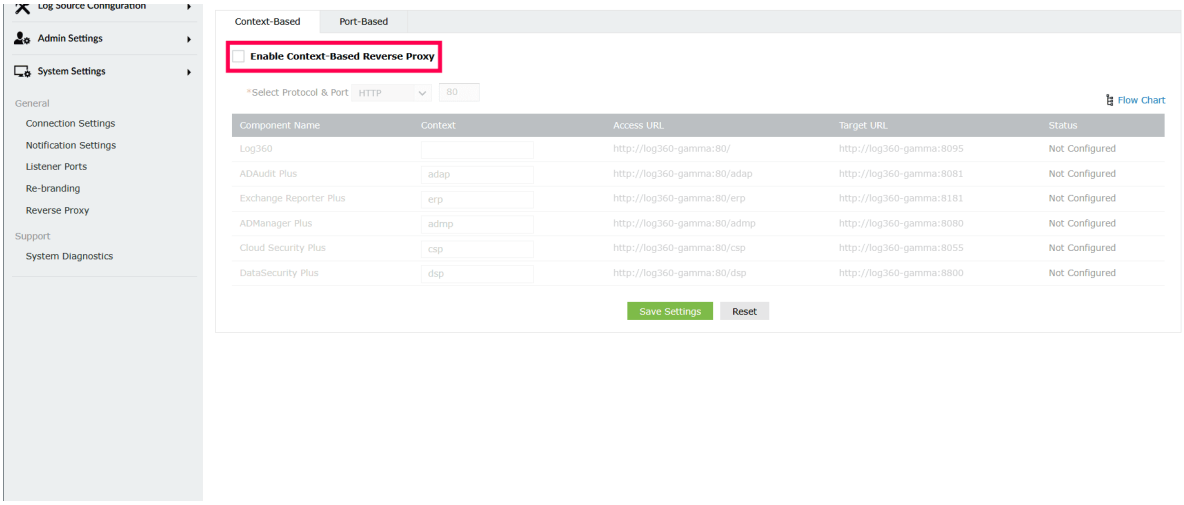


Figure 2: Enabling context-based reverse proxy

5. From the Protocol dropdown, choose the required protocol (HTTP or HTTPS).

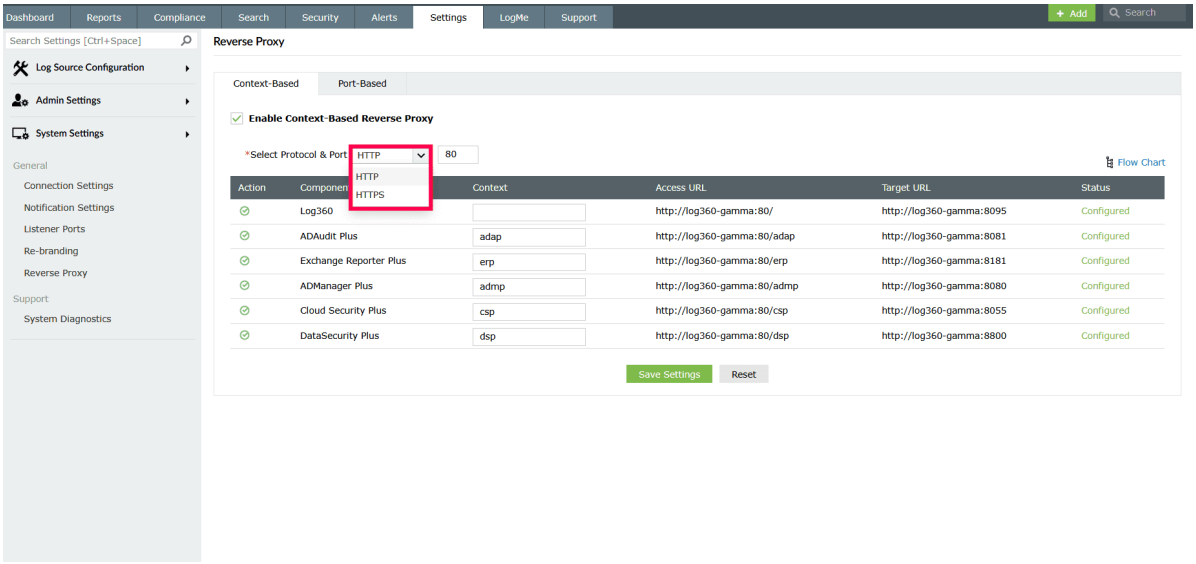


Figure 3: Selecting protocol for context-based reverse proxy

6. In the Port field, enter a port number that is not used by other applications.

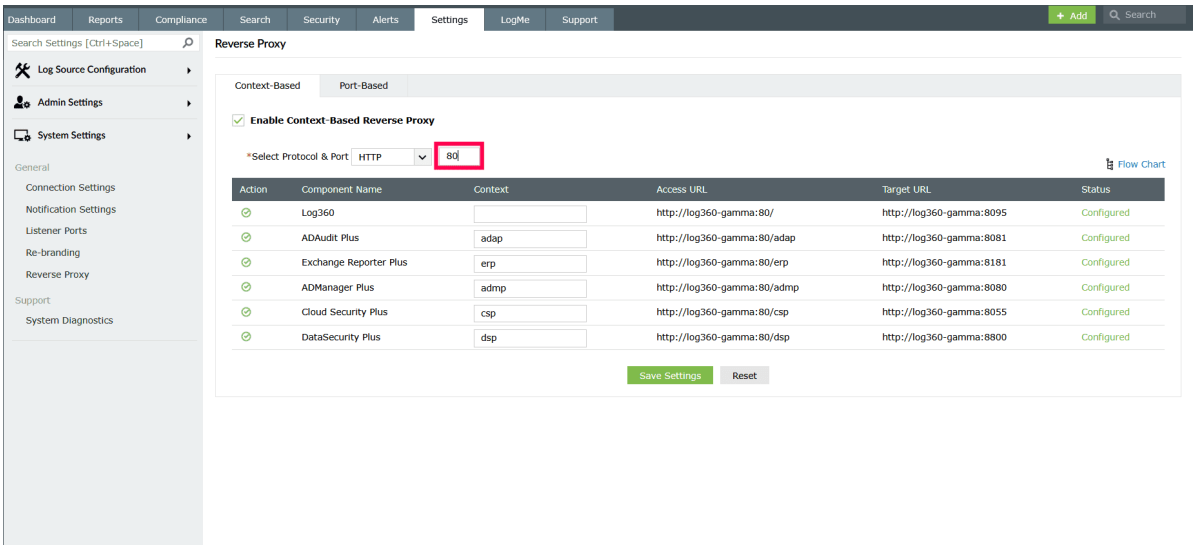


Figure 4: Configuring port number

7. Under the Context column, provide a unique context path for the product and each integrated component.

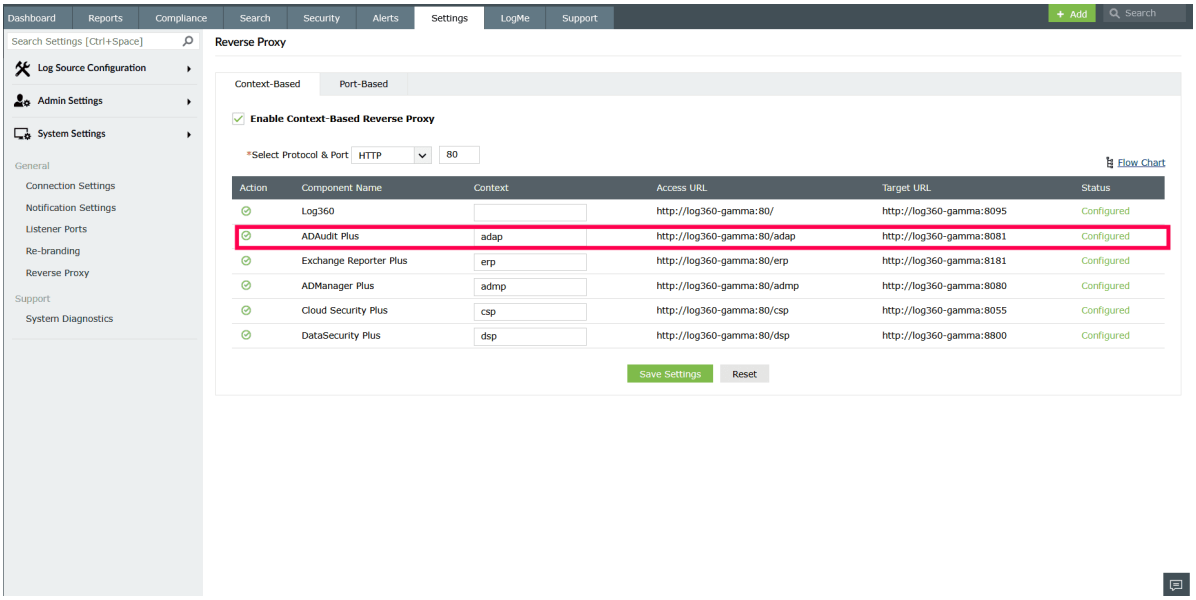


Figure 5: Configuring context path

8. Note down the Access URLs displayed for each component. These URLs will be used by external users.

9. Click Save Settings to apply the configuration.

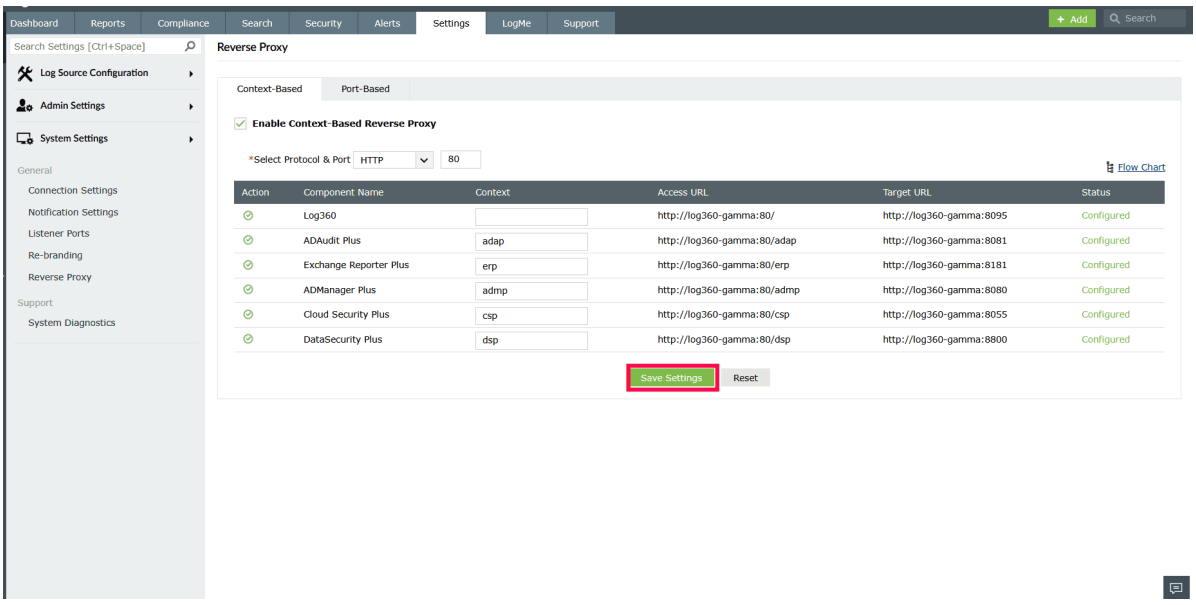


Figure 6: Enabling context-based reverse proxy

Enabling port-based reverse proxy

1. Log into the product console as an administrator.

2. Navigate to the Settings tab.

3. Under System Settings, click Reverse Proxy.

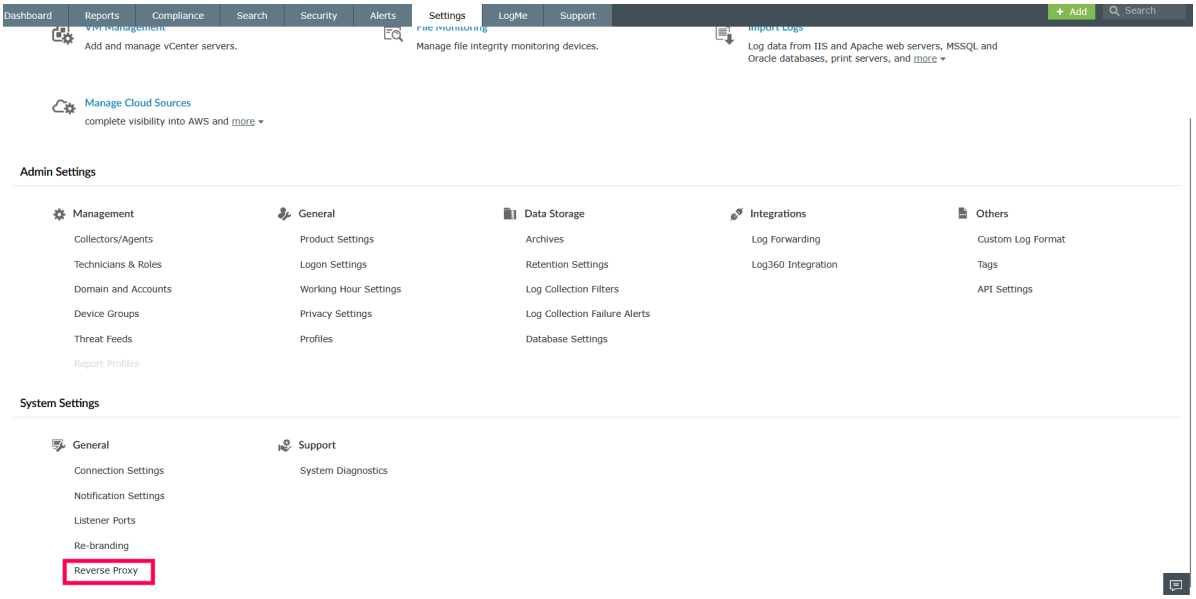


Figure 7: Enabling reverse proxy

4. In the Port-Based tab, select the checkbox Enable Port-Based Reverse Proxy.

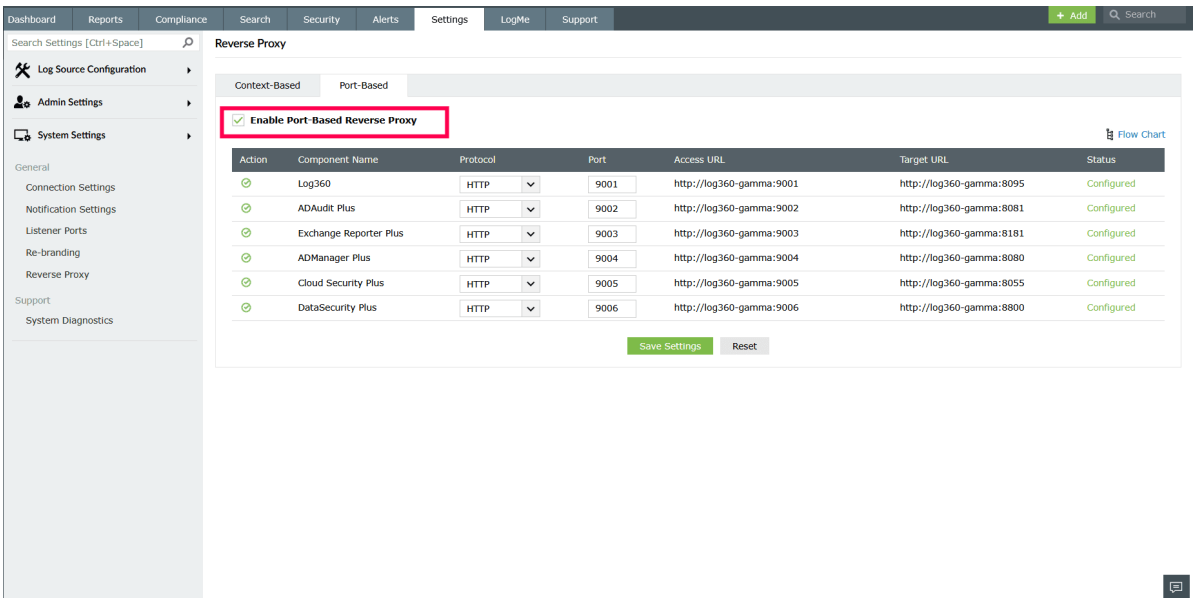
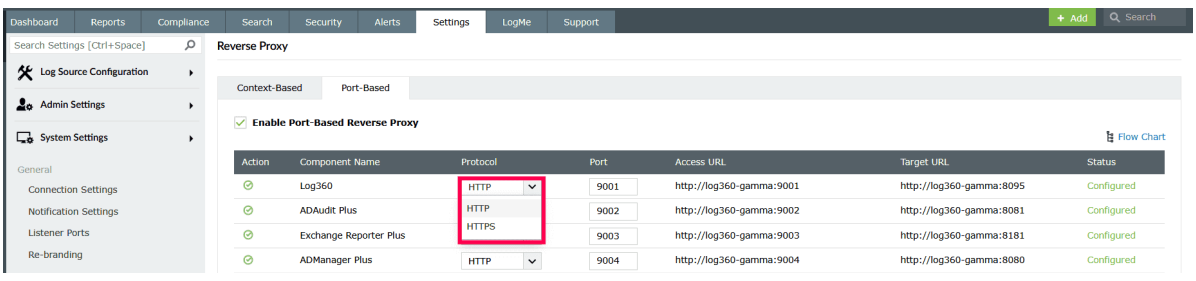


Figure 8: Enabling port-based reverse proxy

5. In the Protocol column, select the required protocol (HTTP or HTTPS) for each component.



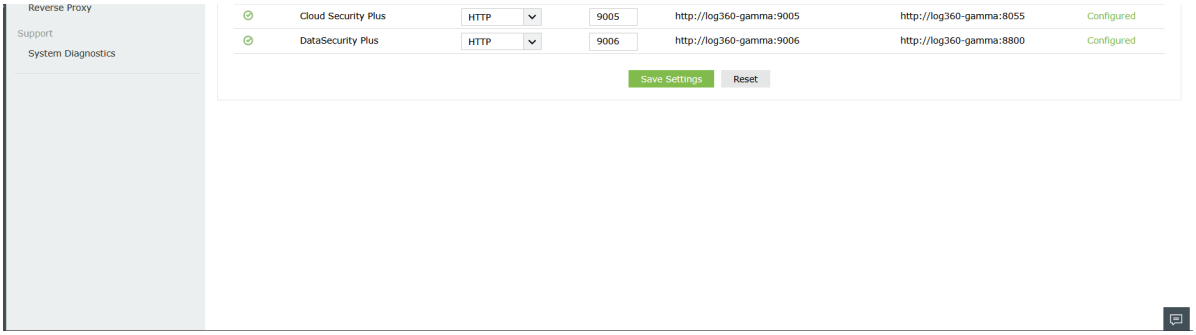


Figure 9: Selecting protocol for port-based reverse proxy

6. In the Port column, enter a unique port number for the product and its integrated components. Ensure the port numbers are not used by other applications.

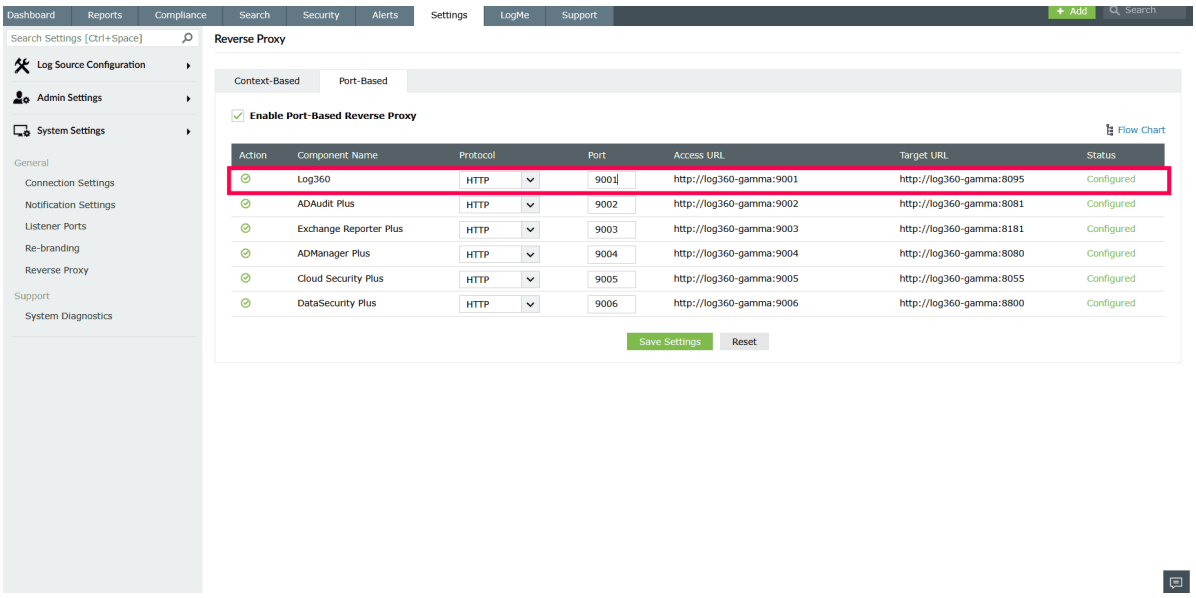


Figure 10: Configuring port number

7. Note down the Access URLs displayed for each component. These URLs will be used by external users.
8. Click Save Settings to apply the configuration.

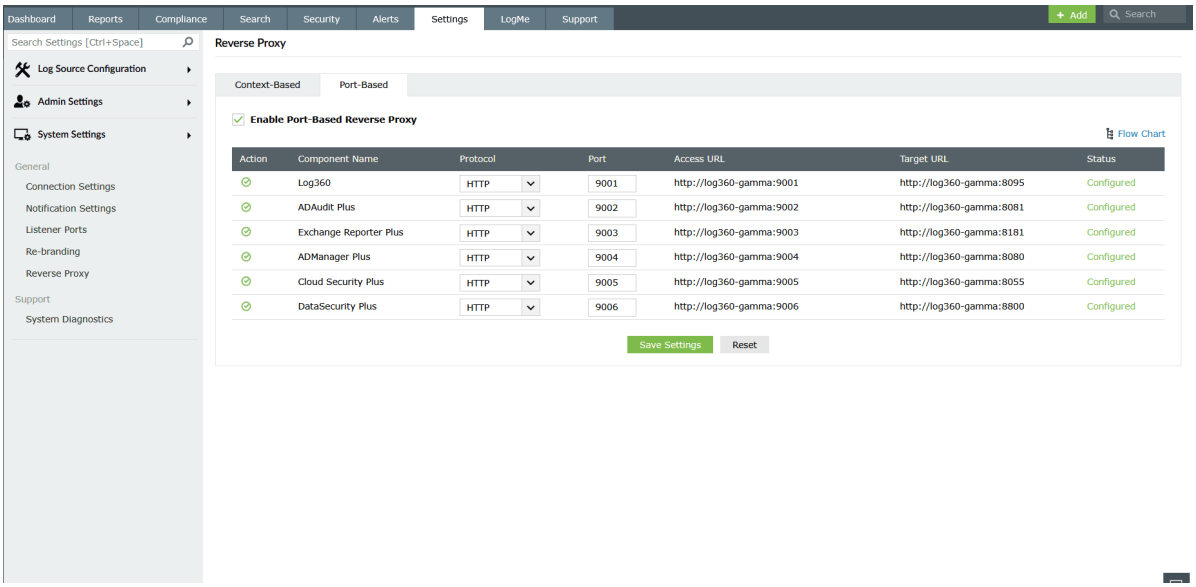


Figure 11: Enabling port-based reverse proxy

Disabling reverse proxy

1. In the Reverse Proxy page, locate the component you want to disable.
2. Under the Actions column, click the icon to disable the reverse proxy.
3. The component's Status will change to Not Configured.

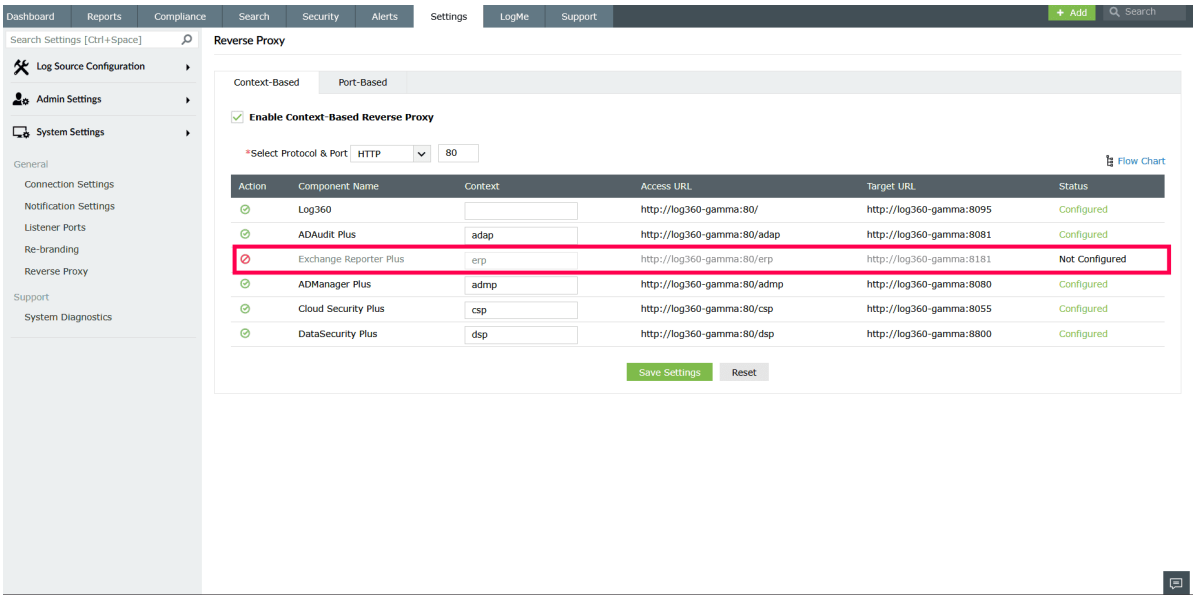


Figure 12: Disabling a reverse proxy

4. Click Save Settings to apply the changes.

Read also

This document explained how to manage the reverse proxy in Log360. To learn how Log360 uses a reverse proxy to secure communication.

- Overview

5.4.1. Overview

Last updated on: September 12, 2025

Log360 is a unified SIEM solution that integrates multiple security and IT management components under a single console. It supports the integration of the following six components:

Component	Description
ADAudit Plus	ADAudit Plus is a real-time change auditing and user behavior analytics solution that helps keep your Active Directory, Azure AD, member servers, file servers, and workstations secure and compliant.
ADManager Plus	ADManager Plus is an enterprise Identity Governance and Administration (IGA) solution that comes with AD management, access certification, risk assessment, risk exposure management, identity life cycle management, workflow orchestration, and integration capabilities to streamline identity management effortlessly.
DataSecurity Plus	Provides data visibility and security through file server auditing, data discovery, and leak prevention. Monitors file integrity, reviews permissions, and blocks sensitive data leaks to meet compliance needs.
Exchange Reporter Plus	A comprehensive reporting, change auditing, and monitoring solution for Exchange Server, Exchange Online, and Skype for Business Server.
Cloud Security Plus	Provides complete visibility into AWS and Azure environments, with reports, search, and customizable alerts to monitor, analyze, and respond to cloud security events.
PAM360	A privileged access security solution that enables businesses to identify and prevent exploitation of any unmanaged, unmonitored, and unknown privileged access pathways to mission-critical assets.

Integrating these components allows administrators to manage all modules from one platform, enable data synchronization across components, and streamline navigation between the modules.

Key benefits of integration:

1. Data synchronization across components

When components are integrated, Log360 automatically synchronizes key configuration details across all modules. This eliminates the need to repeat the same setup steps multiple times and ensures consistency throughout the environment. Any update made in one component is reflected across all others.

throughout the environment. Any update made in one component is reflected across all others.
Two critical settings are synchronized:

- Domain settings: Adding or updating a domain in any component automatically applies the change to all others. Administrator credentials associated with the domain are also synchronized.
- Integration settings: These settings define how different components communicate with each other for features like single sign-on, domain sharing, and secure data exchange. Parameters such as hostnames, port numbers, and connection protocols must remain aligned across all components to ensure uninterrupted interaction. With integration, any updates made to these details on the Log360 Integration page are automatically applied to every component, eliminating the need for manual updates in multiple consoles.

2. Unified access

Integration enables administrators to access all components from a single Log360 console, eliminating the need to manage separate interfaces for each module. This provides a centralized point for navigation, making it easy to move between components without multiple logins or separate consoles.
Integration also introduces options that centralize access, simplify authentication, and enable unified session and shutdown management across all components. These capabilities improve operational efficiency and ensure unified management of all components.

Read also

This page provided an overview of integration and its key benefits. To learn how to configure and use the integrated components, refer to the following articles:

- Downloading and installing components
- Integrating the components

5.4.2. Downloading and installing components

Last updated on: September 12, 2025

In this page

Overview

Steps to download and install components

Overview

This section explains how to download and set up the components required for integration. The process includes selecting components, downloading their installers, and completing the installation to make them available for integration.

Step to download and install components

To begin the integration process, download and install the required components by following these steps:

> **NOTE**
>
> If the components are already installed and running, you can skip this step and proceed to integrating the components.

1. In your account, navigate to the Settings tab.
2. Under Admin Settings, go to Integrations, then click Log360 Integration.

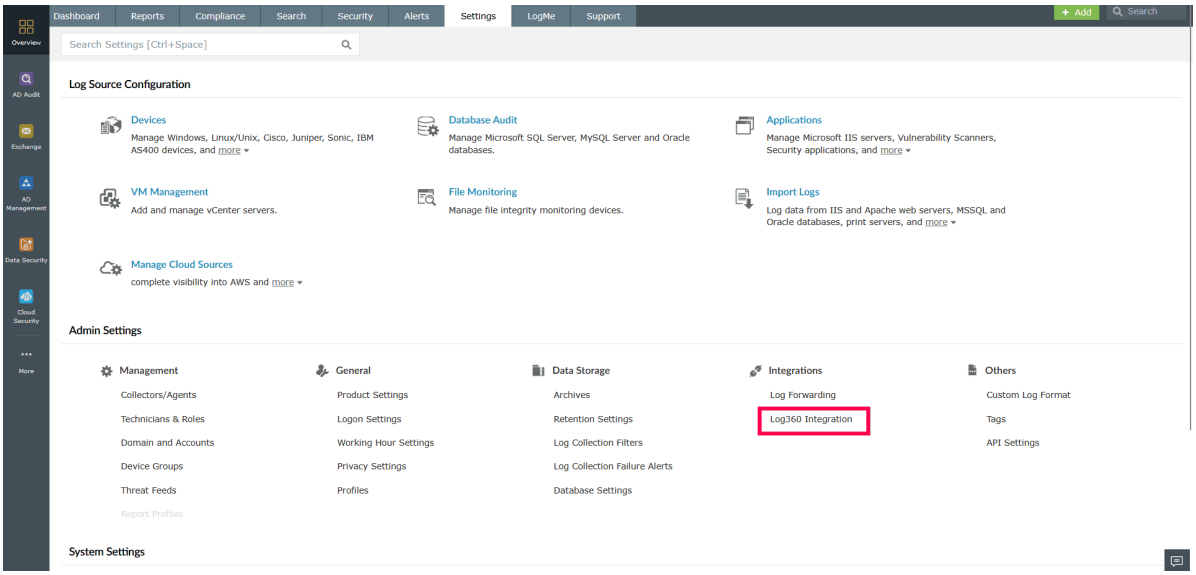


Figure 1: Navigating to Log360 Integration

3. In the Manage Components page, locate the component you want to install and click Configure.

> **NOTE**
>
> Ensure that you integrate ADAudit Plus version 6065 or above when using the latest or upcoming builds of Log360 (Build 5214 and above)

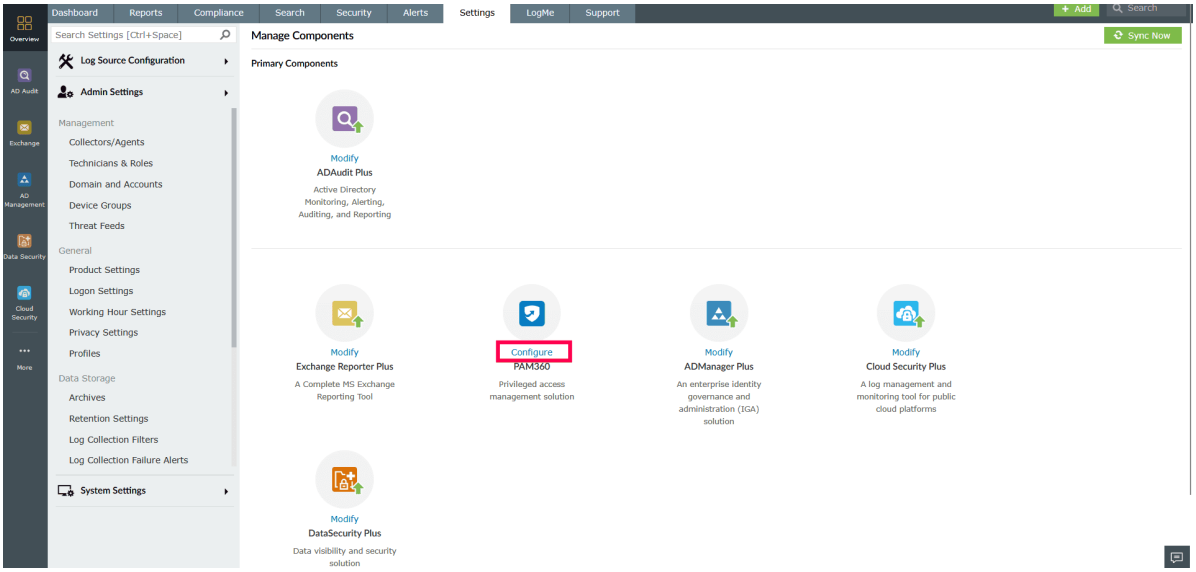


Figure 2: Installing a component

4. On the Integrate Component page, click Download Now to download the installer.

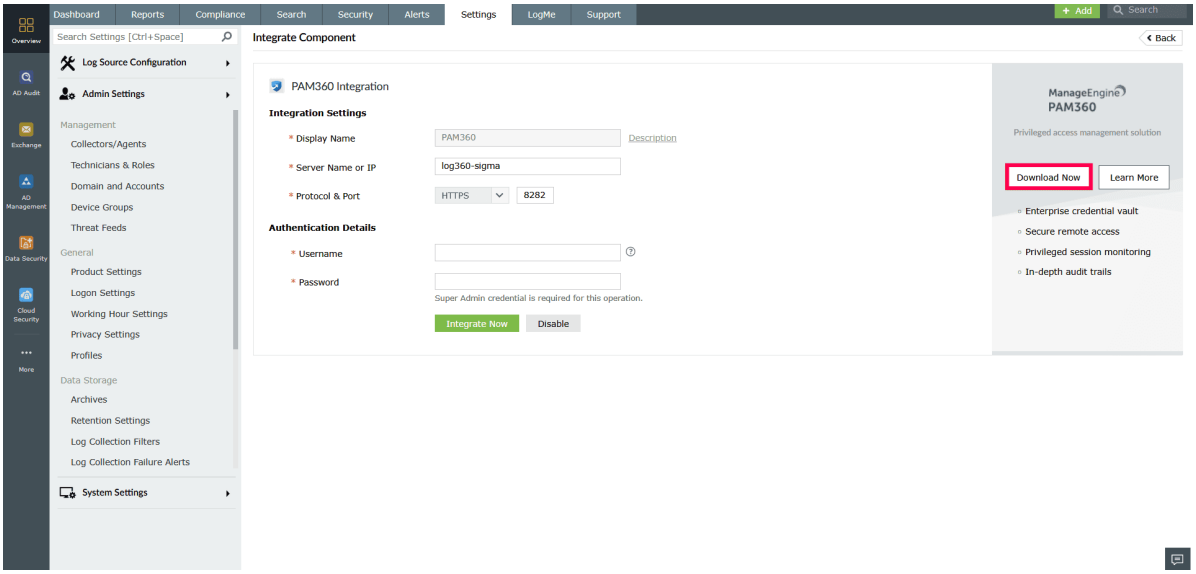


Figure 3: Downloading the installer

5. Launch the installer.

- On the welcome screen, click Next to begin the setup.



Figure 4: Installing ManageEngine PAM360 setup

- Read and accept the license agreement by selecting Yes.



Figure 5: Installing ManageEngine PAM360 setup

- Select the folder where the component will be installed. Click Browse to choose the folder, then click Next.



Figure 6: Selecting the installation folder for the component

- In the Server Selection panel, choose the appropriate server type: High Availability Primary Server, High Availability Secondary Server, or Read-Only Server, and click Next.

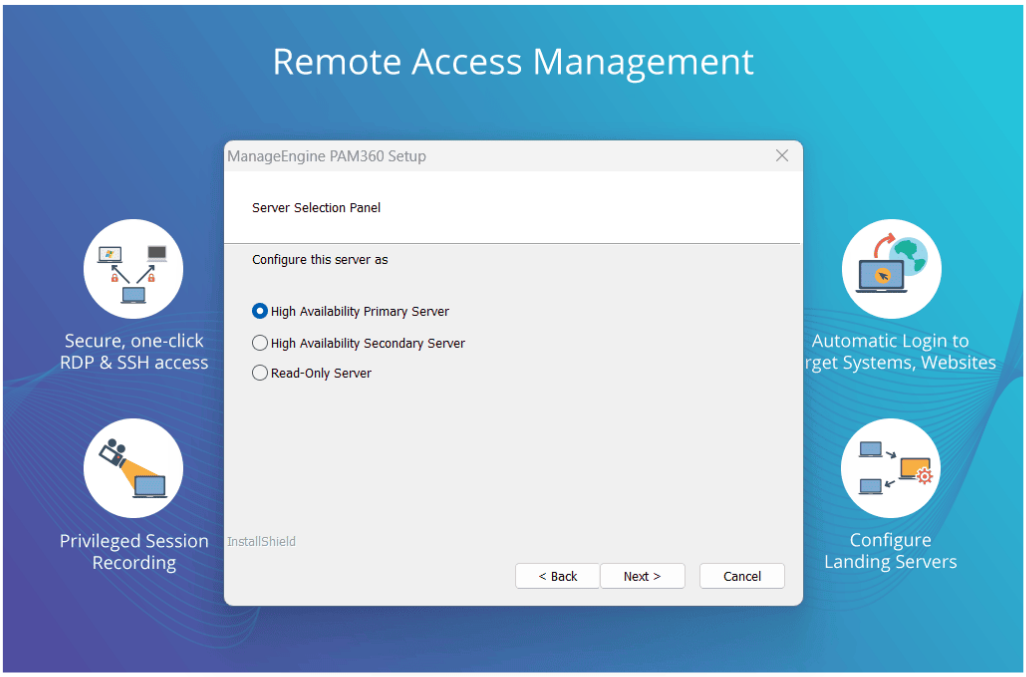


Figure 7: Selecting the server type

- Review the settings and click Next to proceed with the installation.

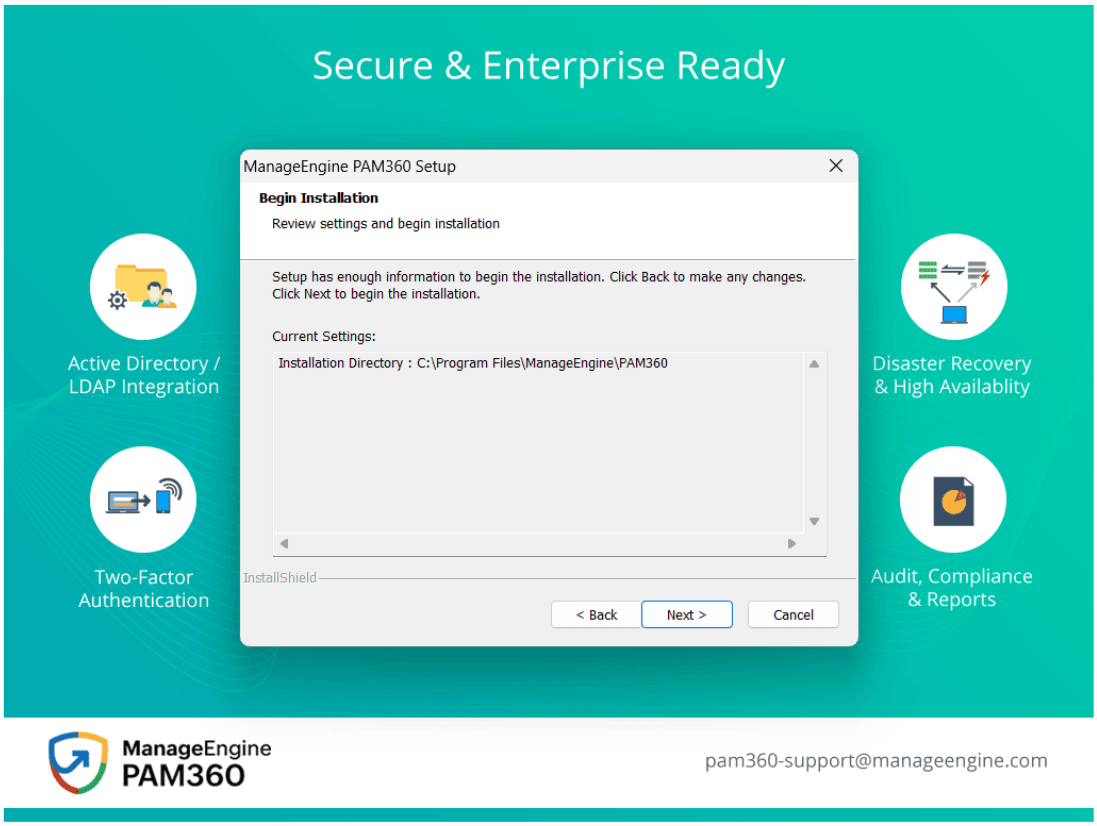


Figure 8: Installing ManageEngine PAM360

- Repeat these steps for all other components that need to be integrated.
- You can also download the component from this website.

Read also

This page explained how to download and install the components. To learn how to integrate and navigate between them, refer to the following articles:

- Integrating the components
- Navigating across the components

5.4.3. Integrating the components

Last updated on: September 12, 2025

In this page

Overview

Steps to integrate the components

Overview

This section explains how to integrate the installed components with the product console to enable centralized management. Integration involves configuring connection details such as the component's server name or IP address, port number, and administrator credentials within the product console.

Steps to integrate the components

1. In your account, navigate to the Settings tab.
2. Under Admin Settings, go to Integrations, then click Log360 Integration.

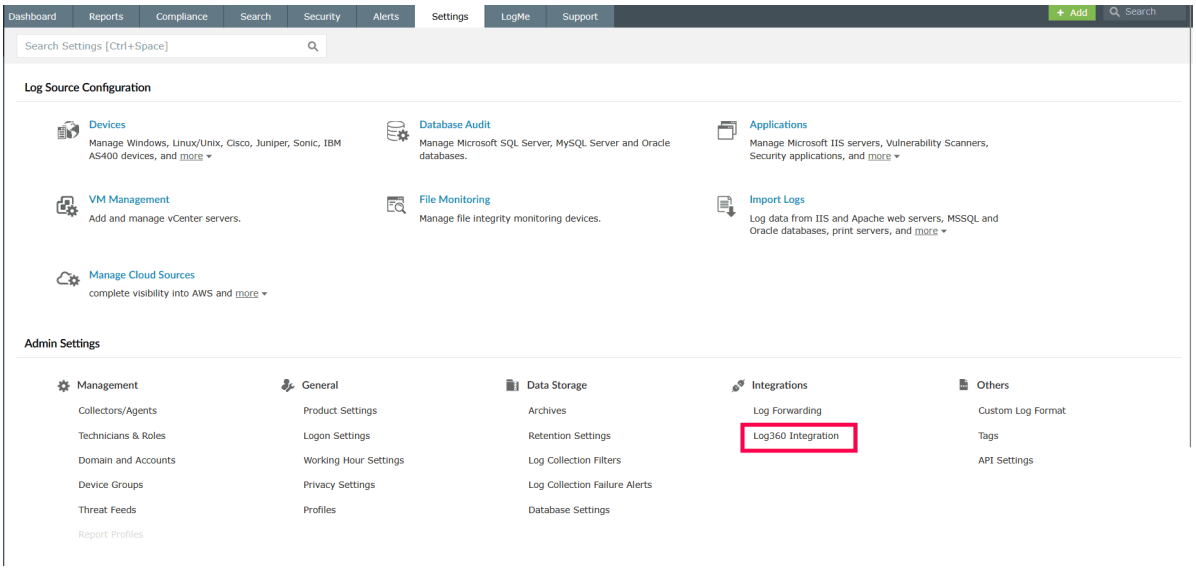
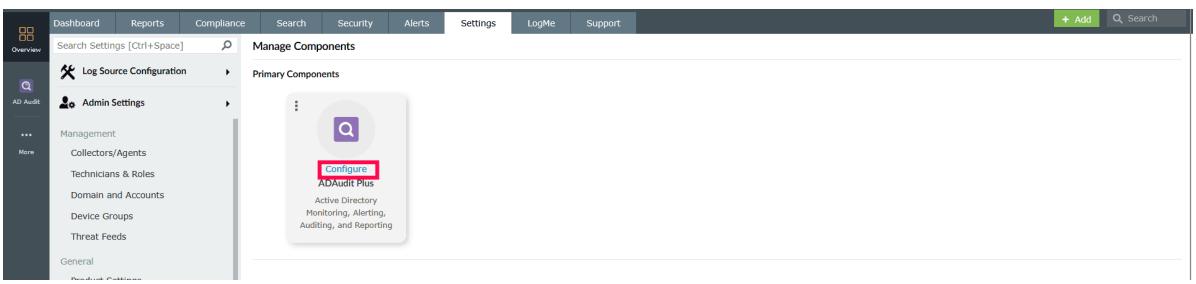


Figure 1: Navigating to Log360 Integration

3. In the Manage Components page, click Configure under the component you want to integrate.



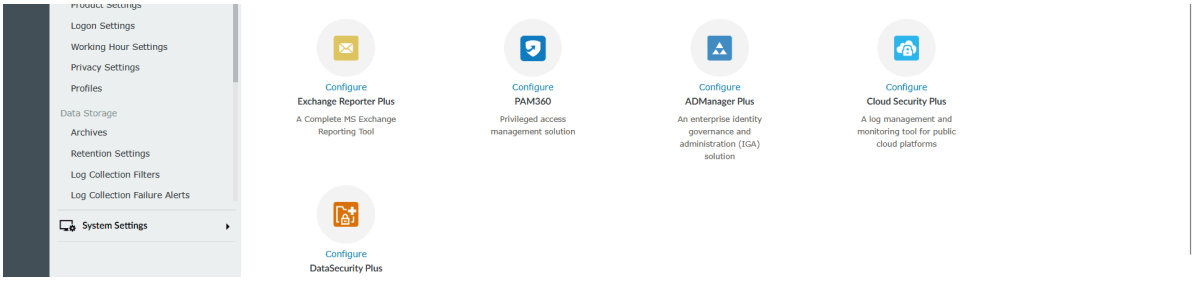


Figure 2: Integrating a component

4. On the Integrate Component page, under Integration Settings, enter the following details:
   - Server Name or IP Address of the machine where the component is running.
   - Port number and Protocol used by the component.

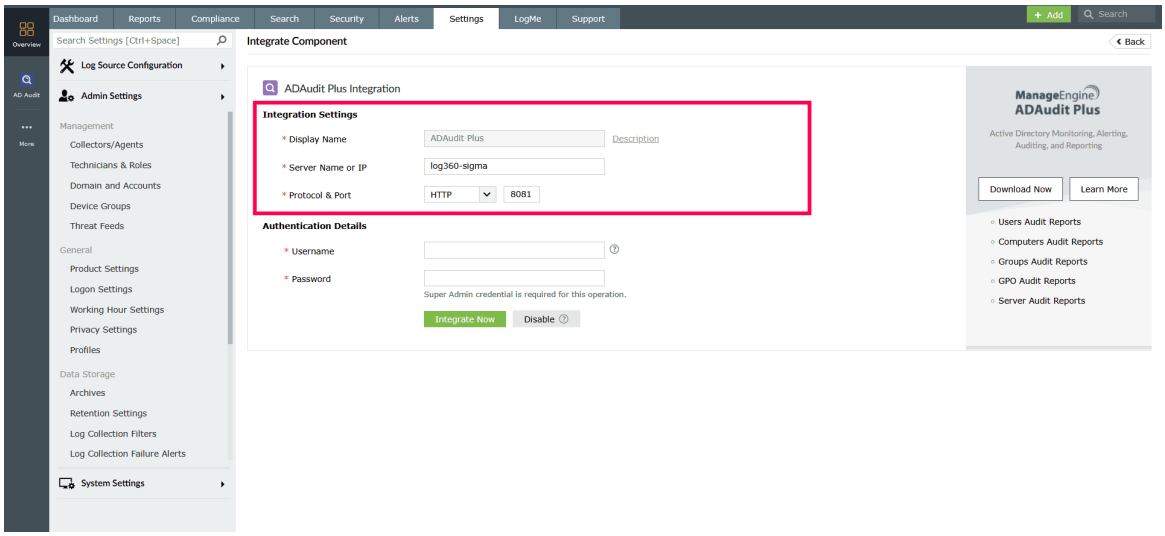


Figure 3: Configuring Integration Settings

5. Under Authentication Details, enter the Super Admin credentials of the component.

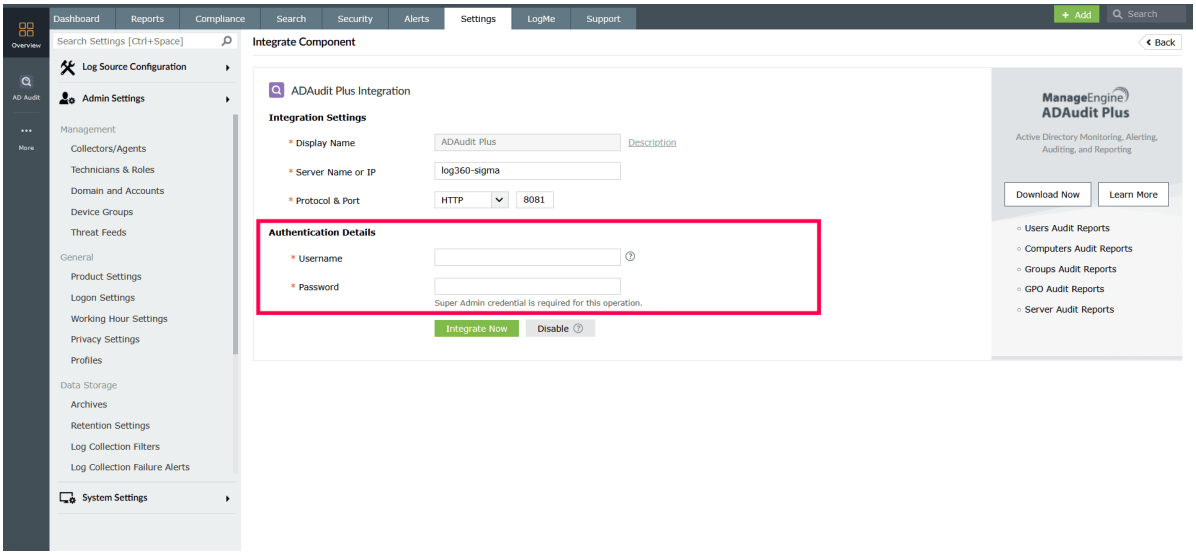


Figure 4: Configuring Authentication Settings

6. Click Integrate Now to complete the integration.

6. Click Integrate Now to complete the integration.

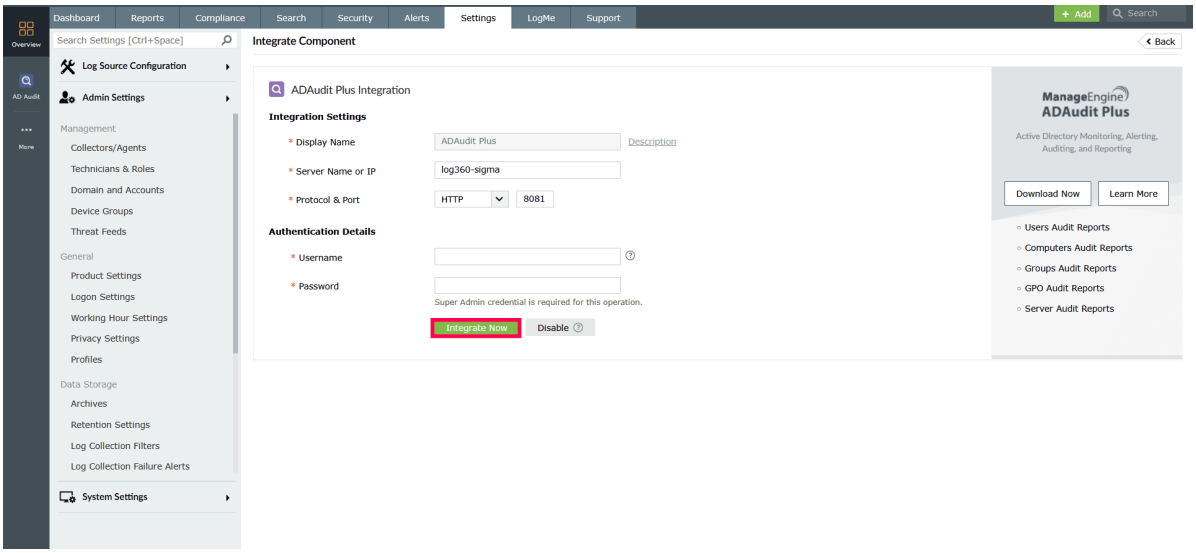


Figure 5: Integrating a component

7. Repeat the steps for all other components you want to integrate.
8. To remove the integration, click Disable. Removing a component will completely disable its functionality and delete all its integration details.
9. To modify settings, click Modify under the component you want to update.

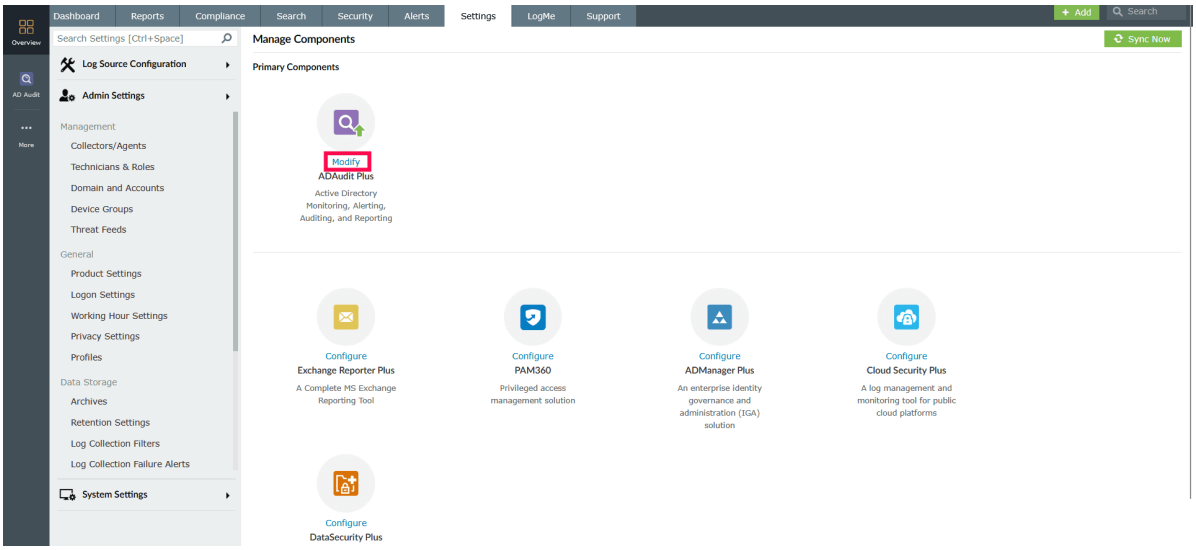
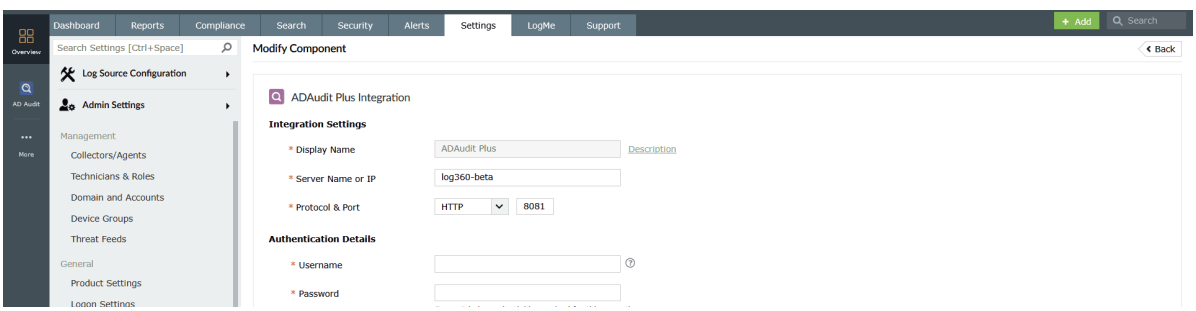


Figure 6: Modifying a component

10. Make the necessary changes, and click Update Settings.



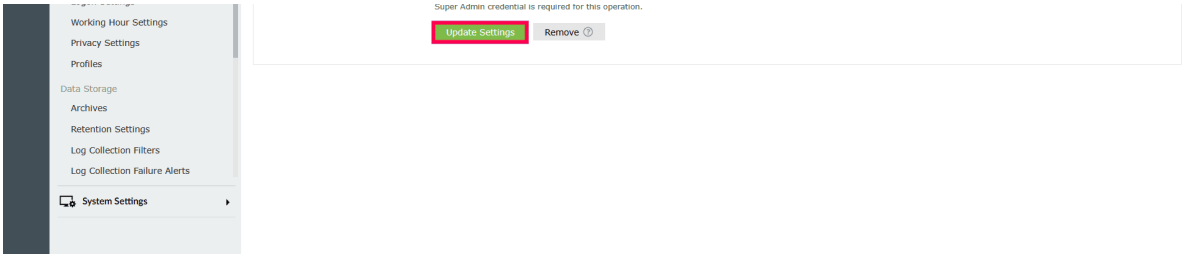


Figure 7: Modifying a component

11. To remove the integration, click Remove. Removing a component will completely disable its functionality and delete all its integration details.

> NOTE
>
> When PAM360 is integrated with Log360, ADManager Plus won't integrate with PAM360 unless the respective product certificates are imported into PAM360.
>
> - Learn how to integrate PAM360 with Log360 UEBA
> - Learn how to integrate PAM360 with ADManager Plus

Read also

This page explained how to integrate Log360 components. To learn how to navigate across components and access additional integration capabilities, refer to the following articles:

- Navigating across components
- Additional configurations

5.4.4. Navigating across components

Last updated on: September 12, 2025

In this page

Overview

Steps to navigate across components

Overview

Once the components are integrated, Log360 provides a centralized interface for seamless navigation between modules. Administrators can switch between components without separate logins, ensuring a unified experience.

This section explains the navigation options available for accessing different components within Log360.

Steps to navigate across components

1. Click the # icon at the top-left corner of the console.
2. In the Related Products pop-up, select the required component.
3. If the component is not listed in the pop-up, click Show All to display all available components.

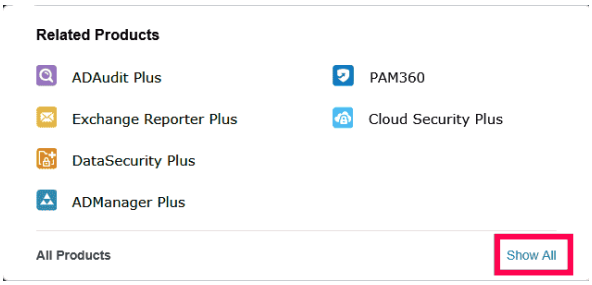


Figure 1: Accessing components

4. Alternatively, select the component from the app pane if it is displayed there.

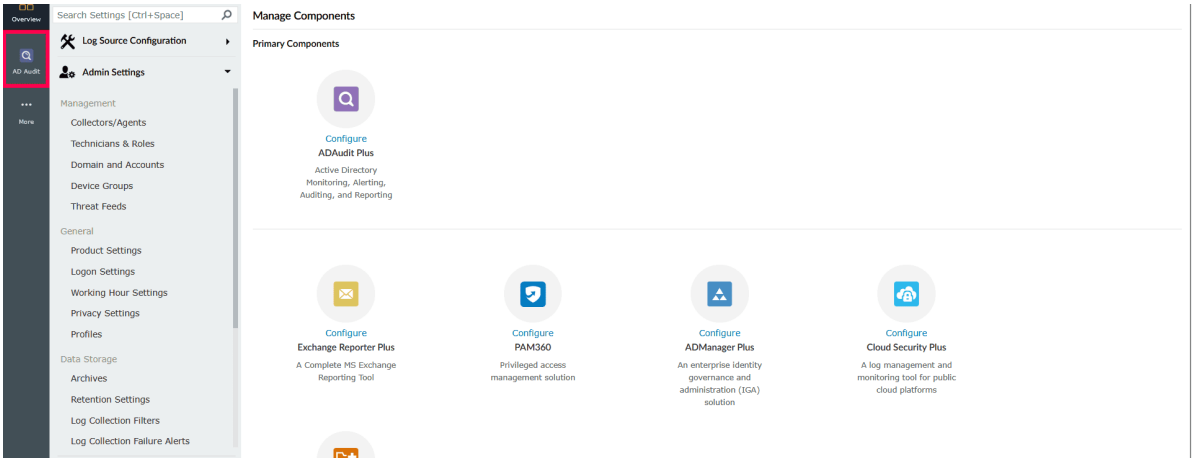




Figure 2: Selecting components from the app pane

5. If the component is not visible in the App Pane, click More in the left navigation panel to locate and select the component.

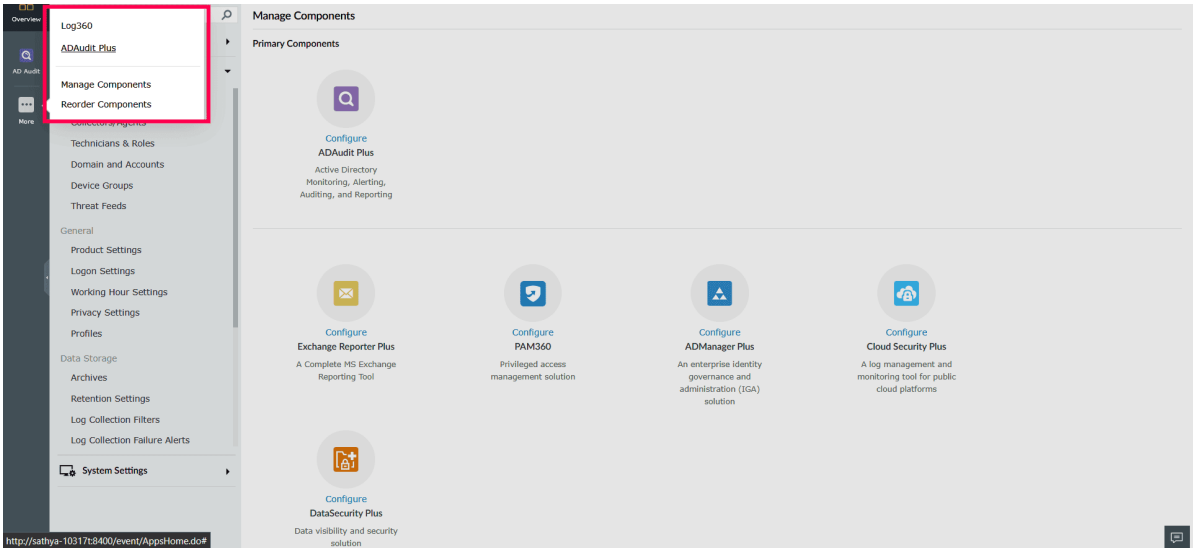


Figure 3: Locating components from the app pane

6. To customize the order of components, click Reorder Components.
7. In the Reorder Components window, click and drag the ⠿ icon next to a component name to rearrange the order.

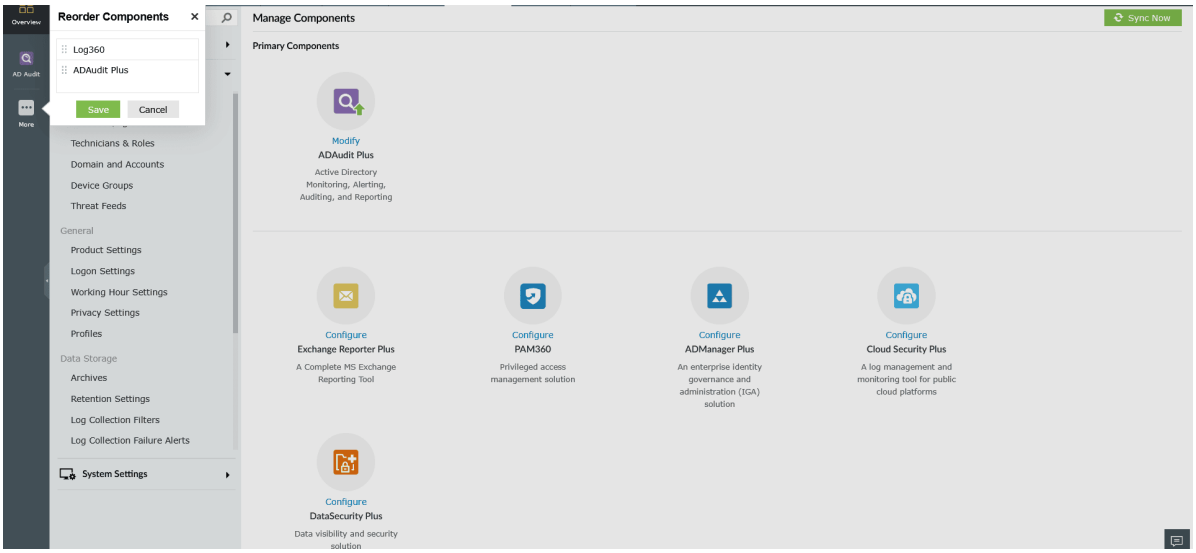


Figure 4: Re-ordering components

8. After rearranging, click Save to apply the changes.

Read also

This page covered how to switch between integrated components. To learn how to use integration capabilities

This page covered how to switch between integrated components. To learn how to use integration capabilities effectively, refer to the following articles:

- Additional configurations
- Downloading and installing components

5.4.5. Additional configurations

Last updated on: September 12, 2025

In this page

Overview

Using additional configurations

Overview

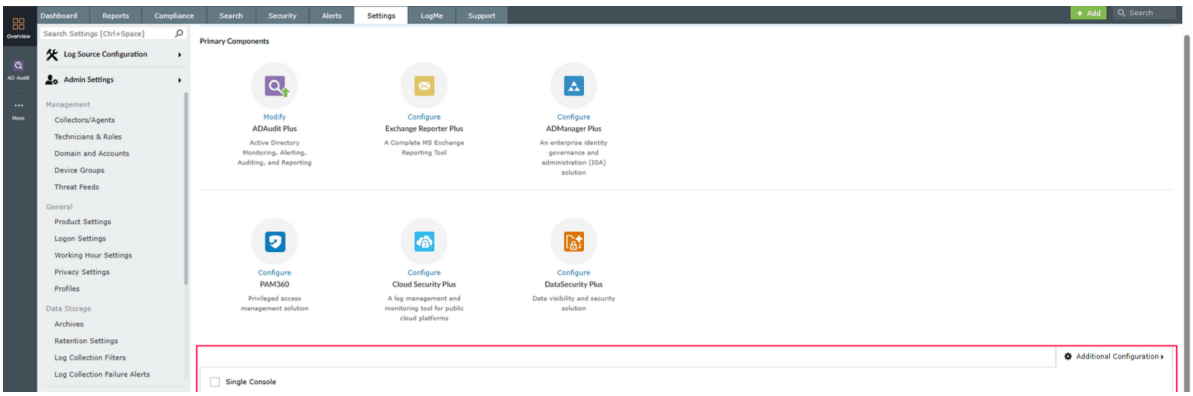
This page details how additional configurations allow admins to enable centralized features that simplify navigation, session control, and system management across integrated components. These options enhance usability and improve operational efficiency.

Using additional configurations

1. In the Log360 Integration page, click Additional Configuration. A pane will open, displaying the following options:
   - Single Console: Enables you to access the product console and other integrated components from the Apps Pane within any component.
   - Single Sign-On: Allows switching between components without entering multiple login credentials.
   - Single Sign-Out: Ensures that signing out from the product console logs you out of all integrated components simultaneously.
   - Single Shutdown: Enables you to shut down all integrated components when shutting down the product console.

   > NOTE
   >
   > This option does not apply to remotely installed components or when High Availability is enabled.

2. Click Save to apply the settings or Reset to discard changes.



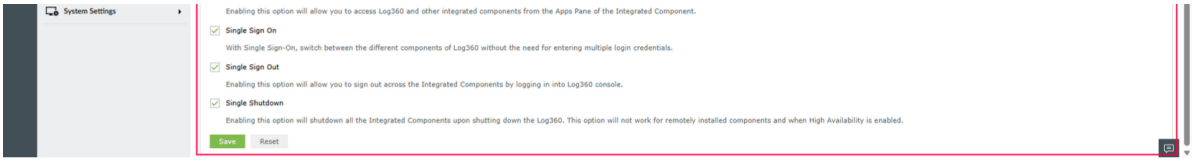


Figure 1: Using additional configurations

This page detailed how to configure additional integration settings. To learn more about integration capabilities, refer to the following articles:

- About Log360 integration
- Downloading and installing components

6.1.1. Overview

Last updated on: September 12, 2025

In this page

Use cases

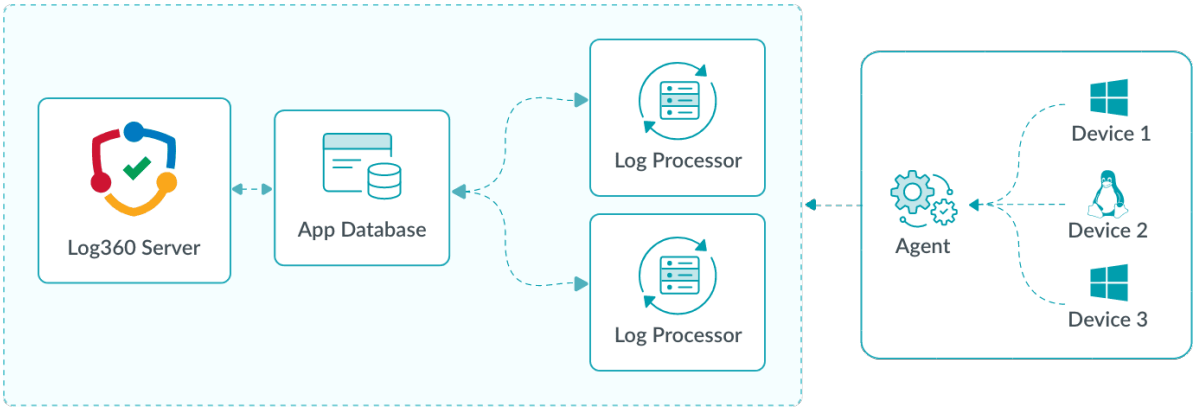
Roles and functions

Each installed instance of ManageEngine Log360 runs as a Log Processor. It receives logs from various sources and performs operations such as parsing, correlation, enrichment, indexing, archiving, alerting, and log forwarding. In scalable deployments, multiple Log Processors form a cluster where load balancing distributes logs evenly and roles can be assigned to optimize performance. This ensures higher throughput, eliminates bottlenecks, and provides reliable log management at scale.

- To learn more about scalability in Log360, refer to this document.
- To learn when to scale your Log360 deployment, refer to this document.
- To learn about Log360 capacity planning, refer to this document.
- To plan a scalable deployment, refer to this document.

Use cases

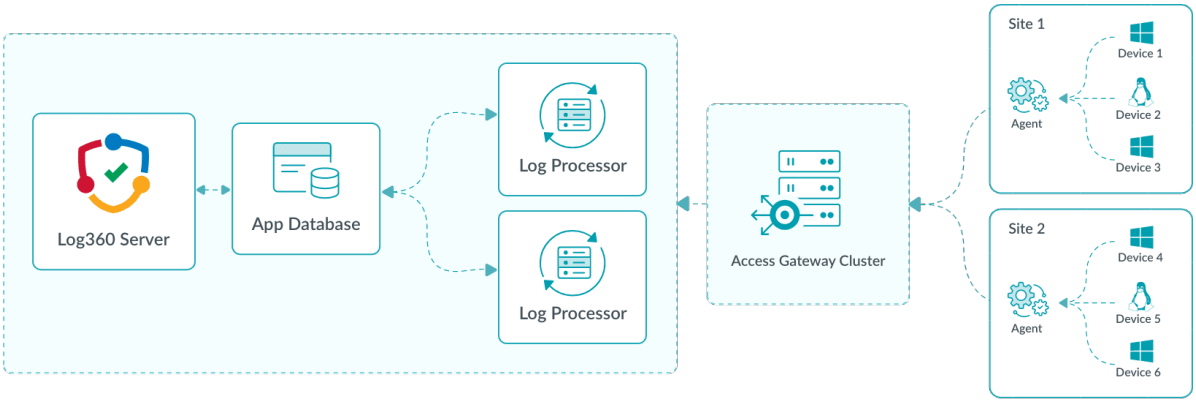
1. Scalable log processing: By deploying multiple Log Processor nodes in a cluster, the processing capacity can be scaled horizontally with logs distributed evenly for balanced workloads and uninterrupted performance.
   How it works?



   Logs generated by devices are collected by agents, which parse, filter, compress, and securely upload them to the Log Processor. Each Log Processor executes its assigned roles, such as parsing, indexing, or enrichment. The App Database maintains role assignments and routing information, ensuring logs are directed to the appropriate processor. As additional processors are deployed, workloads are automatically balanced, enabling horizontal scalability and preventing performance bottlenecks.

2. Reliable log ingestion: The Log Processor uses a distributed queuing mechanism to temporarily store incoming logs in categorized queues, handling spikes without data loss.

3. Role-based specialization for optimized performance : Log Processors can be configured to handle specific modules, such as indexing, correlation, alerting, archiving, or log forwarding, isolating heavy workloads for maximum efficiency.
   How it works?

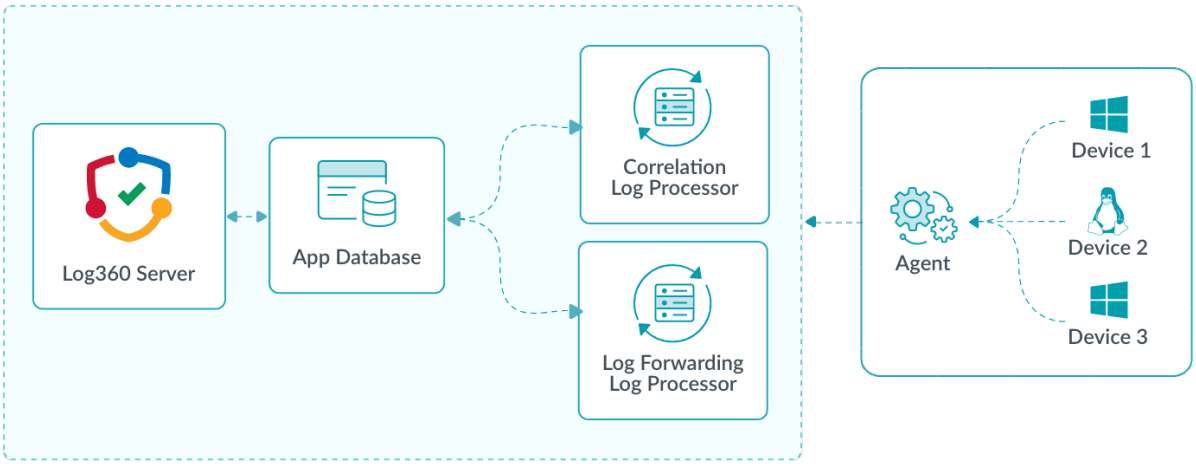


   Agents upload logs to the processing layer, where they are distributed to role-specific processors. For example:

   - The Correlation Log Processor evaluates events against security rules.
   - The Log Forwarding Processor sends logs to external tools or destinations for further analysis or storage.

   The App Database stores configuration and routing details, ensuring that logs are directed to the appropriate processor based on their role. By assigning processors to specific roles, organizations can optimize resource utilization and scale each component independently. For example, if correlation workloads increase, more Correlation Processors can be added without impacting log forwarding capacity.

4. Distributed log collection: Multi-site deployment ensures that logs from remote sites can be monitored and managed from a single, central console, with the Access Gateway Cluster protecting internal processor details.
   How it works?



   Agents at remote sites upload logs to a single public-facing endpoint, the Access Gateway Cluster. The cluster forwards the logs securely to Log Processors in the central environment. Acting as a bridge, the Access Gateway Cluster hides internal processor details from external agents, reducing exposure risks. Logs are then routed to the appropriate processors for parsing, indexing, or enrichment, with the App

Database maintaining configurations and routing information. As log volumes grow, additional processors can be added at the central site without requiring changes at remote agents.

Roles and functions

A Log Processor can be configured to perform one or more roles, each with specific functions. The processor used to add and manage other processors is designated as the primary processor. Only the primary processor can perform cluster operations such as add, delete, or edit. Roles are categorized as follows:

1. Default Roles: Predefined roles that are essential for core processing. These include:
    - Processing Engine: Enriches parsed logs, handles log forwarding, alerts, and archiving.
    - Correlation Engine: Evaluates events against security rules.
    - Search Engine: Indexes data and handles user queries.
    - Log Queue Engine: Manages event flow between components and prevents data loss.
2. Custom Roles: Roles that can be added based on specific requirements. These include:
    - Alerts: Triggers alerts when logs or events match specific criteria.
    - Archive: Handles log archiving for long-term storage.
    - Log Forwarding: Sends logs to external tools or destinations for further analysis or storage.

> NOTE
>
> When you assign a custom role such as Alerts, Archive, or Log Forwarding to a Log Processor, the Processing Engine will no longer handle these functions.

Read also

This document outlines the scalable architecture of Log360 and outlines key use cases. To learn how to configure and manage these components effectively, refer to the following articles:

- Configuring Log Processors
- Managing Log Processors

6.1.2. Configuring Log Processors

Last updated on: September 12, 2025

In this page

Overview

Pre-requisites

Configuring pre-requisites

Adding a primary processor

Adding additional Log Processors

Overview

This page covers the prerequisites for deploying Log Processors, how to configure them, and the steps to add both primary and additional Log Processors.

Pre-requisites

Before adding a Log Processor, ensure the following basic requirements are met:

- At least one Log Processor node of the same version is available and running.

> NOTE
>
> If the primary server has multiple network interfaces, follow these steps to select the interface for cluster communication.
>
> - In your account, navigate to Settings tab.
> - Under System Settings, select Connection Settings.

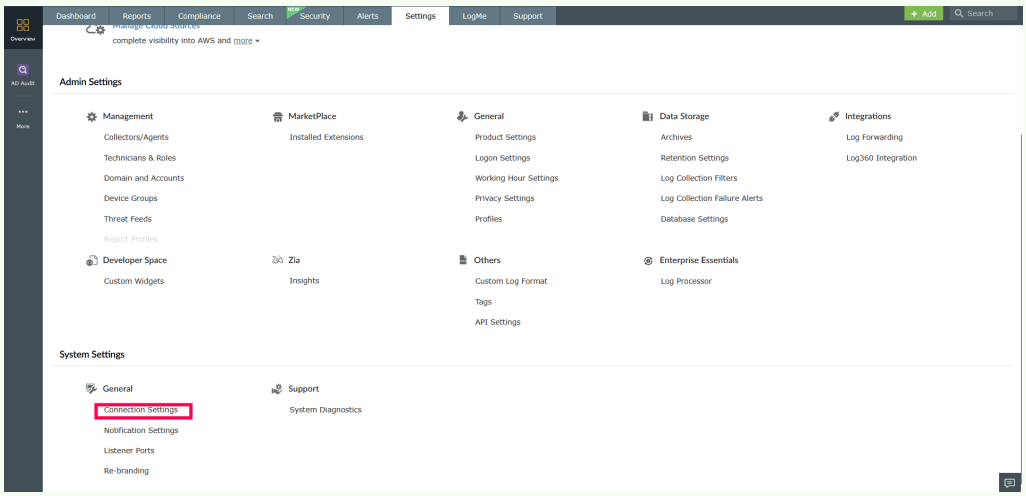


Figure 1: Navigating to connection settings

- Click Advanced, and in the Bind Address dropdown select the appropriate network interface (IP address) that the new Log Processor will use to connect to the primary server.

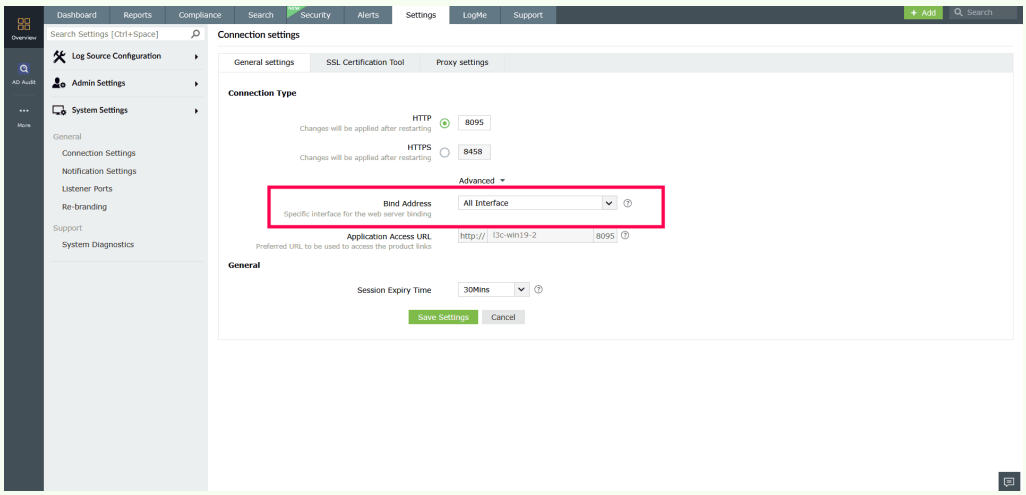


Figure 2: Configuring advanced settings

- Click Save Settings.

- A common database is configured.
- A shared storage location is configured for:
  - Archive policies

    > NOTE
    >
    > The archive policy location must be changed from a local path to a shared storage location or S3.

  - Elasticsearch archive data
  - Communication across processors
- Existing archive ZIP files are moved from local storage to the newly configured shared path.

Configuring pre-requisites

1. Log in to your account.
2. Go to the Settings tab.
3. Under Admin Settings, navigate to Enterprise Essentials and select Log Processors.
4. Click Add Log Processor.



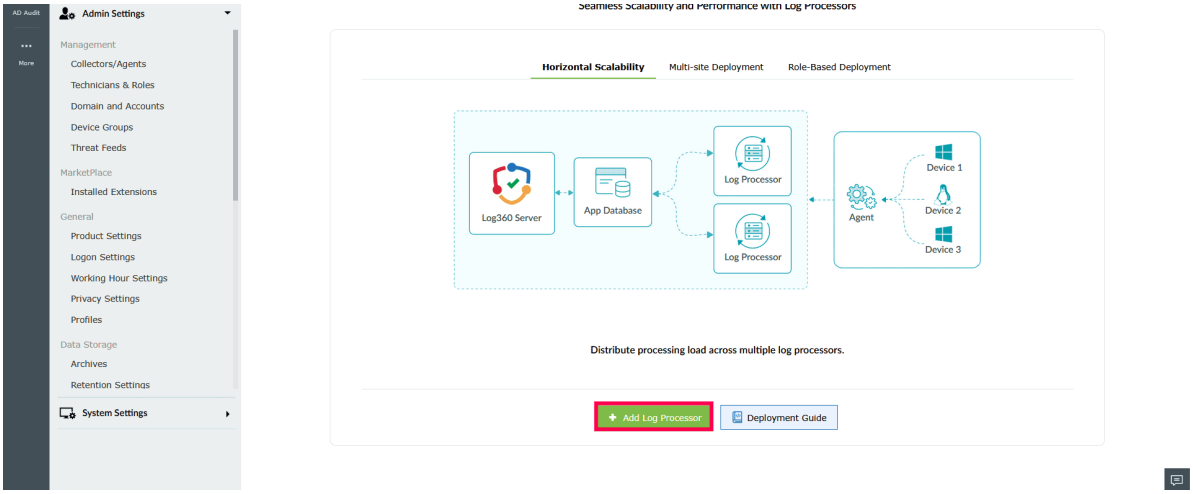


Figure 3: Adding a Log Processor

5. In the setup window that appears, click Proceed to begin the configuration.

> NOTE
>
> 1. Review all the steps shown in the pop-up window carefully and ensure they are completed before clicking Proceed.
> 2. Verify that the Server Name, port, and Administrator credentials of the Log360 instance are entered accurately, as these details are mandatory for integrating the log processor with the main processor cluster.

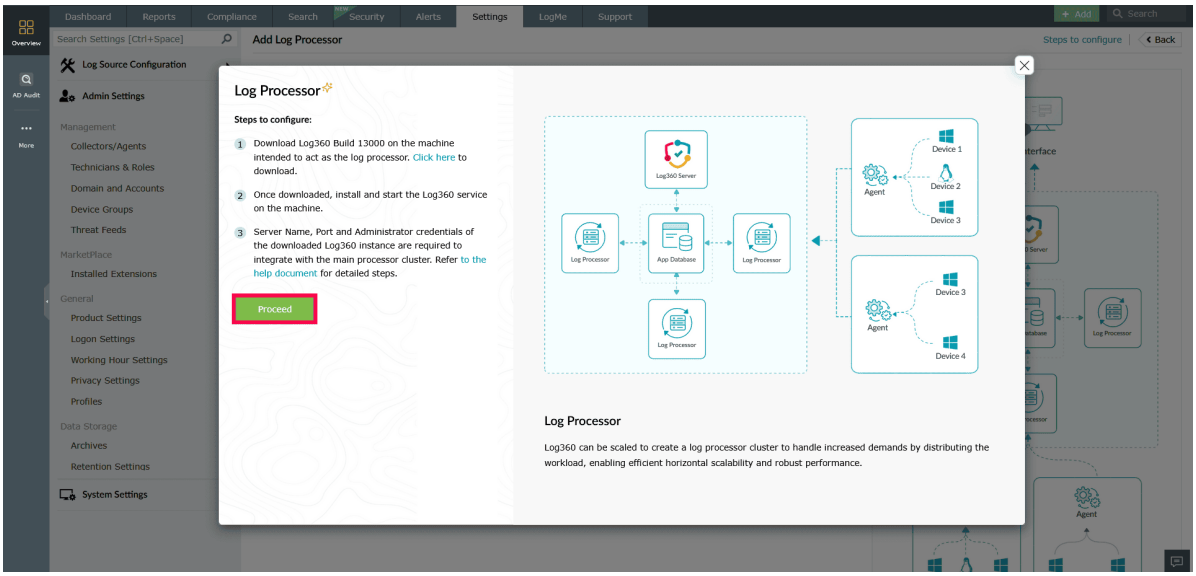


Figure 4: Configuring a Log Processor

To proceed with adding a Log Processor, the following prerequisites must be configured:

6. A common database must be configured.

NOTE

Refer to this help document to configure the common database.

7. A shared storage location must be set up for communication across processors.

- Click Configure next to the prerequisite to open the shared storage setup window.

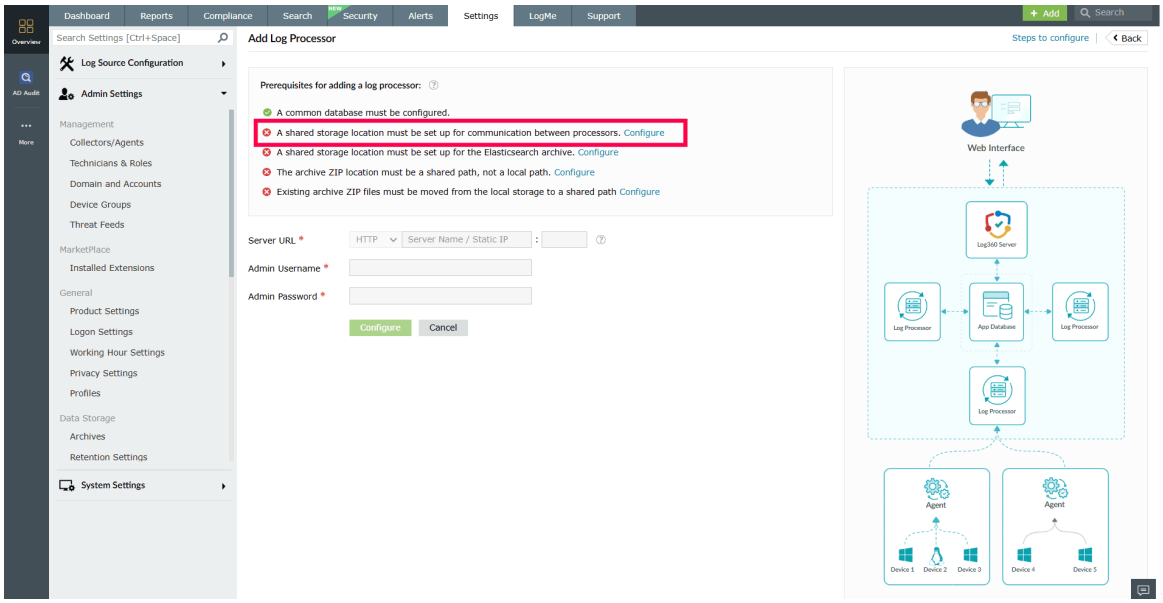


Figure 5: Configuring shared storage location

- Enter the shared storage location that is accessible and available to all Log Processors to prevent disruptions in data processing.

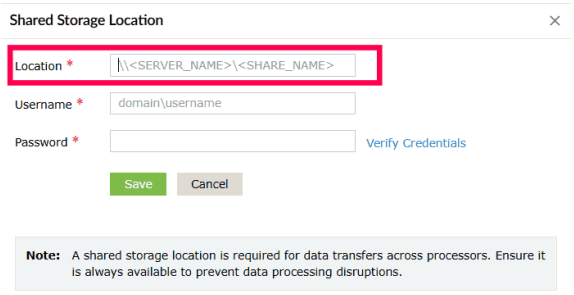


Figure 6: Configuring shared storage location

- Enter the username and password.

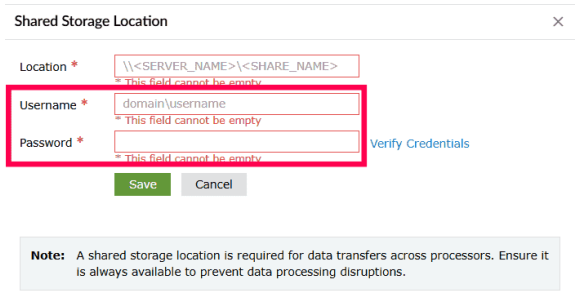


Figure 7: Configuring shared storage location

- Click Verify Credentials to validate access.

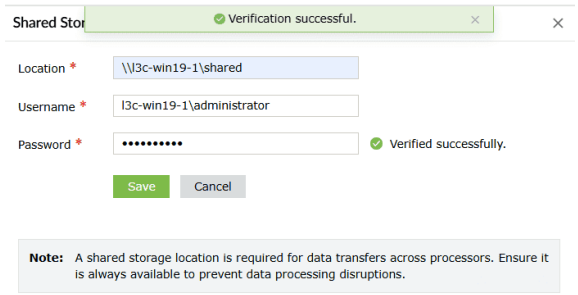


Figure 8: Configuring shared storage location

- Once verified, click Save to complete the configuration.

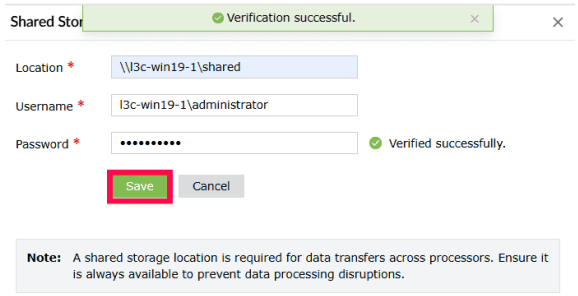


Figure 9: Configuring shared storage location

- After configuration, select Update to modify the shared storage path or credentials.

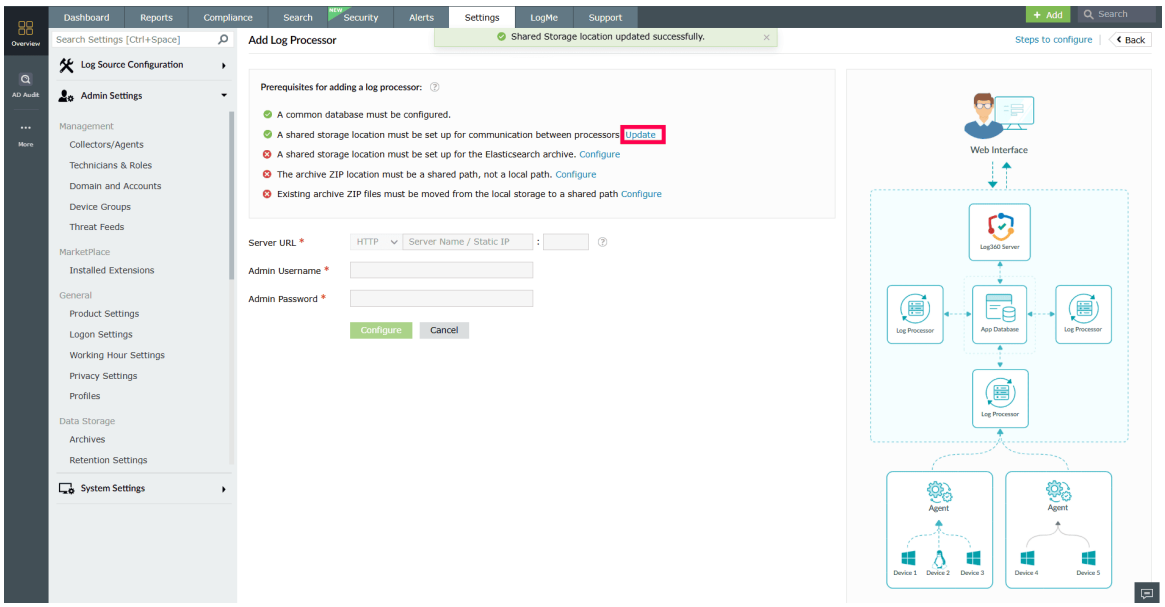


Figure 10: Updating shared storage path and credentials

- Select Update to save the changes.

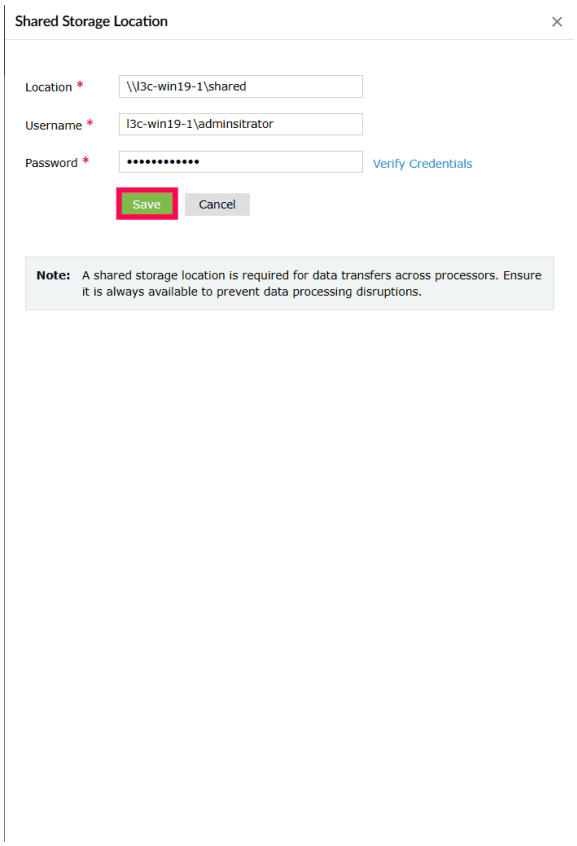


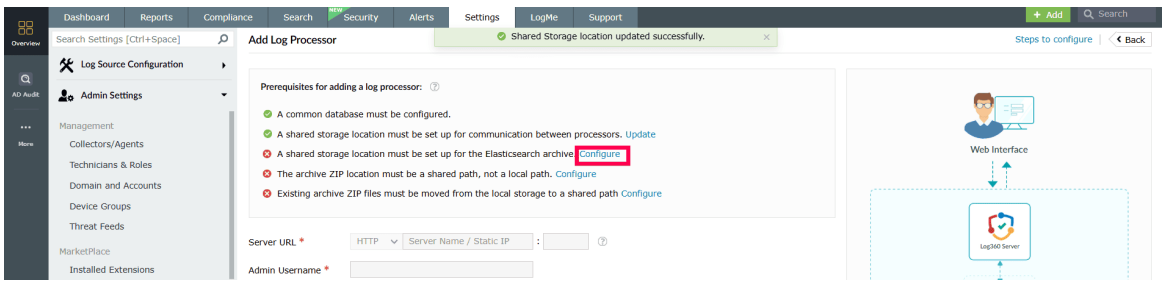
Figure 11: Updating shared storage path and credentials

8. A shared storage location must be set up for the Elasticsearch archive.

> NOTE
>
> The product uses the configured shared storage path to store data that exceeds the Elasticsearch retention period. Ensure the path is accessible to all Log Processors. If the storage is unavailable, it can affect archiving and log retrieval.

For Windows systems:

- Click Configure next to the prerequisite to open the Elasticsearch Archive Data Path window.



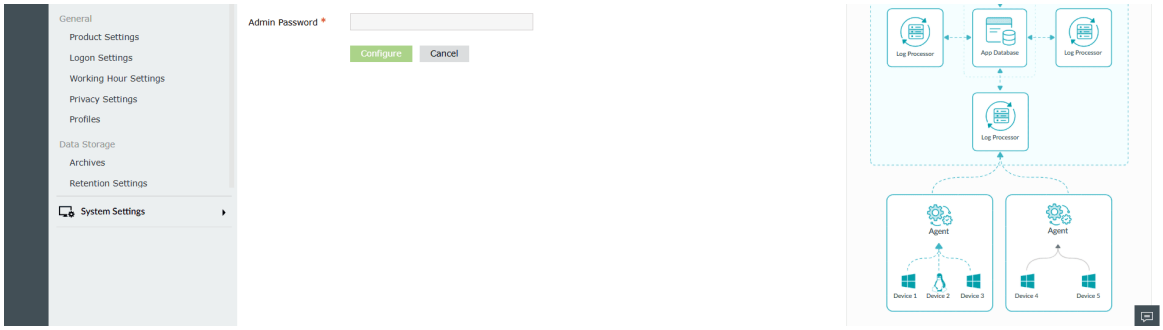


Figure 12: Configuring a shared storage location for Elasticsearch Archive

- Select the checkbox if existing data has been manually moved to the shared location.

> **NOTE**
>
> If you have existing data under <Log360 _HOME >\ES\archive, move that data to the same shared path before configuring. If there's no existing data, you can directly enter a new shared location.

- Enter the location path to the shared archive directory.

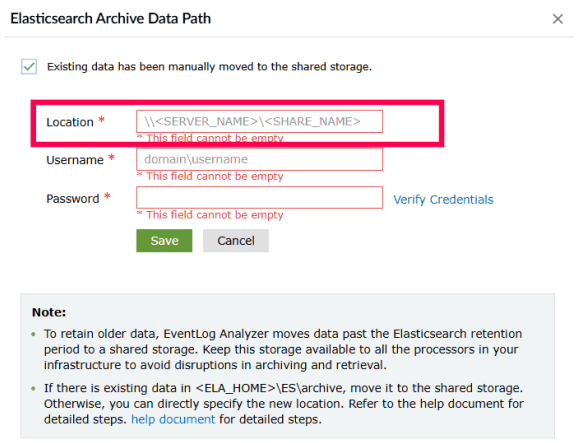


Figure 13: Configuring a shared storage location for Elasticsearch Archive

- Enter the Username and Password.
- Click Verifv Credentials to validate access

- Click Save to complete the configuration.
- After completing the configuration, click Update to modify the shared storage path for the Elasticsearch archive, if needed.

For Linux systems:

- Click Configure next to the prerequisite to open the Elasticsearch Archive Data Path window.
- Select the checkbox if existing data has been manually moved to the shared location.

> **NOTE**
>
> If you have existing data under \ES\archive, move that data to the same shared path before configuring. If there's no existing data, you can directly enter a new shared location.

- Enter the location path to the shared archive directory.
- Select the Auth Type from the dropdown menu: NFS or SMB.
- In case of SMB, enter the Username and Password required to access the shared storage.

> **NOTE**
>
> In case of NFS, credentials are not required.

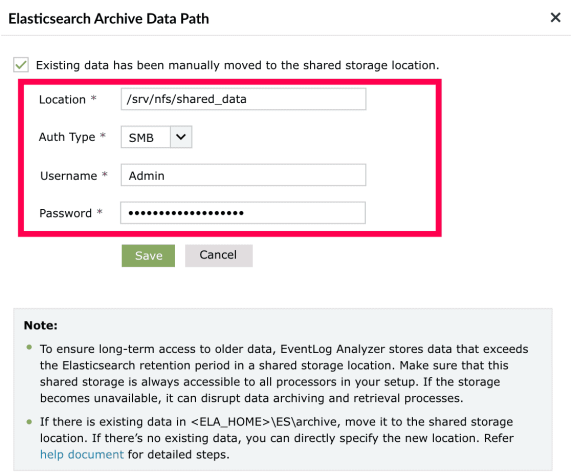


Figure 14: Configuring a shared storage location
for Elasticsearch Archive

- Click Save to complete the configuration.
- After completing the configuration, click Update to modify the shared storage path for the Elasticsearch archive, if needed.

9. The archive ZIP location must be set to a shared path, not a local one.

> **NOTE**
>
> If the archive ZIP location is already configured to a shared path or S3, you can skip the steps below. If not, follow the steps to update the configuration.

- Click Configure next to the prerequisite to open the Archive Settings window.

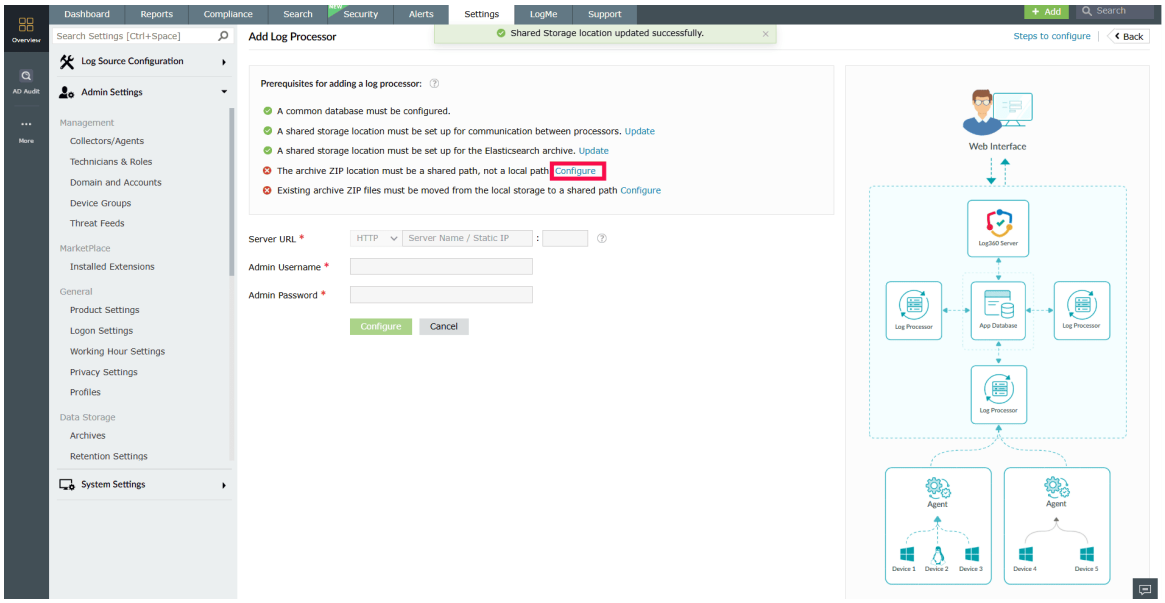
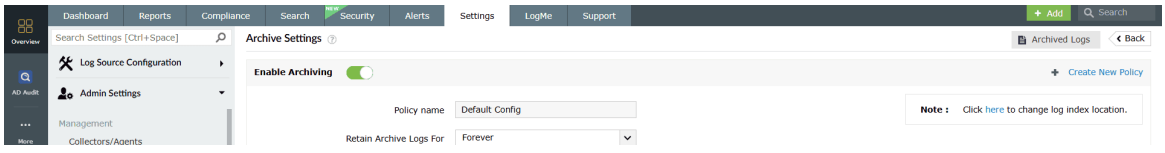


Figure 15: Configuring Archive Settings

- Under Archive ZIP Location, choose Shared, and enter the shared network path.

> **NOTE**
>
> For each archive policy, the archive ZIP location must be set to a shared path or S3.

- Click Save to apply all configured settings.



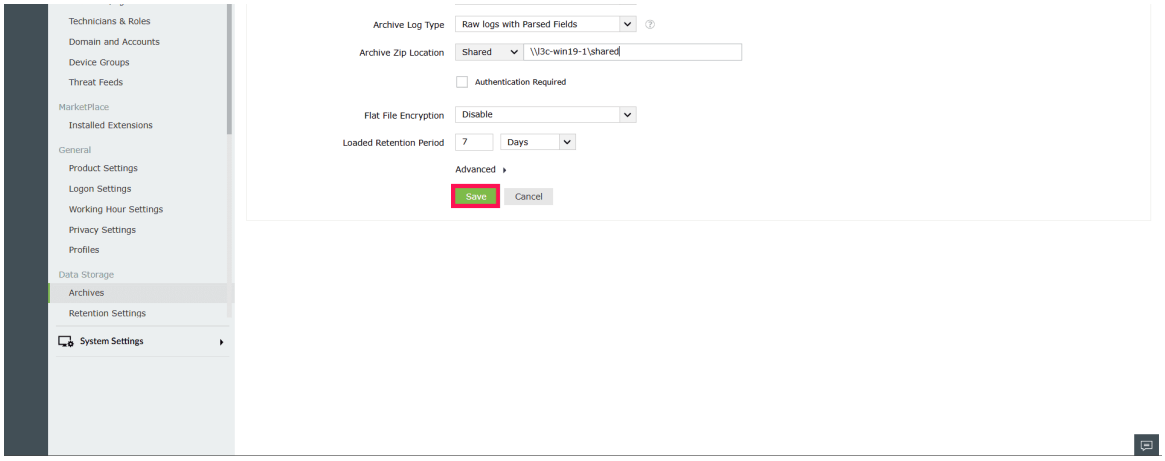


Figure 16: Configuring Archive Settings

- After completing the configuration, click Update to modify the shared storage path for the archive ZIP, if needed.

> NOTE
>
> If local storage was previously used for archiving, any existing archive ZIP files must be moved manually to the configured shared path.

10. Any existing archive ZIP files must be moved from local storage to the shared path.
    - Click Configure next to the prerequisite.
    - In the Archive Data - Update Paths window, select the checkbox Existing archives have been manually moved to the shared storage location only if the archive files have been manually transferred to the shared path.

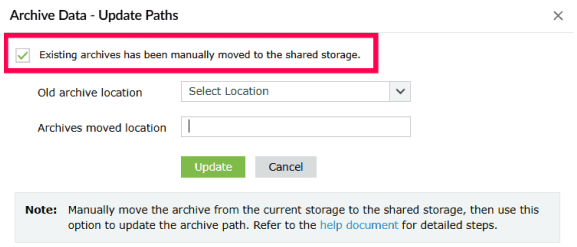


Figure 17: Updating the shared storage path for archive ZIP files

- In the Old archive location dropdown, select the previous archive path.
- In the Archives moved location field, enter the shared storage path where the archive files were moved.

> NOTE
>
> The number of file entries is shown beside the old and new archive paths. Ensure they match to confirm a successful migration.

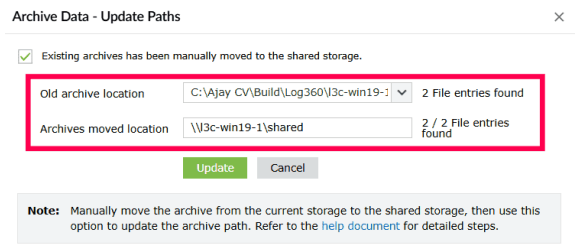


Figure 18: Updating the shared storage path for archive ZIP files

- Click Update to apply the changes.
- After completing the configuration, click Update to modify the shared storage path for existing ZIP files, if needed.

Adding a primary processor

Once the prerequisites are configured, follow the steps below to add a new Log Processor:

1. In the Add Log Processor window, fill in the following:

- Server URL: Choose the protocol (HTTP/HTTPS), enter the server name, and port.
- Enter the Admin Username and Admin Password for the Log Processor.

2. Click Configure to complete the setup.

> NOTE
>
> The primary Log Processor, usually the first one added cannot be deleted.

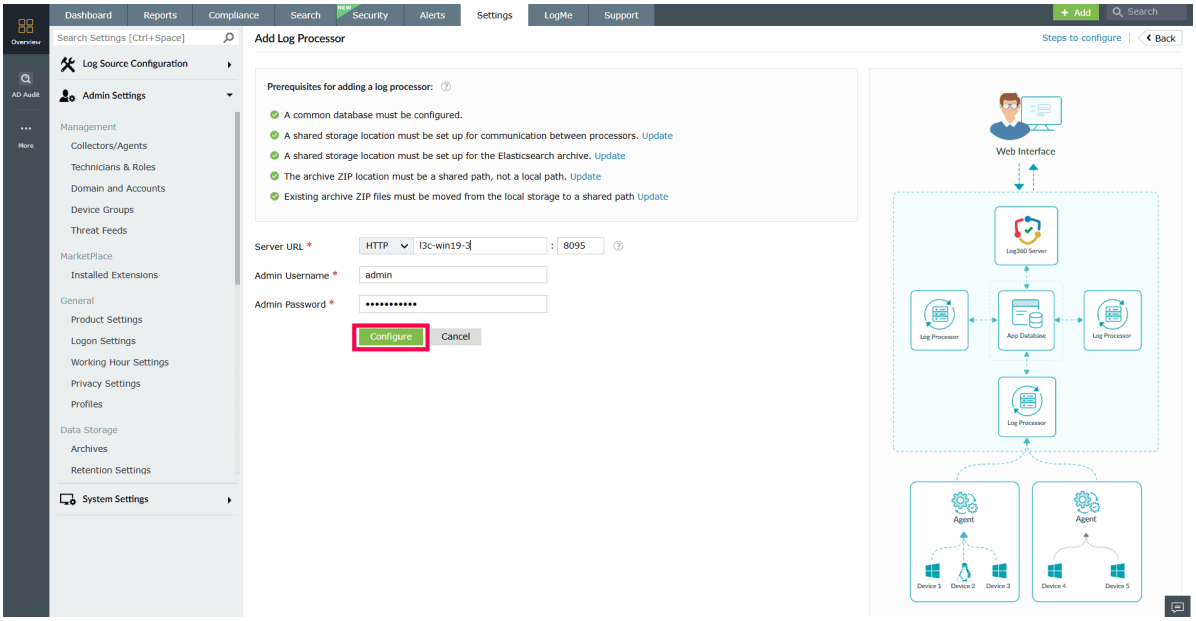
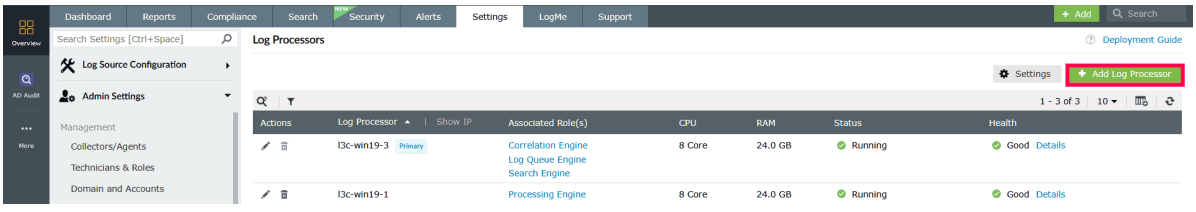


Figure 19: Adding a Log Processor

> NOTE
>
> The Log Processor server will restart automatically and be added to the Log Processor cluster. Once restarted, the Log Processor will be fully configured and ready for log processing.

Adding additional Log Processors

1. In your account, go to the Settings tab and select Admin.
2. Navigate to Enterprise Essentials and select Log Processor.
3. In the top-right corner, click Add Log Processor.



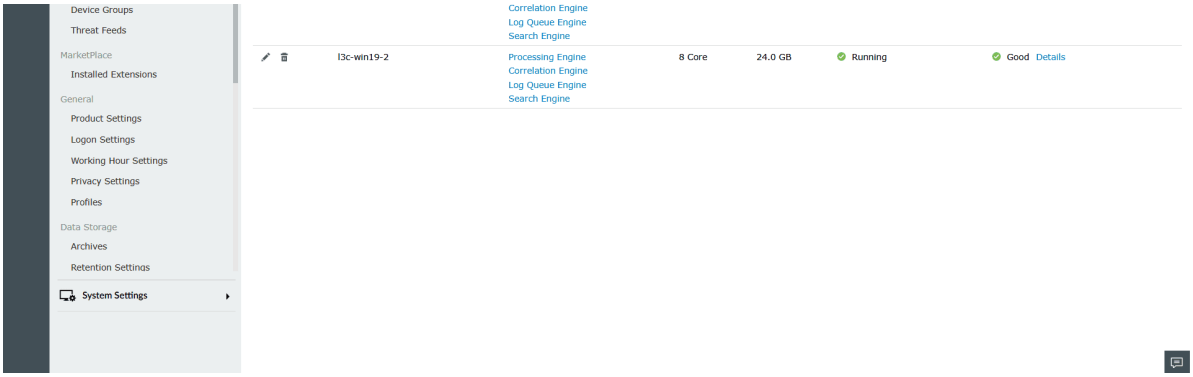


Figure 20: Adding additional Log Processors

4. In the Add Log Processor window, fill in the following:
   - Server URL: Choose the protocol (HTTP/HTTPS), enter the server name, and port.
   - Enter the Admin Username and Admin Password for the Log Processor.
5. Click the Advanced Settings dropdown for additional configuration options.

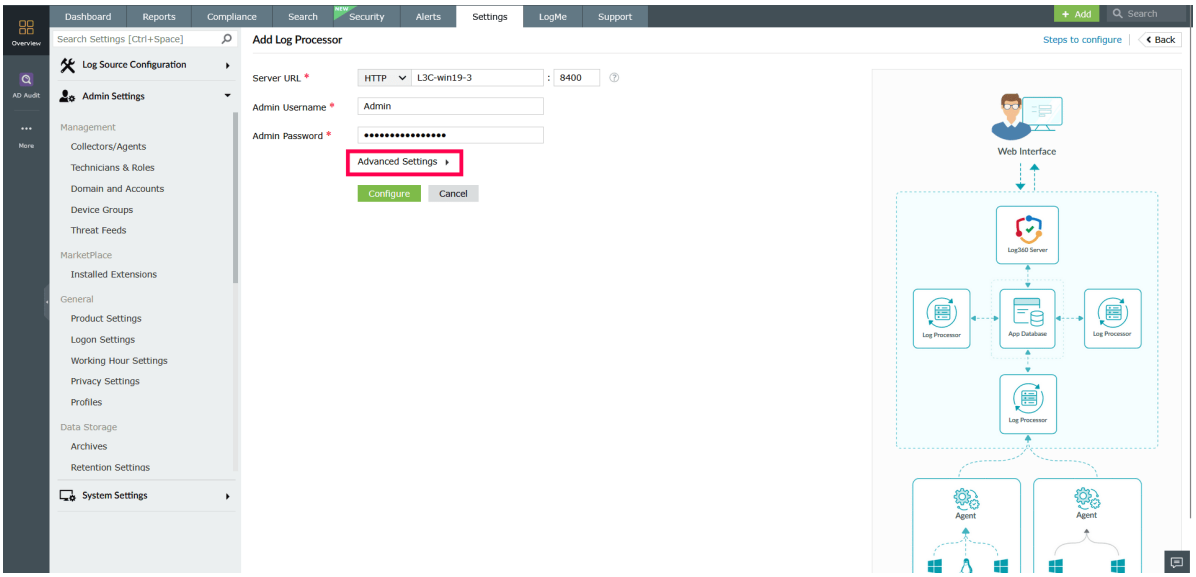


Figure 21: Configuring Advanced Settings

> NOTE
>
> When adding a Log Processor, you can only enable or disable existing roles using the Advanced Settings. Refer to this section to add and manage custom roles.

6. In the Associated Roles field, use the drop-down to select the roles you want this Log Processor to handle.
   - Default roles include: Processing Engine, Correlation Engine, and Kafka Engine, and more.
   - Custom roles include: Log Forwarding, Alerts, and more.

> NOTE

Only the selected roles will be assigned to the Log Processor.

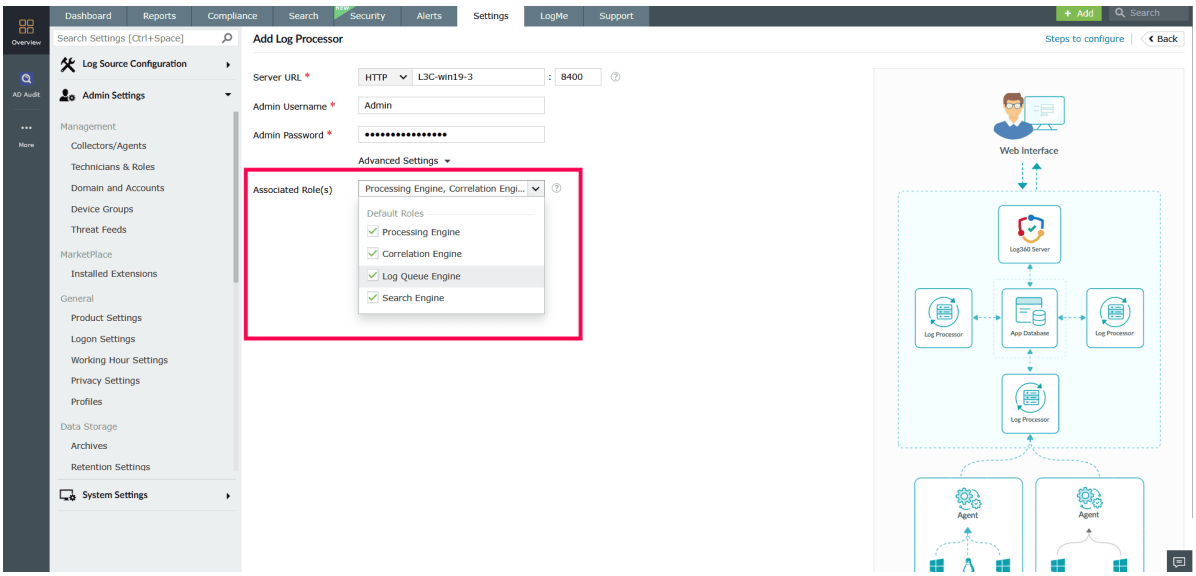


Figure 22: Assigning roles via Advanced Settings

7. To disable a role, uncheck the box next to the role you wish to disable.

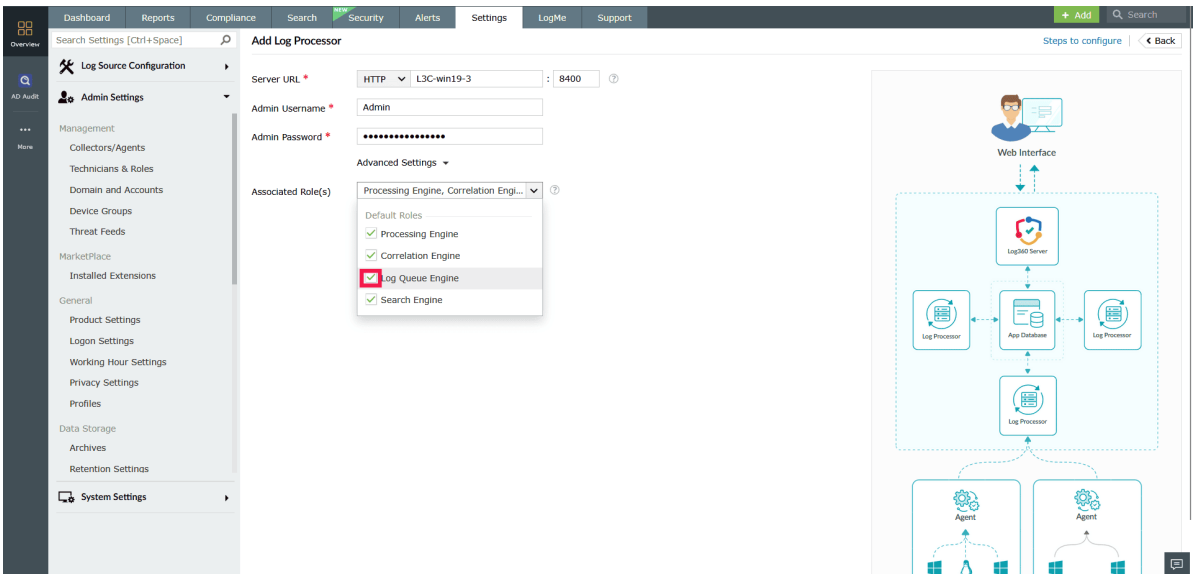


Figure 23: Assigning roles via Advanced Settings

8. In the confirmation pop-up window that appears, click Disable to confirm.

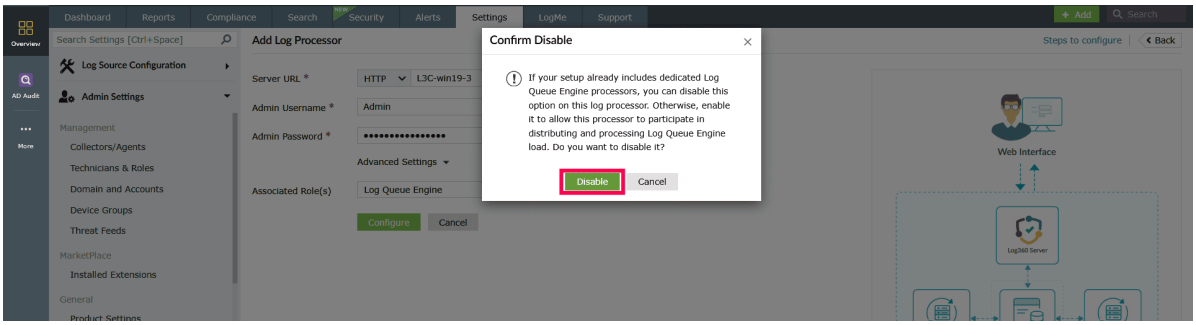




Figure 24: Assigning roles via Advanced Settings

9. ClickConfigureto add the Log Processor.

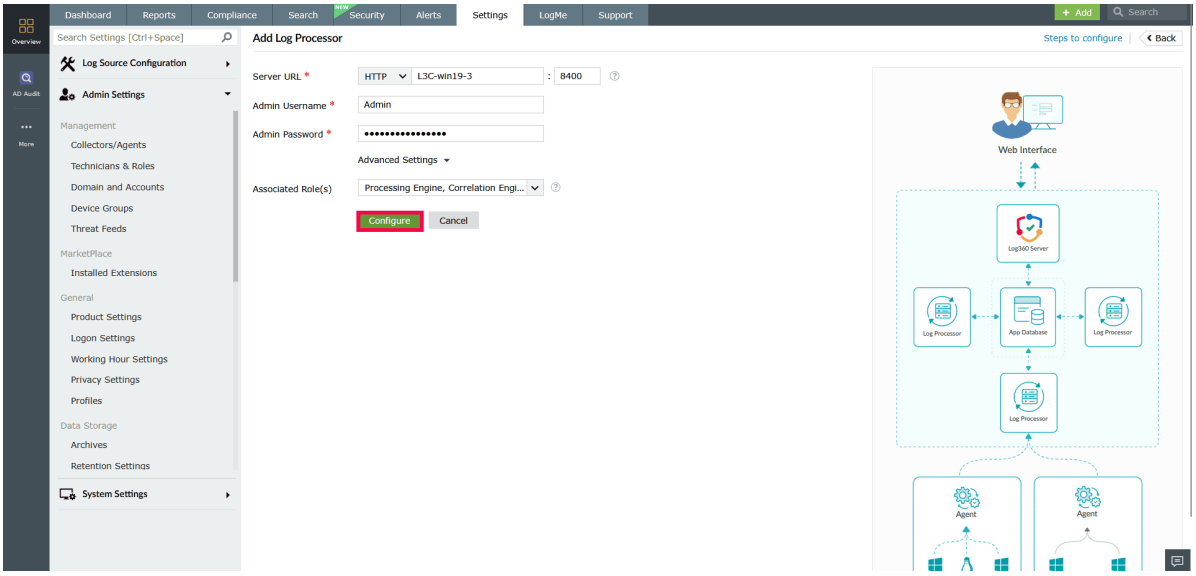


Figure 25: Configuring the Log Processors

Read also:

This document explained how to configure Log Processors. For a complete overview of architecture and management, refer to the following articles:

- Overview
- Managing Log Processors

6.1.3. Managing Log Processors

Last updated on: September 12, 2025

In this page

Overview

Modifying roles

Updating settings

Monitoring status and performance

Managing roles

Editing custom roles

Deleting Log Processors

Deleting roles in a Log Processor

Overview

This page explains how to manage Log Processors in your deployment. You can modify processor configurations, update settings, monitor performance and health, assign or modify custom roles, and remove processors or roles when they are no longer required.

Modifying roles

You can update the Log Processor to change its assigned roles: Log Collection, Log Processing, or both, depending on your deployment needs. This allows you to enable or disable specific roles for the Log Processor as required.

To modify the roles of a Log Processor:

1. Navigate to the Log Processors page and click the ✎ icon next to the processor you want to update.

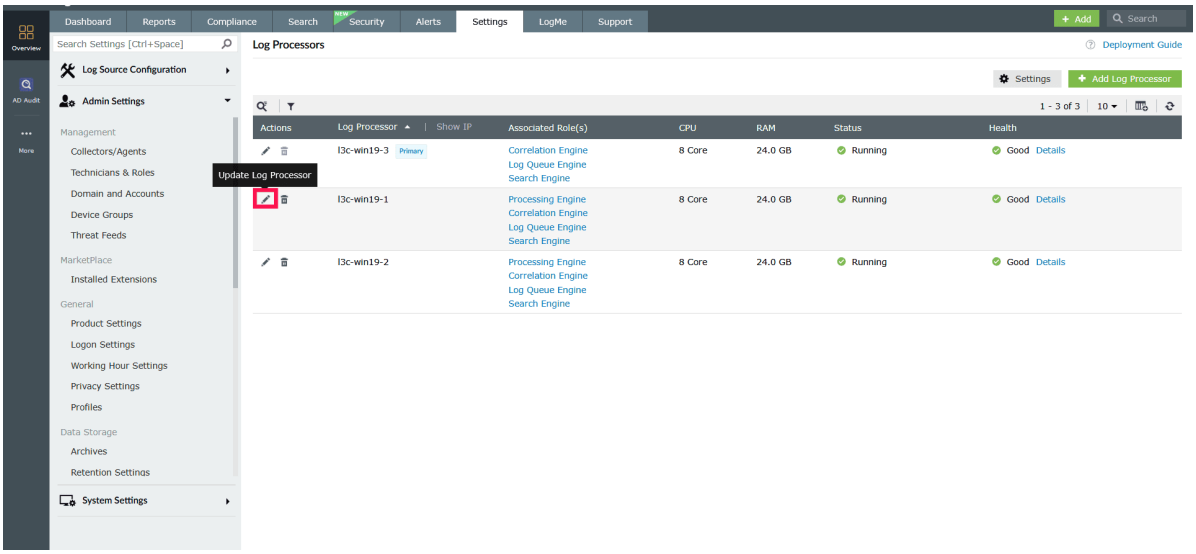


Figure 1: Modifying roles in a Log Processor

2. In the Edit Log Processor window, the Display Name of the selected Log Processor will appear. If needed, you can edit the Log Processor display name.

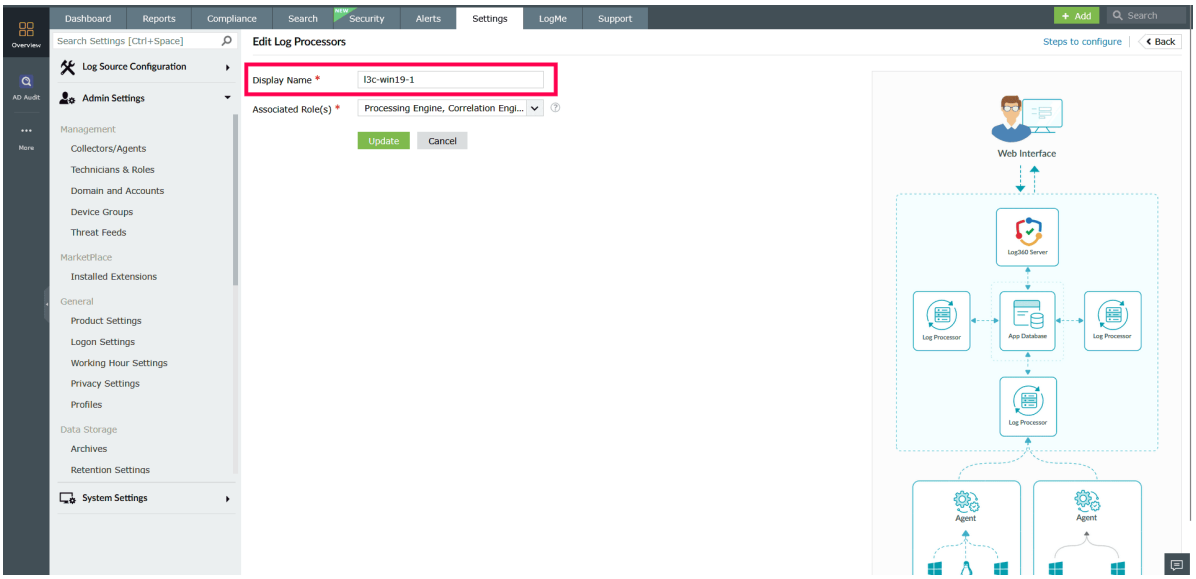
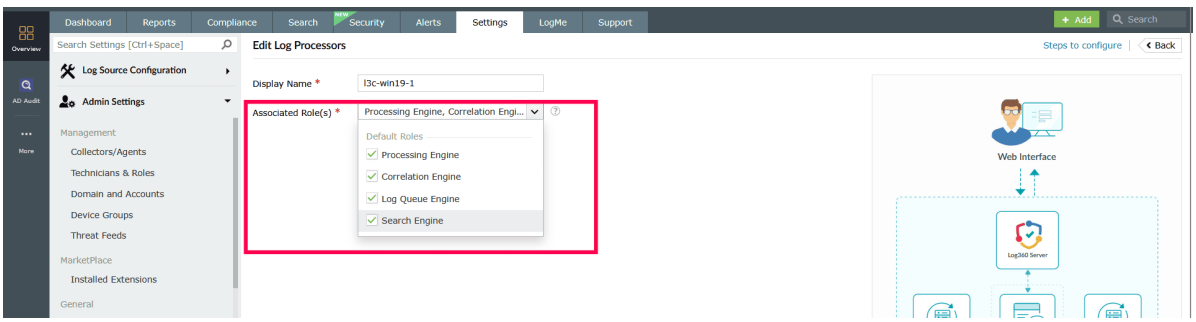


Figure 2: Modifying roles in a Log Processor

> NOTE
>
> You can configure the associated roles only when the cluster has three or more Log Processors This is because certain functions, such as Log Queue Engine and Search Engine, require at least two Log Processors in the cluster.

3. In the Associated Role(s) checklist, select or unselect roles based on your deployment needs. Available roles include:

- Processing Engine
- Correlation Engine
- Search Engine
- Log Queue Engine
- Custom roles such as Log Forwarding or Alerts



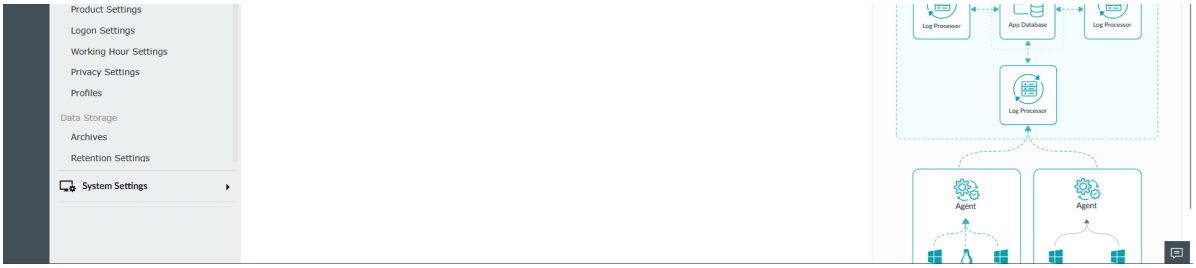


Figure 3: Modifying roles in a Log Processor

> **NOTE**
>
> A Log Processor must have at least one role assigned. It cannot be saved with all roles disabled.

4. Click Update to apply the changes.

Updating Log Processor settings

In the Log Processors page, click Settings in the top-right corner. This opens the Log Processor Settings window with the following tabs.

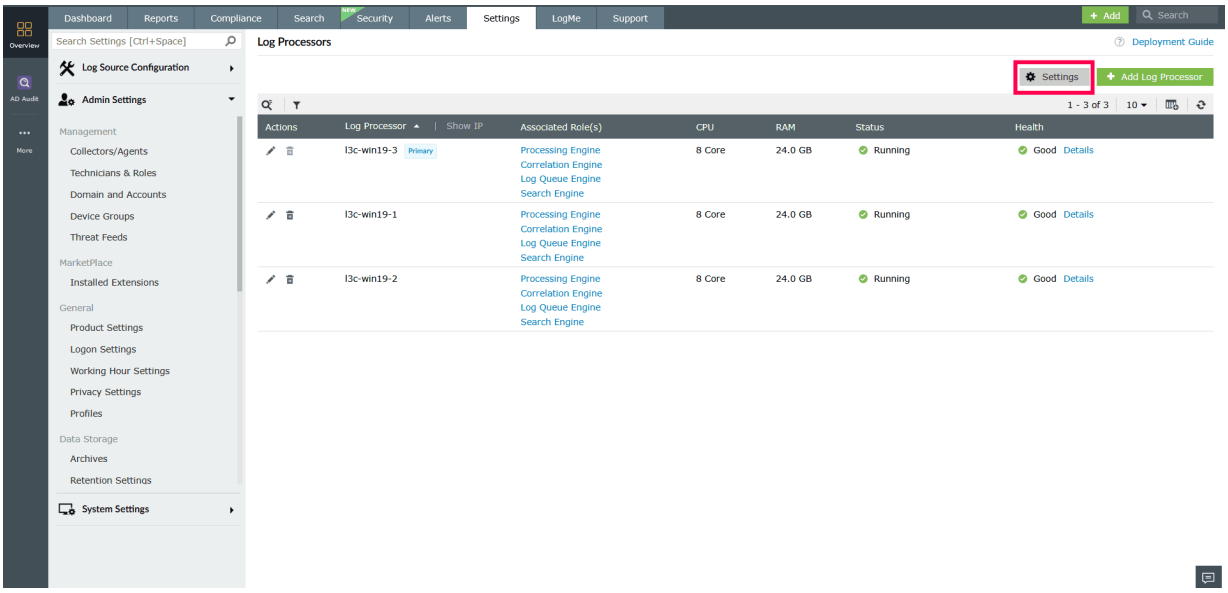


Figure 4: Updating Log Processor settings

1. Shared Storage Location

   - Enter the shared folder path.

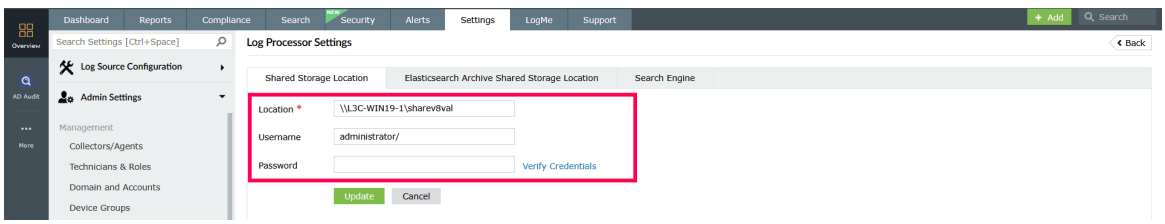




Figure 5: Configuring Shared Storage Location

- Enter the Username and Password.
- Click Verify Credentials to validate access.
- Click Update to save changes.

> NOTE
>
> Shared storage is required for transferring data between processors. Ensure the path is accessible always to avoid interruptions in log processing.

2. Elasticsearch Archive Shared Storage Location
   - Enter the archive path.
   - Enter the Username and Password.
   - Click Verify Credentials to validate access.
   - Click Update to save changes.

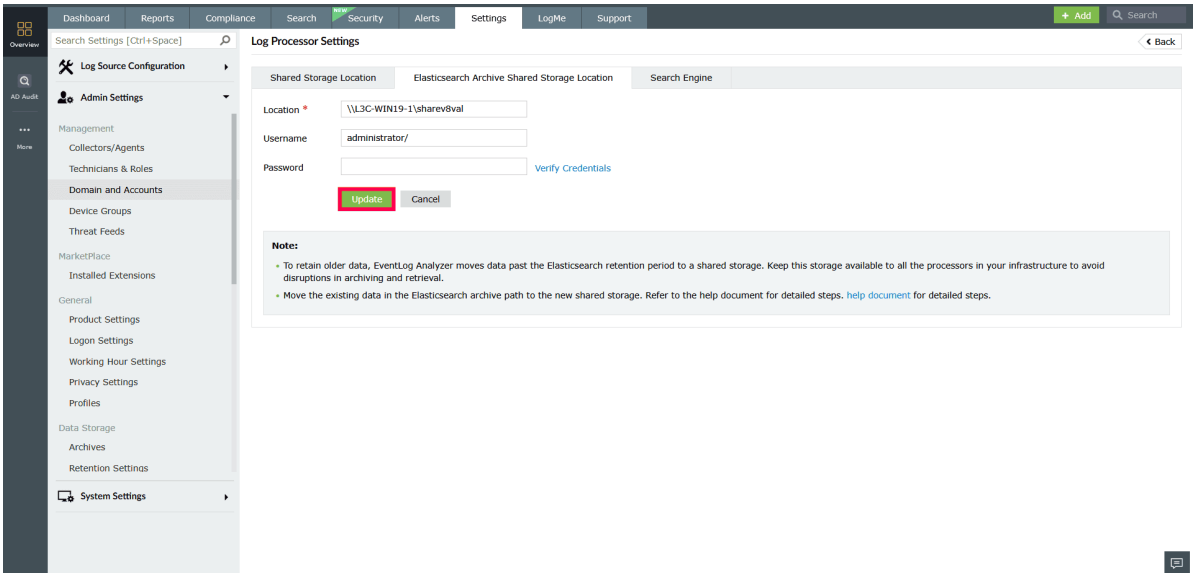


Figure 6: Configuring Elasticsearch Archive Shared Storage Location

> NOTE

This path is used to store archived Elasticsearch data. Ensure the location is accessible from all Log Processors and has enough storage capacity to accommodate archived data over time.

3. Search Engine
   - Check Enable Replica(s) to create a backup copy of indexed data.
   - Click Update to apply all changes.

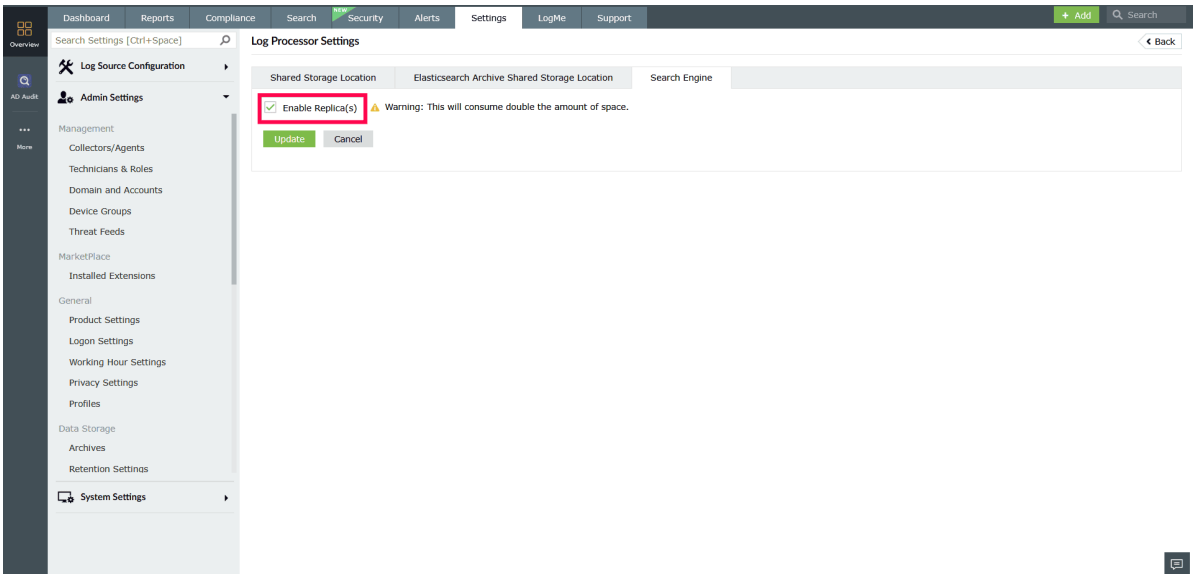


Figure 7: Configuring Search Engine

NOTE

Enabling replicas will store duplicate copies of search indexes, which requires additional disk space.

Monitoring status and performance

The Log Processors page provides real-time insights into the operational status and resource health of each processor in your deployment.

Status indicators:

- Running - The Log Processor is online and functioning normally.
- Down - The Log Processor is unreachable or has been shut down.
- Service Status Unavailable - The processor is reachable, but internal services are not reporting properly.

Health indicators:

- Good - The processor is operating without issues.
- Needs Attention - Minor issues or misconfigurations have been detected, or certain modules may not be functioning properly.

- Critical - Major issues are affecting processor functionality.

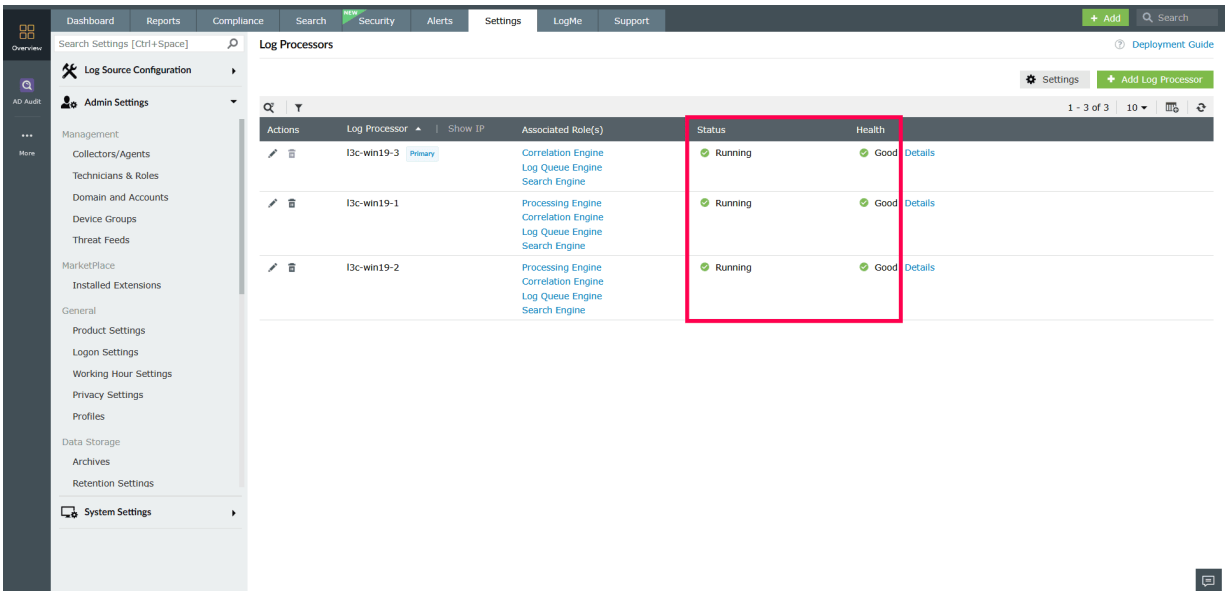


Figure 8: Status and health of Log Processors

Viewing Performance Metrics

To enable CPU and RAM monitoring:

1. In the Log Processor list view, click the icon on the right.
2. Select the CPU and RAM checkboxes.

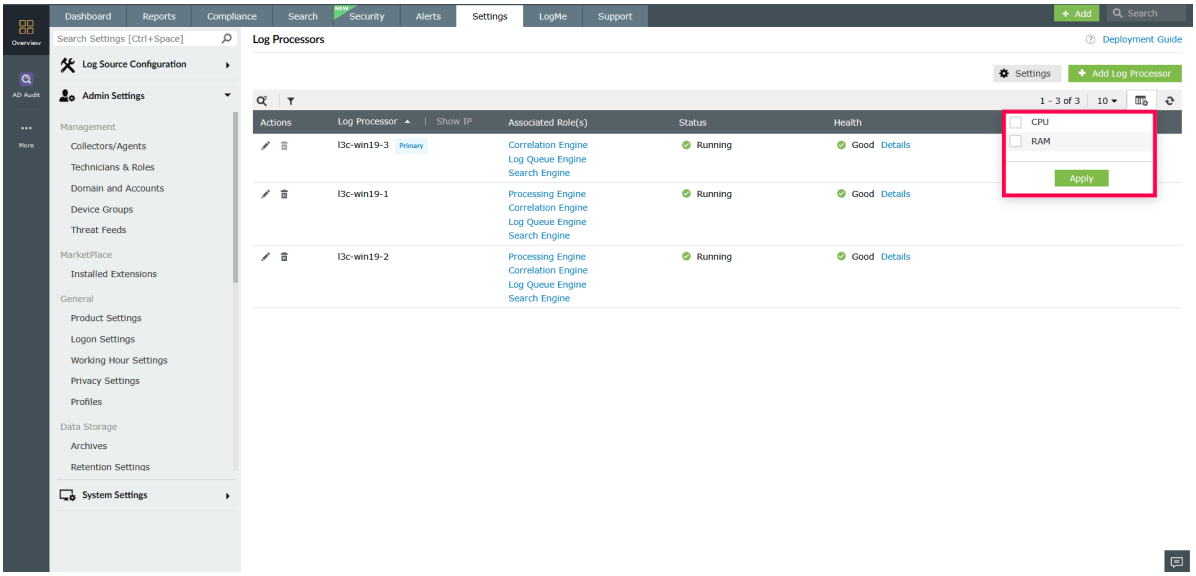
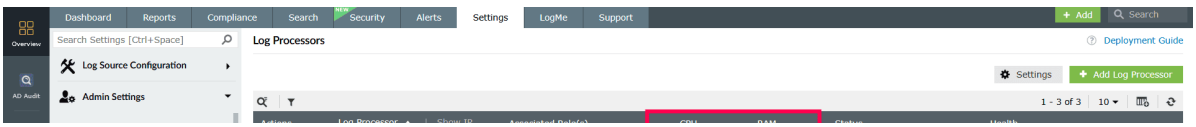


Figure 9: Enabling CPU and RAM monitoring

3. Click Apply to display these columns for all processors.



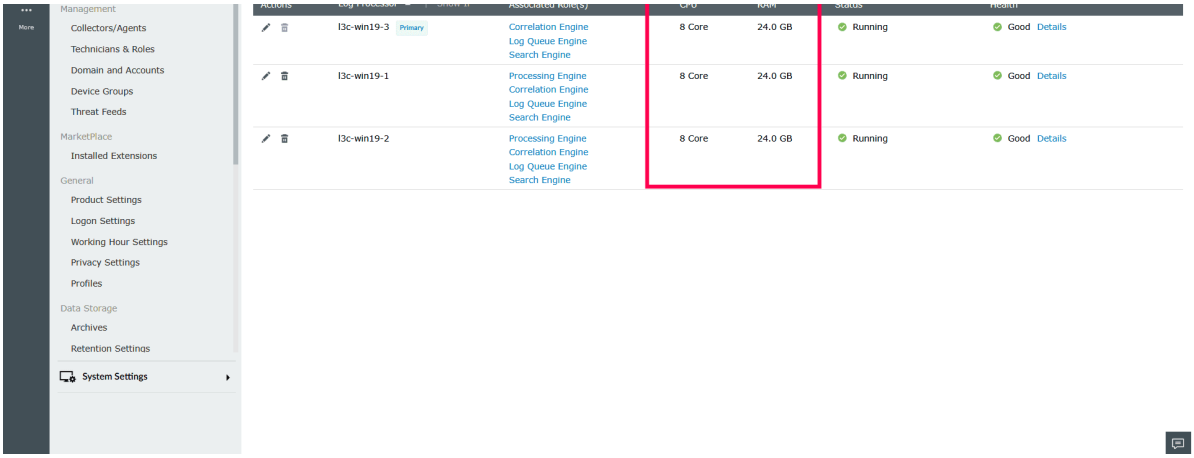


Figure 10: Enabling CPU and RAM monitoring

To view detailed metrics:

Click Details next to a Log Processor to view detailed information about its configuration, performance, and module health. The details are grouped under the following tabs.

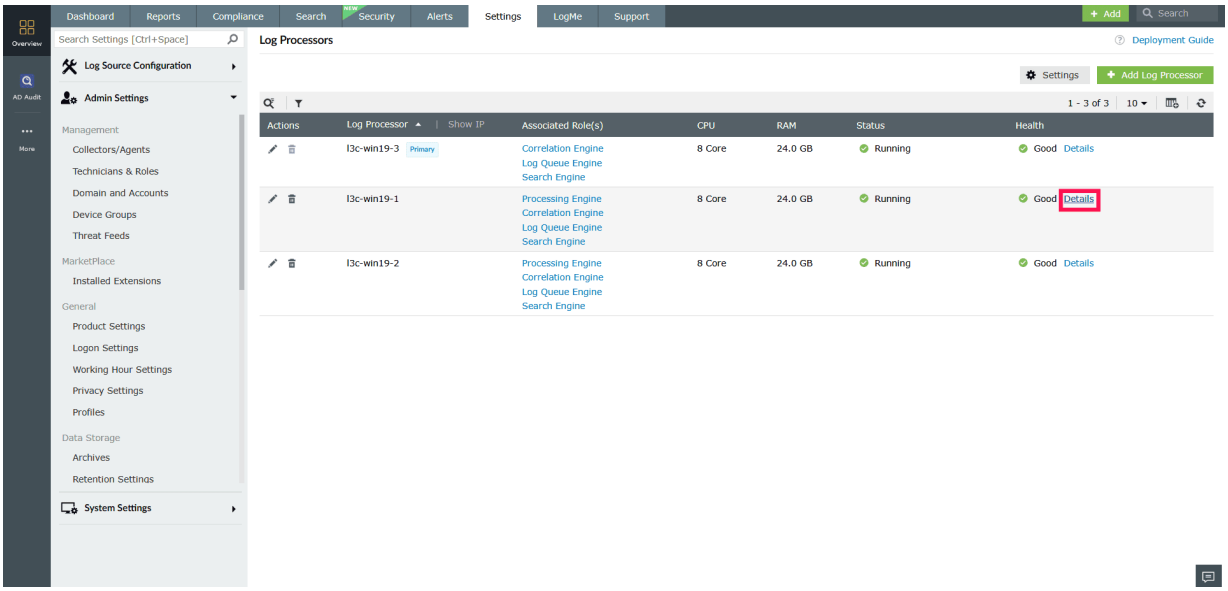


Figure 11: Detailed metrics of Log Processors

1. Health

   Shows the status of modules such as Archive, Index, Alerts, and Workflow. Each module is marked as active, inactive, or not reachable.

> NOTE
>
> You can click the Detailed Usage Report link next to the Correlation module to view in-depth performance statistics and usage history.



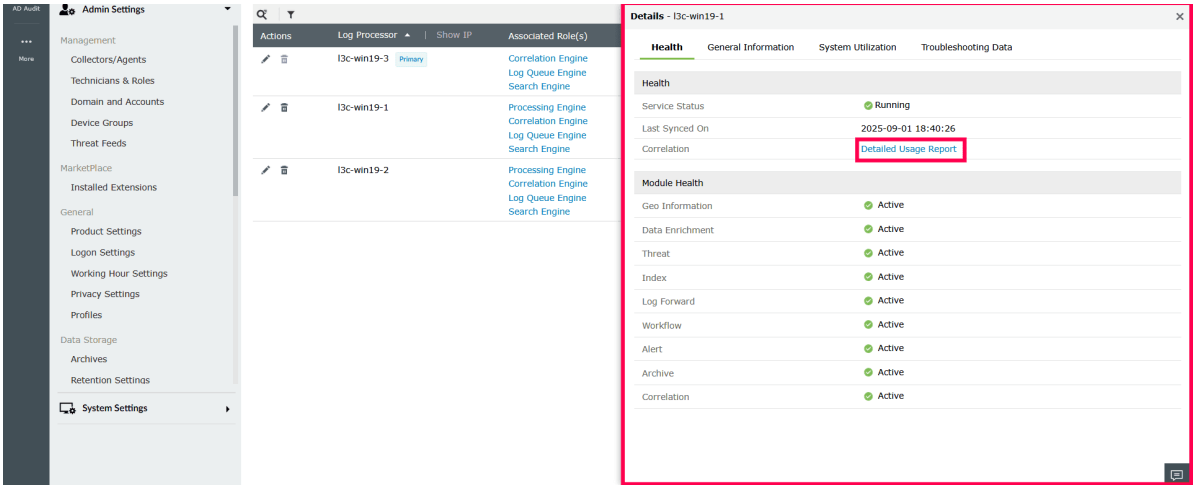


Figure 12: Viewing health metrics of Log Processors

2. General Information

   Displays system-level information including display name, IP address, operating system, JVM memory usage, working directory, number of CPU cores, total RAM, system uptime, and product version.

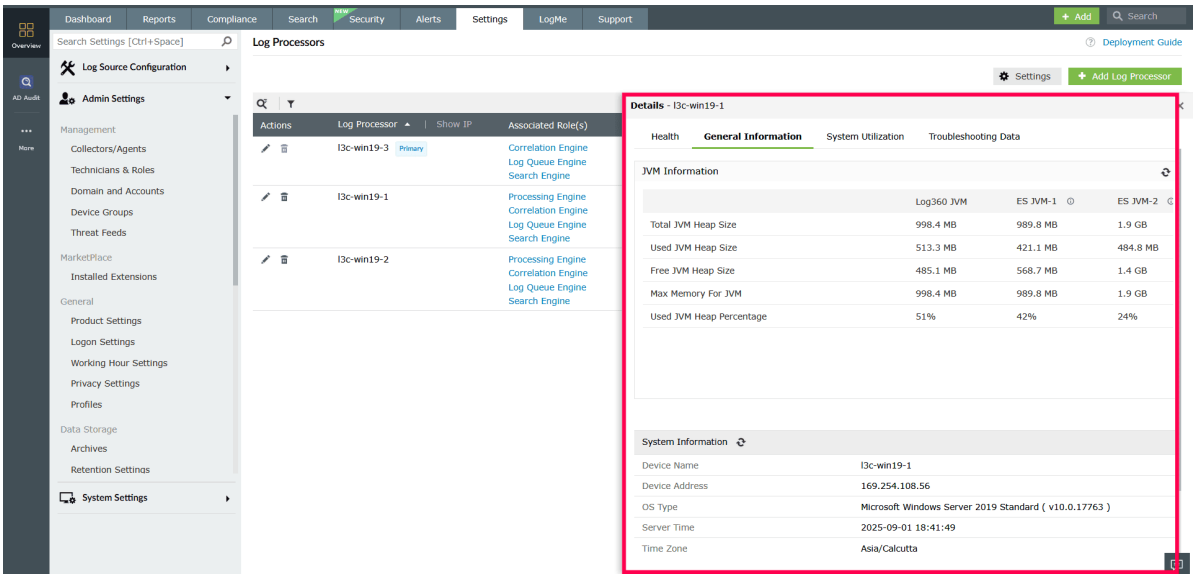


Figure 13: Viewing system information of a Log Processor

3. System Utilization

   Provides real-time metrics including total disk usage categorized by raw logs, index, archive, and database, along with CPU usage and indexed log count.

   - In the System Utilization tab, you can switch between Today and Trend views.
     - The Today view shows current usage metrics.
     - The Trend view allows you to analyze data for up to the last 30 days.

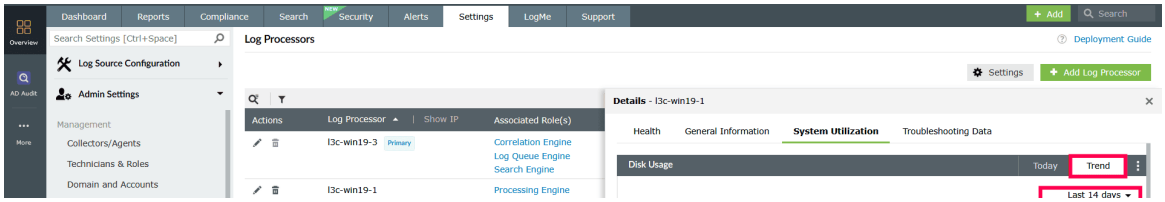




Figure 14: Monitoring resource usage in a Log Processor

- Click the ⋮ icon in the top-right corner to refresh the chart or pin it to the dashboard for easier monitoring.

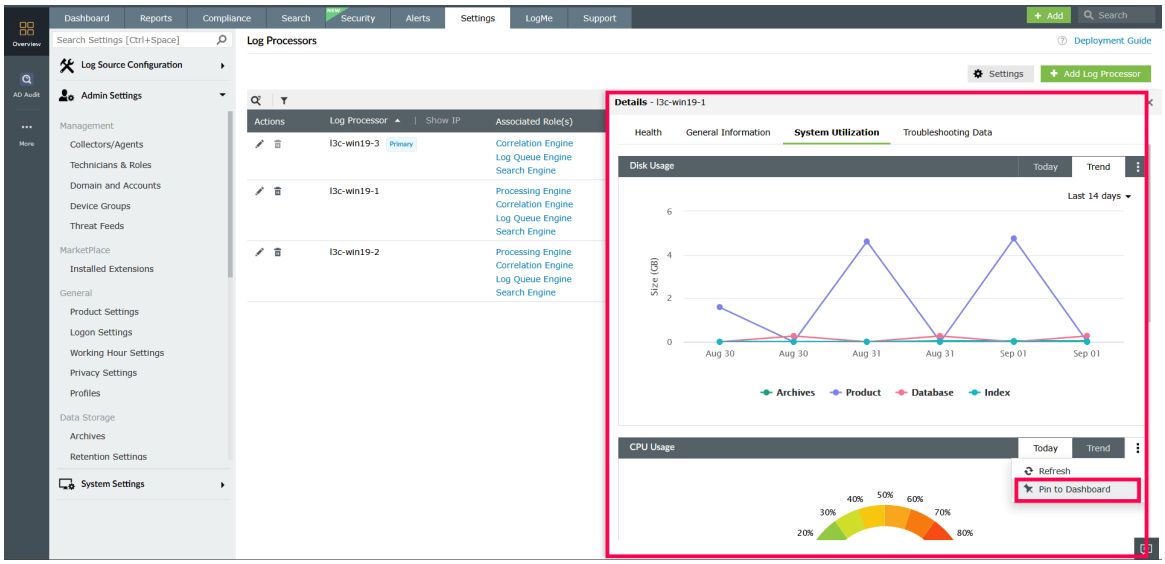


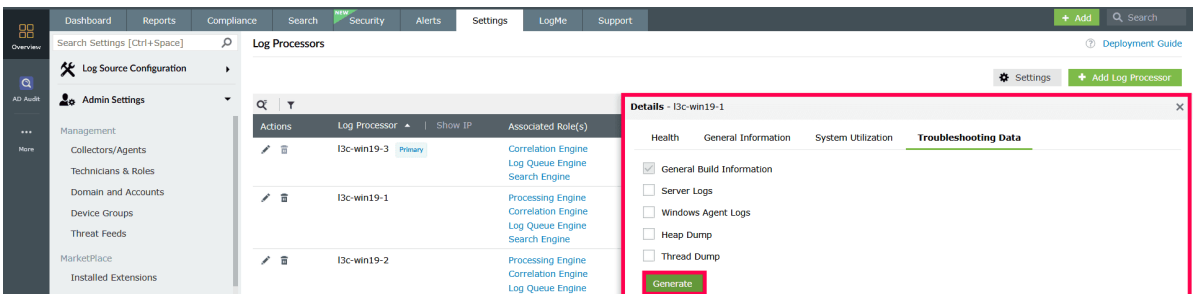
Figure 15: Monitoring resource usage in a Log Processor

4. Troubleshooting Data

   This section allows you to generate and download diagnostic files such as server logs, thread dumps, and memory dumps.

   - Select the required options from the checklist and click Generate to initiate the process.

> **NOTE**
>
> Agent logs are generated only for the Primary Log Processor.



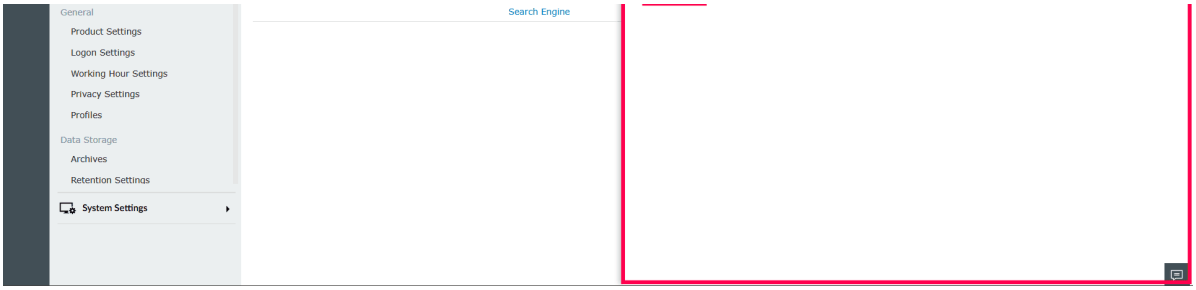


Figure 16: Generating diagnostic files for troubleshooting

Filtering Log Processors

Use the filter bar in the Log Processors page to view processors based on their assigned roles and current operational status.

To apply filters:

1. In the Log Processor page, select ▼ icon above the Log Processors list.

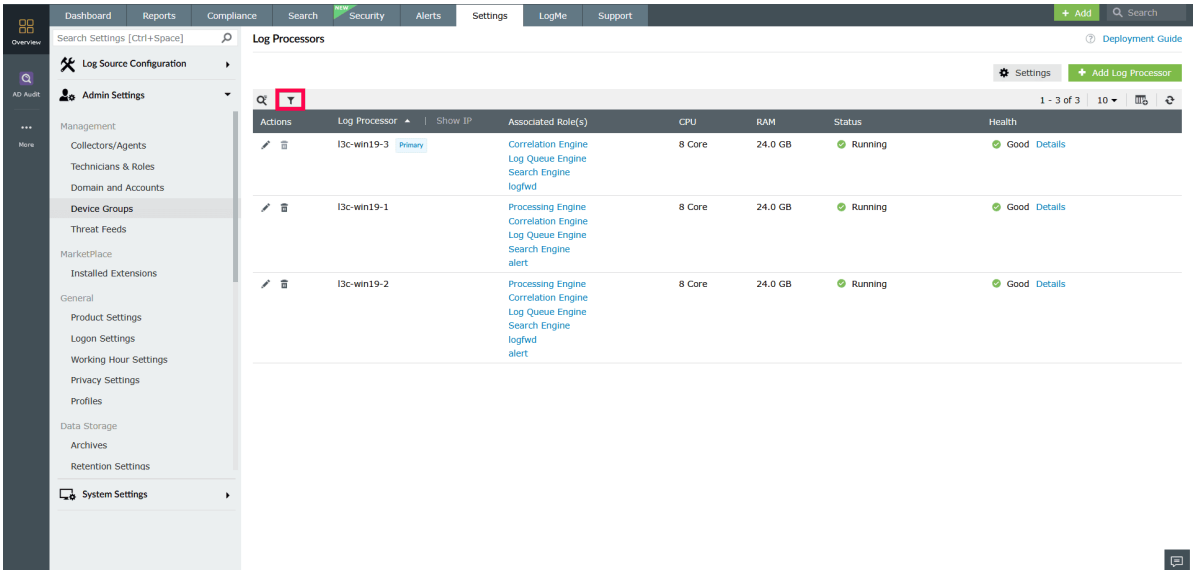


Figure 17: Applying filters to Log Processors

2. Use the Roles filter to view processors assigned to a specific role, or select All to display processors across all roles.

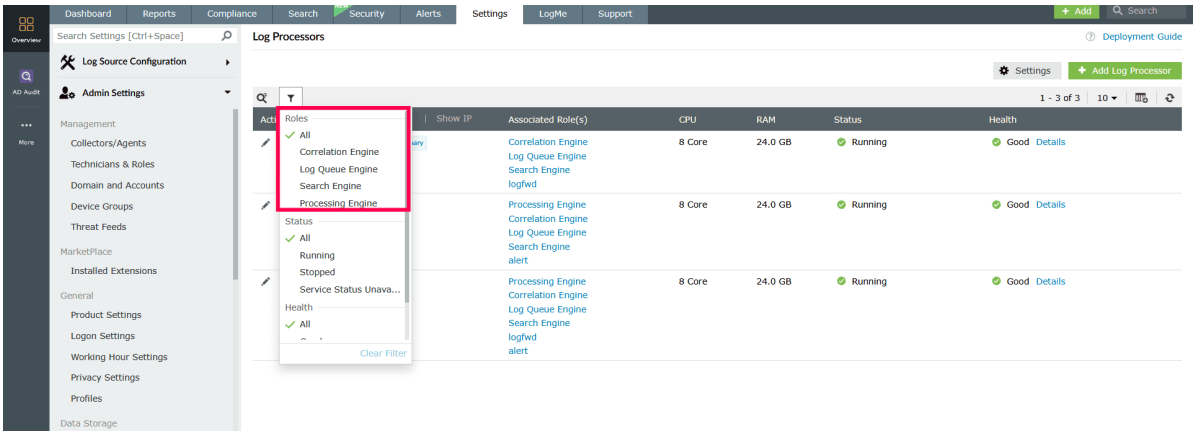




Figure 18: Applying filters to Log Processors

3. Use the Status filter to display Log Processors with a specific status, or choose All to view processors of all statuses.

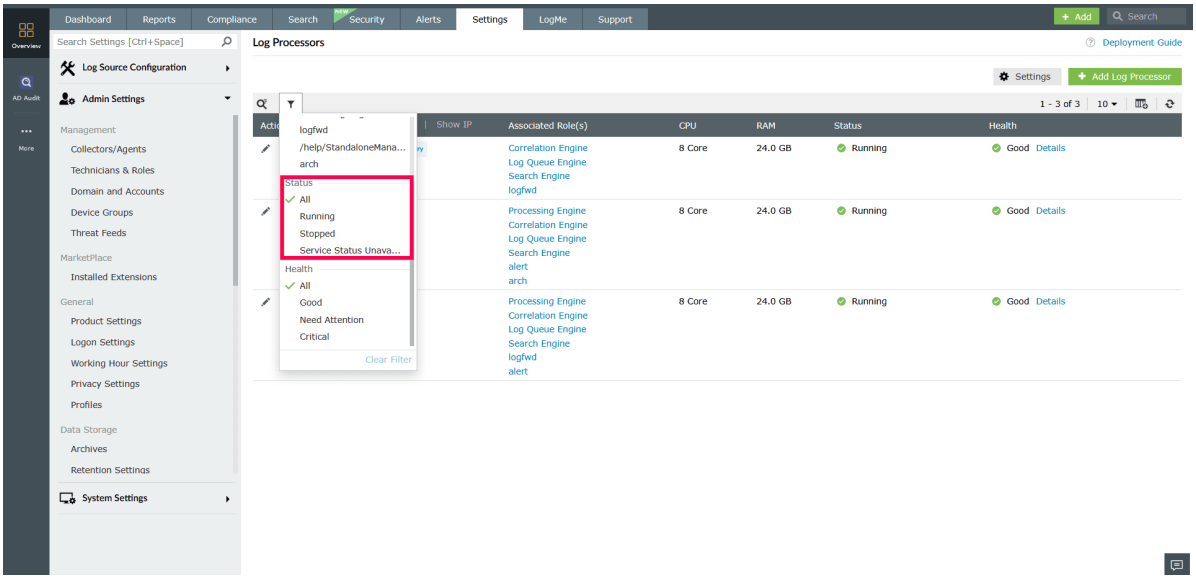
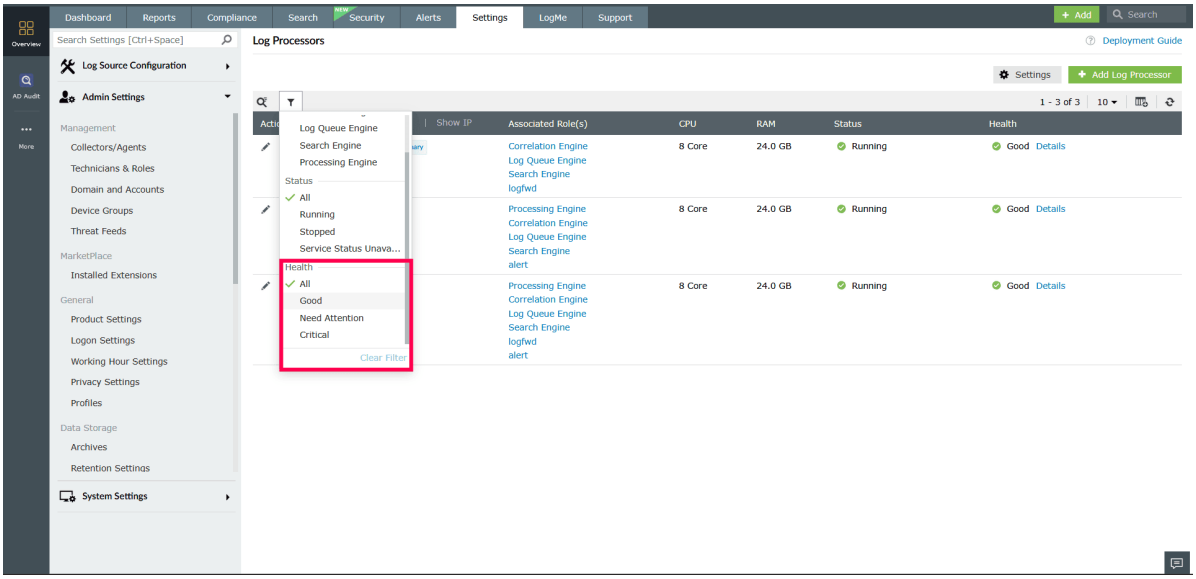


Figure 19: Applying filters to Log Processors

4. Use the Health filter to display Log Processors with a specific health status, or select All to include processors of all health states.



5. The list updates automatically to reflect your selections.

> **NOTE**
>
> You can also use the icon near the filter bar to search for a Log Processor by name.

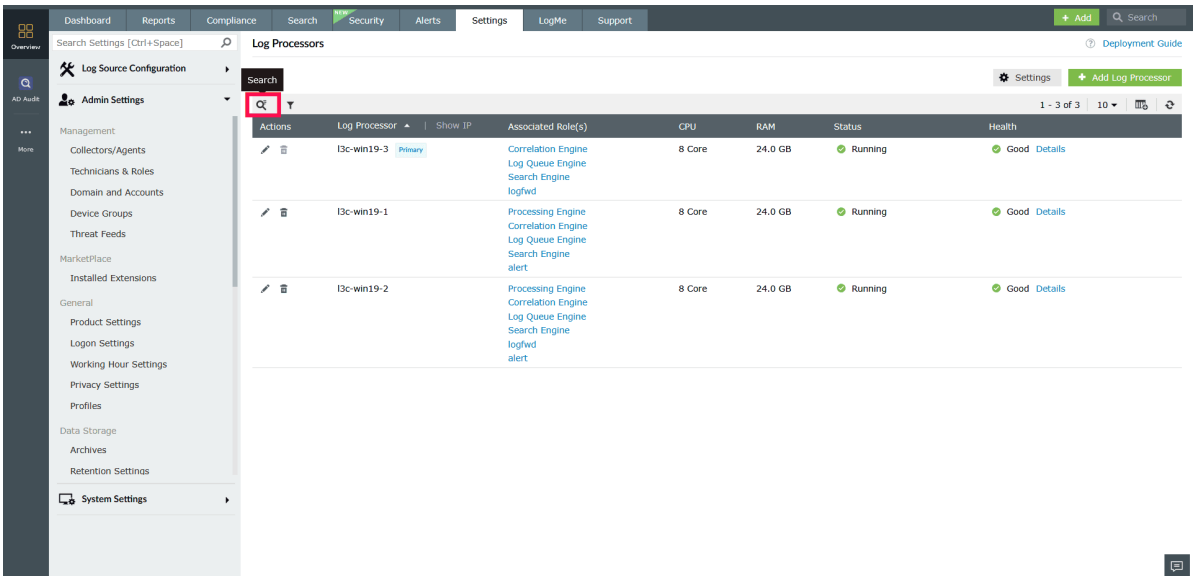


Figure 20: Locating specific Log Processors using Search

Managing roles

1. In the Log Processors page, click any role listed under Associated Role(s).

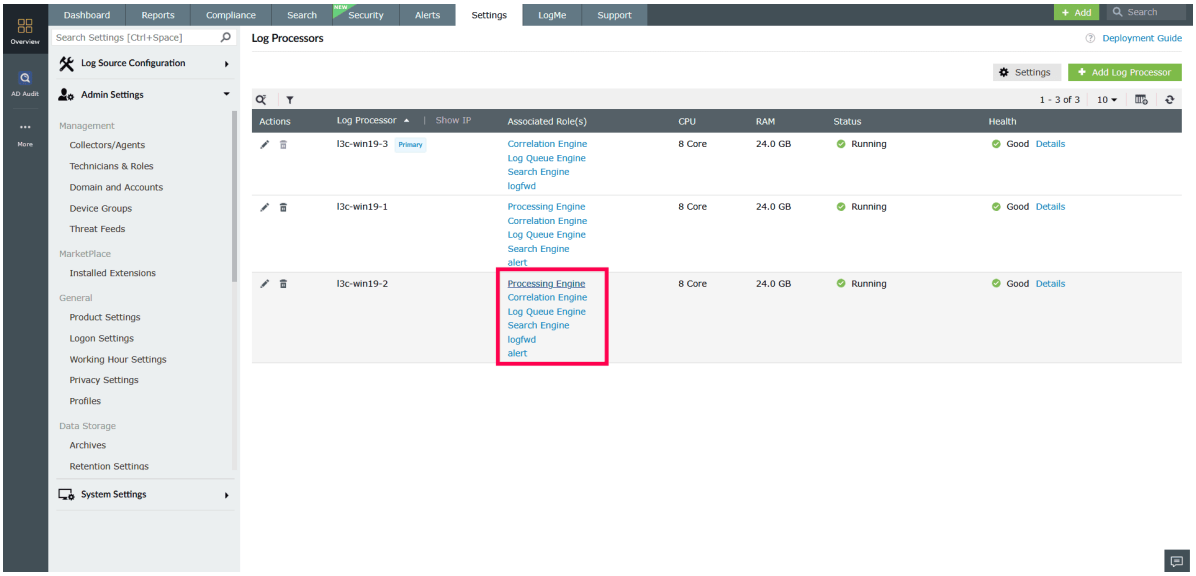
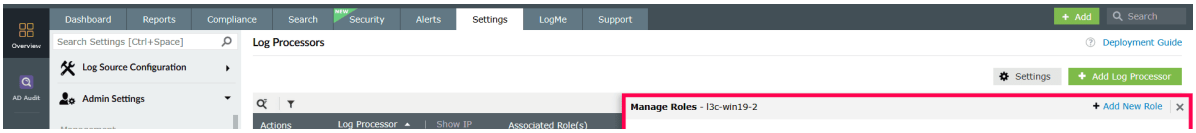


Figure 21: Managing roles

2. The Manage Roles window will open for the selected processor.
3. In the Manage Roles window, you can view the list of modules assigned to each role.



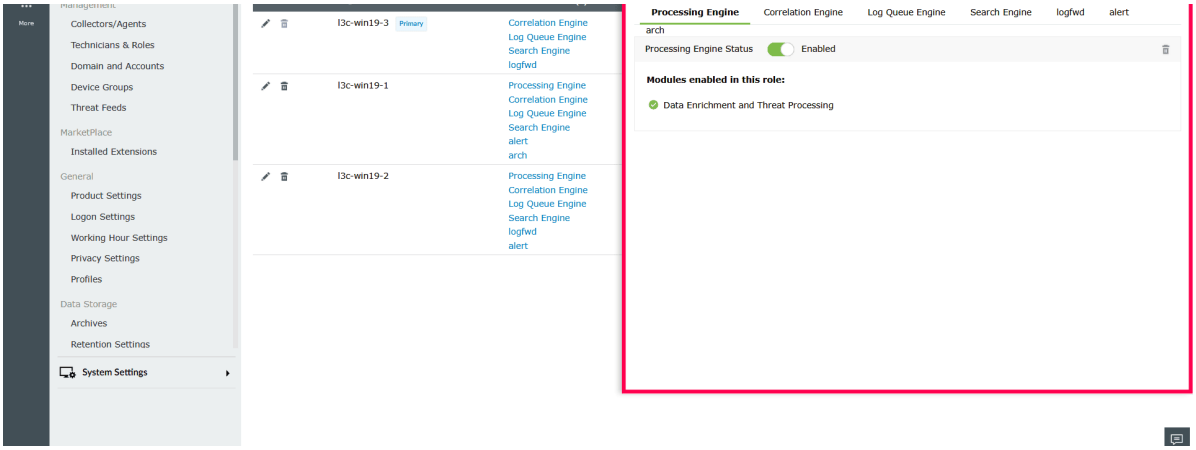


Figure 22: Managing roles

> NOTE
>
> Refer to this section to modify the roles assigned to a Log Processor. The Log Queue Engine and Search Engine roles can be disabled only here.

Adding a custom role

1. In the Manage Roles window, click Add New Role.

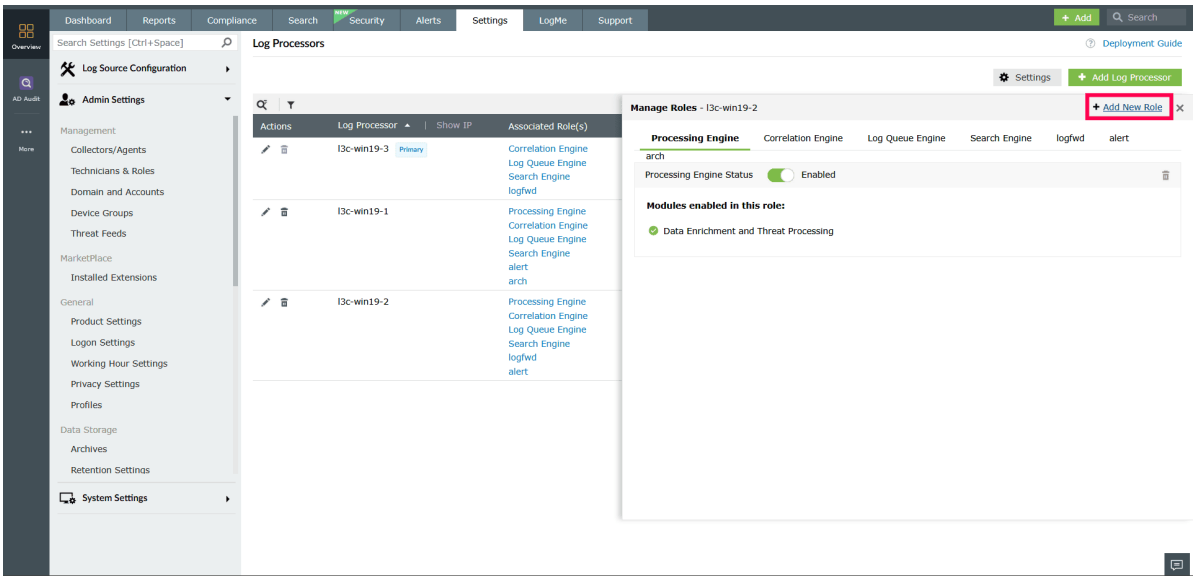


Figure 23: Adding a new role

2. Enter a name for the new role.
3. Select the required modules from the list.



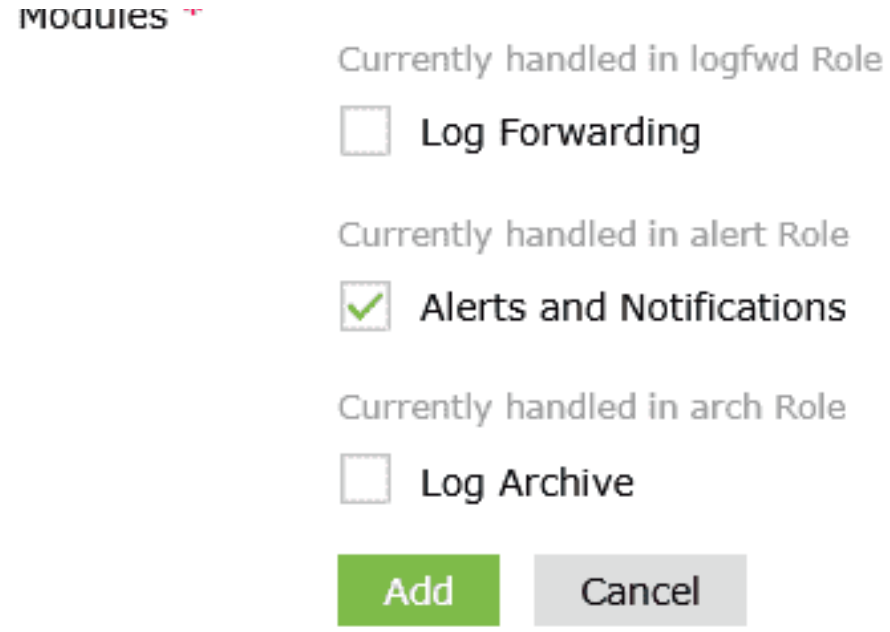


Figure 24: Adding a new role

4. Click Add to create the role.
5. Click Proceed in the confirmation popup to complete the role creation.

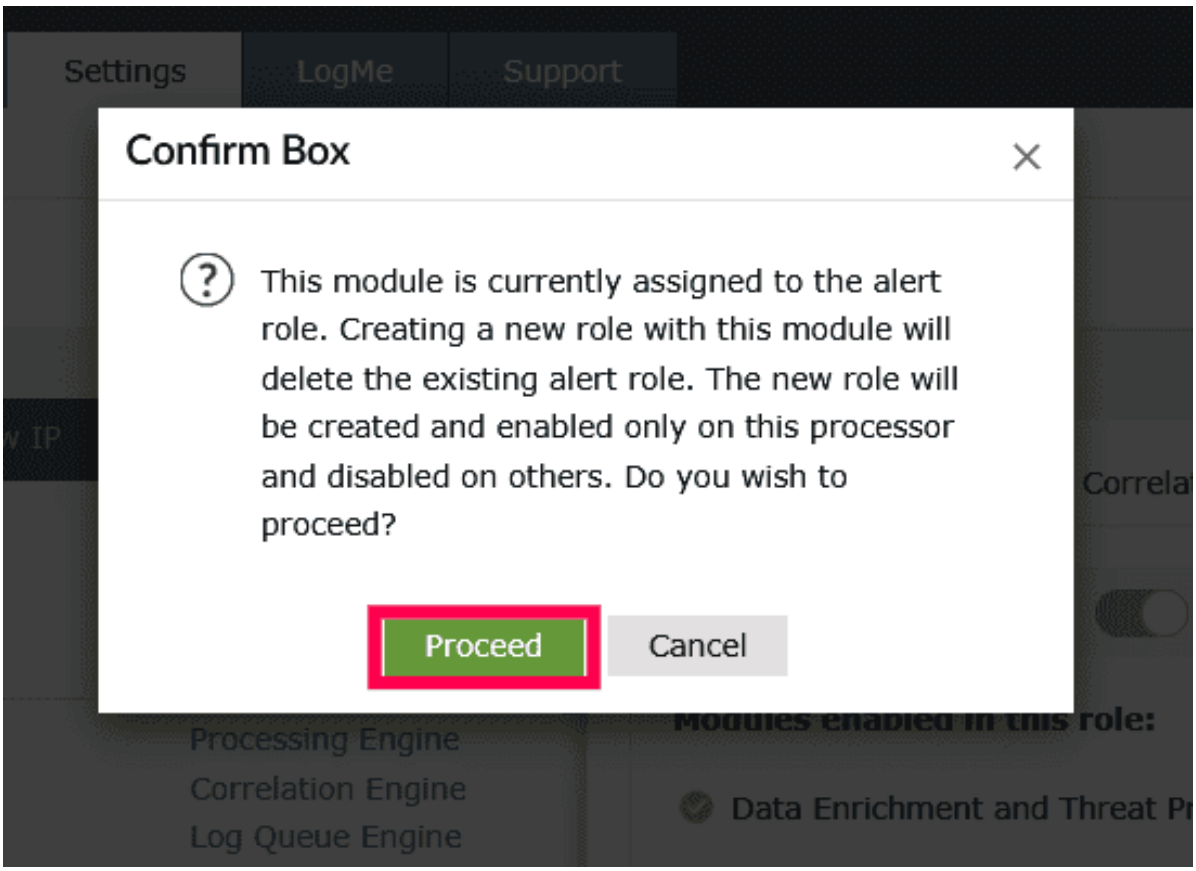


Figure 25: Adding a new role

NOTE

If a selected module is already assigned to another role, it will be removed from the existing role and reassigned to the new one.

Refer to the following examples to understand how this reassignment works:

-If the Log Archive module is currently part of the Processing Engine role and the Alerts and Notification module is part of the Alerts role, and you include both while creating a new role named Archive and Alerts, the modules will be moved from their existing roles to the new role.

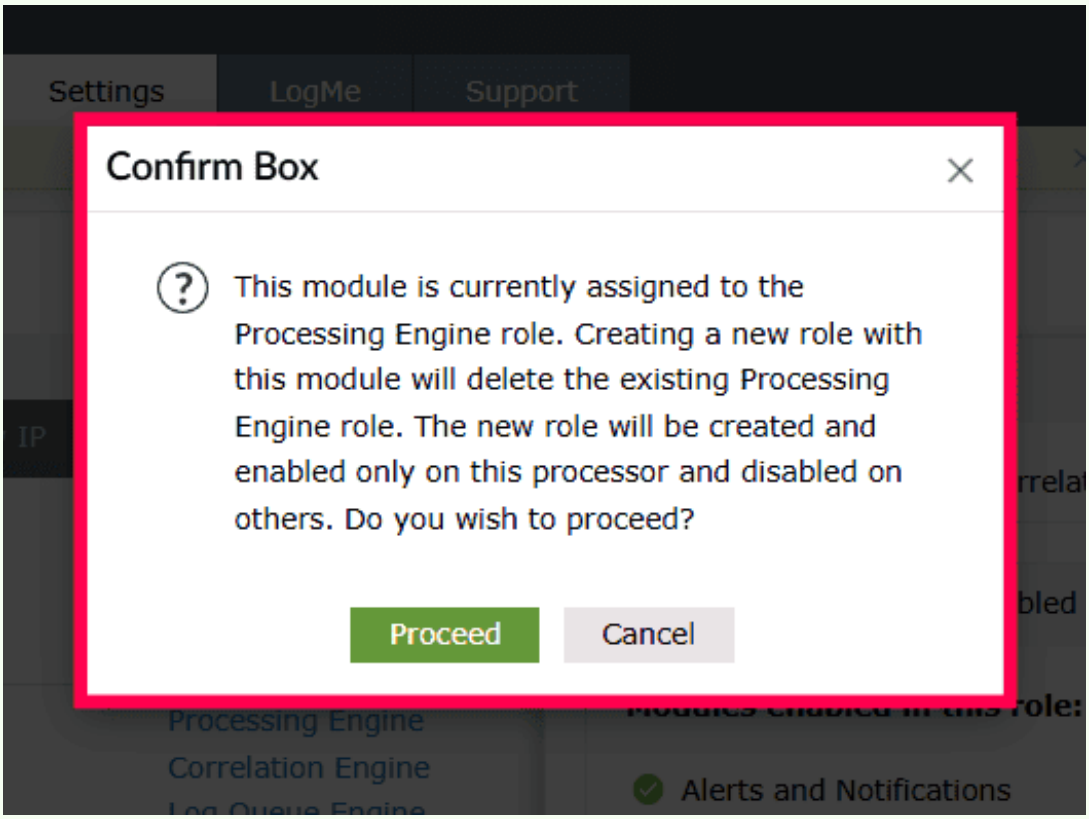


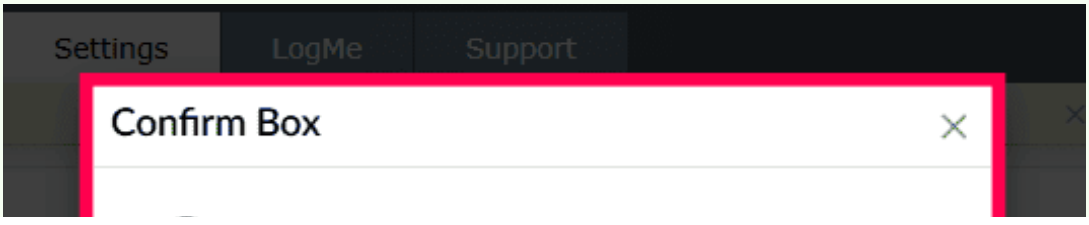
Figure 26: Adding a new role

- If the Log Archive module is currently part of the Processing Engine role, Log Forwarding is part of the Log Forwarding role, and Alerts and Notification is part of the Alerts role, and all three modules are selected to create a new role named Archive and Alerts, then:

- Log Archive will be removed from the Processing Engine role,

- Log Forwarding will be deleted from the Log Forwarding role,

- Alerts and Notification will be deleted from the Alerts role, and all three (Log Archive, Log Forwarding, Alerts and Notification) will be reassigned to the new role Archive and Alerts.



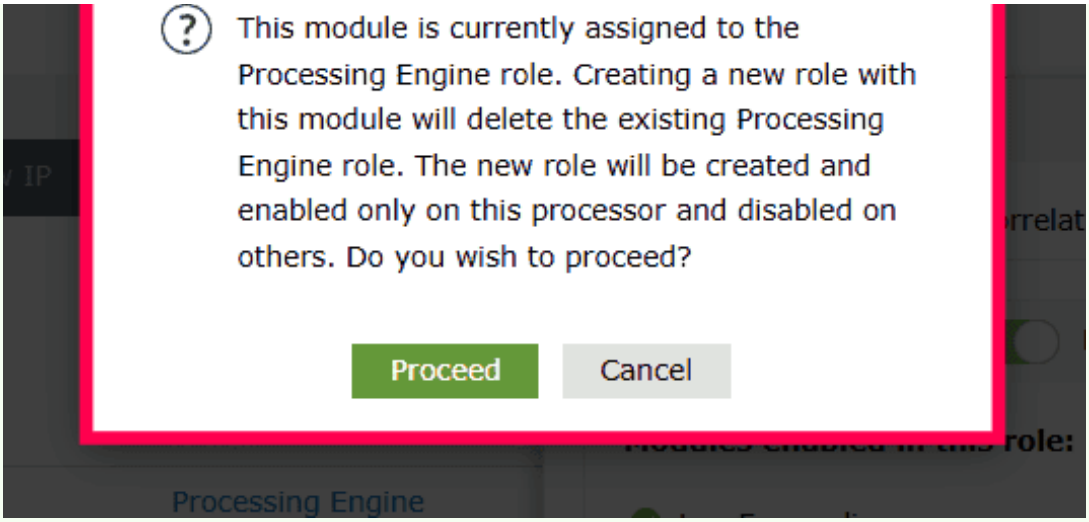


Figure 27: Adding a new role

Editing custom roles

1. In the Manage Roles window, go to the role tab you want to edit.
2. Click the ✎ icon on the top right corner.

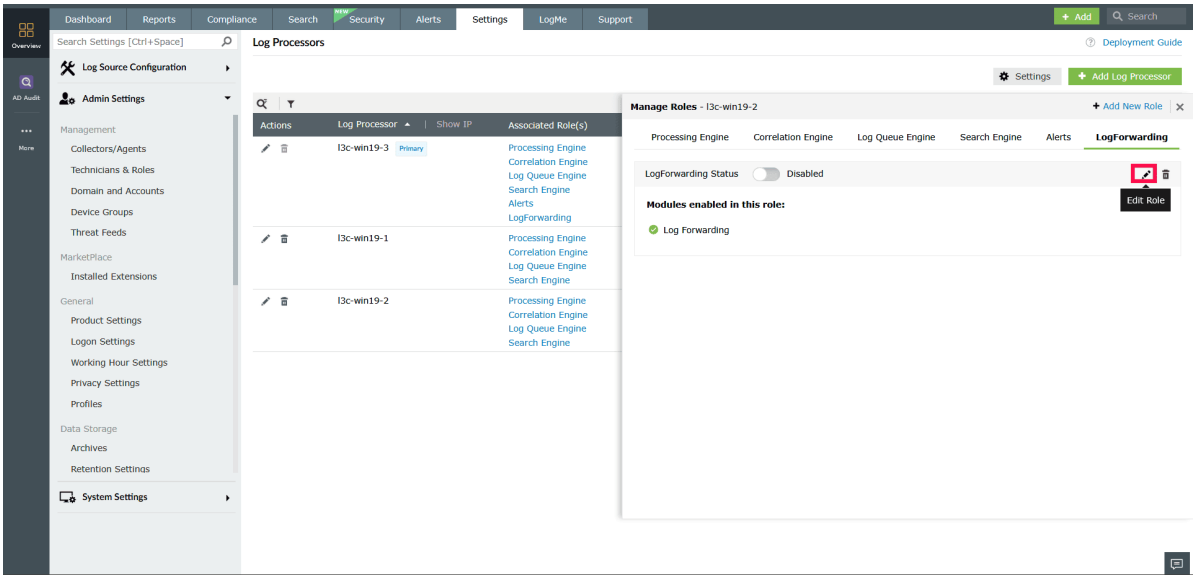


Figure 28: Editing custom modules

3. In the Edit Role panel, select or deselect the modules as needed.



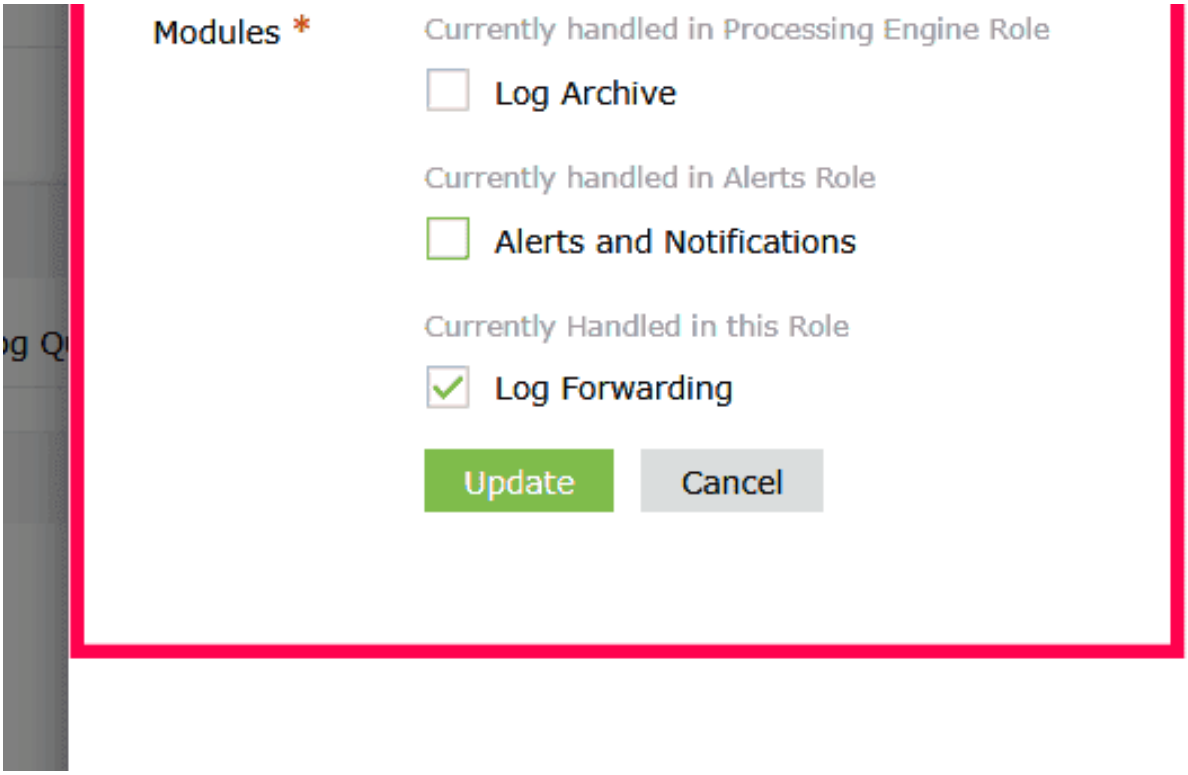


Figure 29: Editing custom modules

4. Click Update to save the changes.

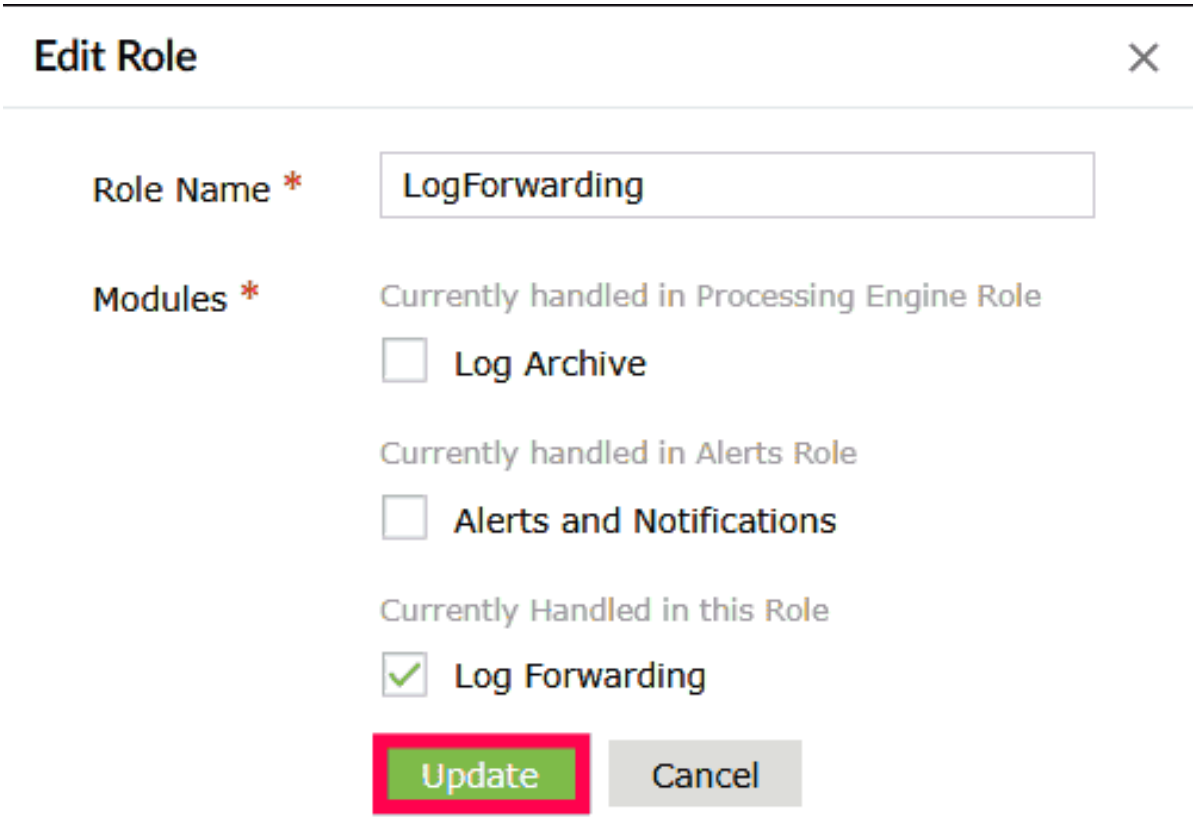


Figure 30: Editing custom modules

Deleting Log Processors

When managing Log Processors, you can delete a specific Log Processor based on your operational requirements. If you prefer to retain the Log Processor but temporarily stop its functions, you also have the option to disable specific roles.

Disabling roles

You can disable certain roles, such as the Correlation Engine, while keeping essential roles like the Kafka Engine and Search Engine enabled. This allows the Log Processor to continue handling core operations such as queuing and indexing, even if other functions are disabled.

To disable roles:

1. In the Log Processors page, click the icon next to the Log Processor you want to modify.

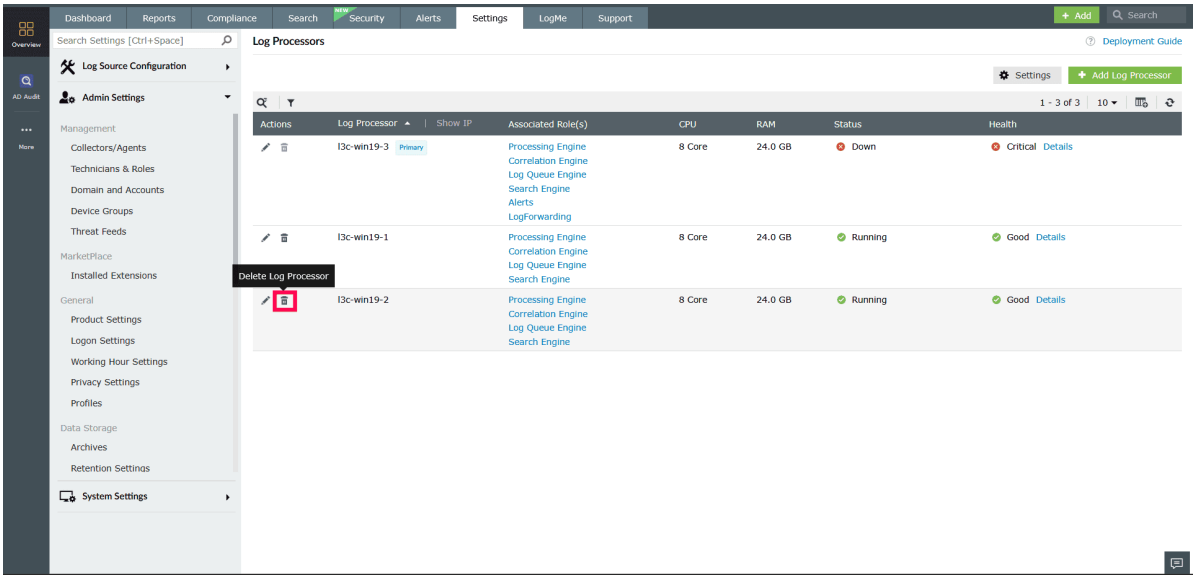


Figure 31: Disabling roles in a Log Processor

2. In the Confirm Deletion popup, click Disable Roles.

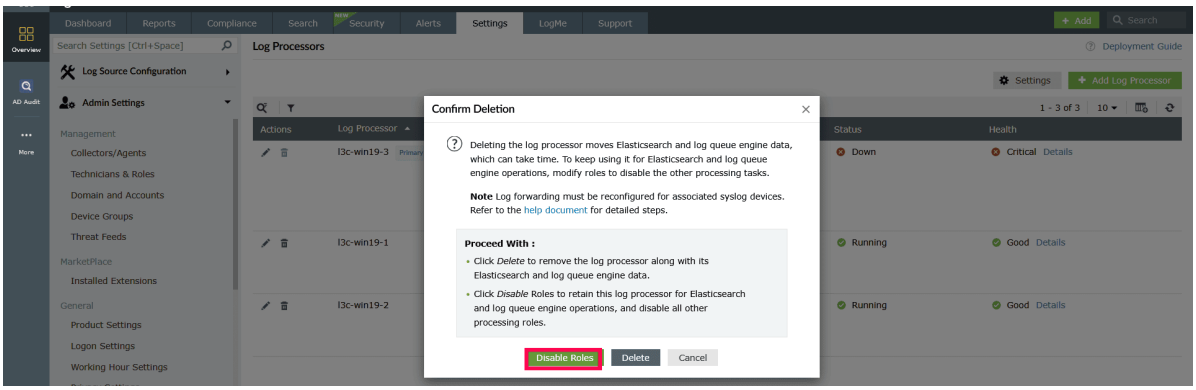




Figure 32: Disabling roles in a Log Processor

Deleting Log Processors

If a Log Processor is no longer required, you can delete it completely along with all its associated roles and data.

To delete a Log Processor:

1. In the Log Processors page, click the 🗑 icon next to the processor.

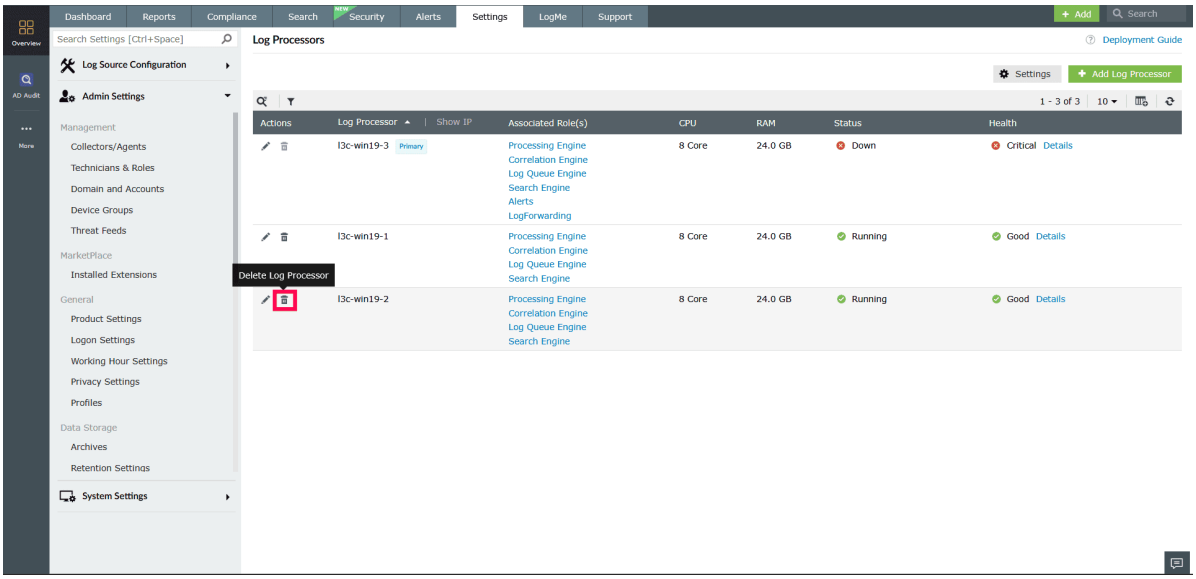
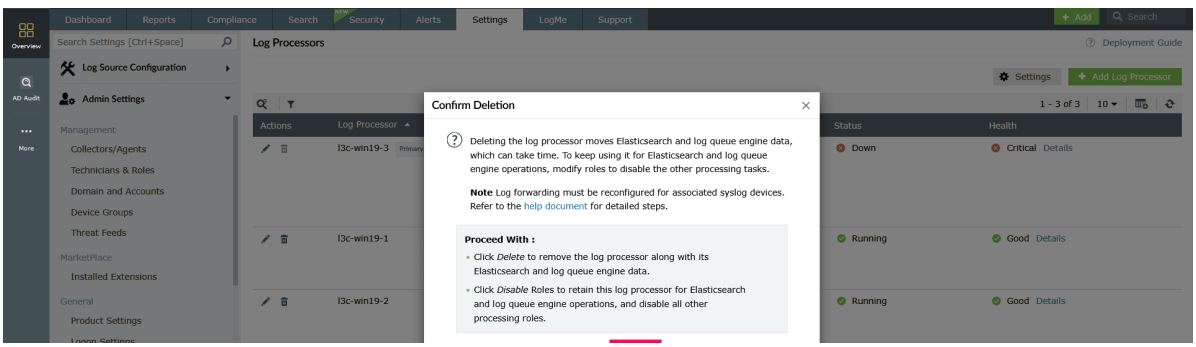


Figure 33: Deleting a Log Processor

2. In the Confirm Deletion popup, click Delete.

> **NOTE**
>
> After deletion, you must reconfigure log forwarding for any syslog devices that were associated with the deleted Log Processor.



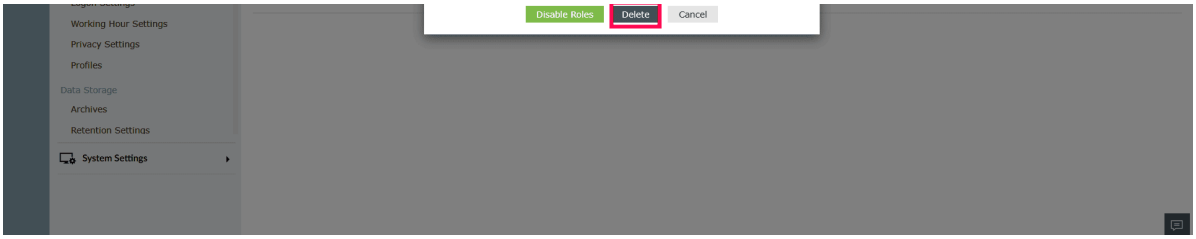


Figure 34: Deleting a Log Processor

> **NOTE**
>
> Deleting a Log Processor is irreversible, removes all associated Elasticsearch and Log Queue Engine data, may take time based on the volume of stored data, and requires.

Deleting custom roles in a Log Processor

1. Select the tab for the role you want to remove
2. Click the icon in the top-right corner of the role tab.

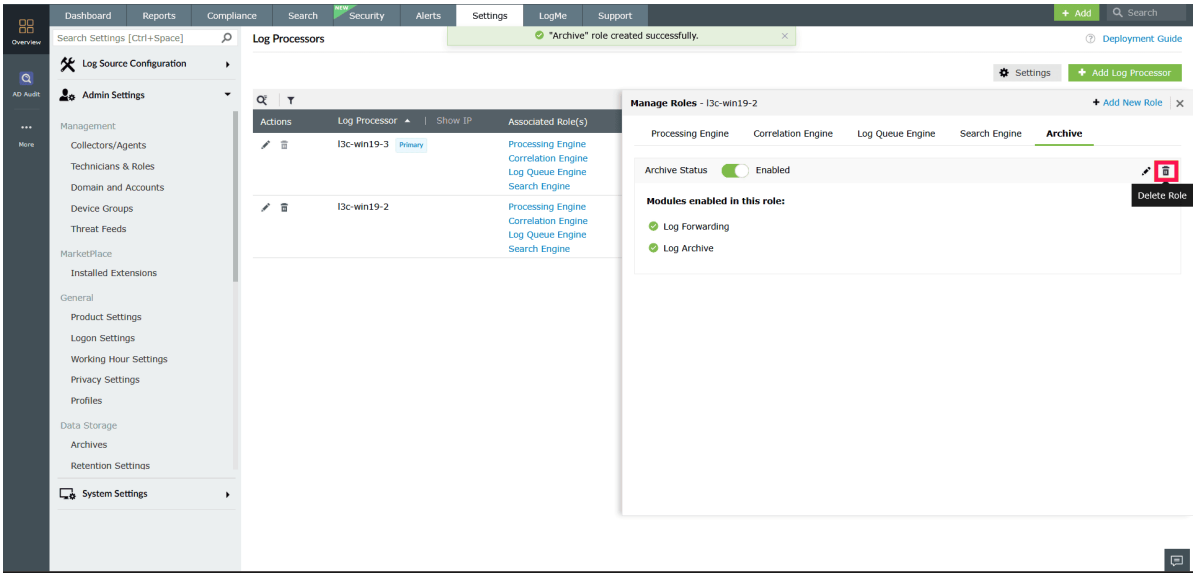
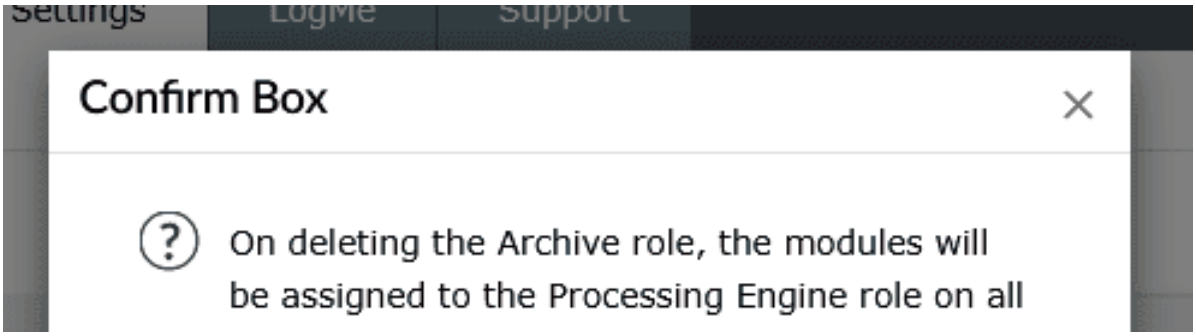


Figure 35: Deleting roles in a Log Processor

3. In the Confirm Deletion popup, click Proceed.



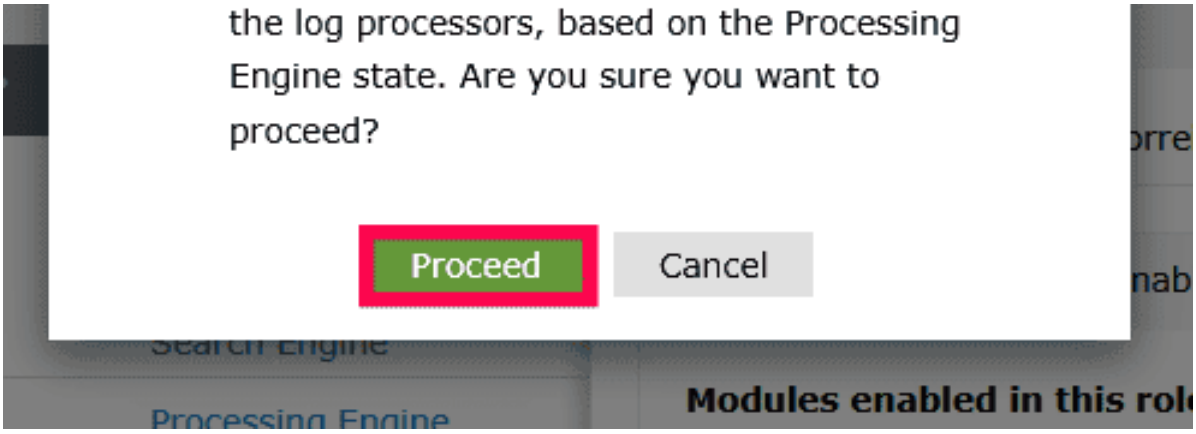


Figure 36: Deleting roles in a Log Processor

> NOTE
>
> Default roles such as Processing Engine, Correlation Engine, Search Engine, and Log Queue Engine cannot be deleted. Only custom roles, like Archive and Alerts, can be removed.

Read also

This document explained how to manage Log Processors in the product console. For a comprehensive overview of scalability and instructions on how to leverage its capabilities effectively, refer to the following articles:

- Overview
- Configuring Log Processors

6.1.4. Troubleshooting tips for Log Processors

Last updated on: September 12, 2025

In this page

- Overview
- Common issues and resolutions
- Collecting logs for support
- Service recovery steps

Overview

This page helps you troubleshoot common Log Processor issues, including connectivity, service failures, delayed log processing, and performance problems. It also explains how to collect diagnostic data and restore services.

Common issues and resolutions

1. My Log Processor status appears Down. What should I check?

- Confirm that the Log Processor service is running.
- Verify network connectivity (ping, firewall, DNS).
- Ensure the processor is running the same product version as the other processors.

2. The Log Processor status shows Service Status Unavailable. What does this mean?

- The processor is reachable, but its internal services are not responding.
- Review the product logs for initialization or startup errors.
- Restart the Log Processor service and recheck the status.

3. Why am I unable to add a new Log Processor?

Possible causes include:

- The common database is not configured or unreachable.
- The shared storage path is not configured or inaccessible.
- An incorrect Admin Username/Password was provided.

Solution: Verify that all pre-requisites are met before adding the processor.

4. Logs are not being processed or are delayed. What could be the cause?

- The distributed queue may be overloaded.
- Roles may be incorrectly configured, such as the Processing Engine is disabled.
- Shared storage may be unavailable or at capacity.

Solution: Validate role assignments, monitor system utilization, and confirm storage availability.

5. Elasticsearch archive data is not accessible. Why?

- The shared archive path may not be accessible from all processors.

Solution: Update the Elasticsearch archive location to a shared path, validate access credentials, and manually move existing data if necessary.

6. The system health status shows Needs Attention. What does this indicate?

- Minor configuration issues or module-level failures exist.
- Example: the Archive module is inactive, or Alerts are disabled.

Solution: Refer to this section and identify the affected module.

7. A role, such as Alerts or Log Forwarding, has stopped functioning. Why?

- The role may have been removed during custom role reassignment.

Solution: Refer to this section to reassign the required modules.

8. After deleting a Log Processor, logs from associated devices are not reaching the system. Why?

- Devices may still be configured to forward logs to the deleted processor.

Solution: Update device or syslog forwarding to direct logs to an active Log Processor.

9. Search and indexing performance is slow. What can I do?

- Verify accessibility of the Elasticsearch archive path.
- Enable replicas in Search Engine settings to improve performance.
- Assign additional processors dedicated to the Search role if required.

10. My Log Processor terminated unexpectedly. Why?

- The processor's Log Queue Engine went down.
- Disk space fell below the 16 GB threshold.

Solution:

- Check the Log Queue Engine health on the affected processor.
- If disk space is below the threshold, free up or increase disk capacity.
- Restart the processor after ensuring sufficient disk space.

11. Log Processor startup is paused during module population and then terminated. Why?

- The Log Queue Engine failed to find enough active processors to start the cluster.

Solution:

- Verify that the LogQueueEngine-enabled processors are running.
- Ensure that the majority of processors are up and healthy.
- Check available disk space and make sure it exceeds 16 GB.
- If the processor has stopped, restart it to reconnect to the cluster.
- Once the majority of processors are up, a paused processor will automatically resume startup.

12. A Log Queue Engine-enabled processor was added to the existing cluster, but it failed to start. Why?

- The LogQueueEngine cluster might be unstable due to one or more nodes being unavailable.

Solution:

- Check the health status of existing LogQueueEngine nodes.
- Once the majority of processors are up and running, restart the newly added processor to allow it to join the

cluster.

Collecting logs for support

- Refer to this section to generate diagnostic files such as:
  - Server logs
  - Thread dumps
  - Memory dumps

> NOTE
>
> Agent logs can be collected only from the Primary Processor.

Service recovery steps

1. My Log Processor is Down. How do I bring it back up?

1. Log in to the server hosting the Log Processor.
2. Open Services (services.msc).
3. Locate ManageEngine Log360 Service.
4. Right-click and select Start (or Restart if already running).
5. Wait for the service to initialize, then refresh the Log Processor status in the product console.

Read also

This document outlines troubleshooting tips for Log Processors. For a complete overview of configuration and management, refer to the following articles:

- Configuring Log Processors
- Managing Log Processors

7.1.1. Overview

Last updated on: September 12, 2025

Windows log collection is a critical part of security and compliance monitoring. Logs from Windows systems help in detecting anomalies, investigating incidents, and auditing user and system activities.
Log360 supports two modes of log collection from Windows devices:

- Agent-based collection: In this method, a lightweight agent is installed on the target device to collect and forward logs to the Log360 server. Agent-based collection is particularly useful when collecting logs across WANs, through firewalls, or from devices in restricted network zones such as DMZs, where direct connectivity may not be feasible. It's also ideal in environments without a stable network connection. Additionally, using agents helps reduce the CPU load on the Log360 server and offers better control over the events per second (EPS) rate.
- Agentless collection: By default, EventLog Analyzer uses agent-less log collection when a device is added. In this method, the server remotely connects to Windows devices and collects logs using WMI (Windows Management Instrumentation) or similar protocols. This approach does not require installing a separate agent on each device. Instead, the EventLog Analyzer server itself handles the collection of Windows event logs and syslog messages. This minimizes overhead on the monitored devices and simplifies deployment, although it does require administrative credentials and proper network configuration.

7.1.2. Working

Last updated on: September 12, 2025

Agent - Less Log collection

- No agents/client software required for log collection : For event log collection, eventlog analyzer application does not require a separate agent to be installed on each machine from which logs are collected. Rather the agent that collects Windows event log. In this way, eventlog analyzer application performs event log collections task without introducing additional load on the devices.
- Windows event log collection: EventLog Analyzer collects events generated by Windows. Setting up EventLog Analyzer to collect and report on events from a server, is a simple process for both Windows and UNIX systems.
- Automatically collect logs for the period, ELA Log Collector process is down: This critical log collection feature ensures that the logs are not lost even during the log collector process down time.<Need to add architecture diagram>

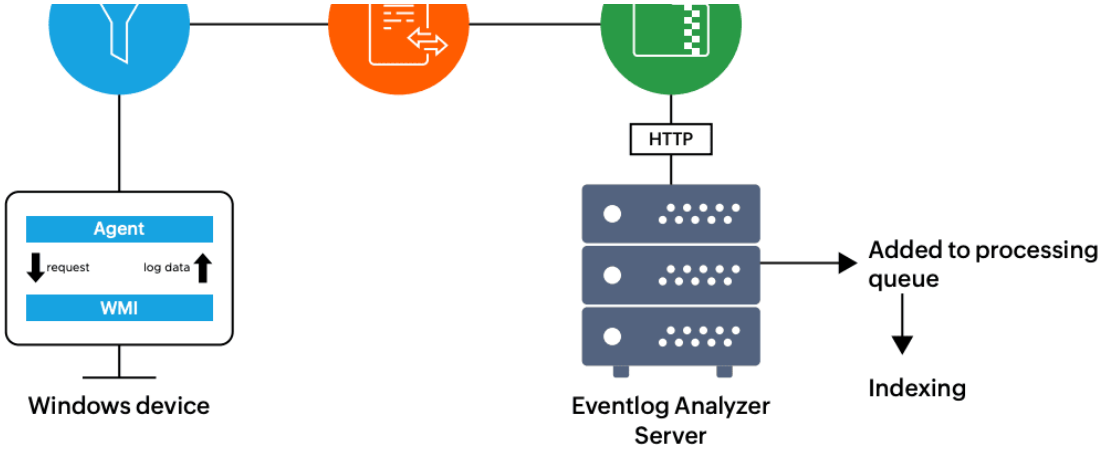
Agent for event log collection

The EventLog Analyzer Agent simplifies the collection of event logs from Windows devices. Once installed—either automatically or manually—it runs as a service on a chosen server within the network or subnet. The installation status is shown as Success, Failed (with reason), or Retry. If automatic installation fails, manual deployment is available.
After deployment, the agent is automatically discovered by the EventLog Analyzer server. It remotely collects, pre-processes, and transmits logs to the server in real time without interruption. Each agent can support log collection from approximately 25 devices, and devices can be flexibly assigned or reassigned between agents as needed. Additionally, logs can be collected directly by the server without using agents.
If an agent is uninstalled or the host device is removed, log collection for the assigned devices seamlessly switches to agent-less mode, ensuring continuity without manual intervention.

Architecture

This section illustrates the architecture of the agent-based log collection deployment. The agent should be installed on the desired device in order to remotely collect log data from it, and then send the collected log data to the EventLog Analyzer server. Whereas, in the case of agent-less log collection, the agent resides within the EventLog Analyzer server itself, rather than being present on the remote device. To deploy the agent on a specific device, execute the 'EventLogAgent.msi' file located in lib\native directory in the installation folder.





- The agent accesses the WMI infrastructure of the device internally and obtains the log data directly through WMI querying.
- Once the log data is collected, the agent does the pre-processing which includes log filtering as well as field extraction at the source, before zipping the log file and sending the log data to the EventLog Analyzer server securely through the HTTPS protocol.
- Since the log data has already been processed at this point, the server only needs to index the logs to generate the reports and alerts in real-time. This will reduce the overhead load on the server.

7.1.3. Prerequisites

Last updated on: September 12, 2025

Ports required for agentless communication

PORTS	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
TCP/135	Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Event Log Readers • Distributed COM Users User Permissions:For root\cimv2 in WMI Properties: • Enable Account • Remote Enable • Read Security. Firewall Permissions:Predefined Rule:Windows Management Instrumentation (WMI)
TCP/139	Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
TCP/445	Windows Device	EventLog Analyzer Server	SMB RPC/NP	
Dynamic ranges of RPC ports - TCP/49152 to 65,535	Windows Device	EventLog Analyzer Server	RPC randomly allocates high TCP ports for Windows Server 2008 and later versions, as well as for Windows Vista and subsequent versions	

Service account permissions

- Domain Setup
- Workgroup Setup

Domain Setup

For admin users

In a domain setup, the domain admin privilege allows admins to collect logs in Windows devices.

For non-admin users

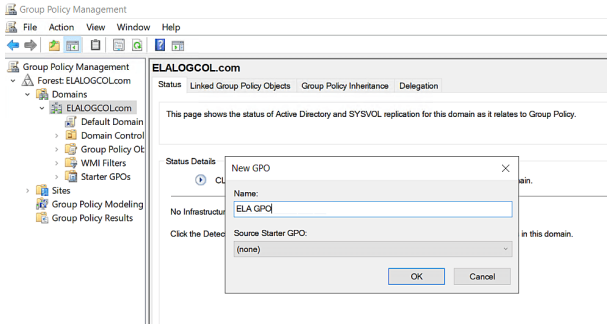
A service account has to be set up with the least privileges to collect logs in a domain setup. To create a service account with least privileges, follow the steps below.

Step 1: Create a new user

1. Log in to your domain controller with domain admin privileges.
2. Open the Run command and type dsa.msc to open Active Directory Users and Computers.
3. Right click on your domain → New → User.

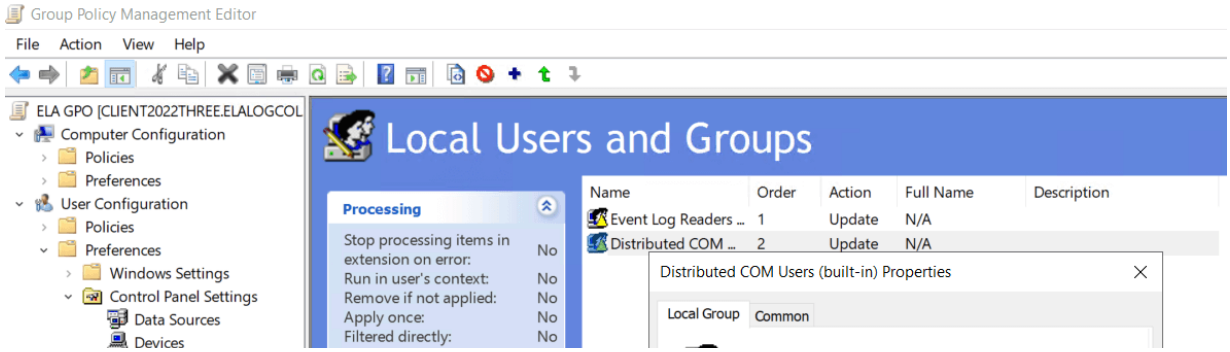
Step 2: Create a new domain level GPO and link the GPO

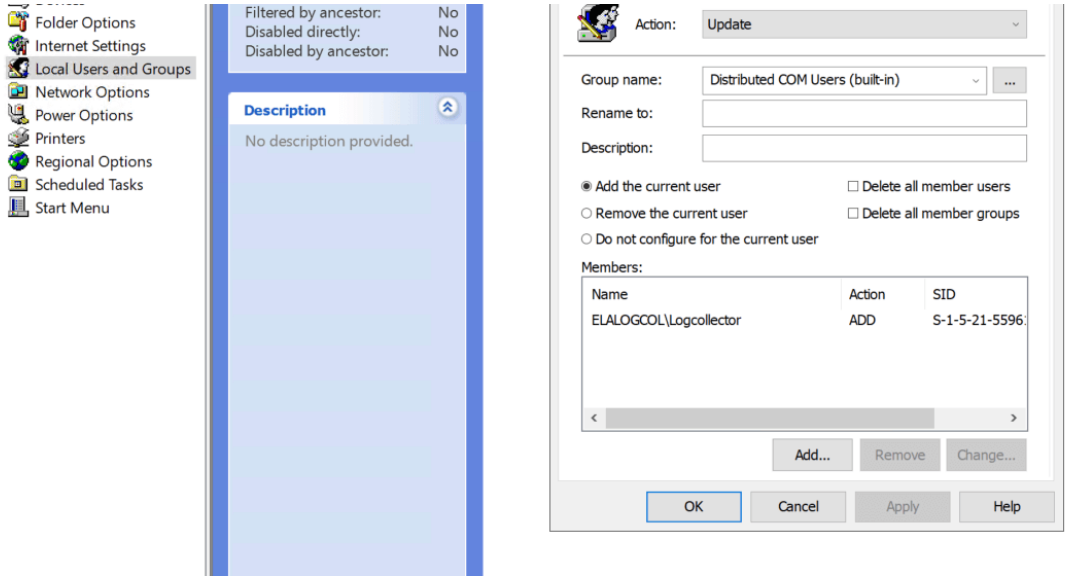
1. Open the Run command in domain controller and type gpmc.msc to open Group Policy Management Console.
2. Right click on the domain → Create a GPO in this domain and link it here.
3. Name the GPO as "ELA GPO" and click OK.



Step 3: Add user to Event Log Readers and Distributed COM user

1. Open the Run command in domain controller and type gpedit.msc to open the Group Policy Management Console.
2. Right click on the created GPO → Edit.
3. In the Group Policy Management Editor, click on User Configuration →Preferences → Control Panel Settings → Local Users and Groups.
4. Right click on Local Users and Groups → New → Local Group.
5. Under group name, select Event Log Readers group → Add the current user → Add and select the created user.
6. To add Distributed COM users, repeat step 5 by selecting Distributed COM Users group under group name.

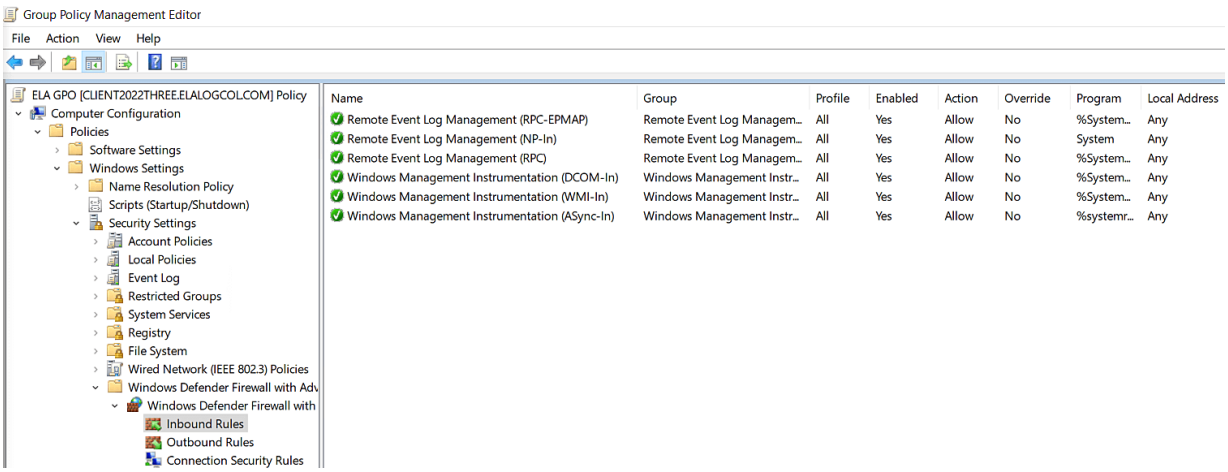




> **Note**
>
> Event Log Readers: Members of this group are allowed to read event logs.
> Distributed COM Users: Members of this group are allowed to launch, activate, and use Distributed COM objects on the computer.

Step 4: Enable WMI and Remote Event Log Management traffic through Firewall

1. Open the Run command and type gpmc.msc to open the Group Policy Management Console.
2. Right click on the GPO created → Edit.
3. Select Computer configuration → Policies → Windows Settings → Security Settings → Windows Firewalls with Advanced Security → Inbound Rules.
4. Right click on Inbound Rules → New Rule and select WMI in predefined field → select all rules → Allow connection.
5. To allow Remote Event Log Management connection, repeat step 4 by selecting Remote Event Log Management in the predefined field.



Note

These rules open ports of the range, 49152 - 65535, that are exclusive for WMI communication and so these cannot be accessed by other applications.

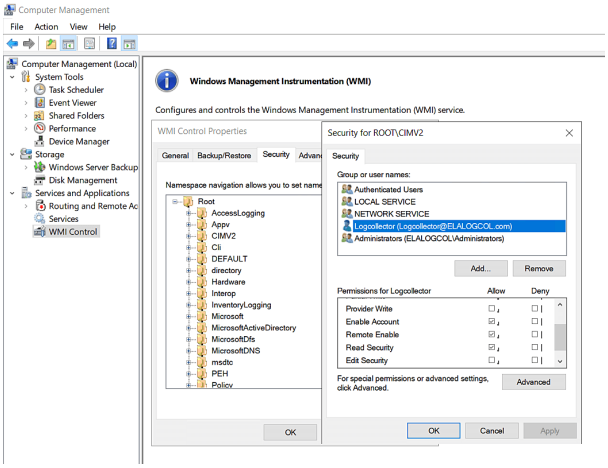
Step 5: Force the group policy

1. Open command prompt and enter → gpupdate /force in the domain controller.
2. Repeat the above step for all domain computers with admin privilege.

Step 6: Grant necessary WMI permissions

a. For Single Computer (Domain/Workgroup)

1. Search Computer Management from Start menu and select Open as Administrator.
2. Select Services and Applications → WMI controller
3. Right click on WMI controller → Properties → Security tab → select Root\cimv2 in the namespace → Security.
4. Add the non-admin user and provide permissions such as Enable account, Remote Enable, Read Security, and Execute Methods.
5. Select Advanced → User name → Add → Applies to: This namespace and subnamespaces and click OK.



Note

Enable Account: Allows users to enable WMI account.
Remote Enable: Allows users to enable remote access to WMI resources.
Read Security: Allows users to read the security setting of WMI resources.
Execute Method: Allows users to execute a method defined within WMI classes.
These permissions are applied to the namespace and subnamespaces.

b. For Multiple Domain Computers (Windows servers and workstations)

Grant WMI Namespace Security Rights using GPO (PowerShell script)

Make sure that the user has the privilege to run the script in the workstation. If not, please refer to the steps below to enable the privilege:

In the Local Group Policy Editor,

- Navigate to Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell.
- Double-click on the Turn on Script Execution option.

Script download link

1. Add the script WMIrights.ps1 file in the shared location in the domain.
2. Right click on the created WMI NameSpace Security Rights GPO → Edit.
3. Select PowerShell Scripts tab → Add.
4. In the Add Script dialog box, click Browse and select the PowerShell script (WMIrights.ps1) file from the shared location and set the parameter as "domainname\username".
5. Click OK to return to the Startup Properties dialog box → Apply → OK.

Configuring Administrative Template Settings

1. On the left pane of the Group Policy Management Editor, navigate to Computer Configuration Administrator Templates System.
2. Under System, select Scripts.
3. On the right pane of the GPO Editor, double-click on Run logon scripts synchronously, and enable it → Apply → OK.
4. Enable Maximum wait time for Group Policy scripts and set the maximum time at 10 seconds.
5. Navigate to Logon under System, on the right pane double-click Always wait for the network at startup and logon, and enable it → Apply → OK
6. Navigate to Group Policy under System, on the right pane double-click Configure Group Policy slow link detection, and enable it → Apply → OK.

Apply the GPO

1. On the left pane of the Group Policy Management Editor, right-click the required GPO → Properties.
2. Navigate to the Security tab and unselect the Apply Group Policy permissions for Authenticated Users → Add.
3. In the dialog box that appears, click Object Types.
4. Enter the names of the required computers and groups and click Check Names.
5. Select the required computers and groups and click OK to return to the properties dialog box.
6. In the Security tab, select "Apply Group Policy" permissions to the selected computers and groups → Apply → OK.
7. Restart the computers and repeat Step 5 to activate the GPOs for granting WMI permissions.

Note:

- After all the required devices are given WMI permissions, remove the script from Computer Configuration

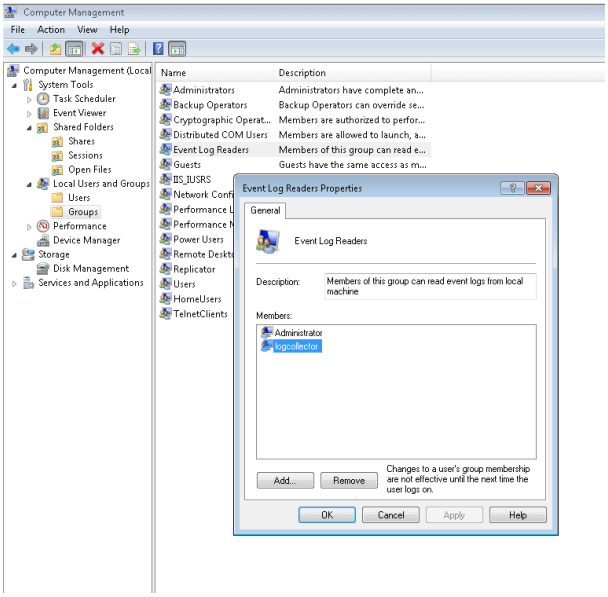
Policies Windows Settings Scripts (Startup/Shutdown) → Startup or the scripts will run every time during startup.

- Not applicable for Multiple workgroup devices.

Workgroup Setup

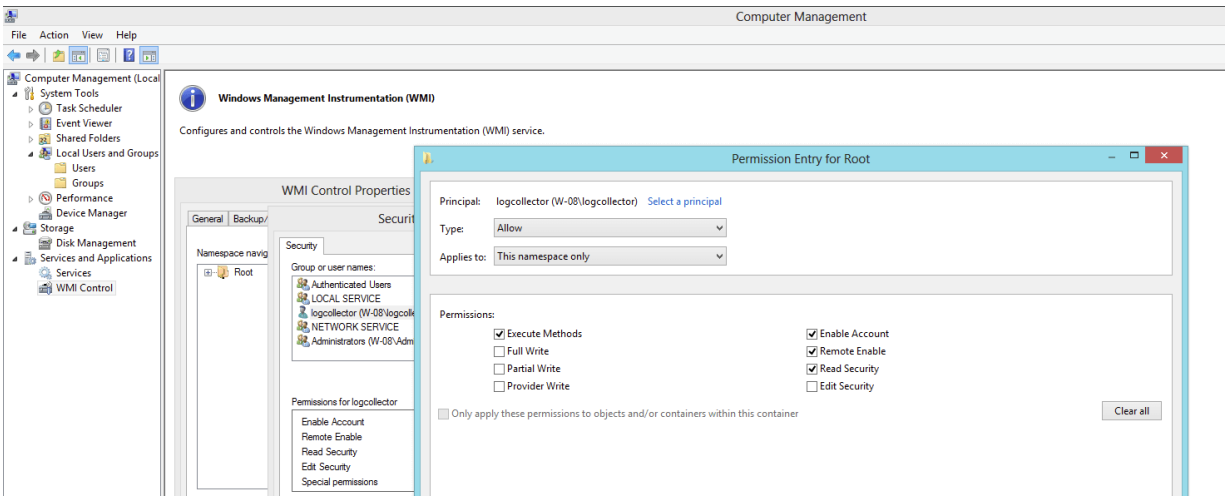
Step 1: Add user to EventLogReader and Distributed COM users

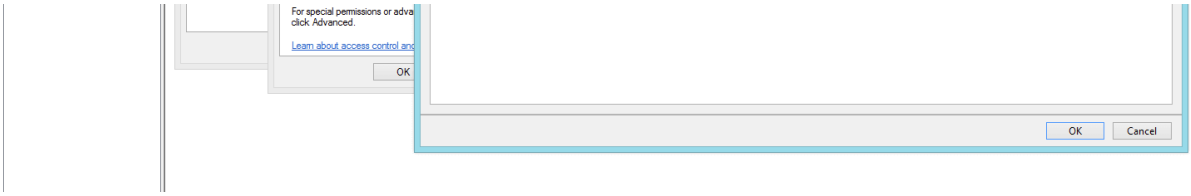
1. Log in to your workgroup with admin privileges and open the Run command and type compmgmt.msc to open Computer Management → Local User and Group.
2. Right click on user and add new user.
3. Right click on Groups → Select distributed COM users → Properties → Add the created user.
4. To add user in Event Log Reader group, repeat step 3 and select Event Log Reader group.



Step 2: Grant necessary WMI permissions:

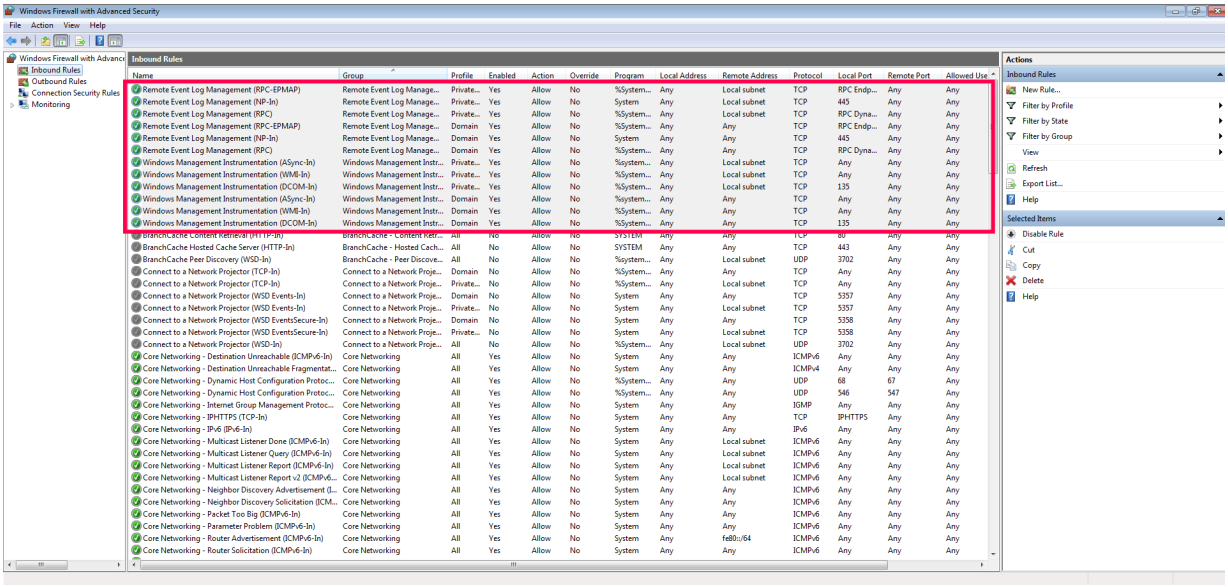
1. Refer Step 6: Grant necessary WMI permissions.





Step 3: Enable WMI and Remote Event Log Management traffic through Firewall

1. Open the Run command and type wf.msc to open Windows Firewall with Advanced Security.
2. Right-click on Inbound Rules → New Rule and select Windows Management Instrumentation in predefined field → select all rules → Allow connection
3. To allow Remote Event Log Management connection, repeat step 2 by selecting Remote Event Log Management in the predefined field.

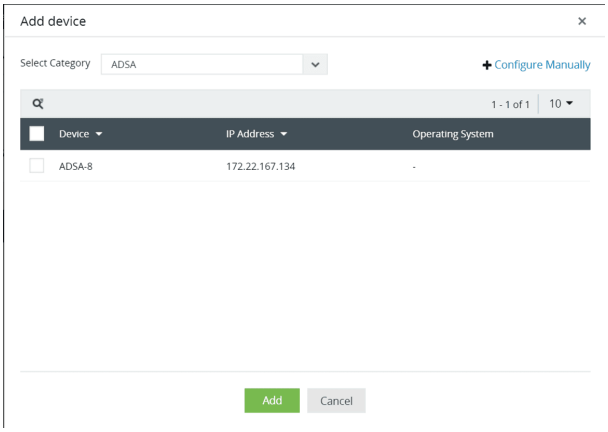


7.1.4. Adding windows device

Last updated on: September 12, 2025

Domain

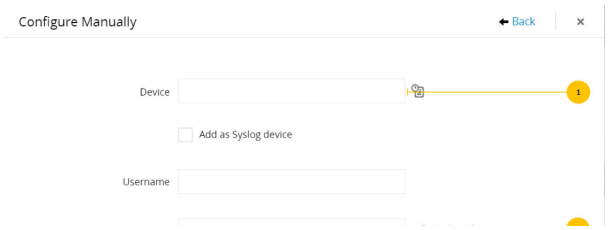
1. Click on +Add Device(s) and select the domain from the select category drop down menu. The Windows devices in the selected domain will be automatically discovered and listed.
2. Select the device(s) by clicking on the respective checkbox(es). You can easily search for a device using the search box or by filtering based on the OU using OU Filter.
3. Click on the Add button to add the device(s) for monitoring.

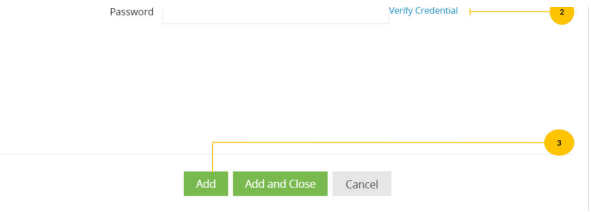


Workgroup

1. Choose the workgroup under the workgroups option in Select Category drop down menu.
2. Select the device(s) by clicking on the respective checkbox(es).
3. Click on the Add button to add the device(s) for monitoring.

> **Note**
>
> You have the option to update, reload and delete a workgroup by clicking on the respective icons next to the Select Domain drop down window. Optionally, you can manually add the device as shown below by clicking on the Configure Manually link.



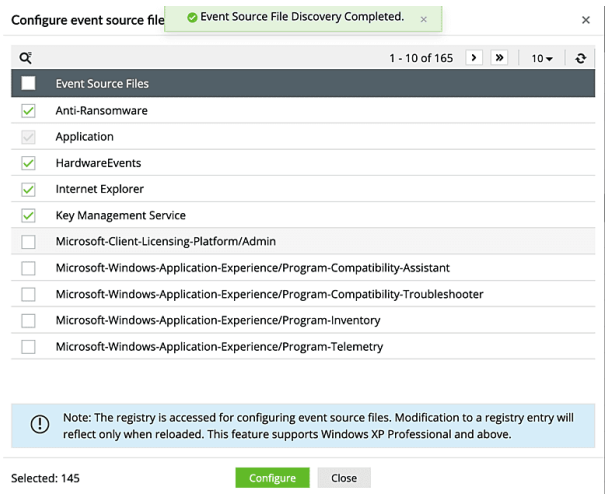


1. Enter the Device name or IP address. You can add the device as a Syslog device by clicking the Add as Syslog device checkbox.
2. Enter the Username and Password with administrator credentials, and click on Verify Credential.
3. Click on the Add button to add the device for monitoring.

How to configure event source files in a device

1. Go to Settings > Configuration > Manage Devices > Windows.
2. Click the Configure Event Source Files icon for the device.
3. In the Event source files dialog box, select the type(s) of event source files.
4. Click Configure.

> **Note**
>
> The registry is accessed for configuring event source files. Modifications to a registry entry will reflect only when reloaded. This feature supports Windows XP Pro and above.



Historic log collection

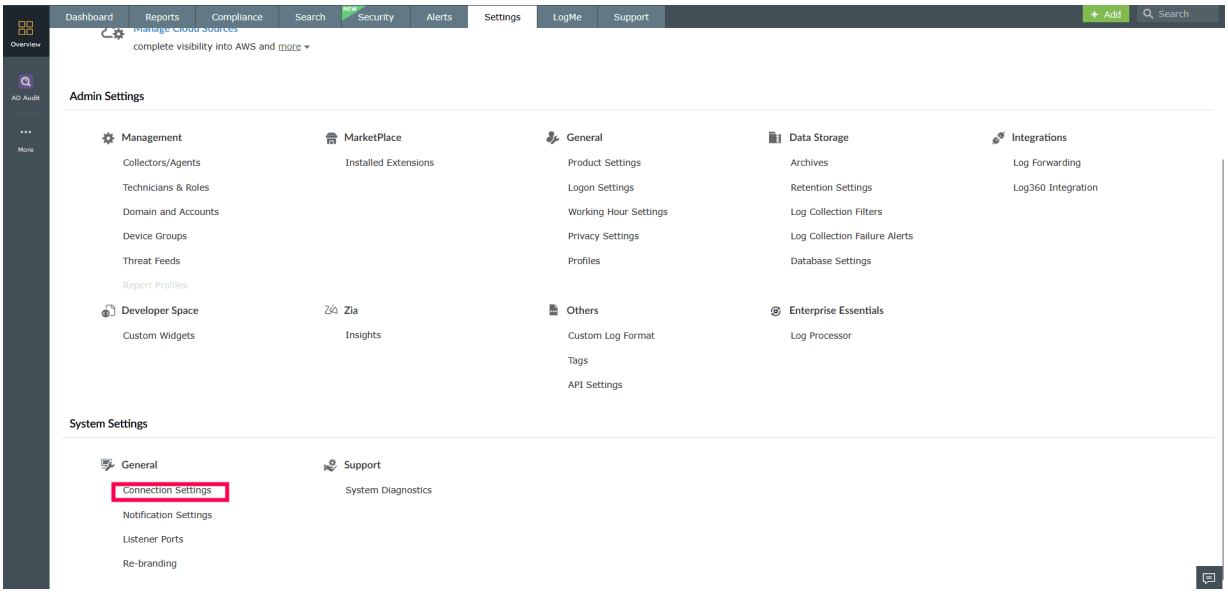
- Navigate to Settings > Configuration > Manage Devices > Add Devices. Select the device, click the icon on the right to enable historic log collection, and click Add.

7.1.5. How to monitor logs from an Amazon Web Services (AWS) Windows instance

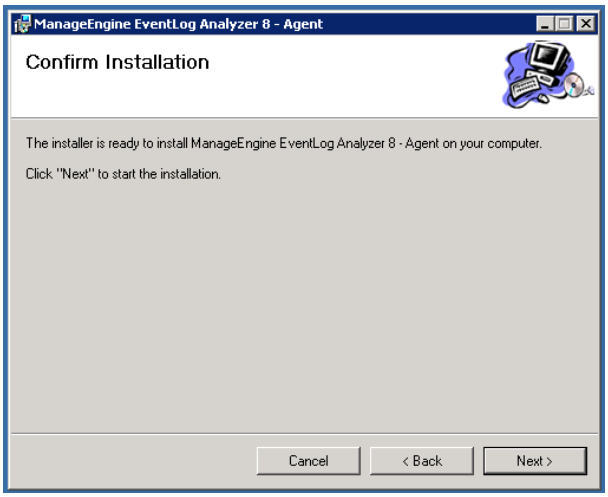
Last updated on: September 12, 2025

Installation procedure

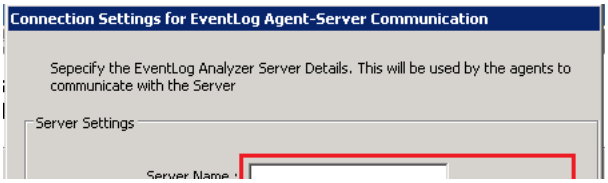
Ensure that EventLog Analyzer server can access EC2 Windows instance.

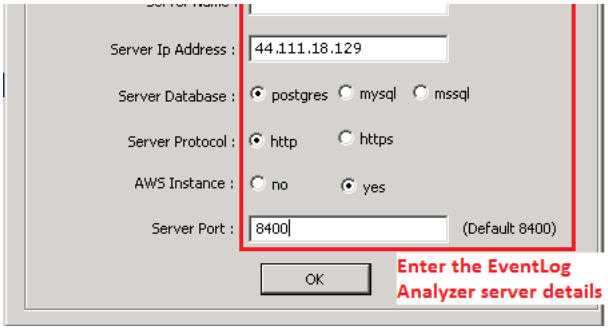


Welcome screen with copyright protection message appears.



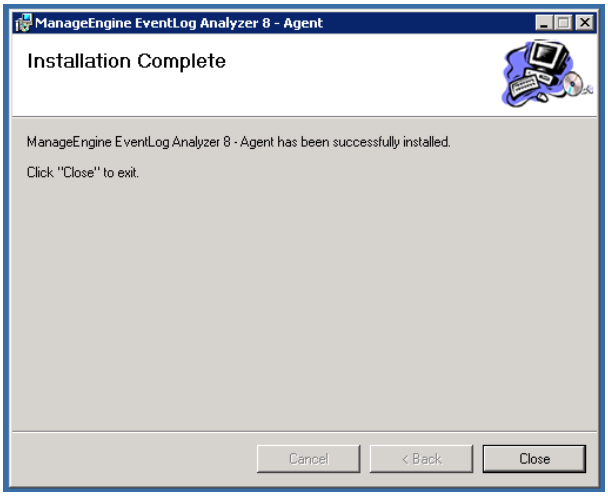
Confirm the agent installation.



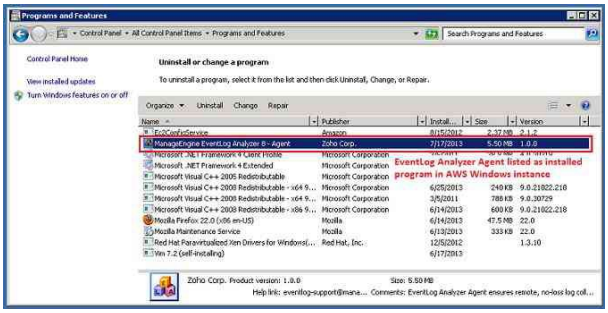


Confirm the agent installation.

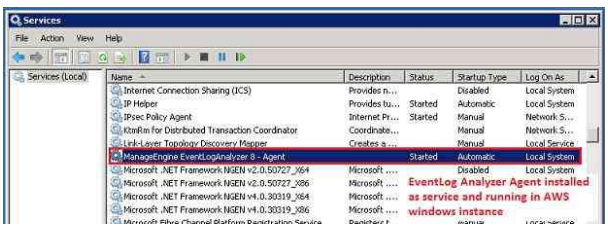
Enter the server details: Server Name or Server IP Address, Server Database, Server Protocol, AWS Instance (choose Yes if agent installation is on AWS, No if it is not), Server Port (mention the HTTP/HTTPS server port, default port is 8095).



Confirm the agent installation.



EventLog Analyzer agent is installed as a service in AWS Windows instance.

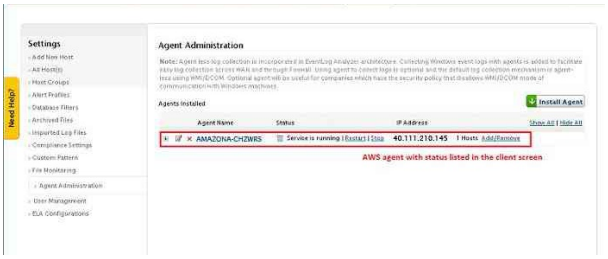




Check whether the service is running.



EC2 server name is resolved from the IP address provided.



EC2 server name is resolved from the IP address provided.

You can check that the AWS instance is displayed in both the Devices tab and the Agent Administration settings page.



EC2 server name is resolved from the IP address provided.

After five minutes you can view the reports rolling out for the AWS instance.

Note

- Install one agent on each AWS Windows server instance.
- You should not associate other AWS server instances with an AWS agent.

7.1.6. Setting up Windows Event Log Reports

Last updated on: September 12, 2025

EventLog Analyzer comes packaged with over 1,000 predefined reports that help organizations view consolidated security events, conduct security audits, and meet various compliance requirements. T
help organizations visualize security events in their network and meet various security and compliance requirements.
In this help document, you will learn to set up Windows report generation.

Setting up Windows report generation

In EventLog Analyzer, most Windows reports get generated automatically when the device is added for monitoring and the event source is configured. To learn how to add a device, check out this page.
to configure an event source, check out the How to configure event source files in a device? section in this page.
There are certain reports, mentioned in the table below, that will require manual creation of keys in your Windows Registry. To set up the generation of these reports, follow the steps given below.

- Please make sure event logging has been enabled by right clicking on the event source > Properties > checking the Enable logging box, in Event Viewer.
- Open the Registry Editor and navigate to HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Service > EventLog. Here, create the keys given in the New keys column of table below.
- Next, open Local Group Policy Editor and navigate to Computer Configuration > Windows Setting > Security Setting. Further paths and steps to enable the generation of reports are given in the Au
column.

Reports	New keys	Audit policies	Other prerequisites
Application Whitelisting Reports	• Microsoft-Windows-AppLocker/EXEandDLL • Microsoft-Windows-AppLocker/MSI and Script	Enable AppLocker under Application Control Policies	• Start the service Application Identity. • On creation of the two new keys, a event source Microsoft-Windows-AppLocker/EXEandDLL will be created panel of Event Viewer. Right click on the event source, click Properties, and copy the Log path. • Then navigate to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channel Windows-AppLocker/EXE and DLL, and create an expandable string value with name File. Use the copied l from the previous step as Value data. • Configure the Executable rules, Windows Installer rules, and Script rules under the mentioned audit policies. • Restart the machine.
Windows Firewall Auditing Reports	• Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Enable Audit MPSSVC Rule - Level Policy change, under Advanced Audit Policy Configuration > Policy Change.	To Enable Windows Firewall logs, execute the below commands in the target device from where the logs are to b
Removable Disk Auditing	• Microsoft-Windows-DriverFrameworks-UserMode/Operational	Enable Audit Handle Manipulation, Audit Removable Storage and Audit File System (required for auditing delete operation in NT Version 6.2), under Advanced Audit Policy Configuration > Object Access.	To start logging removable storage events, navigate to Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Storage and add new DWORD re named as HotPlugSecureOpen and set value as 1.
Registry changes		Enable Audit Registry, under Advanced Audit Policy	Set SACL for the registry key by right-clicking on the required registry and navigating to Permission > Advance > Registry Editor

changes Reports	New keys	Audit Policy Configuration Audit policies Object Access.	Registry Editor. Other prerequisites
Windows Backup & Restore Reports	• Microsoft-Windows-Backup	No modification required.	
Windows System Events	• Microsoft-Windows-GroupPolicy/Operational • Microsoft-Windows-NetworkProfile/Operational • Microsoft-Windows-WindowsUpdateClient/Operational • Microsoft-Windows-Winlogon/Operational • Microsoft-Windows-WLAN-AutoConfig/Operational • Microsoft-Windows-TerminalServices-Gateway/Operational • Microsoft-Windows-TerminalServices-RDPClient/Operational • Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational • Microsoft-Windows-Wired-AutoConfig/Operational	No modification required.	
Hyper-V Server Events Hyper-V VM Management Reports	• Microsoft-Windows-Hyper-V-Worker-Admin • Microsoft-Windows-Hyper-V-VMMS-Storage • Microsoft-Windows-Hyper-V-VMMS-Networking • Microsoft-Windows-Hyper-V-VMMS-Admin • Microsoft-Windows-Hyper-V-Hypervisor-Operational • Microsoft-Windows- Hyper-V-Config • Microsoft-Windows-Hyper-V-High-Availability • Microsoft-Windows-Hyper-V-Hypervisor • Microsoft-Windows-Hyper-V-Integration • Microsoft-Windows- Hyper-V-SynthFC • Microsoft-Windows-Hyper-V-SynthNic • Microsoft-Windows- Hyper-V-SynthStor • Microsoft-Windows- Hyper-V-VID • Microsoft-Windows- Hyper-V-VMMS	No modification required.	
Program Inventory Reports	• Microsoft-Windows-Application-Experience/Program-Inventory	No modification required.	
IIS	• Microsoft-IIS-Configuration/Operational	No modification required.	To access IIS reports, open EventLog Analyzer and navigate to Reports > IIS W3C web server > IIS Admin Con Reports.
Print service	• Microsoft-Windows-PrintService/Operational • Microsoft-Windows-PrintService/Admin	No modification required.	

Reports	New keys • Microsoft-Windows-TerminalServices-Gateway/Operational	Audit policies No modification required.	Other prerequisites
Terminal			

EventLog Analyzer will now start generating the reports mentioned in the table.

7.2.1. Adding Syslog Devices

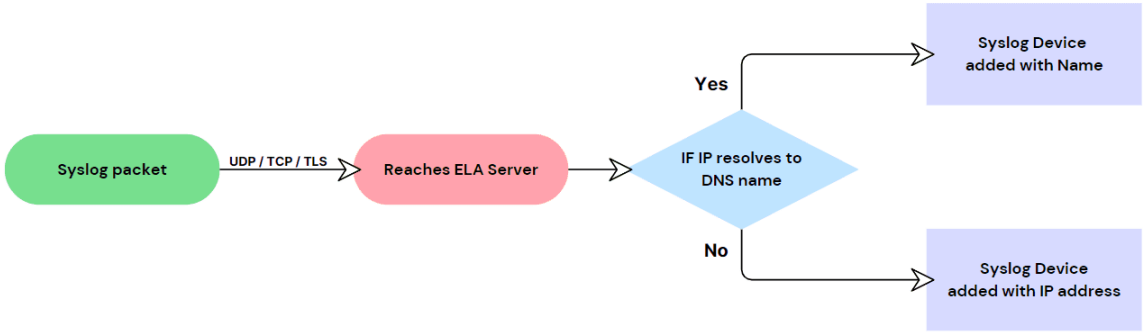
Last updated on: September 12, 2025

Automatic Syslog Device Addition

Prerequisite: Click here to configure the syslog services on your device.
When syslogs are forwarded to the EventLog Analyzer server, syslog devices can be added automatically. This capability is particularly useful for adding multiple syslog devices without requiring manual involvement.

How it works:

When a syslog packet reaches the EventLog Analyzer server, it attempts to determine the source IP address and resolve it to a corresponding name.



- If resolution is successful : The syslog device will be added with a resolved hostname.
- If resolution is unsuccessful : The syslog device will be added using the IP address.

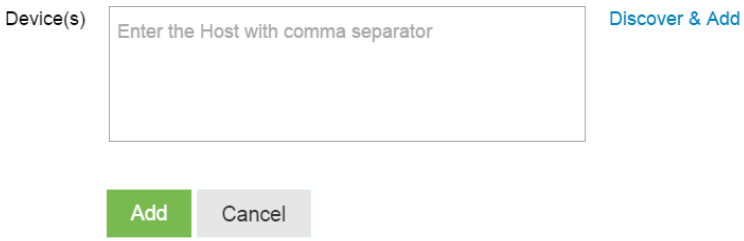
Note

1. Make sure that the default ports : UDP- 513,514 , TCP- 514 are open in inbound rules of the firewall.
2. To configure the TLS ports, click here.
3. If the source IP address or resolved hostname already exists in the database, incoming logs will be associated with that device.

Manual Syslog Device Addition

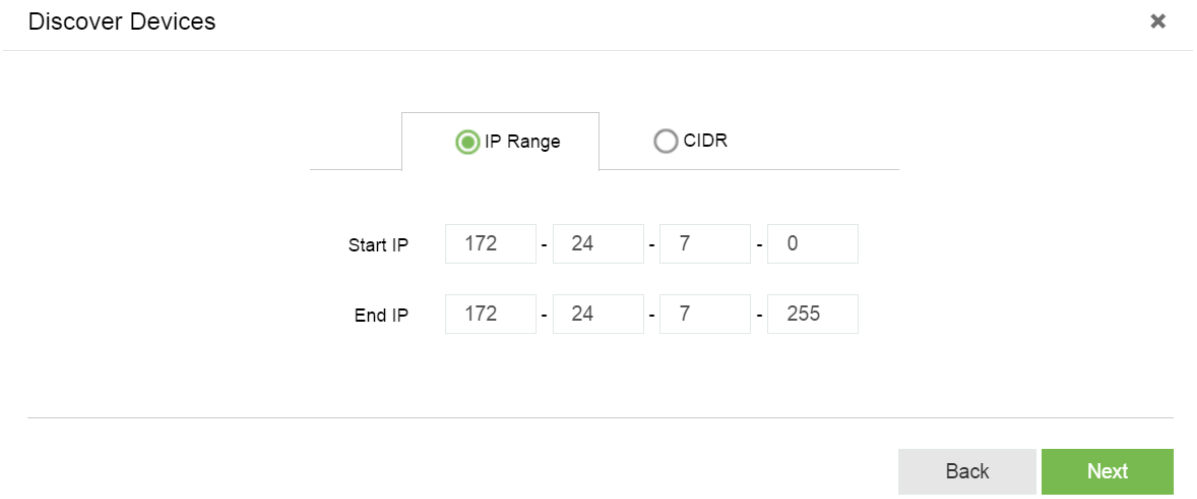
In the Manage Devices page, navigate to the Syslog Devices tab and click on the +Add Device(s) button.

Add Syslog Devices

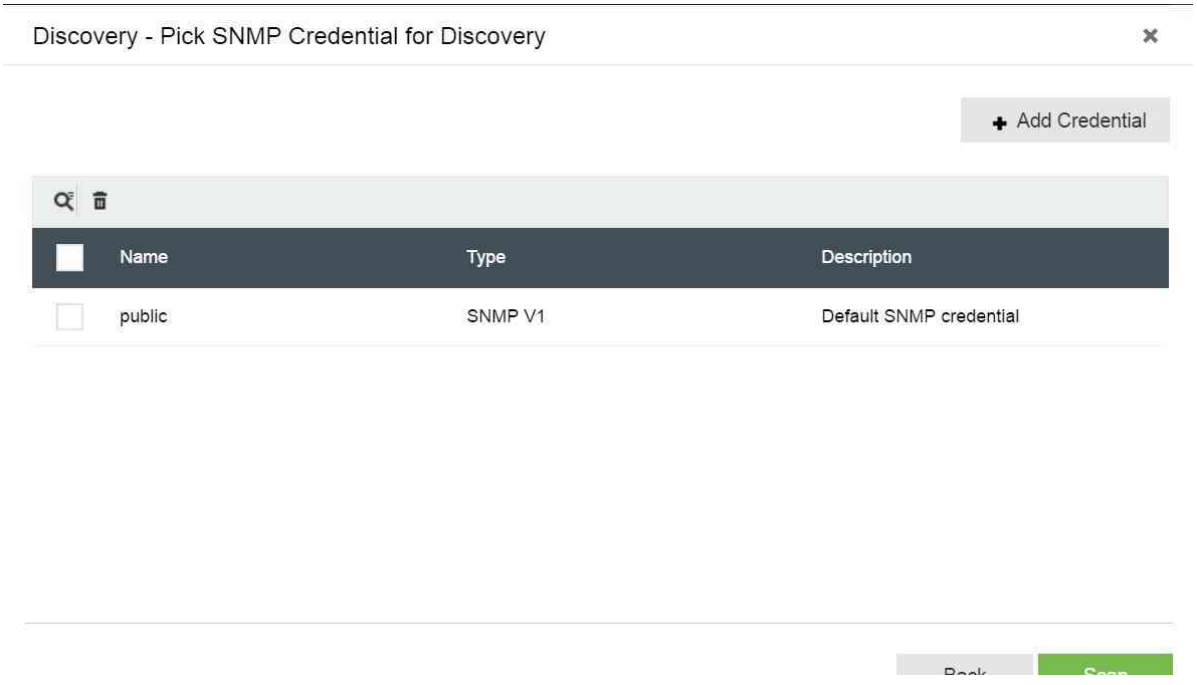


Enter the device name or IP address in the Device(s) field and click on the Add button. Follow the steps below to discover and add the Syslog devices in your network automatically:

1. Click on the Discover & Add link in the Add Syslog Devices window. You can discover the Syslog devices in your network based on the IP range (Start IP to End IP) or CIDR.

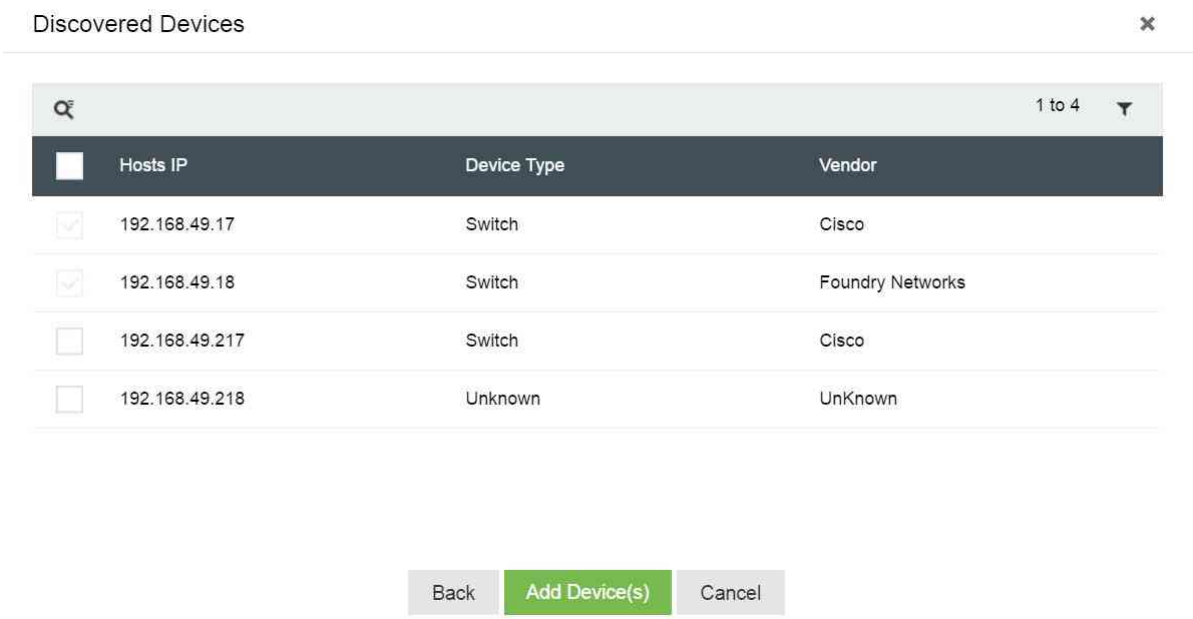


2. Enter the Start IP and End IP or the CIDR range in order to discover the Syslog devices and click on Next.





3. Pick the SNMP credentials to automatically discover the Syslog devices in your network. By default, the public SNMP credentials can be used to scan the Syslog devices in your network.
4. You may also add an SNMP credential by clicking on the +Add Credential button. Once you pick the SNMP credential, click on the Scan button to automatically discover the Syslog devices in the specified IP or CIDR range.
5. Select the device(s) by clicking on the respective checkbox(es). You can easily search for a device using the search box or by filtering based on the Device Type and Vendor.



6. Click on the Add Device(s) button to add the devices for monitoring.

Once a Unix device has been added, you will be prompted to Configure Auto Log Forward.

> Note
>
> Refer here to configure Auto Log forwarding manually for other devices.

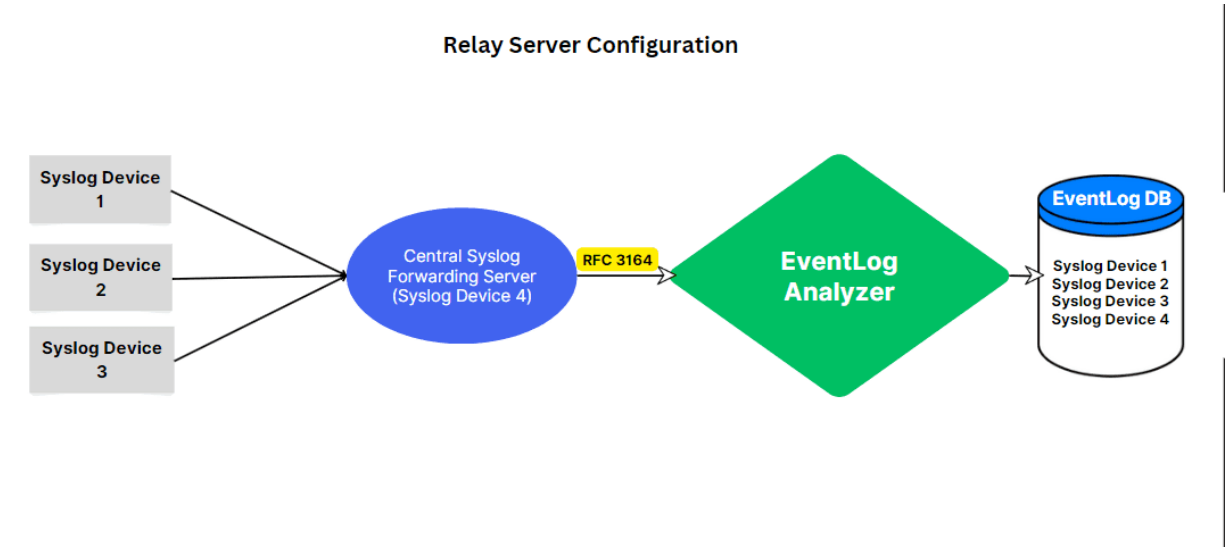
Relay Server Configuration

Usecase: Multiple syslog devices deliver packets to a single central syslog server, which then forwards them to the EventLog Analyzer server.

How it works:

Prerequisite: Forwarded syslogs should adhere to standard RFC 3164 and the corresponding Relay server configuration must be enabled in EventLog Analyzer

configuration must be enabled in EventLog Analyzer.



Sample Log - <34>Oct 18 22:00:15 rootmachine su: 'su root' failed for test on /dev/pts/

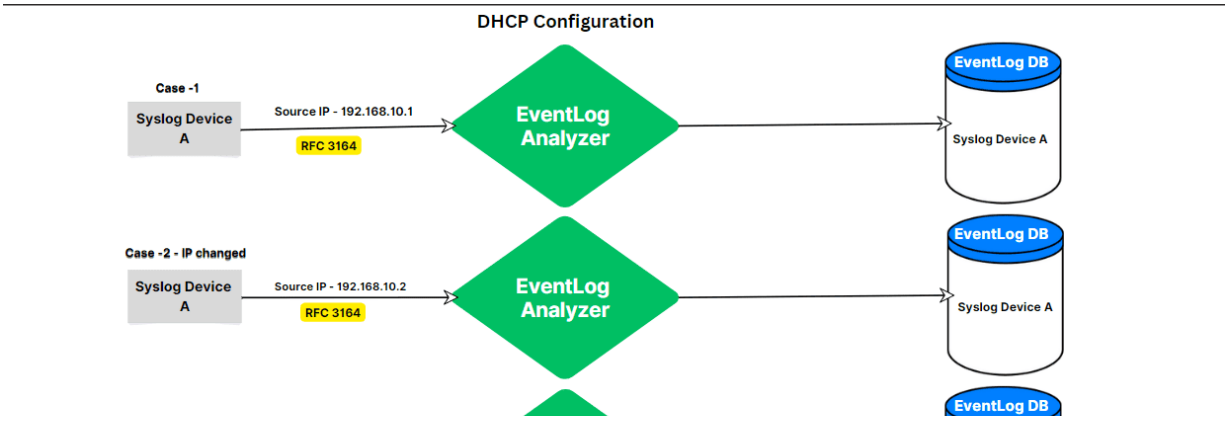
> Note
>
> - The hostname (rootmachine) is parsed from the syslog packet and the syslog device is added with the hostname.
> - If the hostname is already present in the database, then the logs will be mapped to that device.
> - The syslog device can be Unix, Cisco, Fortinet, Palto Alto,etc.

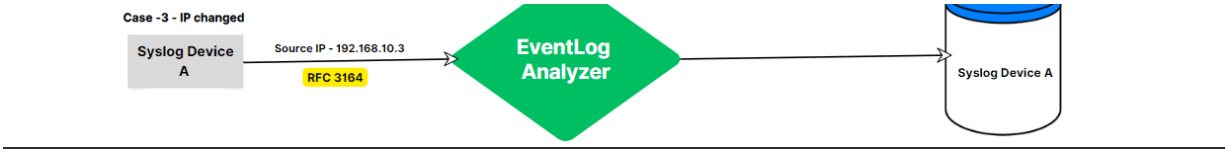
DHCP Configuration

Usecase: When the IP addresses of syslog devices change frequently due to DHCP, a new device is added with a new IP address whenever the IP changes and if the name cannot be resolved.

How it works:

Prerequisite: Forwarded syslogs from all the syslog devices to Eventlog Analyzer should adhere to standard RFC 3164 and the corresponding DHCP configuration must be enabled in EventLog Analyzer.





Sample Log - <34>Oct 18 22:00:15 rootmachine su: 'su root' failed for test on /dev/pts/8

Note

- The hostname(rootmachine) is parsed from the syslog packet and the syslog device is added with the hostname.
- If the hostname is already present in the database, then the logs will be mapped to the respective device.

7.3.1. Adding Unix devices

Last updated on: September 12, 2025

7.3.2. Adding Mac OS devices

Last updated on: September 12, 2025

7.4.1. Adding SQL server

Last updated on: September 12, 2025

7.4.2. Adding MySQL Server

Last updated on: September 12, 2025

7.4.3. Adding Oracle Server

Last updated on: September 12, 2025

7.5.1. Configuring the Syslog Service on FireEye devices

Last updated on: September 12, 2025

1. Login to the FireEye device as an administrator.
2. Navigate to Settings > Notifications, select rsyslog and the Event type.
3. Click Add Rsyslog Server.
4. In the dialog box that opens, enter the EventLog Analyzer server IP address in the given field. Choose UDP as the protocol and the format as CEF (default).
5. Click Save.

7.5.2. Configuring the Syslog Service on Malwarebytes devices

Last updated on: September 12, 2025

To configure the Syslog service in your Malwarebytes devices, follow the steps below:

1. Log into the Management console of the Malwarebytes device.
2. Move to the Admin pane and open the Syslog Settings tab.
3. Click Change and tick the Enable Syslog check box.
4. To export traffic monitoring logs to EventLog Analyzer server, enter the following details in the space provided:
   - Address <EventLog Analyzer server IP address>
   - Port <513/514>
   - Protocol
   - Payload format <CEF>
5. Click OK to save.

> **Note**
>
> At the moment, only the Malwarebytes Management Console (MBMC) is supported.

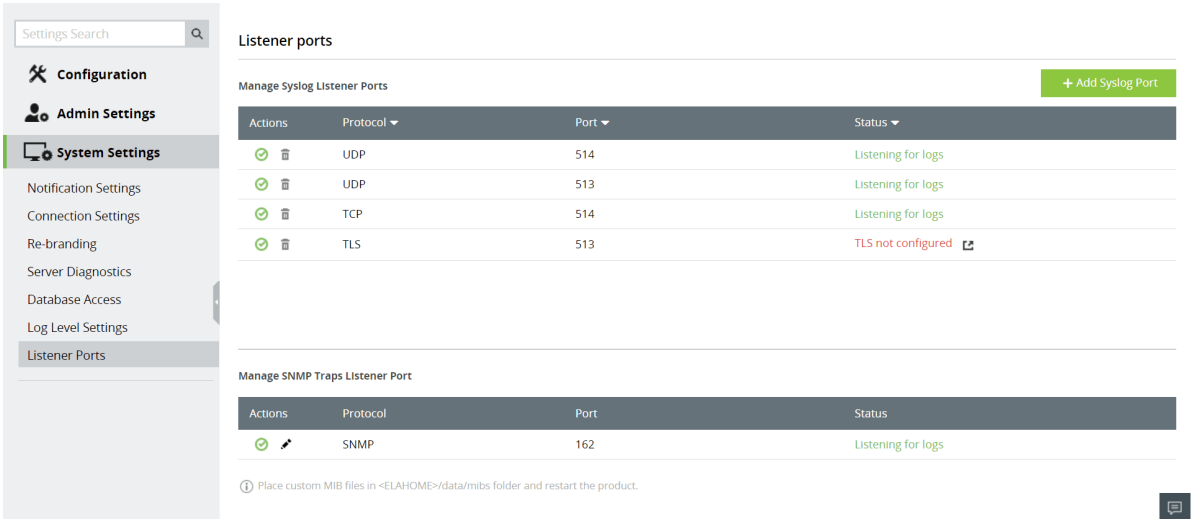
7.5.3. Configuring McAfee Solutions

Last updated on: September 12, 2025

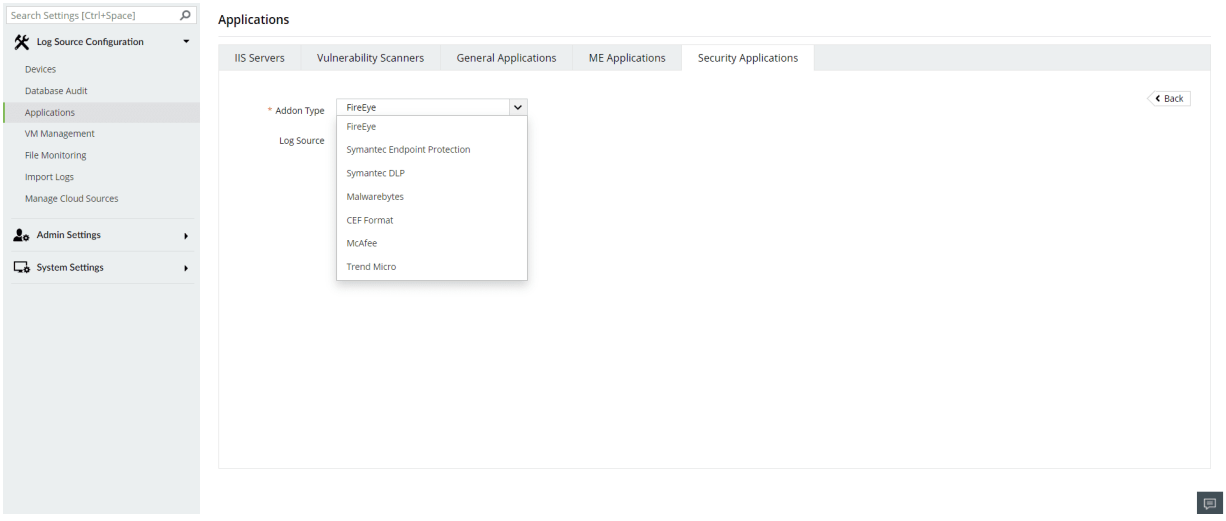
EventLog Analyzer collects log data from McAfee solution and presents it in the form of graphical reports. For the solution to start collecting this log data, it has to be added as a threat source.

To configure McAfee in EventLog Analyzer, please follow the steps below.

1. Configure HTTPS in EventLog Analyzer.
2. Enable the required TLS port. Settings > System Settings > Listener ports

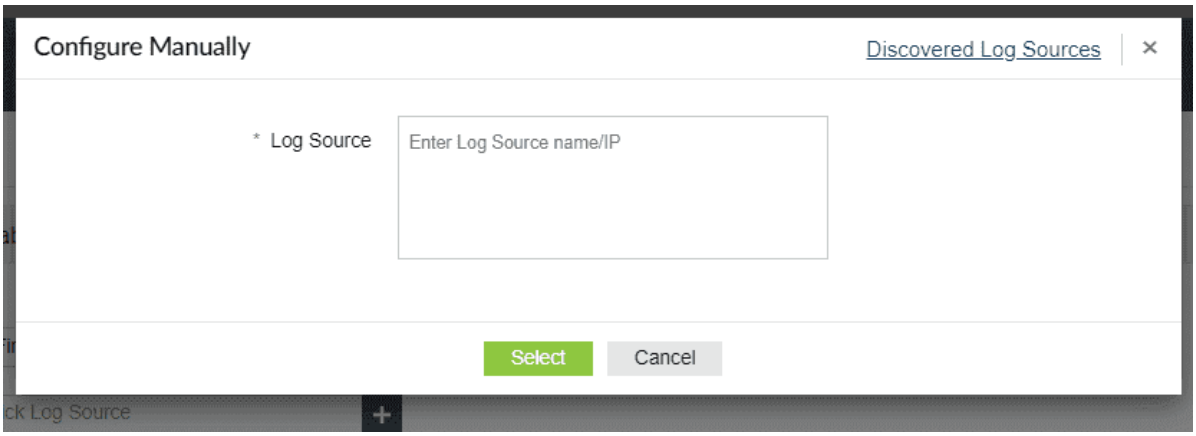


3. Configure your McAfee ePO server to use the newly created syslog server.
4. Add a new registered server and select Syslog for the type of server.
5. Enter the FQDN of the Syslog server.
6. Enter 6514 for the port number. If the listener port number was changed in the TLS, enter that port number.
7. Click on enable event forwarding.
8. Click on test connection. A Syslog connection success message will be displayed.
9. Click on save.



Once the threat source is added, EventLog Analyzer will start parsing the fields in the logs. This log data can now be viewed in the form of reports.

1. In the EventLog Analyzer console, navigate to Settings > Log Source Configurations > Applications > Security Applications > Add Security Applications
2. Select Add-on type as McAfee
3. Expand the list by clicking the "+" icon to add a new device.
4. Choose from the drop-down menu to add Configured devices, Workgroup devices, domain devices, etc.
5. To add new devices manually, click on Configure Manually and enter Log Source >Select and click on Add.



Available reports:

- McAfee Events
- McAfee Threat Reports
- McAfee Virus Reports

7.5.4. Configuring the Syslog Service on Symantec DLP devices

Last updated on: September 12, 2025

1. Locate and open the config\Manager.properties file. The file path is as follows
2. Windows - \SymantecDLP\Protect\config directory
3. Linux - /opt/SymantecDLP/Protect/config directory
4. Uncomment the systemevent.syslog.host= line and specify the EventLog Analyzer server IP address as follows:
   systemevent.syslog.host=xxx.xx.xx.xxx
5. Uncomment the systemevent.syslog.port= line and specify 514 as the port to accept connections from the Symantec Enforce Server as follows:
   systemevent.syslog.port=514
6. After making the above mentioned changes, save and close the properties file.

7.5.5. Configuring the Syslog Service on Symantec Endpoint Protection devices

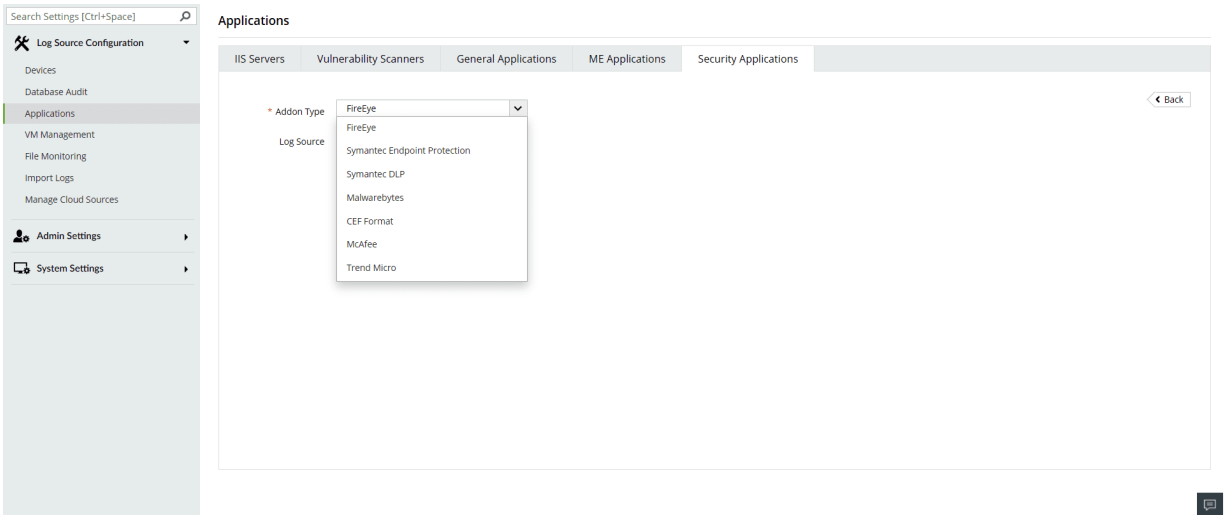
Last updated on: September 12, 2025

1. Login to the Symantec Endpoint Protection device as an administrator.
2. Navigate to Admin > Servers. Select the local site or remote site from which log data must be exported.
3. Click Configure External Logging.
4. In the General tab, from the Update Frequency list, choose how often log data should be sent to the file.
5. In the Master Logging Server list, select the management server to which the logs should be sent.
6. Check the Enable Transmission of Logs to a Syslog Server option.
7. Enter the following details in the given fields.
   - Syslog Server- Enter the EventLog Analyzer IP address or domain name .
   - Destination Port - Select the protocol to use and enter the destination port that the Syslog server should use to listen for Syslog messages.
   - Log Facility - Enter the number of the log facility that you want the Syslog configuration file to use. Valid values range from 0 to 23. Alternatively, you could use the default.
8. Click OK.

7.5.6. Configuration steps for Syslog forwarding from Trend Micro - Deep Security devices to EventLog Analyzer

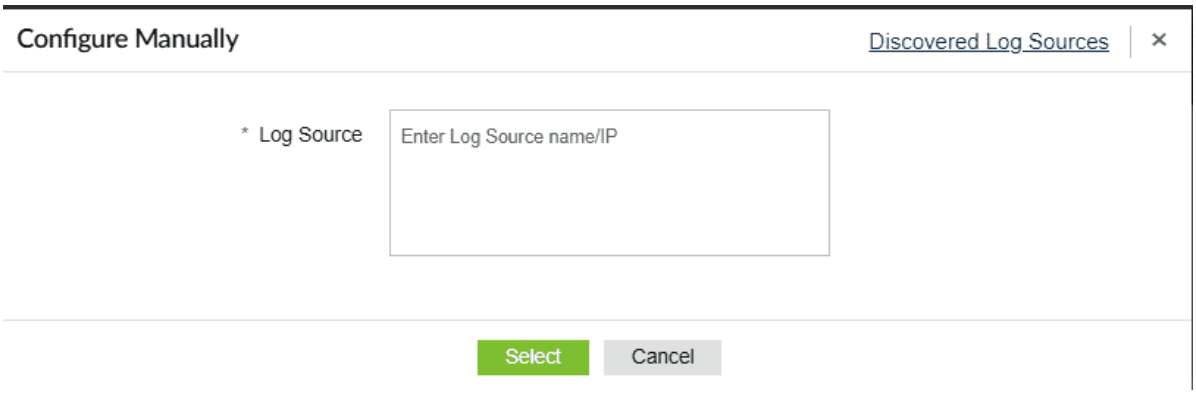
Last updated on: September 12, 2025

1. To forward system events to ELA server:
   - Go to Administration → System Settings → Event Forwarding.
   - Select Forward System Events to a remote computer (via Syslog) in the SIEM section.
   - Specify the following information and then click Save:
     - Hostname <EventLog Analyzer IP>
     - UDP port <default 514>
     - Syslog Format <CEF>
     - Syslog Facility
2. To forward security events to ELA server:
   - Go to Policies.
   - Double-click the policy you want to use for computers to forward security events via the Deep Security Manager.
   - Go to Settings > SIEM and select Forward Events To > Relay via the Manager for each applicable protection module.
   - Specify the following information that is required for relaying events via the Deep Security Manager and then click Save:
     - Hostname <EventLog Analyzer IP>
     - UDP port <default 514>
     - Syslog Format <CEF>
     - Syslog Facility



Once the threat source is added, EventLog Analyzer will start parsing the fields in the logs. This log data can now be viewed in the form of reports.

1. In the EventLog Analyzer console, navigate to Settings > Log Source Configurations > Applications > Security Applications > Add Security Applications
2. Select Add-on type as Trend Micro
3. Expand the list by clicking the "+" icon to add a new device.
4. Choose from the drop-down menu to add Configured devices, Workgroup devices, domain devices, etc.
5. To add new devices manually, click on Configure Manually and enter Log Source >Select and click on Add.



7.6.1. Configuring the Syslog Service on a HP-UX/Solaris/AIX Device

Last updated on: September 12, 2025

1. Login as root user.
2. Edit the syslog.conf file in the /etc directory as shown below.
   .emerg;.alert;*.crit;*.err;*.warning;*.notice;*.info;*.debug<tab-separation>@<ela_server_name>
   where <ela_server_name> is the name of the machine where EventLog Analyzer is running. Ensure that there is only a tab separation in between *.debug and @<ela_server_name>.

   > Note
   >
   > For a Solaris device, it is enough to include *.debug<tab-separation>@<ela_server_name> in the syslog.conf file.;

3. Save the configuration and exit the editor.
4. Edit the services file in the /etc directory.
5. Change the syslog service port number to 514, which is one of the default listener of EventLog Analyzer. But if you choose a different port other than 514 then remember to enter that same port when adding the device in EventLog Analyzer.
6. Start the syslog daemon on the OS with the appropriate command:

   (for HP-UX) /sbin/init.d/syslogd start
   (for Solaris) /etc/init.d/syslog start
   (for Solaris 10) svcadm -v restart svc:/system/system-log:default
   (for IBM AIX) startsrc -s syslogd

7.6.2. Adding Arista Switches

Last updated on: September 12, 2025

7.6.3. Configuring the Syslog Service on Cisco Switches

Last updated on: September 12, 2025

1. Login to the switch.
2. Go to the config mode.
3. Configure the switch as below (here, we have used Catalyst 2900) to send the logs to the EventLog Analyzer server:
   <Catalyst2900># config terminal
   <Catalyst2900>(config)# logging <ela_server_IP>
   For the latest catalyst switches
   Catalyst6500(config)# set logging <ela_server_IP>
   We can also configure logging facility and trap notifications with the below commands:

> **Note**
>
> The same commands are also applicable for Cisco Routers.
>
> Please refer Cisco® documentation for detailed steps on configuring the Syslog service in the respective routers or switches. Contact eventlog-support@manageengine.com if the Syslog format of your Cisco devices are different from the standard syslog format supported by EventLog Analyzer.

7.6.4. Configuring the Syslog Service on Cisco Firepower devices

Last updated on: September 12, 2025

Step 1: Syslog server configuration

To configure a Syslog Server for traffic events, navigate to Configuration > ASA Firepower Configuration > Policies > Actions Alerts and click the Create Alert drop-down menu and choose option Create Syslog Alert. For web interfaces, navigate to Policies > Actions Alerts. Enter the values for the Syslog server.

- Name: Specify the name which uniquely identifies the Syslog server.
- Host: Specify the IP address/hostname of Syslog server.
- Port: Specify the port number of Syslog server.
- Facility: Select any facility that is configured on your Syslog server.
- Severity: Select any Severity that is configured on your Syslog server.
- Tag: Specify tag name that you want to appear with the Syslog message.

Step 2: Enable external logging for Connection Events

- Connection Events are generated when traffic hits an access rule with logging enabled. In order to enable the external logging for connection events, navigate to ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy. For web interfaces, navigate to Policies > Access Control Policy. Edit the access rule and navigate to logging option.
- Select the logging option either log at Beginning and End of Connection or log at End of Connection. Navigate to Send Connection Events to option and specify where to send events.
- In order to send events to an external Syslog server, select Syslog, and then select a Syslog alert response from the drop-down list. Optionally, you can add a Syslog alert response by clicking the add icon.

Step 3: Enable external logging for Intrusion Events

- Intrusion events are generated when a signature (snort rules) matches some malicious traffic. In order to enable the external logging for intrusion events, navigate to ASDM Configuration > ASA Firepower Configuration > Policies > Intrusion Policy > Intrusion Policy. For web interfaces, navigate to Policies > Intrusion Policy > Intrusion Policy. Either create a new Intrusion policy or edit an existing one. Navigate to Advanced Setting > External Responses.
- In order to send intrusion events to an external Syslog server, select option Enabled in Syslog Alerting then click the Edit option.
  Logging Host: Specify the IP address/hostname of Syslog server.
  Facility: Select any facility that is configured on your Syslog server.
  Severity: Select any Severity that is configured on your Syslog server.

> Note
>
> - From Version 6.3 and above, make sure to enable timestamping in the RFC 5242 format in Firepower Threat Defense for collecting syslogs along with their timestamps.

- To forward audit logs from Cisco Secure Firewall Management Center (formerly Firepower Management Center) to EventLog Analyzer, please follow the steps here.

7.6.5. Configuring the Syslog Service on SonicWall devices

Last updated on: September 12, 2025

To configure the Syslog service on SonicWall devices, follow the steps below:

1. Login to the SonicWall device as an administrator.
2. Navigate to Log > Automation, and scroll down to Syslog Servers.
3. Click on the Add button.

Use a web browser to connect to the SonicWall management interface and login with your username and password.

1. Click on the Log button on the left menu. This will open a tabbed window in the main display.
2. Click on the Log Settings tab.
3. Under Sending the Log, enter the IP address of the machine running the Kiwi Syslog Server into the field Syslog Server 1. If you are listening on a port other than 514, enter that value in the field Syslog server port 1.
4. The Syslog ID must be firewall for the effective parsing of firewall logs.
5. Under Automation, set the Syslog format to Enhanced Syslog.
6. Under Categories > Log, check all the types of events that you would like to receive Syslog messages for.
7. Click on the Update button.

For SonicOS 6.5 and above:

1. Login to the SonicWall device as an administrator.
2. Click on Manage tab and expand Log Settings> SYSLOG
3. Click Add under Syslog Servers.
4. From the Add Syslog Server window, enter the IP address or host name of the Eventlog Analyzer server.
5. Enter the port number and set the Server Type to Syslog.
6. Set the Syslog format to Enhanced Syslog.
7. The Syslog ID must be firewall for the effective parsing of firewall logs.
8. Click OK to configure.

A reboot of the SonicWall may be required for the new settings to take effect.

7.6.6. Configuring the Syslog Service on Juniper devices

Last updated on: September 12, 2025

To configure the Syslog service on SonicWall devices, follow the steps below:

1. Login to the Juniper device as an administrator.
2. Navigate to the Configure tab.
3. Expand CLI Tools on the left pane, click on CLI editor in the subtree, and navigate to syslog under system.
4. For standard logs, insert the host node with the required values such as the host name, severity, facility and log prefix. Consider the following command:
   host ela-server{
   any any;
   port 513;
   }
   This will forward the log data in standard format. You can customize the syslog severity level by editing the command.
5. For structured logs, mention 'structured-data' in the command line. Consider the following command.
   host ela-server{
   any any;
   port 513;
   structured-data;
   }
   This will forward the log data in a structured format.
6. Click on Commit to save the changes. To view the changes, click on the CLI viewer.

> **Note**
>
> It is recommended to use structured logs

7.6.7. Configuring the Syslog Service on PaloAlto devices

Last updated on: September 12, 2025

To configure the Syslog service in your Palo Alto devices, follow the steps below:

1. Login to the Palo Alto device as an administrator.
2. Navigate to Device > Server Profiles > Syslog to configure a Syslog server profile.
3. Configure Syslog forwarding for Traffic, Threat, and WildFire Submission logs. First, navigate to Objects > Log Forwarding, and click on Add to create a log forwarding profile.
4. Assign the log forwarding profile to security rules.
5. Configure Syslog forwarding for System, Config, HIP match, and Correlation logs.
6. Click on Commit for the changes to take effect.

For version 7.1 and above:

1. Login to the Palo Alto device as an administrator.
2. Configure a Syslog server profile for the EventLog Analyzer server
    - Select Device > Server Profiles > Syslog.
    - Click Add and provide a name for the profile.
    - If the firewall has more than one virtual system (vsys), select the Location (vsys or Shared) where this profile is available.
    - For the EventLog Analyzer server, click Add and enter the requested information.
    - Click OK.
3. Configure syslog forwarding for Traffic, Threat, and WildFire Submission logs.
    - Create a log forwarding profile.
        - Select Objects > Log Forwarding, click Add, and enter a Name to identify the profile.
        - For each log type and each severity level or WildFire verdict, select EventLog Analyzer's Syslog server profile and click OK.
    - Assign the log forwarding profile to security rules.
4. Configure syslog forwarding for System, Config, HIP Match, and Correlation logs.
    - Select Device > Log Settings.
    - For System and Correlation logs, click each Severity level, select EventLog Analyzer's syslog server profile, and click OK.
    - For Config, HIP Match, and Correlation logs, edit the section, select EventLog Analyzer's syslog server profile, and click OK.
5. Click Commit to save your changes.

Source: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/monitoring/configure-syslog-monitoring

Note

It's recommended to use BSD format in syslog profiles.

Once you have completed the configuration steps, the logs from your Palo Alto device will be automatically forwarded to the EventLog Analyzer server.

Note

Under "Syslog Server Profile" -> "Custom Logformat" all "Log Type" must be "default"

7.6.8. Configuring the Syslog Service on Cisco devices

Last updated on: September 12, 2025

1. Login to the Firewall.
2. Go to the config mode;
3. Configure the switch as given below (here, we have used Catalyst 2900) to send the logs to the EventLog Analyzer server:
   Cisco-ASA# config terminal
   Cisco-ASA (config)# logging host <EventLog _server_IP> [TCP/UDP]/< Port_Number >

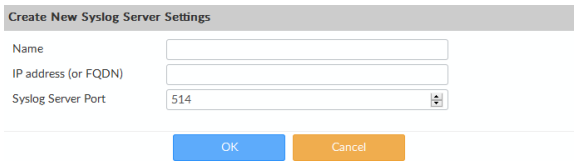
Cisco-ASA (config)# logging trap information
Cisco-ASA (config)# logging facility local7

7.6.9. Configuring the Syslog Service on Fortinet devices

Last updated on: September 12, 2025

To configure the Syslog service in your Fortinet devices follow the steps given below:

1. Login to the Fortinet device as an administrator.
2. Define the Syslog Servers. It can be defined in two different ways,
   - Either through the GUI System Settings > Advanced > Syslog Server



     Configure the following settings and then select OK to create the syslog server.

Name	Enter a name for the syslog server.
IP address (or FQDN)	Enter the IP address or FQDN of the EventLog Analyzer.
Syslog Server Port	Enter the EventLog Analyzer's port number. The default port is 514.

   - Or with CLI commands:
3. Use the following CLI commands to send Fortinet logs to the Eventlog Analyzer server.
4. Severity and Facility can be changed as per the requirements.

Once you have completed the configuration steps, the logs from your Fortinet device will be automatically forwarded to the EventLog Analyzer server.
For more details refer the source: Link.

7.6.10. Configuring the Syslog Service on Check Point devices

Last updated on: September 12, 2025

To configure the Syslog service in your Check Point devices, follow the steps below:

1. Login to the Check Point device as an administrator.
2. To override the lock, click on the lock icon on the top-left corner of the screen.
3. Click Yes on the confirmation pop-up that appears.
4. Navigate to System Management > System Logging.
5. Under the Remote System Logging section, click Add.
6. In the Add Remote Server Logging Entry window, enter the IP address of the remote server (EventLog Analyzer server).
7. From the Priority drop-down, select the severity level of the logs to be sent to the remote server.
8. Click OK.

7.6.11. Configuring the Syslog Service on NetScreen devices

Last updated on: September 12, 2025

The Syslog service in your NetScreen devices, can be configured in two ways:

Enabling Syslog Messages using the NetScreen Device:

1. Login to the NetScreen GUI.
2. Navigate to Configuration> Report Settings> Syslog.
3. Check the Enable Syslog Messages check-box.
4. Select the Trust Interface as Source IP and enable the Include Traffic Log option.
5. Enter the IP address of the Eventlog Analyzer server and Syslog port (514) in the given boxes. All other fields will have default values.
6. Click Apply to save the changes.

Enabling Syslog Messages the CLI Console:

7.6.12. Configuring the Syslog Service on WatchGuard devices

Last updated on: September 12, 2025

To configure the Syslog service in your WatchGuard devices, follow the steps below:

1. Login to the WatchGuard device as an administrator.
2. Navigate to System> Logging> Syslog.
3. Enable the Send log messages to the syslog server at this IP address checkbox.
4. Type the EventLog Analyzer server's IP address in the box provided for IP address.
5. Select 514 in the box provided for Port.
6. Select Syslog from the Log Format drop-down list.
7. If you want to include date and time in the log message details, enable the Time stamp checkbox.
8. If you want to add serial numbers in log message details, enable Serial number of the device checkbox.
9. Select a syslog facility for each type of log message in the Syslog settings section drop-down list.
   - For high-priority syslog messages, such as alarms, select Local0.
   - To assign priorities for other types of log messages select Local1 - Local7.
   - To not send details for a message type, select NONE.

     Note: Lower numbers have greater priority.
10. Click SAVE

7.6.13. Configuring the Syslog Service on Sophos devices

Last updated on: September 12, 2025

To configure the Syslog service in your Sophos devices, follow the steps below:

Enabling Sophos-UTM Syslog:

1. Login to Sophos UTM as administrator.
2. Navigate to Logging & Reporting > Log Settings >Remote Syslog Server
3. Enable Syslog Server Status
4. Configure the syslog server by filling the following details
   Name: < Any >
   Server: < EventLog Analyzer server IP Address >
   Port: < 513 >
5. Navigate to Remote Syslog > select the logs that has to be sent to the EventLog Analyzer server.
6. Click on Apply

Enabling Sophos-XG Syslog:

1. Login to Sophos-XG as administrator.
2. Navigate to System > System Services > Log Settings > Syslog Servers > Add
3. Configure the syslog server by filling the following details
   Name: < Any >
   Server: < EventLog Analyzer server IP Address >
   Port: < 513 >
   Facility: < DAEMON >
   Severity: < INFORMATION >
   Format: < Standard Format >
4. Click on Save
5. Navigate to System > System Services > Log Settings> select the logs that has to be sent to the EventLog Analyzer Server.

7.6.14. Configuring the Syslog Service on Barracuda devices

Last updated on: September 12, 2025

The Syslog service in your Bararacuda devices, can be configured by following these five steps:

1. Enable the Syslog Service
   - Navigate to CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming.
   - Click on Lock.
   - Enable the Syslog service.
   - Click Send Changes and Activate.
2. Configure Logdata Filters
   - Navigate to CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming.
   - From the menu select Logdata Filters.
   - Click on Configuration Mode > Switch to Advanced View > Lock
   - Click on + icon to add a new entry.
   - Enter a descriptive name in the Filters and click OK.
   - In the Data Selection table, add the log files to be streamed. (e.g. Fatal_log, Firewall_Audit_Log, Panic_log)
   - In the Affected Box Logdata section, define what kind of box logs are to be affected by the Syslog daemon from the Data Selection list.
   - In the Affected Service Logdata section, define what kind of logs created by services are to be affected by the Syslog daemon from the Data Selection list.
   - Click on Send Changes and Activate.
3. Configure Logstream Destinations
   - Navigate to CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming.
   - From the menu select Logstream Destinations.
   - Expand the Configuration Mode > Switch to Advanced View > Lock.
   - Click on + icon to add a new entry.
   - Enter a descriptive name and click OK.
   - In the Destinations window select the Remote Loghost.
   - Enter the EventLog Analyzer server IP address as destination IP address in the Loghost IP address field.
   - Enter the destination port for delivering syslog message as 513, 514.
   - Enter the destination protocol as UDP.
   - Click OK
   - Click on Send Changes and Activate.

4. Disable Log Data Tagging
5. Configure Logdata Streams
    - Navigate to CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming.
    - From the menu, select Logdata Streams.
    - Expand the Configuration Mode menu and select Switch to Advanced View.
    - Click the + icon to add a new entry.
    - Enter a descriptive name and click OK.
    - Configure Active Stream, Log Destinations and Log Filters settings.
    - Click on Send Changes and Activate.

7.6.15. Configuring the Syslog Service on Huawei Firewall devices

Last updated on: September 12, 2025

To configure the Syslog service in your Huawei firewall devices, follow the steps below:

1. Login to the Huawei firewall device.
2. Navigate to System view > Log monitoring > Firewall log stream
3. To export traffic monitoring logs to EventLog Analyzer server, enter the following details in the space provided:
   Info-center loghost <EventLog Analyzer server IP address> 514 facility <facility>
4. Exit the configuration mode.

7.6.16. Configuring the Syslog Service on Meraki devices

Last updated on: September 12, 2025

To configure the Syslog service in your Meraki devices, follow the steps below:

1. Login to the Meraki device as an administrator.
2. From the dashboard, navigate to Network-wide > Configure > General.
3. Click on the Add a syslog server link. In the given fields enter the EventLog Analyzer server IP address and UDP port number.
4. Define the roles so that data can be sent to the server.

   > Note
   >
   > If the Flows role is enabled on a Meraki security appliance then logging for individual firewall rules can be enabled/disabled. This can be done by navigating to the Security appliance > Configure > Firewall and editing the Logging column.

5. Click Save.

7.6.17. Configuring the Syslog Service on pfSense devices

Last updated on: September 12, 2025

1. Login to the pfSense device.
2. Navigate to Status > System Logs > Settings.
3. Enable Remote Logging.
4. Choose BSD (RFC 3164, default) as the Log Message Format.
5. Specify the IP address and Port of the EventLog Analyzer server.
6. Check all the Remote Syslog Content.
7. Click Save.

7.6.18. Configuring the Syslog Service on H3C devices

Last updated on: September 12, 2025

1. Login to the H3C security device as an administrator.
2. Navigate to System view mode.
3. Enable the Info cente check box.
4. Configure an output rule for the host:
   info-center source {<module-name>|default} {console|monitor|logbuffer|logfile|loghost} {deny|level <severity>}
5. Specify a log host and configure the below parameters:
   info-center loghost {<ELA_SERVER_IP>} [port <port_number>][facility <local-number>]
6. Now you have successfully configured the H3C security device.

7.6.19. Configuration the Syslog service on Stormshield firewall

Last updated on: September 12, 2025

To enable log collection from Stormshield devices, follow the below steps:

1. Login to the firewall.
2. Click on the Configuration tab.
3. Click on the Notification button. Select Enable to start the Syslog service.
4. In the Destination field, enter the IP address of EventLog Analyzer.
5. Click Save.

7.6.20. Configuration steps for Syslog forwarding from F5 devices to EventLog Analyzer

Last updated on: September 12, 2025

1. To forward system logs:
   - Login into Configuration Utility.
   - Navigate to System > Logs > Configuration > Remote Logging.
   - Enter the remote IP. The remote IP in this case would be EventLog Analyzer server's IP address.
   - Enter the remote port number. The default remote port for EventLog Analyzer is 514.
   - Click on Add.
   - Click on Update.
2. To forward event logs. (Ex: Firewall Events, Application Security Event)
   - Create management port destination
     - Login to Configuration Utility.
     - Navigate to System > Logs > Configuration > Log Destinations.
     - Click on Create.
     - Enter a name for the log destination.
     - To specify the log type, click management port.
     - Enter the IP address of the EventLog Analyzer server.
     - Enter the listening port of the EventLog Analyzer server. The default listening port is 514.
     - For protocol, select the UDP protocol.
     - Click on Finish.
   - Create a formatted remote syslog destination.
     - Now navigate to System > Logs > Configuration > Log Destinations.
     - Click on Create.
     - Enter a name for the log destination.
     - To specify the log type, select remote syslog.
     - Under syslog settings, set the syslog format as syslog and select the forward to management Port as the syslog destination.
     - Click on Finish.
   - Create a log publisher to forward the logs.
     - Navigate to System > Logs > Configuration > Log Publishers.
     - Click on Create.
     - Enter a name for the log publisher configuration.

- Enter a name for the log publisher configuration.
    - In the available list, click the previously configured remote syslog destination name and move it to the selected list.
    - Click on Finish.
- Create a logging profile for virtual servers.
    - Navigate to Security > Event Logs > Logging Profiles.
    - Click on Create.
    - Enter a profile name for the logging profile.
    - Then enable the Network Firewall or Application Security or Both by clicking on the checkbox.
        - For network firewall event logging, follow the steps below
            - Under the network firewall configuration, enter the publisher. Enter the previously configured Syslog publisher.
            - Under log rule matches, click Accept, Drop, and Reject. (Note: If you do not want any logs, you can disable it).
            - Leave other options in default. (Note: Storage Format should be none)
        - For application security event logging, follow the below steps
            - Under application security configuration, select storage destination as Remote Storage.
            - Select logging format as Key-Value Pairs (Splunk).
            - Select the protocol as UDP or TCP.
            - Enter Eventlog Analyzer server IP address and port (513/514) and click on Add.
    - Then click on Create.
- Apply Logging Profile to corresponding Virtual Server
    - Now navigate to Local Traffic > Virtual Servers
    - Select your virtual server to which you want to apply logging profile.
    - On the top, tap on the security tab and click on the policy.
    - Go to Network Firewall.
    - Set Enforcement: Enabled, and select your network firewall policy.
    - Under log profile, enable the log profile and select the previously configured logging profile.
    - Then click on Update.

7.6.21. Adding Forcepoint devices to EventLog Analyzer

Last updated on: September 12, 2025

For EventLog Analyzer to collect logs from Forcepoint devices, log forwarding has to be enabled in the Forcepoint NGFW Security Management Center.

1. From the Security Management Console go toConfiguration > Network Elements > Servers > Log Server
2. Right-click on Log Server and select Properties. The Log Server - Properties pop-up will open.
3. Click on Add. The following fields have to be filled with the information below.
4. Enter the hostname or IP address of the EventLog Analyzer server.
5. Enter port numbers 513 for TCP and 514 for UDP.
6. Select the CEF format in log format.
7. Select the Log Forwarding tab and click on OK.

Forwarding Forcepoint Audit Logs.

1. From the Security Management Console go toConfiguration > Network Elements > Servers > Log Server
2. Right-click on Management Server and select Properties. The Log Server - Properties pop-up will open.
3. Click on Add. The following fields have to be filled with the information below.
4. Enter the hostname or IP address of the EventLog Analyzer server.
5. Enter port numbers 513 for TCP and 514 for UDP.
6. Select the CEF format in log format.
7. Select Audit Forwarding and click on OK.

7.6.22. Adding Dell switches to EventLog Analyzer

Last updated on: September 12, 2025

For EventLog Analyzer to collect logs Dell switches, logging has to be enabled on the switch.
Logging can be enabled in Dell switches by entering the following commands in the command prompt.

Command	Parameters
console# configure	Enter configuration mode.
console(conf)# logging <IP address of the EventLog Analyzer server>	Set IP address or hostname identifying the external syslog server to send the log output.(Optional) UDP and TCP port designation can be entered as well.

> **Note**
>
> For more information, kindly refer to the documentation of your Dell switch.

7.6.23. Configuring the Syslog Service on Topsec devices

Last updated on: September 12, 2025

To configure the Syslog service in your Topsec devices, follow the steps below:

1. Login to the Topsec device as an administrator.
2. Navigate to Logs and alarms > Log Settings
3. Configure the details as mentioned below:
   - Server address - Provide EventLog Analyzer's server address
   - Server port - Enter 513 or 514 which is EventLog Analyzer's default syslog collection port
   - Transmission type - Syslog
   - Select the Whether to transmit check box.
   - Ensure that you DO NOT select 'Whether to combine transmission data' and 'Whether the data is encrypted or not' check boxes.
   - Log level - Information
   - Check all the necessary Log Type boxes
   - Select Input Log language as English
4. Click Apply to save the above settings

Topsec reports

EventLog Analyzer supports Topsec Firewall and provides out-of-the-box reports for the following categories of events:

Topsec Events:

Provides information on all the events associated with Topsec devices.

Logon Reports

These reports provide information on successful logons, logoffs, failed logons, and logon overview.

Firewall Allowed and Denied Traffic:

Provides insights on traffic based on source, destination, protocol and also generates a report on traffic trends.

Firewall IDS/IPS Events:

Provides insights on attacks based on source and destination IP address, also provides a report on attack trends.

Firewall Policy Management

The reports in this category provide useful information on policies added, deleted or modified.

Firewall Account Management

This category provides reports on users and roles added, deleted or modified.

Interface Events

The reports in this category let you monitor interface events such as Interface Up and Interface Down.

System Events:

Provides reports on configuration changes and system reboot.

Device Severity Reports:

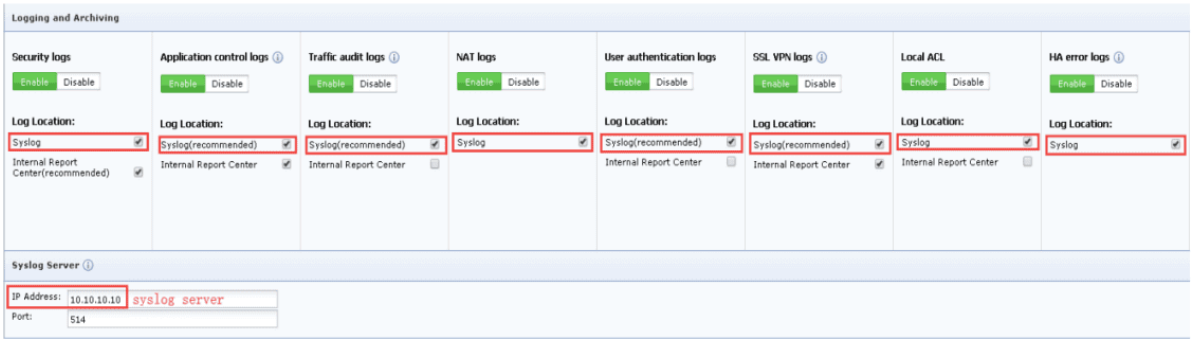
Provides reports on emergency, alerts, critical, error, warning, and notice events.

Configuring the Syslog Service on Sangfor devices

Last updated on: September 12, 2025

To configure the Syslog service in your Sangfor NGAF devices, follow the steps below:

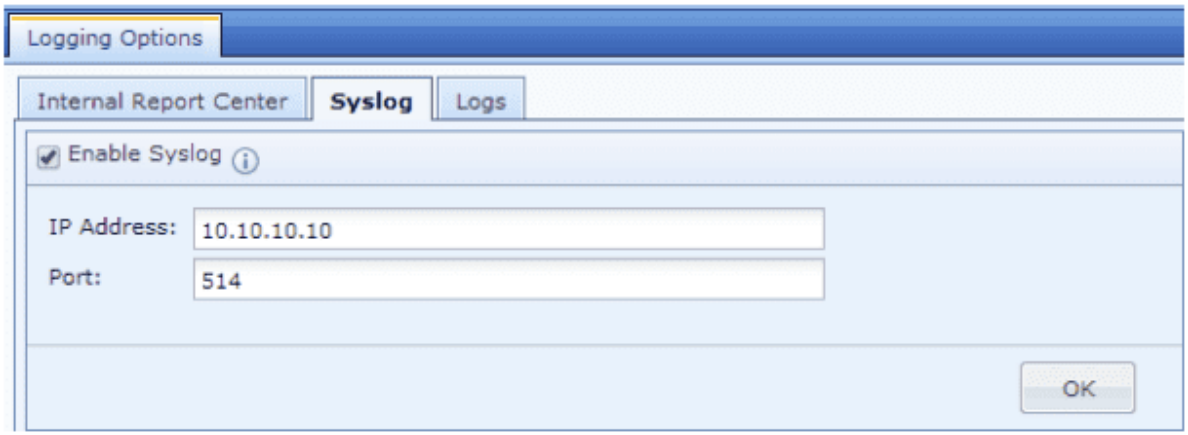
1. Access the NGAF Web Interface.
2. Open a web browser and navigate to the NGAF's management IP address. Login using your administrator credentials.
3. Navigate to System > Logging Options
4. Check all Syslog checkboxes under Log Location for the type of logs to be forwarded.



5. In Syslog Server tab, enter the IP address of EventLog Analyzer server and port (514), which is EventLog Analyzer's syslog listener port, in the respective boxes.
6. Click OK to apply changes.

For NGAF version 6.4 and below:

1. Access the NGAF Web Interface.
2. Open a web browser and navigate to the NGAF's management IP address. Login using your administrator credentials.
3. Navigate to System > Logging Options > Syslog
4. Check Enable Syslog checkbox.

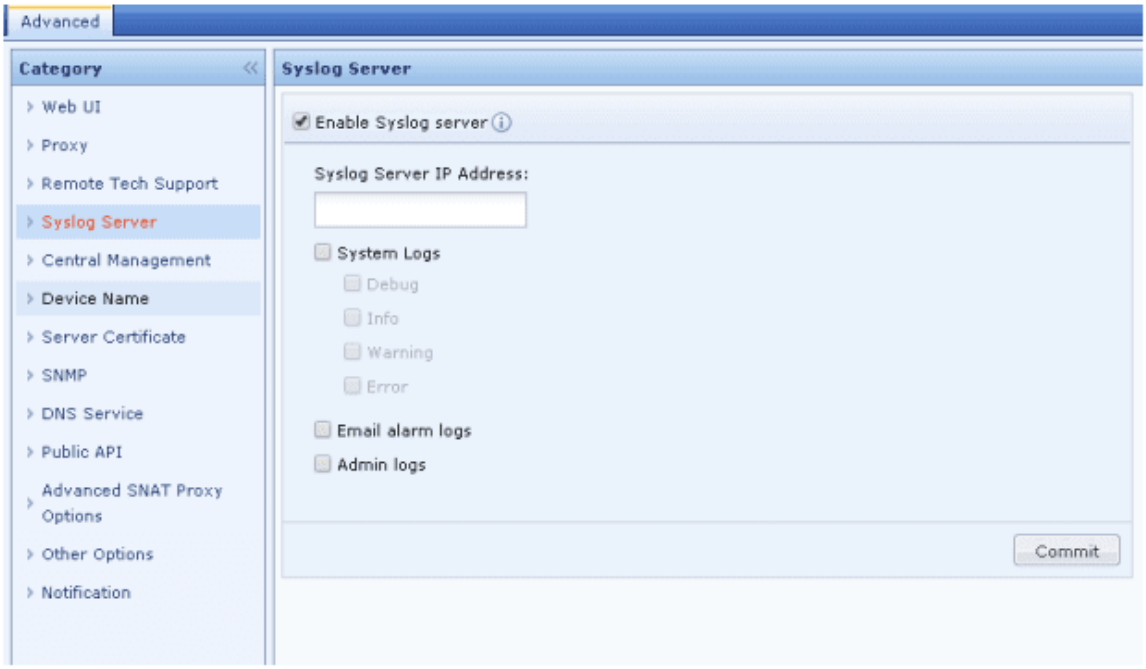


1. Enter the IP address of the EventLog Analyzer server and port (514), which is EventLog Analyzer's syslog listener port, in the respective boxes.

2. Click OK to apply changes.

To configure the Syslog service in your Sangfor IAM devices, follow the steps below:

1. Access the IAM Web Interface.
2. Open a web browser and navigate to the IAM's management IP address. Login using your administrator credentials
3. Navigate to System > General> Advanced > Syslog Server.



4. Check the Enable Syslog Server checkbox.
5. Enter the IP address of the EventLog Analyzer server and EventLog Analyzer's syslog Listener port in the given box as ipaddress:port example: 10.10.10.1:514
6. Click Commit to apply changes.

Sangfor reports
EventLog Analyzer supports Sangfor Firewall and provides out-of-the-box reports for the following categories of events:

Sangfor Events:

Provides information on all the events associated with Sangfor devices.

Logon Report

These reports provide information on successful logons, logoffs, and logon overview.

Firewall Allowed and Denied Traffic:

Provides insights on traffic based on source, destination, protocol, and also generates a report on traffic trends.

Firewall IDS/IPS Events:

Provides insights on attacks based on source and destination IP address, also provides a report on attack trends.

VPN Reports:

Provides insights on VPN logons, failed logons, logons trend, VPN blocked connections.

System Events:

Provides reports on configuration changes.

Device Severity Reports:

Provides reports on emergency, alerts, critical, error, warning, and notice events.

7.6.25. Enabling Stackato Logging

Last updated on: September 12, 2025

EventLog Analyzer automatically adds and collects your stackato logs upon executing the following command in your tty console:$kato config set logyard drainformats/<Format Name>[<PRI>{{.Text}}]
For UDP based log collection:
$kato drain add ela udp://<ela_server_name>:<udp_port_no> -f systail-ela-local
For TCP based log collection:
$kato drain add ela tcp://<ela_server_name>:<tcp_port_no> -f systail-ela-local

Example:

$kato config set logyard drainformats/systail-ela-local[{<13>{{.Text}}]
$kato drain add ela udp://ELA:514 -f systail-ela-local
By default, EventLog Analyzer uses 513 and 514 as default UDP ports. In case you have changed the UDP port number, specify the same here.

Logyard will now drain all logs in the format name as specified to EventLog Analyzer's UDP port number as given. EventLog Analyzer can now collect all the stackato logs as syslogs and analyze them with special reports.

7.6.26. Configuring Zscaler NSS

Last updated on: September 12, 2025

Navigate to Edit NSS Feed in the console and specify the following details:

Navigate to Edit NSS Feed in the console and specify the following details:

1. Enter the EventLog Analyzer server IP address in the field SIEM IP address.
2. Enter 514 as the SIEM TCP Port. If you have changed the default TCP port, then specify the changed port number here.
3. Select the Field Output Type as Tab-separated.
4. Append <96> at the start of the Feed Output Format before "%s... which specifies to EventLog Analyzer that the log messages must be processed.

7.7.1. Adding Common Event Format (CEF) Devices

Last updated on: September 12, 2025

1. Login to the application or device which supports CEF log format.
2. Go to syslog server configuration.
3. In the field for Log Format, select CEF Format.
4. In the Syslog Server IP address field, enter the <EventLog Analyzer IP address>.
5. Enter the syslog port and save the configuration.

To add CEF devices to EventLog Analyzer, click here.

7.7.2. Adding Print Servers

Last updated on: September 12, 2025

To configure and monitor the logs of Print Servers, follow the procedure below.

- Navigate to Settings > Log Source Configuration > Applications. You can also click on the +Add button on the top-right corner of the Home page and select Application.
- Next, select the General Application -> Add General Applications .
- Choose the Application Type as Printer.
- Expand the list by clicking the "+" icon to add a new device.
- Choose from the drop-down menu to add Configured devices, Workgroup devices, domain devices, etc.
- To add new devices manually, click on Configure Manually and enter Log Source.
- If the device type is syslog, check the Add as Syslog device box. If the device type is Windows, enter Username > Password > Verify Credentials.
- Click on Select and Add to add the log source.

Print Server Configuration

Enable Print Server Log: Go to Event Viewer > Application and Service Logs > Print Service. Right click on this and select 'Enable Log'. This will enable logging for the corresponding 'Admin', 'Debug' or 'Operational' processes. The logs can be viewed in Event Viewer.

> Note
>
> If the print server device is a 64-bit Windows OS machine (i.e., Windows Vista and above), carry out the following registry configuration:

- Open the registry editor 'regedit' of the print server machine in the Command Line Window.
- Navigate to Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\
- To create a new key, right click on eventlog, click new > key. You can name the key as Microsoft-Windows-PrintService/Operational or Microsoft-Windows-PrintService/Admin or Microsoft-Windows-PrintService/Debug as per your logging process requirement.
- For instance, if you need to enable logging for the Operation process, create a new key with the name Microsoft-Windows-PrintService/Operational.

This will convert the log type to 'Administrative' thus enabling you to perform searches and generate reports out of these logs.
This configuration is not required for a 32-bit Windows OS versions.
In order to obtain the document name, you have to enable the audit policy:
Computer Configuration>Administrative Templates>Printers>Allow job name in event logs
(or) Registry edit:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows NT\Printers]
"ShowJobTitleInEventLogs"=dword:00000001

7.7.3. Adding Terminal Servers

Last updated on: September 12, 2025

- Navigate to Settings > Log Source Configuration > Applications. You can also click on the +Add button on the top right corner of the Home page and select Application.
- Next, select the General Application -> Add General Applications .
- Choose the Application Type as Terminal.
- Expand the list by clicking the "+" icon to add a new device.
- Choose from the drop-down menu to add Configured devices, WorkGroup devices, domain devices, etc.
- To add new devices manually, click on Configure Manually and enter Log Source.
- If the device type is syslog, check the Add as Syslog device box. If the device type is Windows, enter Username > Password > Verify Credentials.
- Click on Select and Add to add the log source.

Configuring Terminal Server: Open Event Viewer > Application and Service Logs > Microsoft > Windows > TerminalServices-Gateway > Operational and right click and select 'Enable Log'. This will enable logging for the corresponding 'Gateway' or 'Operational' processes. The logs can be viewed in Event Viewer.

> Note
>
> If the terminal server device is a 64-bit Windows OS machine (i.e., Windows Vista and above), carry out the following registry configuration:

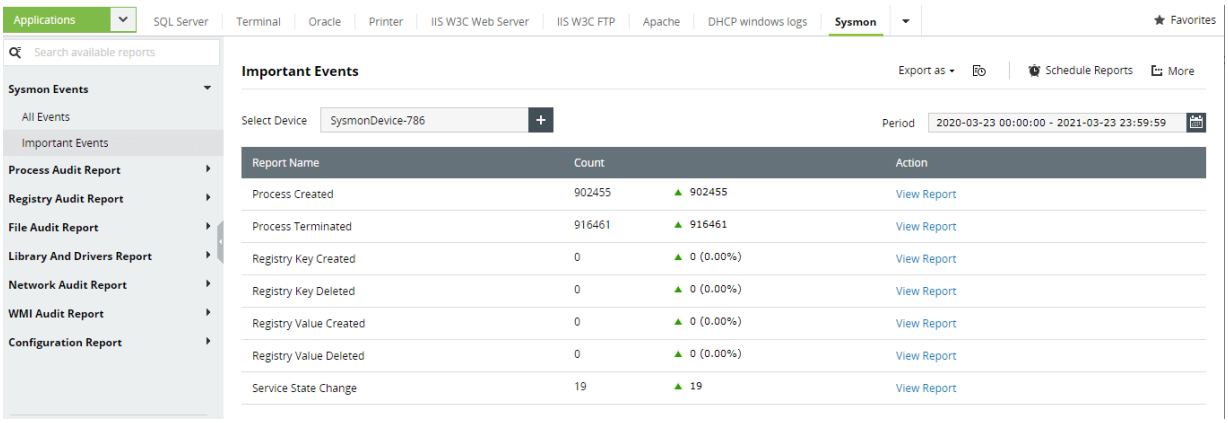
- Open the registry editor 'regedit' of the Terminal Server machine in the Command Line Window.
- Navigate to Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\
- To create a new key, right click on eventlog, click new > key. You can name the key as Microsoft-Windows-TerminalServices-Gateway/Operational.

This will convert the log type to 'Administrative' thus enabling you to perform searches and generate reports out of these logs.
The above configuration is not required for 32-bit Windows OS versions.

7.7.4. Adding Sysmon Application

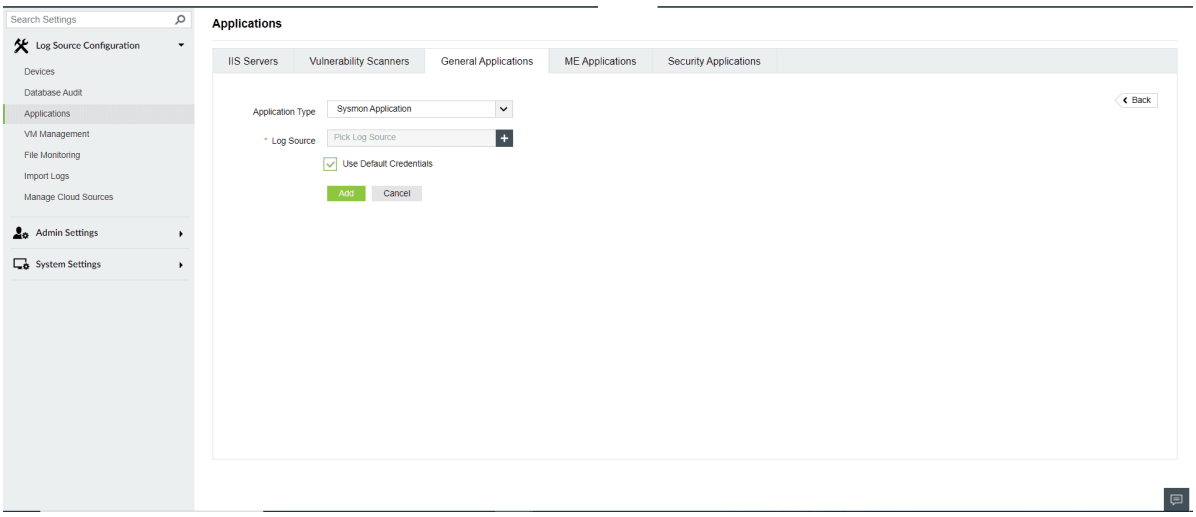
Last updated on: September 12, 2025

Sysmon (System Monitor), when installed on a system, audits the activities of the system, which include registry activities, file activities, process activities, network driver activities and more.
Devices that have Sysmon installed in them can be added as Sysmon Application to categorize the events into different reports.



Procedure to add a device as Sysmon Application is given below,

- Navigate to Settings > Log Source Configuration > Applications. You can also click on the +Add button on the top right corner of the Home page and select Application.
- Click on the General Application -> Add General Applications .
- Choose Sysmon Application as Application Type

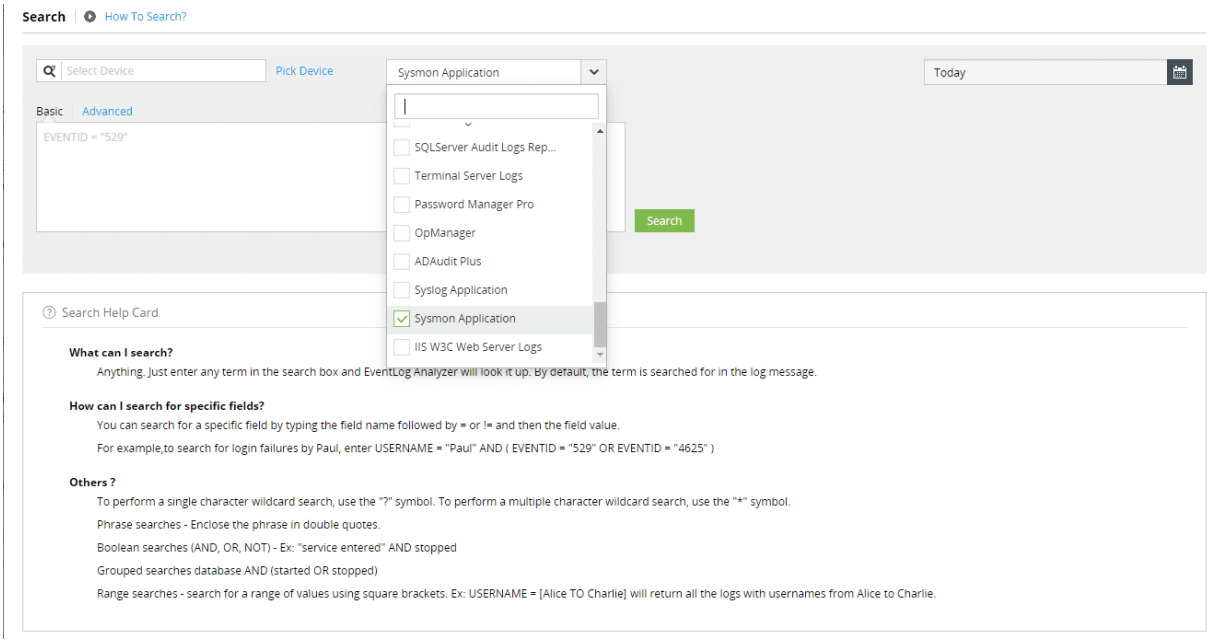


- Expand the list by clicking the "+" icon to add a new device.
- Choose from the drop-down menu to add Configured devices, WorkGroup devices, domain devices, etc.
- To add new devices manually, click on Configure Manually and enter Log Source.
- If the device type is syslog, check the Add as Syslog device box. If the device type is Windows, enter Username > Password > Verify Credentials.

- Click on Select and Add to add the log source.

In Search

Navigate to Search. You can search for Syslog Application logs by clicking the drop down box and scrolling down. You will find a specific logtype categorization for Sysmon Application.



To gain more insights from Sysmon Application logs, you can extract or create custom/new fields from the logs. Click here to know more.

EventLog configurations for logging

Please note that these configurations will be added automatically when the device gets added as a Sysmon Application, provided the credentials have the privilege to access the registry and add the key. If not configured automatically, this key has to be added and enabled for logging to take place.

Steps to add the key in the registry

Using the Command Line window, open the registry editor 'regedit' of the print server machine.
Navigate to Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\
To create a new key, right click on eventlog, click new > key. You can name the key as Microsoft-Windows-Sysmon/Operational.

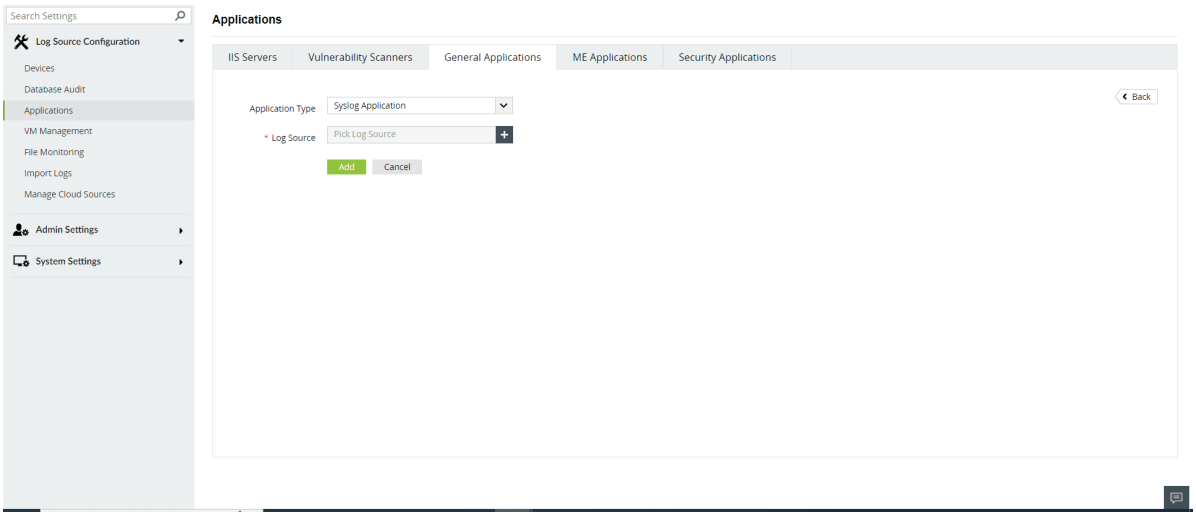
7.7.5. Adding a Syslog Application

Last updated on: September 12, 2025

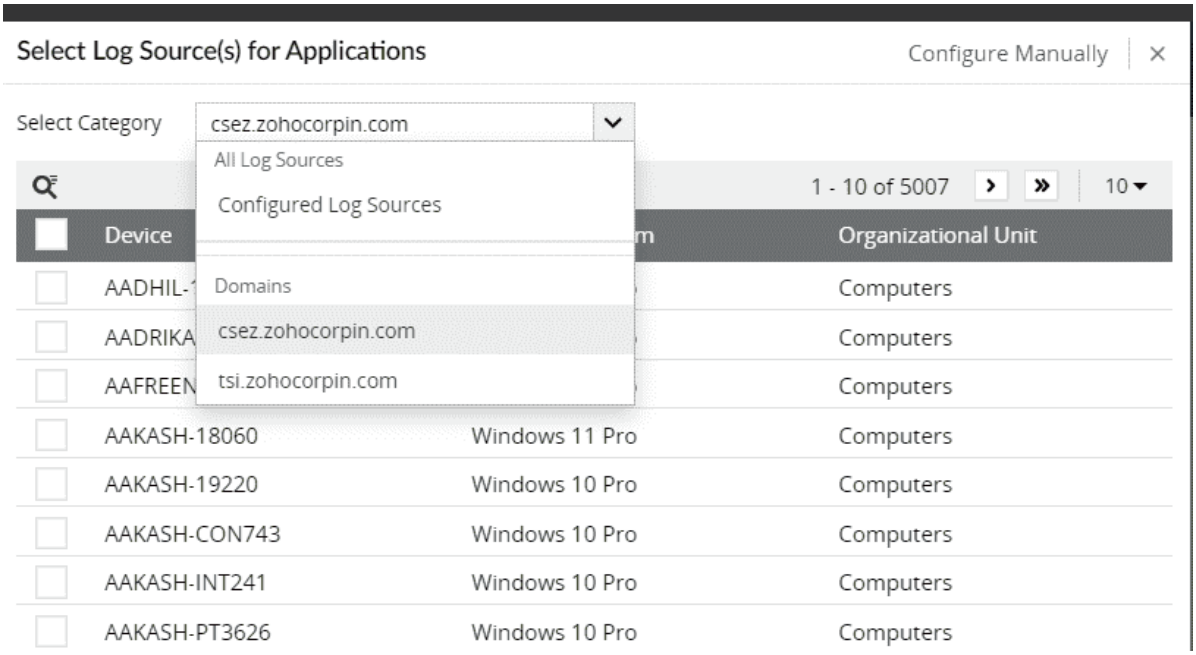
When should the Syslog Application be used?

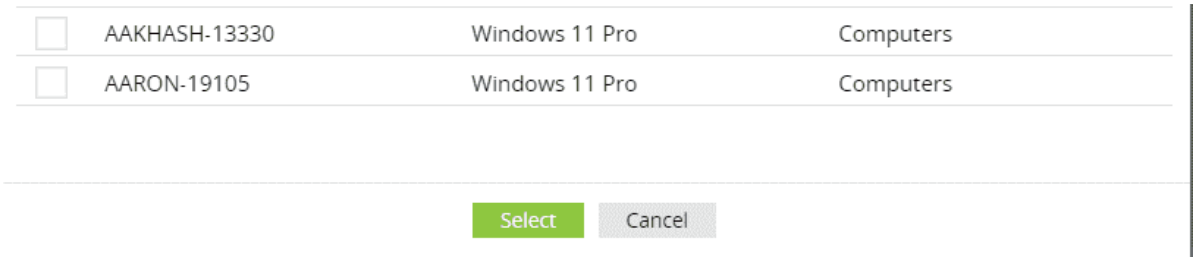
If syslog is simultaneously forwarded from a device that has already been configured as a Windows device, EventLog Analyzer server will ignore the syslog in order to maintain a single base log source. If you want to configure EventLog Analyzer server to receive syslog too from a Windows device, follow the procedure given below:

- Navigate to Settings > Log Source Configuration > Applications. You can also click on the +Add button on the top-right corner of the Home page and select Application.
- Click on the General Application -> Add General Applications .
- Choose Syslog Application as Application Type

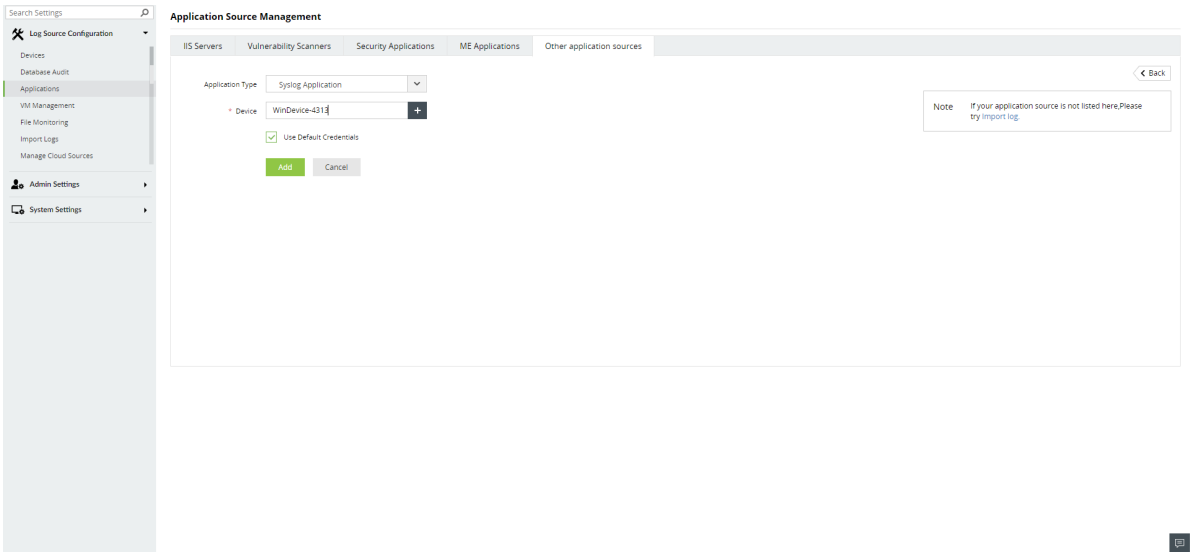


- Expand the list by clicking the "+" icon to add a new device.
- Choose from the drop-down menu to add Configured devices, Workgroup devices, domain devices, etc.



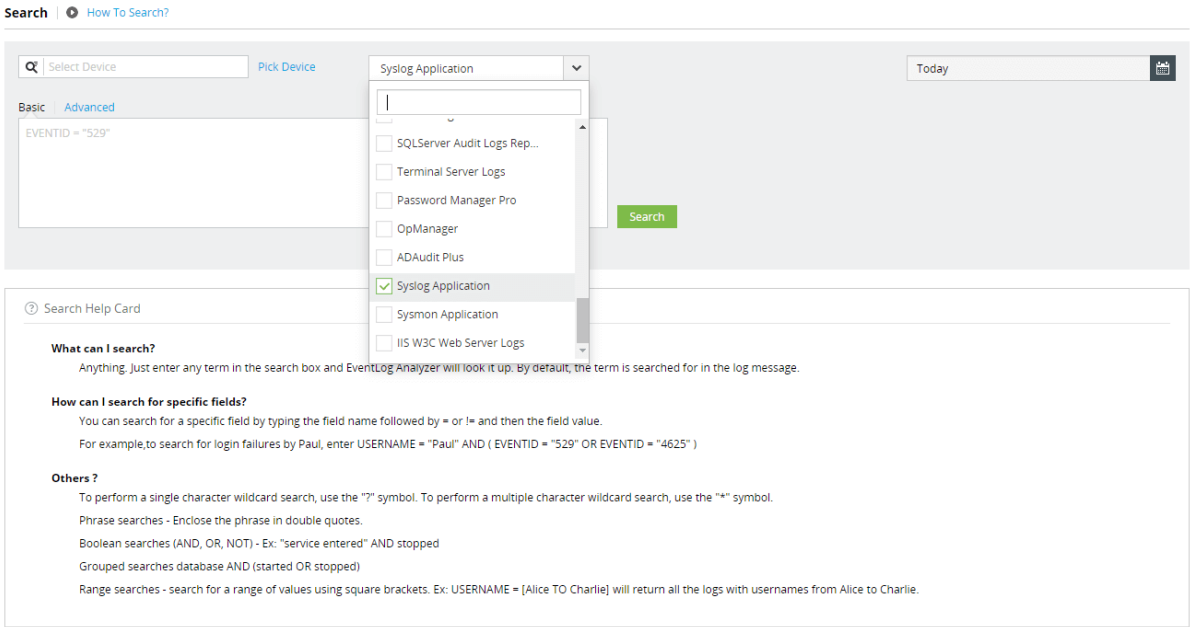


- To add new devices manually, click on Configure Manually and enter Log Source > Select and click on Add.



In Search

Navigate to Search. You can search for Syslog Application logs by clicking the drop down box and scrolling down. You will find a specific logtype categorization for Syslog Application.



To gain more insights from Syslog Application logs, you can extract or create custom/new fields from the logs. Click here to know more.

7.8. Adding ManageEngine Applications

Last updated on: September 12, 2025

EventLog Analyzer can be integrated with various other ManageEngine Applications such as:

- ADAudit Plus
- ADManager Plus
- Endpoint Central
- ADSelf Service Plus
- ITOM Solution Products
- Password Manager Pro
- ServiceDesk Plus

These integrations help users receive debug, server, and security information, that can be analyzed and displayed as actionable reports on EventLog Analyzer. Apart from this, integration with applications like Password Manager Pro enables users to correlate activities that are tracked within Password Manager Pro like the sharing of passwords, and events within Windows environment, like starting a remote sessions. This ensures early threat detection, mitigation and response.
Through the integration with ManageEngine's Endpoint Central, IT teams can generate alerts from Endpoint Central logs such as information on software and patches installed, policy modifications, and remote actions performed by Endpoint Central administrators. The integration also facilitates administrators to conduct forensics, correlate logs from both products, detect patterns, and run a response workflow to mitigate identified threats.

Steps to configure ManageEngine applications

Import Configuration

Configuring ManageEngine EventLog Analyzer to import ManageEngine Products' Logs.

- Navigate to Settings tab and click Applications under Log Source Configuration menu.
- Select ME Applications tab under Application Source Management component.
- Click Add ME Application button.
- Select the required ManageEngine Application from the Application drop down box.
- Select or Add device from the Device modal.
- Check Import File Logs check box.
- Configure the following in the Import File Logs component.
  - Protocol: select the desired protocol to import logs from the protocol dropdown box.
  - Provide Port number to the protocol if required.
  - Username: Enter the username of the selected device.
  - Password: Enter the password associated with that protocol (Windows user password in case of SMB-Windows protocol).
  - Log Folder: Click Browse button to browse and select the log folder of the selected Application.
  - Monitor Schedule: Configure the required interval to import logs.
- Click Add button to configure the selected ManageEngine AD Application with the selected device

> Note
>
> Only access logs and debug logs are imported in import configuration
> The supported products are:
> - ADAudit Plus
> - ADSelfServicePlus
> - ADManager Plus
> - OpManager
> - OpManager Plus
> - OpManager MSP
> - Firewall Analyzer
> - Netflow Analyzer
> - Network Configuration Manager
> - ServiceDesk Plus

Syslog Configuration

Configuring ManageEngine ADAudit Plus

- Log in to ADAudit Plus and navigate to the Admin tab.
- Under Configuration, click SIEM Integration.
- Check Enable Log forwarding of ADAudit Plus application logs check box.
- From the displayed component check EventLog Analyzer tab checkbox.
- Configure the following:
  - Server where Eventlog Analyzer is running: Enter the machine name or IP where EventLog Analyzer has been installed.
  - Eventlog Analyzer port number: Enter the port number where EventLog Analyzer is running.
  - Username: Enter the user name of the EventLog Analyzer user with the admin privilege.
  - Password: Enter the password of the EventLog Analyzer user with the admin privilege.
  - Protocol Settings: Select the protocol used by EventLog Analyzer from the Protocol Settings radio buttons.
  - Syslog Standard: Select the desired syslog standard to forward logs from the Syslog Standard radio buttons.
- Click Choose categories to forward button and select the logs to be forwarded to EventLog Analyzer from the Choose Application Log categories to forward modal.

> Note
>
> Only the ADAudit Plus user with admin tab and configuration setting privilege can enable integration with EventLog Analyzer.

Logs types description:

- Access Logs: ADAudit Plus web server access logs.
- Debug Logs: ADAudit Plus internal server operation logs : Server started, failed logons, successful logons and more.

Configuring ManageEngine ADManager Plus

- Log in to ADManager Plus and navigate to the Admin tab.
- Under System Settings, click Integrations.
- Under Log Forwarding, click EventLog Analyzer.
- Check the Enable Integration box to enable the integration.
- Configure the following:
  - Server where Eventlog Analyzer is running: Enter the name of the machine where EventLog Analyzer has been installed.
  - Eventlog Analyzer port number: Enter the port number where EventLog Analyzer service is running.
  - Protocol Settings: Enter the protocol used by EventLog Analyzer service.
  - Authentication: Enable this check box if EventLog Analyzer is hosted in a remote machine.
- Configure the following:
  - Username: Enter the Super admin user name of EventLog Analyzer.
  - Password: Enter the Super admin password.
  - Log Type: Select the log category of the logs to be forwarded to EventLog Analyzer. You can find more details at the log types description section given below.
  - Configure Syslog Port Manually: Check this option if the ports and protocol to forward the logs are to be changed manually. By default this information will be populated automatically based on the ports configured in EventLog Analyzer.
  - Syslog Protocol: Protocol to which logs will be forwarded.
  - Syslog Port: Destination EventLog Analyzer Port to which logs will be forwarded.
- Click 'Test Connection and Save' to establish connection and save the settings.

> Note
>
> For security reasons, only the ADManager Plus built-in admin can enable integration with EventLog Analyzer.

Logs types description:

- Access Logs: ADManager plus web server access logs.

- Debug Logs: ADManager plus internal server operation logs : Server started, failed logons,successful logons and more.
- User Activity Logs: Actions performed by users in ADManager plus will be forwarded in this category.

Configuring ManageEngine ADSelfServicePlus

- Log in to ADSelfService Plus and navigate to the Admin tab.
- Under Product Settings, click Integration Settings.
- Choose Log360 - EventLog Analyzer.
- Configure the following:
  - Server where Eventlog Analyzer is running: Enter the name of the machine where EventLog Analyzer has been installed.
  - Eventlog Analyzer port number: Enter the port number where EventLog Analyzer service is running.
  - Protocol Settings: Enter the protocol used by EventLog Analyzer service.
  - Username: Enter the Super admin user name of EventLog Analyzer.
  - Password: Enter the Super admin password.
  - Log Type: Select the log category of the logs to be forwarded to EventLog Analyzer. You can find more details at the log types description section given below.

> Note
>
> For security reasons, only the ADSelfService Plus built-in admin can enable integration with EventLog Analyzer.

Logs types description:

- Access Logs: ADSelfService plus web server access logs.
- Debug Logs: ADSelfService plus internal server operation logs : Server started, failed logons, successful logons and more.

Configuring ManageEngine ITOM solution products

Access logs and Debug logs Configuration for ITOM solution products

- Go to Settings -> General Settings -> Third Party Integrations.
- Now, click on the "Configure" button found at the bottom-right corner of the Log 360 - EventLog Analyzer section.
- Now, fill in the following details:
  - Server IP/DNS Name: Enter the IP address or the DNS name of the EventLog Analyzer-installed server, along with the port and the protocol.
  - Username: Enter the user name of the EventLog Analyzer user with the admin privilege.
  - Password: Enter the password of the EventLog Analyzer user with the admin privilege.
  - Select Log File: Select the logs to be forwarded to EventLog Analyzer, from the Select Log File drop down box.
    - Access logs: Logs that contain requests made to a web server, capturing information like the IP address, timestamp, requested resources, and outcomes of each request
    - Debug logs: Logs that are generated by OpManager during its operation, containing information used for diagnosing and troubleshooting issues.

> Note
>
> The following products from ManageEngine ITOM Solution support syslog integration with EventLog Analyzer:
> - OpManager
> - OpManager Plus
> - OpManager MSP
> - Firewall Analyzer
> - Netflow Analyzer
> - Network Configuration Manager

Alarms Configuration for ITOM Solution products

The following are the steps to configure ManageEngine ITOM Solution applications.

1. Login to the ITOM Solution application.
2. Navigate to Settings -> Notifications.
3. Click Add.

   Profile Type

Select Syslog Profile and enter the following details.

- Destination Host - EventLog Analyzer server name or IP address.
- Destination Port - Any port that the EventLog Analyzer instance is listening to.
- Severity and Facility must be the default values i.e. $severity and kernel.

For EventLog Analyzer to parse logs from OpManager, the message variables in the syslog profile of OpManager should be entered in the following format:
Mandatory message variables

- ALARM_MESSAGE:$message
- ALARM_ID:$alarmid
- ALARM_CODE:$alarmid

Other important message variables

- ALARM_SOURCE:$displayName
- ALARM_CATEGORY:$category
- ALARM_SEVERITY:$stringseverity
- ALARM_TRIGGER_TIME:$strModTime
- ALARM_EVENT_TYPE:$eventType
- Entity: $entity
- Last Polled Value: $lastPolledValue

4. Click Next.

Criteria

- Click on the Criteria check-box.
- Enable the notification for all severities and click Next.

Device Selection

- Select the By Device option and select all the devices listed under Remaining Devices and click Next.

Schedule

- You don't have to configure anything in this section. Click Next.

Preview

- Enter a profile name and click Save.

> **Note**
>
> If the same machine is running two or more ManageEngine products, ensure the following:

- The ports used by the products are unique.
- The EventLog Analyzer port receiving logs from OpManager and Password Manager Pro is not used by other ManageEngine products.



> **Note**

The following products from ManageEngine ITOM Solution Support Alarms Configuration:

- OpManager
- OpManager Plus
- OpManager MSP

Configuring ManageEngine Password Manager Pro

Here are the steps to configure Password Manager Pro.

1. Login to Password Manager Pro.
2. Navigate to Audit -> Resource Audit -> Audit Actions -> Configure Resource Audit. Enable the Generate Syslog option for all operations and click Save.
3. Navigate to Audit -> User Audit -> Audit Actions -> Configure User Audit. Enable the Generate Syslog option for all operations and click Save.
4. Navigate to Admin -> Integration -> SNMP Traps / Syslog Settings and click Syslog Collector.
   - Enter the EventLog Server name and a port that the EventLog Analyzer instance is listening to.
   - Select the protocol (UDP/TCP) and a facility name. Click Save.

HTTPs Action Log Collection Configuration

Configuring ManageEngine Endpoint Central

- Log in to Endpoint Central and navigate to the Admin tab.
- Under Integrations tab, click Log360 - EventLog Analyzer.
- Configure the following:
  - Server name where Eventlog Analyzer is running: Enter the machine name or IP where EventLog Analyzer has been installed.
  - Server Port: Enter the port number where EventLog Analyzer is running.
  - API Token: Find the steps to generate AuthToken here.
    - Component: EventLog Analyzer
    - Required scope : "http_listen"
  - Protocol: By default, HTTPS has been set to ensure secure communication. Since protocol is restricted to HTTPS, EventLog Analyzer should be configured to the same. Find the steps to enforce HTTPS here.
  - Data Transfer Interval: Select the interval in which the collective action logs have to be synced.

Note

- Only Endpoint Central users with admin tab and integrations setting privilege can enable the integration with EventLog Analyzer.
- If EventLog Analyzer using self signed SSL certificate, follow these steps to extract and import the SSL certificate used in EventLog Analyzer into Endpoint Central.

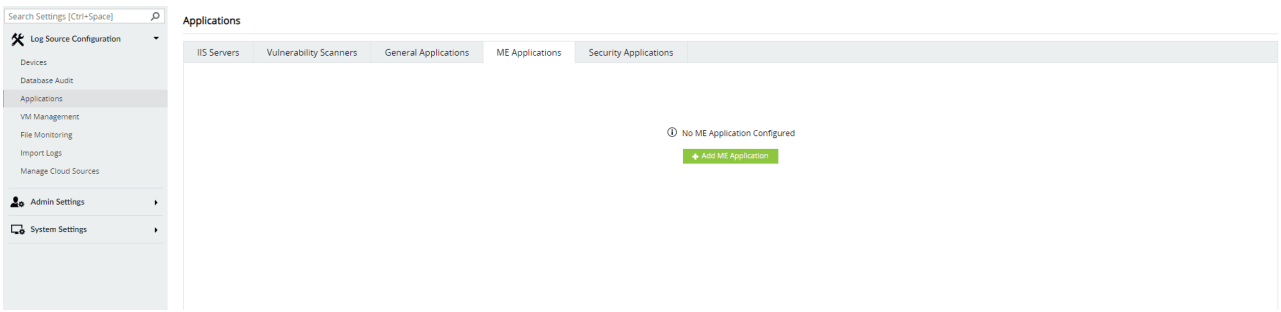
Data Enrichment Configuration for ManageEngine Endpoint Central and Vulnerability Manager Plus

By combining security data points from ManageEngine Endpoint Central or Vulnerability Manager Plus and advanced threat detection in Log360, you can quickly and effectively investigate and respond to security incidents.

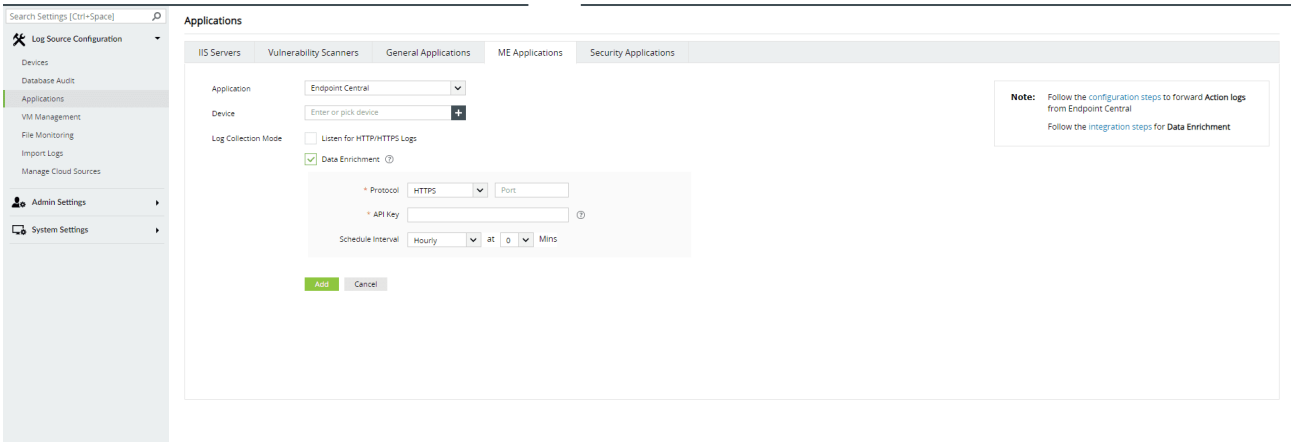
Configuring ManageEngine Endpoint Central and Vulnerability Manager Plus On-Premises Version

To configure,

- Navigate to the Settings tab and click Applications under the Log Source Configuration menu.
- Select ME Applications tab under Applications component.



- Click the Add ME Application button.



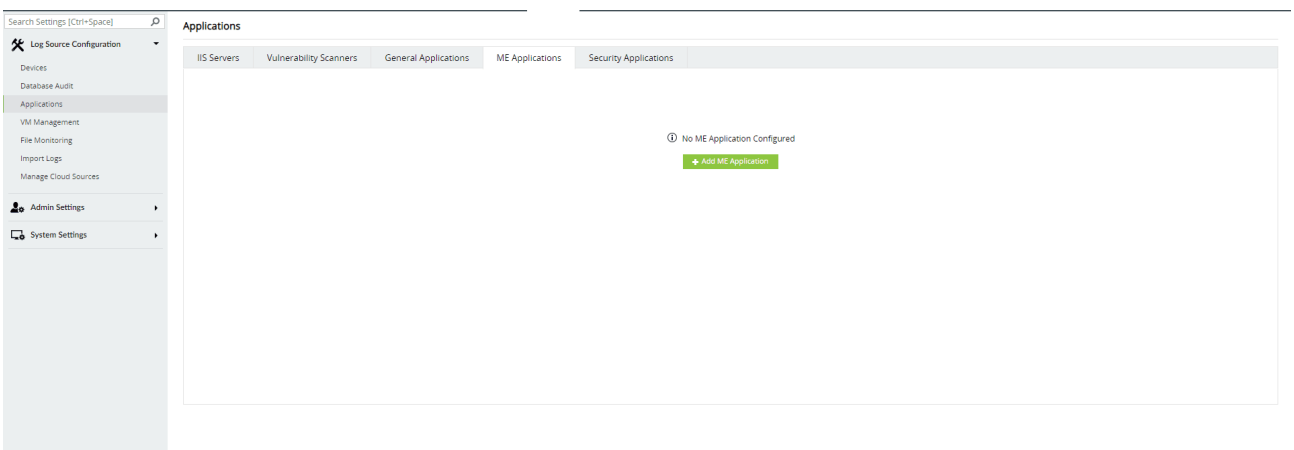
- Select Endpoint Central from the Application drop-down box.
- Enter or pick a device from the Device list. (Note: The device on which the Endpoint Central server runs.)
- Check the Data Enrichment box.
- Configure the following in the Data Enrichment component.
  - Protocol: Select the desired protocol to fetch data from the protocol dropdown box.
  - Provide a Port number to the protocol (Default port number for HTTP: 8020 & HTTPS: 8383)
  - Provide the API key generated from the Endpoint Central API Explorer. (Visit the API Explorer in Endpoint Central -> Admin tab & follow the steps given for authentication in this help document)
    - Note: Kindly make sure the user have following permissions [VulnerabilityMgmt_Read, PatchMgmt_Read, PatchMgmt_Write]
- Click Add to configure the chosen Endpoint Central application with the selected device. Note: Ensure the credentials have sufficient permissions to access APIs.

> Note
>
> - Kindly enable predefined alert profiles and correlation rules to use Data Enrichment.
> - To ensure seamless integration between EventLog Analyzer and Endpoint Central, follow these steps to import the SSL certificate of Endpoint Central (/webapps/DesktopCentral/client-data/server-certificates/DMRootCA.crt) into EventLog Analyzer.
> - You can follow the same steps mentioned above to integrate with Vulnerability Manager Plus as well.

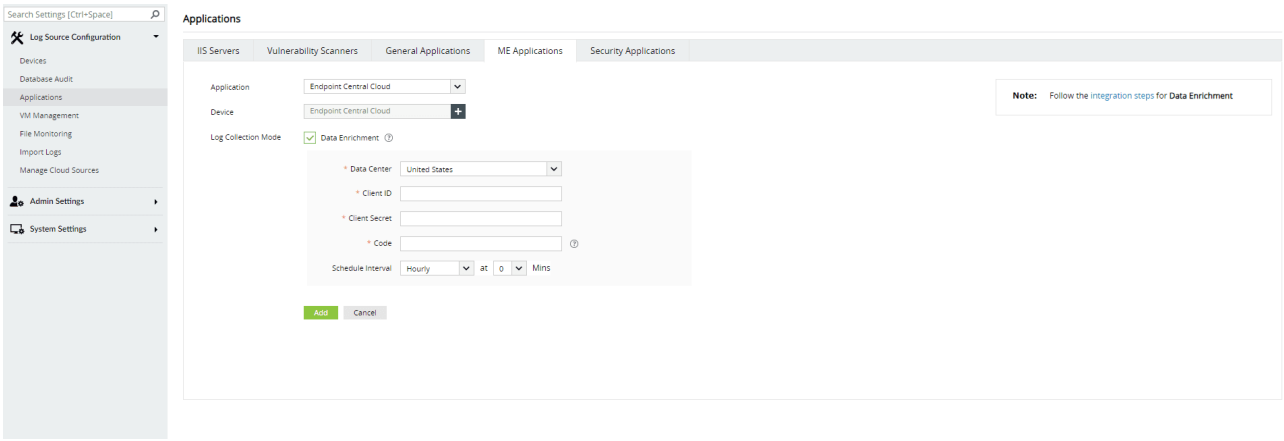
Configuring ManageEngine Endpoint Central Cloud Version

To configure,

- Navigate to the Settings tab and click Applications under the Log Source Configuration menu.
- Select ME Applications tab under Applications component.



- Click the Add ME Application button.



- Select Endpoint Central Cloud from the Application drop-down box.
- Check the Data Enrichment box (will be checked by default).
- Configure the following in the Data Enrichment component.
  - Data Center: Choose the data center where Endpoint Central Cloud is hosted.
  - Visit the respective Developer Console and follow the steps for authentication (Self Client Method) provided in this help document to obtain the following credentials:
    - Client ID: Paste the copied client ID under the Client Secret tab.
    - Client Secret: Paste the copied client secret under the Client Secret tab.
    - Code: Provide generated code.
      - Scopes to be considered while generating code.
        DesktopCentralCloud.PatchMgmt.UPDATE,DesktopCentralCloud.PatchMgmt.read,DesktopCentralCloud.Common.read,DesktopCentralCloud.VulnerabilityMgmt.READ
  - Schedule the required interval to sync data.
- Click Add to configure the chosen Endpoint Central Cloud application.

> **Note**
>
> Ensure the credentials have sufficient permissions to access APIs.

> **Note**
>
> Kindly enable predefined alert profiles and correlation rules to use Data Enrichment.

> **Note**
>
> This integration enhances your security posture by leveraging data from Endpoint Central. Here's what's new:
> - Vulnerability and misconfiguration comparators: Identify devices with vulnerabilities or misconfigurations using custom correlation rules and alerts.
> - Streamlined patch management: Approve and install patches directly through incident workflows.
>
> Using vulnerability and misconfiguration comparators:
> These comparators are available only after successful integration and can be used with device fields.
> - Is Vulnerable: Check if a device is tagged as vulnerable in Endpoint Central.
> - Vulnerable To: Identify devices vulnerable to specific attacks (e.g., CVE-2023-38831).
> - Misconfigured For: Detect devices with misconfigurations identified by Endpoint Central (e.g., Windows Credential Guard disabled).
>
> Creating custom correlation rules:
> Click here to learn how to create custom correlation rules using vulnerability and misconfiguration comparators.
> Creating custom alert profiles:
> Click here to learn how to create custom alert profiles using vulnerability and misconfiguration comparators.
> Managing patches with workflows:
> This integration introduces two new workflow actions:
> - Approve Patches
> - Install Patches

Click here to learn how to create incident workflows utilizing these actions.

Configuring ManageEngine ServiceDesk Plus

Prerequisite: ServiceDesk Plus built-in admin privilege is necessary to enable integration with EventLog Analyzer.

- Login to ServiceDesk Plus and navigate to the Admin tab.
- In the Admin Settings, select Integrations under Apps & Add-ons.
- Select ManageEngine SIEM under the ManageEngine tab.
- Check the Enable EventLog Analyzer box to enable the integration and configure the following:
  - Hosted URL: Enter the full URL where the EventLog Analyzer service is hosted. The URL should include the protocol (http or https), the host name or IP address, and the port number.
  - Username: Enter the Super Admin user name of EventLog Analyzer.
  - Password: Enter the Super Admin password.
  - Log Type: Select the category of logs to be forwarded to EventLog Analyzer. You can find more details in the log type description section given below.

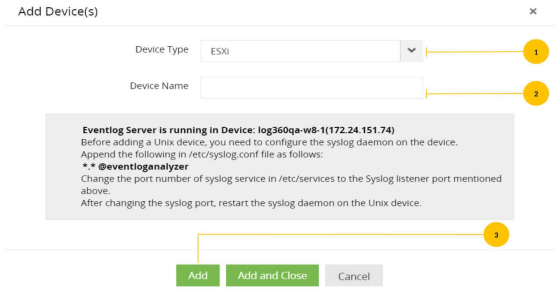
Logs types description:

- Access Logs: ServiceDesk Plus web server access logs.
- Debug Logs: ServiceDesk Plus internal server operation logs—Server started, failed logons, successful logons and more.

7.9.1. Adding Other Devices

Last updated on: September 12, 2025

In the Manage Devices page, navigate to the Other Devices tab and select the device type as required.

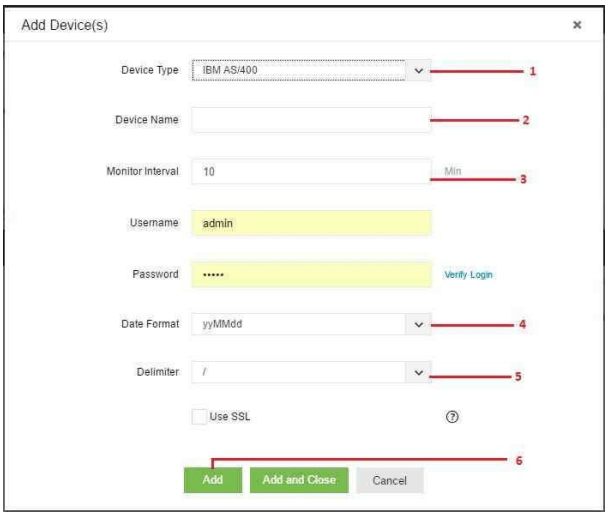


1. Select the Device Type as ESXi/IBM AS/400.
2. Enter the Device Name.
3. Click on the Add button to add the device for monitoring.

7.9.2. Adding IBM iSeries (AS/400) devices

Last updated on: September 12, 2025

Keep the ports 446-449, 8470-8476, 9470-9476 open in EventLog Analyzer to receive IBM AS/400 machine logs.
In the Manage Devices page, navigate to the Other Devices tab and click on the Add Device(s) button. This will open the Add Device(s) window.

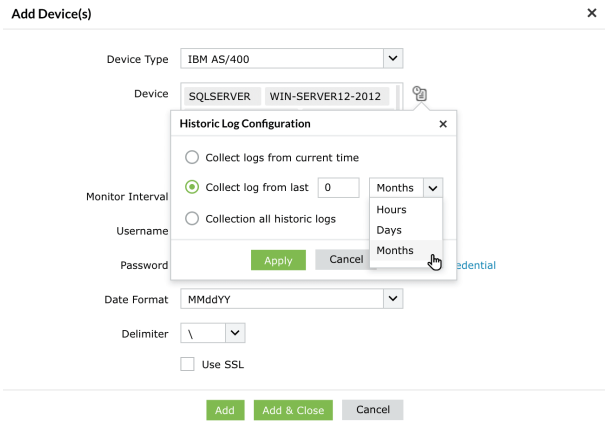


1. Choose the Device type as IBM AS/400.
2. Use the Device Name box to type a single device name, or a list of device names separated by commas.
3. Specify the Monitor Interval to configure the frequency at which EventLog Analyzer should fetch logs from the IBM AS/400 machines. The default (and minimum) monitor interval is 10 minutes.
4. Enter credentials (Login Name and Password) with an authority level of 50. Verify the details using the Verify Credential link beside the password text.
5. Select the Date Format and the Delimiter. This is the date format used in the logs that will be collected from the IBM AS/400 devices.
6. Click Add and Close to add this device and return to the list of device monitored, or click Add to add this device and continue adding more devices.

To import SSL certificate, follow the steps below:

1. Save the SSL certificate in the location C:\test.cer
2. In the command prompt navigate to <installation folder
3. Run the command keytool -importcert -alias myprivateroot -keystore ..\lib\security\cacerts -file C:\test.cer
4. Now provide the password when prompted. The default password is Changeit
5. To trust the certificate press Y
6. Restart the EventLog Analyzer server. The certificate will be successfully added.

IBM AS/400



IBM AS/400 historic log collection

EventLog Analyzer now allows you to collect logs according to the time period for IBM AS/400 devices. To collect logs according to time:

1. Click the historic log collection icon that is next to the Device option.
2. Next, under the Collect Logs from last option, select the number of hours/days/weeks/months for which you would like to collect the logs.
3. Click on Apply.

> **Note**
>
> The credentials provided must have an authority level of 50. Otherwise, EventLog Analyzer will not be able to login to fetch History logs from these devices.

Configuration to receive logs

For analyzing journal logs of IBM AS400/iSeries devices, you need to enable auditing in those systems.
To enable auditing for AS400/iSeries journal logs you have to:

1. Create a journal receiver.
2. Attach the journal receiver to a journal.
3. Specify the audit logs that are to be stored in the journal receiver.

Once the journal receiver is created and the logs specified are collected in it, EventLog Analyzer will fetch those logs for monitoring, report generation and alert notification.

> **Note**
>
> For setting up Security auditing in AS 400/iSeries machines, you must have the *AUDIT special

authority.

Create a journal receiver

You can create a journal receiver in a library of your choice by using the following command:

> **Note**
>
> This example uses a library called JRNLIB for journal receivers.

- Place the journal receiver in any library of your choice. Ensure that it is not placed in the QSYS library, which is a system library.
- Enter a name for the journal receiver.
- When you want the naming convention to be applied to naming all journal receivers, use the *GEN option.
- Specify an appropriate threshold level that suits your system size and activity. The size you choose should be based on the number of transactions on your system and the number of actions you choose to audit. For system change journal management support, the threshold must be at least 5000KB.
- To limit access to the information stored in the journal, specify *EXCLUDE on the AUT parameter.

Attach the journal receiver to a journal

- Create the QSYS/QAUDJRN journal by using the following command:
- The journal name QSYS/QAUDJRN must be used.

> **Note**
>
> To create this journal you must have the authority to add objects to QSYS.

- Specify the journal receiver name that you created, using the JRNRCV parameter.
- Specify *EXCLUDE on the AUT parameter to limit access to the information stored in the journal.
- (*SYSTEM) is passed as the parameter for Manage Receiver (MNGRCV). Thus when the attached journal receiver reaches its threshold size, the system itself detaches this receiver and creates and attaches a new journal receiver.
- Avoid detaching receivers and creating & attaching new receivers manually, using the CHGJRN command.
- To retain the detached journal receivers, specify (*NO) as the value for DLTRCV. This will prevent the automatic deletion of detached receivers by the system.
- QAUDJRN receivers are your security audit trail. Hence, ensure that they are adequately archived.

Specify the logs that are to be captured by the journal receiver

- Use the following command to specify the logs that are to be stored in the journal receiver created:

- To specify which actions are to be logged into the audit journal for all the users on the system, you need to set the audit level to the QAUDLVL system value using the WRKSYSVAL command.
- If you want to set action and object auditing for specific users, use the CHGUSRAUD command.
- You can also set object auditing for specific objects as per your requirement, using the CHGOBJAUD and CHGDLOAUD commands.
- Setting the QAUDENDACN system value helps you determine the systems action when it is unable to write an entry to the audit journal.
- With the QAUDFRCLVL system value parameters, you can control the transfer of audit records from memory to auxiliary storage.
- To start auditing set the QAUDCTL system value to any value other than *NONE.

Once this security auditing set up is completed, EventLog Analyzer will automatically fetch the logs collected in the journal receiver of the AS400/iSeries device that is added for monitoring. If the AS400/iSeries machine is not added to EventLog Analyzer server, add the device to begin collecting its logs.

7.9.3. File Integrity Monitoring (FIM)

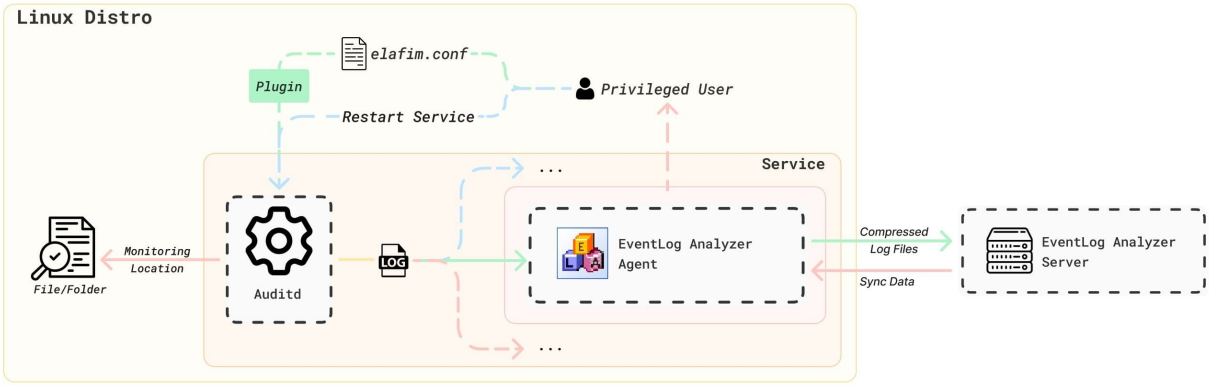
Last updated on: September 12, 2025

File Integrity Monitoring is a feature that helps you monitor all changes (addition/deletion/modification) made to files and folders in Windows and Linux systems.

Important Note

1. It is recommended that FIM be implemented for strictly necessary files and folders so as to avoid disk space issues that may rise due to the high volume of generated logs.
2. In Windows FIM module,
   - If a Windows file server is configured for FIM, both Windows Server and file server licenses are required.
   - If a Windows server is configured for FIM, only a Windows Server license is required.
   - If a Windows workstation is configured for FIM, only a Windows workstation license is required.

Linux FIM Agent Architecture:



To install packages, please find the syntax here.

Prerequisites for File Integrity Monitoring

Windows:

- When you enable File Integrity Monitoring for Windows, certain access policies will be automatically enabled on the file server. If there are overriding GPOs for audit policy in your domain, follow the below procedure to manually enable them

- In administrator command prompt enter the command, auditpol/get/category:"Object Access"
- Then proceed to enable the following access policies
  - Audit file share
  - Audit file system
  - Audit handle manipulation
  - Audit detailed file share
  - Audit other object access events.

- SACLs should be enabled for the monitored file/folders. These are automatically enabled by the product. If not, manually update SACLs with the following permissions
  - Execute files/ traverse folder
  - Write data/create files
  - Append data/create folders
  - Write attributes
  - Write extended attributes
  - Delete subfolders and files
  - Delete read permissions
  - Change permissions
  - Take ownership

Linux:

- The following packages should be installed on the agent machine
  - openssh-server [For UI related operations]
  - auditd
  - acl
- Ensure that,
  - SSH Port (default port 22) is reachable from the server.
  - ELA Server Port (default port 8095) is reachable from the agent machine.

  To verify if a port is reachable, you can use the below commands:
  Example: echo > /dev/tcp/ubuntu/8095 && echo "Port is Reachable"
  (or)
  Example: telnet ubuntu 8095
- Also ensure that the:
  - Linux kernel version is 2.6.25 or higher
  - Linux audit framework version is higher than 1.8
- Remove the following rules from /etc/audit/audit.rules file if they are enabled and then reboot the machine.

- Syscall block rule, "-a never,task", and
- Immutable rule, "-e 2".

- If you are enabling auditing for SUSE machines, set the following rule:
  - Navigate to /etc/sysconfig/auditd
  - Set AUDITD_DISABLE_CONTEXTS = no
- If Security-Enhanced Linux (SELinux) exists, then it must either be in the permissive mode or disabled:
  - Check SELinux status using the command: getenforce.
  - If the status is 'Enforced', navigate to file/etc/selinux/config and make this edit: SELINUX = permissive.
  - Restart the machine.

> Note
>
> The server utilizes the agent credential only for the actions mentioned in the document.
> Configuring FIM for Linux audits the following actions on Linux files:
> - Read
> - Write
> - Execute
> - Attribute change

Since auditd requires root or sudo privileges, if the user does not have the privileges, please follow the privileges steps.

Privileges for Installing FIM Agent:

1. Adding AgentManager to the Sudoers file.
2. Create a directory and assign privileges to it.

1. Adding AgentManager to the Sudoers file:
To run AgentManager with sudo privileges for the Non-Sudo User, please follow the below instructions:

- Use the root user for configuring the privileges.
- Please execute the below command:
- Add the below line to the sudoers file:
  Example:
  - visudo -f /etc/sudoers.d/testuser
  - testuser ALL=NOPASSWD: /opt/ManageEngine/EventLogAnalyzer_Agent/bin/AgentManager *

> Note

Ensure that AgentManager is added to the sudoers file prior to installation. To verify, follow the below command.
cat /etc/sudoers.d/<username>
Example: cat /etc/sudoers.d/testuser
Expected Output: testuser ALL=NOPASSWD: /opt/ManageEngine/EventLogAnalyzer_Agent/bin/AgentManager *

Reason for adding AgentManager in the Sudoers file:
The following actions require sudo privileges:

- Transfer the ownership of the Agent Directory and elafim.conf file [Under audit [or] audisp directory], to the root user.
- Restarting auditd service may also require root privileges.

2. Create a directory and assign privileges to it

To prevent unauthorized access to directories other than ManageEngine, follow the below commands as the root user for the non-sudo user.
Create a directory:
Granting privileges to the directory:
For CentOS/RHEL v8 and later/Ubuntu/openSUSE/Debian/Fedora:
For CentOS/RHEL v6 to v7.9:
Granting privilege to the audit.rules:
Example: setfacl -m u:testuser:rwx /opt/ManageEngine/

Configuring File Integrity Monitoring

To configure File Integrity Monitoring, go to

- Navigate to Settings > Configurations > Manage File Integrity Monitoring.
- Depending on which device the files and folders that you wish to monitor are located in, click on either the Windows or Linux tab.
- Click Add FIM.
- Pick the device in which the files/folders are located, enter correct credentials, browse and select the files and folders you wish to monitor. Alternatively, you can enter the location of the files/folders.

> **Note**
>
> For Linux devices, in addition to entering the details mentioned above, you will also be prompted to enter the SSH port number.

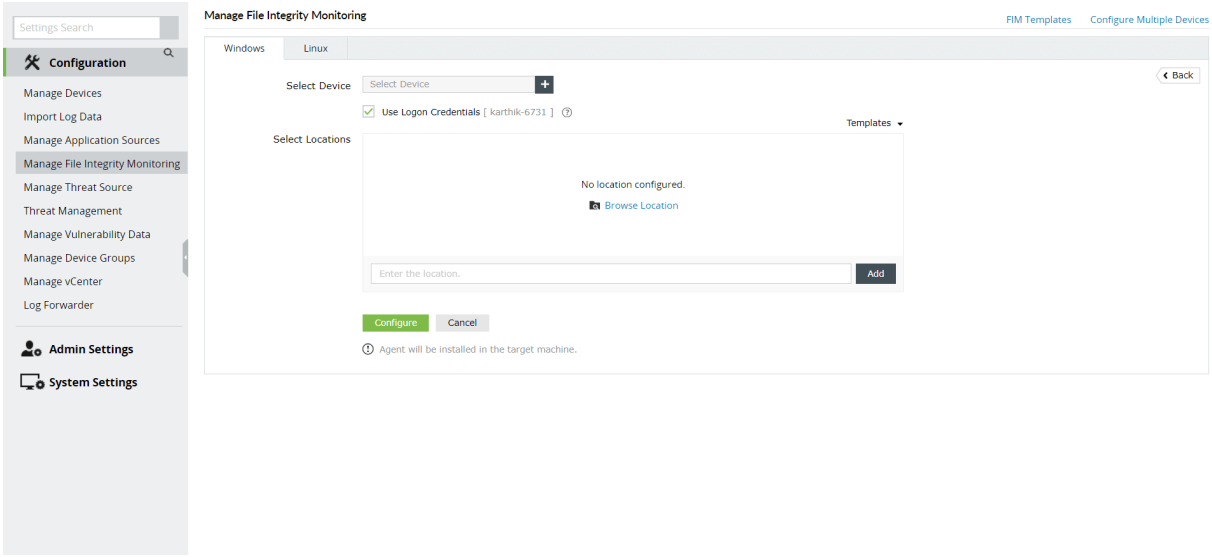
- The Exclude Filter gives you an option to exclude

- Certain file types.
- Certain sub-locations within the main location.
- All sub-locations within the main location.

- If you want to know who has made the change to the file or folder, check the Audit Username checkbox.

> **Note**
>
> For Linux devices, username is audited by default.

- Click Configure.



Configuring Bulk File Integrity Monitoring

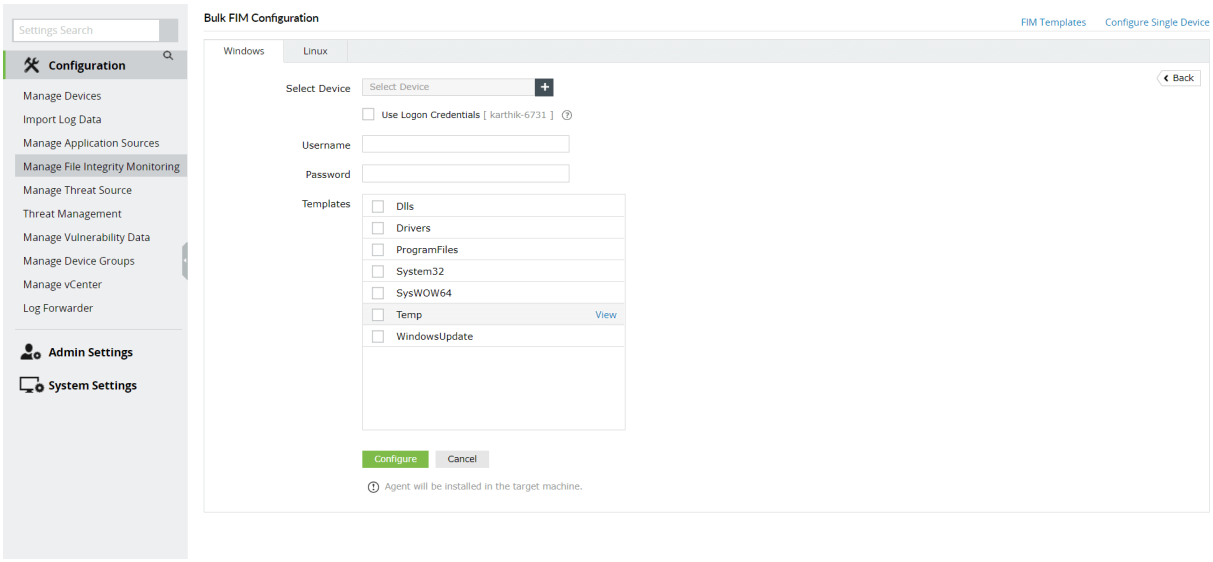
If the same files and folders located in multiple devices need to be added for monitoring, then the Bulk File Integrity Monitoring feature can be used.

- Navigate to Settings > Configurations > Manage File Integrity Monitoring.
- Depending on which device the files and folders that you wish to monitor are located in, click on either the Windows or Linux tab.
- Click Add FIM. Select Configure multiple devices on the top right corner.
- Pick the device in which the files/folders are located, enter correct credentials, and select the file template(s).

> **Note**
>
> For Linux devices, in addition to entering the details mentioned above, you will also be prompted to enter the SSH port number.

- Click Configure.

- Click Configure.



> **Notes**
>
> - If an agent is already installed in the device whose files you want to monitor, file monitoring will automatically be enabled in the agent.
> - If no agent is installed in the device for which you want to monitor the files, then an agent will be installed and file monitoring will be enabled in the agent.
> - Please note that the volume of logs generated for each change occurring on the folders can affect the performance of the file server. It is a recommended practice to limit file/folder monitoring to the required files/folders.

Manage File Integrity Monitoring (FIM) Templates

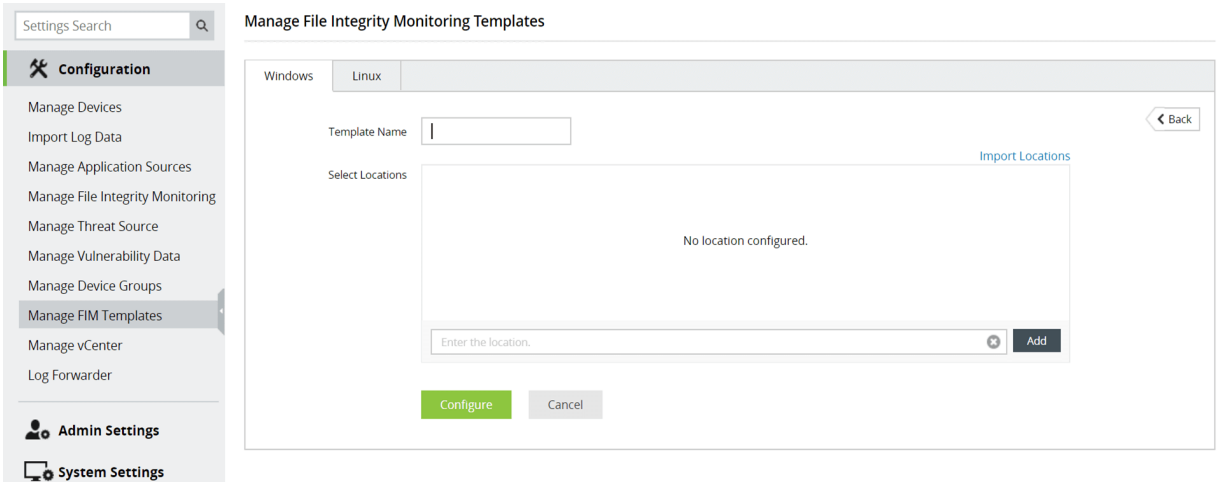
If the same file or folder needs to be monitored in a number of devices, then a template can be created and assigned to these devices. To create a FIM template follow the steps below:

- Navigate to Settings > Configurations > Manage File Integrity Monitoring > FIM Templates.
- Depending on which device the files and folders that you wish to monitor are located in, click on either the Windows or Linux tab.
- Click Add FIM.
- Enter a name for the template and select the locations of the files and folders.

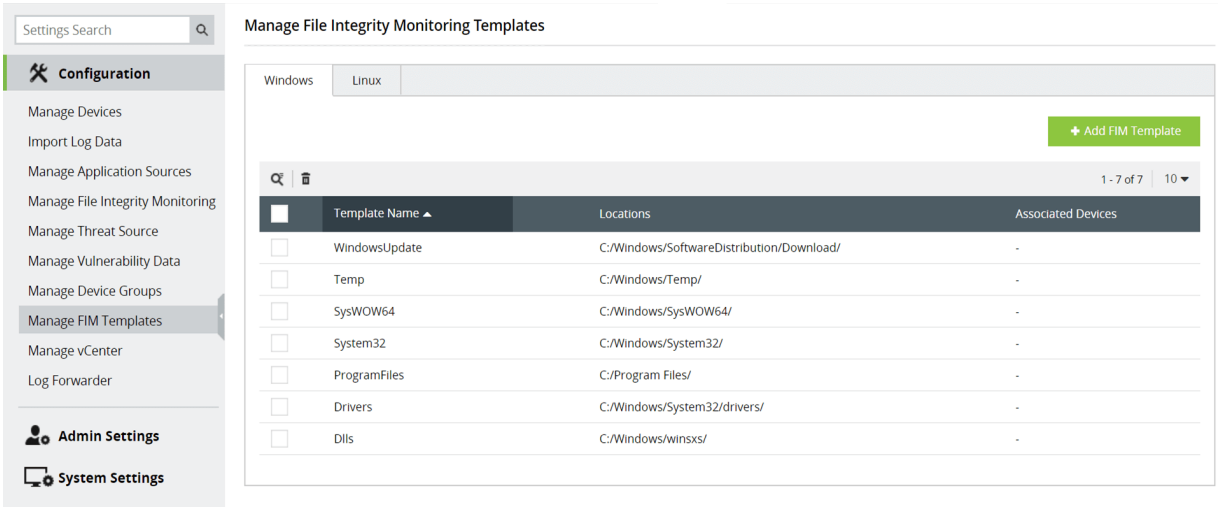
  Alternatively, you can enter the location of the files/folders.
- The Exclude Filter gives you an option to exclude
  - Certain file types.
  - Certain sub-locations within the main location.
  - All sub-locations within the main location

- All sub-locations within the main location.

- If you want to know who has made the change to the file or folder, check the Audit Username checkbox.
- Click Configure.



All the created templates are listed in a tabular column with an option to edit / delete them.



7.10.1. Import Log Files

Last updated on: September 12, 2025

EventLog Analyzer helps you collect and analyze logs from different sources such as servers, network devices, and applications. The solution provides actionable intelligence that helps security teams stay on top of security threats in the organization.
This solution provides you the capability to import log files. The supported log formats include Windows and syslog device formats, application log formats and archived files log formats.

Windows and syslog device log formats

- Windows Eventlog (EVTX format)
- IBM AS/400
- Linux/Unix Syslog format (RFC 5424 and 2131)

> **Note**
>
> To import .evt logs (Windows XP and Windows 2003), you will need to convert the .evt to .evtx using the command wevtutil export-log application.evt application.evtx /lf in your EventLog Analyzer installation.

Application log formats

- Apache access logs
- DHCP Linux logs
- DHCP Windows logs
- IBM Maximo logs
- IIS W3C FTP logs
- IIS W3C Web Server logs
- MSSQL Server logs
- MySQL logs
- PostgreSQL Logs
- ADAudit Plus logs
- ADManager Plus logs
- ADSelfService Plus logs
- ITOM solution logs
- ServiceDesk Plus Logs

Archived files log formats

Archived files log formats

- Cisco archive files
- Syslog archive files
- Windows archive files

Steps to import log files

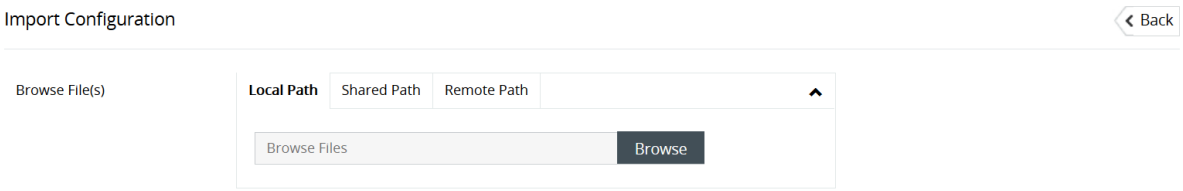
Navigate to the Import Configuration page using any one of the following menu options:

- +Add >Import Logs
- Settings > Configurations > Import Log Data
- Home > Applications > Imported Logs
- Home > Applications > Actions > +Import

Importing log files from different locations

EventLog Analyzer allows you to import:

- Log files from a local path.
- Log files from a shared path.
- Log files from a remote path.
- Log files from cloud storage.



Log file import from a local path

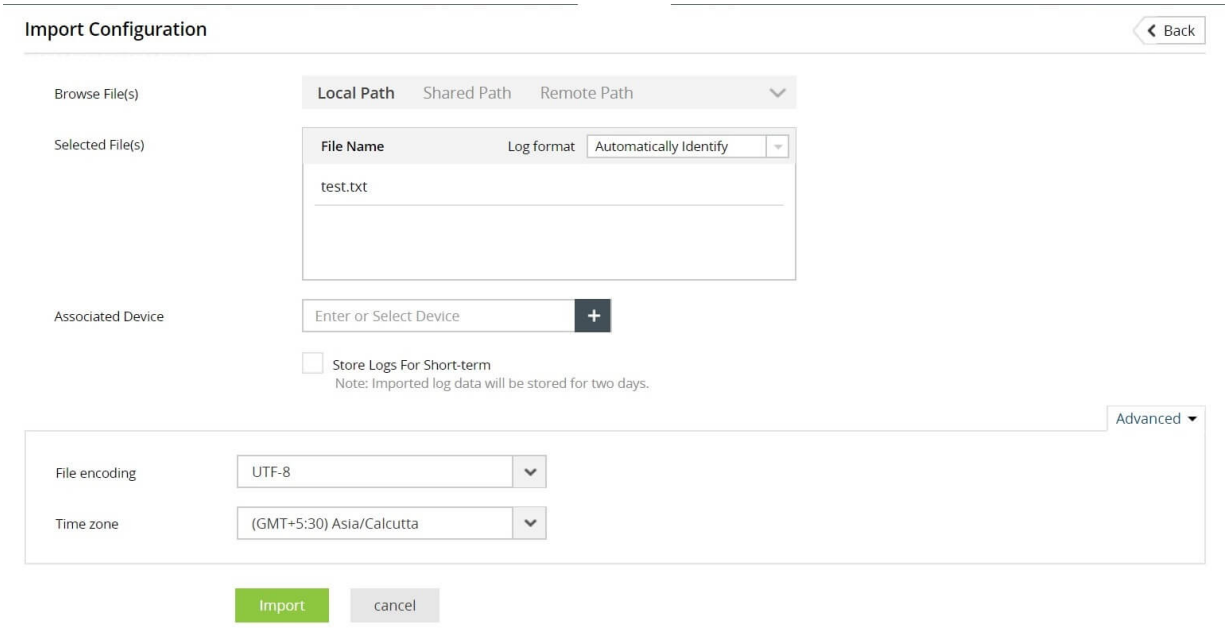
With this option, you can import log files from any device that has access to EventLog Analyzer.

> **Note**
>
> Log import cannot be scheduled to run at regular time intervals.

1. From the File Location option, select Local Path.
2. Click on Browse to select the necessary file(s) from your local device. Alternatively, you can enter the device name (or) IP address of the device (or) specify the full UNC path, then click on Open. The necessary file(s) is selected.
3. If you know the log format of the log file, select the log format from the given drop-down. If you do not know the log format select Automatically Identify.

> **Note**
>
> You can view a preview of the selected log file and extract the desired fields, by clicking on the View symbol of the attached log file and enabling the pop-up window option in your browser.

4. Click on the + button and OK to select the device that the log file is associated to. You can also enter the name of the device or select the device from the pop-up that appears.
5. If you wish to store the imported logs for 2 days, enable the Store logs for a short term option. By default, the log storage time-period is 32 days.
6. Click on Import.



Log file import from a shared path or UNC path

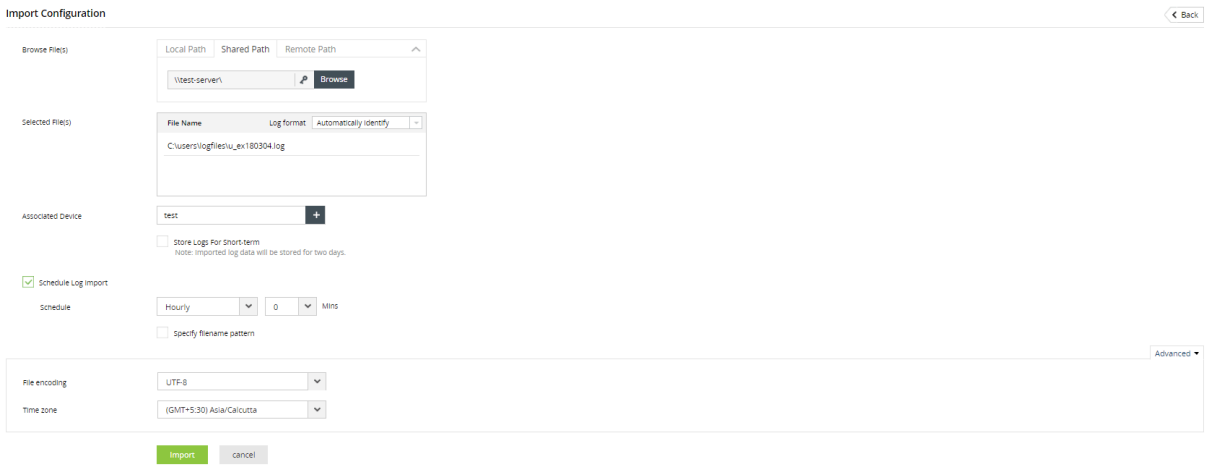
The log file import via Universal Naming Convention (UNC) path allows you to access shared network folders on a local area network (LAN).

1. From the File Location option, select Shared Path.
2. Enter the device name or IP address from which you wish to upload the log file. Alternatively, you can click on Browse to select the Windows device.
3. Select the desired file from the device and click OK. The necessary file is selected.
4. If you know the log format of the log file, select the log format from the given drop-down. If you do not know the

log format select Automatically Identify.

> **Note**
>
> You can view a preview of the selected log file and extract the desired fields, by clicking on the View symbol of the attached log file and enabling the pop-up window option in your browser.

5. Click on the + button and OK to select the device that the log file is associated to. You can also enter the name of the device or select the device from the pop-up that appears.
6. If you wish to store the imported logs for 2 days, enable the Store logs for a short term option. By default, the log storage time-period is 32 days.
7. If you want to automate a log file import at regular time intervals, enable the Schedule log import option.
8. With the Schedule drop-down menu you can customize the time interval between each log file import.
9. Additionally, you can build a file name pattern for the imported log files, using the time format options given. The name of the file stored at the specified time is updated in accordance to the file name pattern.
10. Click on Import.



Log file import from a remote path

Importing log files from a remote path in EventLog Analyzer needs authentication. This authentication can be achieved in two ways:

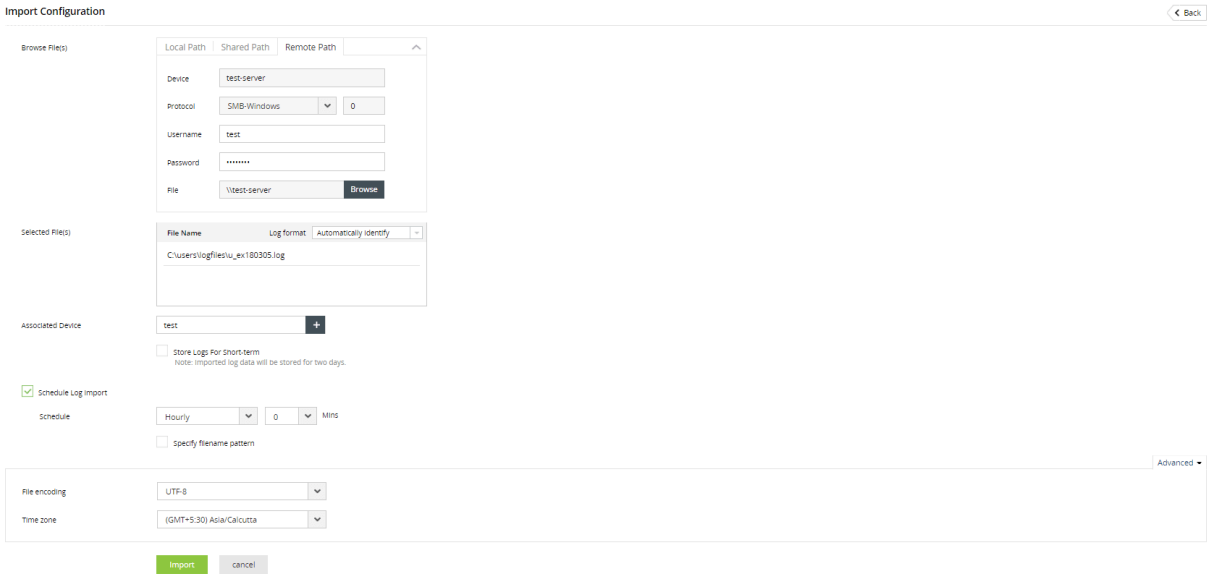
1. Username and password
2. SSH private key file sharing (Specific to SFTP protocol)

Authentication type: Password

1. From the Browse Files option, select Remote Path.
2. Enter the device name from which you wish to import the log file. Alternatively, you can click on the + icon to browse and select the Windows device.
3. Choose the required protocol (Ethernet, FTP and SFTP) and enter the port number.
4. Select the desired file from the device and click OK.

5. Provide the Username of the remote device and select Authentication Type as Password.
6. Enter the password in the field below.
7. Browse and select the Associated Device.
8. The Store Logs for Short-term option will store the imported log data in EventLog Analyzer for a brief period of two days. If the option is left unchecked, the logs will be stored as per your database retention configuration.
9. You can choose to schedule the log import at specific time intervals.

Authentication type: SFTP-based SSH private key file sharing



1. Select Remote Path from the Browse Files options listed.
2. Enter the device name from which you wish to import the log file. Alternatively, you can click on the + icon to browse and select the Windows device.
3. Choose SFTP as the protocol and enter the port number. (Default port value is 22)
4. Provide the username and choose Key File as the Authentication Type.

> **Note**
>
> EventLog Analyzer supports OpenSSH key file format only.

5. Browse and select the key file from the device. You can refer to this link to learn how to generate a key file with ssh-keygen, a standard component of Secure Shell protocol.
6. If the key file is passphrase protected, select the Use Passphrase checkbox and enter the phrase in the field below.
7. Browse and select the Associated Device.
8. The Store Logs for Short-term option will store the imported log data in EventLog Analyzer for a brief period of two days. If the option is left unchecked, the logs will be stored as per your database retention

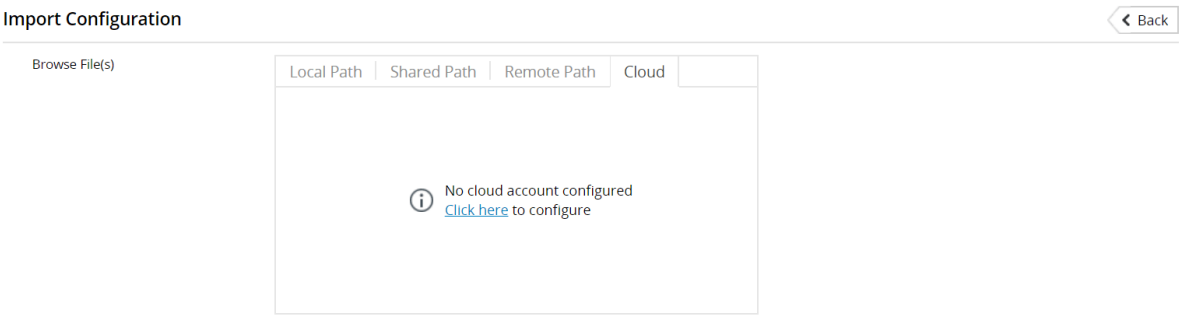
configuration.

9. If you would like to automate a log file import at regular time intervals, enable the Schedule Log Import option.
10. With the Schedule drop-down menu, you can customize the time interval between each log file import.
11. Additionally, you can build a Filename Pattern for the imported log files using the time format options given. The name of the file stored at the specified time will be updated in accordance to the file name pattern.
12. Click on Import to save the configuration.

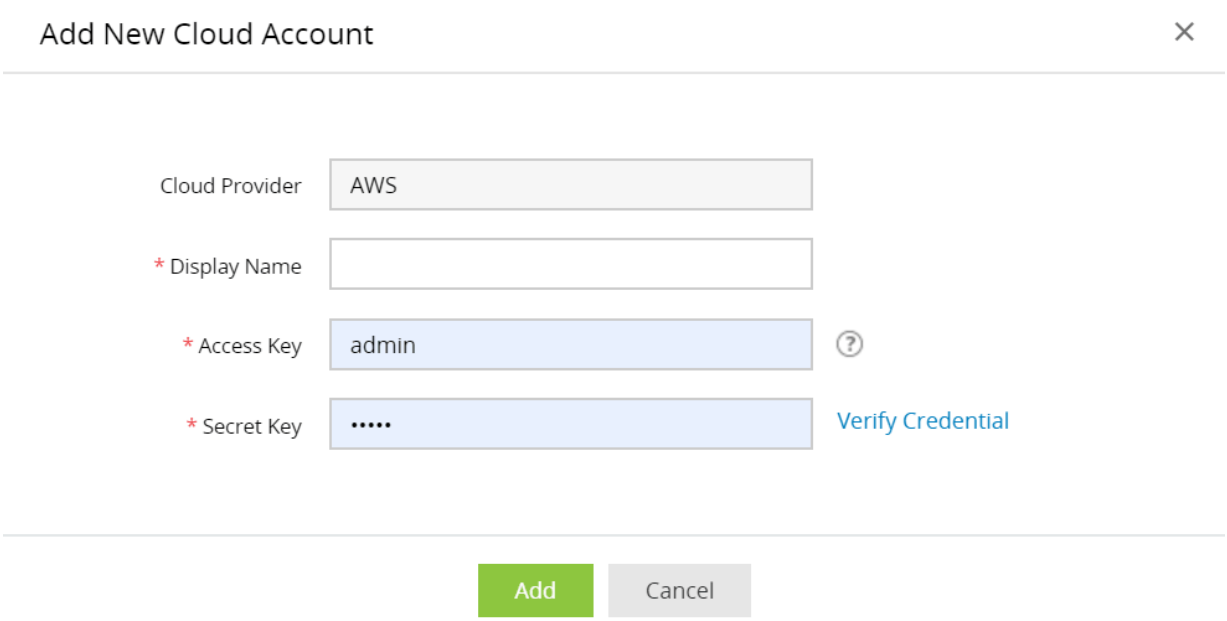
Log file import from cloud storage

To import logs from AWS S3 buckets, you first need to create an IAM user with access to the S3 bucket(s). You can also grant users access to only specific S3 buckets by following the steps given in this link.
To configure AWS S3 buckets for importing logs,

- In the Cloud tab, click the link displayed to configure the AWS account.



- Enter the Display Name, Access Key, and Secret Key of the AWS account and click Add.

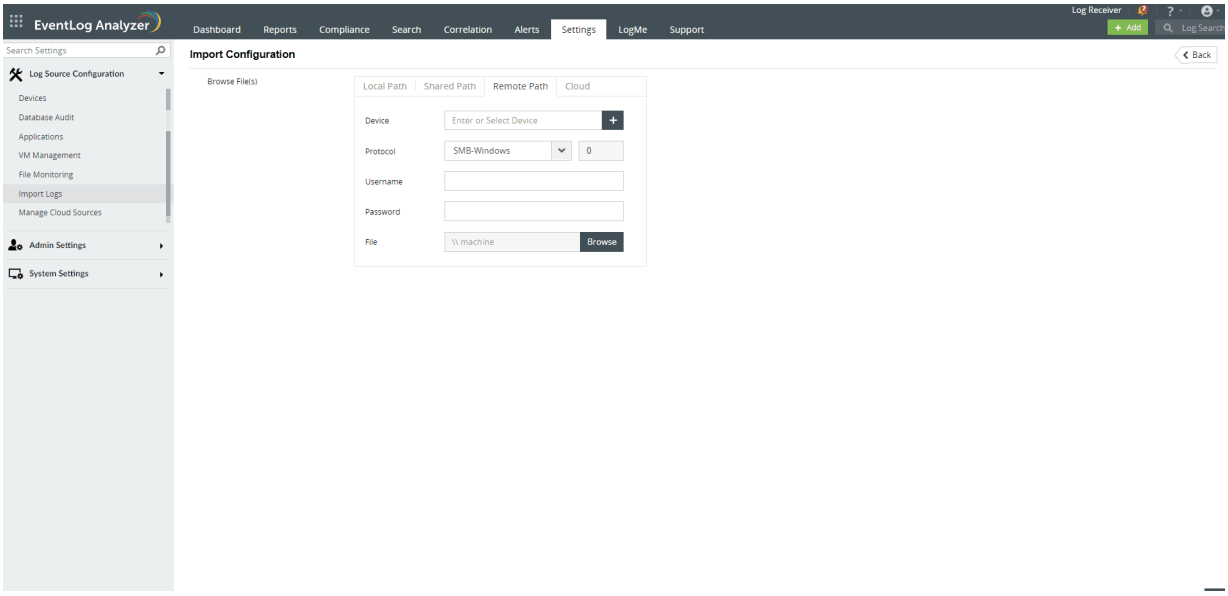


- Once the AWS account gets added, it will be displayed in the drop-down list available in the Cloud tab.
- From the drop-down list, select the AWS account and then the S3 bucket from which logs are to be imported.
- Click Import to initiate log importing.

Steps to create specific naming conventions for files

- Identify the log writing pattern from your application's log folder or from your application's configurations.
- In Eventlog Analyzer, navigate to Settings → Import Logs → + Import logs → Remote Path and fill in the required details.
- Browse the files and select the log file for which the log collection schedule has to be configured.
- The selected log file's naming should follow a pattern (date, time, or any pattern according to your needs) which will be replicated in the subsequent files created by the product.
- After selecting the log file, check the Schedule log import box and as well as the Specify filename pattern.
- Click Advanced Options. There will be a text box for every file which has been selected for the scheduled pattern import respectively.
- In the text box, input the filename pattern such that it matches the file name.

For example, consider an application which writes logs on a date-based schedule. Lets take the file name generated on Nov 22, 2023, as LOG_22_11_2023. Here the first part, "LOG_", will remain constant, and the latter part, i.e. the date "22_11_2023" changes daily. Keeping this in mind, select the pattern as "LOG_${DD}_${MM}_${YYYY}" from the drop down menus.
The drop down menu will provide multiple options to choose from as shown in the GIF below.



MySQL Logs

EventLog Analyzer supports only error logs and general logs from MySQL. MySQL logon failures are taken into account from MySQL general query logs.
To enable logging in MySQL,

- Open the my.cnf file (in case of Linux) or my.ini file (in case of Windows) and add the below entries to the file.
- For error logs: log_error=<error-log-file-name>

- For general logs:
  - >= v5.1.29:
    general_log_file=<general-log-file-name>
    general_log=1 (or) ON
  - < v5.1.29:
    log=<log-file-name>
- Restart the MySQL instance for the changes to take effect.

To import MySQL logs in EventLog Analyzer,

- You can import MySQL log files from a local path, a shared path , or a remote path.
- To import MySQL log files, you need to manually choose the log format. Once you've selected the right file, select MySQL Logs from the Log Format drop-down list in the Selected File(s) section.
- Click Import to initiate the log importing process.

PostgreSQL Logs

Log format of PostgreSQL logs is determined by log_line_prefix parameter, set in postgresql.conf file.
The default format of PostgreSQL logs is '%m [%p] ' which logs a time stamp and the process ID.
This format is supported by default in EventLog Analyzer.

Importing additional fields in EventLog Analyzer

If the user wants to add additional fields, log_line_prefix parameter in the postgresql.conf file must be changed.
The log_line_prefix parameter must follow the format(key- value pair) given below in the postgresql.conf file.

log_line_prefix format:

log_line_prefix = 'time_stamp=%m or %t process_id=%p application_name=%a database_name=%d connection_from_with_port=%r connection_from=%h session_id=%c transaction_id=%x user_name=%u command_tag=%i sql_state_code=%e session_start_time=%s '

log_line_prefix Parameter	Key	Value
Time stamp with milliseconds or time stamp without milliseconds	time_stamp	%m or %t
Process ID	process_id	%p
Application name	application_name	%a
Database name	database_name	%d

log_line_prefix Parameter	Key	Value
Remote host name or IP address, and remote port	connection_from_with_port	%r
Remote host name or IP address	connection_from	%h
Session ID	session_id	%c
Transaction ID	transaction_id	%x
User name	user_name	%u
Command tag: type of session's current command	command_tag	%i
SQLSTATE error code	sql_state_code	%e
Process start time stamp	session_start_time	%s

SAP ERP Audit Logs

To add the SAP ERP application for monitoring, the audit logs have to be enabled.
To enable the SAP ERP audit logs:
To the DEFAULT.PFL file in the location <SAP_installed path>\sys\profile, add

- rsau/enable = 1
- rsau/local/file = <log location>/audit_00

> Note The user should have permission to read this audit file while importing.

DHCP Logs

EventLog Analyzer can read and report on DHCP server software for Windows and Linux systems. It provides

various reports that simplifies network administration.
For Windows:

> Note Once you share the DHCP log location in Windows (i.e. %windir%\System32\Dhcp), you can automatically use this UNC path to fetch and import logs to EventLog Analyzer on a daily basis.

To configure, follow these steps:

1. Share the DHCP log folder.
2. Open EventLog Analyzer and go to Settings > Import Log > + Import Log > Shared\Remote path > browse the file and select DHCP Windows Log from the Log Format.
3. To learn how to import log files from different locations, refer here.

For Linux:
The default DHCP log location in Linux is "var/log/syslog" OR "var/log/messages" (for older versions).
If DHCP server logs are not available on the above files, please follow below steps. To store the DHCP server logs alone in a separate file, an admin would have to make changes to the following configuration files:

- /etc/dhcp/dhcpd.conf- DHCP Server configuration file
- /etc/rsyslog.conf- rsyslog configuration file

1. Lookup the value of "log-facility" in the dhcpd.conf file.
2. Lookup the log file path corresponding to the log-facility identified in the previous step in the ryslog.conf file. That is the DHCP server log file path.

To configure DHCP in EventLog Analyzer, follow these steps:

1. Share the DHCP log folder.
2. Open EventLog Analyzer and go to 'Settings' tab > Import Log > Shared\Remote path > browse the file.
3. To learn how to import log files from different locations, refer here.

DB2 Audit Logs

Db2 database systems allow auditing at both the instance and database levels. The db2audit tool is used to configure the auditing process. The tool can also be used to archive and extract audit logs, from both instance and database levels. The audit facility can be configured by following these six steps.

1. Configuring db2audit data path, archive path, and scope.
2. Creating an audit policy for database auditing.
3. Assigning the audit policy to the database.
4. Archiving the active logs.
5. Extracting the archived logs.
6. Importing the logs to EventLog Analyzer

6. Importing the logs to EventLog Analyzer.

EventLog Analyzer also supports diagnostic logs. Click here to learn how to generate the diagnostic logs report.

1. Configuring db2audit data path, archive path, and scope

The configure parameter modifies the db2audit.cfg configuration file in the instance's security subdirectory. All updates to this file will occur even when the instance is stopped. Updates occurring when the instance is active will dynamically affect the auditing being done by the Db2 instance. To know more on all possible actions on the configuration file, refer source

- Open DB2 Command Line Processor with administrator privilege.
- Run the following command:

> Note Replace the given paths with the paths of your choice for data path and archive path respectively.

- Run the following command:

> Note
>
> Replace the given parameters with the parameters of your choice.

- Run the following command:

Now the logs will be generated for the DB2 instance in the given data path.

2. Creating an audit policy for database auditing

- Open DB2 Command Line Processor with administrator privilege.
- Run the following command to connect to a database:

> Note Replace your_database with the database name of your choice.

- Run the following command to create an audit policy for the database:

> Note Replace policy_name with the policy name of your choice. Replace the given parameters with the command parameters of your choice. To know more on the allowed command parameters, refer source.

- Run the following command to commit:

Now the audit policy has been created.

3. Assigning the audit policy to the database

- Open DB2 Command Line Processor with administrator privilege.
- Run the following command to assign a policy to the database:

> Note Replace policy_name with the name of the audit policy that you created.

- Run the following command to commit:

Now the created audit policy is assigned to the database.

4. Archiving the active logs

You can archive the active logs from both instance and database. The logs will be archived to the archive path that you configured in the first step.

- Open DB2 Command Line Processor with administrator privilege.
- Run the following command to archive the active database logs:

> Note Replace your_database with the name of the database.

- Run the following command to archive active instance logs:

Now the logs will be archived to a new file with a timestamp appended to the filename. An example of the filename is given below.

- Instance Log file: db2audit.instance.log.0.20060418235612
- Database Log file: db2audit.db.your_database.log.0.20060418235612

Both files have to be extracted into a human-readable format to be imported into EventLog Analyzer.

5. Extracting the archived logs

- Open DB2 Command Line Processor with administrator privilege.
- Run the following command to extract the archived instance logs:

> Note Replace the instancelog with the filename of your choice. Replace db2audit.instance.log.0.20060418235612 with the filename of the archived instance logs.

- Run the following command to extract archived database logs:

> Note Replace databaselog with the filename of your choice. Replace db2audit.db.your_database.log.0.20060418235612 with the filename of the archived database logs.

Both files will be extracted to the given archive path and can be imported into EventLog Analyzer.

6. Importing the logs to EventLog Analyzer

Now you will have to import the extracted database and instance log files into EventLog Analyzer. Here is a comprehensive guide on how to import log files in EventLog Analyzer.

Diagnostic Logs

EventLog Analyzer also provides a report for diagnostic logs. To generate the diagnostic logs report, follow the given steps.

- Run the following command to find the location of the diagnostic log file.

or or

> Note The path corresponding to Current member resolved DIAGPATH is the path to the diagnostic log file.

- Navigate to the specified path and import the file named db2diag.txt to EventLog Analyzer. Here is a comprehensive guide on how to import log files in EventLog Analyzer.

Import Troubleshooting tips

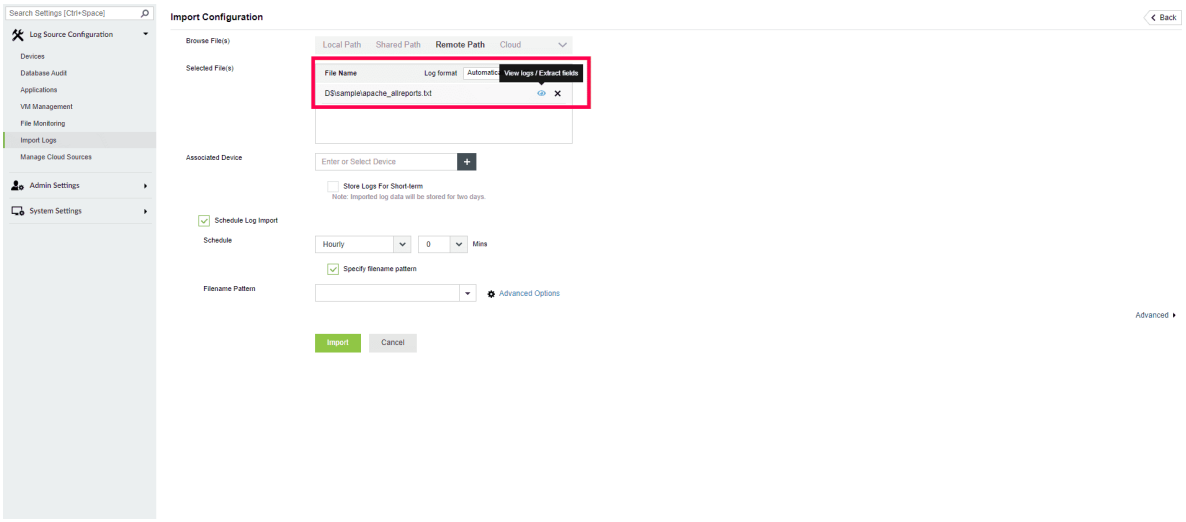
If you are unable to import a log file, ensure the following:

1. The credentials used are valid and have the necessary permissions.
2. The device is reachable.
3. The specified file exists and is accessible.
4. The log file format selected from the drop-down matches the log format of the chosen file.

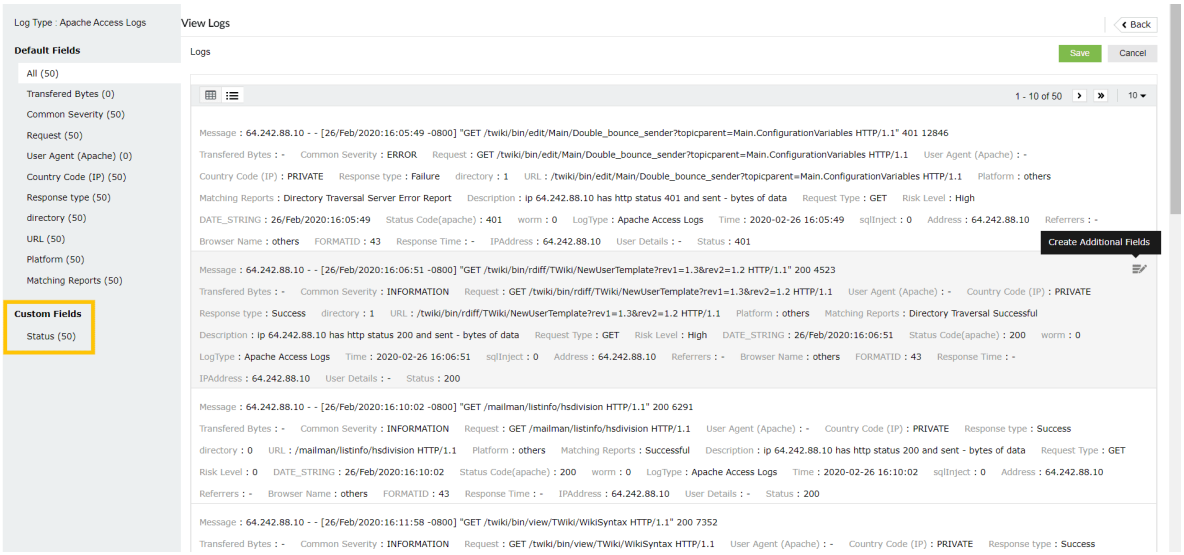
Field extraction from logs

- Navigate to the Import Configuration page.

- Select the desired file(s) from a local, shared or remote path.
- Under Selected files, click on the eye beside the required file.



- You can create a custom field by clicking on the tools icon at the top-right corner of your log message. Follow the steps given in this page to use custom patterns for logs.

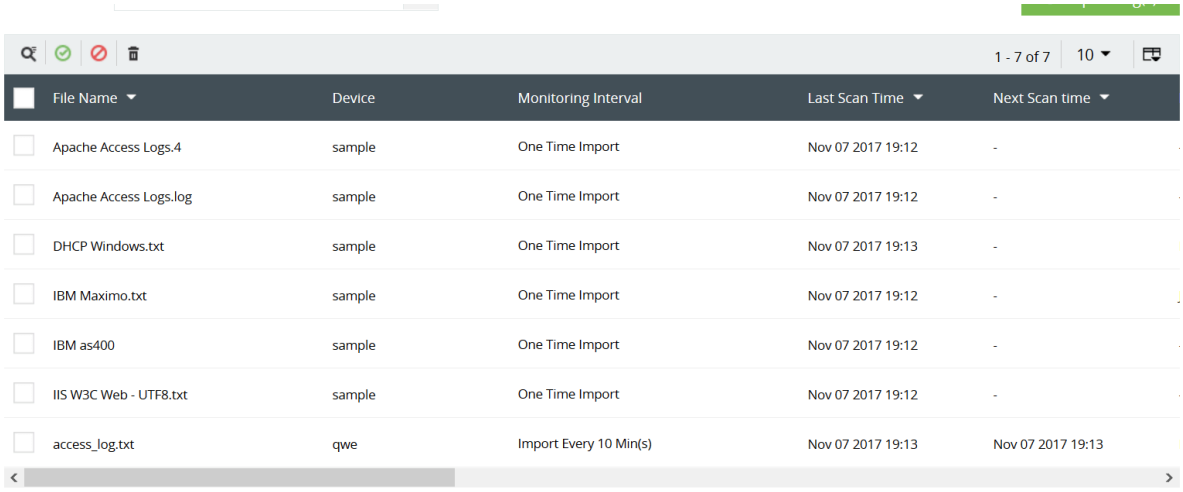


- You can see the created custom fields on the left pane.
- Finally, click Save.

List of imported log files

You can view a list of all imported log files in your EventLog Analyzer installation. This is the default page that appears when the import log option is selected. This page provides details of the imported log file including, filename, device, monitoring interval, time taken to import the log file, log format, and size of the log file.



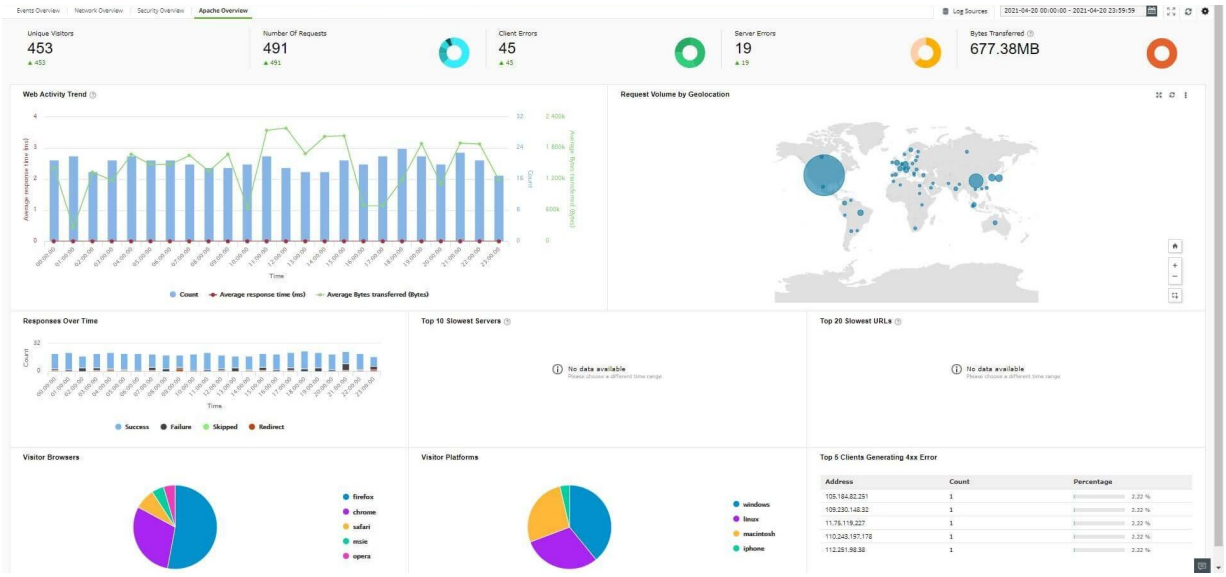


File Name	Device	Monitoring Interval	Last Scan Time	Next Scan time
Apache Access Logs.4	sample	One Time Import	Nov 07 2017 19:12	-
Apache Access Logs.log	sample	One Time Import	Nov 07 2017 19:12	-
DHCP Windows.txt	sample	One Time Import	Nov 07 2017 19:13	-
IBM Maximo.txt	sample	One Time Import	Nov 07 2017 19:12	-
IBM as400	sample	One Time Import	Nov 07 2017 19:12	-
IIS W3C Web - UTF8.txt	sample	One Time Import	Nov 07 2017 19:12	-
access_log.txt	qwe	Import Every 10 Min(s)	Nov 07 2017 19:13	Nov 07 2017 19:13

Apache Overview Dashboard: Parsing Additional fields by modifying the log format

The Combined Log Format is one of the log formats commonly used with Apache logs.
The Combined Log format is:
While importing the log files in the Combined log format, the log files will not include the values for the fields response time and bytes received.
The following widgets in the Apache Overview dashboard can display their values accurately only if the response time and bytes received fields are parsed.

1. Bytes Transferred
2. Top 20 Slowest URLs
3. Web Activity Trend
4. Top 10 Slowest Servers



In order to parse these additional fields, the log format has to be modified. The values for the additional fields can be obtained once the logs are configured with the parameters "%{ms}T" and "%I".

Eventlog Analyzer can parse the modified log format by default.
The modified log format containing the parameters for response time and bytes received is:
%{ms}T - time taken to serve the request (in milliseconds) %I - bytes received, including headers

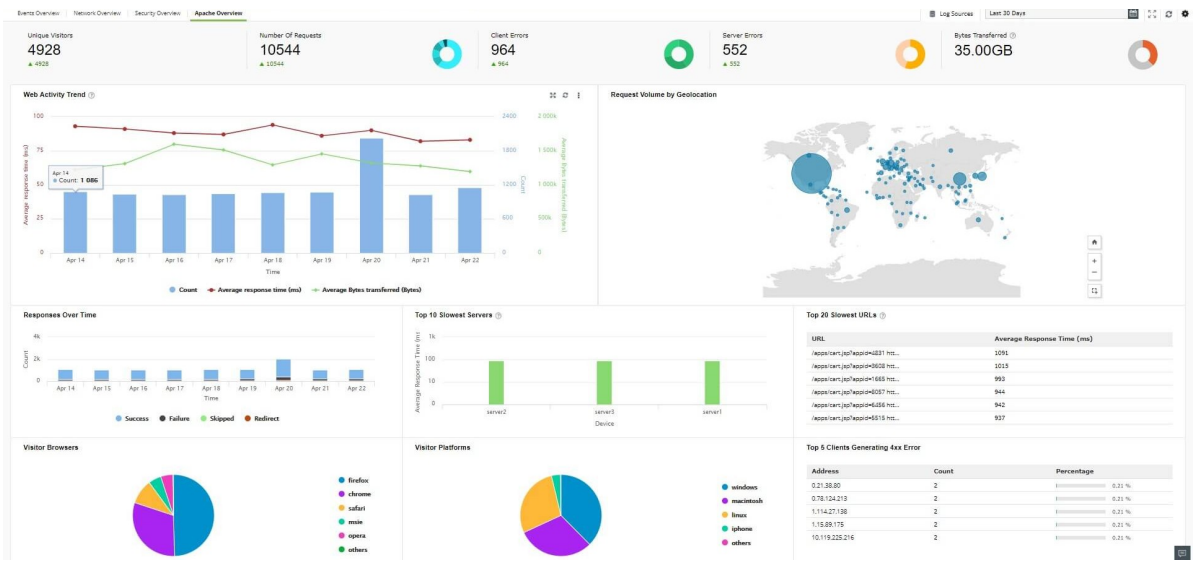
> Note Requires modlog_io to be enabled https://httpd.apache.org/docs/2.4/mod/mod_logio.html

The modified log has 2 directives in addition to the commonly used Combined Log Format. These directives are present at the end of the format, therefore, the combined log format will continue to be parsed as it was parsed in the previous versions.

Procedure to change the Apache log format

> Note The configuration files by default are located at /etc/apache2/ in Debian/Ubuntu/Linux Mint or, /etc/httpd/conf on Red Hat/Fedora/CentOS

1. Define a new log format and assign a label to it.
2. The label can be used to reference the new format string as the customLog directive.
3. The new format will go into effect when the webserver is restarted.
   After the log files have been imported, the updated Apache Overview dashboard has been displayed below:



7.11.1. Configuring the Syslog Service on VMware

Last updated on: September 12, 2025

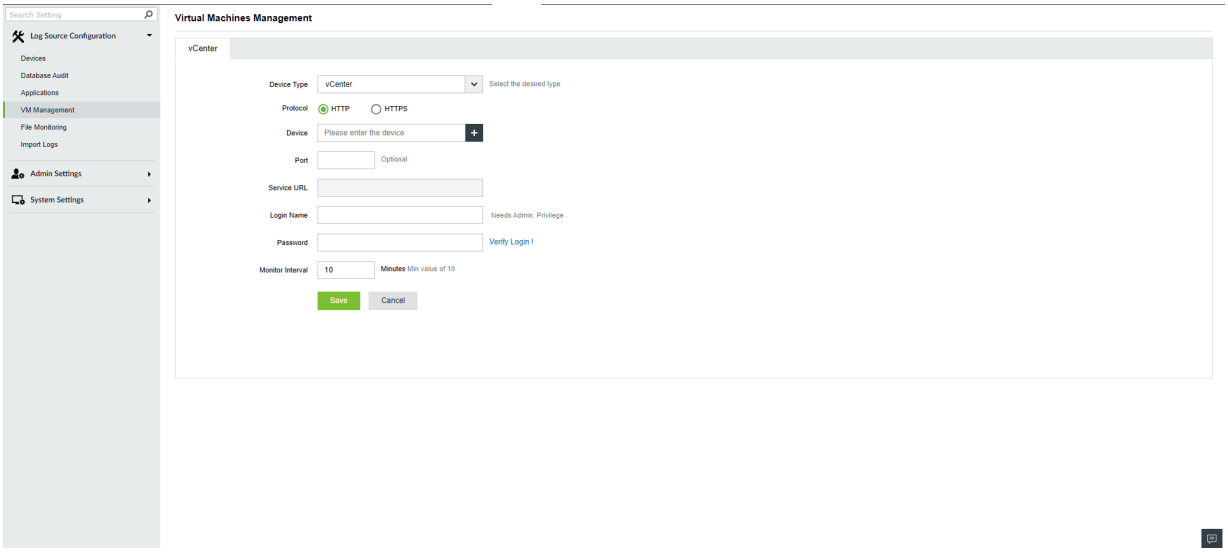
All ESX and ESXi devices run a syslog service (syslogd), which logs messages from the VMkernel and other system components to a file.
To configure the syslog service on an ESX device::
Neither vSphere Client nor vicfg-syslog can be used to configure syslog behavior for an ESX device. To configure syslog for an ESX device, you must edit the /etc/syslog.conf file.
To configure the syslog service on an ESXi device:

1. On ESXi devices, you can use the vSphere Client or the vSphere CLI command vicfg-syslog to configure the following options:
   - Log file path: Specifies a datastore path to the file where syslogd logs all messages.
   - Remote host: Specifies a remote device to which syslog messages are forwarded. In order to receive the forwarded syslog messages, your remote host must have a syslog service installed.
   - Remote port: Specifies the port used by the remote host to receive syslog messages.
2. Configuration using vSphere CLI command: For more information on vicfg-syslog, refer the vSphere Command-Line Interface Installation and Reference Guide.
3. Configuration using vSphere Client:
   - In the vSphere Client inventory, click on the host.
   - Click the Configuration tab.
   - Click Advanced Settings under Software.
   - Select Syslog in the tree control.
   - In the Syslog.Local.DatastorePath text box, enter the datastore path to the file where syslog will log messages. If no path is specified, the default path is /var/log/messages.
     The datastore path format is [<datastorename>] </path/to/file> where the path is relative to the root of the volume backing the datastore.
     Example: The datastore path [storage1] var/log/messages maps to the path / vmfs/volumes/storage1/var/log/messages.
   - In the Syslog.Remote.Devicename text box, enter the name of the remote host where syslog data will be forwarded. If no value is specified, no data is forwarded.
   - In the Syslog.Remote.Port text box, enter the port on the remote host where syslog data will be forwarded. By default Syslog.Remote.Port is set to 514, the default UDP port used by syslog. Changes to Syslog.Remote.Port only take effect if Syslog.Remote.Devicename is configured.
   - Click OK.

7.11.2. Adding vCenter

Last updated on: September 12, 2025

The vCenter servers to be monitored by EventLog Analyzer can be added by navigating to Settings > Log Source Configuration > VM Management and using the Add vCenter button. You can also view and manage the vCenter servers that are being monitored.



7.12.1. Exporting data from vulnerability scanners

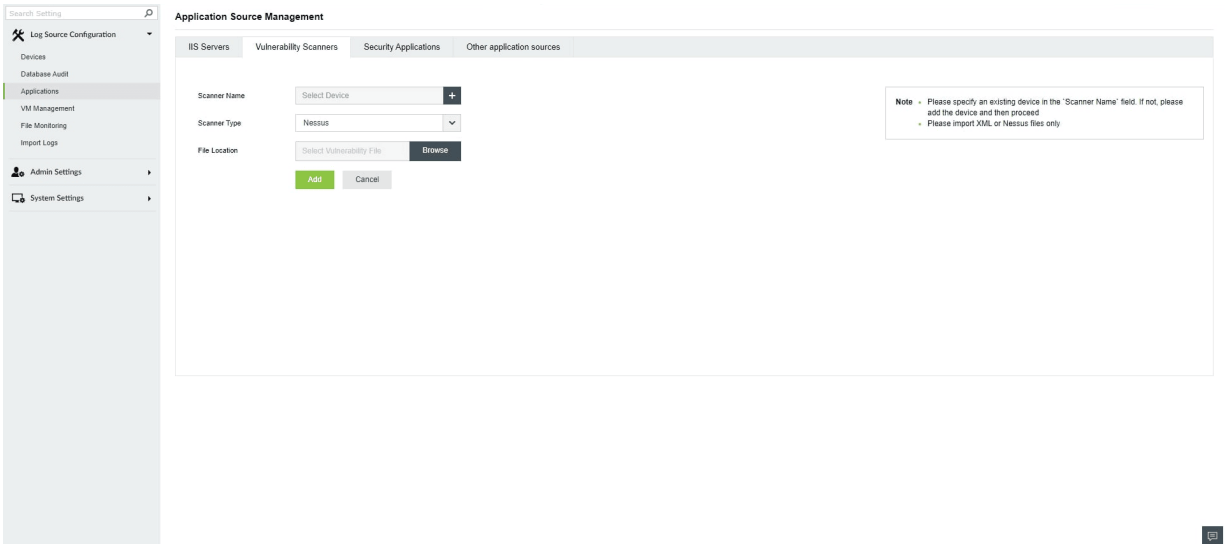
Last updated on: September 12, 2025

EventLog Analyzer analyses data from vulnerability scanners and provides insights to help identify vulnerabilities within the network. For this you need to export data from the respective vulnerability scanners and then import it to EventLog Analyzer. You can export the data by following the steps below

1. Select a scan under Scans Tab.
2. In the upper-right corner, click Export
3. From the drop-down box, select Nessus.

Adding vulnerability scanners to EventLog Analyzer

To monitor vulnerability scanner data in EventLog Analyzer, you need to import the corresponding log data to the EventLog Analyzer server. You can import log data by navigating to Settings > Vulnerability Data Analysis > Import.

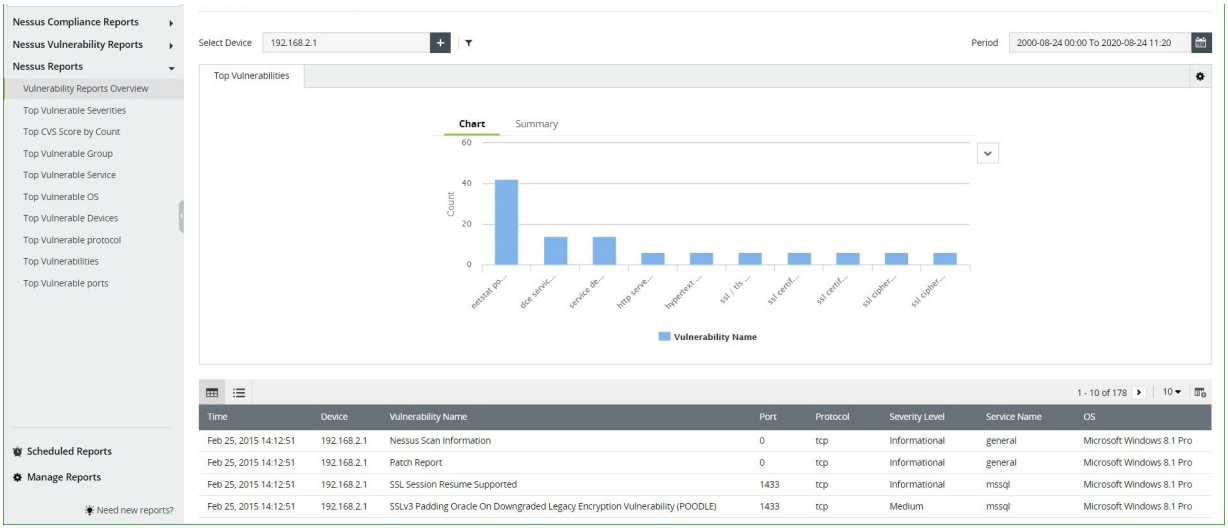


1. Enter the vulnerability scanner's name.
2. Choose the vulnerability scanner's application type.
3. Specify the location of the log file which has to be imported.
4. Click on Import.

Reports on Nessus vulnerability data

The information on potential vulnerabilities in a network including credential failures, elevated privilege failures, registry access failures gathered from Nessus are provided as reports. The information in the reports is also presented in the graphical format for improved insights.





Available reports:

- GHOST in Linux - This report lists any detected instance of the GHOST vulnerability in Linux.
- Shellshock Report - This report contains information on the detected instances of the Shellshock privilege escalation vulnerability in Linux systems in your network.
- Admin Discovery Report - An overview of all the admin accounts in a network will be available in this report.
- Top exploitable vulnerabilities - An overview of the vulnerabilities in your network that are most prone to attacks will be available here.
- Credential failures report - An account of all instances of credential failures in your network will be displayed here.
- Elevated privilege failures report - Failed attempts at privilege escalation will be displayed here.
- Registry access failures - Failed attempts at accessing the Windows Registry will be recorded here.
- Patch report - A report of all the patches applied in the device will be displayed.
- Overall Nessus report - An overview of events in Nessus vulnerabilty scanners in your network will be available here.

Ensuring Compliance to regulatory mandates:

EventLog Analyzer helps in complying with regulatory mandates such as the GDPR, PCI DSS and NIST. These regulations mandate that critical events in devices and applications that could potentially lead to a data breach need to be monitored. If any indication of a breach is detected, remediating action has to be taken to mitigate this risk. Information from vulnerability scanners like Nessus form a critical part of the data that needs to be monitored.

For instance, the risk assessment (ID.RA) section of NIST compliance that states,

"The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. Threat and vulnerability information is received from information sharing forums and sources."

The data from vulnerability scanners that can be used to ensure compliance to regulations are also categorized according to the device types, in EventLog Analyzer. The solution categorizes the reports as follows based on

the devices' data that Nessus analyzes.

- Windows devices
- Unix devices
- Databases
- Cisco IOS
- Huawei
- Unix file contents
- IBM iSeries
- SonicWall, SonicOS
- Citrix XenServer
- VMware, nessus, and vSphere infrastructure

Once the Nessus vulnerability scanner is added, this data from Nessus can be manually imported into EventLog Analyzer or automated imports can be scheduled. This data is then collated into comprehensive reports to comply with PCI DSS requirements.

- Denial of remote access software
- Denial of insecure communication
- Handling false positives

7.12.2. Exporting data from vulnerability scanners

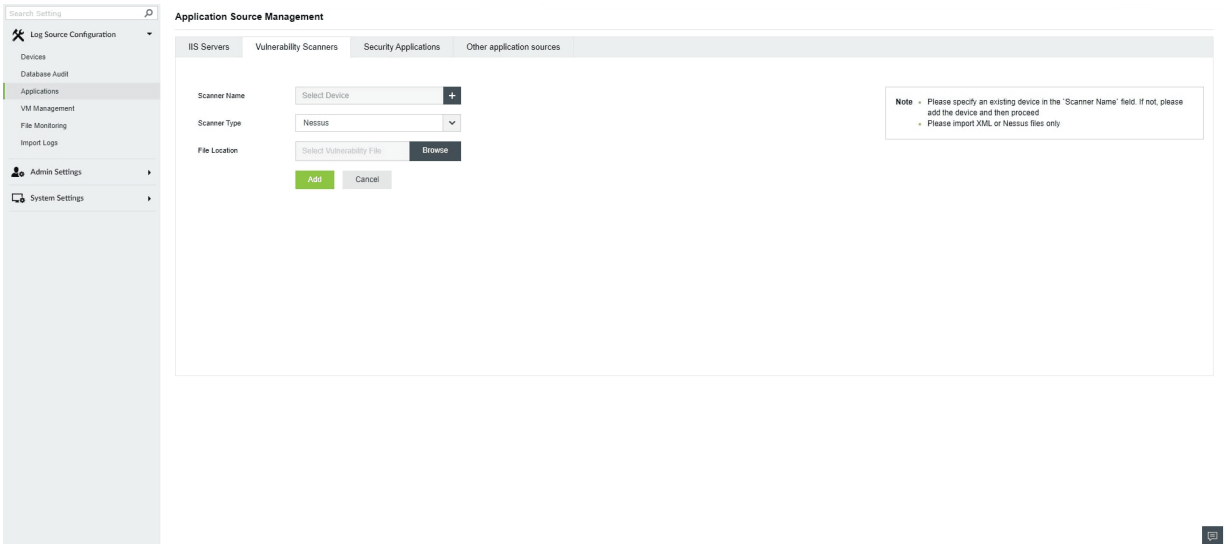
Last updated on: September 12, 2025

EventLog Analyzer analyses data from vulnerability scanners and provides insights to help identify vulnerabilities within the network. For this you need to export data from the respective vulnerability scanners and then import it to EventLog Analyzer. You can export the data by following the steps below:

1. Go to the Scan menu and select the scan that you want to save.
2. Click Save Scan.
3. In the Save dialog box, choose the format as Nmap XML format

Adding vulnerability scanners to EventLog Analyzer

To monitor vulnerability scanner data in EventLog Analyzer, you need to import the corresponding log data to the EventLog Analyzer server. You can import log data by navigating to Settings > Vulnerability Data Analysis > Import.



1. Enter the vulnerability scanner's name.
2. Choose the vulnerability scanner's application type.
3. Specify the location of the log file which has to be imported.
4. Click on Import.

7.12.3. Exporting data from vulnerability scanners

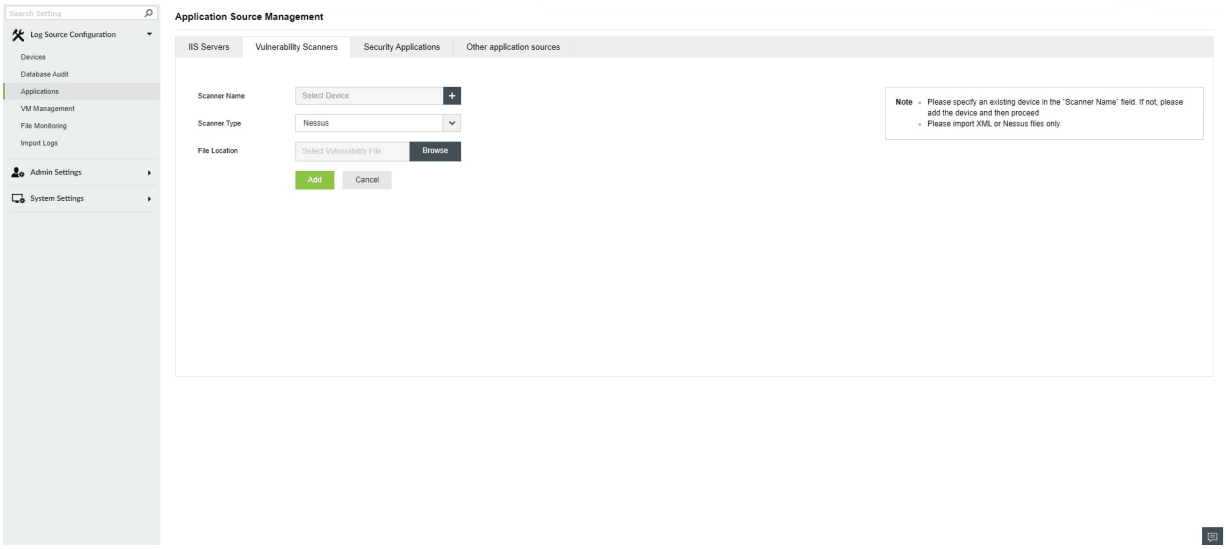
Last updated on: September 12, 2025

EventLog Analyzer analyses data from vulnerability scanners and provides insights to help identify vulnerabilities within the network. For this you need to export data from the respective vulnerability scanners and then import it to EventLog Analyzer. You can export the data by following the steps given below:

1. Click the Reports icon.
2. Under the Create a report tab select Export.
3. Select XML Export or XML Export 2.0.
4. Add the site and then click Save and run report.

Adding vulnerability scanners to EventLog Analyzer

To monitor vulnerability scanner data in EventLog Analyzer, you need to import the corresponding log data to the EventLog Analyzer server. You can import log data by navigating to Settings > Vulnerability Data Analysis > Import.



1. Enter the vulnerability scanner's name.
2. Choose the vulnerability scanner's application type.
3. Specify the location of the log file which has to be imported.
4. Click on Import.

7.12.4. Exporting data from vulnerability scanners

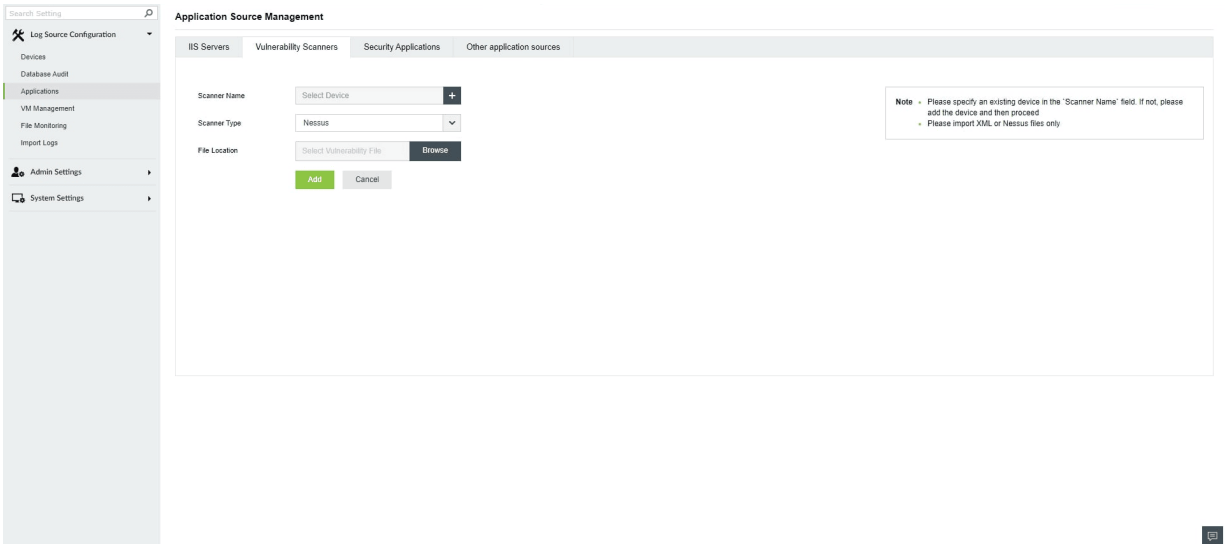
Last updated on: September 12, 2025

EventLog Analyzer analyses data from vulnerability scanners and provides insights to help identify vulnerabilities within the network. For this you need to export data from the respective vulnerability scanners and then import it to EventLog Analyzer. You can export the data by following the steps given for each of the vulnerability scanners.

1. Under the Scans menu, select Vulnerabilities
2. If there is no Vulnerabilities tab, choose Results.
3. Click Export page contents from the bottom right corner.

Adding vulnerability scanners to EventLog Analyzer

To monitor vulnerability scanner data in EventLog Analyzer, you need to import the corresponding log data to the EventLog Analyzer server. You can import log data by navigating to Settings > Vulnerability Data Analysis > Import.



1. Enter the vulnerability scanner's name.
2. Choose the vulnerability scanner's application type.
3. Specify the location of the log file which has to be imported.
4. Click on Import.

7.12.5. Exporting data from vulnerability scanners

Last updated on: September 12, 2025

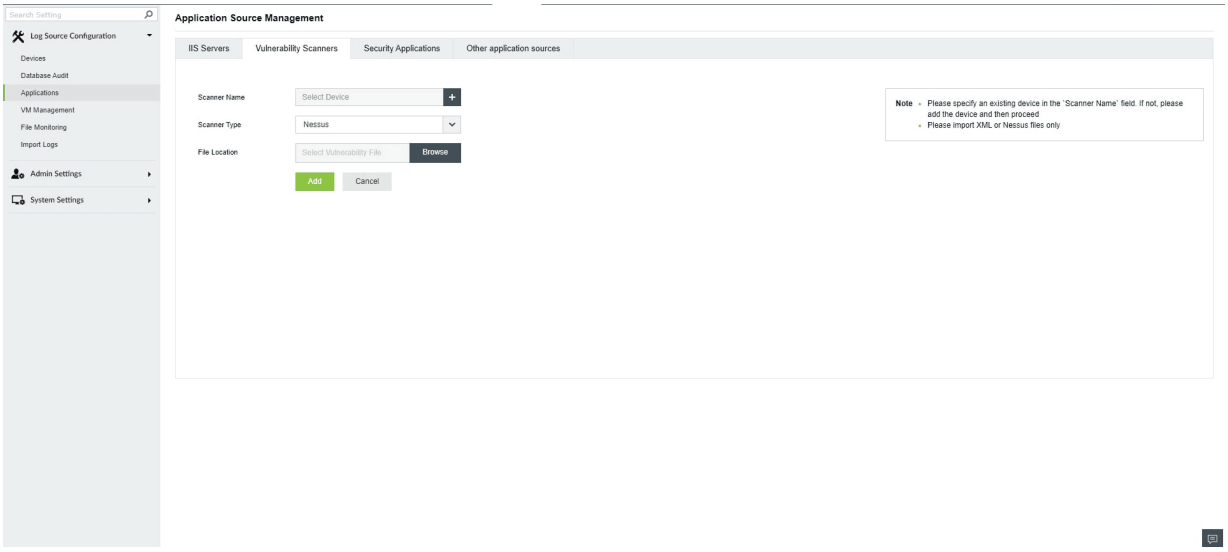
EventLog Analyzer analyses data from vulnerability scanners and provides insights to help identify vulnerabilities within the network. For this you need to export data from the respective vulnerability scanners and then import it to EventLog Analyzer. You can export the data by following the steps given fbelow:

1. Go to the Scans menu in the dashboard.
2. Right-click the scan report that you need to export.
3. Select Download from the Quick Actions menu.
4. Select Download Format as Extensible Markup Language(XML).

Once you have exported the data from the corresponding scanners, you need to import the log data to the EventLog Analyzer server.

Adding vulnerability scanners to EventLog Analyzer

To monitor vulnerability scanner data in EventLog Analyzer, you need to import the corresponding log data to the EventLog Analyzer server. You can import log data by navigating to Settings > Vulnerability Data Analysis > Import.



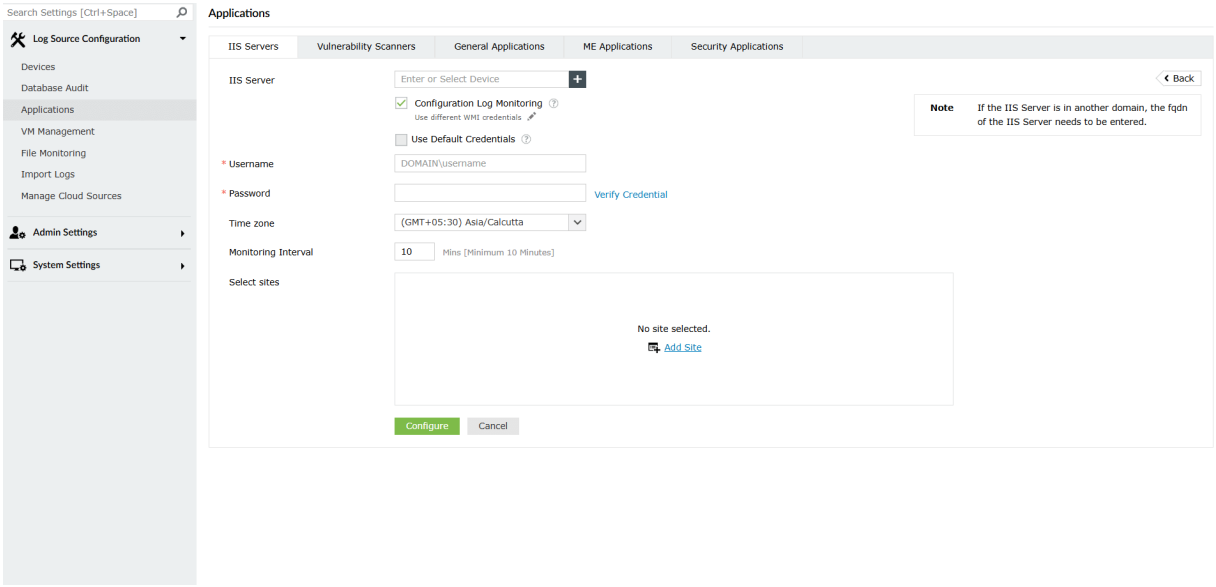
1. Enter the vulnerability scanner's name.
2. Choose the vulnerability scanner's application type.
3. Specify the location of the log file which has to be imported.
4. Click on Import.

7.13.1. Adding an IIS server

Last updated on: September 12, 2025

Prerequisite for adding an IIS server

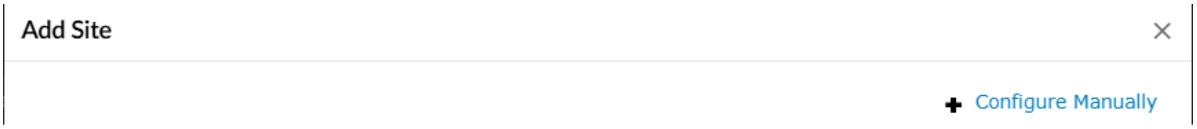
When configuring IIS log source in EventLog Analyzer for the first time, administrative privileges are required. (Administrator shares privileges are required eg : Admin$,c$)

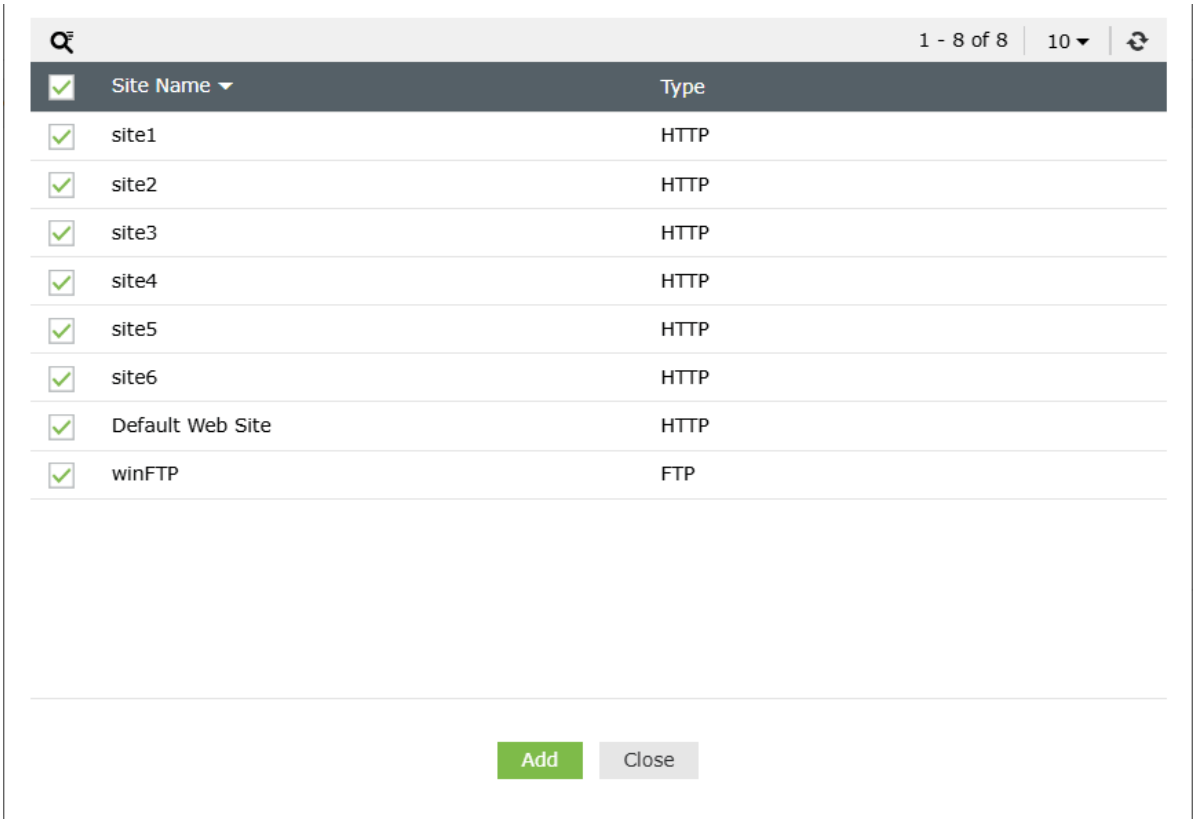


1. Navigate to Settings > Log Source Configuration > Applications.
2. In the Application Source Management page, click the + Add IIS server button.
3. Click the + icon to browse and add IIS servers.
4. If you wish to configure log collection, select the check box Configuration Log Monitoring.
5. You can choose to use default credentials, or enter the Username and Password for the IIS Server in the credentials field.
6. Select the Time Zone from the dropdown menu and enter the desired Monitoring Interval.

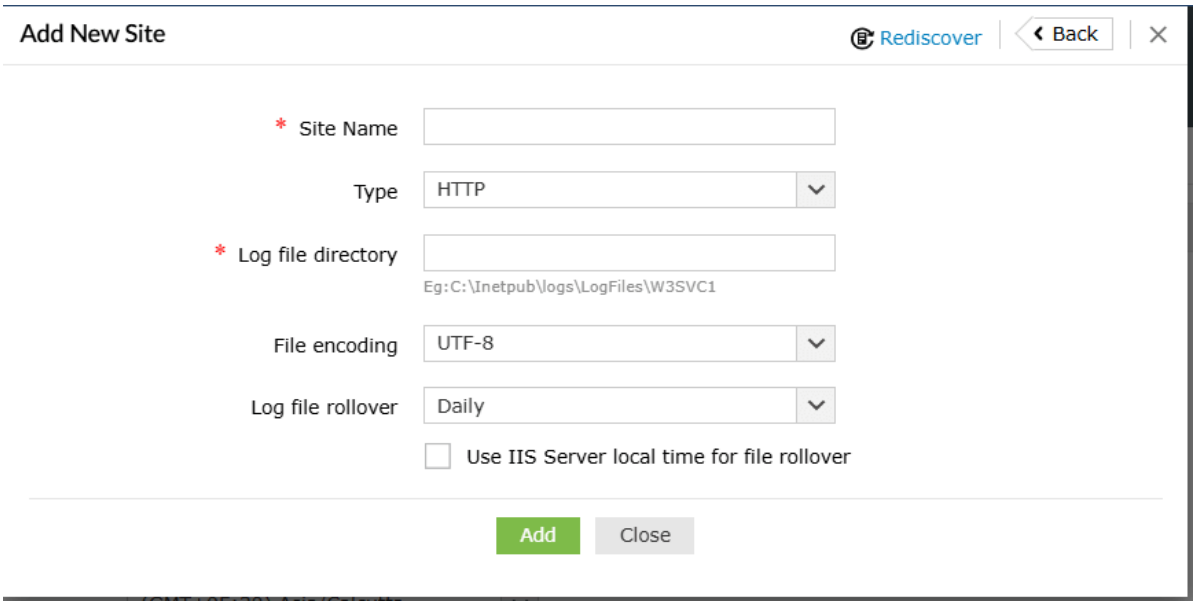
> **Note**
>
> The time-zone selected must be the same as that of the IIS server. Also, EventLog Analyzer uses port 445 (TCP) to read IIS log files using the Server Message Block (SMB) protocol.

7. You can use separate credentials for configuring log collection.
8. Click on + Add Sites. From the list of discovered sites, choose the sites you wish to monitor





Alternatively, you can manually add a site by entering the site name, protocol, and log file path in the pop-up that appears. Choose the file encoding scheme and schedule the log file rollover.



Click Add and then Configure to start monitoring the site.

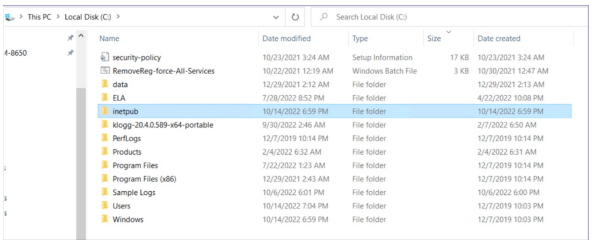
> **Note**
>
> Once the initial configuration is complete, the account can be modified to be used as a service account.

Configuring an IIS site for non-admin users

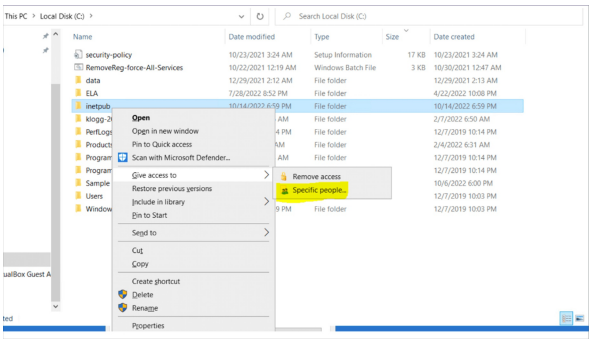
> **Note**
>
> Any Configuration Changes made in IIS Manager will not be synced on next scheduling if non admin credentials is used

Steps to configure the IIS site in EventLog Analyzer for non-admin users:

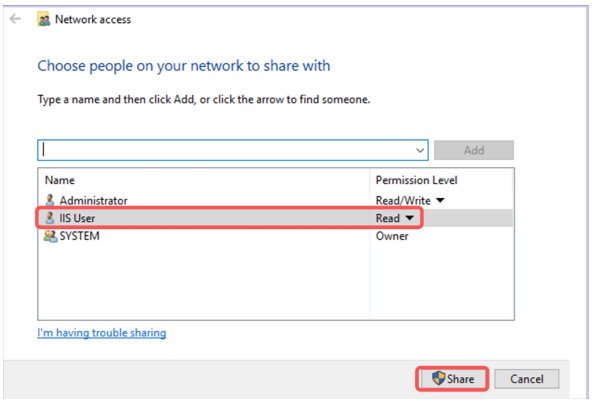
1. In the IIS server, navigate to the C directory (Note: The default location may vary)



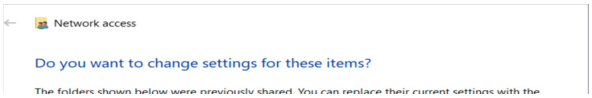
2. Right-click inetpub and select Give access to → Specific people.

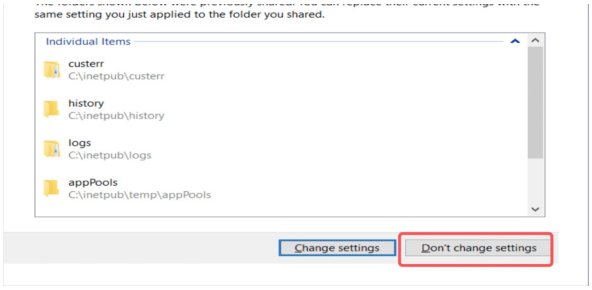


3. Add the service account user with read permission level and click on Share

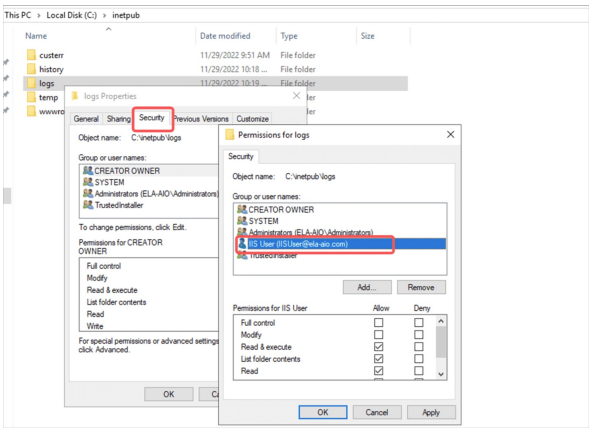


4. If the pop-up occurs, click on Don't change settings.



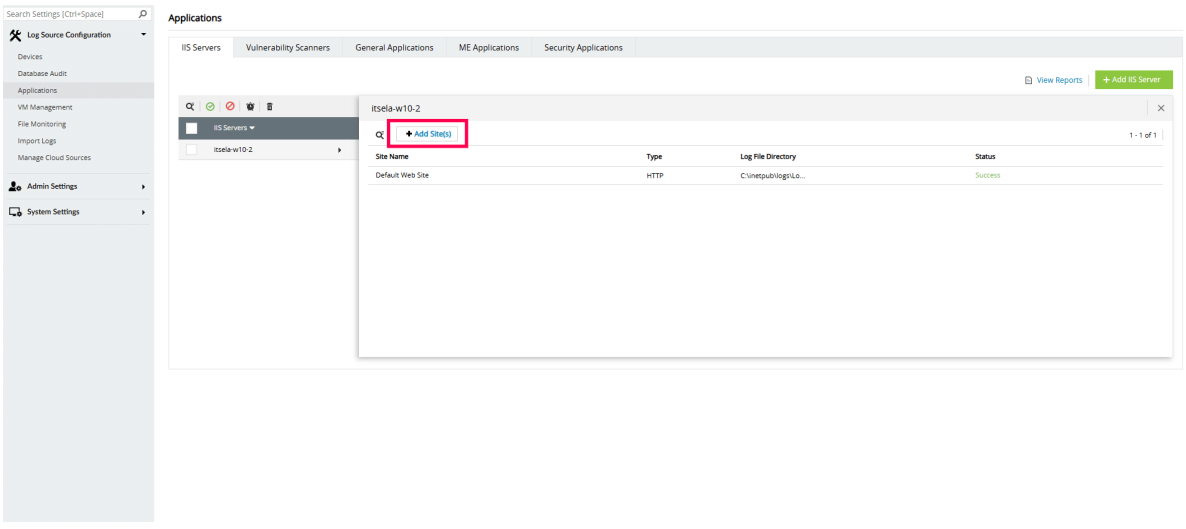


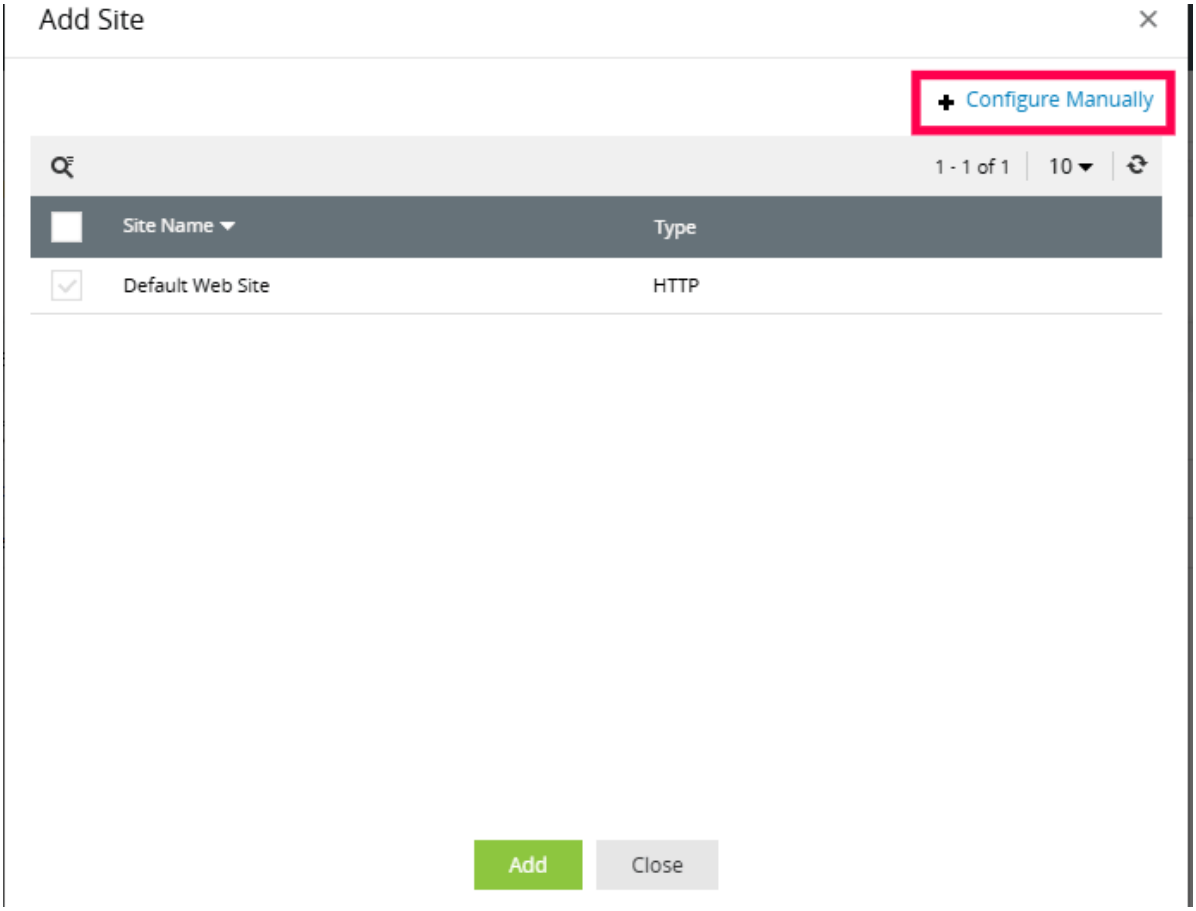
5. Navigate to inetpub → logs → properties → Security → add the service account with read access permission. (Note: The default location may vary)



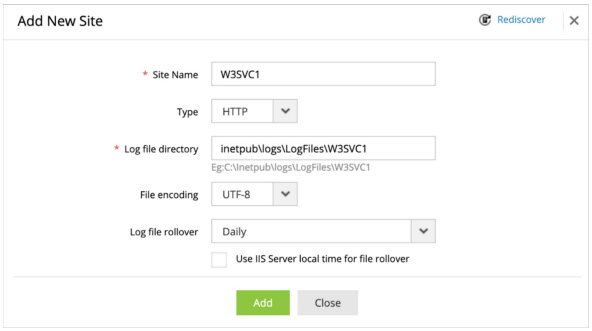
> **Note**
>
> Ensure that both the main folder (inetpub) and only the folder and sub-folder with the logs have the required permissions for the service account, as sometimes only the main folder gets the necessary privileges.

6. Navigate to EventLog Analyzer console → Settings → Application → IIS site, Enter the Username and password of service account (Do not verify the credentials - when you do it will display verification failed) > Add site





7. Enter the IIS site name, path → Add and configure

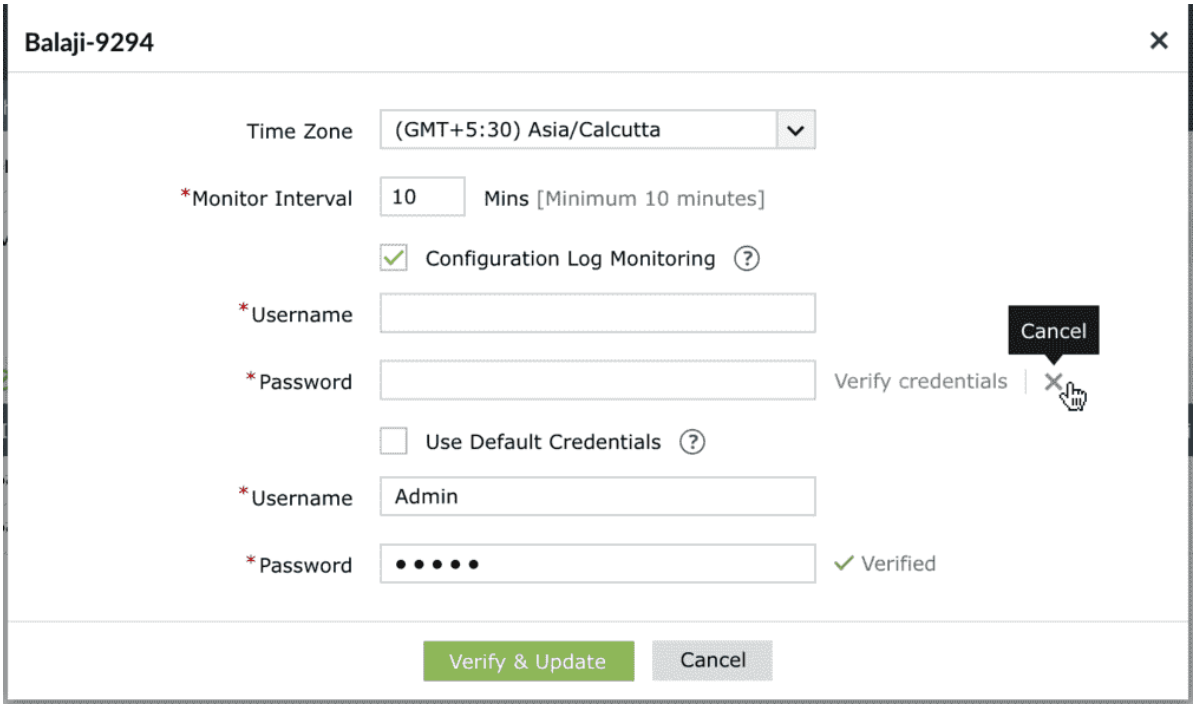


IIS Configuration Change Logs

Configuration change logs are collected in the IIS similar to how logs are collected for Windows. These logs are collected through the Microsoft-IIS-Configuration/Operational event source file.

Troubleshooting steps:

1. Ensure that configuration log has been successfully configured. If not, you must configure it.
2. The device that has been configured must be enabled. This can be done in the Manage Devices tab.
3. Ensure that the Microsoft-IIS-Configuration/Operational option is enabled in the configure event source file for the device. This option can be enabled in the Manage Devices tab.
4. The Configuration log monitoring credential provided must have the WMI access.


Balaji-9294
Time Zone
(GMT+5:30) Asia/Calcutta
*Monitor Interval
10
Mins [Minimum 10 minutes]
Configuration Log Monitoring
*Username
*Password
Cancel
Verify credentials
Use Default Credentials
*Username
Admin
*Password
Verified
Verify & Update
Cancel

7.14.1.1. Microsoft 365

Last updated on: September 12, 2025

In this page

Overview

Key functionalities

Overview

Log360 provides centralized visibility into user activities, administrative actions, and security events across Microsoft 365. It collects audit logs from services such as Microsoft Entra ID, Exchange Online, SharePoint Online, M365 General (including Teams, OneDrive, and other M365 services), and Exchange MailTrace, consolidating them into a single platform for monitoring, analysis, and compliance.

Organizations can monitor critical activities such as user sign-ins, mailbox access, file sharing, and collaboration. Reports provide insights from all Microsoft 365 sources, including Entra ID, Exchange Online, SharePoint, OneDrive, and Microsoft Teams, covering mailbox traffic, spam and malware incidents, inactive users, and soon-to-expire licenses, etc. The product console also offers compliance reports for these services to help organizations meet regulatory standards such as HIPAA, SOX, and PCI-DSS.

Administrators can also configure alerts to receive notifications about important activities, define which mailboxes to monitor for unusual behavior, and get detailed information on the actions triggering each alert. By combining reporting, alerting, and management into a unified workflow, the product helps organizations maintain security, simplify investigations, and ensure compliance across their Microsoft 365 environment.

Key functionalities

- Track critical activity: Gain visibility into user sign-ins, mailbox access, file sharing, and collaboration across Microsoft 365 services to monitor day-to-day operations.
- Detect suspicious behavior: Identify unusual patterns such as Login from an anonymized IP address, role changes, or unauthorized changes to mailbox permissions.
- Strengthen compliance posture: Securely retain audit logs and generate detailed reports to support compliance with IT regulations and standards.
- Accelerate incident analysis: Use consolidated logs, reports, and real-time alerts to analyze and respond to incidents.
- Object synchronization and filtering: Sync Active Directory objects such as users, groups, and service principals using object filters. The synced data show details of the entity (user or service principal) that initiated the action in the Incident Workbench and used in the Rules module for log enrichment.

Read also

This document explains managing, reporting, and alerting for Microsoft 365 tenants using the product console and its key functionalities. To set up and manage Microsoft 365 tenants, see the articles below:

- Tenant configuration

- Tenant configuration
- Adding data source
- Managing M365 accounts

7.14.1.2. Adding data source

Last updated on: September 12, 2025

In this page

Overview

Steps to add a data source

Overview

This page explains how to add Microsoft 365 services as data sources in the product console after configuring a tenant. Once the tenant is configured, you can select the account and add any of the following services as data sources to enable log collection: Exchange Online, SharePoint Online, M365 General, and Exchange MailTrace.

Steps to add a data source

1. In your product console, navigate to the Settings tab.
2. Under Log Configuration, select Manage Cloud Sources.

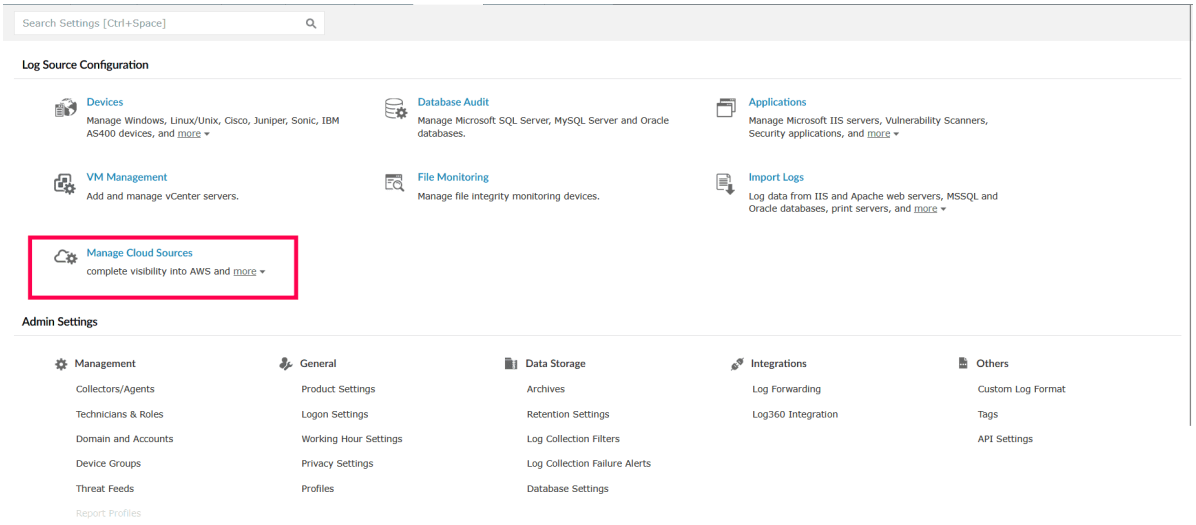


Figure 1: Navigating to Manage Cloud Sources

3. On the Manage Cloud Sources page, click Add Data Source in the top-right corner.

> NOTE
>
> Microsoft Entra ID will be added as a data source by default.

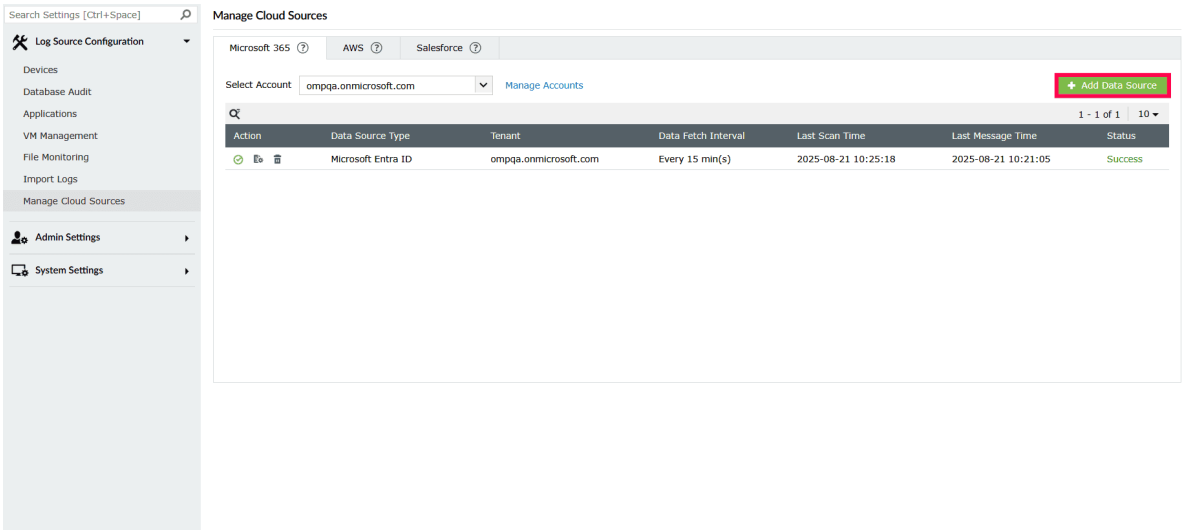


Figure 2: Adding a data source

4. In the Add Data Source window, select an account from the Select Account drop-down.

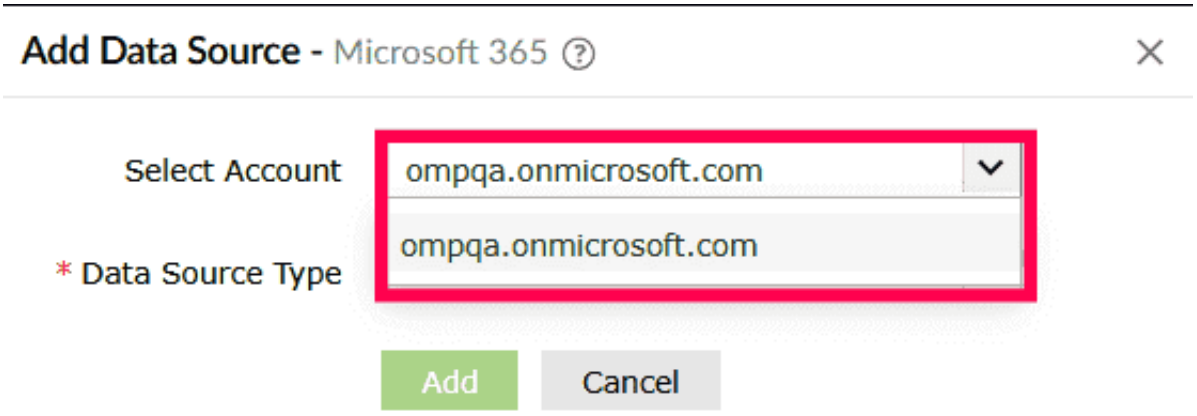
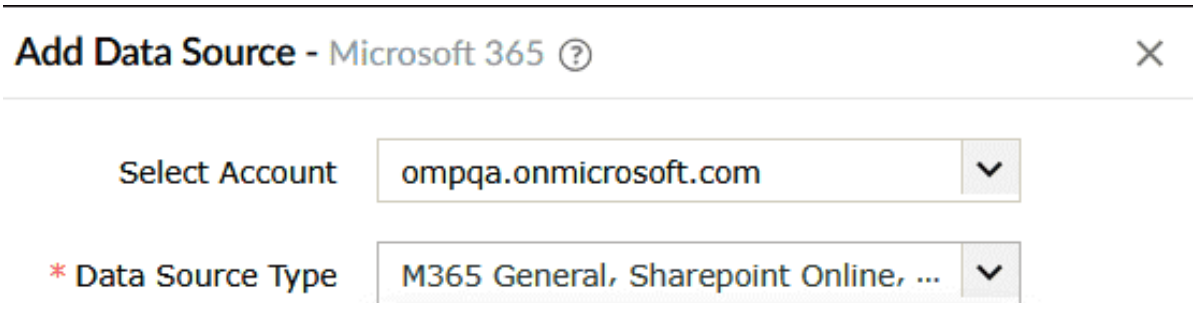


Figure 3: Selecting an account

5. From the Data Source Type drop-down, choose the Microsoft 365 service(s) you want to add.

> NOTE
>
> You can add one or more services at a time. The available options are: Microsoft Entra ID, Exchange Online, SharePoint Online, M365 General, and Exchange MailTrace.



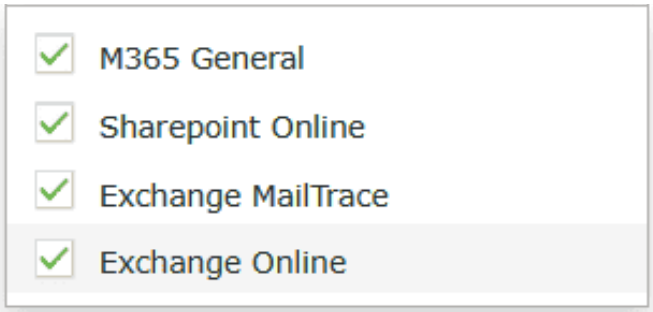


Figure 4: Selecting data source types

6. Click Add to add the selected data sources.

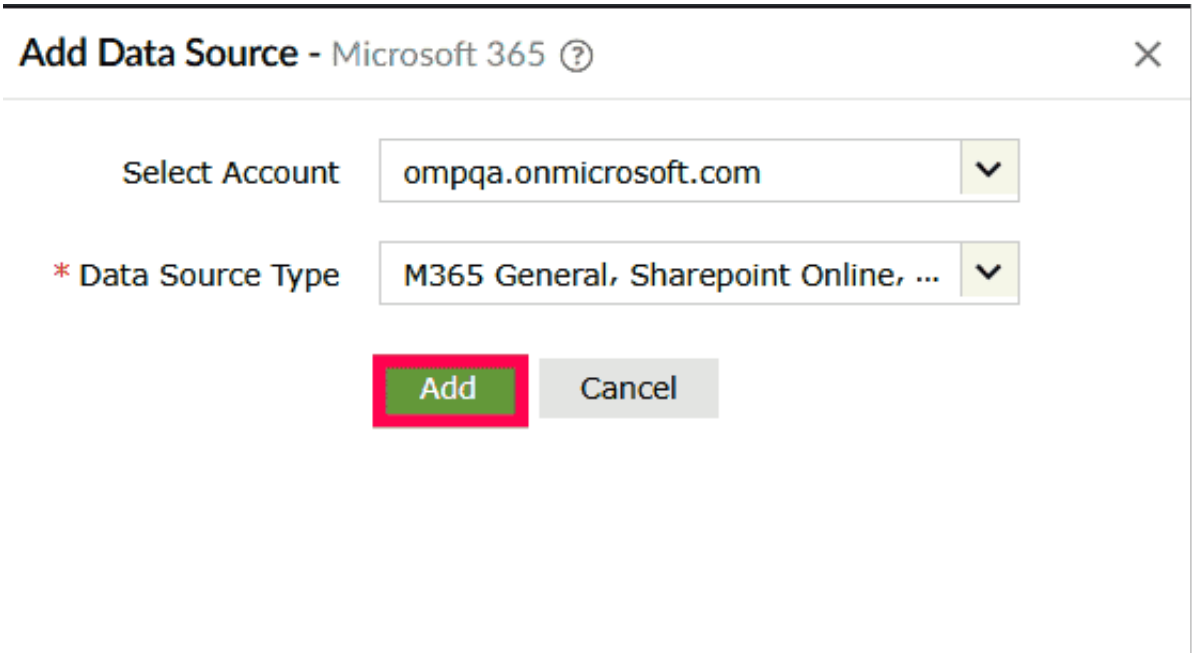


Figure 4: Selecting data source types

Read also

This page detailed how to add Microsoft 365 services as data sources in the product console after configuring a tenant. To learn more about related configurations, see the articles below:

- Managing Microsoft 365 accounts
- Managing cloud sources

7.14.2. Troubleshooting Microsoft 365

Last updated on: September 12, 2025

In this page

Overview

Common integration issues

Overview

This section provides troubleshooting steps for common Microsoft 365 integration issues in Log360. Errors may occur due to missing configurations, expired credentials, or disabled settings in the Microsoft 365 environment. The following guidance will help you identify and resolve these issues.

Common integration issues

1. Audit Logging must be turned on to fetch data

Cause:
Audit logging is not enabled in the Microsoft 365 environment, which prevents user and admin activity from being recorded and fetched into Log360.
Solution:
Enable audit logging using either of the following methods:

- Through the Microsoft 365 portal
  - Log in to the Microsoft 365 portal and navigate to the Admin tab.
  - Go to Admin centers > Compliance > Solutions > Audit. Alternatively, directly open Audit Log Search.
  - If auditing is not turned on, a banner will prompt you to enable activity recording.
  - Select Start recording user and admin activity.

> NOTE
>
> Changes may take up to 60 minutes to take effect

- Turn on audit logging through PowerShell
  - Run the following cmdlets in PowerShell.
  - $UserCredential = Get-Credential;$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection;Import-PSSession $Session -CommandName Set-AdminAuditLogConfig
  - Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled:$True

- Remove-PSSession $Session

2. Invalid Application Password

Cause:

This error occurs if the configured Microsoft 365 application password is deleted or has expired.

Solution:

Create a new application password in Microsoft 365 and update it in the product's Tenant Settings.

3. Missing Microsoft Entra ID Application

Cause:

This error occurs if the Microsoft Entra ID application associated with Log360 has been deleted from the Azure portal.

Solution:

Reconfigure the application in the Azure portal. Follow the manual configuration steps outlined here.

Read also

This page explained common Microsoft 365 integration issues and their solutions, such as enabling audit logging, handling expired application passwords, and reconfiguring deleted applications.

For more details, refer to:

- Adding a data source
- Configuring and managing

7.14.3. Amazon Web Services (AWS)

Last updated on: September 12, 2025

To monitor your AWS environment, EventLog Analyzer requires a valid IAM user with necessary permissions. The solution will use the designated IAM user to collect logs from your AWS environment.

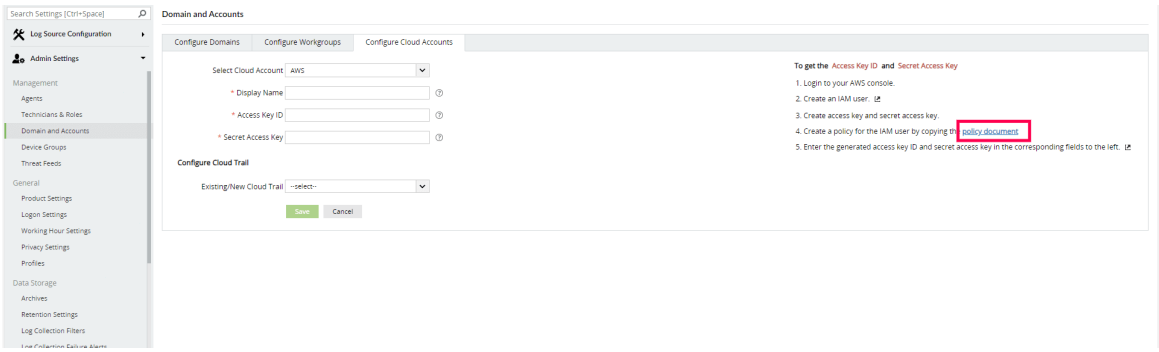
> **Note**
>
> EventLog Analyzer supports all AWS regions, except the AWS China (Beijing) region.

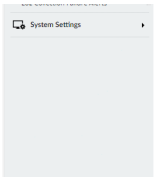
Creating a new IAM user in the AWS console

An IAM user is an entity that you create in AWS to represent the person or service that uses it to interact with AWS.
To create a new IAM user, follow these steps.

1. Login to the AWS console.
2. Navigate to IAM
   - Go to AWS Services → Security, Identity and Compliance → IAM.
3. Create a new user:
   - Select Users from the Left pane and click on Create User.
   - Enter an appropriate User name and click Next.
4. Attach Policies
   - Click on Attach policies directly and then Click on Create Policy.
   - A new tab named Create Policy will open. Select JSON.
   - Depending on whether you want to manually or automatically configure CloudTrail, copy and paste the inline policies accordingly.
     - Auto-configuration: For automatic CloudTrail configuration by EventLog Analyzer, copy and paste the provided inline policy.
     - Manual configuration: For manual CloudTrail configuration, copy and paste the provided inline policy.

   You can find the inline policy in the highlighted section of the image below.





- Click Next.
- Fill in the Policy Name field and click Create Policy.
- Return to the previous tab, refresh the policy table, select the newly created policy, and click Next.

5. Finalize the user creation
   - Verify the details and click Create user.
6. Create security credentials
   - Click on the created User.
   - Go to Security Credentials and click on Create access key under the Access keys section.
   - Choose Third-party service and check the confirmation box.
   - Click Next and then click Create access key.
   - Download the .csv file to save the Access key and Secret access Key.

The generated access key and secret key pair should be used inside EventLog Analyzer to configure the AWS account.

Enter AWS credentials in EventLog Analyzer

- Go to the EventLog Analyzer console.
- Click on EventLog Analyzer Account Settings
- Click on Add Account
- Select the Cloud Type as AWS.
- Enter a Display name in the given box.
- Enter the Access Key ID and Secret Access Key of the IAM user in the given fields.
- Add CloudTrail.
  - Auto-configuration: Select the Region. EventLog Analyzer automatically creates and configures CloudTrail. Click Save.

    Note: EventLog Analyzer will create the following resources:

    - S3 bucket: (accountnumber)-cloudtraillogs-(region)
    - SNS topic: cloudtrailtopic
    - SQS queue: cloudtrailqueue

- SQS queue: cloudtrailqueue
- CloudTrail: cloudtrail

- Manual configuration: Click Connect an existing CloudTrail and follow the steps given in the Logging setup for AWS CloudTrail.

To setup logging for your AWS environment, refer S3 server access logging and ELB access logging.

Manage Cloud Sources:

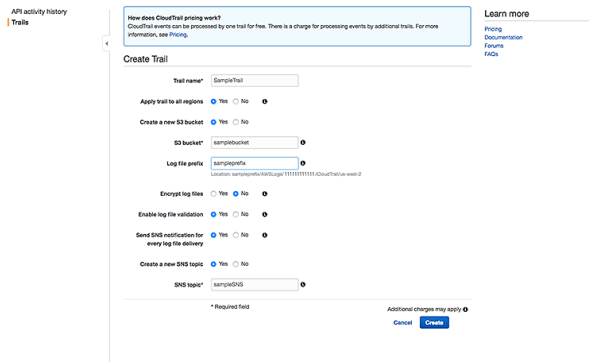
- Logging setup: Amazon CloudTrail Logs
- Logging setup: Amazon S3 server access logs
- Logging setup: Amazon ELB access logs
- Enable/disable cloud source
- Delete a cloud source

Logging setup: Amazon CloudTrail Logs

CloudTrail is an API log monitoring web service offered by AWS. It enables AWS customers to record API calls and sends these log files to Amazon S3 buckets for storage. The service provides details of API activity such as the identity of the API caller, the time of the API call, the source IP address of the API caller, the requests made and response elements returned by the AWS service. In addition, it captures a few non-API events (AWS service events and AWS console sign-in events).
CloudTrail can also be configured to publish a notification for every log file that is delivered, allowing users to take action upon log file delivery.
(I) Enable CloudTrail

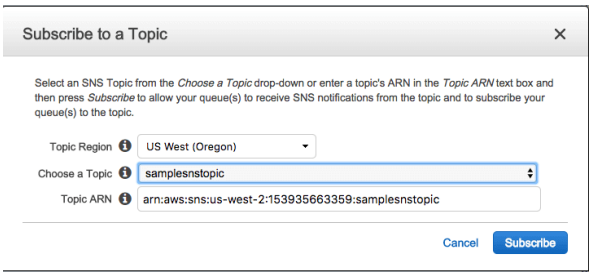
- Login to the AWS console.
- Go to AWS Services → Management Tools → CloudTrail.
- Click Add new trail.
- Click Advanced and fill in the missing information.

(II) Configure an SNS topic
Create an SNS topic. Select the following options: Apply trail to all regions → Yes Create a new S3 bucket → Yes S3 bucket → Provide a new name Log file prefix → Provide the prefix Encrypt log fies → No Enable log file validation → Yes Send SMS notification for every log file delivery → Yes Create a new SNS topic → Yes New SNS topic → Name the topic Select → Create



(III) Create an SQS queue and subscribe to the SNS topic created in Step II

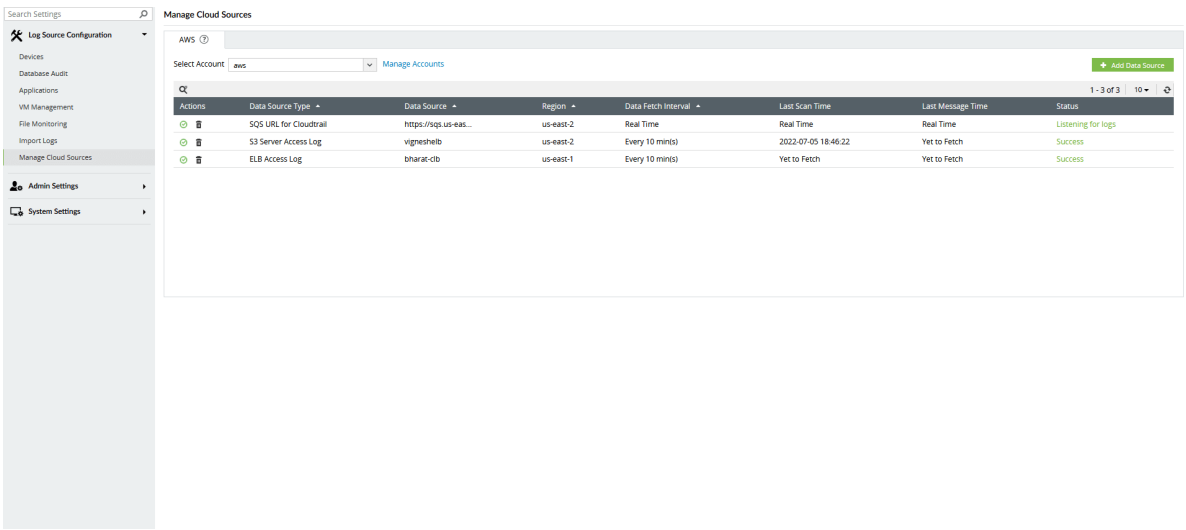
- Go to AWS Services → Messaging → Simple Queue Service (SQS).
- Click Create New Queue and fill in the necessary information.
- Now, this SQS queue must be subscribed to the SNS Topic created when you enabled CloudTrail. Follow the below given steps.
  - Select the SQS queue created.
  - From the Queue Action drop down menu, select Subscribe Queue to SNS Topic.



> **Note**
>
> Amazon SNS raw message delivery needs to be disabled.

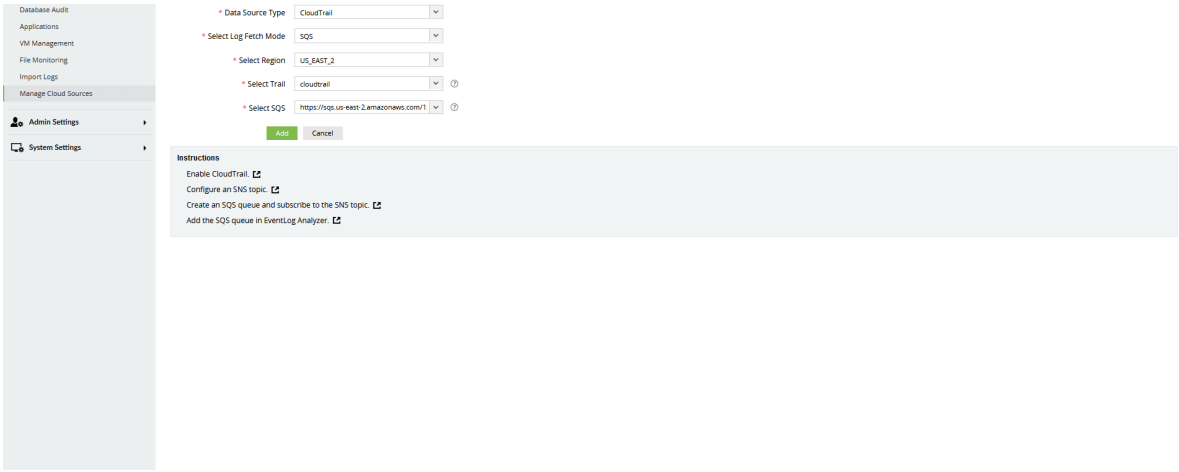
(IV) Add the created SQS queue as a data source in EventLog Analyzer

- Login to the EventLog Analyzer console.
- Go to Settings and click on Manage Data Source.



- Select CloudTrail from the Data source drop-down menu.
- Choose the AWS region, the trail and the SQS queue.





- Click Save.

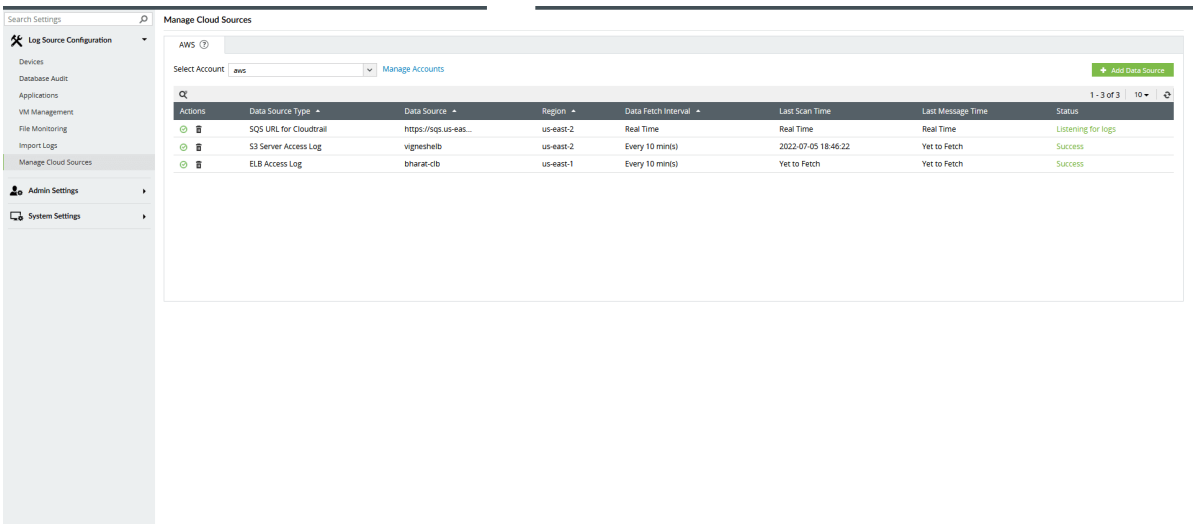
Logging Setup: Amazon S3 server access logs

What is S3 server access logging?

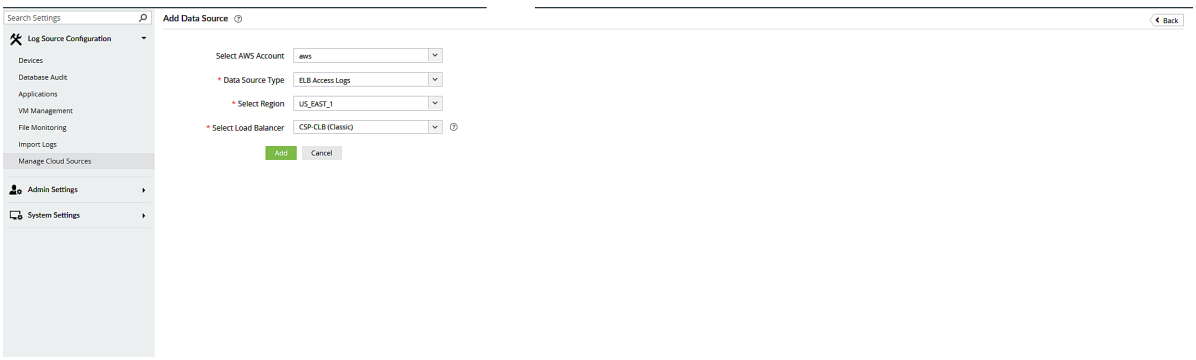
Requests to access S3 bucket can be tracked via access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any. This access log information can be useful in identifying the nature of traffic.

Follow the below given steps to add Amazon S3 server access logs as a data source in EventLog Analyzer.

- Login to the EventLog Analyzer console.



- Go to Settings > Configuration > Manage Cloud Sources and click on Add Data Source.
- Select S3 Server Access Logs from the Data source drop-down menu.

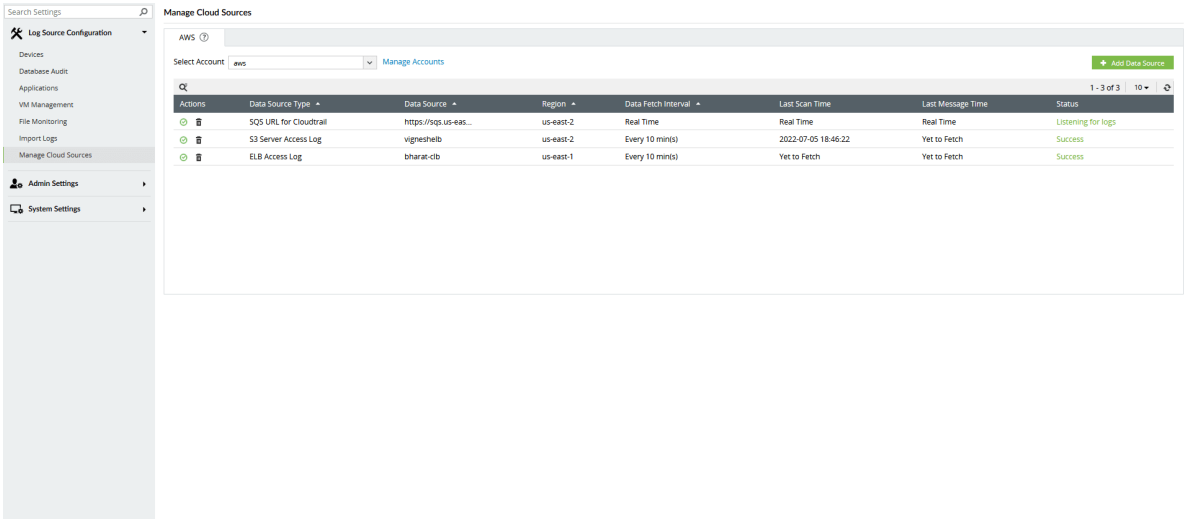


- Select the S3 Bucket for which you want to enable access logging.
- Click Configure..

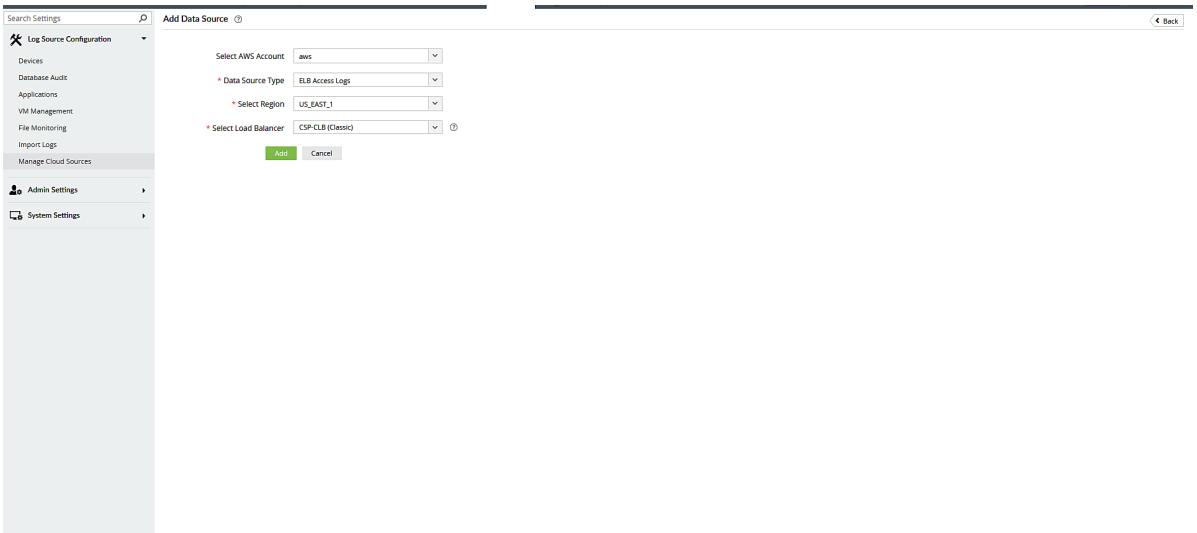
Logging setup: Amazon ELB access logs

Elastic Load Balancer access logs capture information about requests made to load balancers and can be used to analyze traffic patterns and troubleshoot issues. These logs contain details such as the time the request was received, the client's IP address, latencies, request paths, and server responses.
Follow the below given steps to add Amazon ELB access logs as a data source in EventLog Analyzer

- Login to the EventLog Analyzer console.
- Go to Settings > Configuration > Manage Cloud Sources and click on Add DataSources.



- Select ELB Access Logs from the Data source drop-down menu.
- Select the Region and Load Balancer for which you want to enable access logging.



- Click Configure.

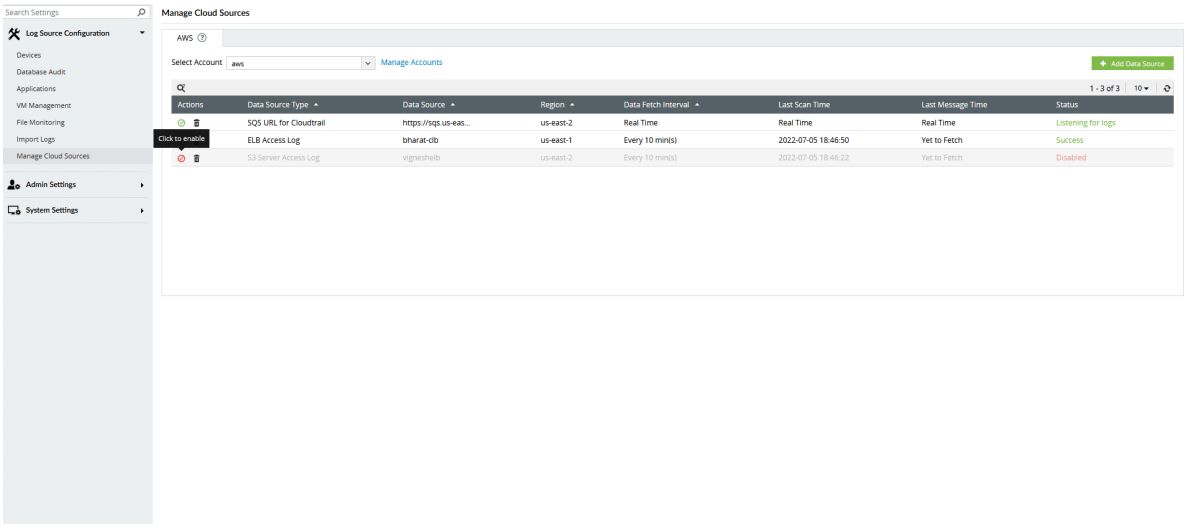
> **Note**
>
> Currently EventLog Analyzer only supports classic load balancers. Network and application load balancers are not supported.

Enable/disable cloud source

Enabling a cloud source:

To enable a cloud source in EventLog Analyzer,

- Click the icon located under the Actions column for the data source you want to enable.

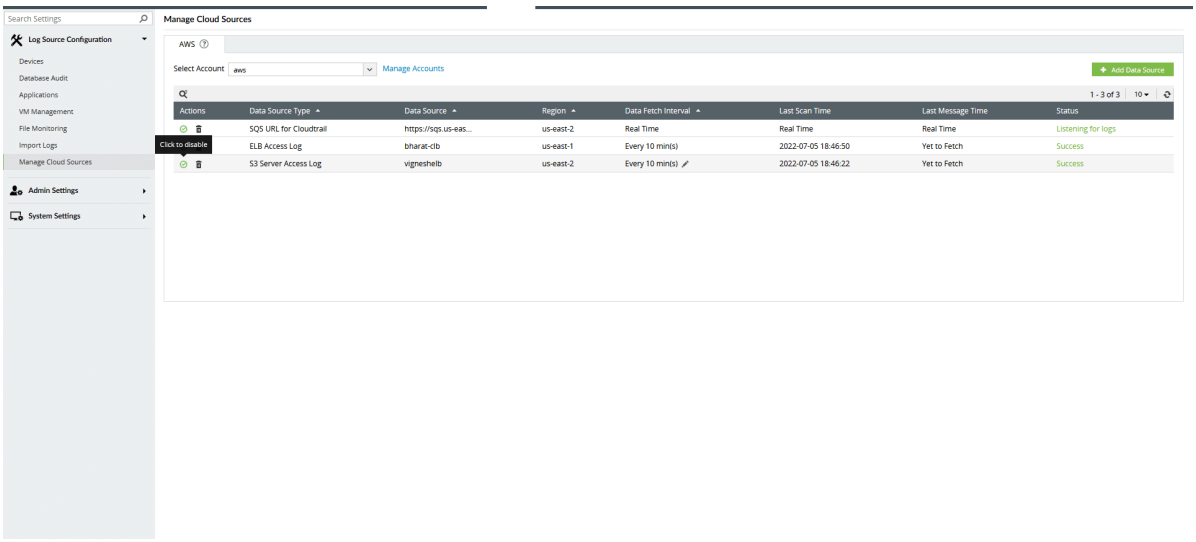


- The data source will be enabled.

Disabling a cloud source:

To disable a cloud source in EventLog Analyzer,

- Click the icon located under the Actions column for the data source you want to disable.

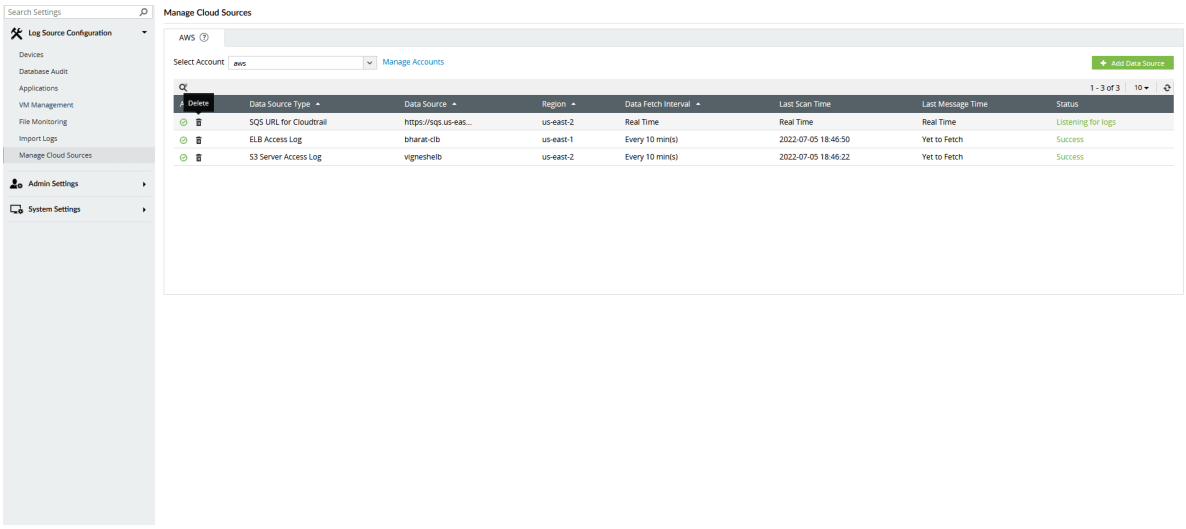


- The data source will be disabled.

Delete a cloud source

To delete a cloud source in EventLog Analyzer,

- Click the delete icon located under the Actions column for that particular data source.



- The data source will be deleted.

Salesforce

EventLog Analyzer helps you analyze Salesforce user activity within the wider context of your overall security posture. By monitoring Salesforce activities, you will be able to spot suspicious login attempts, track privileged user activity, and identify unauthorized access attempts or data modification.

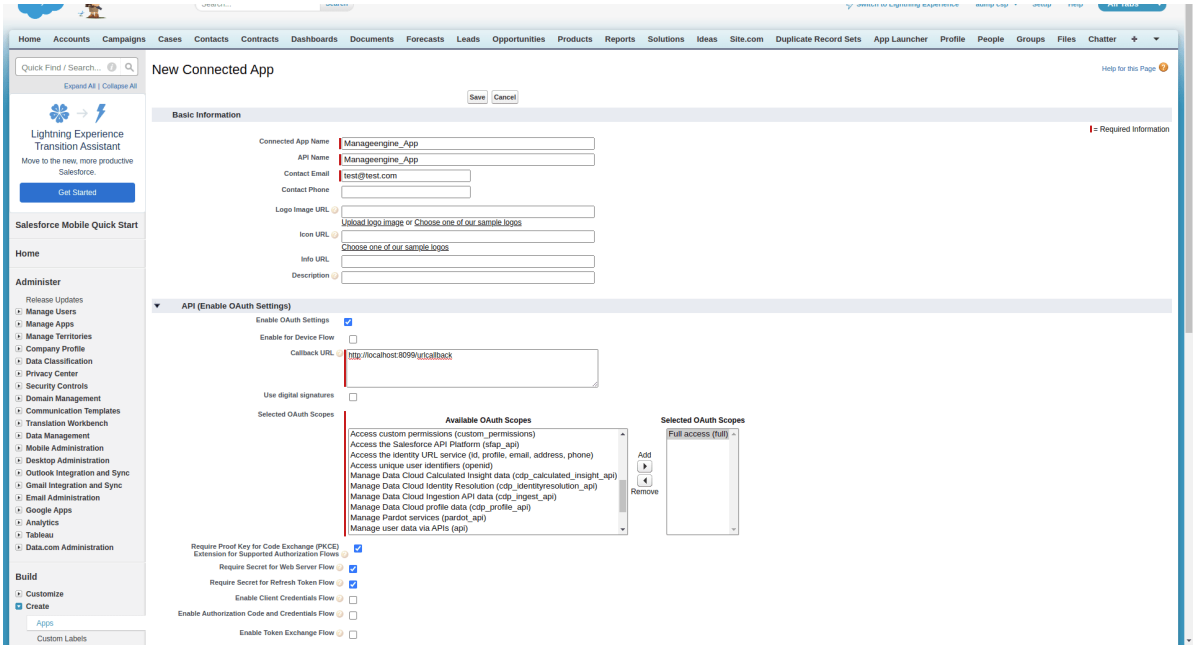
Creating a Connected App with permissions in Saleforce

- Login to your Salesforce account. Ensure that the user account with which you log in has enabled API.

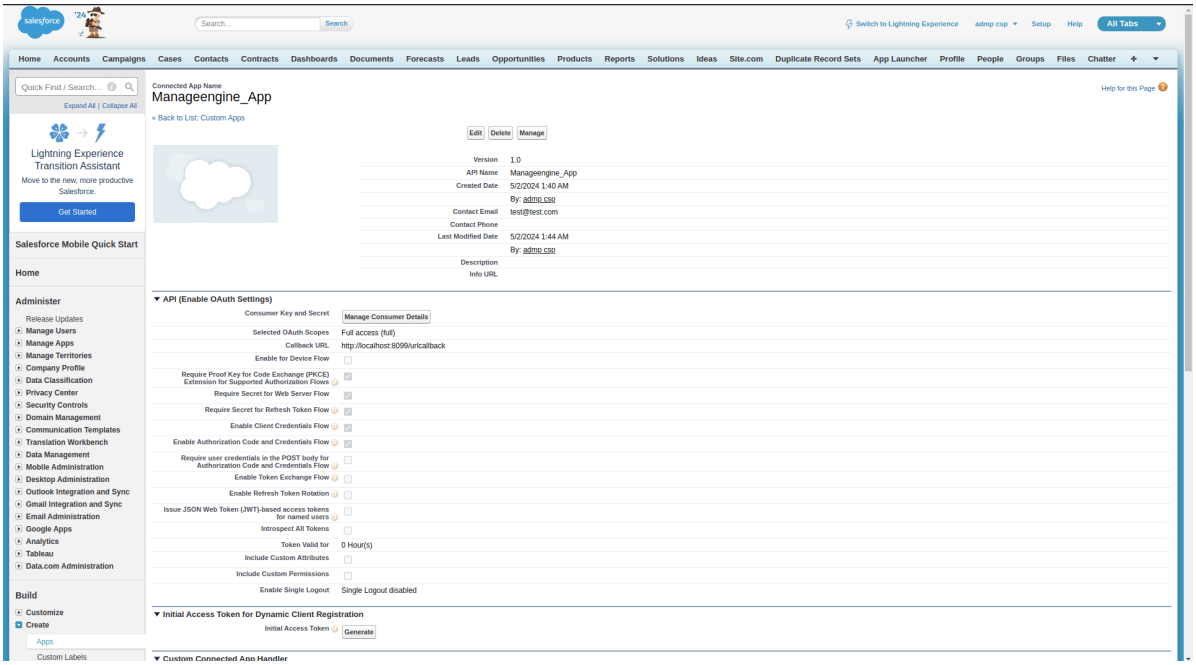
> **Note**
>
> Please make sure you have the Salesforce Event Monitoring add-on license to fetch and analyze Salesforce logs in EventLog Analyzer.
> Ensure that you enable the below permissions in case of using a non-admin user :
> Permissions required:
>
> - View event log files (for collecting event logs)
> - View setup and configuration (for collecting audit logs)
> - View role and role hierarchy(for collecting audit logs)

- Navigate to Setup → Build → Create → Apps → Connected Apps.
- Click on New and fill in the Connected App Name, Contact Email, and Callback URL.

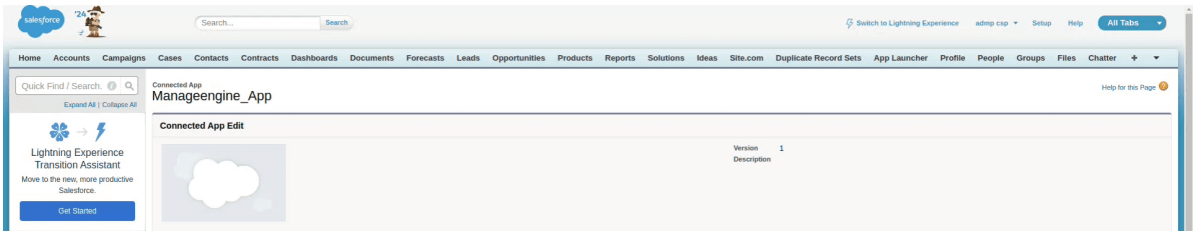


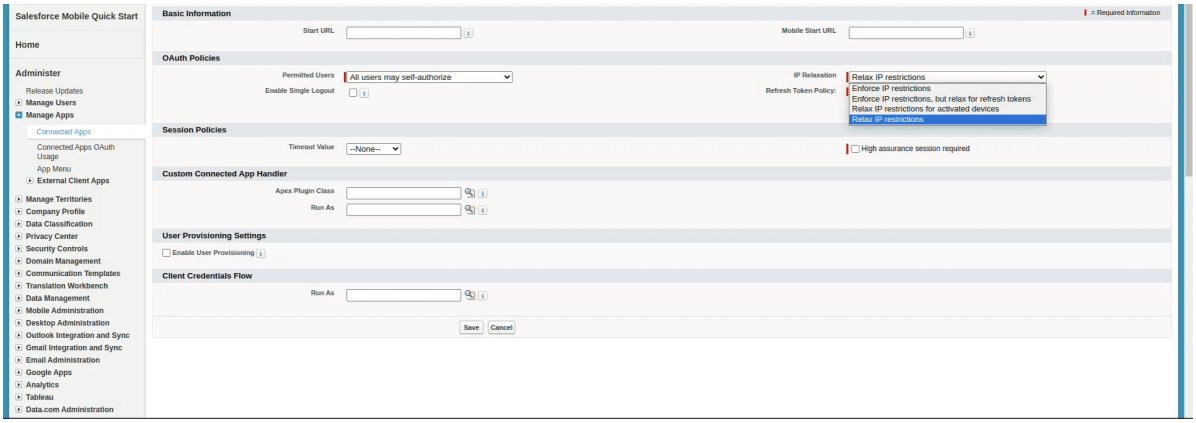


- Enable the OAuth Settings and grant Full access.
- Click Save. The Connected App will be created.
- Click Continue to view the Consumer Key and Consumer Secret.



- Navigate to Setup → Administer → Manage Apps → Connected Apps .
- Click on the newly created Connected App. Under OAuth Policies > IP Relaxation, select Relax IP restrictions from the drop-down.

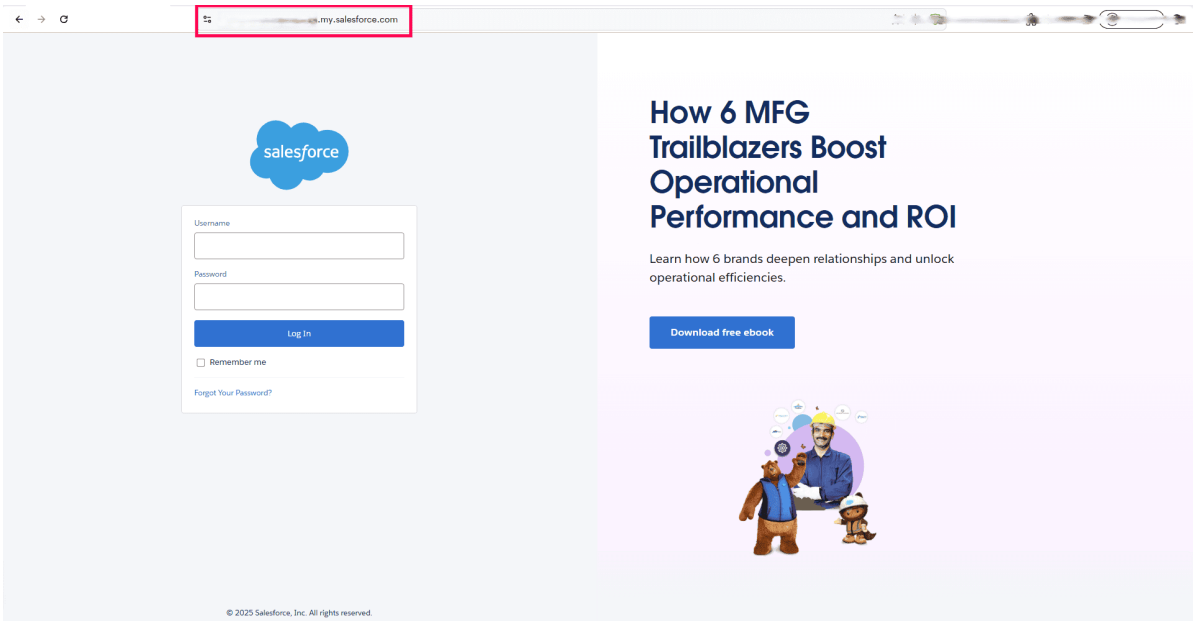




- Click Save.

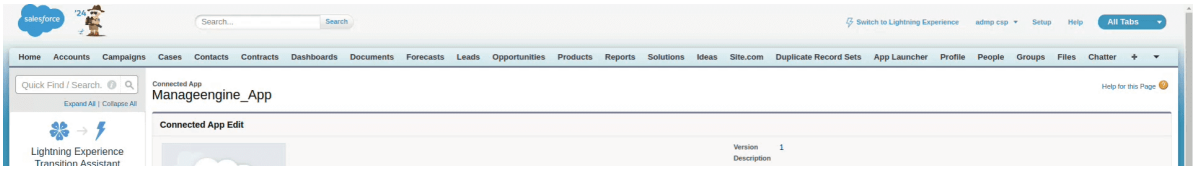
How to get the Salesforce-client-url

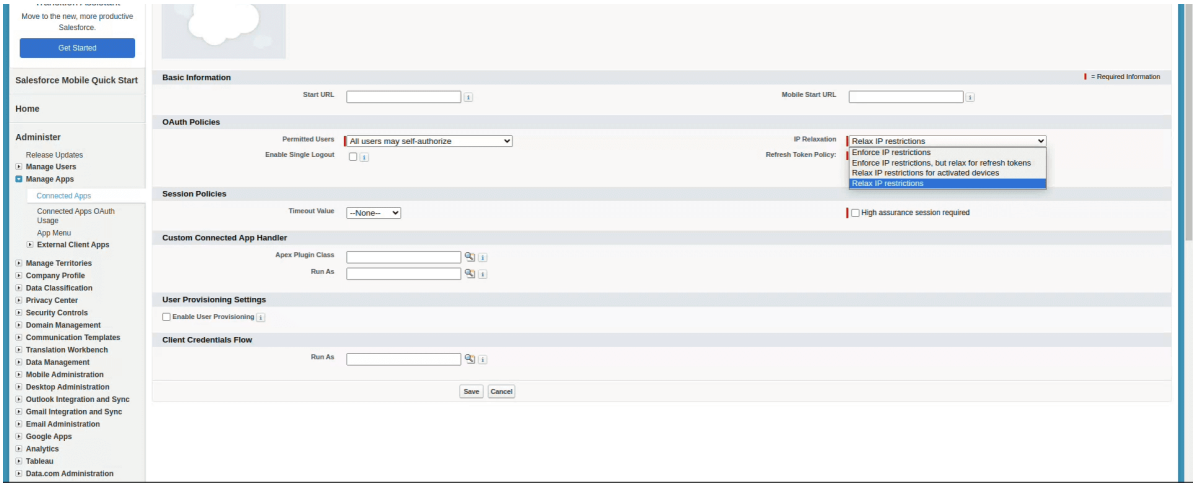
1. Go to the Salesforce login page and copy the URL from your browser's address bar.
2. Paste the URL in the Login URL field(e.g., https://testingtech-ap48.my.salesforce.com).



Enter the Salesforce credentials in EventLog Analyzer

- Click on the Settings tab.
- Navigate to Admin Settings -> Under Management - Domain and Accounts -> Configure Cloud Accounts .
- Select the Cloud Account type as Salesforce.
- Enter a Display Name in the given box.
- Enter the Username, Password, Consumer Key, Consumer Secret and Login URL in the given fields to enable EventLog Analyzer to start collecting logs.




Move to the new, more productive Salesforce.
Get Started
Salesforce Mobile Quick Start
Home
Administer
Release Updates
Manage Users
Manage Apps
Connected Apps
Connected Apps OAuth Usage
App Menu
External Client Apps
Manage Territories
Company Profile
Data Classification
Privacy Center
Security Controls
Domain Management
Communication Templates
Translation Workbench
Data Management
Mobile Administration
Desktop Administration
Outlook Integration and Sync
Gmail Integration and Sync
Email Administration
Google Apps
Analytics
Tableau
Data.com Administration
Basic Information
= Required Information
Start URL
Mobile Start URL
OAuth Policies
Permitted Users
All users may self-authorize
Enable Single Logout
IP Relaxation
Relax IP restrictions
Refresh Token Policy:
Enforce IP restrictions
Enforce IP restrictions, but relax for refresh tokens
Relax IP restrictions for activated devices
Relax IP restrictions
Session Policies
Timeout Value
--None--
High assurance session required
Custom Connected App Handler
Apex Plugin Class
Run As
User Provisioning Settings
Enable User Provisioning
Client Credentials Flow
Run As
Save
Cancel

8.1.1. User Interface Tabs

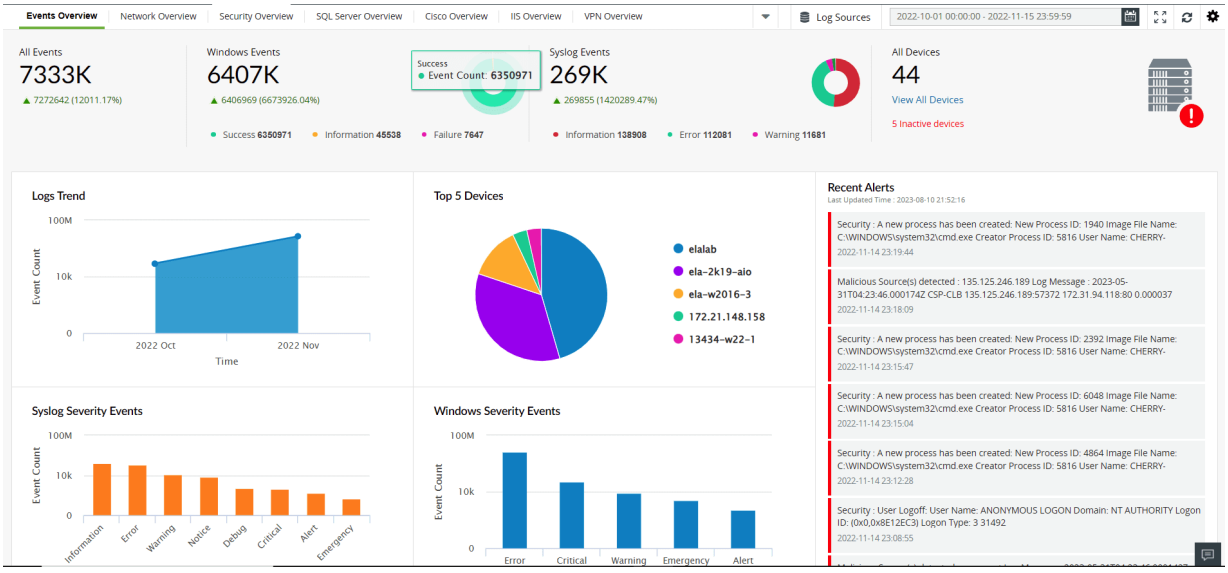
Last updated on: September 12, 2025

EventLog Analyzer's user interface tabs help you navigate to different sections of the product. The tabs include:

Dashboard tab

The Dashboard tab contains multiple dashboards that give you insights into important network activities. The below dashboards are present by default when you click on the Dashboard tab:

- Events Overview
- Network Overview
- Security Overview
- VPN Overview
- Incident Overview



Events Overview

This tab presents a high-level overview of security events by generating graphical reports such as Logs Trend, Syslog Severity Events, Windows Severity Events, and Recent Alerts. These reports are generated for events that occur in a specific time frame (which can be customized). Hovering your mouse pointer over the charts or graphs will give you information about the Event Count of a particular device, its IP address, and the Severity of the event (Information, Notice, Debug, Warning, Alert, Error, Critical, and Emergency).

Network Overview

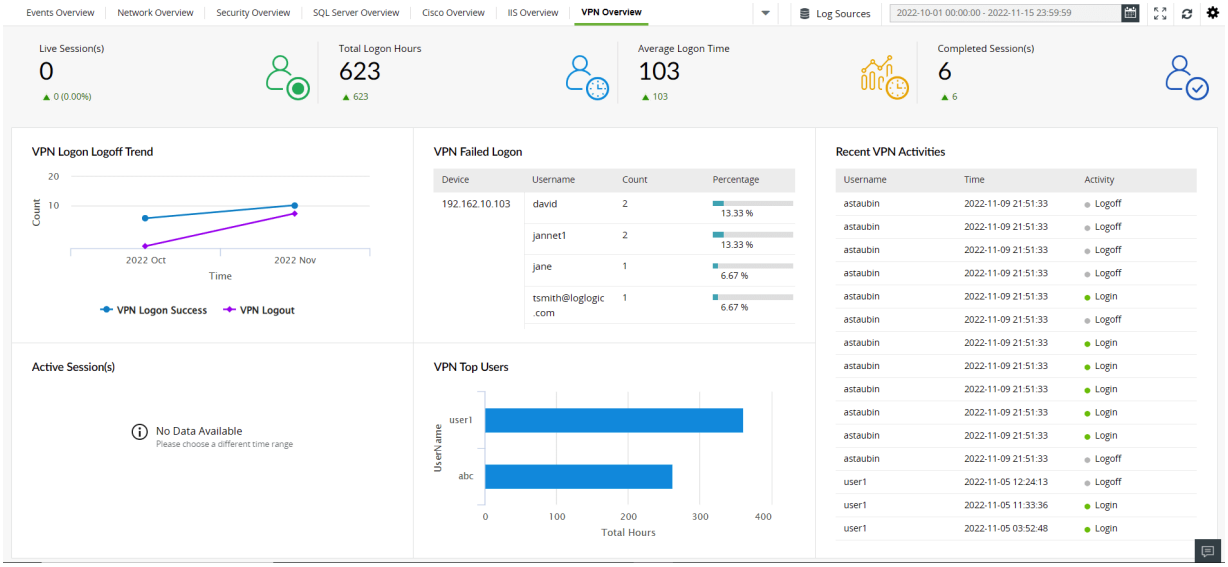
This tab gives you information about network traffic in your environment. It provides details on the traffic trend, allowed and denied network connections, and more to help you track events of interest.

Security Overview

The security overview dashboard consolidates events from network devices such as IDS/IPS, endpoint security solutions, vulnerability scanners, and other threat detection solutions. This dashboard contains reports that help security teams keep tabs on crucial security events such as vulnerabilities and threats. It also has an interactive widget on IDS/IPS attacks, which helps you identify the type of attack, number of attack attempts, and the time when the attack happened.
The dashboard also contains the Alerts Count Overview widget that displays the number of alerts triggered in a given time frame.

VPN Overview

You can customize the Dashboard tab to include the VPN Overview tab by navigating to Settings → Add Tab → VPN Overview. EventLog Analyzer monitors VPN session activities and generates reports to help you visualize events of interest. The VPN Overview dashboard will give you insights on VPN user and session activities by displaying widgets such as Live Sessions Count, Total Logon Hours, Average Login Time, Closed Sessions, and Top Users and Status. You can also customize the VPN dashboard by adding and reordering widgets by navigating to Settings → Add Widgets and Settings → Reorder Widgets respectively.

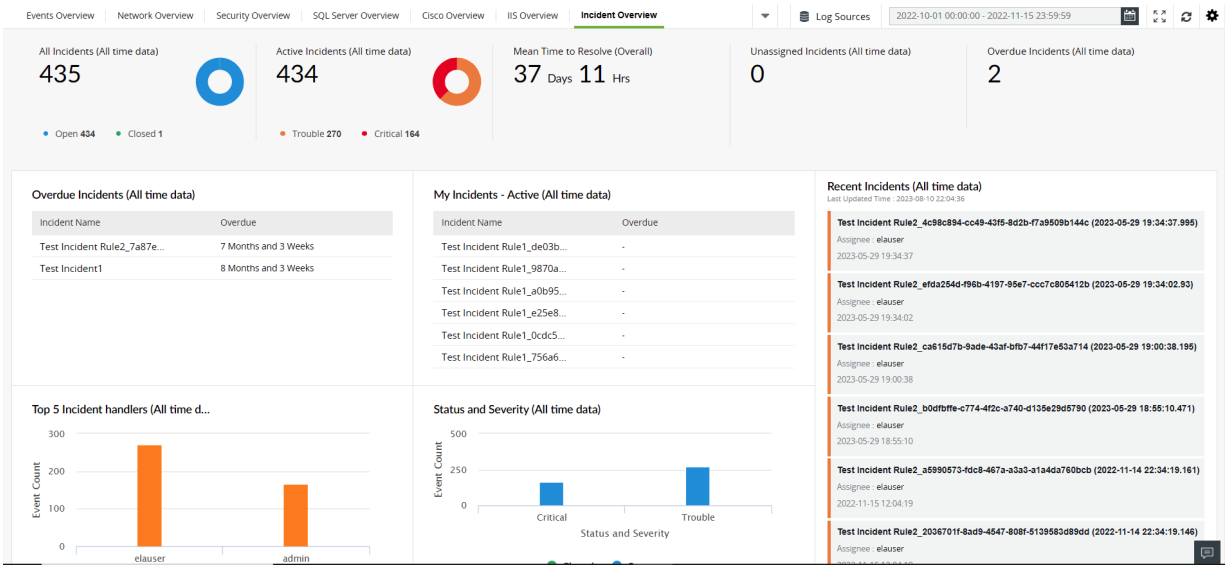


Incident Overview

This tab helps you effortlessly manage the security incidents detected. The dashboard gives you the count of all, active, unassigned and overdue incidents. It also provides the mean time to resolve. The dashboard provides insights such as:

- Overdue incidents's age.
- Personalized incident dashboard where the user can view the incidents assigned to them and their age.
- Top 5 incident handlers.
- The status and severity of the incidents detected.
- Trend graph for the incidents created and resolved.
- User-specific mean time to resolve the incidents.

> **Note**
>
> mean time to resolve refers to the average time taken to resolve an incident.



The Dashboard tab also contains the Log Sources, date and time selection, and settings icons.

Log Sources tab

When you click on the Log Sources tab, three tabs are displayed:

- Devices
- Applications
- File Integrity Monitoring

Devices

The Devices section displays the entire list of systems (Windows, Linux, IBM AS/400, HP-UX, etc.) and devices (routers, switches, etc.), from which EventLog Analyzer is collecting logs. The device list displayed is categorized based on the Device group selected from the drop-down list (default: All Groups). You can add a new device (+Device), or add and schedule new reports (+Schedule) from this section. You can search for a particular device based on its IP Address or Device Name, delete a device or set of devices, and disable/enable log collection from a particular device or set of devices.

The device list table displays details like device type, event summary (error, warning, failure, others), connection status of the device, time when the last log message was fetched, and device group to which the device belongs.

Moving the mouse over any device brings up some options:

- View the last 10 events collected from a particular device.
- Update the device details.
- Ping the device.
- Enable/disable log collection from the device.

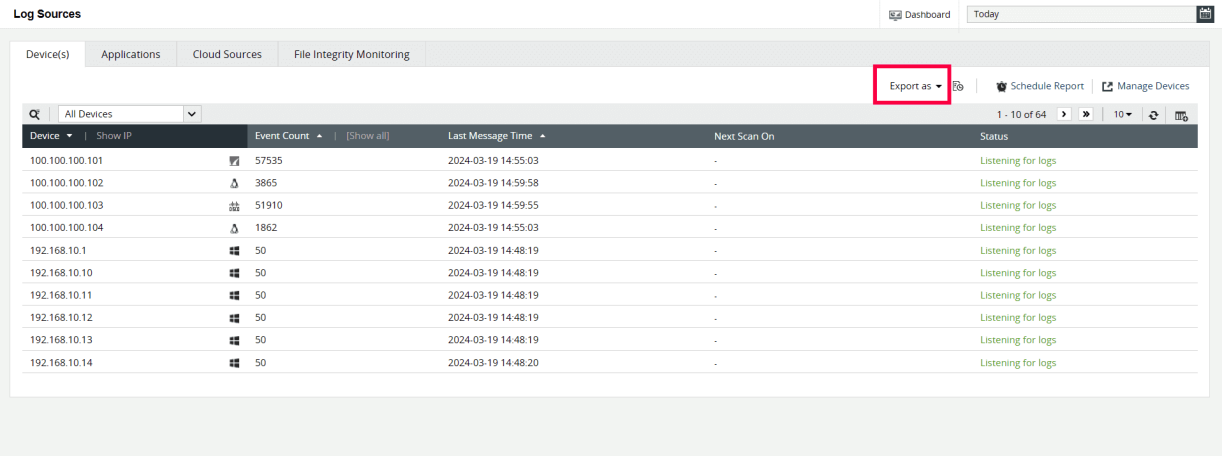
You can even customize the columns you would like to display in the device table by clicking the column selector icon or increase the number of devices that are displayed per page (from a minimum of 5 devices per page to a maximum of 200 devices per page). Using the drop down menu, you can list out only the Active devices or Enabled devices and have the option to exclude synced devices from Active Directory Audit Plus.

Scheduled Reports

EventLog Analyzer lets you schedule report generation, export, and redistribution over email.

1. Go to Dashboards -> View All Devices.
2. To schedule a report, click Schedule Reports on the top right corner of the page.
3. Click on the +Create New Schedule button on the page. This will open the Create New Schedule page.
4. In the Create New Schedule window,
    - Schedule Name: Enter the name of the Schedule.
    - Select Log Sources: Add the Log Sources for which the schedule is for with the help of the + button.
    - Schedule Frequency: Specify the frequency at which reports need to be exported. The frequency can be 'Only Once', 'Hourly', 'Daily', 'Weekly', or 'Monthly'.
    - Export Time Range: Select the time range for which the report needs to be created and later exported along with the timing.
    - Report Format: Choose the file format in which the report needs to be exported i.e. PDF or CSV.
    - Email Address: Configure the email address to which the reports need to be sent.
    - Email Subject: Enter the subject of the mail that contains the exported reports.
5. Once you've entered the necessary details for the schedule, click Save to complete creating the report schedule.

You can also export the reports in PDF or CSV format with the Export as option. These generated reports will include device details such as the display name, IP address, total count, last message time, next scan time, and device status.



Applications

The Applications section provides an overview pie-chart (which can be drilled down to raw log information) and

lists the devices from which application logs for IIS W3C Web Servers, IIS W3C FTP Servers, MS SQL Servers, Oracle Live Audit, DHCP Windows/Linux Servers, Apache Web Servers or Print Servers, have been received or imported into EventLog Analyzer. The device list displayed is categorized based on Application Type selected from the drop-down list. Applications logs can be imported into EventLog Analyzer by selecting +Import from the Actions drop-down list.
The application device list displays details like device name, application type, total events, recent records, time imported, start time and end time. Click on the device name or the corresponding section in the pie chart to get the complete overview of the application event data, and generate corresponding reports. You can even customize the columns you would like to display in the application device table by clicking the column selector icon.

File Integrity Monitoring

The File Integrity Monitoring dashboard gives information about changes made to files and folders of Windows, Linux, and Unix machines. It tabulates and reports on the files and folders created, deleted, modified, and renamed. It also displays changes made to file and folder permissions.
At the top of this dashboard, you can find the Manage File Integrity Monitoring tab which allows you to add, delete, and manage devices for File Integrity Monitoring. The FIM Alert tab allows you to configure alerts for anomalous file and folder modifications. The FIM Scheduled Reports tab helps you view and export scheduled reports.

Date and time

You can generate and view all the audit reports for the required time frame using the date and time box provided.

Settings icon

The settings icon displays multiple options to customize all dashboards by adding, managing, and ordering the widgets and tabs that are displayed. You can also refresh the changes made to the time frame in the product using the Refresh Interval option.

Reports tab

This tab displays a dashboard that contains reports for all events taking place in your network. At the top left corner, you can find a drop-down menu that allows you to choose and view reports based on Devices, Applications, File Monitoring, Threats, Vulnerability, and Virtual Machines. You can also view Custom Reports, User Based Reports, and Top and Trend reports by clicking on the required option from this drop-down menu. The Export As drop-down menu enables you to export reports in either the CSV or PDF formats. You can schedule reports by clicking on the +Add option present in the Schedule Reports tab.
On the left pane, you can find multiple pre-defined reports that are automatically generated when log sources are added to EventLog Analyzer. You can also create custom reports by clicking on the Manage Reports tab present at the lower-left corner of the screen. The Scheduled Reports tab allows you to view existing scheduled reports and export them as and when needed.

Compliance tab

The Compliance tab provides the set of canned reports as required by various compliance policies, namely, FISMA, PCI-DSS, SOX, HIPAA, GLBA, GPG, and ISO 27001:2013. The +Add option allows you to create and select the reports required for a new compliance policy of your choice. The Edit option allows you to customize the reports available under each compliance policy.

Search tab

The Search tab provides two options to search the raw logs: Basic Search or Advanced Search. The search result is displayed in the lower half of the page and the final search result can be saved as a report (in PDF or CSV format) and can also be scheduled to be generated at predefined intervals and be automatically mailed to a set of configured users.
You can use Basic search if you are interested in manually constructing the search query. Here you can use phrase search, Boolean search, grouped search, and wild-card search to build your search query. You can use Advanced search to interactively build complex search queries easily with field value pairs and relational operators. New fields can be extracted from the search result and regular expression (regex) patterns can be constructed to easily identify, parse and index these fields in new logs received by EventLog Analyzer.

Correlation tab

The Correlation engine analyzes logs collected from different parts of the network and generates alerts for suspicious patterns of events. The dashboard, by default, displays the report on Recent Incidents. You can create and modify correlation rules by clicking on the Manage Rules tab present in the dashboard.

Alerts tab

This tab displays the number of Active Alerts in the dashboard along with their severities. You can view tabulated information about the alerts, their time of generation, the status, and their corresponding response workflow (if configured) in the dashboard.

Settings tab

This section allows you to configure EventLog Analyzer as per your requirements. It has three sub-sections as given below:

Configuration Settings

This section allows you to Manage Devices, Device Groups, Application Sources, Import Log Data, Threat Sources, File Integrity Monitoring, Vulnerability Data, FIM Templates, and vCenter. You can also configure threat management and log forwarding from this section.

Admin Settings

Admin Settings

This section allows you to perform various administrative activities by managing Alert Profiles, Archives, Technicians and Roles, DB Retention Settings, Log Collection Filters, Working Hour Settings, Product Settings, Log Collection Failure Alerts, Dashboard profiles, Privacy Settings, Logon Settings, Domain and Workgroups, Report Profiles, Resource Grouping, Custom Log Parsers, Tags, and Log360 Cloud platform.

System Settings

This section can allow you to configure various settings including Notification Settings, System Diagnostics, Database Access, Re-branding, NT Service, Connection Settings, and Listener Ports.

Add tab

This tab allows you to easily add log sources from Devices and Applications. It also has the provision to let you import logs from other sources. You can add Alert Profiles, Log Filters and create custom Reports from this tab.

8.1.2. Log Receiver

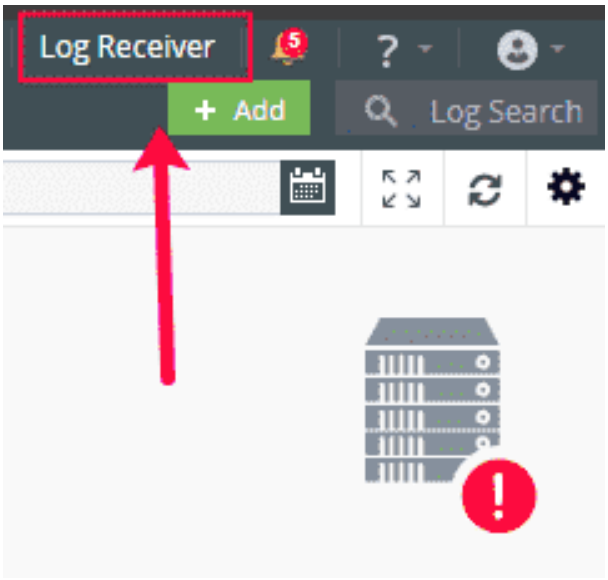
Last updated on: September 12, 2025

In this page

Syslog Viewer

Server Details

EventLog Analyzer includes a functionality called Log Receiver which is a packet capturing tool that displays real-time packets being received at a specified port.
It helps the security analysts by providing supplementary information like live logs being received, and the details related to the server such as server-name,TCP ports and IP address where EventLog Analyzer is set up. (Refer Fig 1)



The Log Receiver tab comes with two default sub-tabs:

1. Syslog Viewer
2. Server Details

Syslog Viewer

The Syslog Viewer tab showcases real-time logs that are currently being forwarded to the EventLog Analyzer server through the default ports (513, 514).

Note

- The list shows the live packets being received at the specified port in your machine. This does not guarantee that EventLog Analyzer has received the Syslog packets.
- The Log Receiver will listen for logs for up to three minutes or until 1000 packets are received.

After reaching this limit, the Log Receiver requires a manual restart to resume listening. Click on Start Listening to resume the process. The option to restart is available under the Syslog Viewer tab.

Point 1: Receiving Syslog packets 280 Packets received. Stop Listening-

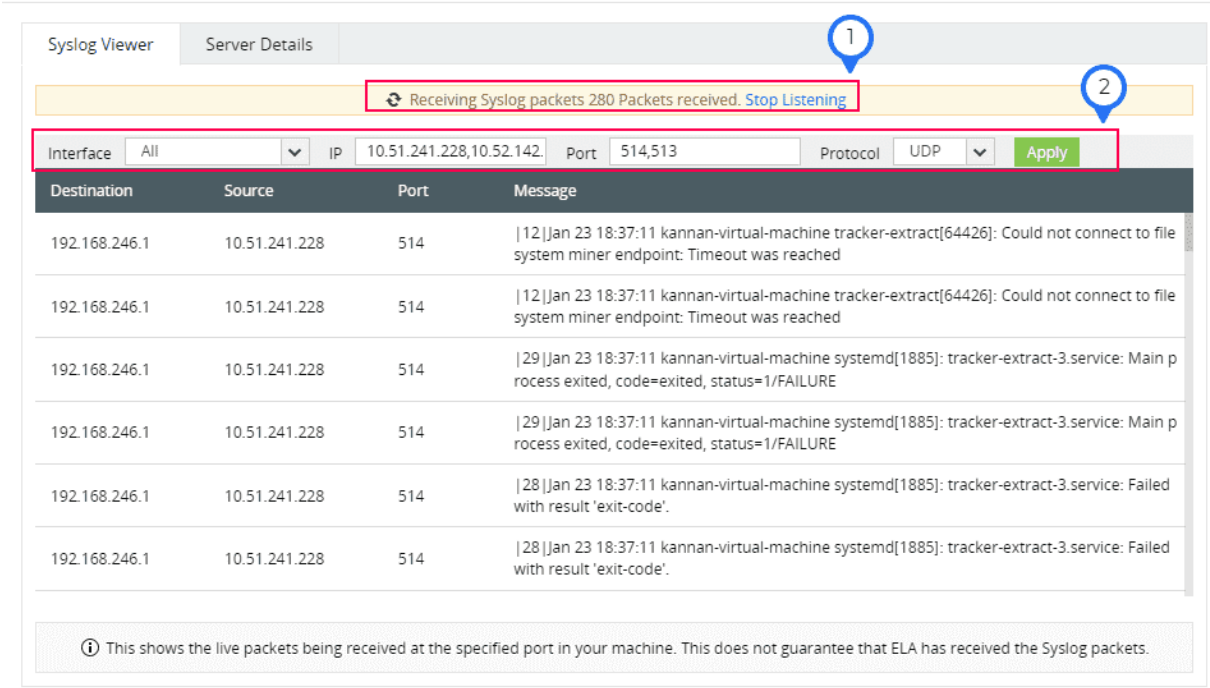
It indicates the log count received and the status, specifying whether the product is actively listening to the logs or not. It can be halted and restarted as needed. (Refer Fig 2)

Point 2 - Apply

It indicates the configurations that can be adjusted to display the live logs received on the server. You can find the associated details below:

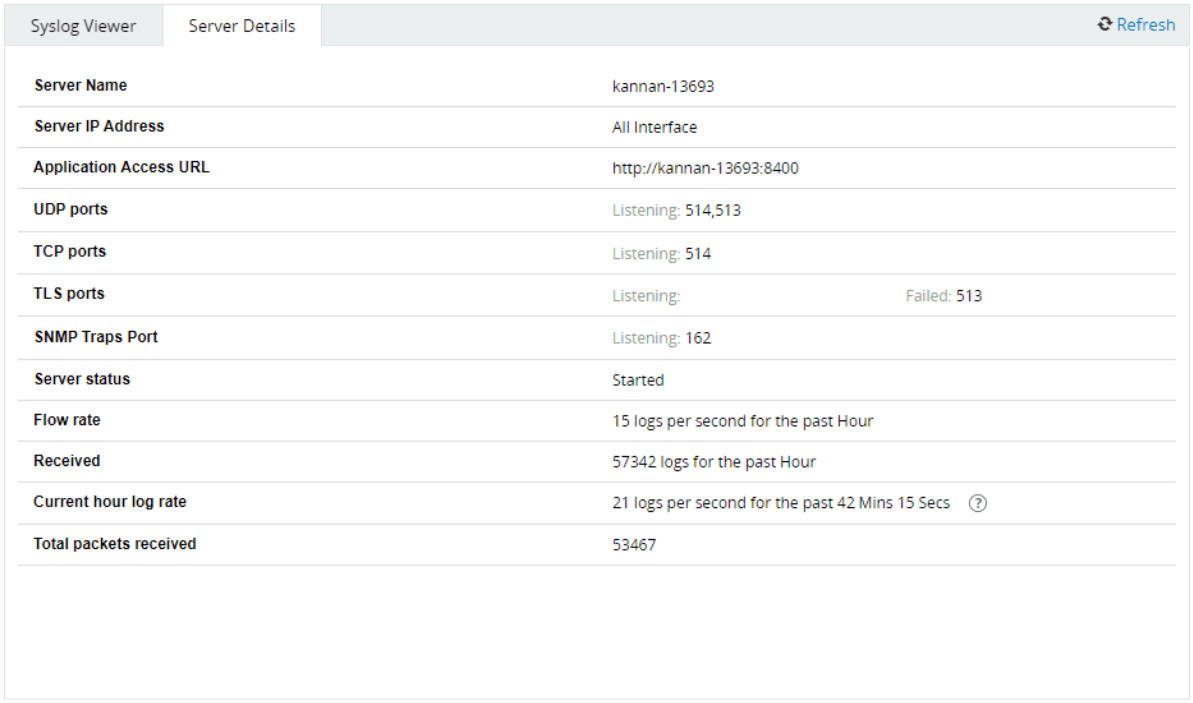
- Interface - It showcases all available network interfaces on the EventLog Analyzer server machine. To examine live logs for a specific interface, you can choose it from the dropdown box. Otherwise, it can be left as "All."
- IP - To verify whether logs from a specific device are received on the server machine, enter the IP address of the machines forwarding logs to EventLog Analyzer. For multiple devices, input their IP addresses with comma-separated values. To check for all devices, leave the field blank.
- Port - Specify the ports to which the logs are being forwarded to the EventLog Analyzer Server.The logs are forwarded to the EventLog Analyzer Server by default on ports 513 or 514.
- Protocol - You can specify the protocol as either UDP or TCP.

Click "Apply" to verify the logs received by the EventLog Analyzer server. The logs will be presented with details such as source IP, destination IP, port, and accompanied by the respective messages.



Server Details

Server Details displays comprehensive information regarding EventLog Analyzer, including server name, IP, Access URL, Port details, Log flow, and more. The details regarding the mentioned fields are provided below. (Refer Fig 3)



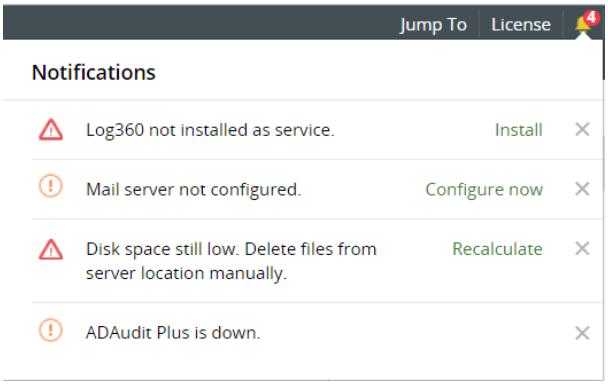
1. Server Name - The name of the current server or machine where EventLog Analyzer is installed.
2. Server IP Address - It indicates the network adapter linked to EventLog Analyzer; if none is specified, it displays "All Interface."
3. Application Access URL - The URL utilized for accessing the EventLog Analyzer application.
4. UDP ports - The UDP ports configured in EventLog Analyzer that are either in a listening state or have encountered failures.
5. TCP ports - The TCP ports configured in EventLog Analyzer that are either in a listening state or have encountered failures.
6. TLS ports - The TLS ports configured in EventLog Analyzer that are either in a listening state or have encountered failures.
7. SNMP Traps Port - The SNMP Trap ports configured in EventLog Analyzer that are either in a listening state or have encountered failures.
8. Server Status - The current status of EventLog Analyzer
9. Flow Rate - The log flow per second for the past hour.
10. Received - The log flow for the previous hour.
11. Current hour log rate - Displays the log flow per second for the current hour.
12. Total Packets Received - Total logs received for the current hour

8.1.3. Notification Center

Last updated on: September 12, 2025

Log360 delivers instant alerts and notifications on any event that requires your attention. These alerts can be accessed from anywhere within the product.

Click the icon in the top right corner of the screen to view alerts from the product.



Alert generating events in Log360

- Reminder to install Log360 as a service.
- Reminder to configure mail server to receive mail notifications.
- Low disk space alert.
- Component down-time alert.

Manage Alerts

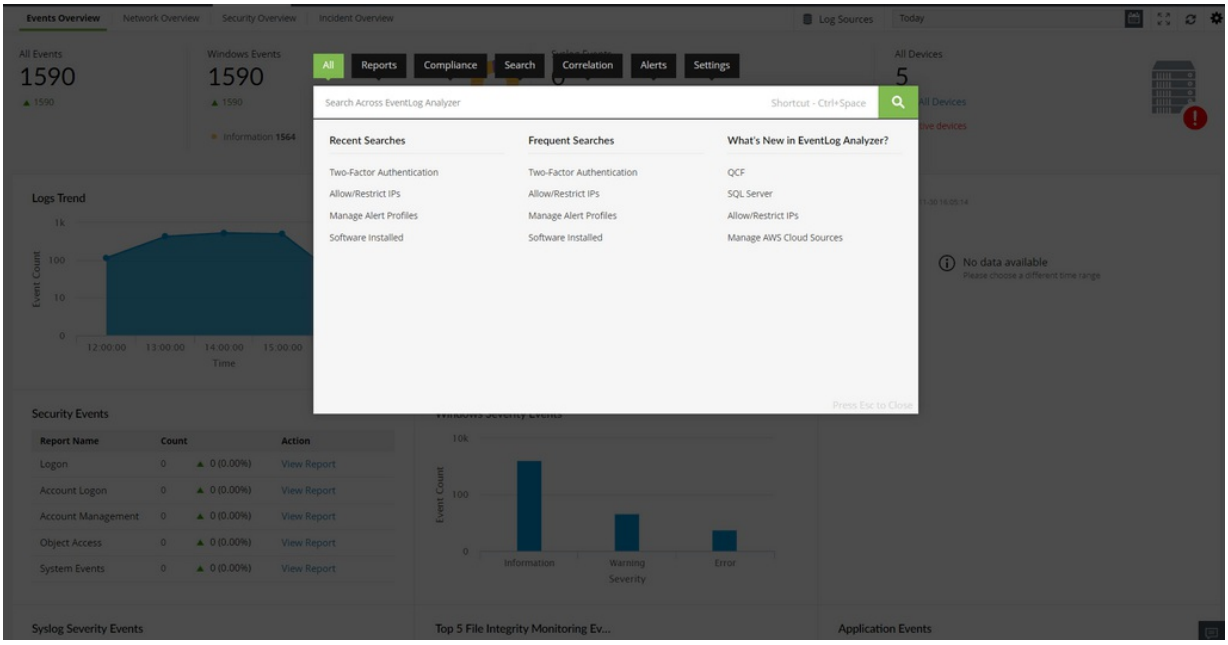
Log360 allows administrators to easily manage alerts, either by making the process of resolution simpler or by deleting alerts that you feel are not important.

- To resolve, click on the action link corresponding to the alert. You will be directed to the screen where changes have to be made.
- To delete, click the icon to hide the alert from your notification tray.

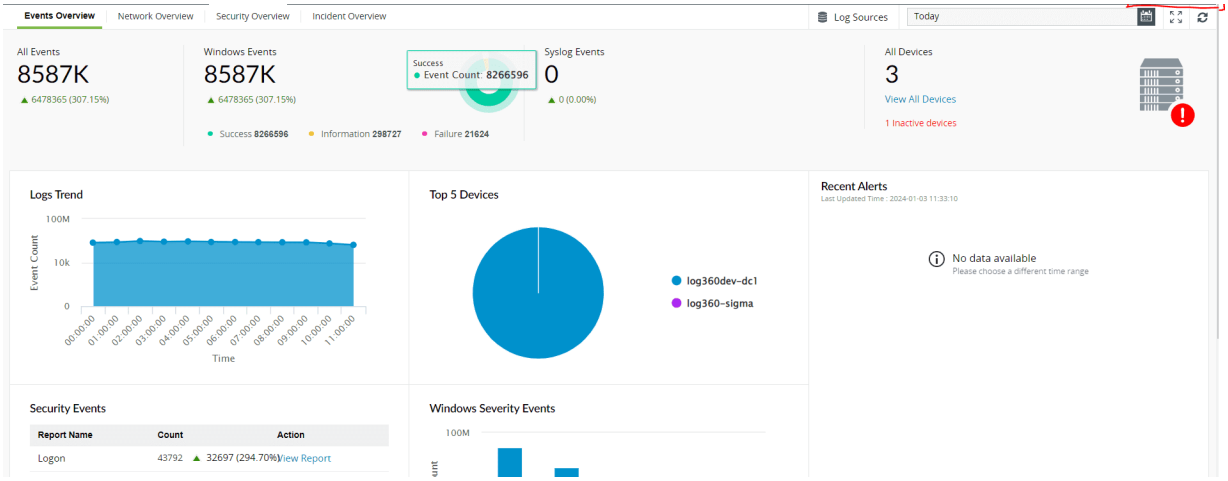
8.1.4. Global Search

Last updated on: September 12, 2025

The global search feature can be used to search across all sections of EventLog Analyzer including Reports, Compliance, Correlation, Alerts, and Settings. This will help in finding particular sections of the product faster, and improves productivity of the SOC team.
For instance, to search for reports related to Windows, type "Windows" in the global search bar. All relevant Reports, and Settings will be displayed in the search screen. This feature can also provide quick access to particular compliance mandates such as HIPAA and PCI-DSS.



To search for a report or a particular setting, click on the search bar in the top right corner of the screen. You can also use the keyboard shortcut Ctrl+Space to access Global Search.



Recent Searches:

The Recent Searches section displays recent searches for each tab in the Global Search feature.

Frequent Searches:

The Frequent Searches section displays the most searched queries in EventLog Analyzer.

What's New in EventLog Analyzer:

This section shows the most recently added features in EventLog Analyzer. Clicking on the features will redirect you to the particular feature section.

8.2.1. User Interface Tabs

Last updated on: September 12, 2025

In this page

Dashboard Tab

Log Sources Tab

Date and Time

Settings Icon

Reports Tab

Compliance Tab

Search Tab

Correlation Tab

Alerts Tab

Settings Tab

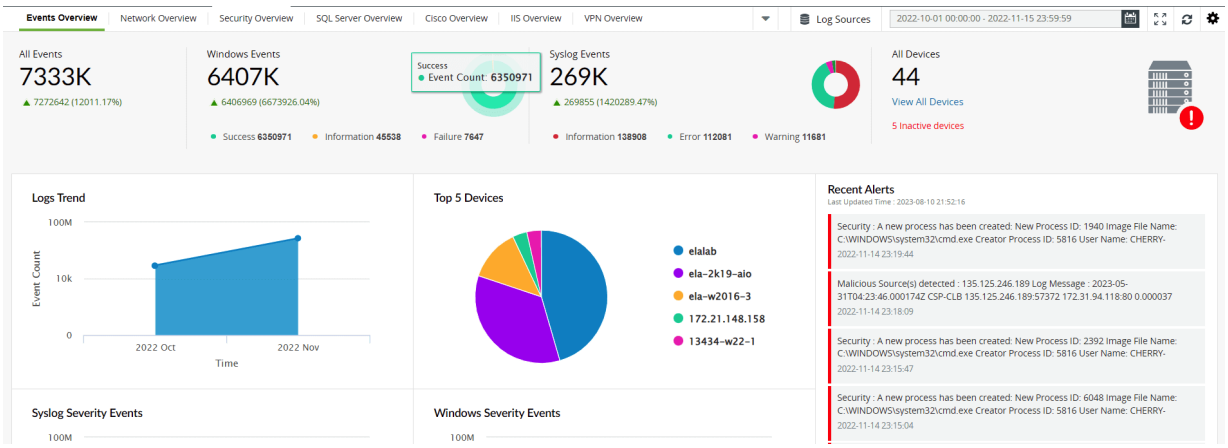
Add Tab

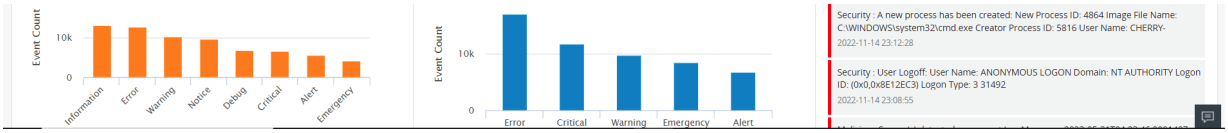
EventLog Analyzer's user interface tabs help you navigate to different sections of the product. The tabs include:

Dashboard tab

The Dashboard tab contains multiple dashboards that give you insights into important network activities. The below dashboards are present by default when you click on the Dashboard tab:

- Events Overview
- Network Overview
- Security Overview
- VPN Overview
- Incident Overview





Events Overview

This tab presents a high-level overview of security events by generating graphical reports such as Logs Trend, Syslog Severity Events, Windows Severity Events, and Recent Alerts. These reports are generated for events that occur in a specific time frame (which can be customized). Hovering your mouse pointer over the charts or graphs will give you information about the Event Count of a particular device, its IP address, and the Severity of the event (Information, Notice, Debug, Warning, Alert, Error, Critical, and Emergency).

Network Overview

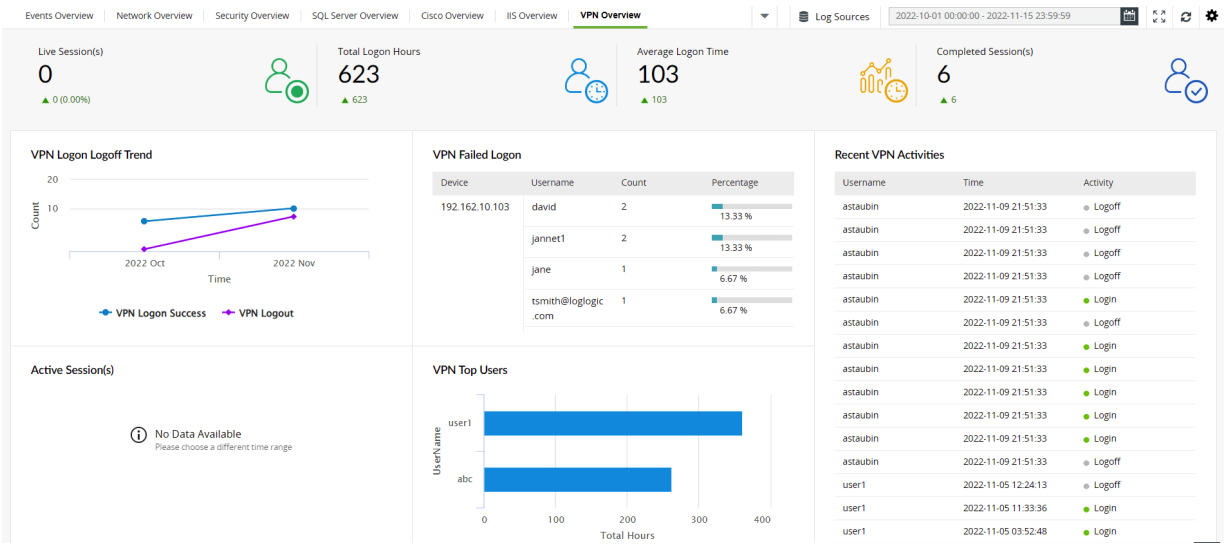
This tab gives you information about network traffic in your environment. It provides details on the traffic trend, allowed and denied network connections, and more to help you track events of interest.

Security Overview

The security overview dashboard consolidates events from network devices such as IDS/IPS, endpoint security solutions, vulnerability scanners, and other threat detection solutions. This dashboard contains reports that help security teams keep tabs on crucial security events such as vulnerabilities and threats. It also has an interactive widget on IDS/IPS attacks, which helps you identify the type of attack, number of attack attempts, and the time when the attack happened.
The dashboard also contains the Alerts Count Overview widget that displays the number of alerts triggered in a given time frame.

VPN Overview

You can customize the Dashboard tab to include the VPN Overview tab by navigating to Settings → Add Tab → VPN Overview. EventLog Analyzer monitors VPN session activities and generates reports to help you visualize events of interest. The VPN Overview dashboard will give you insights on VPN user and session activities by displaying widgets such as Live Sessions Count, Total Logon Hours, Average Login Time, Closed Sessions, and Top Users and Status. You can also customize the VPN dashboard by adding and reordering widgets by navigating to Settings → Add Widgets and Settings → Reorder Widgets respectively.

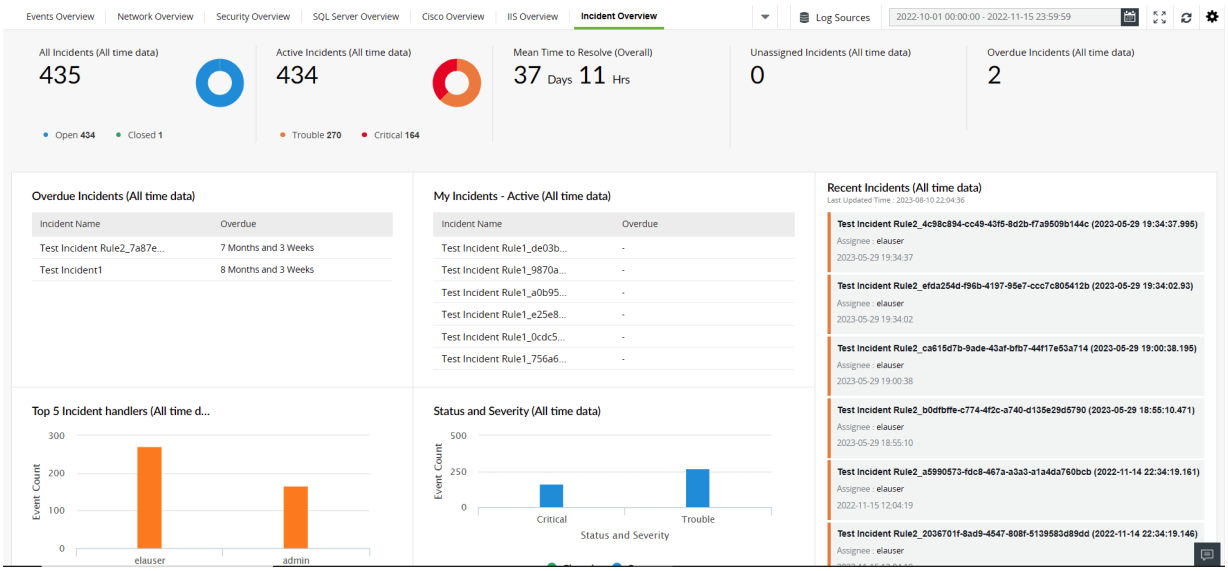


Incident Overview

This tab helps you effortlessly manage the security incidents detected. The dashboard gives you the count of all, active, unassigned and overdue incidents. It also provides the mean time to resolve. The dashboard provides insights such as:

- Overdue incidents's age.
- Personalized incident dashboard where the user can view the incidents assigned to them and their age.
- Top 5 incident handlers.
- The status and severity of the incidents detected.
- Trend graph for the incidents created and resolved.
- User-specific mean time to resolve the incidents.

> **Note**
>
> mean time to resolve refers to the average time taken to resolve an incident.



The Dashboard tab also contains the Log Sources, date and time selection, and settings icons.

Log Sources tab

When you click on the Log Sources tab, three tabs are displayed:

- Devices
- Applications
- File Integrity Monitoring

- File Integrity Monitoring

Devices

The Devices section displays the entire list of systems (Windows, Linux, IBM AS/400, HP-UX, etc.) and devices (routers, switches, etc.), from which EventLog Analyzer is collecting logs. The device list displayed is categorized based on the Device group selected from the drop-down list (default: All Groups). You can add a new device (+Device), or add and schedule new reports (+Schedule) from this section. You can search for a particular device based on its IP Address or Device Name, delete a device or set of devices, and disable/enable log collection from a particular device or set of devices.
The device list table displays details like device type, event summary (error, warning, failure, others), connection status of the device, time when the last log message was fetched, and device group to which the device belongs.
Moving the mouse over any device brings up some options:

- View the last 10 events collected from a particular device.
- Update the device details.
- Ping the device.
- Enable/disable log collection from the device.

You can even customize the columns you would like to display in the device table by clicking the column selector icon or increase the number of devices that are displayed per page (from a minimum of 5 devices per page to a maximum of 200 devices per page). Using the drop down menu, you can list out only the Active devices or Enabled devices and have the option to exclude synced devices from Active Directory Audit Plus.

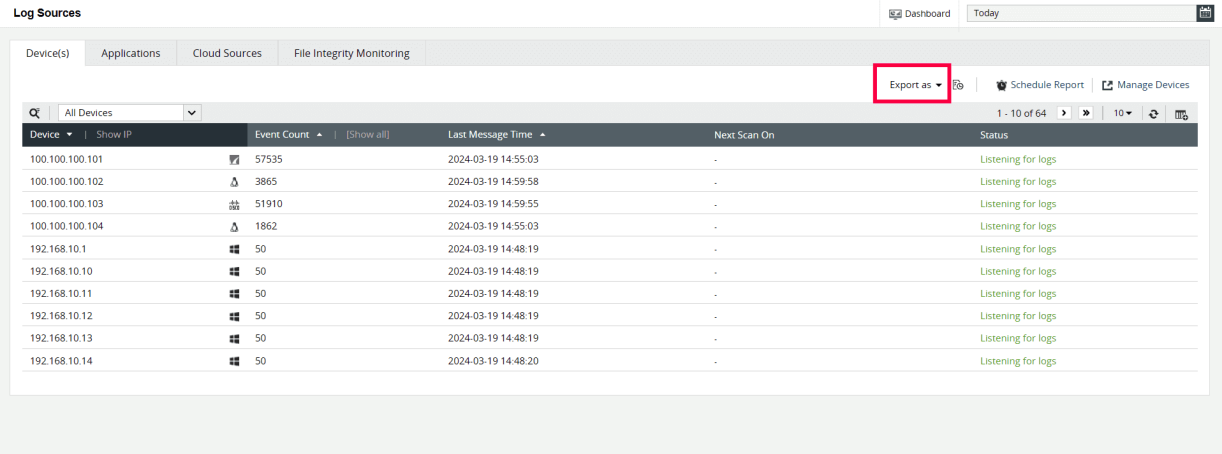
Scheduled Reports

EventLog Analyzer lets you schedule report generation, export, and redistribution over email.

1. Go to Dashboards → View All Devices.
2. To schedule a report, click Schedule Reports on the top right corner of the page.
3. Click on the +Create New Schedule button on the page. This will open the Create New Schedule page.
4. In the Create New Schedule window,
    - Schedule Name: Enter the name of the Schedule.
    - Select Log Sources: Add the Log Sources for which the schedule is for with the help of the + button.
    - Schedule Frequency: Specify the frequency at which reports need to be exported. The frequency can be 'Only Once', 'Hourly', 'Daily', 'Weekly', or 'Monthly'.
    - Export Time Range: Select the time range for which the report needs to be created and later exported along with the timing.
    - Report Format: Choose the file format in which the report needs to be exported i.e. PDF or CSV.
    - Email Address: Configure the email address to which the reports need to be sent.
    - Email Subject: Enter the subject of the mail that contains the exported reports.
5. Once you've entered the necessary details for the schedule, click Save to complete creating the report schedule.

You can also export the reports in PDF or CSV format with the Export as option. These generated reports will include device details such as the display name, IP address, total count, last message time, next scan time, and

include device details such as the display name, IP address, total count, last message time, next scan time, and device status.



Applications

The Applications section provides an overview pie-chart (which can be drilled down to raw log information) and lists the devices from which application logs for IIS W3C Web Servers, IIS W3C FTP Servers, MS SQL Servers, Oracle Live Audit, DHCP Windows/Linux Servers, Apache Web Servers or Print Servers, have been received or imported into EventLog Analyzer. The device list displayed is categorized based on Application Type selected from the drop-down list. Applications logs can be imported into EventLog Analyzer by selecting +Import from the Actions drop-down list.

The application device list displays details like device name, application type, total events, recent records, time imported, start time and end time. Click on the device name or the corresponding section in the pie chart to get the complete overview of the application event data, and generate corresponding reports. You can even customize the columns you would like to display in the application device table by clicking the column selector icon.

File Integrity Monitoring

The File Integrity Monitoring dashboard gives information about changes made to files and folders of Windows, Linux, and Unix machines. It tabulates and reports on the files and folders created, deleted, modified, and renamed. It also displays changes made to file and folder permissions.

At the top of this dashboard, you can find the Manage File Integrity Monitoring tab which allows you to add, delete, and manage devices for File Integrity Monitoring. The FIM Alert tab allows you to configure alerts for anomalous file and folder modifications. The FIM Scheduled Reports tab helps you view and export scheduled reports.

Date and time

You can generate and view all the audit reports for the required time frame using the date and time box provided.

Settings icon

The settings icon displays multiple options to customize all dashboards by adding, managing, and ordering the

widgets and tabs that are displayed. You can also refresh the changes made to the time frame in the product using the Refresh Interval option.

Reports tab

This tab displays a dashboard that contains reports for all events taking place in your network. At the top left corner, you can find a drop-down menu that allows you to choose and view reports based on Devices, Applications, File Monitoring, Threats, Vulnerability, and Virtual Machines. You can also view Custom Reports, User Based Reports, and Top and Trend reports by clicking on the required option from this drop-down menu. The Export As drop-down menu enables you to export reports in either the CSV or PDF formats. You can schedule reports by clicking on the +Add option present in the Schedule Reports tab.
On the left pane, you can find multiple pre-defined reports that are automatically generated when log sources are added to EventLog Analyzer. You can also create custom reports by clicking on the Manage Reports tab present at the lower-left corner of the screen. The Scheduled Reports tab allows you to view existing scheduled reports and export them as and when needed.

Compliance tab

The Compliance tab provides the set of canned reports as required by various compliance policies, namely, FISMA, PCI-DSS, SOX, HIPAA, GLBA, GPG, and ISO 27001:2013. The +Add option allows you to create and select the reports required for a new compliance policy of your choice. The Edit option allows you to customize the reports available under each compliance policy.

Search tab

The Search tab provides two options to search the raw logs: Basic Search or Advanced Search. The search result is displayed in the lower half of the page and the final search result can be saved as a report (in PDF or CSV format) and can also be scheduled to be generated at predefined intervals and be automatically mailed to a set of configured users.
You can use Basic search if you are interested in manually constructing the search query. Here you can use phrase search, Boolean search, grouped search, and wild-card search to build your search query. You can use Advanced search to interactively build complex search queries easily with field value pairs and relational operators. New fields can be extracted from the search result and regular expression (regex) patterns can be constructed to easily identify, parse and index these fields in new logs received by EventLog Analyzer.

Correlation tab

The Correlation engine analyzes logs collected from different parts of the network and generates alerts for suspicious patterns of events. The dashboard, by default, displays the report on Recent Incidents. You can create and modify correlation rules by clicking on the Manage Rules tab present in the dashboard.

Alerts tab

This tab displays the number of Active Alerts in the dashboard along with their severities. You can view tabulated information about the alerts, their time of generation, the status, and their corresponding response workflow (if configured) in the dashboard.

Settings tab

This section allows you to configure EventLog Analyzer as per your requirements. It has three sub-sections as given below:

Configuration Settings

This section allows you to Manage Devices, Device Groups, Application Sources, Import Log Data, Threat Sources, File Integrity Monitoring, Vulnerability Data, FIM Templates, and vCenter. You can also configure threat management and log forwarding from this section.

Admin Settings

This section allows you to perform various administrative activities by managing Alert Profiles, Archives, Technicians and Roles, DB Retention Settings, Log Collection Filters, Working Hour Settings, Product Settings, Log Collection Failure Alerts, Dashboard profiles, Privacy Settings, Logon Settings, Domain and Workgroups, Report Profiles, Resource Grouping, Custom Log Parsers, Tags, and Log360 Cloud platform.

System Settings

This section can allow you to configure various settings including Notification Settings, System Diagnostics, Database Access, Re-branding, NT Service, Connection Settings, and Listener Ports.

Add tab

This tab allows you to easily add log sources from Devices and Applications. It also has the provision to let you import logs from other sources. You can add Alert Profiles, Log Filters and create custom Reports from this tab.

8.2.2. Predefined tabs and widgets

Last updated on: September 12, 2025

In this page

Overview

Dashboard tabs

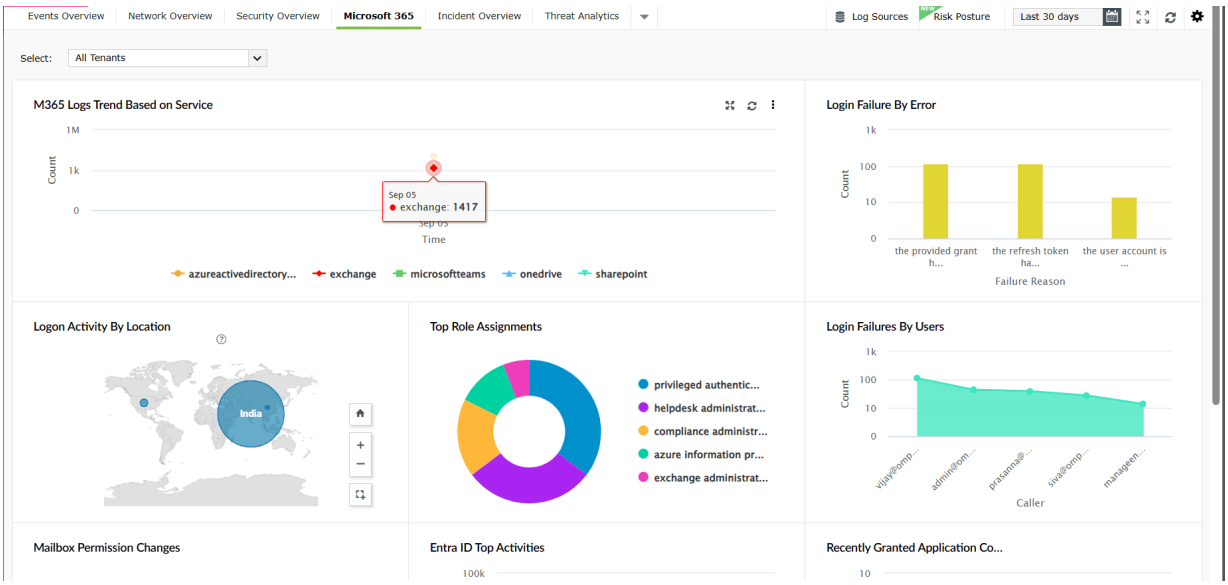
Overview

The Log360 dashboard provides a near real-time view of security-related data through graphs and charts. It helps you identify anomalies, analyze threats and attack patterns, and understand log trends at a glance. The dashboard is organized into tabs, each containing widgets that present specific security information.This guide explains the purpose of each dashboard tab and describes how the widgets help visualize key security data.

Dashboard tabs:

The dashboard comes with the following default subtabs:

- Events Overview
- Network Overview
- Security Overview
- M365
- Incident Overview
- Threat Analytics
- Detection Overview
- AD Audit



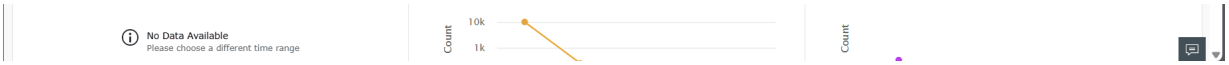


Figure 1: Navigating to the dashboard

Each tab comprises numerous widgets.

Events Overview

This tab presents an overview of various key events monitored by the product console. The widgets in this dashboard provide insights on the various critical events generated in the network within the specified time frame.

The Events Overview tab has the following widgets:

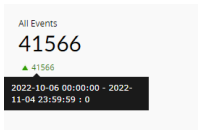
Widget Name	Function	Widget image
All Events	This widget presents the total number of events/logs collected by the SIEM module within the given time frame.	
Windows Events	This widget presents the total number of Windows-based events collected by the SIEM module within the chosen time frame. In addition to that, the pie chart splits the Windows Events into error events, failure events, and warning events. Success/info events are filtered and not displayed.	
Syslog Events	This widget presents the total number of Syslog events collected within the given time frame. Furthermore, the pie chart splits the syslog events into warning, error, and critical events.	
All Devices	This widget provides a count of all the enabled devices from which log data is being collected. The server image in the corner will have a green tick if all logs are being collected successfully. A warning icon indicates that logs aren't being collected from some of the devices. Additionally, this widget has a View All Devices link. Clicking on the link will redirect you to the device dashboard page, which will provide detailed information of each device. Clicking on All Device will take you to the Devices tab, from where you can create a new list of Scheduled Reports	 
Logs Trend	This widget presents a time-based log count trend of all events/logs ingested into the SIEM module. The X-axis represents the time range, which is based on the calendar range you choose. If you choose the time range as less than 24 hours, then the graph will present you with hourly log trend data. The Y-axis represents the Event Count.	

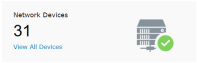
Widget Name	Function	Widget image
Top 5 Devices	This widget presents the top 5 devices based on event count.	
Recent Alerts	This widget presents the 50 most recent alerts for the given time range.	
Security Events	This widget shows a summary of various security events such as Logon, Account Logon, Account Management, and Object Access.	
Windows Severity Events	This widget displays a graph in which the X-axis represents the Severity of a Windows Event and the Y-axis represents the Event Count.	
Syslog Severity Events	This widget displays a graph in which the X-axis represents the Severity of a Syslog Event and the Y-axis represents the Event Count.	
Top 5 File Integrity Monitoring Events	This widget presents a 3D graph which displays the details of the top 5 file servers based on the log count. Each row contains additional data of various file-based events.	
Application Events	This widget displays a pie chart of the top 10 applications like IIS, DHCP etc based on event count.	

Network Overview

This tab gives an overview of various network-related events monitored by generating graphical reports. The widgets in this dashboard provide insights on the various critical events generated in the network within the specified time frame.

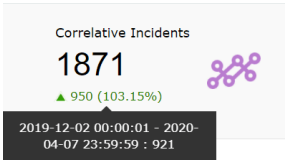
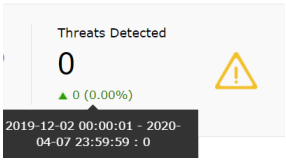
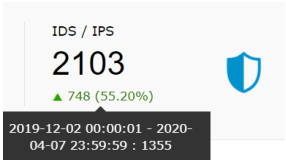
The Network Overview tab has the following widgets:

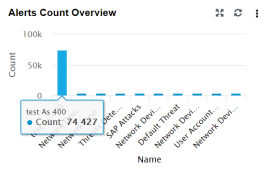
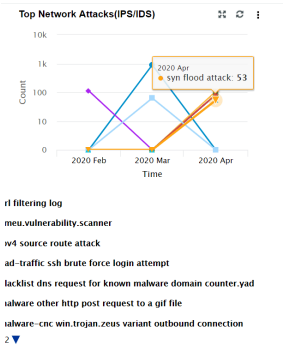
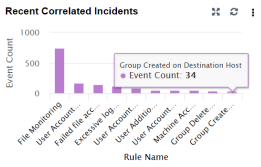
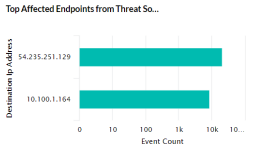
Widget Name	Function	Widget image
All Events	This widget presents the total number of network-based events collected by the SIEM module within the given time frame. Network-based events refer to events collected from network devices such as firewalls, switches, and routers.	
Allowed Connections	This widget presents the count of all the connections that were allowed by the network device. The pie chart highlights the allowed connections from the total number of connections that occurred in the network within the specified time	

Widget Name	Function	Widget image
Denied Connections	This widget presents the count of all the connections that were denied by the network device. The pie chart highlights the denied connections from the total number of connections that occurred in the network within the specified time.	
Network Devices	This widget provides a total count of network devices that are added for monitoring.	

Security Overview

This tab provides an overview of the key security events monitored. The widgets in this dashboard provide insights on the various critical events generated in the network within the specified time frame.
The Security Overview tab has the following Widgets:

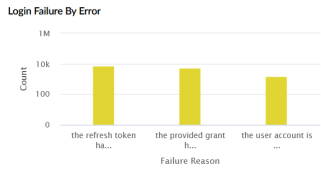
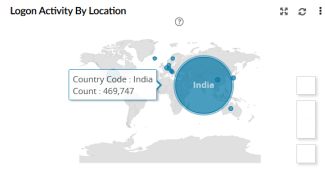
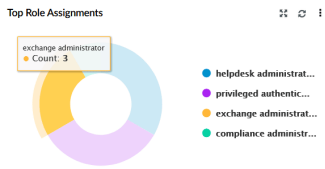
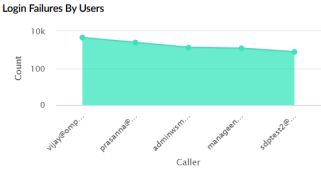
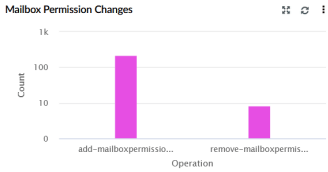
Widget Name	Function	Widget image
Correlative Incidents	This widget refers to the number of incidents detected via SIEM module's correlation engine.	
Threats Detected	This widget shows the logs from Threat Sources that are identified as threats by the SIEM module. These logs are selected based on predefined detection rules.	
Vulnerabilities	This widget displays the total number of vulnerabilities detected by the vulnerability scanner(s) whose data are being imported into SIEM module.	
IDS/IPS	This widget presents the total count of IDS/IPS events within the chosen time frame.	
Threats from Threat Sources	This widget presents the total number of threats from the configured Threat Sources (such as Symantec, McAfee, Malwarebytes etc) within the	

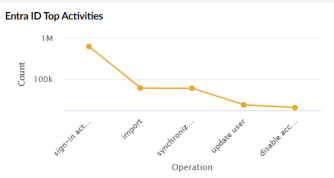
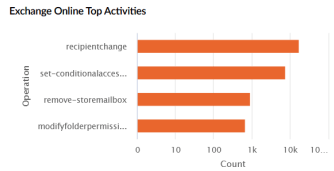
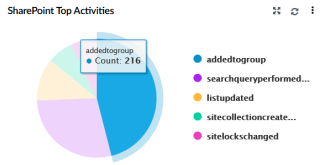
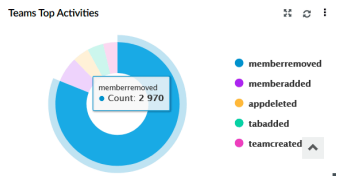
Widget Name	chosen time frame. Function	Widget image
Alert Count Overview	This widget provides an overview of each configured alert profile. The X-axis denotes the alert profile, and the Y-axis denotes the count.	
Top Network Attacks (IPS/IDS)	This widget includes a graph showing a time based trend for IDS/IPS events. The X-axis represents the time range. It will be based on the calendar range you choose. The Y-axis represents the event count, and the Z-axis represents the IDS/IPS event type. Top 10 events are displayed based on the event count.	
Recent Threats Identified	This widget displays the most recent 50 threats based on the calendar range.	
Recent Correlated Incidents	This widget is similar to Alert Count Review. It provides an overview of the recent correlated incidents. The X-axis denotes the correlation rule, and the Y-axis denotes the event count.	
Top Affected Endpoints from Threat Sources	This widget shows the Top 5 endpoint devices in which threats were detected by Threat Sources (Symantec, McAfee, etc)	
Top Vulnerabilities from Vulnerability Scanners	This widget includes a pie chart that displays the top 5 vulnerabilities (selected on the basis of event count) detected in endpoint devices by the vulnerability scanner.	

Microsoft 365

This tab provides an overview of activities and security events from various Microsoft 365 services. The widgets in this dashboard help you monitor login activity, role assignments, service usage, and activity trends across Exchange Online, SharePoint, Teams, OneDrive, and Entra ID.

The M365 Overview tab has the following widgets:

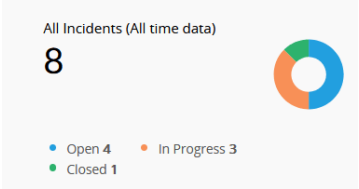
Widget Name	Function	Widget image
M365 Logs Trend Based on Service	Displays the total number of logs received from M365 services (Microsoft Entra ID, Exchange Online, Teams, OneDrive, and SharePoint) over the selected time period. The X-axis represents the time range, and the Y-axis represents the log count.	
Login Failure by Error	Shows failed login attempts categorized by error type, along with their count. The X-axis represents the failure reason, and the Y-axis represents the count.	
Logon Activity by Location	Displays a world map of user login activity by country, highlighting the geographic distribution of sign-ins. Each circle corresponds to the logon count.	
Top Role Assignments	Lists the most assigned roles in the organization, such as global administrator.	
Login Failures by Users	Shows the number of login failures per user within the chosen time range. The X-axis represents users, and the Y-axis represents the failure count.	
Mailbox Permission Changes	Displays mailbox permission modifications performed by users specifically add and remove operations. The X-axis represents the type of operation, and the Y-axis represents the count.	

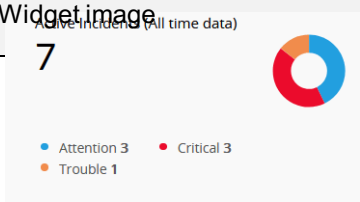
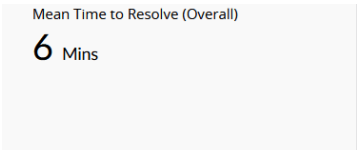
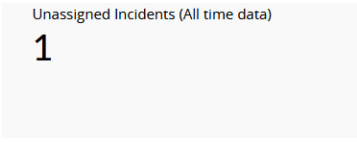
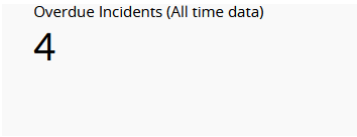
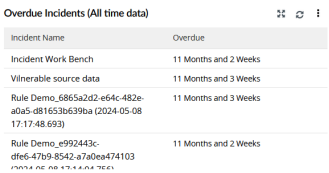
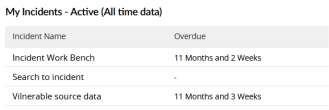
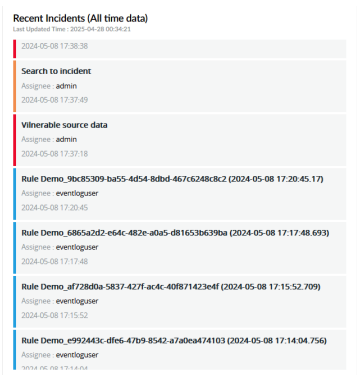
Widget Name	Function	Widget image
Entra ID Top Activities	Shows the most common operations performed in Entra ID such as sign-in activity, import, synchronize, update user, and disable account. The X-axis represents the operation type, and the Y-axis represents the count.	
Recently Granted Consent Applications	Displays applications to which users or admins recently granted consent. The X-axis represents the application name, and the Y-axis represents the permission grant count.	
Exchange Online Top Activities	Lists the top Exchange Online operations performed. The X-axis represents the operation, and the Y-axis represents the count.	
SharePoint Top Activities	Displays a pie chart of the top SharePoint activities such as group additions, search queries, list updates, and site creation.	
Teams Top Activities	Displays a pie chart of the top Teams operations such as member added/removed, team creation, app added, and tab added.	

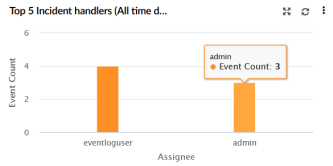
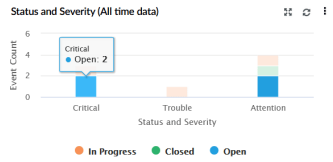
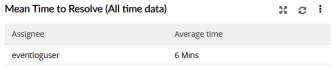
Incident Overview

This tab presents an overview of various security incidents. The widgets in this dashboard provide insights on the various critical incidents detected in the network within the specified time frame.

The Incident Overview tab has the following Widgets:

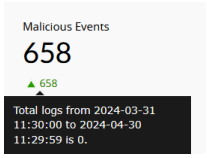
Widget Name	Function	Widget image
All Incidents (All time data)	This widget displays the total number of incidents raised till date, categorized by status: Open (blue), In Progress (orange), and Closed (green).	

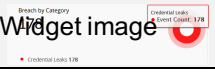
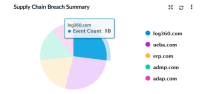
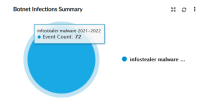
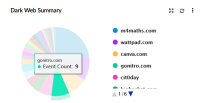
Widget Name	Function	Widget image
Active Incidents (All time data)	This widget represents incidents that are currently Open or In Progress, categorized based on severity: Attention (blue), Trouble (orange), and Critical (red).	
Mean Time to Resolve (Overall)	This widget displays the average time taken to resolve incidents from the time they were created.	
Unassigned Incidents (All time data)	This widget indicates the number of incidents that have not yet been assigned to any user.	
Overdue Incidents (All time data)	This widget shows the count of incidents that have passed their expected resolution date. This helps track unresolved tasks beyond due dates.	
Overdue Incidents (All time data)	This widget displays a table listing the names of overdue incidents along with their overdue duration.	
My Incidents - Active (All time data)	This widget displays active incidents specifically assigned to the current user, along with overdue details.	
Recent Incidents (All time data)	This widget lists the 50 most recent incidents created, including incident name, assignee, and timestamp.	

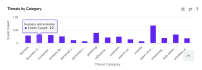
Widget Name	Function	Widget image
Top 5 Incident Handlers (All time data)	This widget represents a bar chart that shows the top 5 users (assignees) based on the number of incidents they are handling. X-axis represents the Asignee, Y-axis shows Event Count.	
Status and Severity (All time data)	This widget represents a bar chart displaying incidents based on both their status (Open, In Progress, Closed) and severity (Critical, Trouble, Attention). X-axis represents Status and Severity, and Y-axis represents Event Count.	
Incident - Created vs Resolved	This widget represents a line graph comparing the number of incidents created (yellow) versus those closed (green) over time. X-axis represents Time, Y-axis representsCount.	
Mean Time to Resolve (All time data)	This widget represents a table showing the average resolution time for each assignee.	

Threat Analytics

This tab presents an overview of various threat-related activities monitored. The widgets in this dashboard provide insights on the various critical threats identified in the network within the specified time frame.
The Threat Analytics tab has the following Widgets:

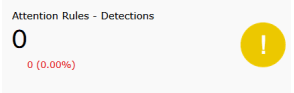
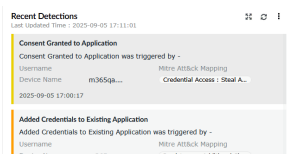
Widget Name	Function	Widget image
Malicious Events	This widget displays the total number of events flagged as malicious based on the threat feeds from the configured threat sources like STIX/TAXII and ATA threat servers.	
Supply Chain Breaches	This widget displays the number of breaches attributed to third-party applications or vendors, helping assess external risk exposure through the supply chain.	

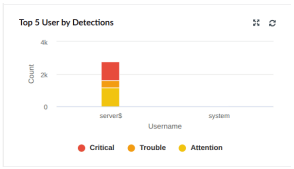
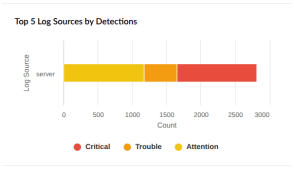
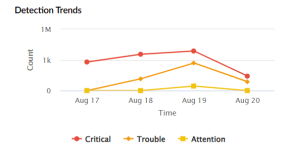
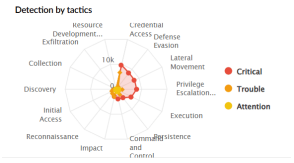
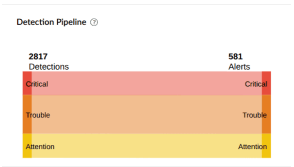
Widget Name	Function	Widget image
Breach by Category	This widget categorizes breaches by the type of data exposed, such as Credential Leaks or Personal Info Leaks, giving insights into the nature of the stolen data.	
Breach by Sourcetype	This widget presents breaches based on their origin, which can be either from Botnet or Breach. Botnet refers to breaches caused by malware infections, while Breach refers to data exposed on the dark web through unknown sources.	
Breach Event Trends	This widget represents a time-based graph showing the frequency of botnet and breach-related events over the selected date range. The X-axis represents the time range, which is based on the calendar range you choose. If you choose the time range as less than 24 hours, then the graph will present you with hourly log trend data. The Y-axis represents the Count.	
Supply Chain Breach Summary	This widget represents a pie chart showing the distribution of breaches across affected third-party services or vendors, offering insight into which external platforms are most compromised.	
Recent Threats	This widget is a real-time feed of the recent threat alerts, both from dark web sources and malicious event detections.	
Botnet Infections Summary	This widget represents a pie chart summarising botnet-related activity by malware type.	
Dark Web Summary	This widget represents a pie chart of leaked data detected across various dark web sources.	
Data Leaked in Dark Web	This widget represents a bar chart displaying the volume of leaked data found on the dark web. X-axis represents the breached source domains, and Y-axis indicates the count of leaked data instances. It distinguishes between Personal Info Leaks (orange) and Credential Leaks (red)	

Widget Name	Function	Widget image
Data Leaked by Botnet Infections	This widget represents a bar chart summarising data leaked specifically due to botnet malware. The X-axis shows the malware type, while the Y-axis represents the count of leaked credentials.	
Top Attacked Host	This widget displays a bar graph listing the most frequently targeted devices. X-axis represents the IP addresses or device names, and Y-axis shows the Event Count.	
Threats by Category	This widget displays a bar chart of malicious events, comparing them based on their threat category. The X-axis lists threat types (e.g., phishing, botnets), while the Y-axis represents the event count, providing insights into which threats have occurred most frequently.	

Detection Overview

The tab provides a centralized view of detections across your environment. It helps security teams monitor threats, analyze patterns, and prioritize incidents using real-time visuals and context-driven insights.

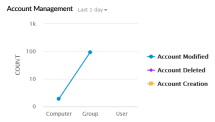
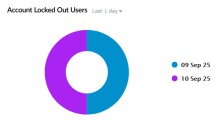
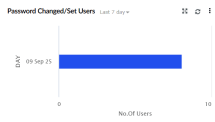
Widget Name	Function	Widget image
All Rules - Detections	Displays the total number of detections triggered by all rules within the selected time frame.	
Critical Rules - Detections	Shows the total number of detections triggered by rules categorized as Critical during the selected time frame.	
Trouble Rules - Detections	Shows the total number of detections triggered by rules categorized as Trouble during the selected time frame.	
Attention Rules - Detections	Shows the total number of detections triggered by rules categorized as Attention during the selected time frame.	
Recent Detections	Lists the most recent detections triggered, along with details such as rule name, username, device	

Widget Name	Function	Widget image
	name, and mapped MITRE ATT&CK tactic.	
Top 5 Users by Detections	Shows the top five users who have generated the highest number of detections, further categorized by severity.	
Top 5 Log Sources by Detections	Displays the top five log sources based on detection count, categorized by severity.	
Top 10 Detections by Rules	Highlights the ten rules that triggered most frequently within the selected time range. The X-axis represents rule identifiers, and the Y-axis shows the detection count.	
Detection Trends	Provides a time-based view of detections. The X-axis represents the time period selected, while the Y-axis shows the count of detections categorized by severity.	
Detection by Tactics	Displays a radar chart of detections mapped to MITRE ATT&CK tactics such as Credential Access, Persistence, Defense Evasion, etc. You can filter by severity.	
Detection Pipeline	Summarizes detections based on severity and shows how many alerts were triggered for each severity type.	

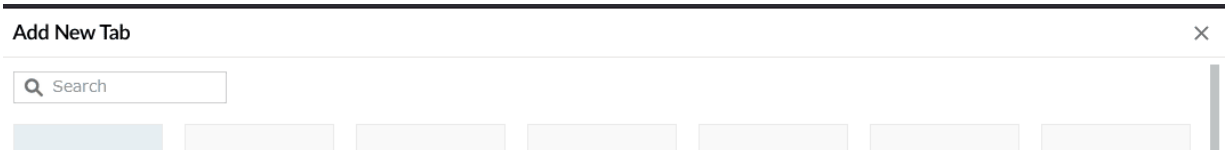
AD Audit

This tab provides an overview of Active Directory logon activities, account changes, GPO modifications, and password resets. The widgets in this dashboard help administrators detect logon anomalies, track object modifications, and monitor account lockouts within the AD environment.

The AD Audit tab has the following widgets:

Widget Name	Function	Widget image
Top User Logon Failures	Displays the users with the most failed logon attempts within the selected time range. The X-axis represents the User Name, and the Y-axis represents the Count of failed logons.	
Account Management	Tracks account-related operations across users, groups, and computers. This includes account creation, deletion, and modification. The X-axis represents the Object Type (User, Group, Computer), and the Y-axis represents the Event Count.	
Logon Failures - Error Code	Categorizes logon failures by error type such as invalid username and invalid password. The X-axis represents the Error Code, and the Y-axis represents the Count.	
Logon Peak Hour Usage	Shows logon activity trends by time of day. The X-axis represents the Hour of the Day, and the Y-axis represents the Logon Count.	
Account Locked Out Users	Displays users whose accounts were locked due to repeated failed login attempts during the selected time period.	
Password Changed/Set Users	Tracks user password resets and change attempts. The X-axis represents the Type of Operation (Password Set, Password Change Attempt), and the Y-axis represents the Number of Users.	
ADFS Logon History	Displays logon activity for Active Directory Federation Services. The X-axis represents the Hour of the Day, and the Y-axis represents the Logon Count, categorized into successful and failed attempts.	

In addition to the above, there are multiple predefined templates available for dedicated monitoring. Select the ⚙ icon and click Add tab to view the list of tabs available.



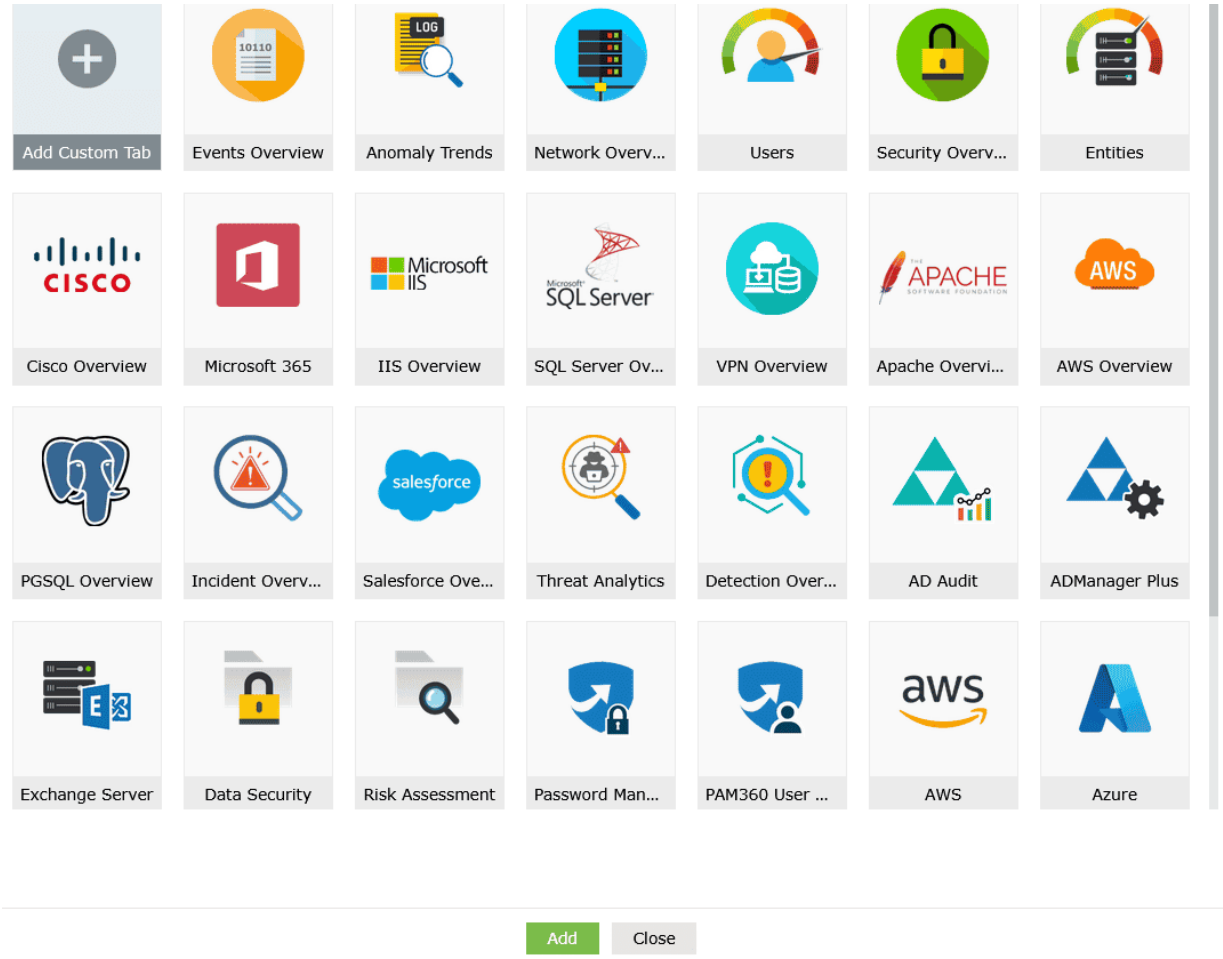


Figure 2: Viewing pre-defined tabs

Read also

This page explained about the predefined dashboard tabs and widgets in Log360. To learn how to customize dashboards and manage widgets, refer to the following documents:

- Customize Dashboard Views

8.2.3. Customize Dashboard Views

Last updated on: September 12, 2025

In this page

- Overview
- Filtering data by time range
- Adding a new tab
- Adding a new widget to a tab
- Editing, deleting, and reordering tabs
- Reordering and resizing widgets
- Editing and deleting widgets
- Viewing the dashboard in full screen mode
- Viewing a widget in full screen mode
- Refreshing the dashboard and widgets
- Changing refresh interval
- Configuring Embed links for dashboard and widgets
- Managing Embed Links

Overview

Customizing the Log360 SIEM dashboard lets you tailor the view to highlight the data most relevant to your log sources.You can add, remove, or reorder tabs and widgets, and modify layout options to create a personalized dashboard that streamlines monitoring and improves visibility. The dashboard is populated using the data collected from various log sources. Click Log Sources on the top-right corner of the dashboard to view the list of devices, applications, and monitored files from which the data is being collected.

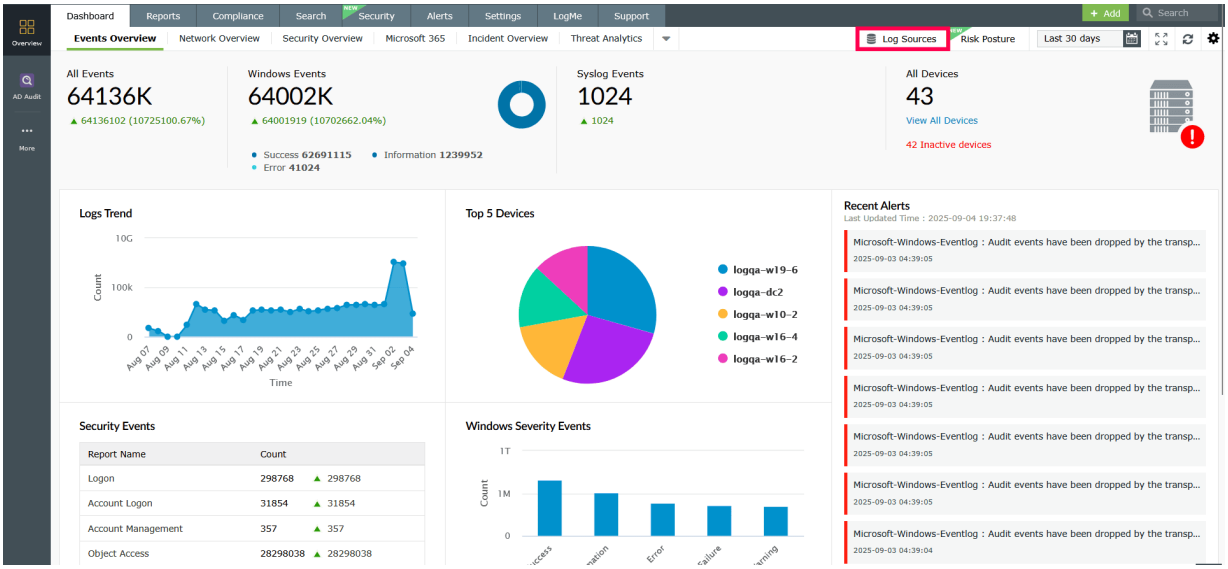




Figure 1: Accessing Log Sources in the dashboard

This page explains the customization options available and how they can be used to tailor a dashboard that fits your monitoring needs.

Filtering data by time range

You can filter the data displayed on the dashboard by selecting a time range.

1. In the top-right corner of the dashboard, click the drop-down.
2. Choose from predefined options such as Today, Yesterday, Last 7 days, Last 30 days, This month, Last month.

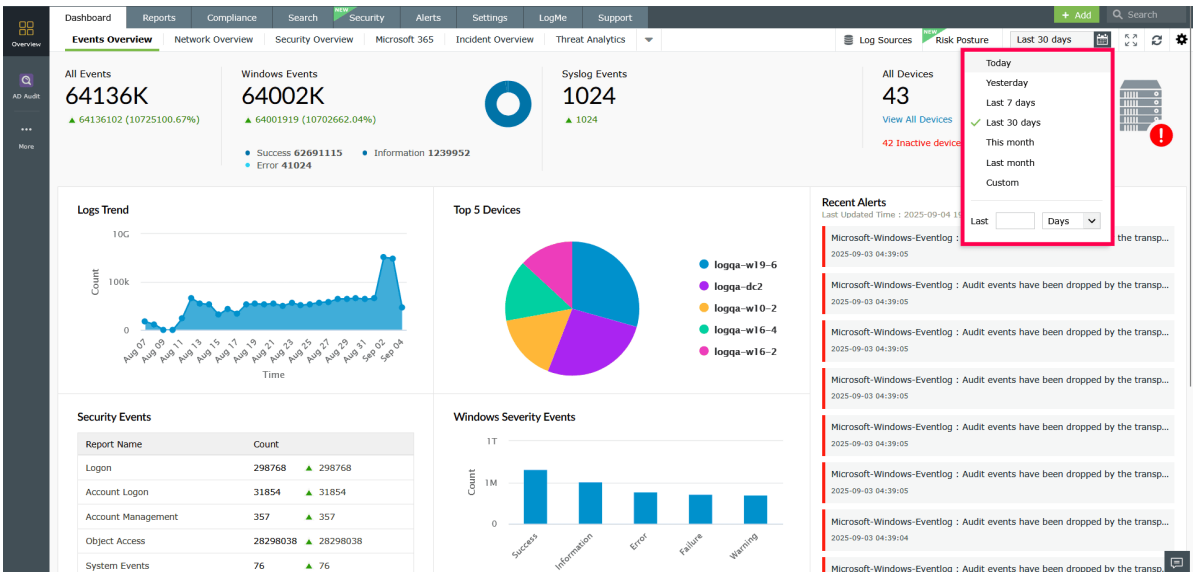


Figure 2: Selecting a time range

3. To define your own range, select Custom and specify the From and To dates and times using the calendar and time fields.

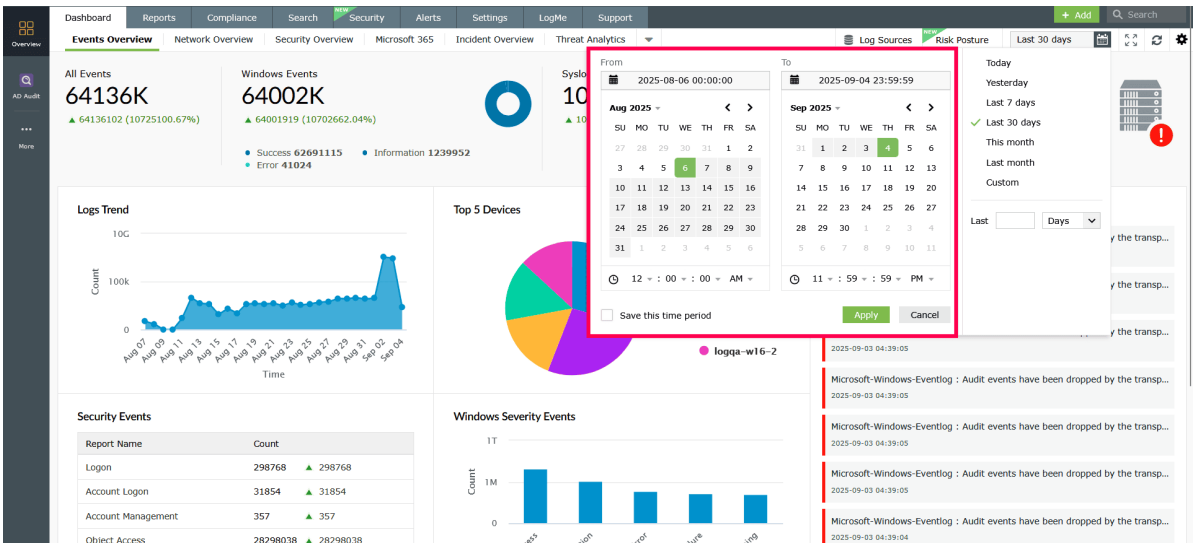




Figure 3: Selecting a time range

4. Alternatively, you can use the Last field to set a relative time range.
5. Click Apply to update the dashboard data for the selected period.

Adding a new tab

To add a new tab to the dashboard,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Add Tab.

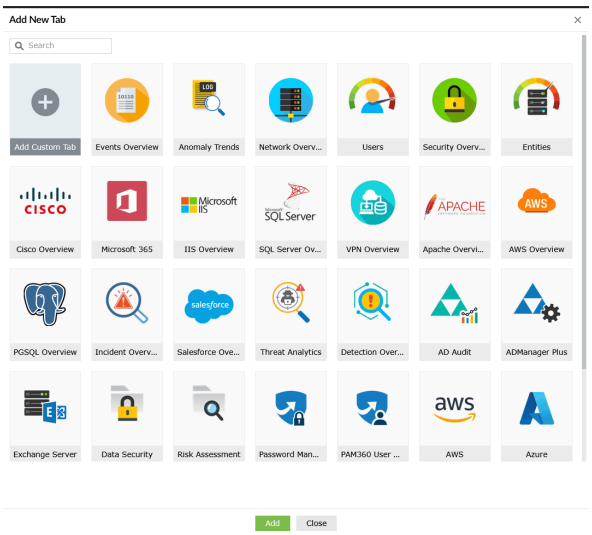
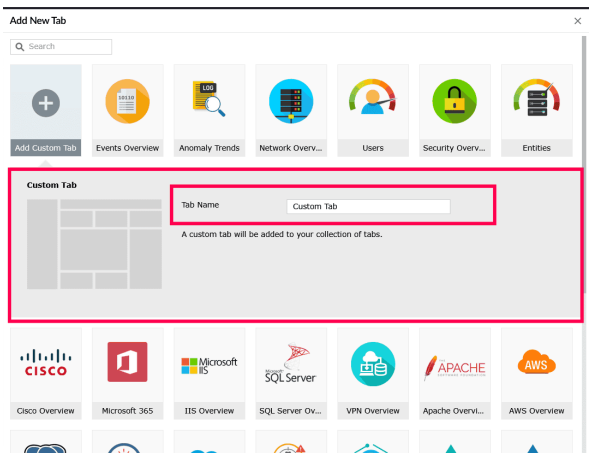


Figure 4: Adding a New Tab in the dashboard

2. In the pop-up box that appears, you can see the following:
3. Default tabs: Events Overview, Network Overview, Security Overview, M365 Overview, Incident Overview, Detection Overview, Threat Analytics, and AD Audit.
4. Other predefined templates
5. Add Custom Tab option
6. Click Add Custom Tab. Enter a name for the tab in the given field and click Add.



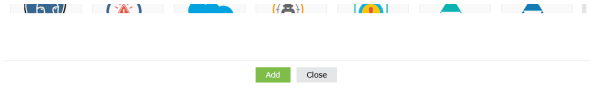


Figure 5: Adding a Custom Tab

Adding a new widget to a tab

To add a new widget,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Add Widgets.
2. In the Add New Widget window, choose a component from the Select Component drop-down.

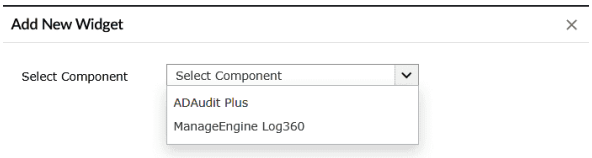


Figure 6: Selecting a component

3. Specify the widget, widget type, chart type, chart color, and provide a display name for the widget.

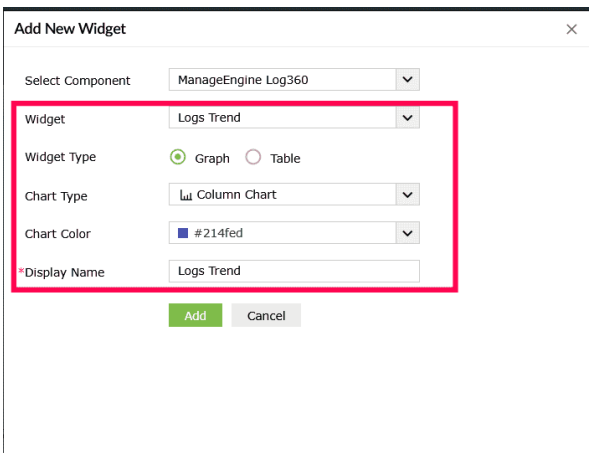


Figure 7: Configuring a New Widget in the dashboard

4. Once configured, select Add to save the widget.

Editing, deleting and reordering tabs

To delete tabs from the dashboard,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Manage Tabs.

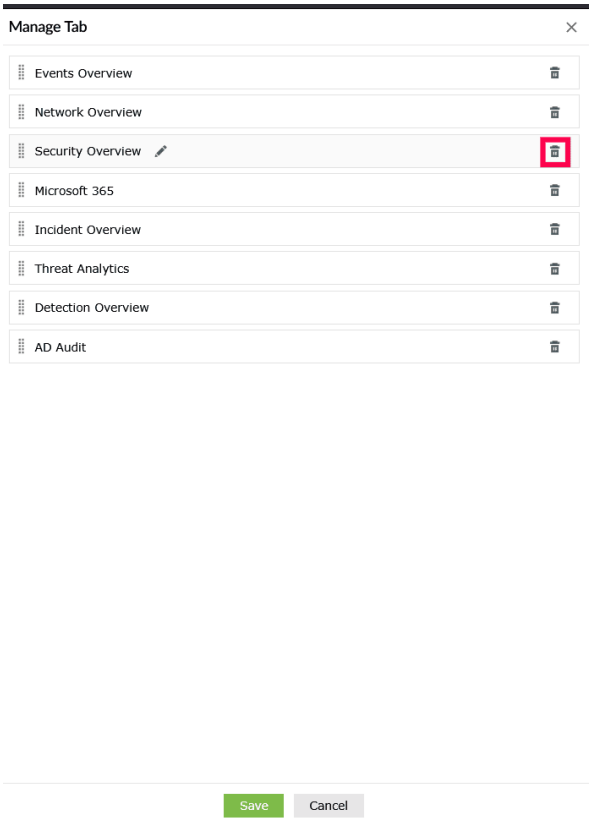


Figure 8: Deleting tabs in the dashboard

2. In the Manage Tab dialog box that appears, click the 🗑 icon corresponding to that tab that you want to delete.
3. In the pop-up confirmation box, click Yes to confirm the deletion of the tab.
4. Click Save to apply the changes to the dashboard.

To reorder the tabs in the dashboard,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Manage Tabs.
2. Click the ⣿ icon and drag and drop the tabs in the order of your choice.
3. Click Save to apply the changes to the dashboard.

To edit a dashboard tab:

1. In the dashboard, click the ⚙ icon on the top-right corner and select Manage Tabs.
2. Hover over the tab you want to edit and click the edit icon.

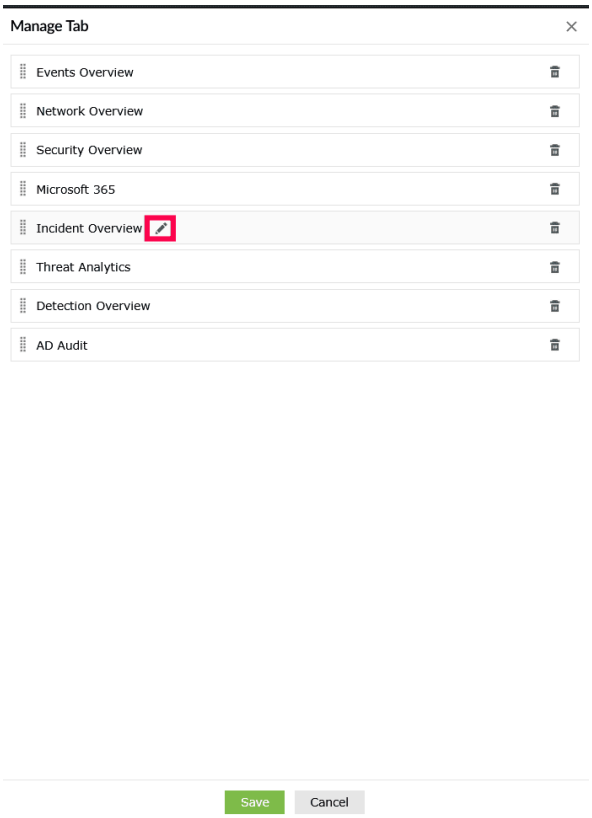


Figure 9: Editing a dashboard tab

3. Modify the tab name and click the ✓ icon to confirm.

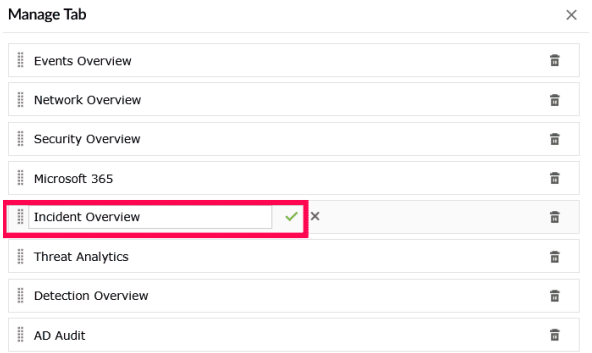




Figure 10: Modifying the tab name

4. Click Save to apply the changes to the dashboard.

Reordering and resizing widgets

To reorder the widgets in a tab,

1. In the dashboard, go to the tab containing the widgets you want to reorder.
2. Click the ⚙ icon on the top-right corner and select Reorder Widgets.

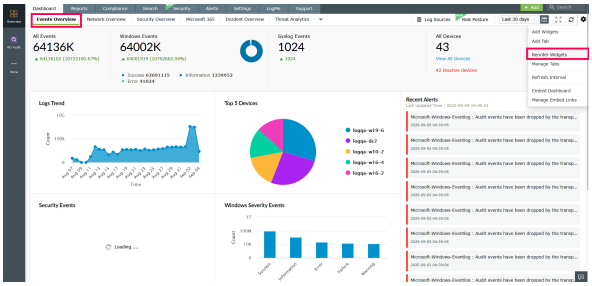


Figure 11: Reordering widgets in the dashboard

3. Click and drag the widgets to your desired positions.
4. Click Save in the top-right corner to apply the changes to the dashboard.

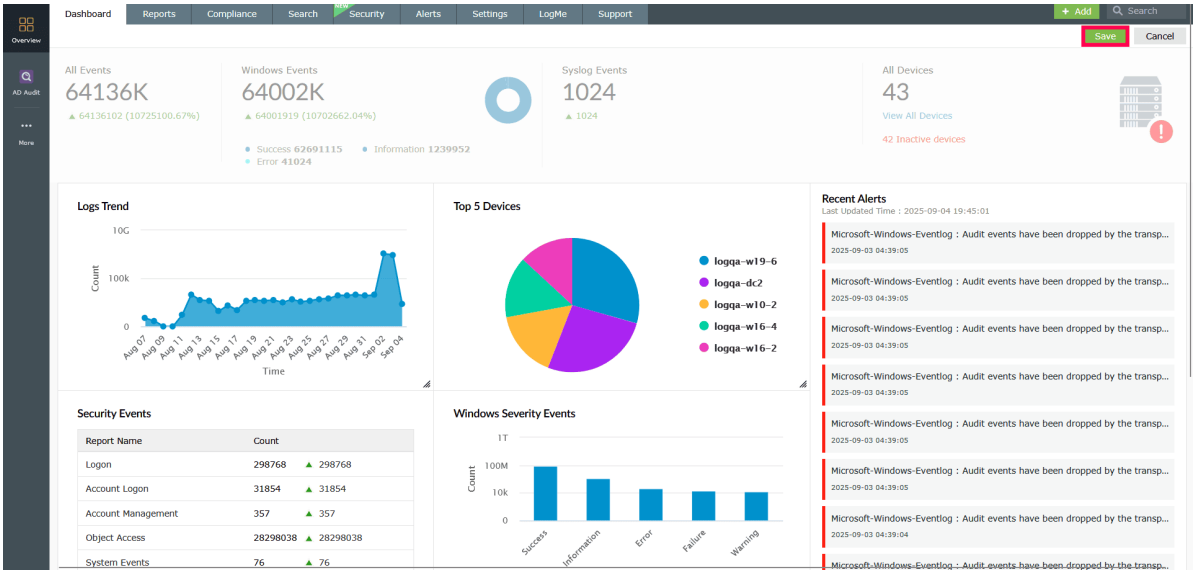


Figure 12: Saving changes to the dashboard

To resize the widgets in a tab

1. In the dashboard, navigate to the tab whose widgets you want to resize.
2. Click the ⚙ icon on the top-right corner and select Reorder Widgets.
3. Hover over the widget you want to resize, click the ⇲ icon, and drag from the bottom-right corner to adjust the size as needed.
4. Click Save in the top-right corner to apply the changes to the dashboard.

Editing and deleting widgets

To edit a widget in a tab,

1. In the dashboard, click the ⋮ icon and select Edit Widget corresponding to the widget that you want to edit.

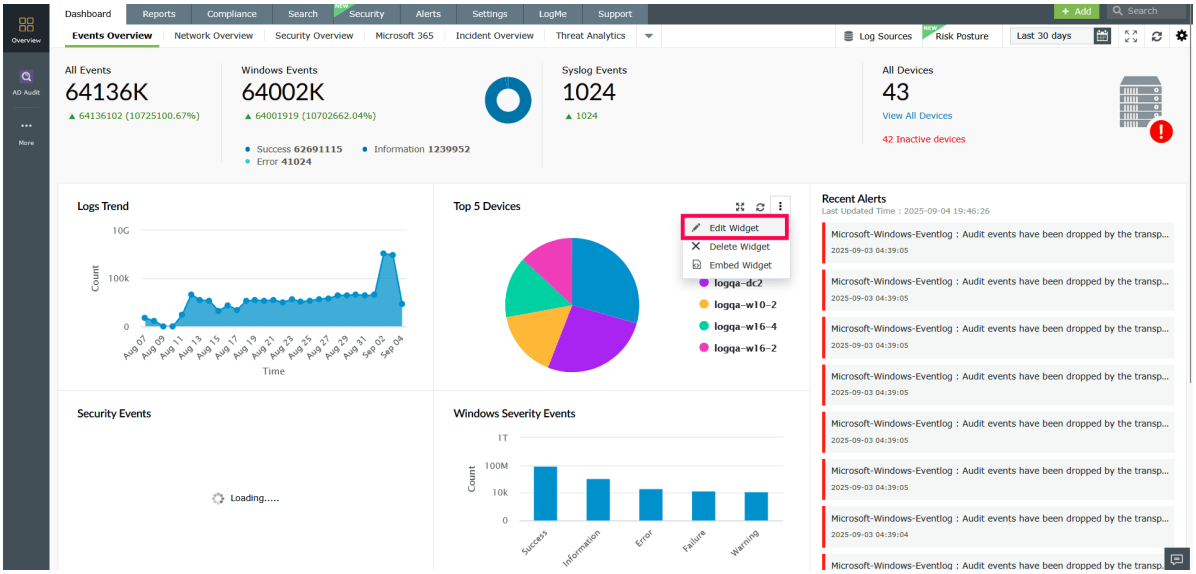


Figure 13: Editing a widget

2. Update the necessary information and click Update.

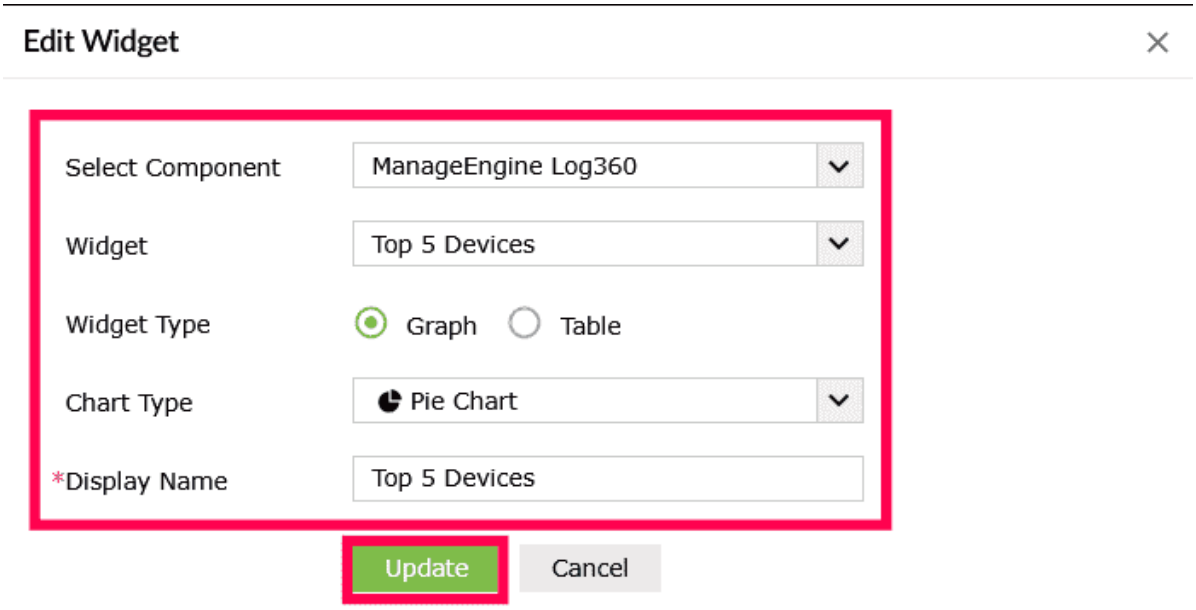


Figure 14: Editing a widget

To delete a widget from a tab,

1. In the dashboard, click the ⋮ icon corresponding to the widget that you want to delete.
2. Select Delete Widget.

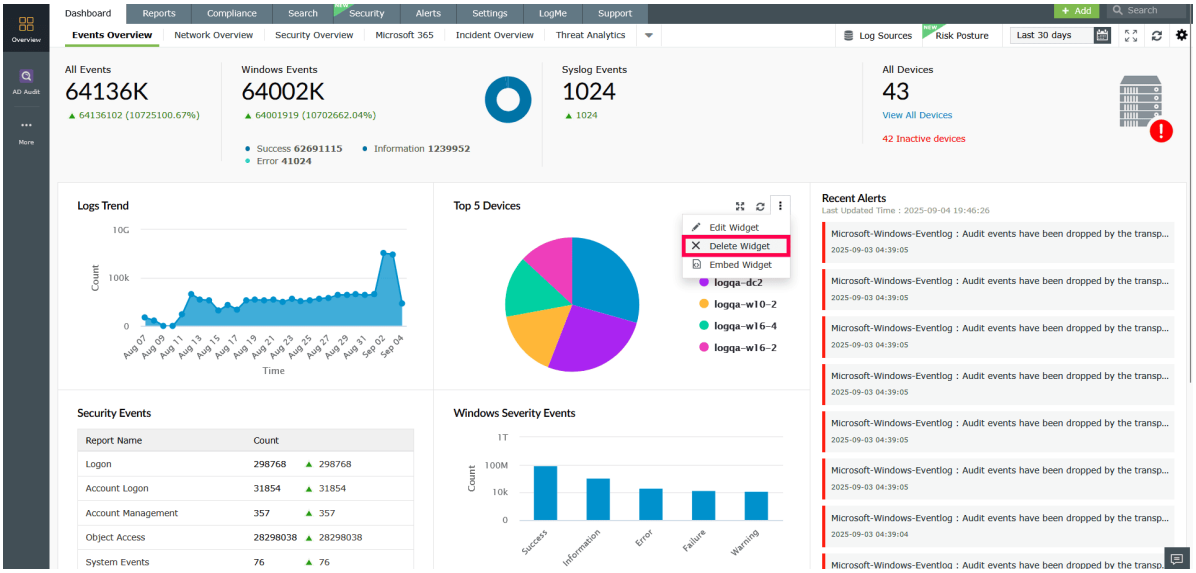


Figure 15: Deleting a widget

3. Click Yes in the pop-up box to complete the deletion.

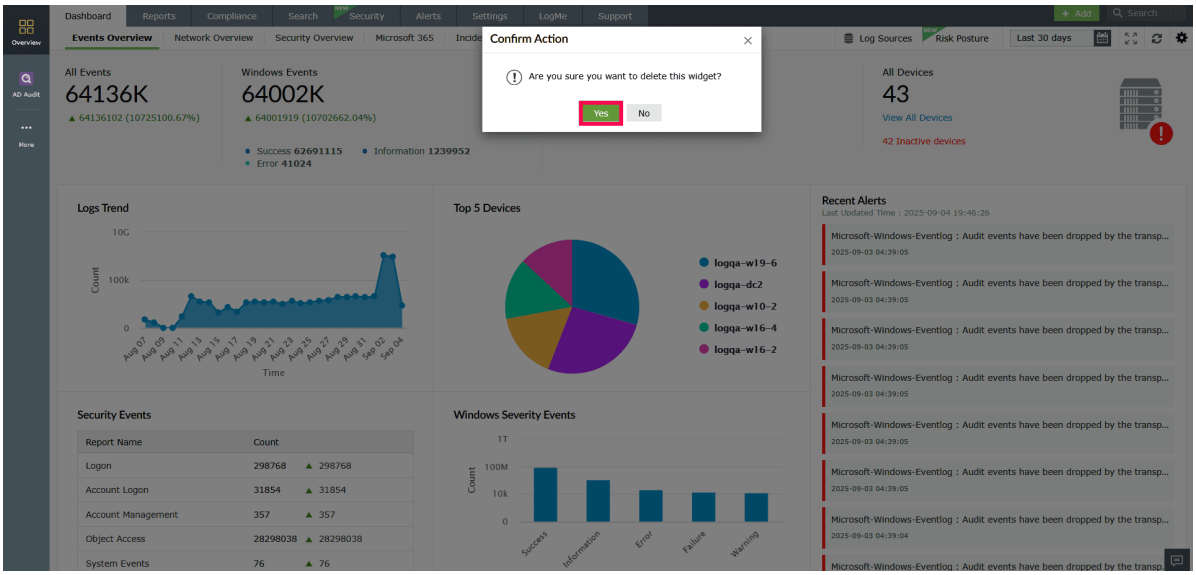


Figure 16: Confirming deletion of a widget

Viewing the dashboard in full screen mode

To view the dashboard in full screen,

1. In the dashboard, click the icon on the top-right corner.

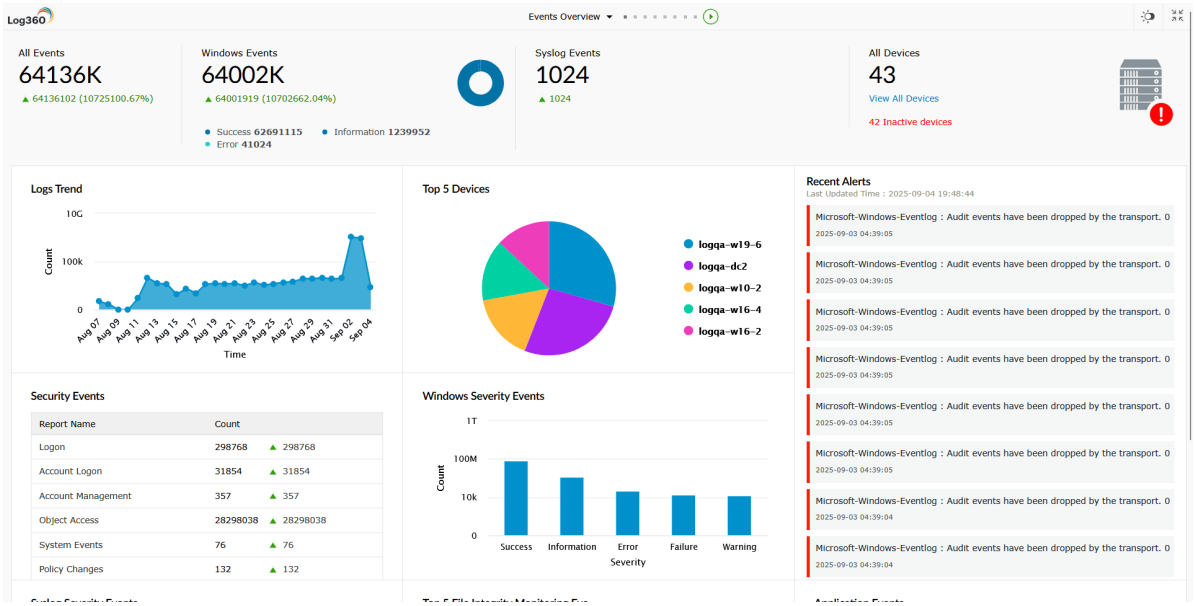
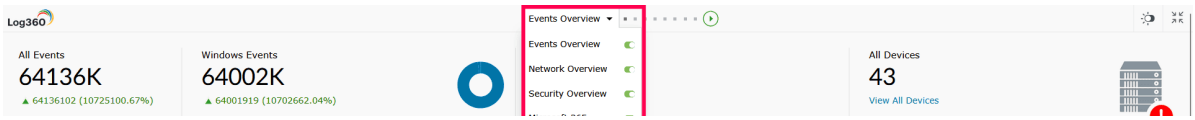


Figure 17: Viewing the dashboard in full screen mode

2. To start a slideshow of the tabs, click the play icon at the top of the screen.

3. To switch between tabs, click the drop-down button at the top of the screen.



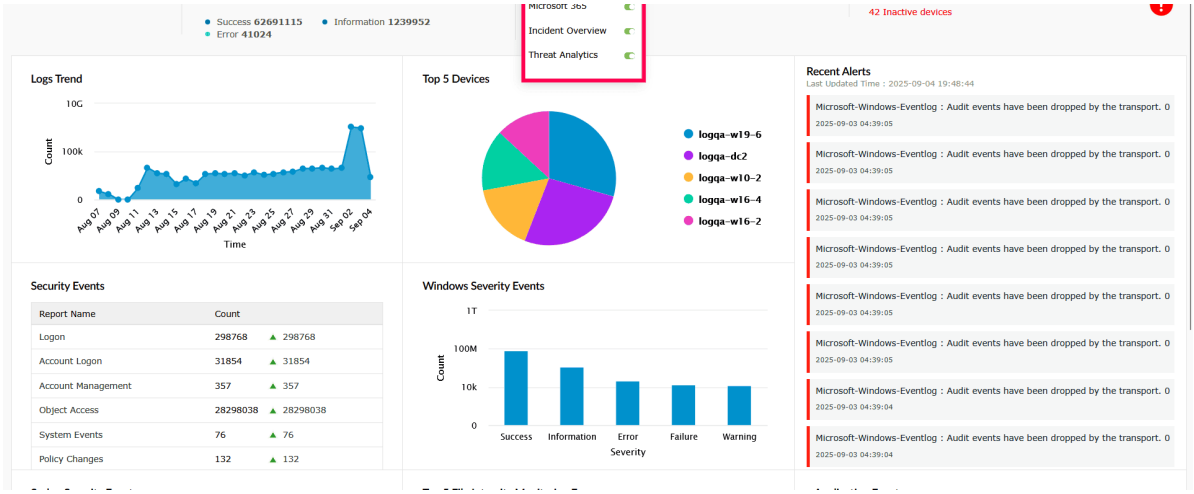


Figure 18: Switching between tabs

4. To remove a particular tab from the slideshow, click the toggle button next to the tab name in the drop-down list.

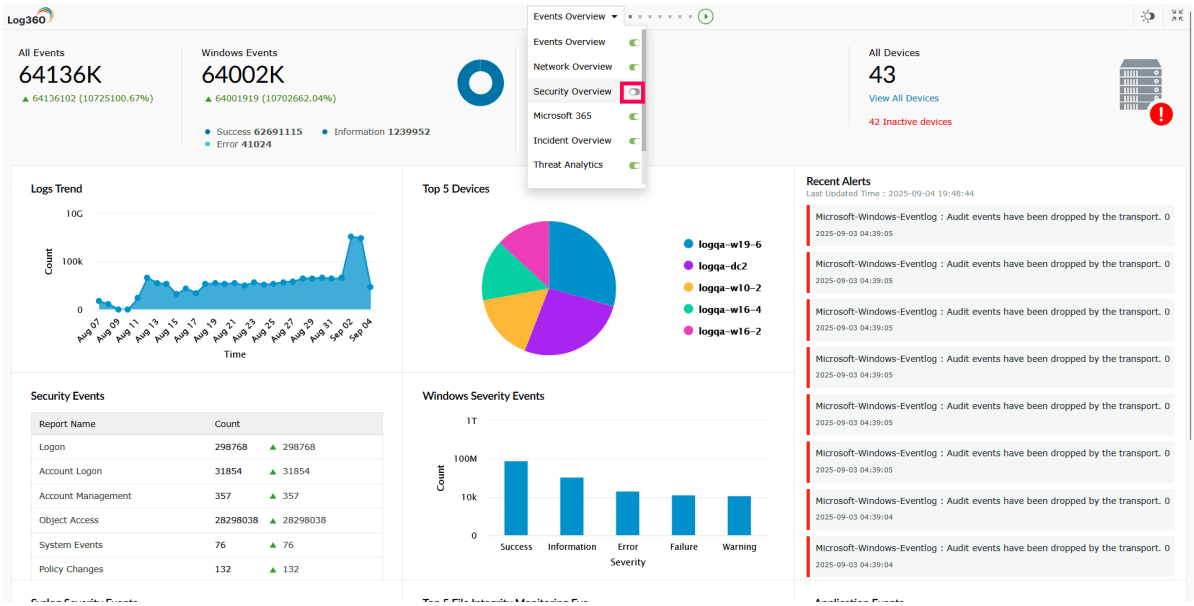
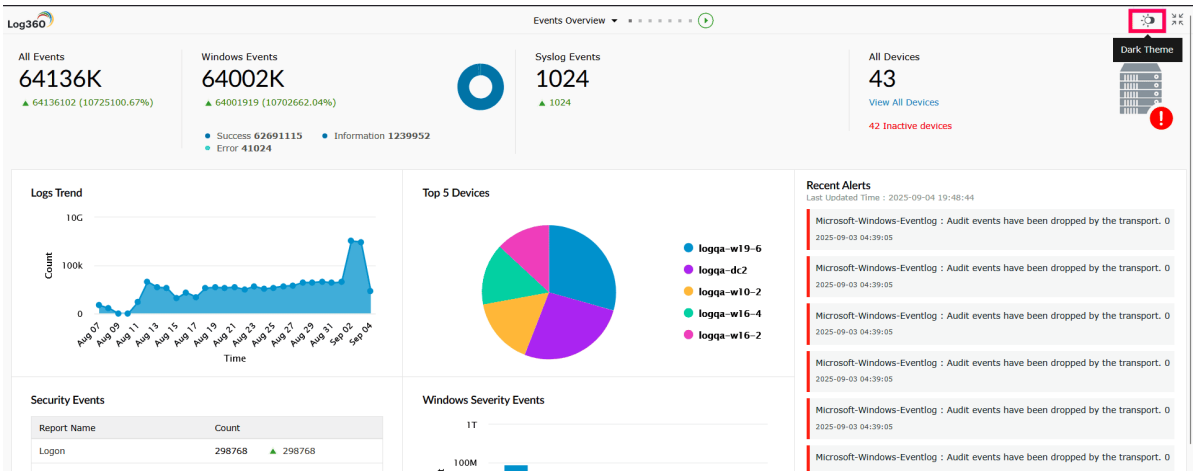


Figure 19: Removing a tab from the slideshow

5. To switch to dark mode, click the toggle button at the top-right corner of the screen.



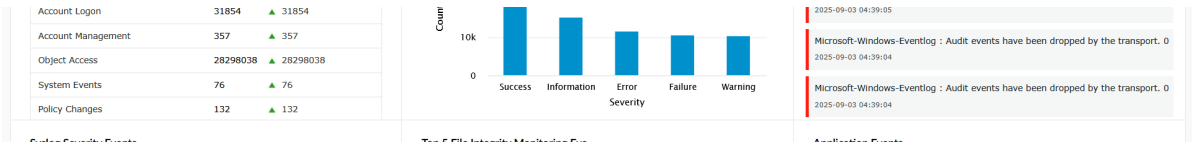


Figure 20: Switching to dark mode

6. To exit full screen mode, click the icon.

Viewing a widget in full screen mode

To view a widget in full screen, in the dashboard, click the icon on the top-right corner of the widget you want to view.

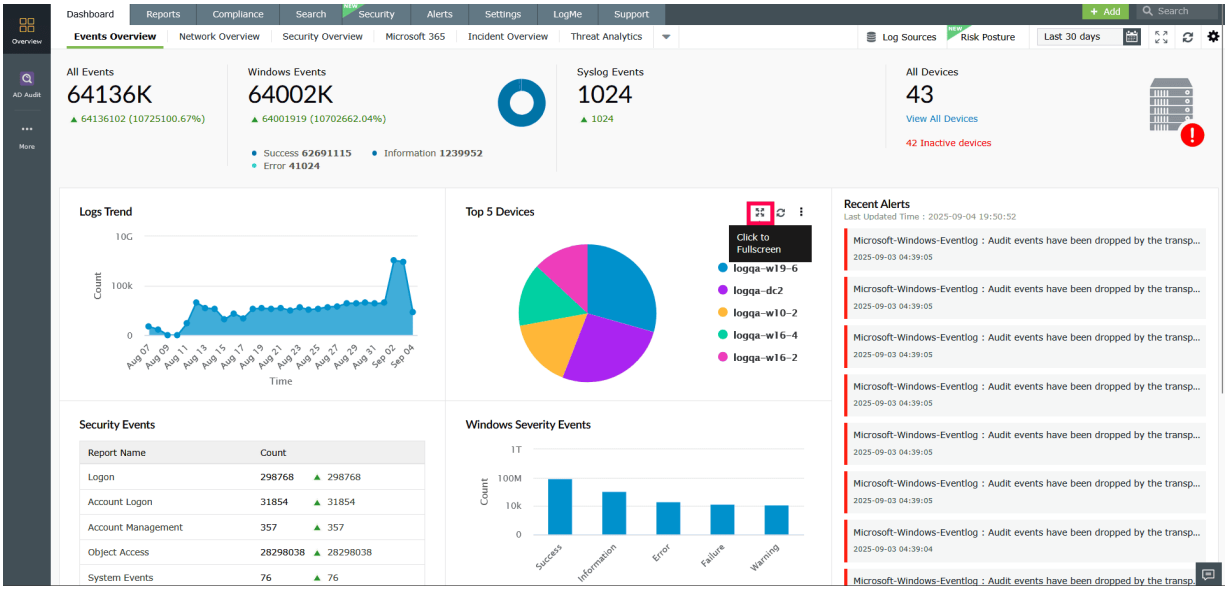


Figure 21: Viewing a widget in full screen mode

Refreshing the dashboard and widgets

To refresh the entire dashboard,

1. In the dashboard, click the icon on the top-right corner of the screen.

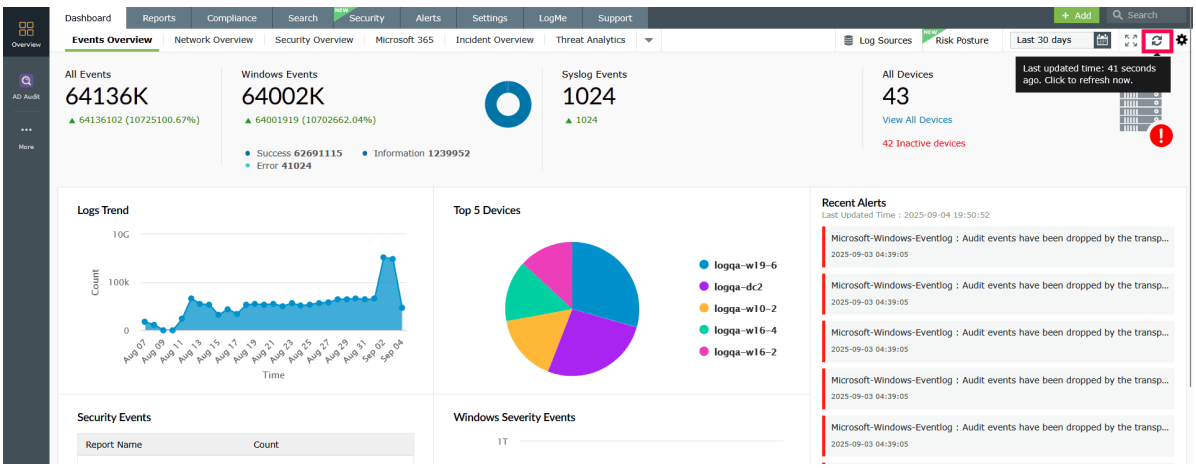




Figure 22: Refreshing the dashboard

To refresh a particular widget,

1. In the dashboard, click the icon on the top-right corner of the specific widget.

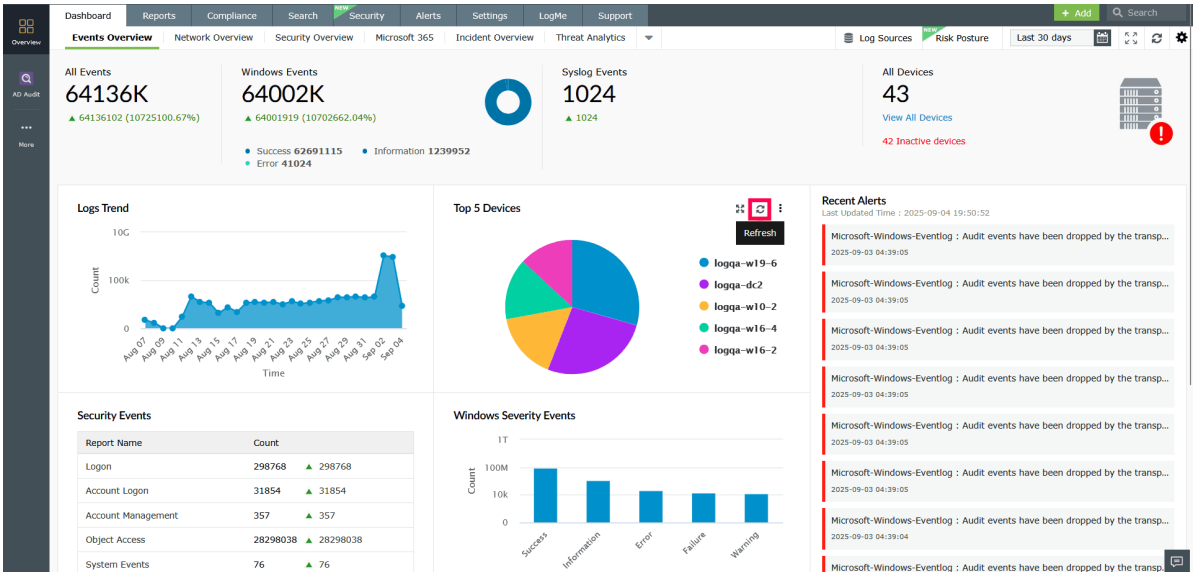


Figure 23: Refreshing a widget

Changing refresh interval

To change the time interval for the automatic refreshing of the dashboard,

1. In the dashboard, click the icon on the top-right corner and select Refresh Interval.

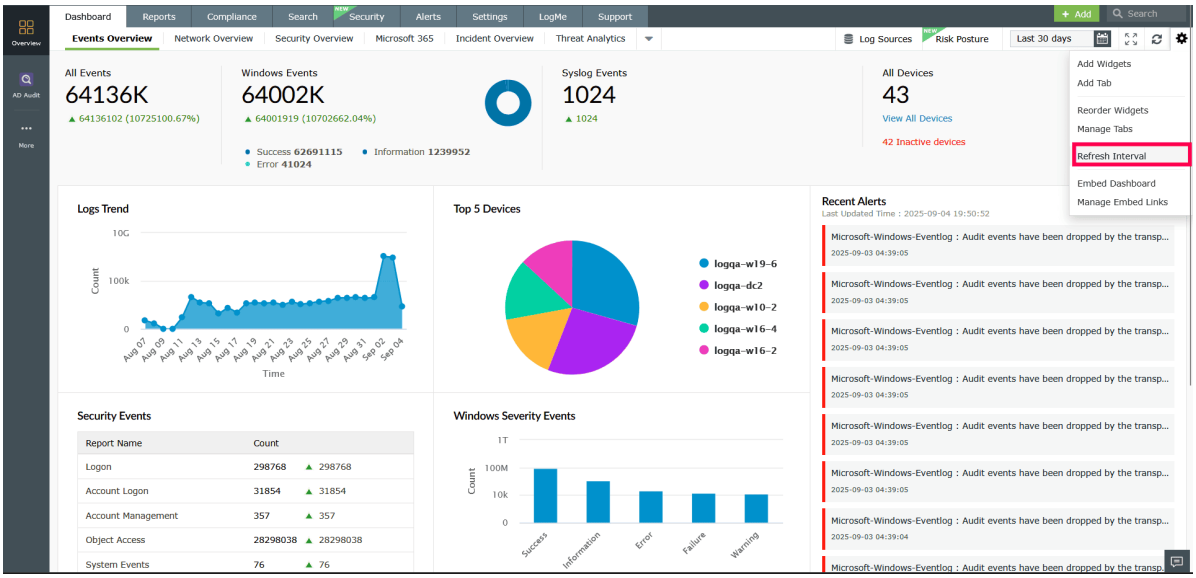


Figure 24: Configuring Refresh Interval in the dashboard

2. In the Dashboard Refresh window, select the refresh interval: Never, 30 seconds, 1 minute, 5 minutes, 10 minutes, or 1 hour.
   NOTE If you select Never, the dashboard will not refresh automatically. You will need to refresh it manually.



Figure 25: Changing the refresh interval

3. Click Save to apply the changes to the dashboard.

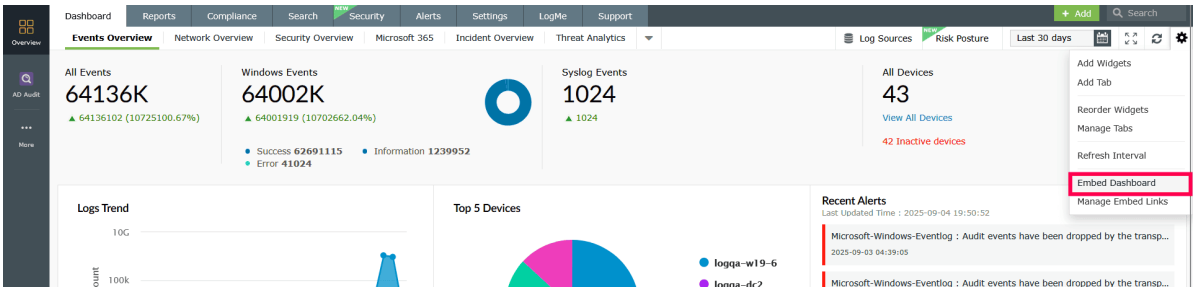
> NOTE
>
> Watch this video for a step-by-step demonstration of customizing the dashboard.

Configuring Embed link for dashboard and widgets

The Embed link enhances data sharing by allowing the creation of external share links for specific tabs or widgets. This enables precise and targeted access to dashboard data, supporting collaboration and visibility across platforms.

To embed a dashboard,

1. In the dashboard, navigate to the tab you want to embed.
2. In the top-right corner, click the ⚙ icon and select Embed Dashboard.



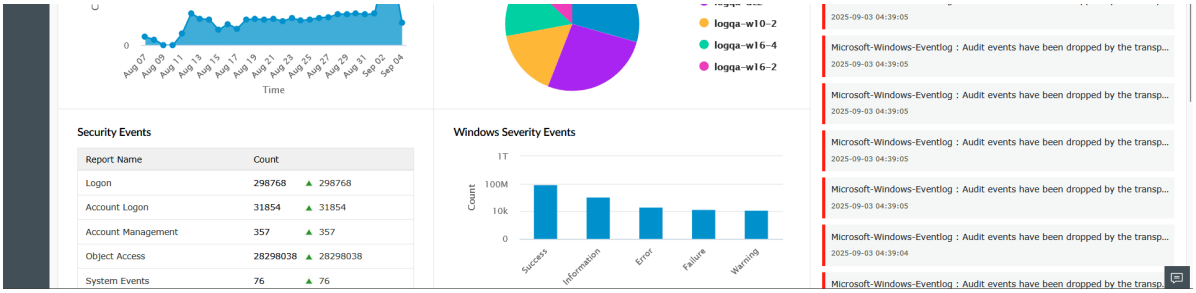


Figure 26: Navigating to Embed Dashboard

3. Provide a unique Link Name.
4. Select the desired Time Range from the drop-down menu.
5. Configure the Refresh Time (60 - 1440 minutes) and Expiry (1 - 365 days) using the drop-down options.

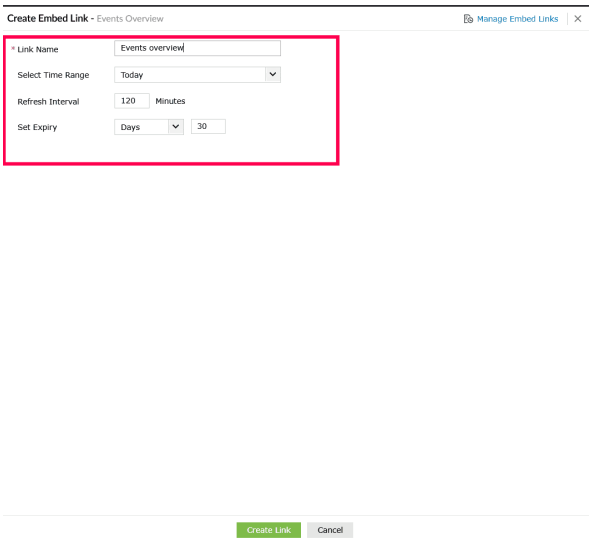


Figure 27: Creating an embed link

6. Click Create Link to generate the embed link for the dashboard.

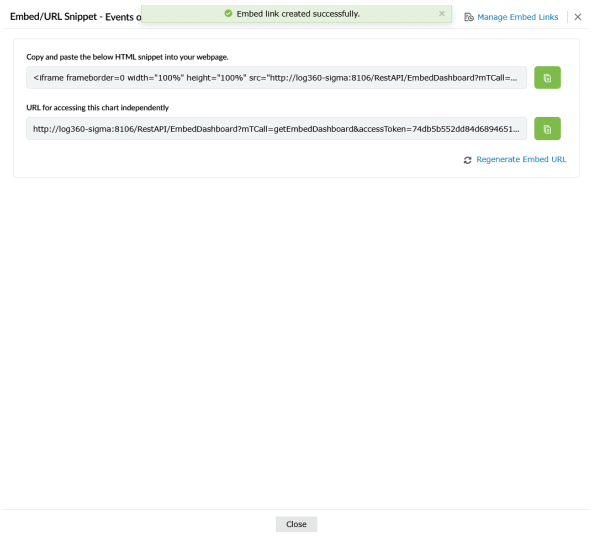


Figure 28: Creating an embed link

7. To regenerate the link, click Regenerate Embed URL.

To embed a widget,

1. In the dashboard, click the ⋮ icon and select Embed Widget corresponding to the widget that you want to embed.

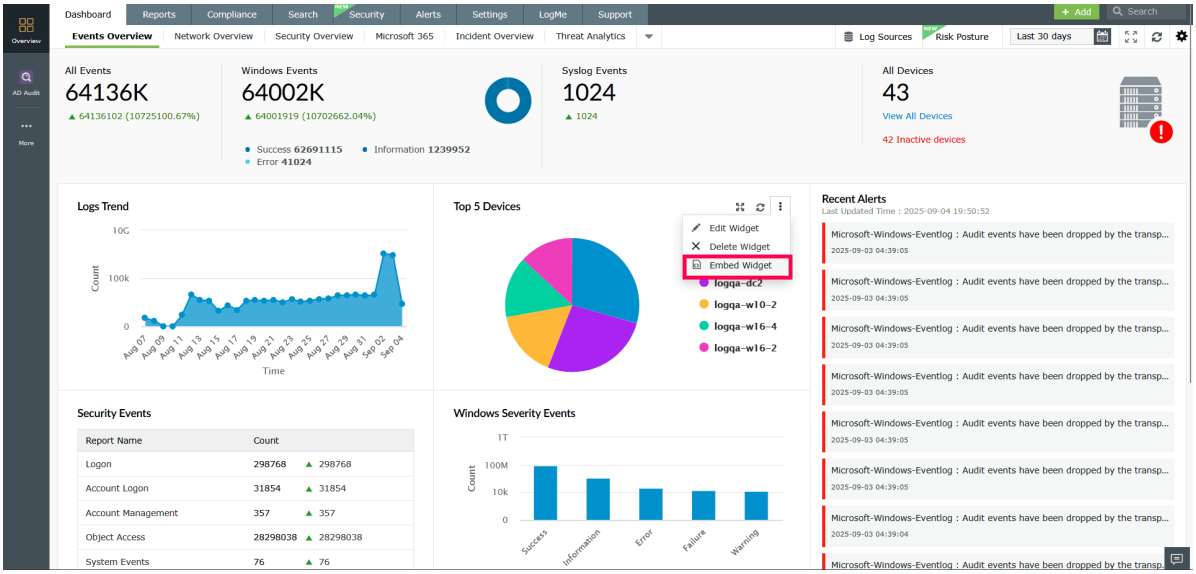


Figure 29: Embedding a widget in the dashboard

2. Provide a unique Link Name.
3. Select the desired Time Range from the drop-down menu.
4. Configure the Refresh Time (60 - 1440 minutes) and Expiry (1- 365 days) using the drop-down options.

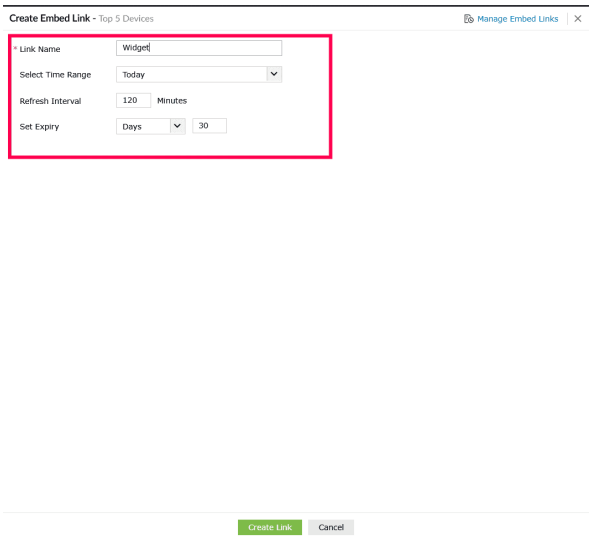


Figure 30: Configuring an Embed widget link

5. Click Create Link to generate the embed widget link.

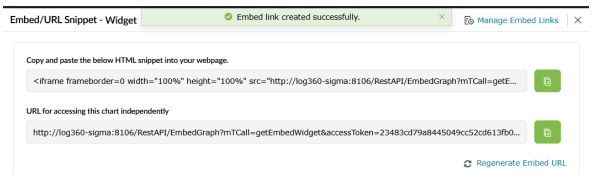


Figure 31: Creating Embed widget links

6. To regenerate the link, click Regenerate Embed URL.

> NOTE
>
> - The embedded widget will refresh automatically at the specified interval.
> - The generated external share link will remain valid only until the specified expiry date.

Managing embed links

To manage embed dashboard links,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Manage Embed Links.

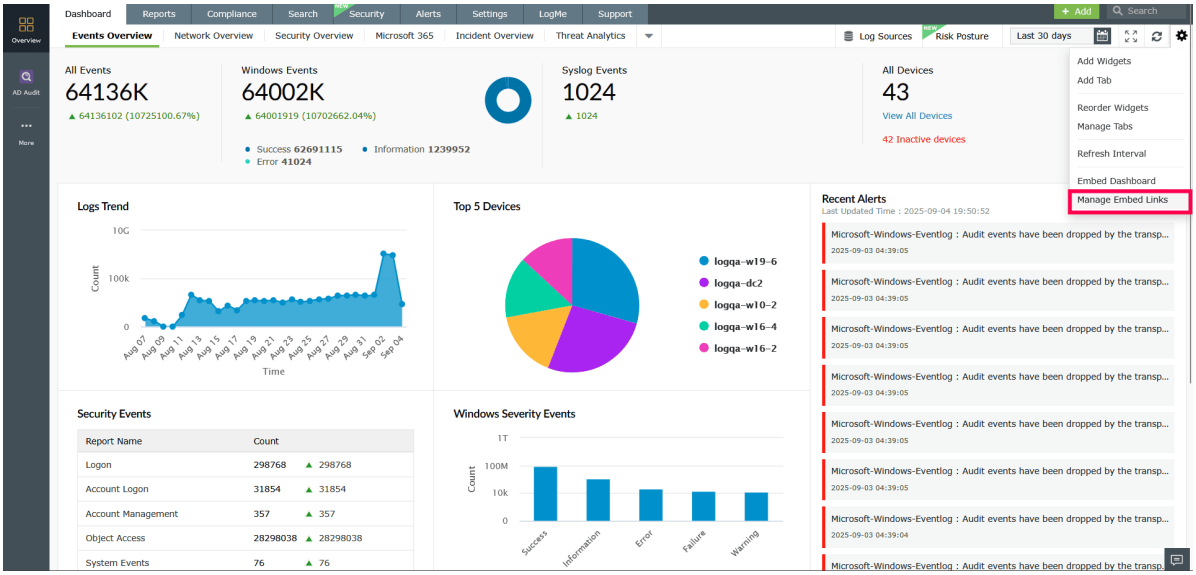
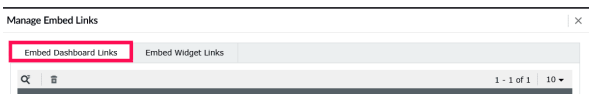


Figure 32: Accessing Manage Embed Links

2. A table will appear displaying all the Active Dashboard Links. Go to Embed Dashboard Links.



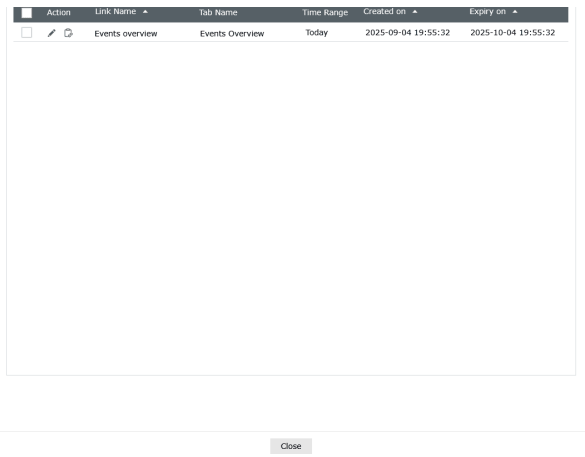


Figure 33: Viewing Active Dashboard Links

3. To edit a specific link, locate the desired entry and click the Edit option next to it.

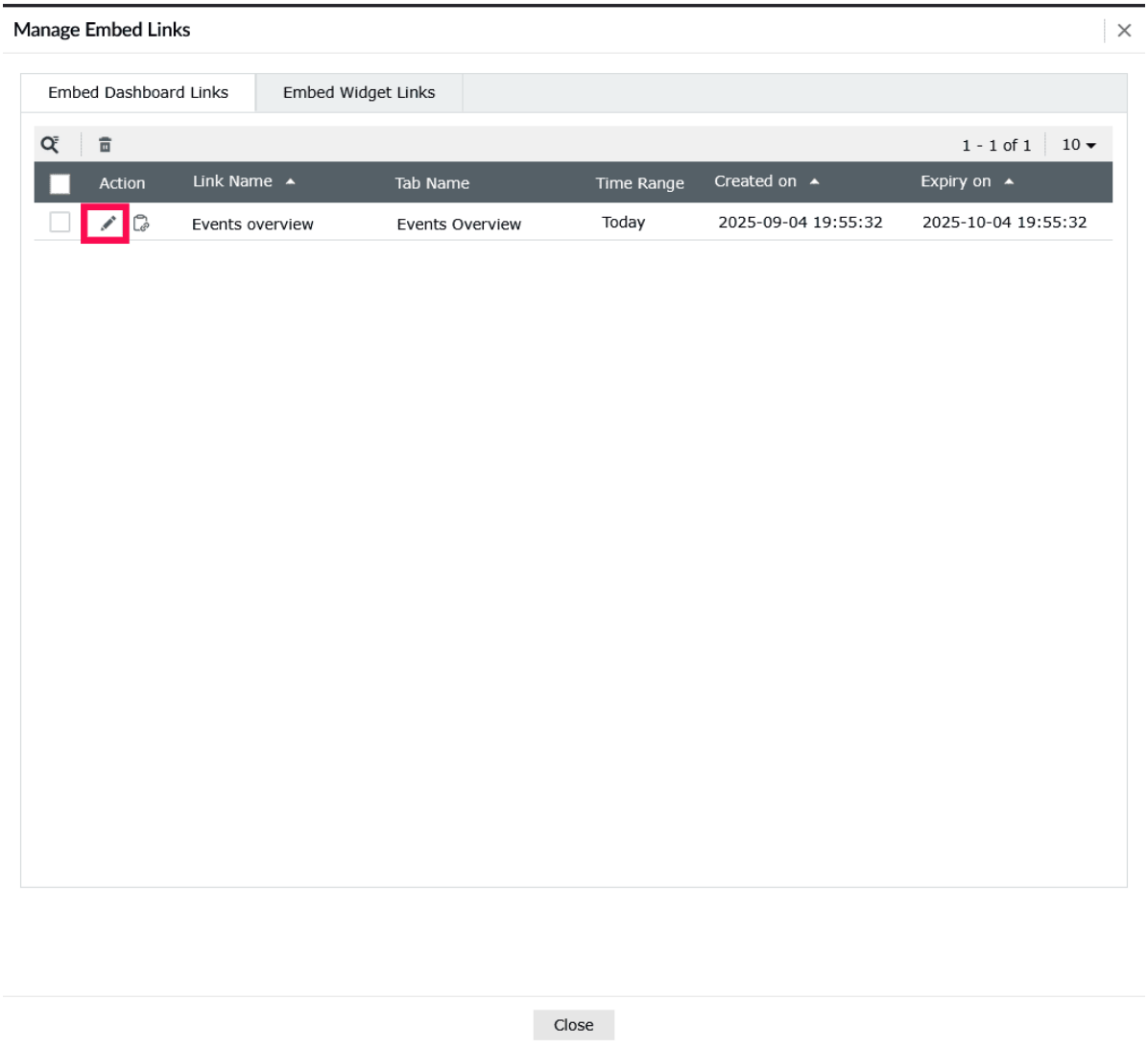


Figure 34: Editing Embed Widget Links

4. A window will appear allowing you to modify the properties of the chosen link. Make the necessary changes.



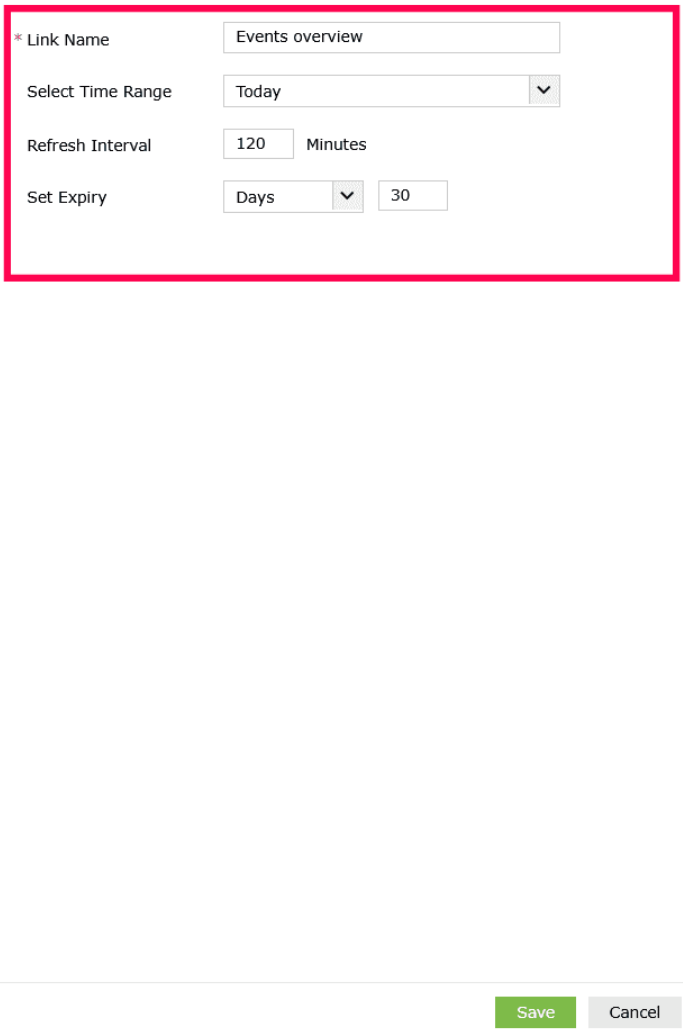


Figure 35: Configuring Edit Embed Link

5. Once done, click Save to apply the updates to the Active Dashboard Link.
6. To delete, select the checkbox next to the entry you want to remove and click the icon.

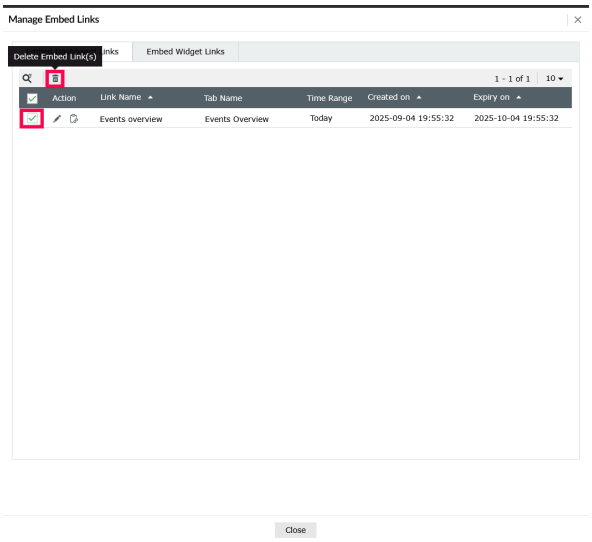


Figure 36: Deleting an embed link

7. In the confirmation pop-up, click Yes to delete the embed link from the list permanently.

8. To regenerate the link, select the icon. In the window that opens, click Regenerate Embed URL to generate a new embed URL while retaining the existing configuration.

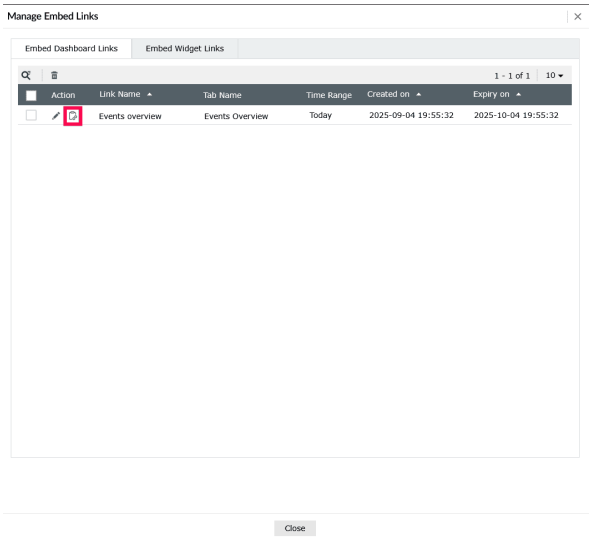


Figure 37: Regenerating Embed URL

To manage embed widget links,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Manage Embed Links.

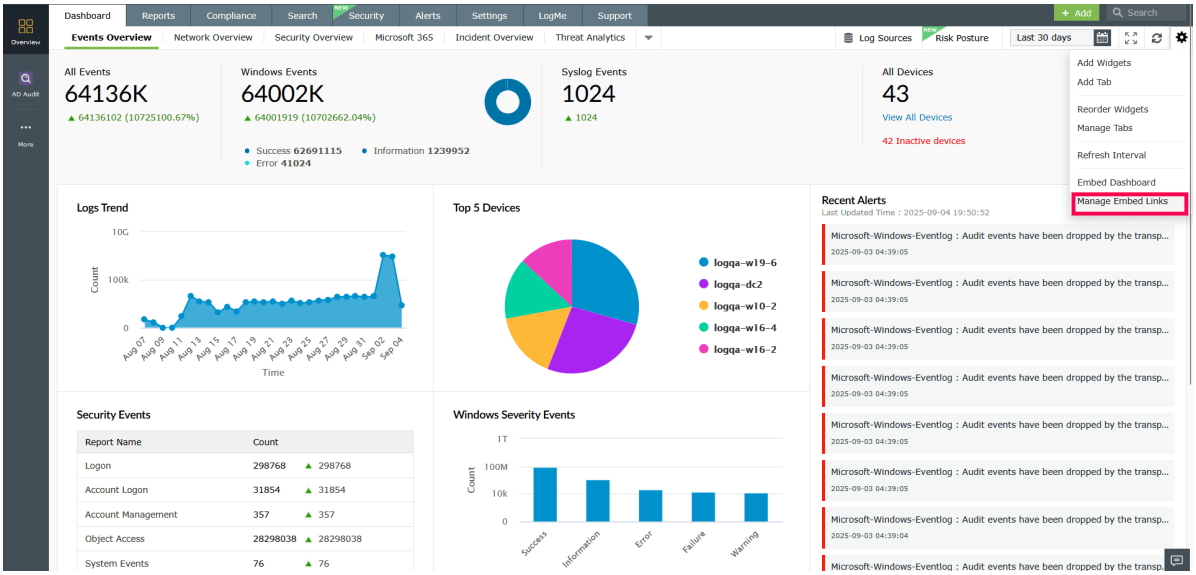


Figure 38: Accessing Manage Embed Links

2. A table will appear displaying all the Active Dashboard Links. Go to Embed Widget Links.

> NOTE
>
> Follow the instructions from this step to edit, delete, or regenerate the embed link for a widget.



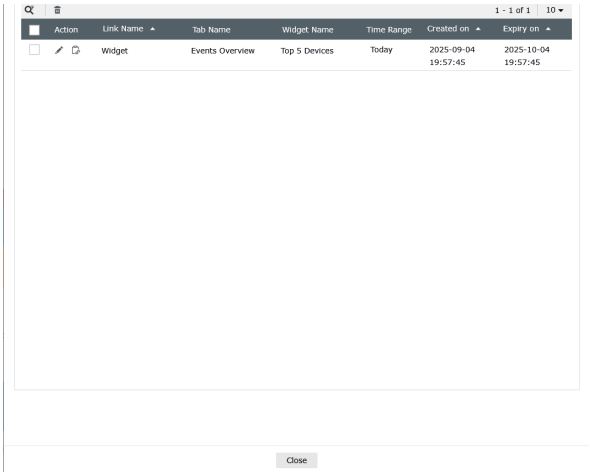


Figure 39: Viewing Active Dashboard Links

Read also

This page explained about customizing the Log360 dashboard to tailor tabs and widgets. To learn more about predefined dashboard views and widget management, refer to the following documents:

- Predefined tabs and widgets

8.3.1. EventLog Analyzer Reports

Last updated on: September 12, 2025

In this page

Windows

Unix

Applications

Network Devices

Custom Reports

EventLog Analyzer offers 1000+ out-of-the-box reports and also the capability to create custom reports as per your requirements. These reports can help review the key security events happening in your network and also meet compliance requirements.
The reports can be accessed from the Reports tab of the UI. The event counts shown in the reports can be drilled down to the raw logs. The logs can be further filtered based on various log fields. EventLog Analyzer also allows you to schedule reports to be automatically generated and emailed periodically.

Types of reports

EventLog Analyzer offers a wide category of reports. Some of them are listed below.

Windows

The Windows reports allow you to get an overview of the events happening in your Windows environment. A few examples are given below:

- Windows Logon Reports
- Policy Changes
- Windows Logoff Reports
- Windows Firewall Threats
- Application Crashes

Unix

The Unix reports allow you to get an overview of the events happening in your Unix environment. A few examples are given below:

- Unix Logon Reports
- Unix Logoff Reports
- Unix Failed Logon Reports
- Unix User Account Management
- SU Commands

Applications

The application reports allow you to get an overview of the events happening in the applications installed in your network. ManageEngine EventLog Analyzer supports a wide range of applications including Terminal Server, DHCP Windows and Linux Servers, MS IIS W3C FTP Server, MS IIS W3C and Apache Web Servers, MS SQL and Oracle Database Servers, Sysmon, and Print Server. These reports also help you to identify the performance and security status of the above applications.
A few examples are given below.

- Terminal Server Gateway Logons
- Terminal Server Gateway Logons
- SQLServer DDL Auditing Report
- Oracle Security Reports
- Printer Auditing

Network Devices

The network devices reports allow you to get an overview of the events happening in your networking devices. A few examples are given below.

- Router Logon Report
- Router Configuration Report
- Router Accepted Connections
- Firewall Account Management
- Network Device Risk Reports

Custom Reports

The custom reports that you have created will be listed in this section.

8.3.2. Manage Predefined Reports

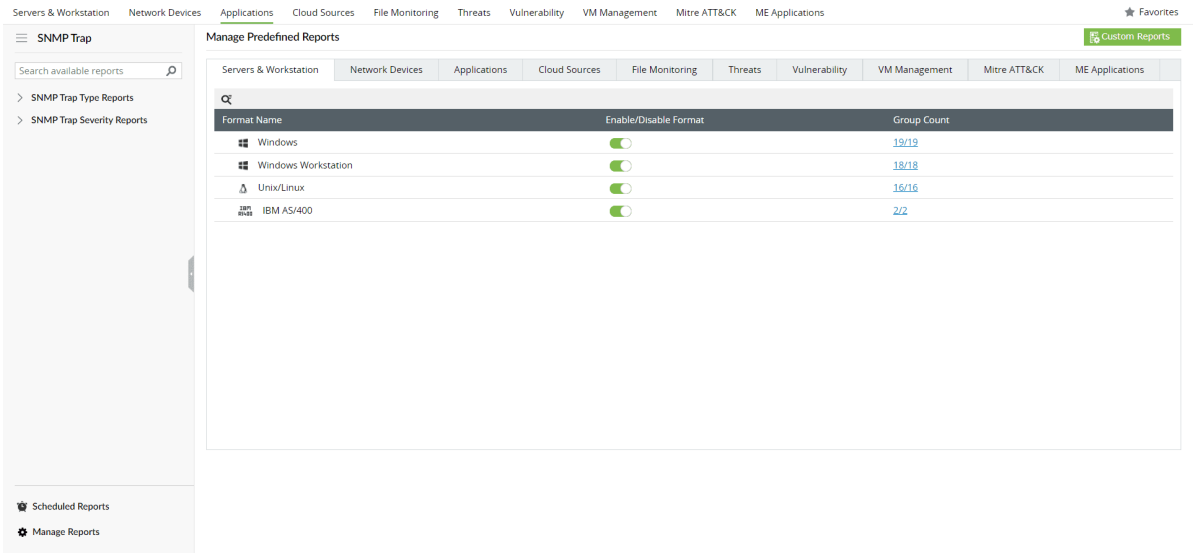
Last updated on: September 12, 2025

EventLog Analyzer allows you to personalize the appearance of the reports page as required. You can customize the arrangement of reports and report groups.

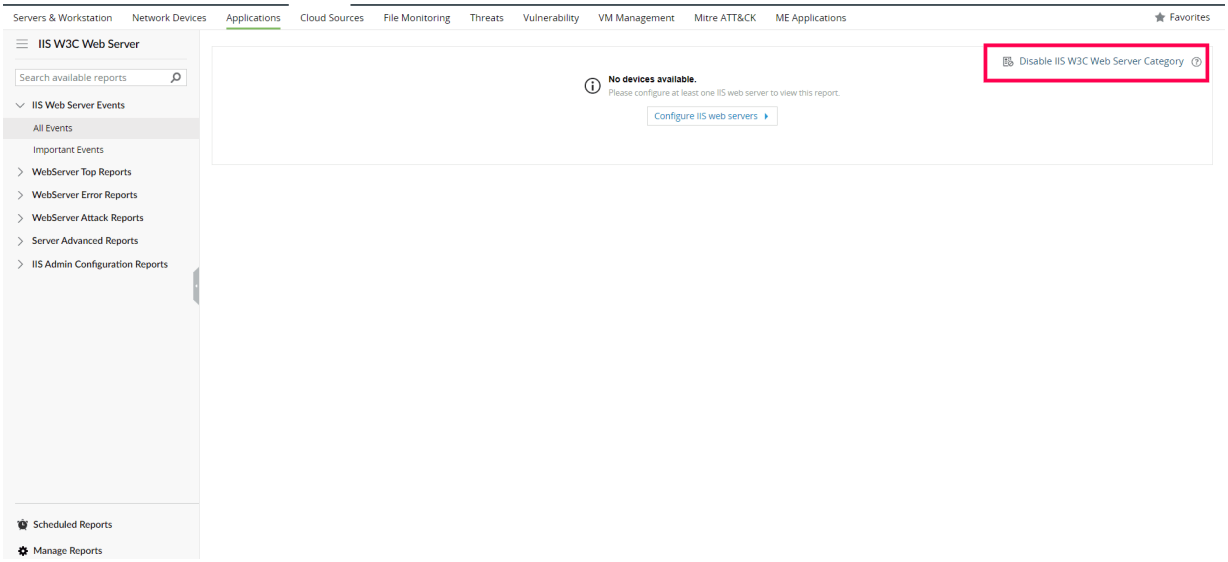
Customizing the arrangement of reports and report groups

To customize the arrangement of reports and report groups, follow the steps given below.

- Open EventLog Analyzer and click on the Reports tab.
- Click on Manage Reports at the bottom of the left panel. Then, click on Manage Predefined Reports at the top right corner.
- Select the required log source by clicking on the corresponding tab.
- The arrangement of the sub-categories of the log sources, as seen on the top bar of the reports page, will be displayed. For example, when Devices is chosen as the log source, the top bar will display the first few devices and the rest is displayed in a drop-down list. You can choose to have your most-used devices displayed first in the top bar to ensure easy access.



- To change the order of devices, hover the mouse pointer on the space to the left of the device name. A ⠿ icon will appear.
- Use the ⠿ icon to drag and drop the devices in the required order.
- You can also enable or disable reports by clicking on the toggle button under the Enable/Disable Format column corresponding to the required device.
- Similarly, you can also rearrange the reports inside each report group by clicking on the report group and following the steps mentioned above.
- If no devices are configured in a category, you can disable it from the reports page using the "Disable Category" button available in the top right corner.


Servers & Workstation
Network Devices
Applications
Cloud Sources
File Monitoring
Threats
Vulnerability
VM Management
Mitre ATT&CK
ME Applications
Favorites
IIS W3C Web Server
Search available reports
IIS Web Server Events
All Events
Important Events
WebServer Top Reports
WebServer Error Reports
WebServer Attack Reports
Server Advanced Reports
IIS Admin Configuration Reports
Scheduled Reports
Manage Reports
Disable IIS W3C Web Server Category
No devices available.
Please configure at least one IIS web server to view this report.
Configure IIS web servers

8.3.3. Schedule Reports

Last updated on: September 12, 2025

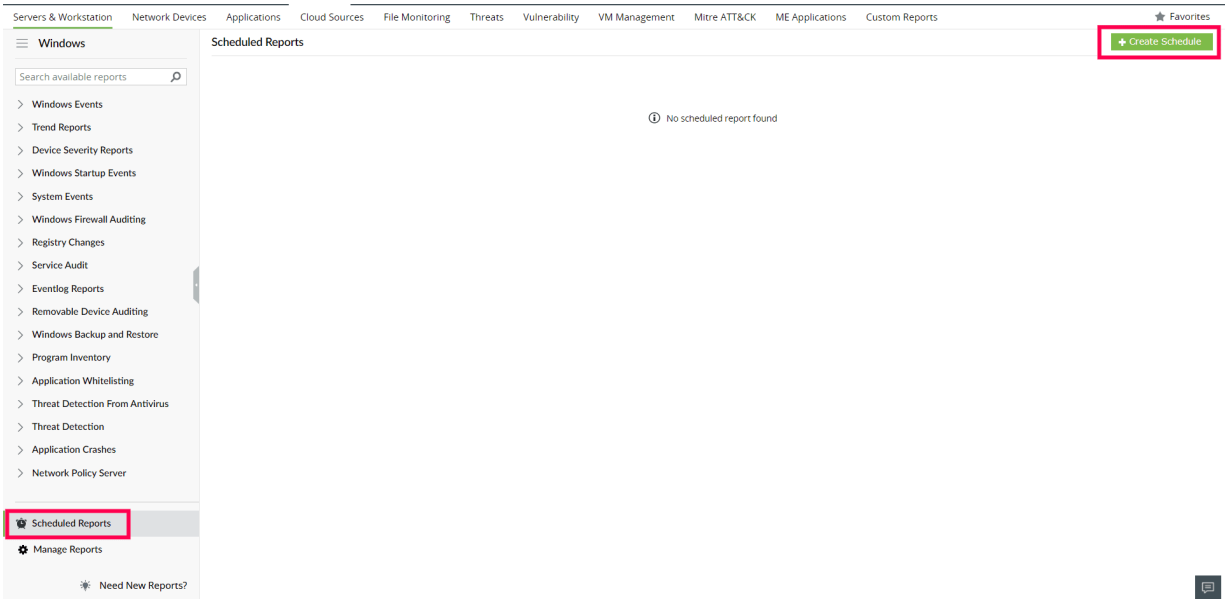
In this page

Creating a New Report Schedule

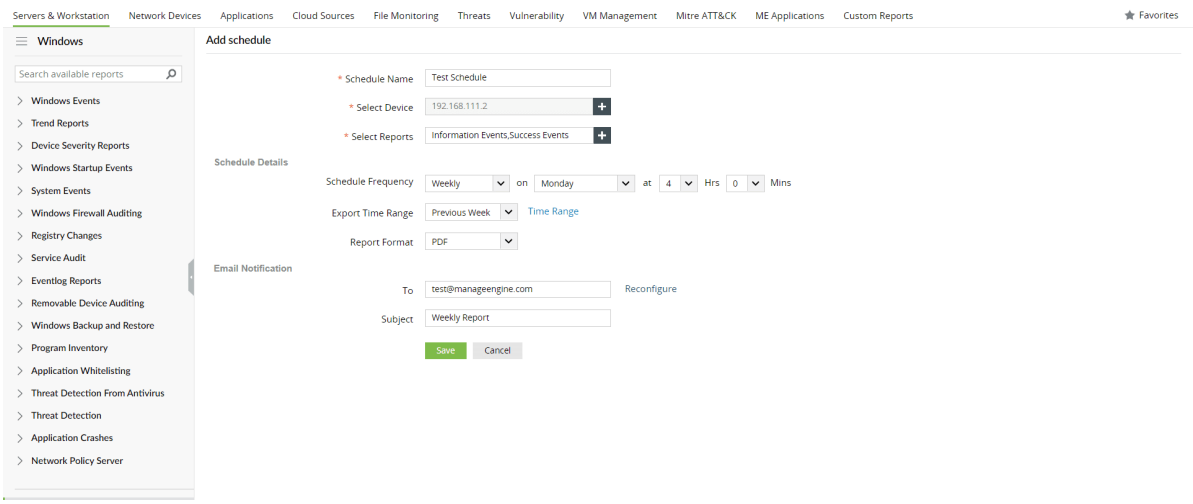
Manage Report Schedules

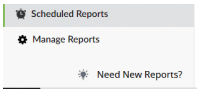
EventLog Analyzer lets you schedule report generation, export, and redistribution over email. This page elaborates on the procedure to create and manage report schedules.

Creating a New Report Schedule



1. Click on the Schedule Report link on top right corner of the Reports page. Alternatively, you can click on the +Create New Schedule button on the top right corner of the Scheduled Reports page. This will open the Create New Schedule page.

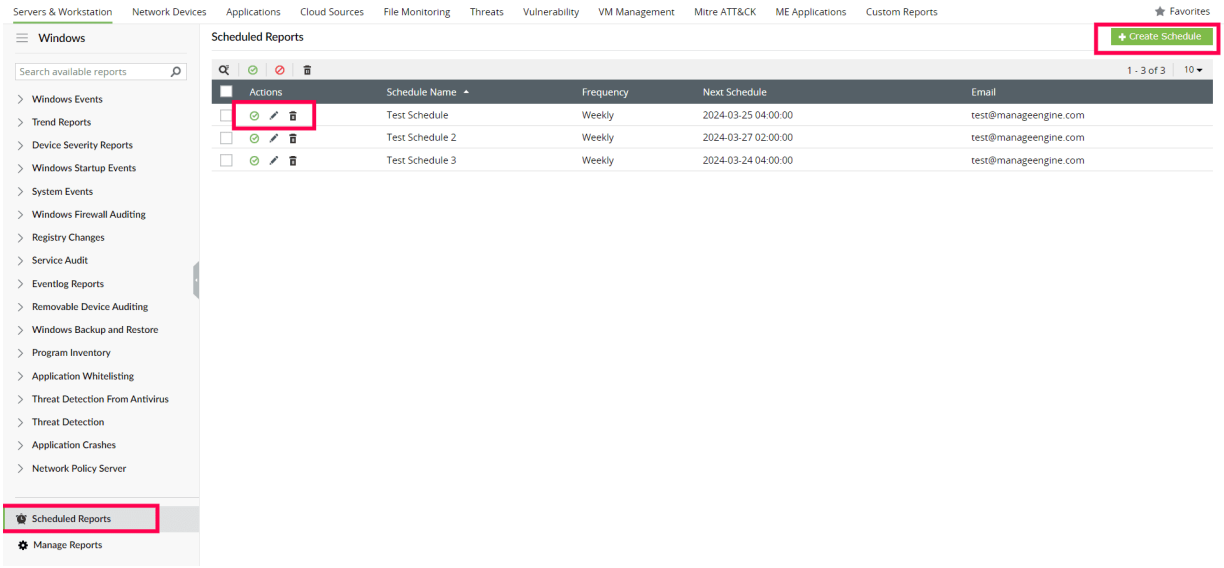




2. In the Create New Schedule window,
   - Enter the name of the schedule, devices for which the schedule is for, and the reports which are to be included in the schedule.
   - Schedule Frequency: Specify the frequency at which reports need to be exported. The frequency can be 'Only Once', 'Hourly', 'Daily', 'Weekly', or 'Monthly'.
   - Export Time Range: Select the time range for which the report needs to be created and later exported.
   - Report Format: Choose the file format in which the report needs to be exported i.e. PDF or CSV.
   - Email Address: Configure the email address to which the reports need to be sent.
   - Email Subject: Enter the subject of the mail that contains the exported reports.
3. Once you've entered the necessary details for the schedule, click Save to complete creating the report schedule.

Manage Report Schedules

You can view, edit, delete, or disable report schedules. The procedure is as below.



1. Navigate to the Reports page.
2. In the left pane, click Scheduled Reports present at the bottom. You can now see a list of report schedules.
   - To edit a report schedule, click the edit icon corresponding to the report schedule and make the necessary changes.
   - To delete a report schedule, click the corresponding delete icon. Click Yes in the pop-up box that appears.
   - To disable a report schedule, click on the corresponding tick in the Actions column.

8.3.4. Custom Reports

Last updated on: September 12, 2025

In this page

Create custom reports

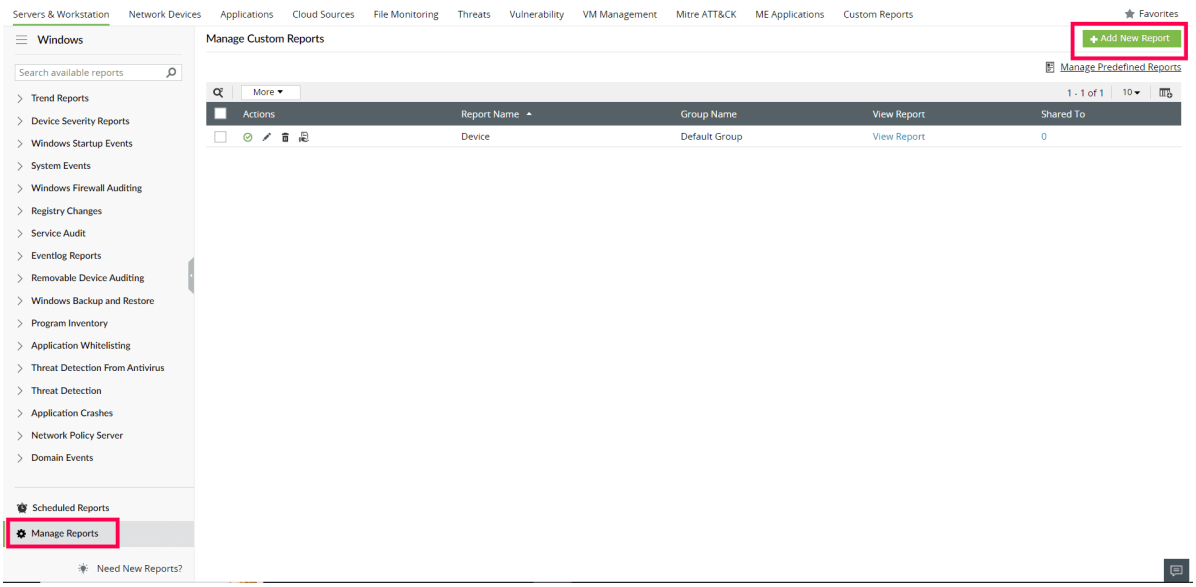
Manage custom reports

Type of views

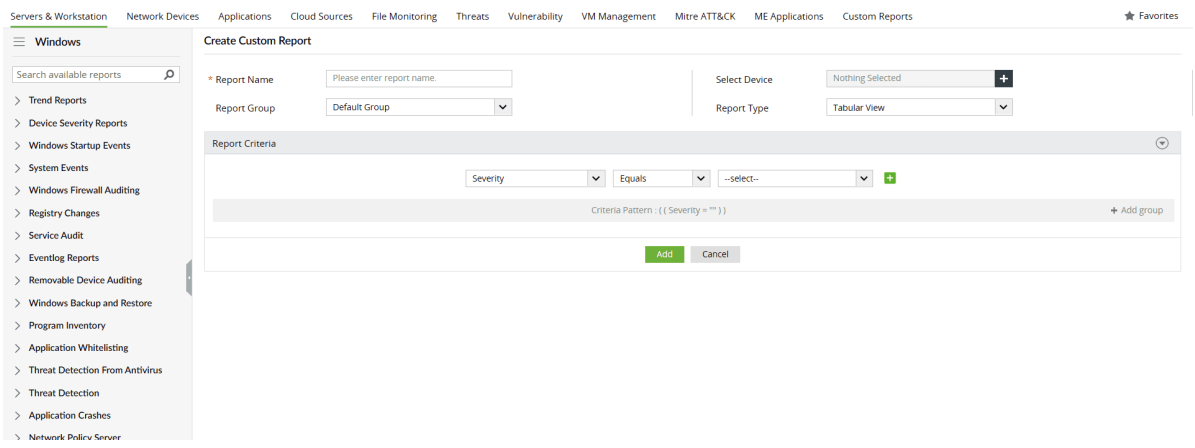
EventLog Analyzer can generate custom reports based on criteria set by you. You can specify the criteria with field values and logical operators. These reports will be listed under Custom Reports.

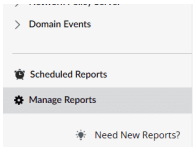
Create custom reports

1. Navigate to Reports and select Manage Reports at the bottom-left. In the Manage Reports dashboard, click +Add new reports button on the top-right.

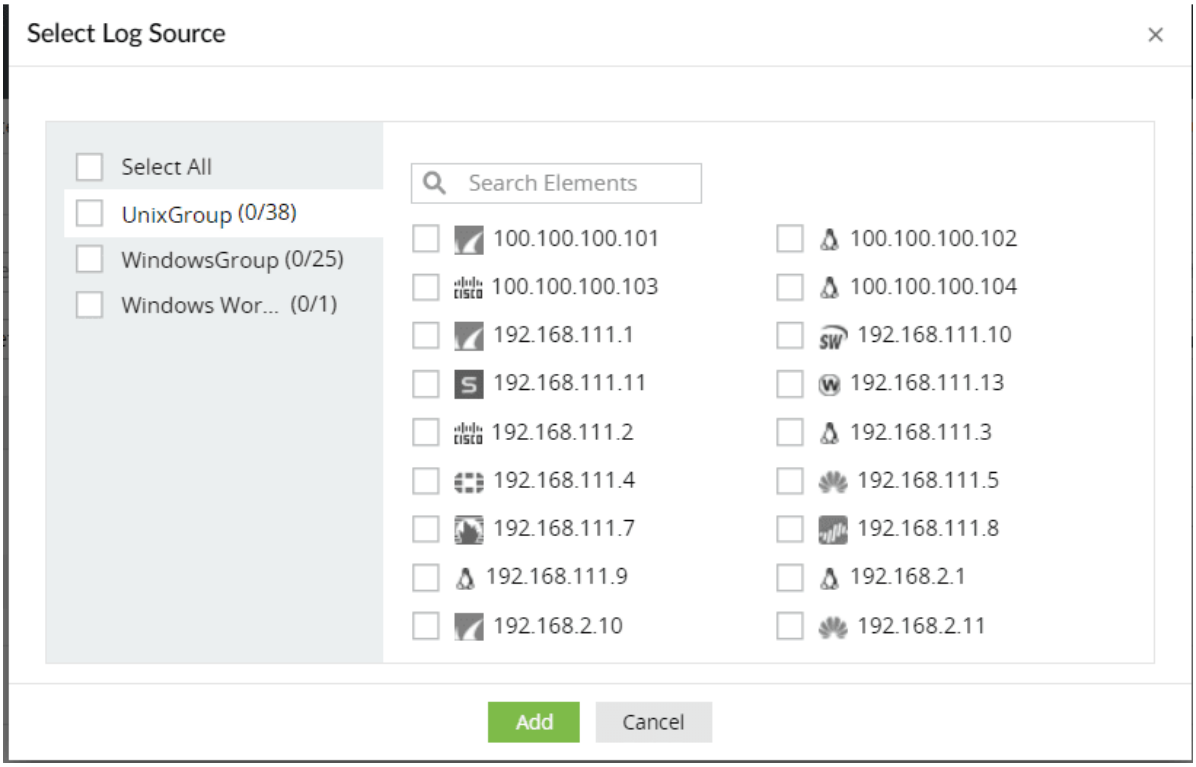


2. In the Create Custom Report dashboard, enter a name for your report.

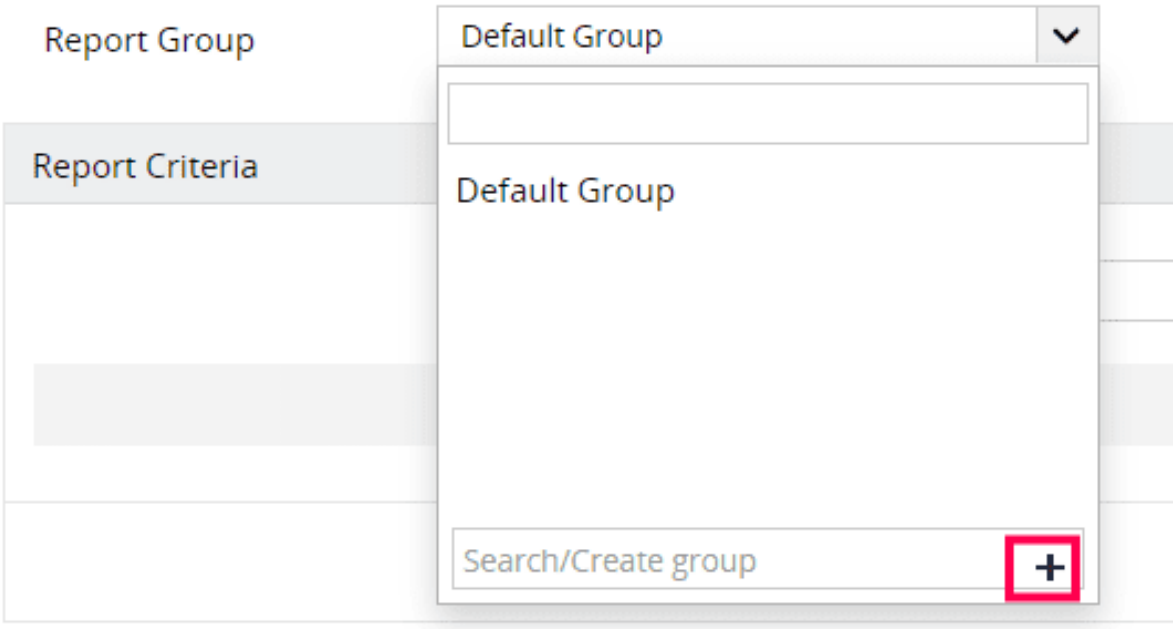




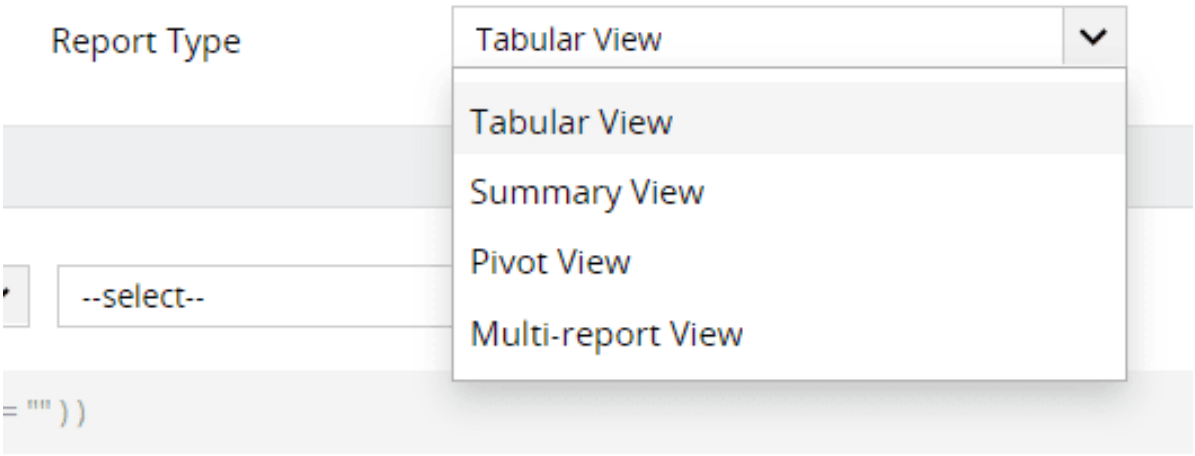
3. Click Select Device to generate reports for specific devices or applications.



4. Click Report Group to add the new report to the desired group. The drop down displays all available report groups under Custom Reports. Select one of these or create your own group and click '+'. If not specified, the custom report will be added to the Default Group.



5. Select the type of view for your report (see types of view).



6. Set the criteria for the report. You can add multiple criteria and perform AND or OR operations between them. You can also add criteria to groups and perform AND or OR operators between the groups.

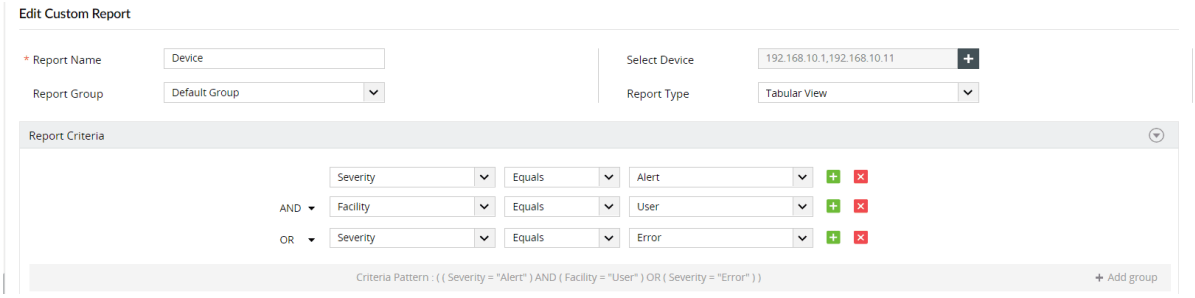
> Note
>
> - When the given criteria is separated by commas, it is treated as a separate criteria with OR condition. (Eg: If the criteria is given as EventID = 4678,4679 , then it is treated as EventID= 4678 OR 4679).
> - If you intend to give a single criteria with a comma character, please use "," instead of "," .

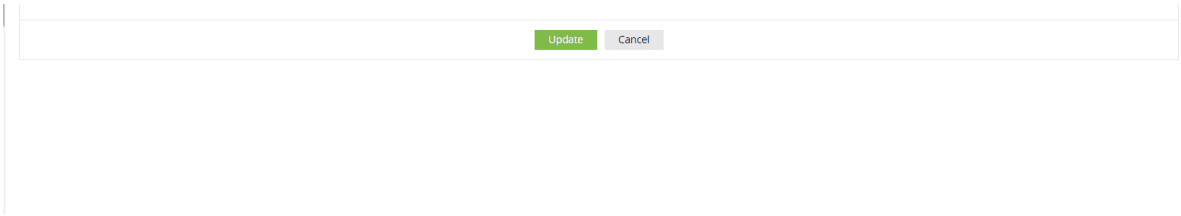
7. Click Add to save.

Manage Custom Reports

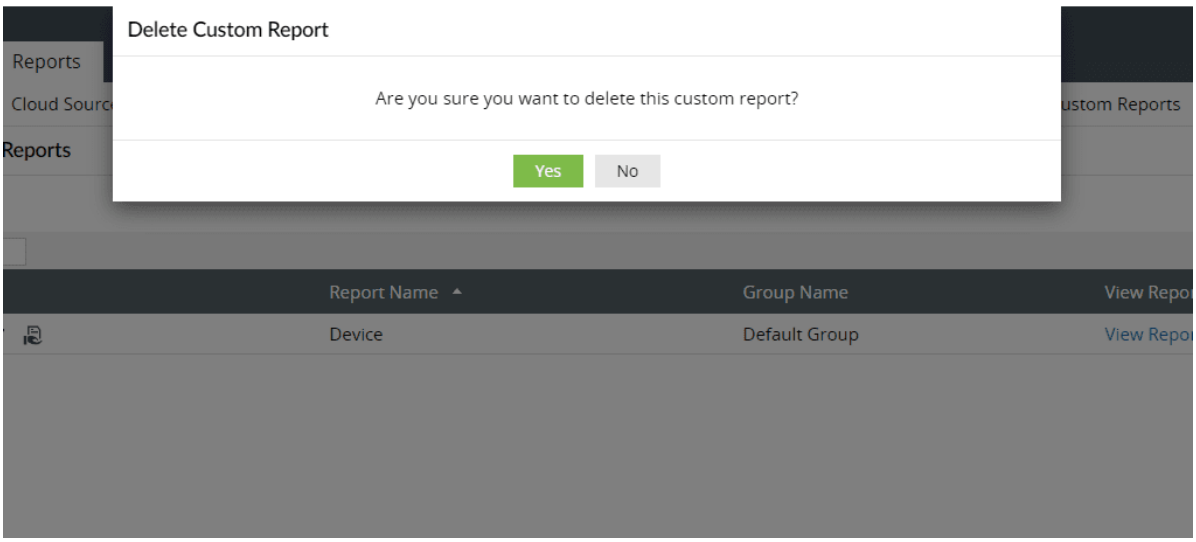
You can edit, delete, or disable the custom reports.

1. Navigate to Reports. Click Manage Reports at the bottom of the left panel.
2. To edit a custom-made report, click on the adjacent edit icon and make the necessary changes. Click Update.

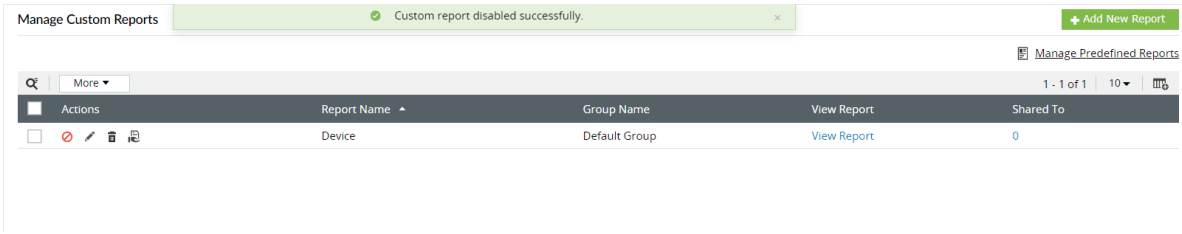




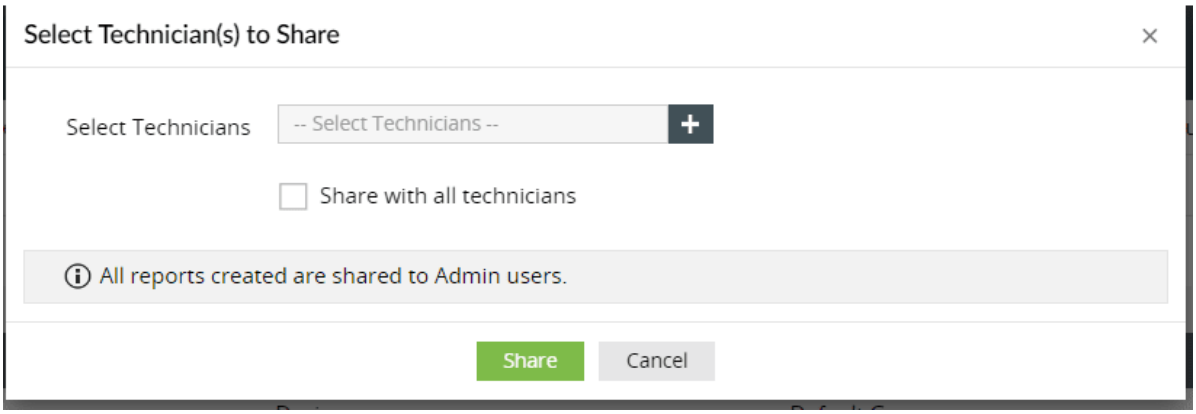
3. To delete a custom-made report, click on the adjacent delete icon. Click Yes in the pop-up box that appears.



4. To disable a custom-made report, click on the corresponding tick box in the Status column.



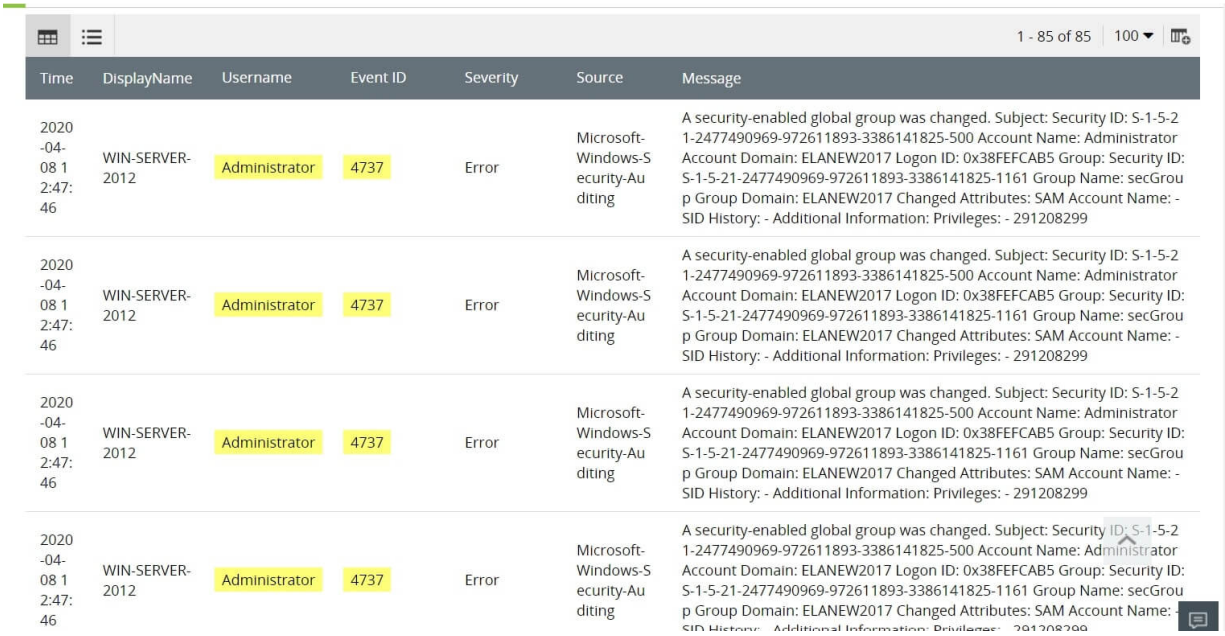
5. To share the reports with technicians, hover over the report and click on the share icon that appears. Select the technician(s) and click Share.



Types of views

Tabular View

This view displays the data in the form of a simple table. You just need to frame the criteria for selecting logs for the report. You can generate different views of the same tabular view report. To create a new view, refer the Manage Report Views section.

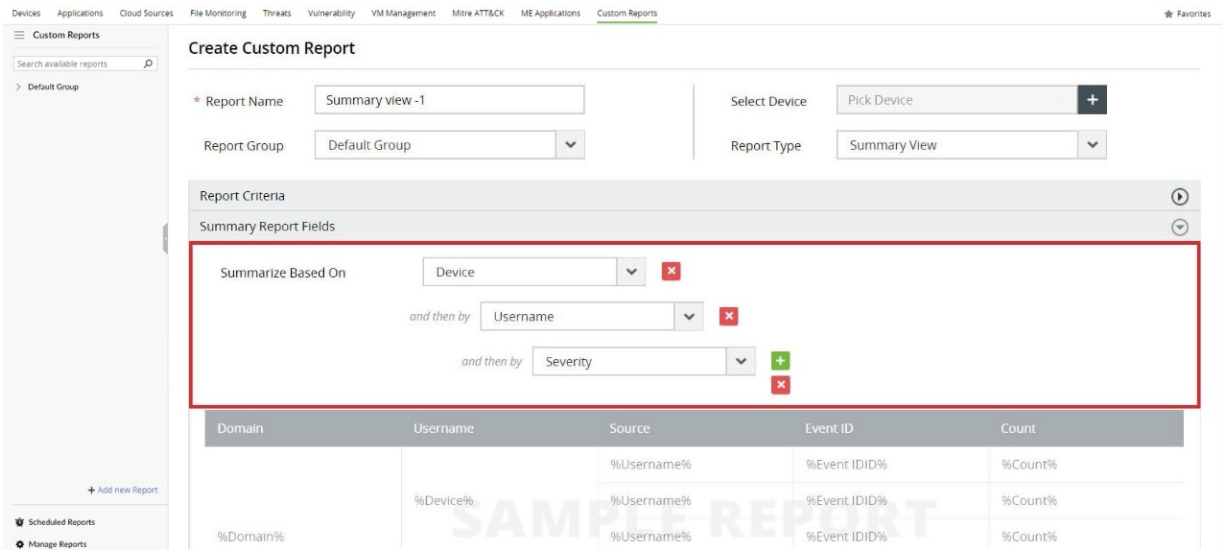


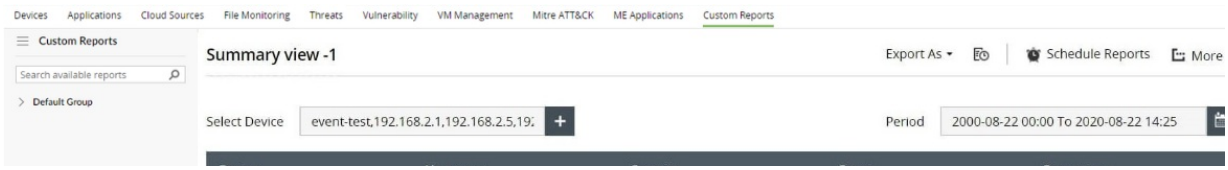
1 - 85 of 85 | 100

Time	DisplayName	Username	Event ID	Severity	Source	Message
2020-04-08 12:47:46	WIN-SERVER-2012	Administrator	4737	Error	Microsoft-Windows-Security-Auditing	A security-enabled global group was changed. Subject: Security ID: S-1-5-21-2477490969-972611893-3386141825-500 Account Name: Administrator Account Domain: ELANEW2017 Logon ID: 0x38FEFCAB5 Group: Security ID: S-1-5-21-2477490969-972611893-3386141825-1161 Group Name: secGroup Group Domain: ELANEW2017 Changed Attributes: SAM Account Name: - SID History: - Additional Information: Privileges: - 291208299
2020-04-08 12:47:46	WIN-SERVER-2012	Administrator	4737	Error	Microsoft-Windows-Security-Auditing	A security-enabled global group was changed. Subject: Security ID: S-1-5-21-2477490969-972611893-3386141825-500 Account Name: Administrator Account Domain: ELANEW2017 Logon ID: 0x38FEFCAB5 Group: Security ID: S-1-5-21-2477490969-972611893-3386141825-1161 Group Name: secGroup Group Domain: ELANEW2017 Changed Attributes: SAM Account Name: - SID History: - Additional Information: Privileges: - 291208299
2020-04-08 12:47:46	WIN-SERVER-2012	Administrator	4737	Error	Microsoft-Windows-Security-Auditing	A security-enabled global group was changed. Subject: Security ID: S-1-5-21-2477490969-972611893-3386141825-500 Account Name: Administrator Account Domain: ELANEW2017 Logon ID: 0x38FEFCAB5 Group: Security ID: S-1-5-21-2477490969-972611893-3386141825-1161 Group Name: secGroup Group Domain: ELANEW2017 Changed Attributes: SAM Account Name: - SID History: - Additional Information: Privileges: - 291208299
2020-04-08 12:47:46	WIN-SERVER-2012	Administrator	4737	Error	Microsoft-Windows-Security-Auditing	A security-enabled global group was changed. Subject: Security ID: S-1-5-21-2477490969-972611893-3386141825-500 Account Name: Administrator Account Domain: ELANEW2017 Logon ID: 0x38FEFCAB5 Group: Security ID: S-1-5-21-2477490969-972611893-3386141825-1161 Group Name: secGroup Group Domain: ELANEW2017 Changed Attributes: SAM Account Name: -

Summary View

This view gives you a more granular representation of the log data. It allows you to select multiple criteria based on which data wil lbe displayed. After framing the report criteria, you need to select the fields based on which the summary view report will be generated.

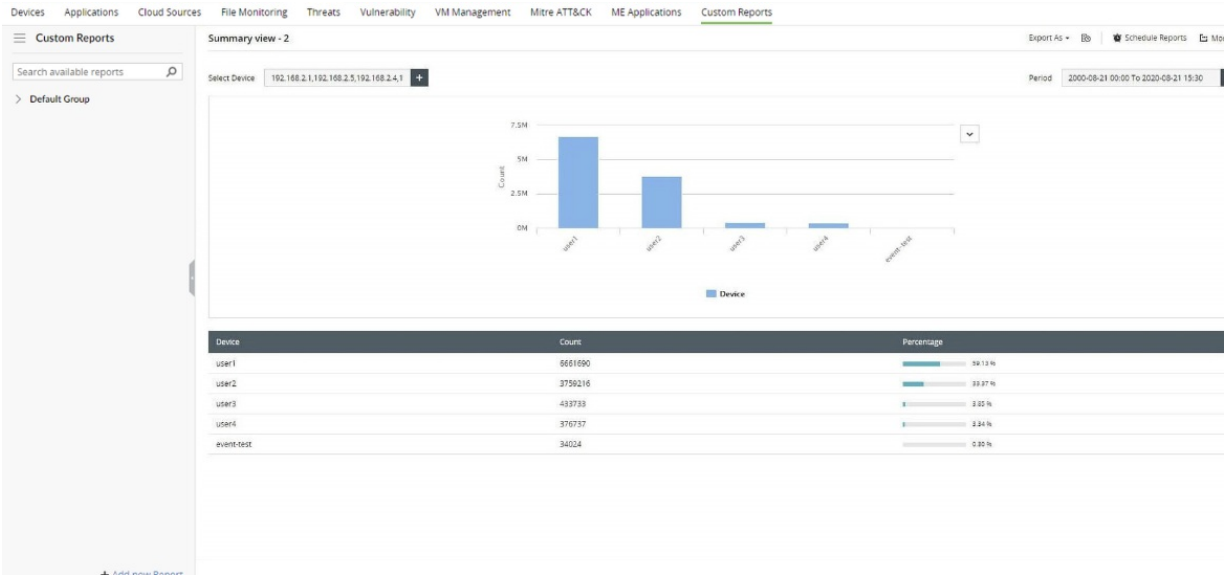






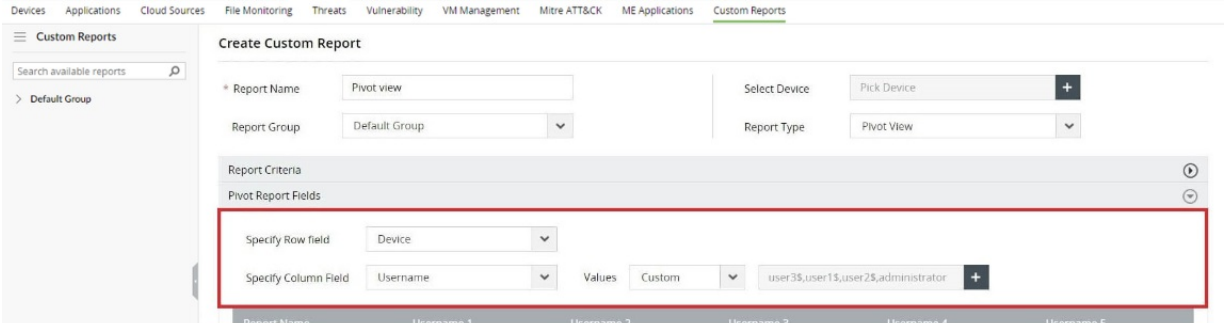
Device	Username	Severity	Count	Percentage
user1	user-1	Error	37882882	50.38 %
		Warning	5	0.00 %
	user-1$	Error	2840896	3.78 %
	local service	Error	14073	0.02 %
	anonymous logon	Error	876	0.00 %
	administrator	Warning	512	0.00 %
	el-k8r2s-64-1$	Warning	386	0.00 %
	system	Error	360	0.00 %
	prabhu	Warning	132	0.00 %
	user-5$	Error	20	0.00 %
	user-6	Error	15	0.00 %
user2	user-2	Error	18176786	24.17 %

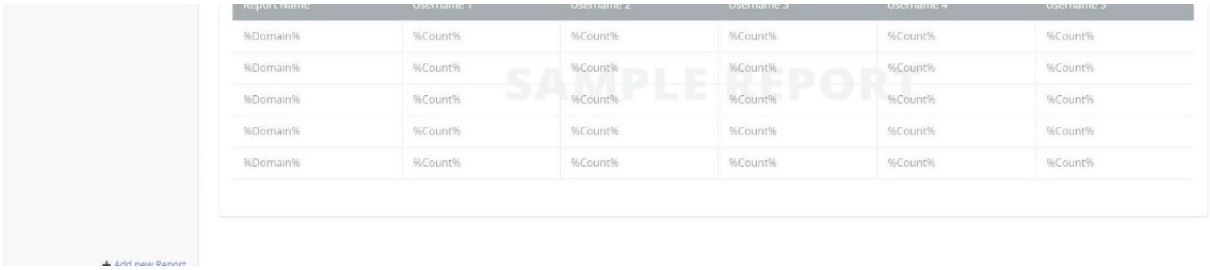
> **Note**
>
> When you apply onlyone criteria, a graph would be generated. When you apply more than one criteria, a graph would not get generated, but the data would be displayed in a table.



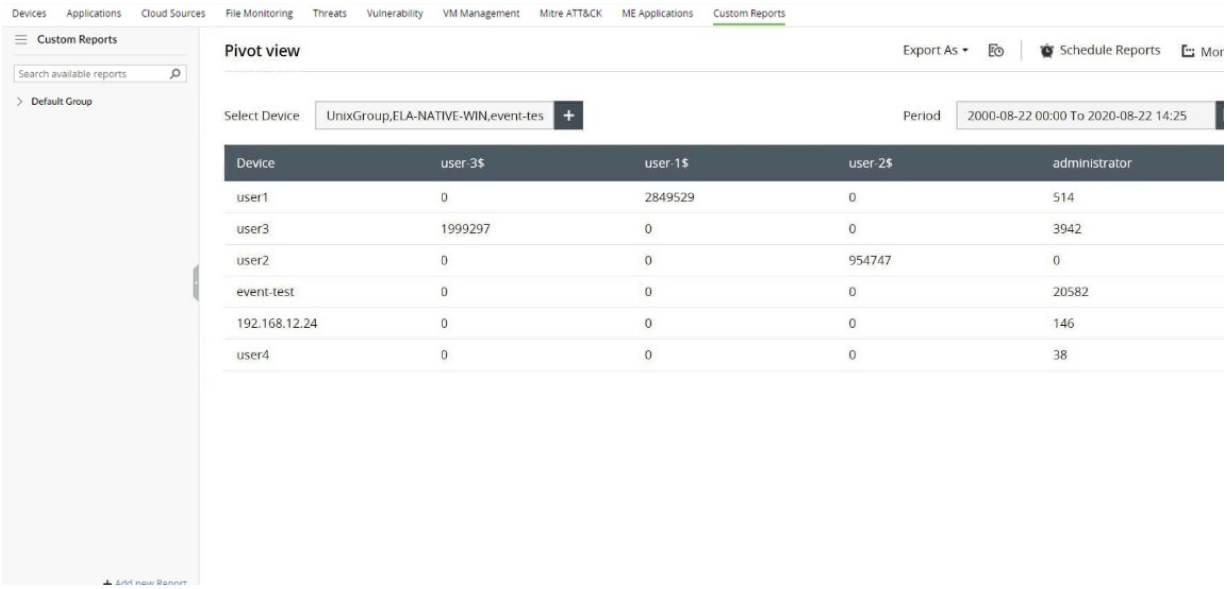
Pivot View

This view is useful when you have to monitor particular values of the field based on which the report is generated. After selecting the report criteria, you can select the field and the values in the field that you want to monitor. Each of those values will be displayed as separate columns with the'count'.



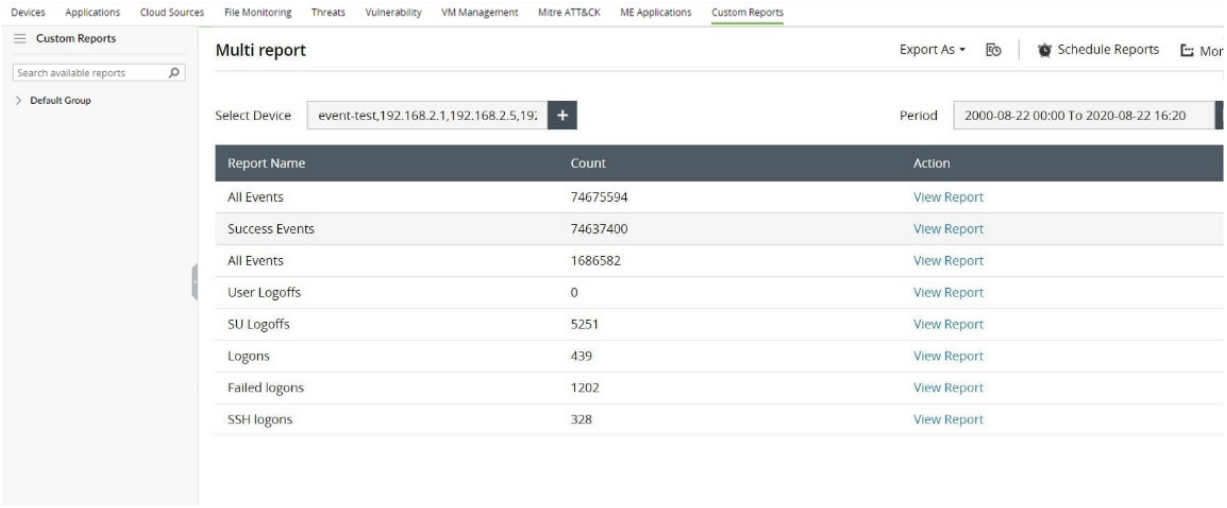


> **Note**
>
> A maximum of five values can be chosen for monitoring.



Multi Report View

This view is useful to monitor numerous reports at one glance. It will give you a holistic view of the reports that you have added to the multi report. In this view, each report has a View Report button that navigates to the original report.



8.3.5. Manage Report Views

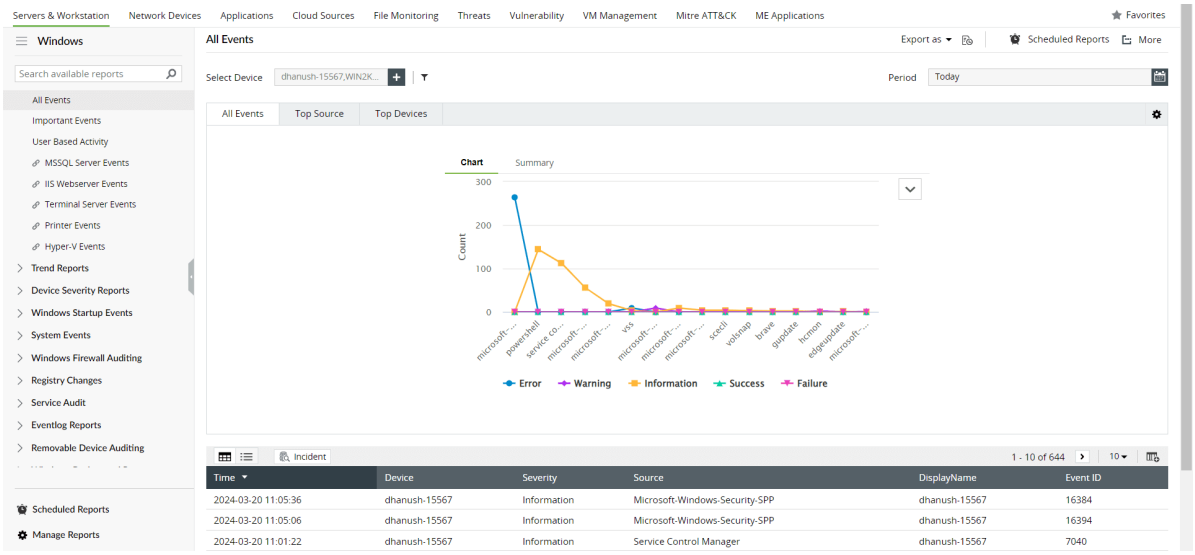
Last updated on: September 12, 2025

EventLog Analyzer allows you to create multiple views of the same report. This enables you to view the report based on different parameters such as time, domain, source, etc. The different views will be generated from the same set of log data.
In this help document, you will learn to perform the following operations.

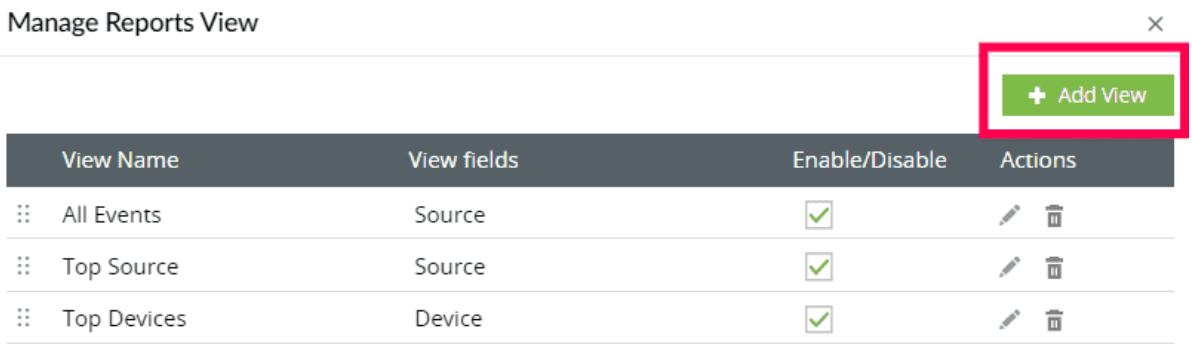
Creating a new report view

To create a new report view,

- Open EventLog Analyzer and select the Reports tab.
- Choose the required report and click on the ⚙ (Manage Custom Views) icon present on the right corner.



- In the pop-up window that appears, click on +Add View.



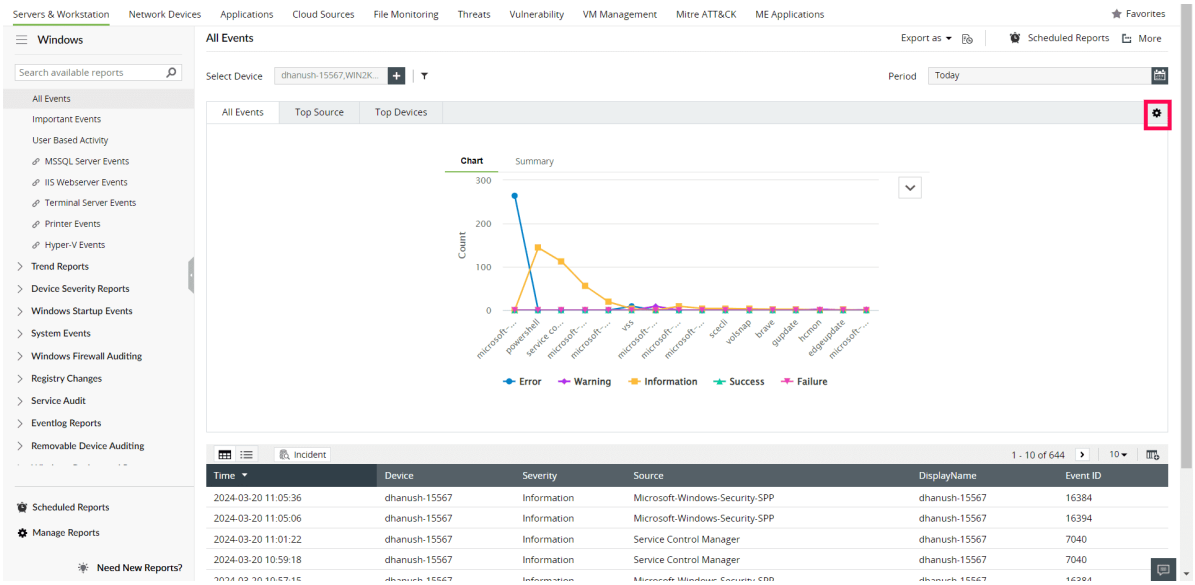


- Enter a suitable name for the view and choose the required parameters on which the view should be based. You can choose up to four different parameters.
- Click on Add.
- The new view will be added as a separate tab in the report.

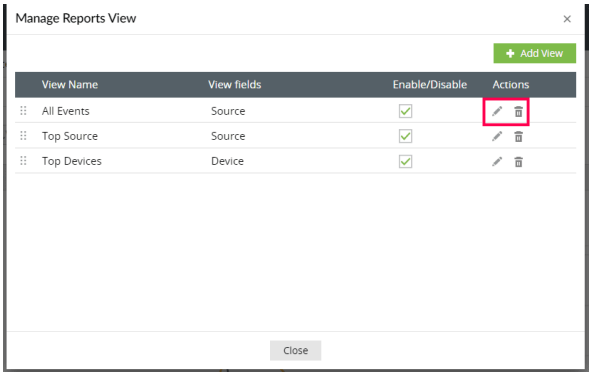
Editing, deleting, or disabling report views

To edit, delete, or disable the views that have been created:

- Open EventLog Analyzer and select the Reports tab.
- Choose the report whose views you want to edit and click on the ⚙ (Manage Custom Views) icon present on the right corner.



- In the pop-up that appears you can see a list of views for that report.



- To edit a report view, click the icon corresponding to the view that you want to modify. Make the required changes and click on Update.
- To delete a report view, click the icon corresponding to the view that you want to delete.
- To enable/disable a report view, check/uncheck the checkbox under the Enable/Disable column, corresponding to the required view.

8.3.6. Adding reports to the Favorites section

Last updated on: September 12, 2025

In this page

Adding a report to the Favorites Section

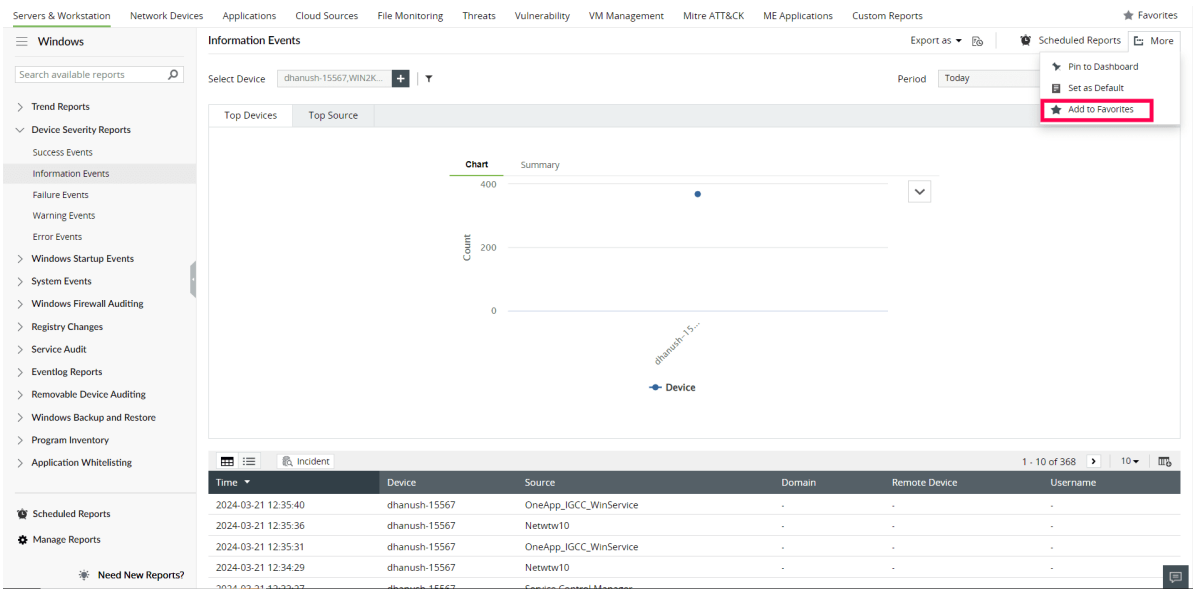
Adding a widget to the EventLog Analyzer Dashboard

If you have reports that you frequently refer to, these can either be added to the "Favorites" section or they can be pinned as a widget in the dashboard for quick access.

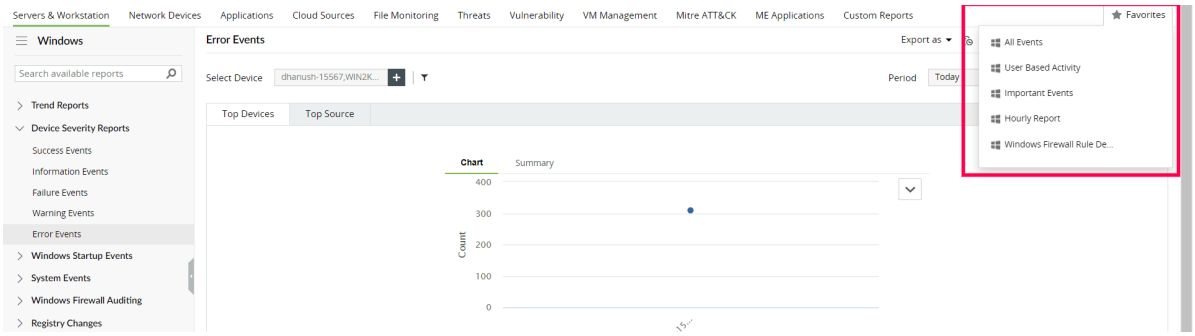
Adding a report to the Favorites Section

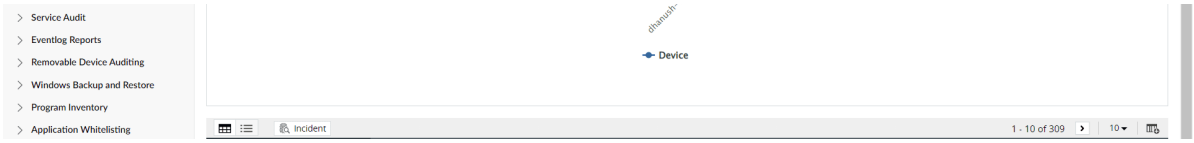
From the list of available reports, you can select up to 20 reports to be added to the Favorites section.
To add reports to Favorites,

- Navigate to the required report.



- On the right top corner of the tab, click on More and select Add to Favorites.
- The selected report will be added to the Favorites section.
- This can now be accessed quickly by clicking on "Favorites" in the top right corner.





Removing a report from the Favorites section,

- Navigate to the report which you want to remove from Favorites.
- On the right top corner of the tab, click More and select Remove from Favorites.

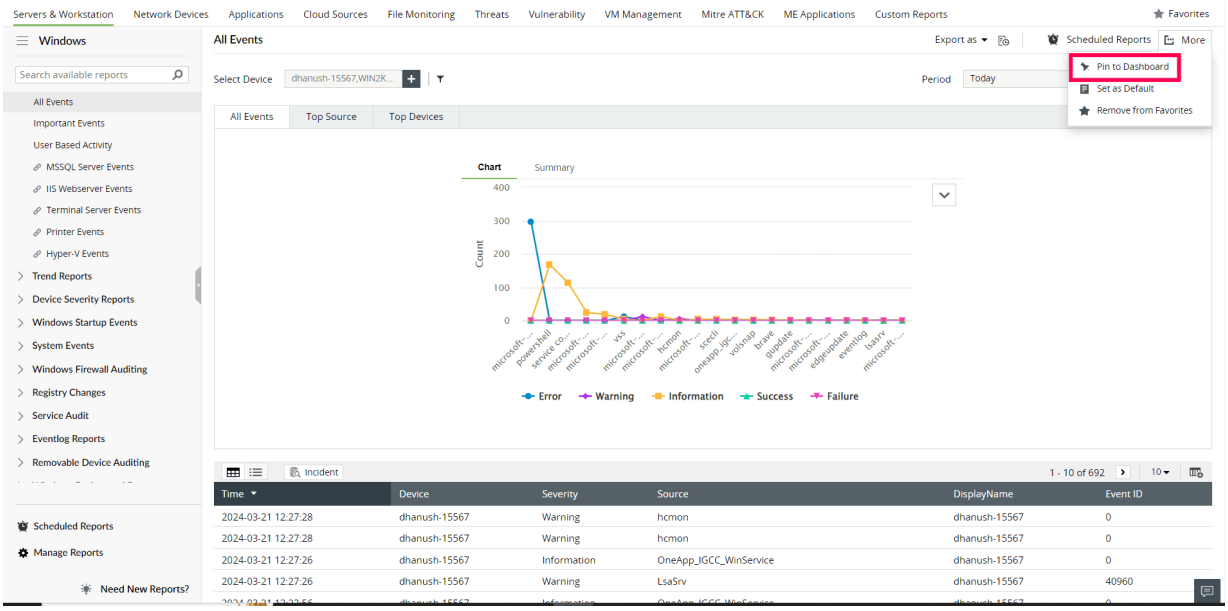
> **Note**
>
> While upgrading to the latest build of EventLog Analyzer, favorite reports in Builds 11212 and below will not be retained.

Adding a widget to the EventLog Analyzer Dashboard

Any report of your choice can be pinned to the EventLog Analyzer dashboard for a quick reference.

To pin a report,

- Navigate to the report you want to pin to the dashboard.
- In the top-right corner of the report, click More and select Pin to Dashboard.
- This report will now get added as a widget in the dashboard.



8.3.7. Report export and customization

Last updated on: September 12, 2025

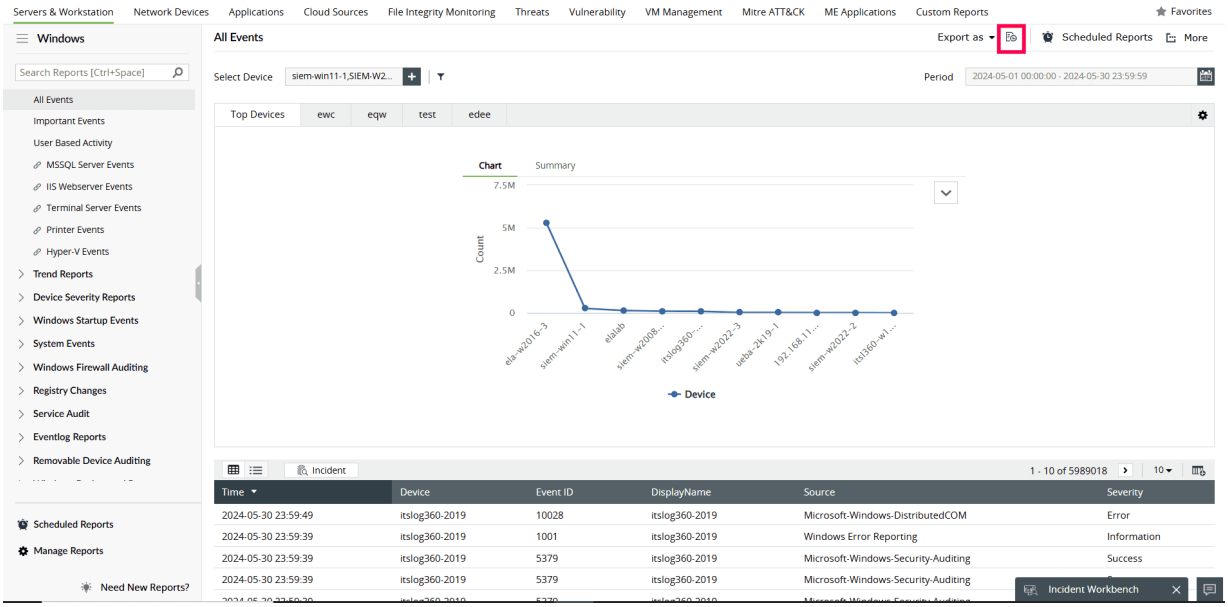
EventLog Analyzer allows you to export reports, add or remove columns in a report and pin the graph to the dashboard.
In this help document, you will learn to perform the following operations.

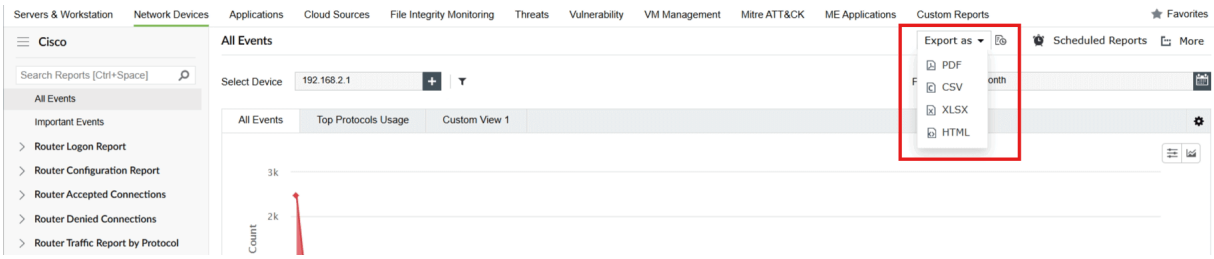
Report exporting:

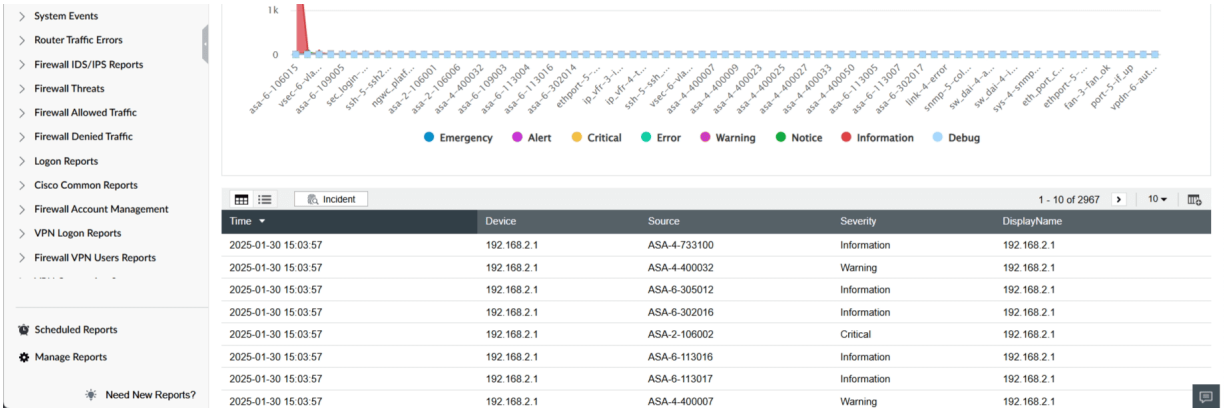
EventLog Analyzer gives users the ability to export reports as PDF, CSV, XLSX(Exports data with a default limit of 50,000 records per sheet) and HTML(Exports data into an HTML file for easier viewing in browsers)
To export reports,

- Select the report you want to export and click the Export as drop-down button on the top-right corner of the report.
- Select the format(PDF, CSV, XLSX and HTML.) in which you want the report to be exported.
- The export history section will open automatically to display the export queue.
- For each export, you have the option of downloading the report from the queue by selecting an appropriate option.

To view export history, click the at the top-right corner of a report. A list of the most recently exported reports will be displayed.







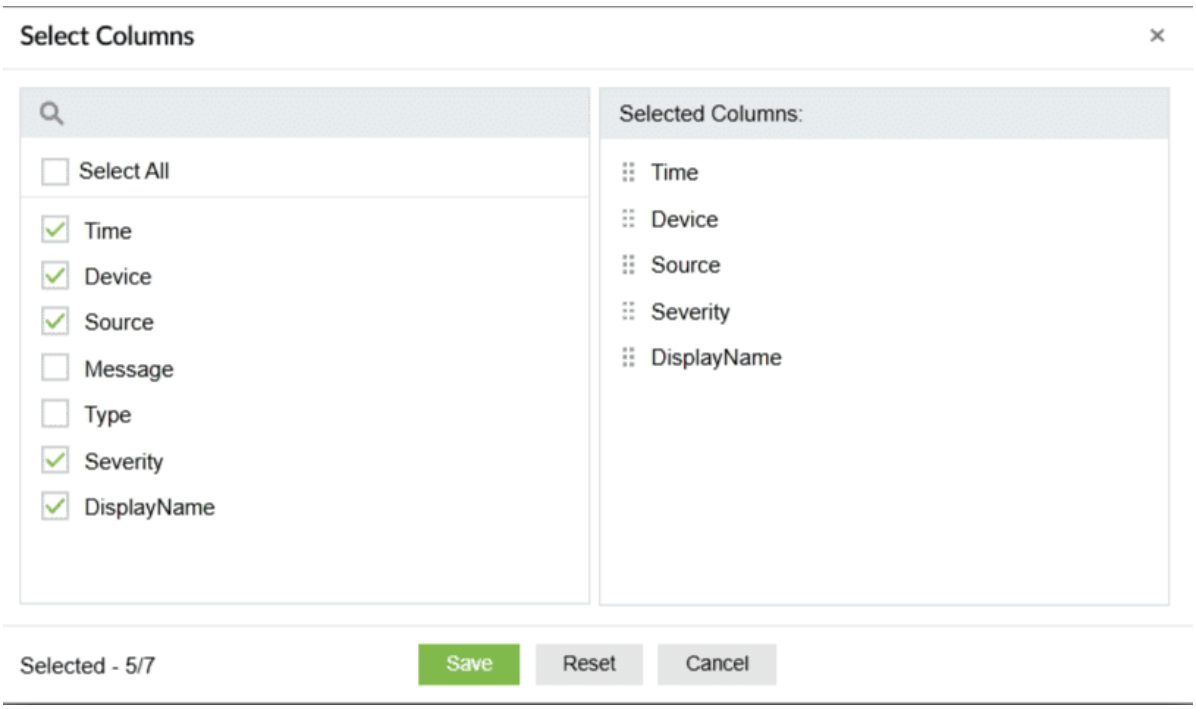
> **Note**
>
> XLSX and HTML exports will include only tabular data and will not include graphs.

Adding or removing columns:

EventLog Analyzer gives users the ability to add or remove columns to the reports.

To add or remove columns:

- Select the report you want to add or remove columns and click on the top-right corner of the report.
- In the pop-up window, select the fields you want to display in the search results by ticking the corresponding boxes. To exclude fields, simply leave the boxes unticked.



- You can also rearrange the selected columns by dragging and dropping the column names accordingly, in the Selected Columns section.

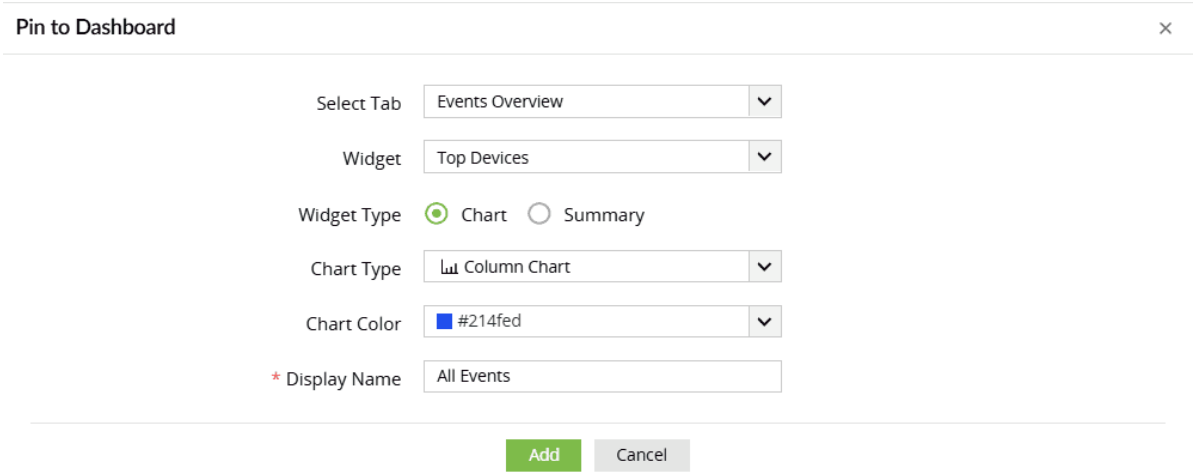
- Click Save to apply your preferences.
- Now you have the options to Select all and Reset back to default settings.

> Note:
> - When the reports are exported, the columns that have been selected will be represented.
> - Select All will be shown only when the Number of Fields is less than 10.

Pinning the graph to the dashboard:

EventLog Analyzer gives users the ability to pin graphs to the dashboard.
To pin a graph:

- Select the report you want to pin.
- Click the More drop-down button on the top right corner and select Pin to Dashboard.
- In the pop-up window, you can select the tab, widget, widget type, and display name of the widget that you'd like to pin.



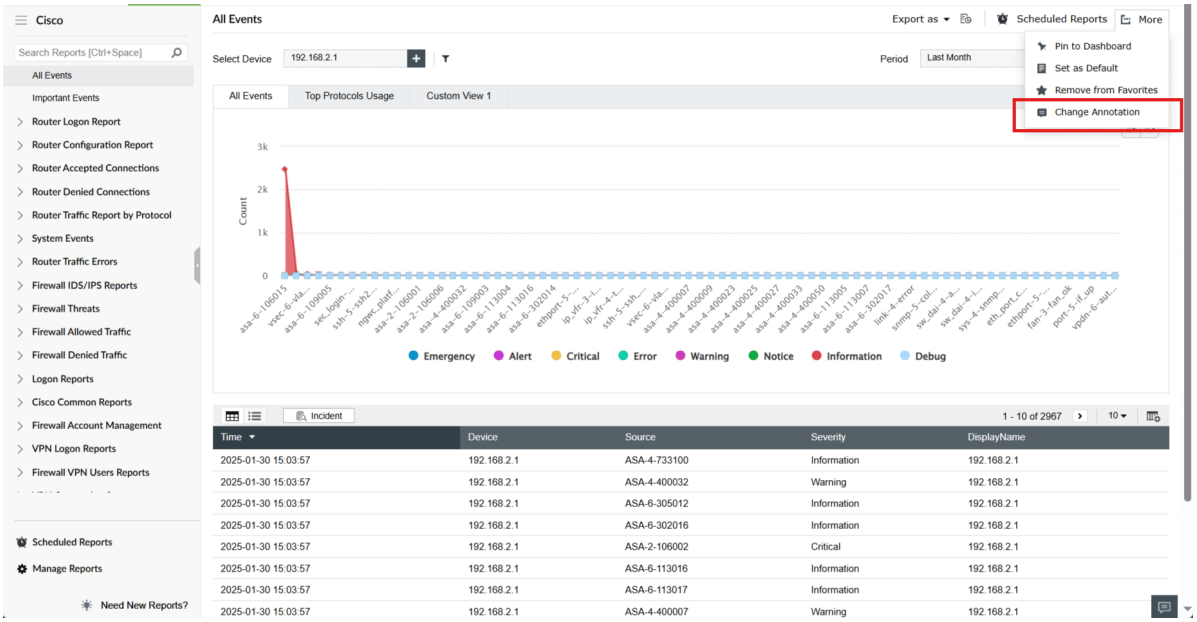
- Click Add to save your preferences.

Adding Annotation to Report Export

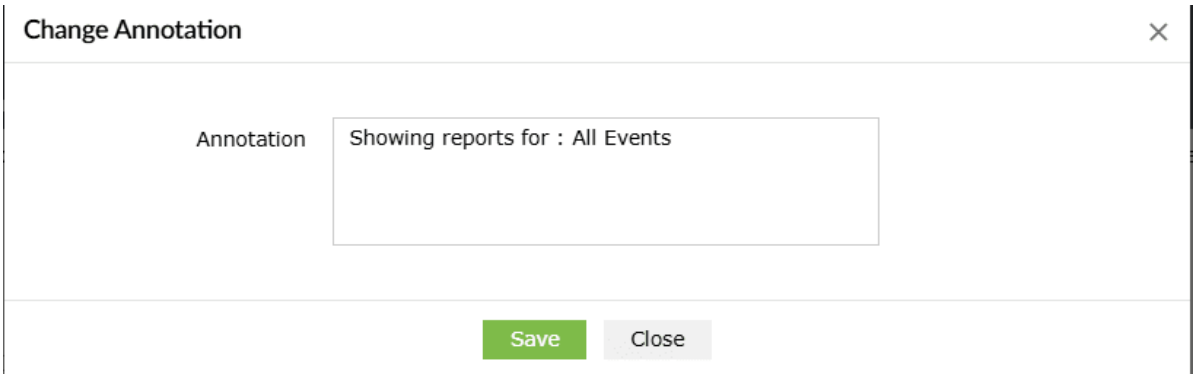
You can add custom annotations for the reports. These annotations will be displayed in PDF, HTML, and XLSX Report exports.
To add annotation,

- Navigate to the report you want to add Annotation.
- In the top-right corner of the report, click More and select Change Annotation.





- Update the annotation to the desired requirement. Click "Save".



- All the above-mentioned exports of this report will have Custom Annotation from now on.

Calendar Functionality

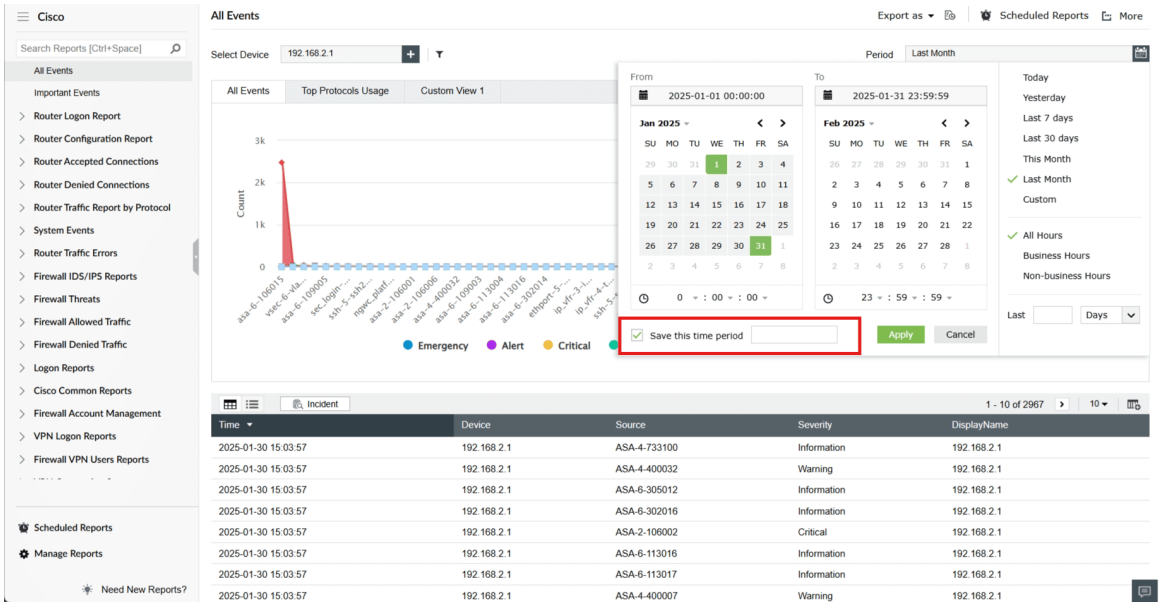
The Calendar Functionality feature introduces enhanced options for managing date ranges. This functionality provides greater flexibility and efficiency when working with date-specific data.

> NOTE: The calendar functionality is also accessible through dashboard, search, correlation, alerts, workflow-history, renindex and compliance tabs.

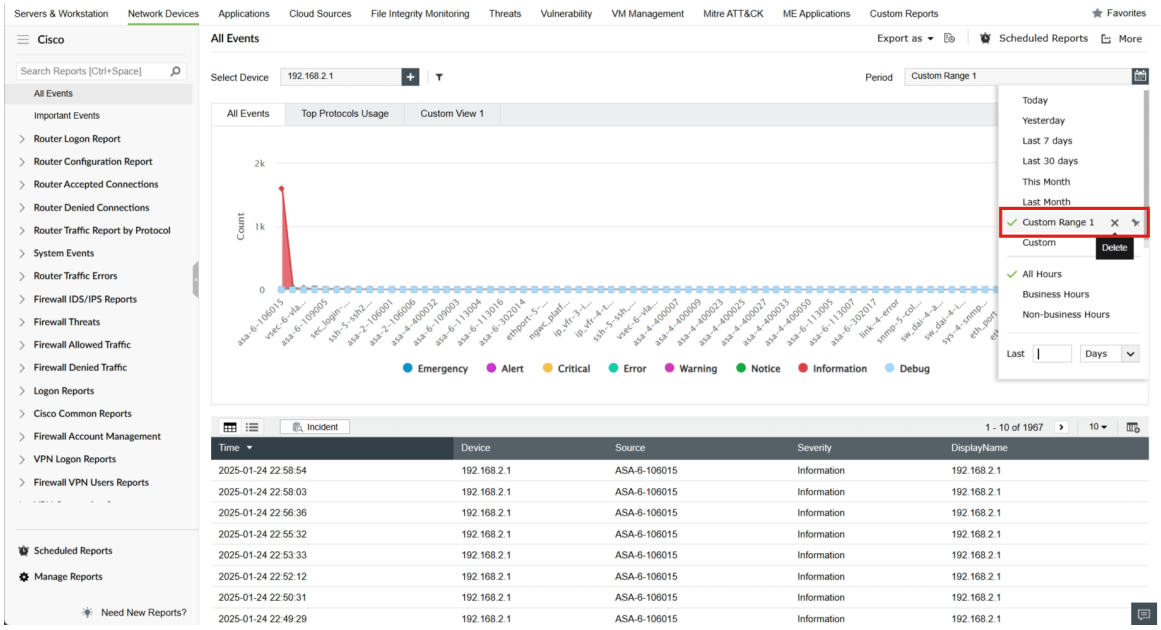
The date ranges can be managed in two ways as follows:

1. Custom Ranges:
   - Create new date ranges by selecting the Custom Range option.



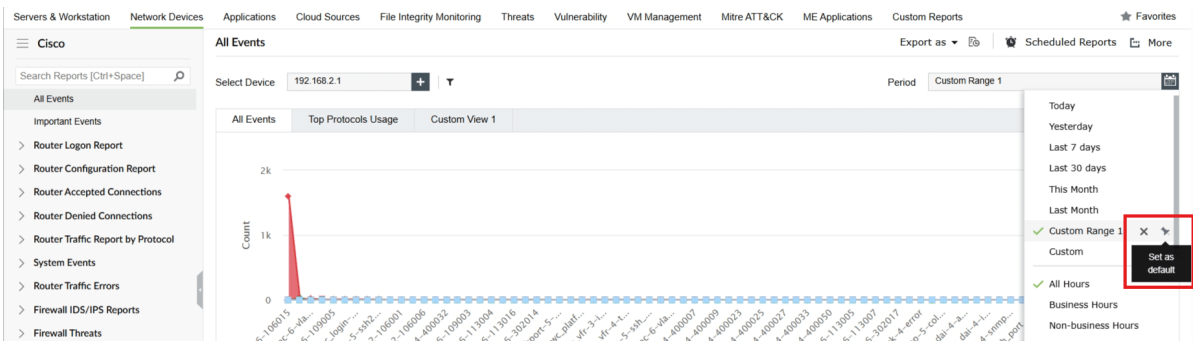


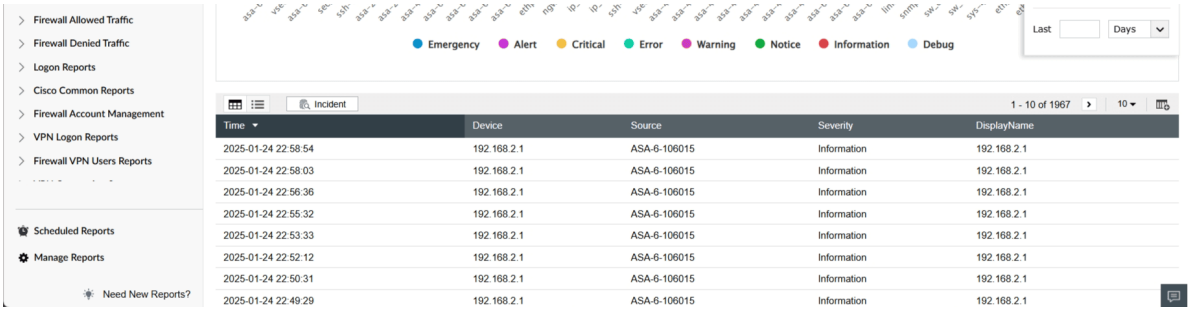
- Easily delete any custom ranges that are no longer needed.



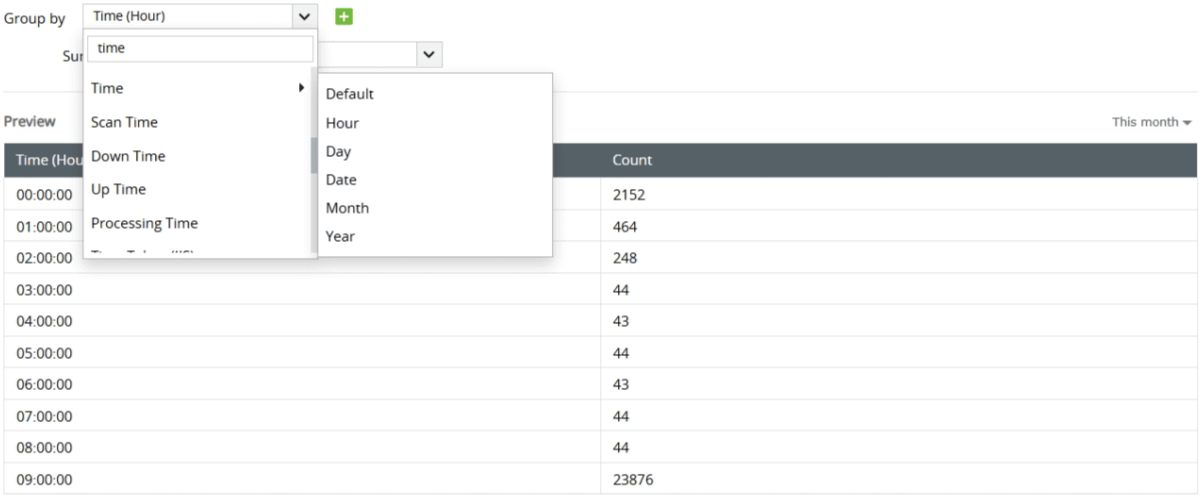
2. 2. Pinned Calendar Ranges:

- Pin a specific calendar range to a report.
- The pinned range will automatically load each time the report is accessed or reloaded, ensuring consistency and saving time.





Field Units



When creating a Custom Report or Report Views based on summary or pivot view, the following units are available for the field Time, which will determine the unit of time:

Hour - The time will be represented hour-wise.

Day - The time will be represented day-wise (by days of the week).

Date - The time will be represented date-wise (by dates of the month).

Month - The time will be represented month-wise (by months of the year).

Year - The time will be represented year-wise.

Default - The time unit will adjust dynamically based on the selected time range in the date range picker. For example, if the time range is more than one hour, the time will be shown hour-wise; if the range exceeds one day, it will be displayed date-wise, and so on.

> **Note**
>
> If a custom report or report view is based on the time unit "Hour", the time range is restricted to a maximum of 12 months for viewing data.

8.4.1. Overview

Last updated on: September 12, 2025

To meet industry and legal standards, organizations are required to retain and monitor audit data that demonstrates their compliance posture. ManageEngine Log360 simplifies this by offering a dedicated compliance reporting module that fetches relevant event data from log sources and displays it as structured reports aligned with various global and industry-specific regulations.
Log360 supports a wide range of predefined compliance mandates. These reports are displayed as visual representations of audit data. In addition to built-in compliance standards, the users can also create custom reports tailored to meet their business requirements.
Below is a list of pre-defined compliance regulations supported by the product.

Compliance	Description
Federal Information Security Management Act (FISMA)	Requires U.S federal agencies to provide security for information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.
Personal Data Protection Act (PDPA)	Aims to protect the personal information of Filipino citizens by regulating organizations to maintain secure systems for storing and managing it.
California Consumer Privacy Act (CCPA)	A privacy regulation that requires businesses to implement security measures to protect the personal data of California residents.
California Privacy Rights Act (CPRA)	An amendment to the CCPA that introduces stricter requirements for protecting personal data. It strengthens consumer privacy rights and mandates businesses to safeguard data, report breaches, and ensure compliance.
Payment Card Industry Data Security Standard (PCI DSS 4.0)	A set of 12 processes and practices designed to ensure the safe and secure transfer of payment card data. It aims to improve the safety of consumer data and trust in the payment ecosystem.
Sarbanes-Oxley Act (SOX)	A law enacted in the United States to ensure the accuracy, reliability, and protection of financial information from unnecessary disclosures by business entities. This compliance regulation is designed to increase transparency around financial reporting with defined processes for internal controls.
Health Insurance	An United States federal law to protect the patient's personally identifiable

Compliance	Description
Portability and Accountability Act (HIPAA) check	An United States federal law to protect the patient's personally identifiable information from fraud and theft while also improving the portability of health insurance coverage for workers.
Gramm-Leach-Bliley Act (GLBA) check	Also known as the Financial Services Modernization Act, this regulation sets standards for financial institutions to ensure the confidentiality and security of customer's financial records and personal information.
Protection of Personal Information Act (POPIA)	A regulatory mandate aimed at safeguarding the personally identifiable information (PII) of South African citizens. It provides conditions for the lawful collection and processing of personal data of the citizens by all public and private organizations residing both in and outside the Republic of South Africa.
Good Practice Guide 13 (GPG13)	A framework with 12 protective monitoring controls (PMCs) for all His Majesty's Government (HMG) organizations. It is defined by the Communications-Electronics Security Group, Britain’s information assurance authority.
Cyber Essentials	A United Kingdom government-backed certification for organizations that ensures organizations have a set of basic security controls to secure their IT infrastructure from common cyber threats. These security controls help protect sensitive data while mitigating cyber risks.
International Organization for Standardization / International Electrotechnical Commission 27001, version 2013 (ISO 27001:2013)	Mandates organizations to manage the security of critical assets such as financial data, intellectual property, employee records, customer data, and other confidential information.
International Organization for Standardization / International Electrotechnical Commission 27001, version 2022 (ISO 27001:2022)	A framework that outlines best practices for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). It ensures that organizations have appropriate controls in place to safeguard information assets such as confidential data, personal information, and intellectual property.
Information security	A security framework that mandates organizations to protect sensitive data and

Compliance	Description
level protection (ISLP)	A security framework that mandates organizations to protect sensitive data and maintain proper information security practices.
Nuclear Regulatory Commission Regulatory Guide 5.71 (NRC RG 5.7)	A U.S. regulation that provides cybersecurity requirements for protecting digital systems used in nuclear facilities. It outlines defensive strategies, security controls, and monitoring practices to prevent cyberattacks that could impact safety, security, or emergency response functions.
General Data Protection Regulation (GDPR)	A European Union regulation that sets strict guidelines on how organizations collect, process, and store personal data. It aims to give individuals more control over their personal information and ensures consistent data privacy practices across the EU.
Family Educational Rights and Privacy Act (FERPA)	A United States federal law that governs the privacy of student education records. It applies to all educational institutions receiving funding from the U.S. Department of Education.
North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)	A set of standards designed to strengthen the security of the bulk power system across the United States, parts of Canada, and one state in Mexico.
Code of Connection (CoCo)	A UK government standard that defines security requirements for local authorities connecting to the Government Connect Secure Extranet (GCSX), a component of the Public Services Network (PSN). It is based on ISO 27001 principles and covers technical, procedural, physical, and human risk categories.
Cybersecurity Maturity Model Certification (CMMC)	A U.S. Department of Defense framework that requires contractors and subcontractors to follow specific cybersecurity practices to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).
National Institute of Standards and Technology (NIST CSF)	A set of voluntary guidelines developed by the U.S. National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risks across their operations and critical infrastructure.
Qatar Cybersecurity	A set of guidelines developed by Qatar's National Cyber Security Committee (NCSC) to help organizations implement and maintain cybersecurity best practices. It outlines six core components: strategy and governance, risk

Framework (QCF) Compliance	management, protection, detection and response, recovery, and collaboration and partnership. Description
Trusted Information Security Assessment Exchange (TISAX)	A cybersecurity standard developed by the German automotive industry association (Verband der Automobilindustrie - VDA) to ensure the secure processing of sensitive data within the automotive sector. TISAX helps manufacturers and suppliers maintain high security standards and build trust across the supply chain.
Saudi Arabian Monetary Authority (SAMA)	A cybersecurity framework established by the central bank of Saudi Arabia to guide and regulate financial institutions. The framework helps member organizations identify and address cybersecurity risks and outlines security requirements for their employees, subsidiaries, third parties, and customers.
Essential Cybersecurity Controls (ECC)	A cybersecurity framework Saudi Arabia that outlines key measures and best practices to help organizations protect their systems and data from cyber threats. It provides structured guidelines and controls covering areas such as access control, incident response, network security, and data protection, aimed at strengthening overall cybersecurity posture and reducing risk.
Personal Data Protection Law (PDPL)	A data privacy law from Saudi Arabia that regulates the collection, processing, disclosure, and retention of personal data. It is designed to protect individuals' privacy and ensure responsible data practices. Initially overseen by the Saudi Data and Artificial Intelligence Authority (SDAIA), its supervision may be transferred to the National Data Management Office.
Criminal Justice Data Communications Network (CJDN)	A secure communication infrastructure operated by the Minnesota Bureau of Criminal Apprehension (BCA) to enable authorized criminal justice agencies to access and share Criminal Justice Information (CJI). CJDN enforces compliance with the FBI's Criminal Justice Information Services Security Policy (CJISSECPOL), ensuring that CJI is transmitted, processed, and stored securely across Minnesota law enforcement networks.
UAE Signals Intelligence Agency (UAE-NESA)	A cybersecurity framework developed by the UAE’s Telecommunications and Digital Government Regulatory Authority (TDRA). It defines a set of management and technical controls to establish, implement, maintain, and enhance the nation’s information security measures and supports the country’s National Cyber Security Strategy.
Service Organization Control Type 2 (SOC 2)	A framework developed by the American Institute of Certified Public Accountants (AICPA) to ensure organizations have cybersecurity measures in place to protect their customer's sensitive data.

Compliance	Description
General Data Protection Law of Brazil (LGPD)	Governs the collection, use, processing, and storage of personal and sensitive data. It aligns Brazil with global data protection standards like the GDPR and mandates strict controls to safeguard individual's privacy.
Federal Act on Data Protection (FADP)	A data protection law enforced in Switzerland that governs the collection, processing, and storage of personal data. It enhances privacy rights, places stricter obligations on organizations handling personal information, and ensures transparency and accountability in data processing activities.
Network and Information Security Directive 2 (NIS 2)	A European Union (EU) directive that sets cybersecurity risk management and reporting requirements for essential and important entities across sectors such as energy, healthcare, finance, and digital infrastructure. It expands the scope of the original NIS Directive, imposes stricter security obligations, and establishes uniform penalties to strengthen resilience against cyber threats within the EU.

Read also

This section explained the importance of compliance reports and how the product aligns with various global and industry-specific regulations. To learn how to configure and manage compliance capabilities in your environment, refer to the following articles:

- Configuring custom compliance reports
- Managing compliance regulations

8.4.2. Configuring custom compliance reports

Last updated on: September 12, 2025

In this page

Overview

Steps to configure custom compliance reports

Overview

This page details how to configure custom compliance reports to meet specific regulatory and organizational requirements. By creating a new compliance mandate, selecting relevant data sources, and mapping appropriate reports, you can generate structured audit data tailored to your compliance needs. These reports support internal audits, demonstrate adherence to standards, and simplify compliance reporting.

Steps to configure custom compliance reports

1. In your Log360 account, navigate to the Compliance tab.
2. In the top-right corner, click Manage Compliance.

> NOTE
>
> You can also configure pre-defined compliance mandates source by clicking the Configure Source option in the Compliance tab.

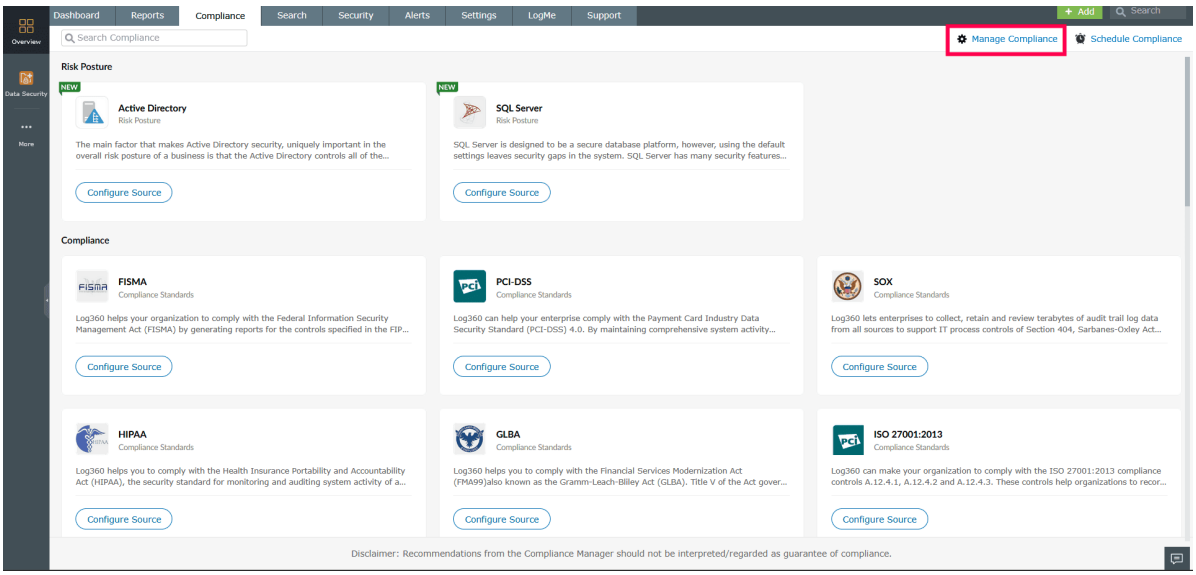


Figure 1: Configuring custom compliance reports

3. Click Create New Compliance.

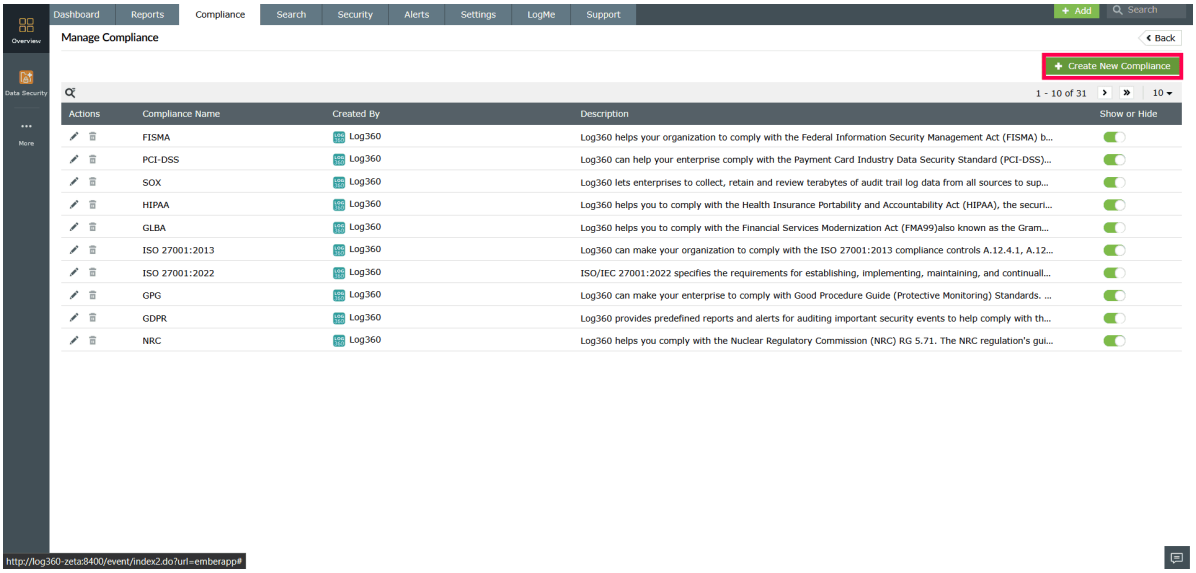


Figure 2: Configuring custom compliance reports

4. In the Add Compliance page, enter a name for the compliance mandate in the Compliance Name field and click the ✓ icon to save it.

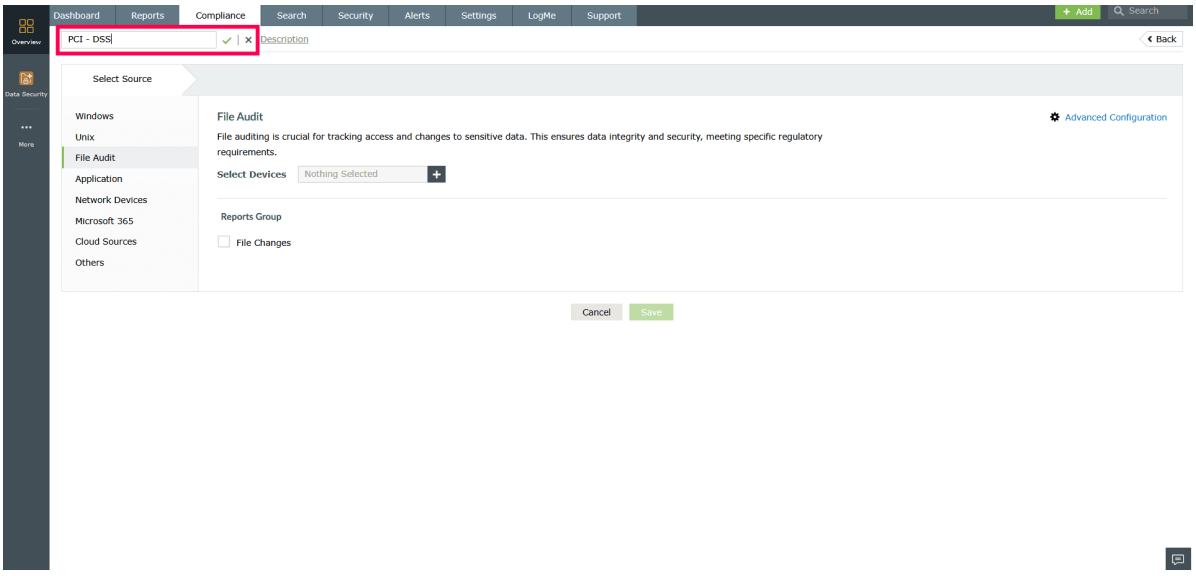


Figure 3: Naming compliance mandate

5. Click Description to add details about the compliance mandate, and click OK to save.

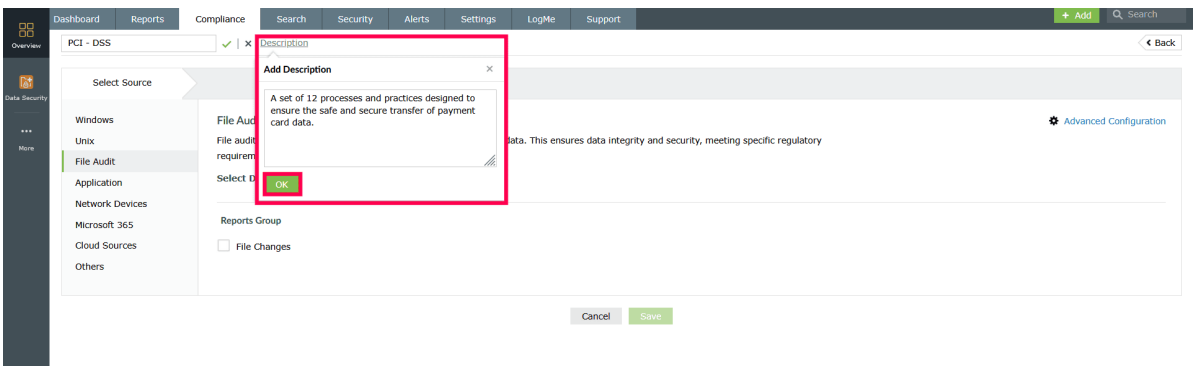


Figure 4: Adding a description for the compliance

6. Under Select Source, click the relevant device tab.

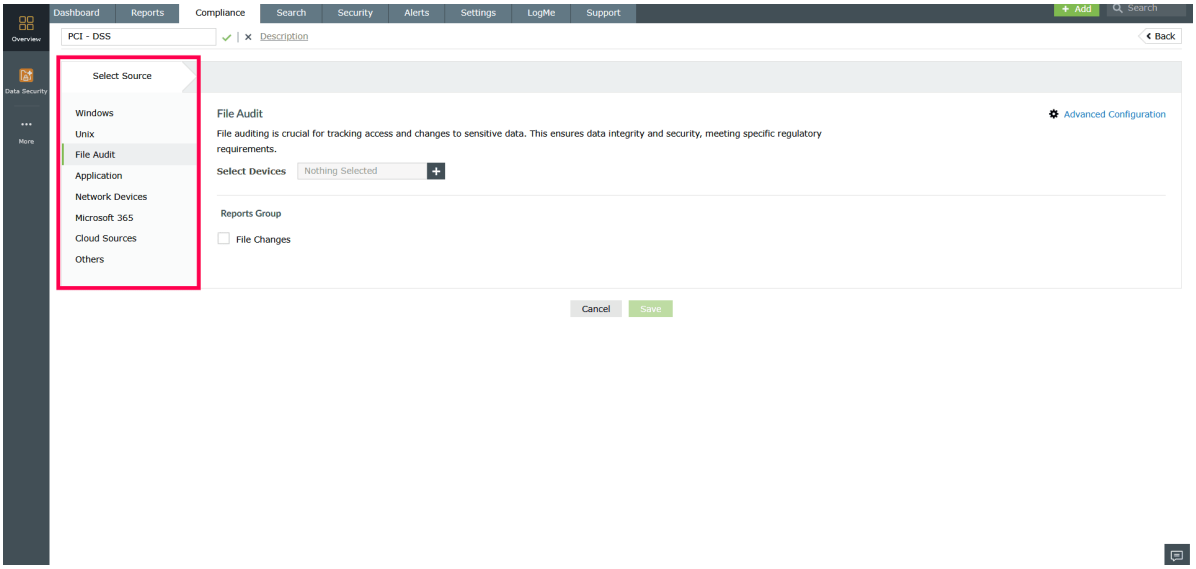


Figure 5: Selecting a source

7. Click Advanced Configuration to select a specific product.

> **NOTE**
>
> Currently, advanced configurations are available only for the File Audit and M365 tabs.

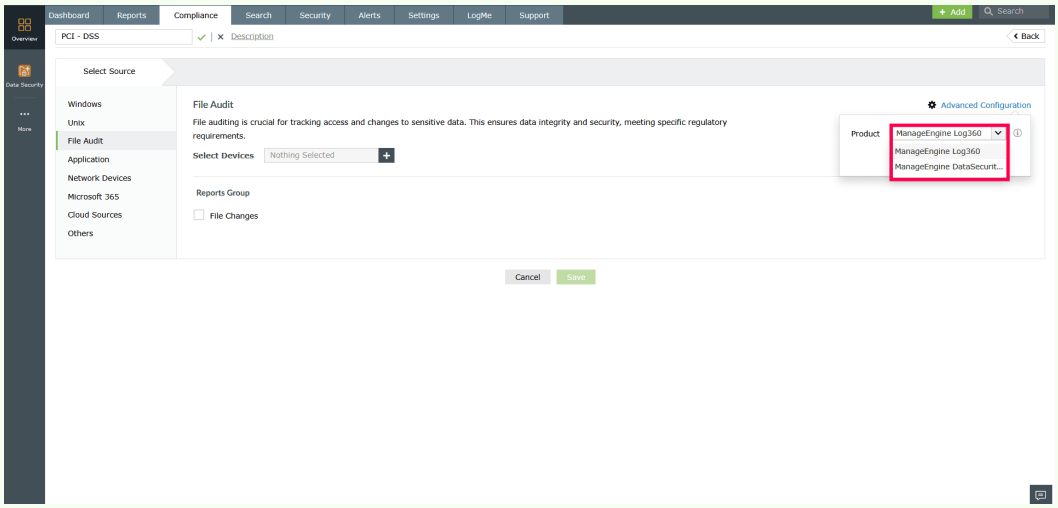


Figure 6: Advanced Configuration settings

8. Click Save to confirm your selection. This will display the corresponding set of available reports and devices.

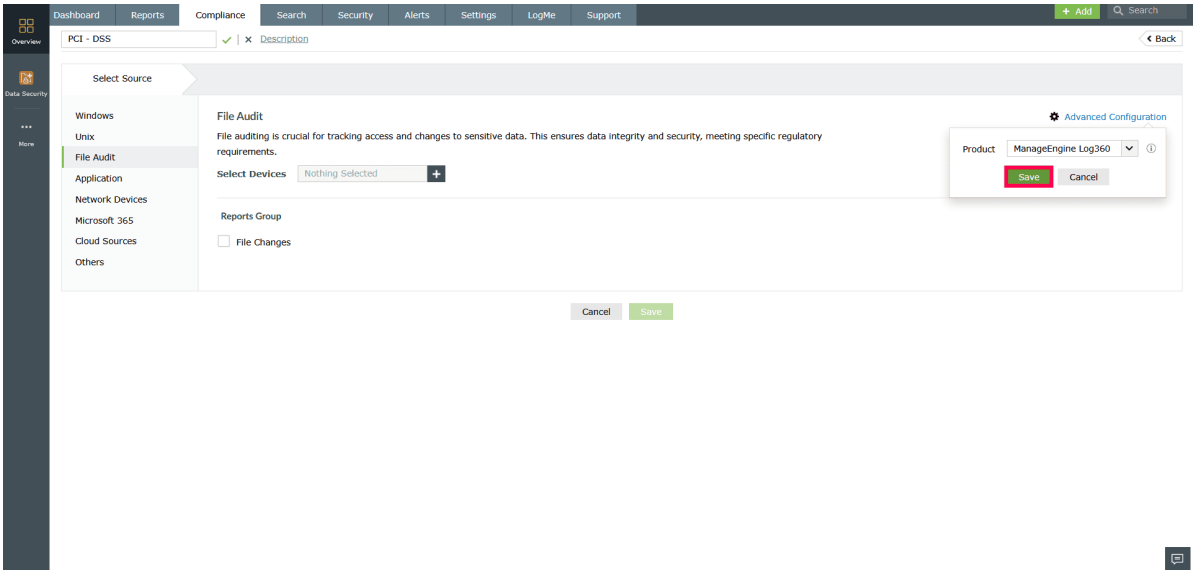


Figure 7: Advanced Configuration settings

9. Select sources based on your requirement.
10. Click Save to finalize the custom compliance configuration.

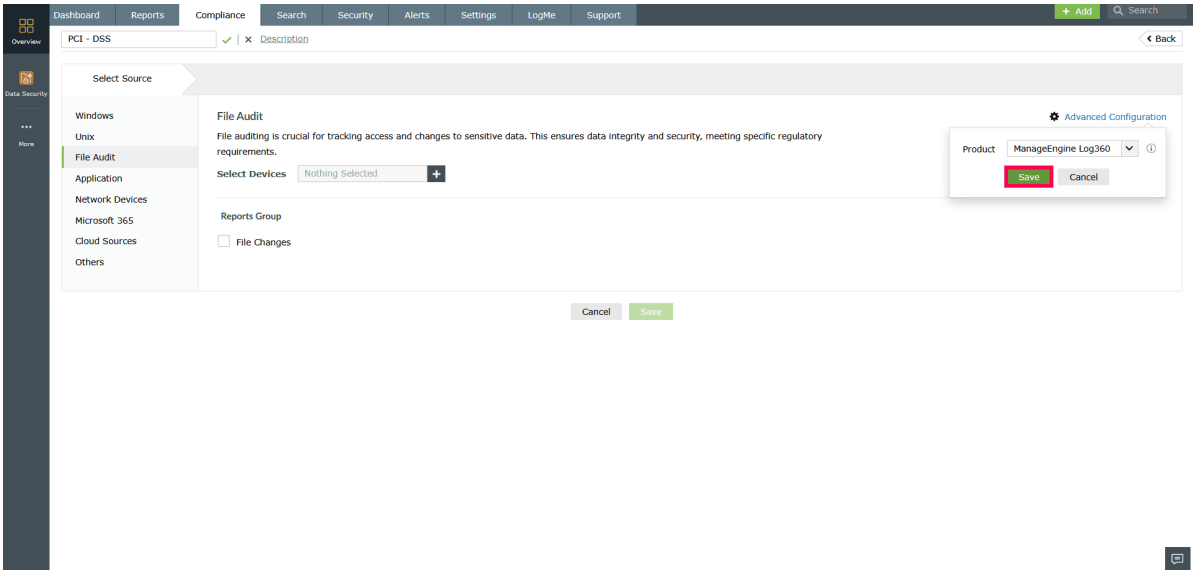


Figure 8: Configuring custom compliance reports

Read also

This page elaborated on configuring custom compliance reports. To manage and schedule compliance reporting, refer to the following articles:

- Managing compliance regulations
- Scheduling compliance reports

8.4.3. Managing compliance regulations

Last updated on: September 12, 2025

In this page

Overview

Searching compliance regulations

Editing compliance regulations

Deleting compliance regulations

Enabling or disabling compliance regulations

Overview

This page elaborates on managing compliance regulations within the product console. It covers key actions such as searching for specific mandates, editing their configurations, enabling or disabling them, and deleting custom compliance mandates. These options help ensure that your compliance framework remains current, relevant, and aligned with your business requirements.

Searching compliance regulations

1. In the Manage Compliance page, click the icon in the top-left corner.
2. Type the name of the compliance regulation.

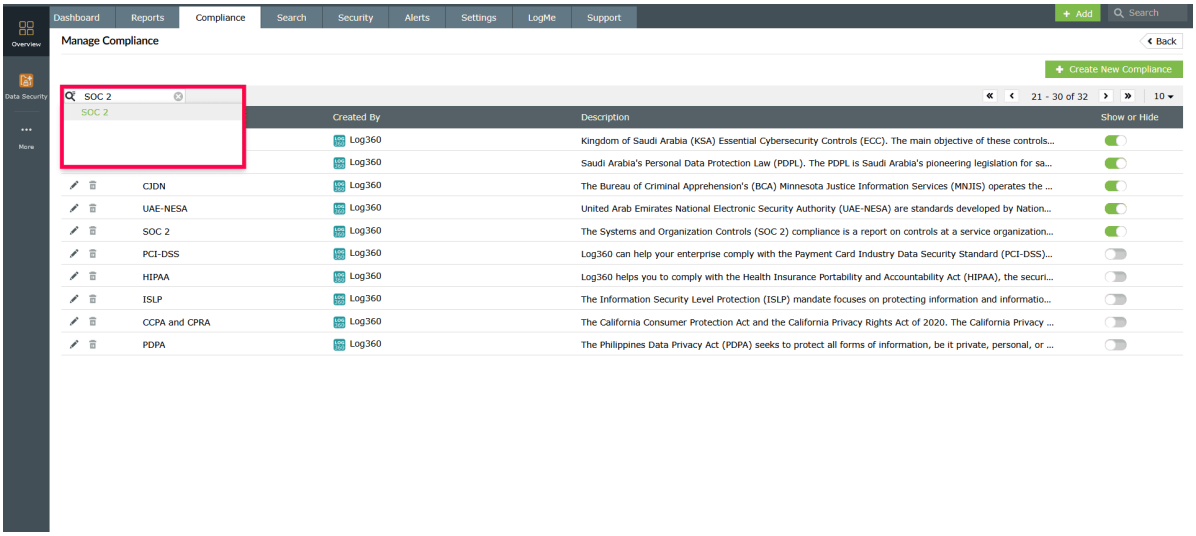
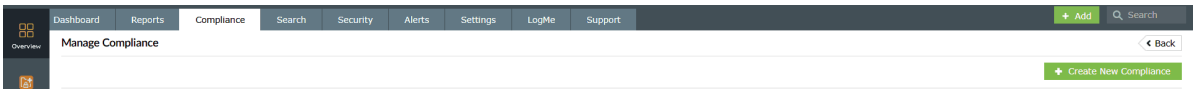


Figure 1: Searching for a compliance mandate

3. Matching results will appear in a dropdown. Select the desired regulation from the list.



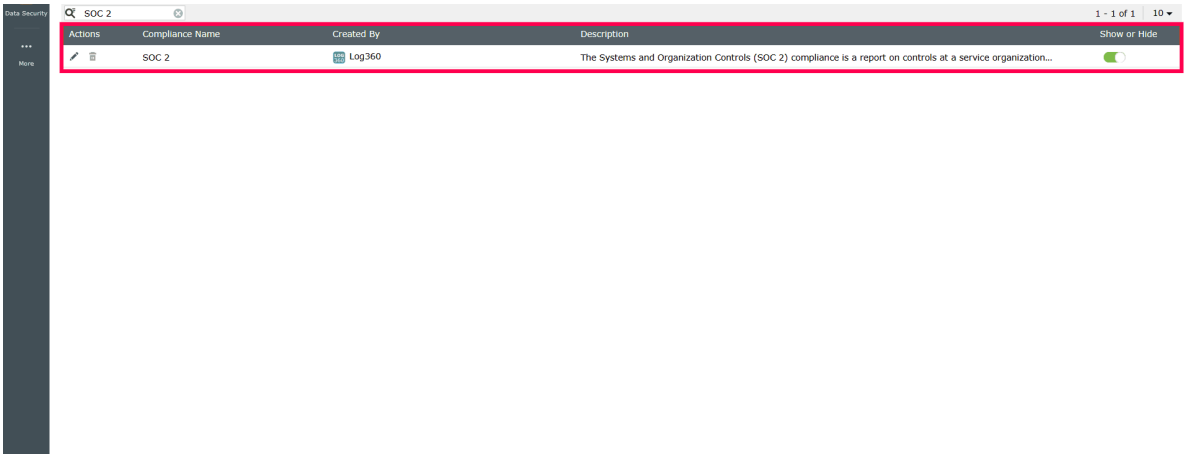


Figure 2: Searching for a compliance mandate

Editing compliance regulations

1. In the Manage Compliance page, click the icon next to the compliance mandate you want to update.

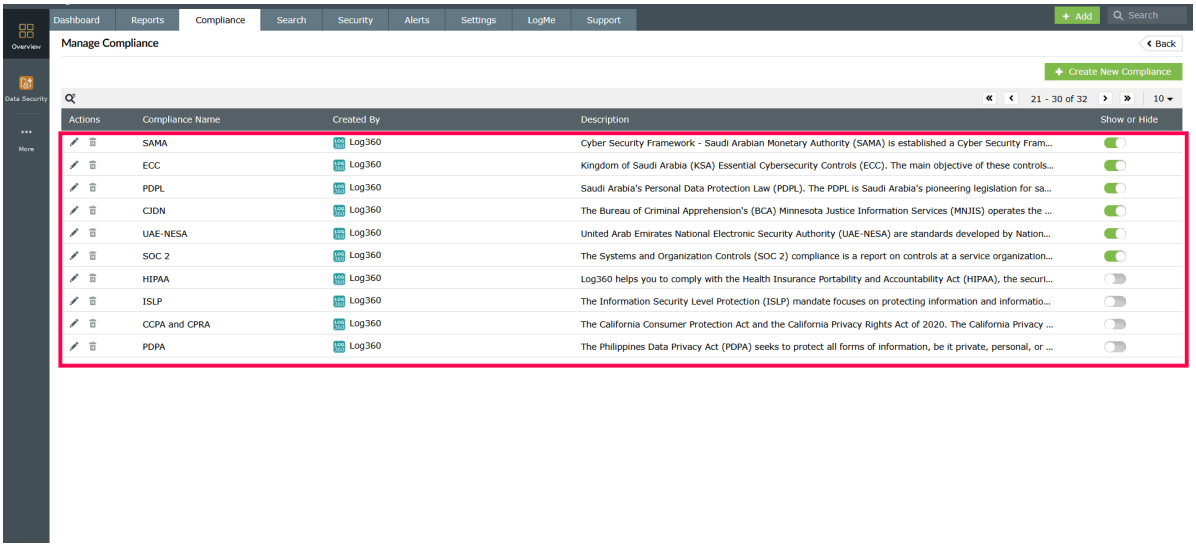


Figure 3: Editing a compliance mandate

2. In the Edit Compliance page, make the required changes.

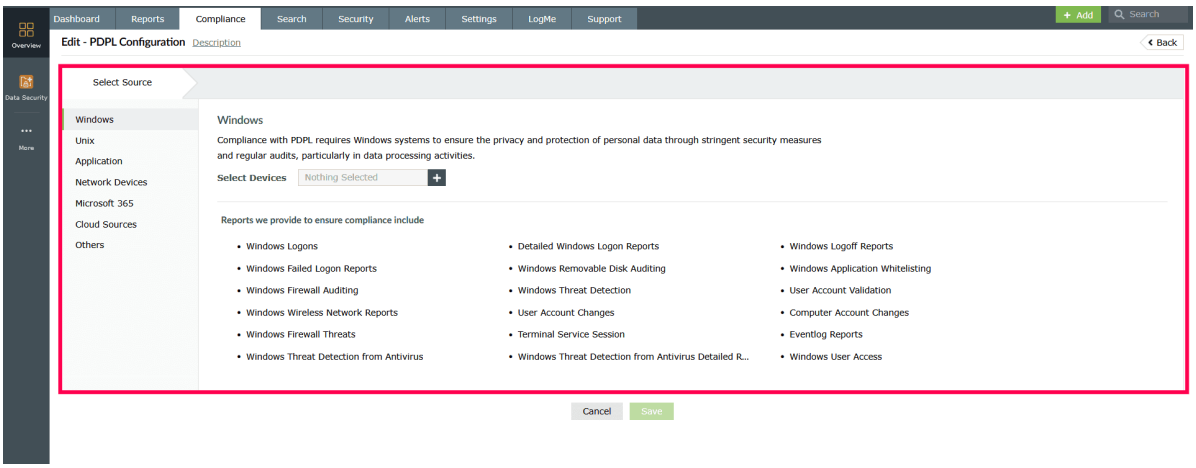


Figure 4: Editing a compliance mandate

3. Click Save to apply the changes.

Deleting compliance regulations

> NOTE
>
> The Default Compliance cannot be deleted.

1. In the Manage Compliance page, locate the compliance mandate you want to remove.
2. Click the icon next to it.

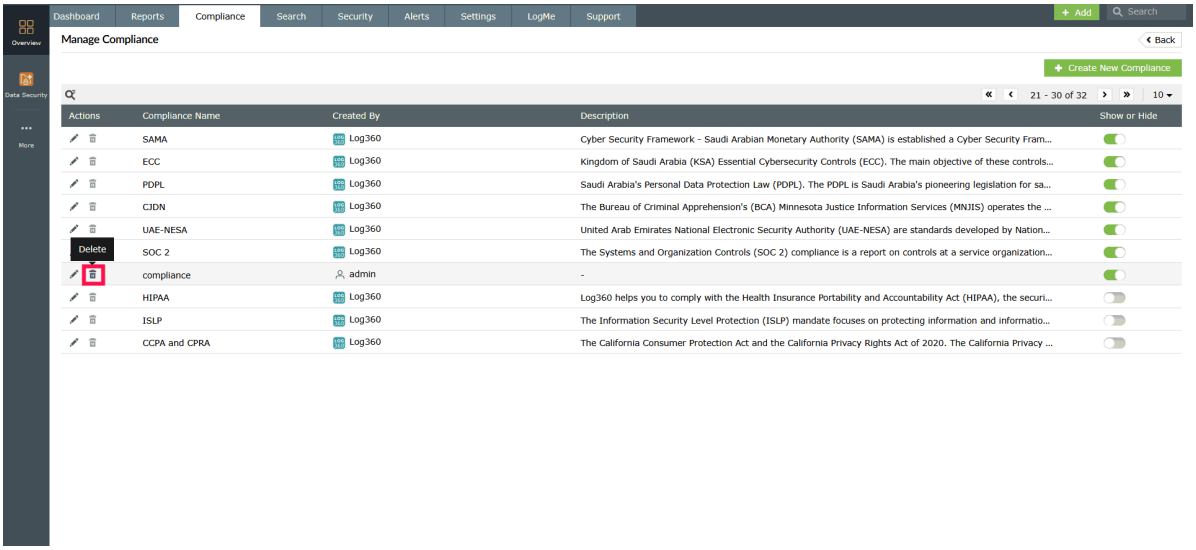


Figure 5: Deleting a compliance mandate

3. In the confirmation dialog, click Yes to proceed.

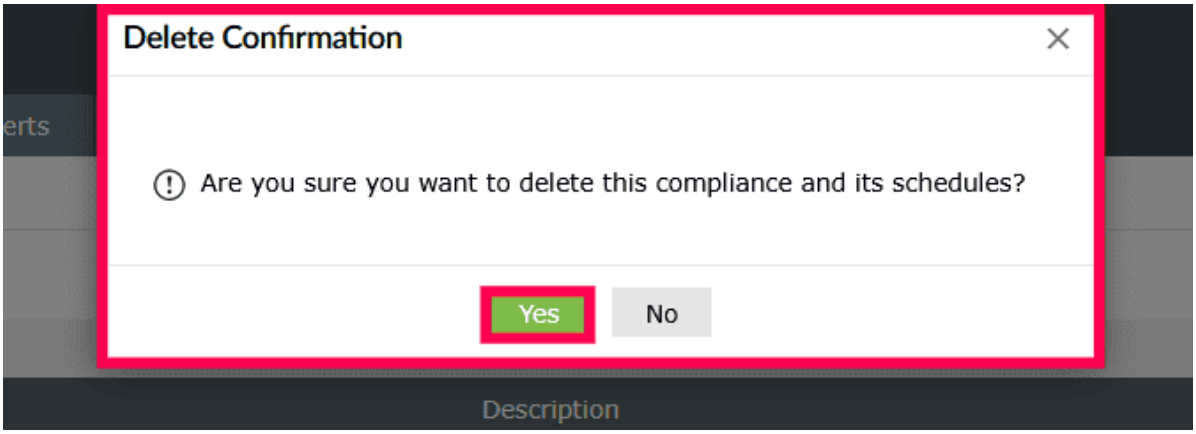


Figure 6: Deleting a compliance mandate

NOTE: Predefined compliance mandates cannot be deleted.

Enabling or disabling a compliance mandate

1. In the Manage Compliance page, use the toggle button next to each compliance mandate to enable or disable it as required.

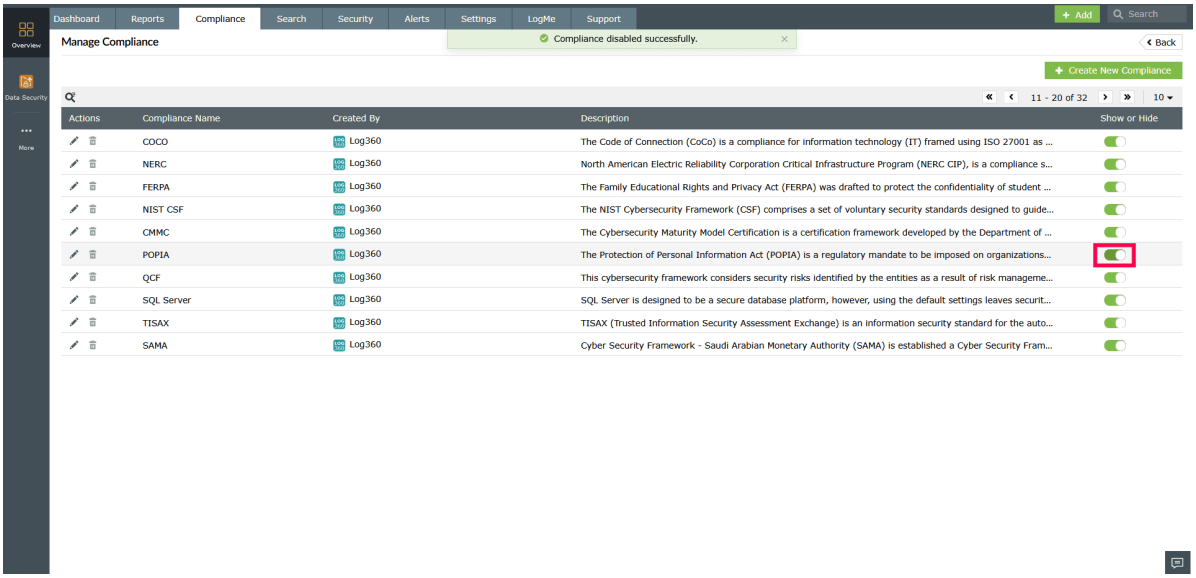


Figure 7: Disabling a compliance mandate

Read also

This page detailed how to manage compliance regulations. To learn how to schedule compliance and manage compliance schedulers, refer to the following articles:

- Scheduling compliance reports
- Managing compliance schedulers

8.4.4. Scheduling compliance reports

Last updated on: September 12, 2025

In this page

Overview

Steps to schedule compliance reports

Overview

This section details how you can create compliance report schedules to have selected reports automatically delivered to your email at specified intervals. This helps eliminate the need to log in repeatedly to access reports.

Steps to schedule compliance reports

> **NOTE**
>
> A schedule cannot be created if sources are not configured. Ensure that the required sources are configured before proceeding.

1. In the product console, navigate to the Compliance tab.
2. Select Schedule Compliance in the top-right corner.

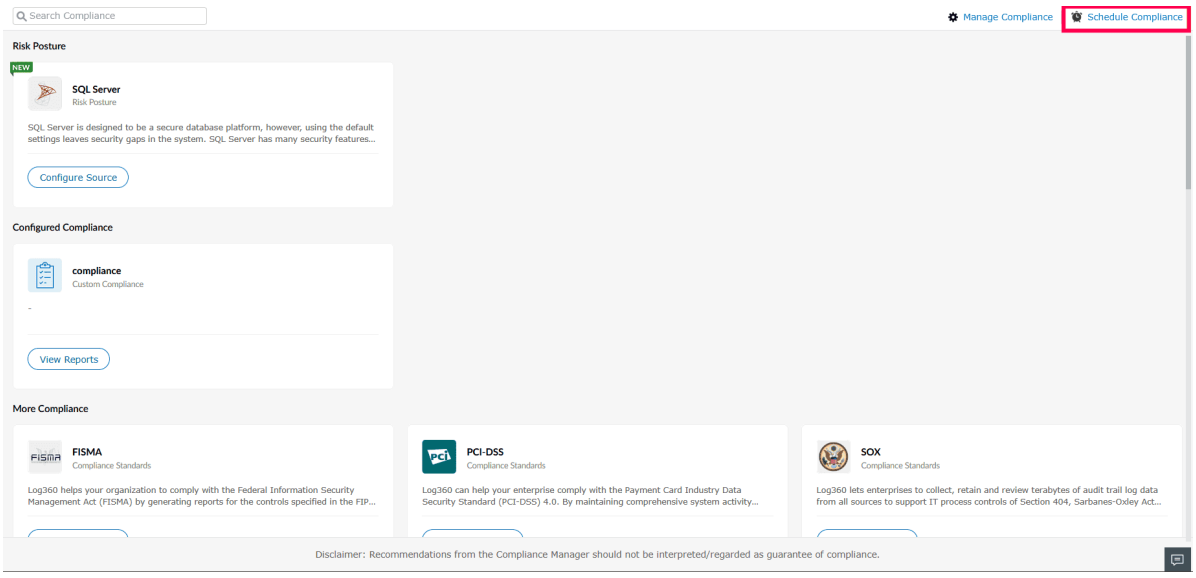


Figure 1: Scheduling compliance reports

3. In the Schedule Compliance page, click Create New Scheduler.

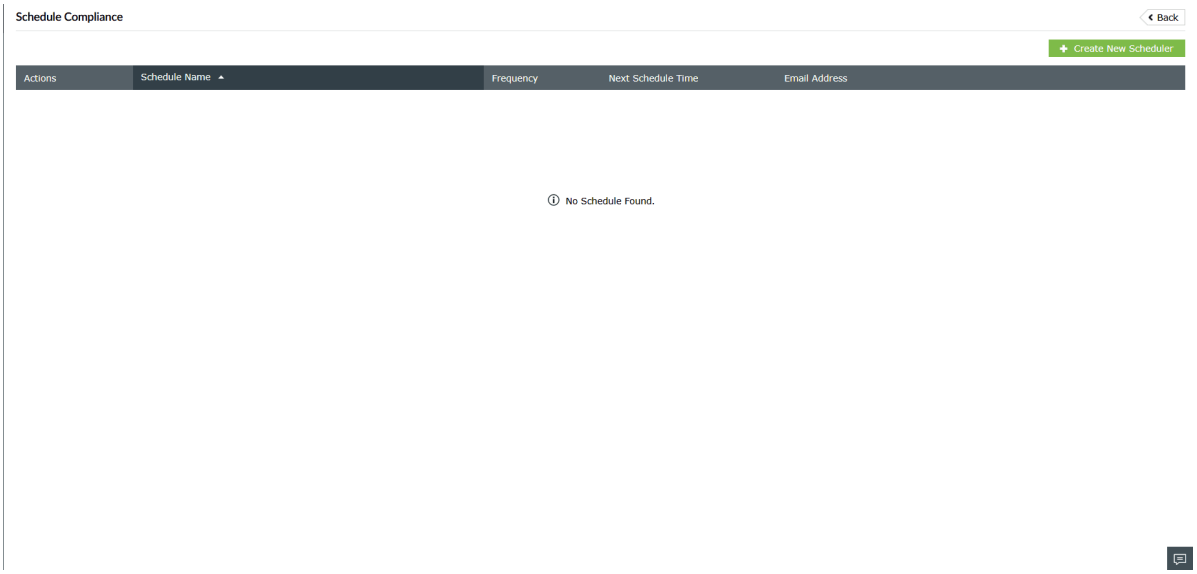


Figure 2: Scheduling compliance reports

4. In the Add Compliance Schedule window, fill in the required details:

- Enter a name in the Scheduler Name field

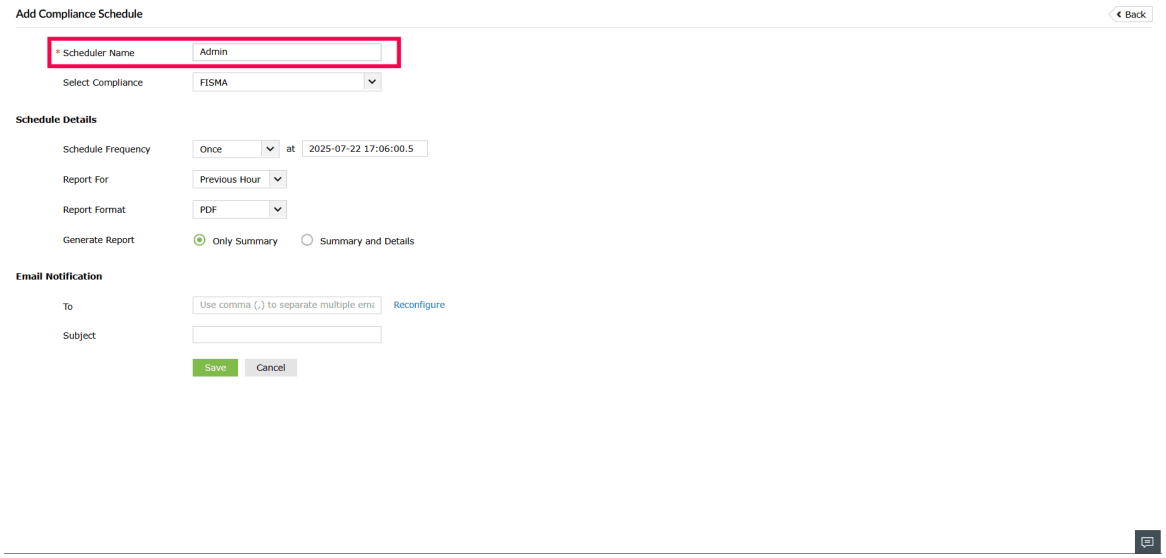
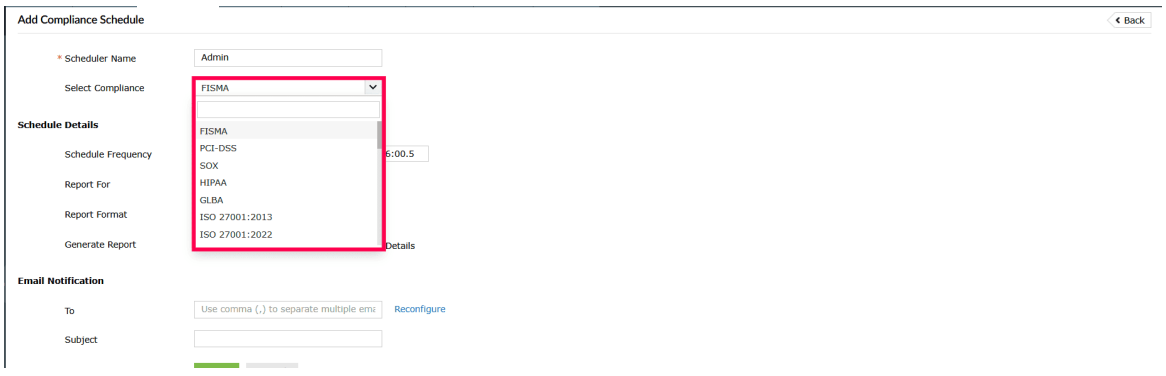


Figure 3: Setting up a compliance report schedule

- Select or search for the relevant compliance mandate from the Select Compliance drop-down.



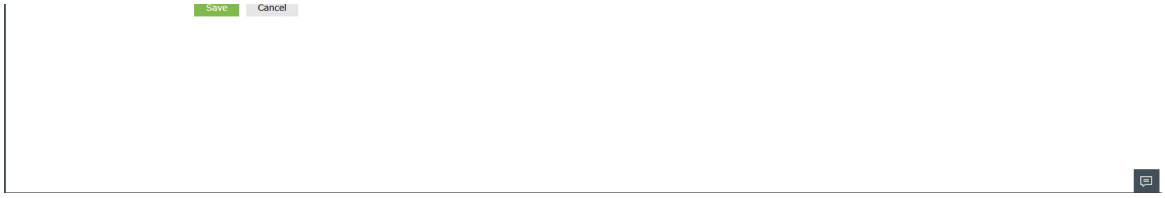


Figure 4: Setting up a compliance report schedule

- Set the Schedule Frequency to Once, Hourly, Daily, Weekly, or Monthly

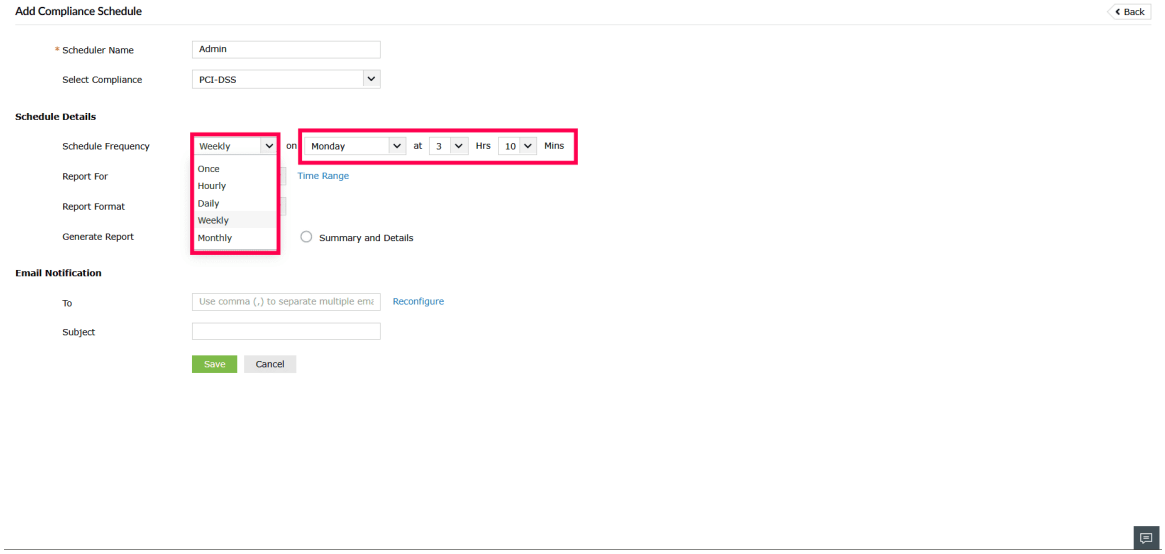


Figure 5: Configuring Schedule Frequency

- Choose the Report For duration from the drop-down

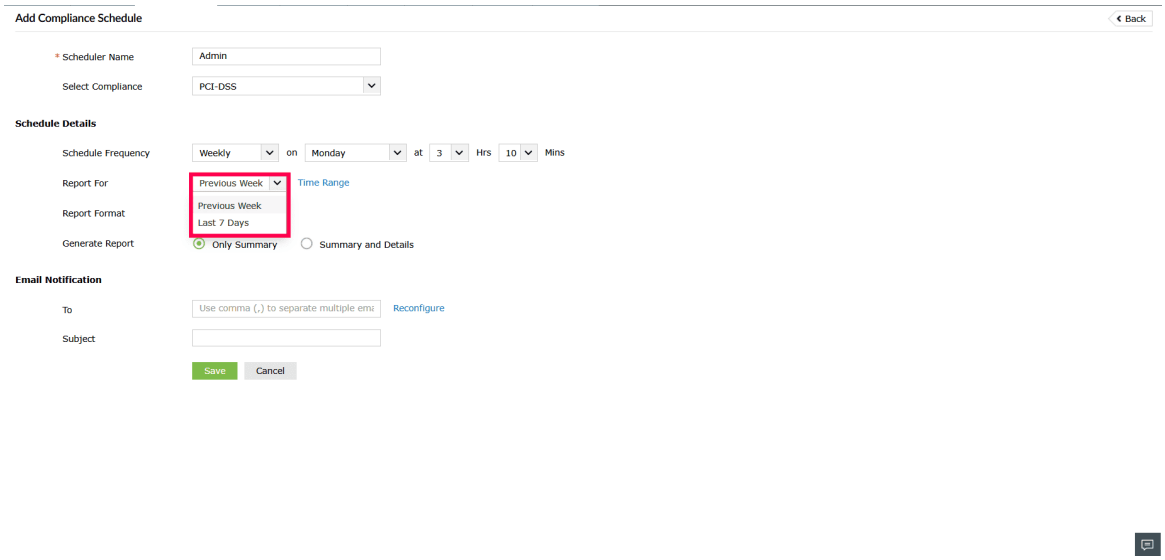
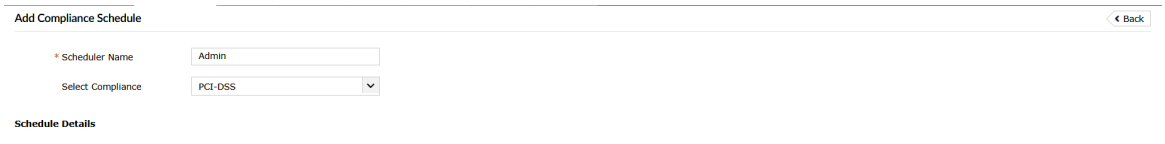


Figure 6: Configuring Schedule Details

- If you choose Daily, Weekly, or Monthly, a Time Range option is available.



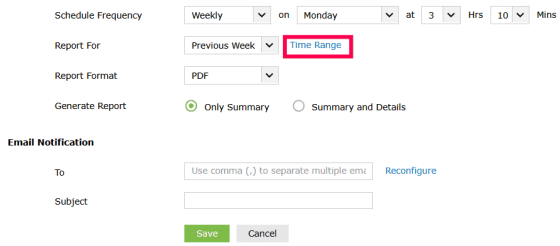


Figure 7: Configuring Schedule Details

- Use the Day Filter to specify the exact day(s) on which the report should be generated as part of the schedule.

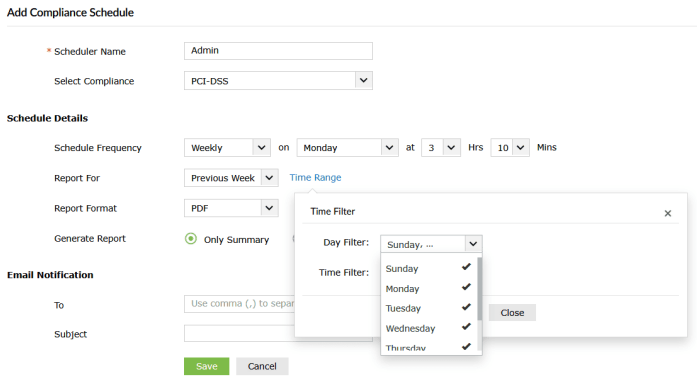


Figure 8: Configuring Time Filter

- Use the Time Filter to select when the report should be generated:
  - All Hours
  - Working Hours
  - Non-working Hours
  - Custom - If selected, specify the desired time range.

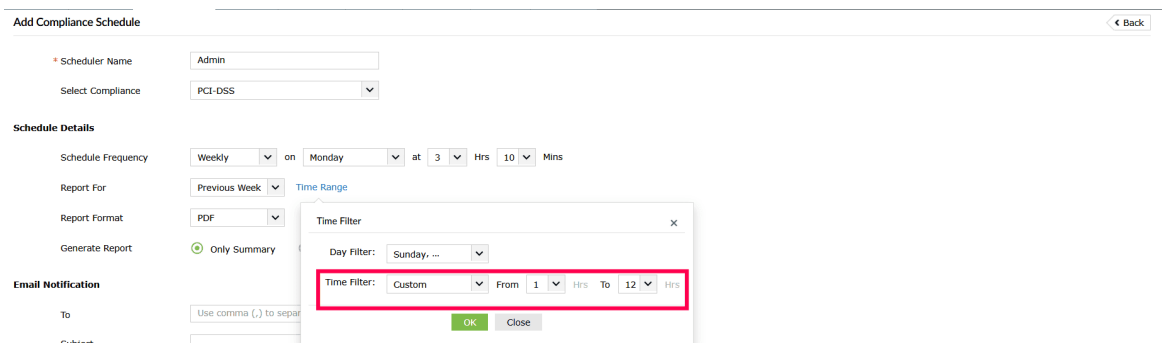




Figure 9: Configuring Time Filter

- Select the Report Format, either PDF or CSV.

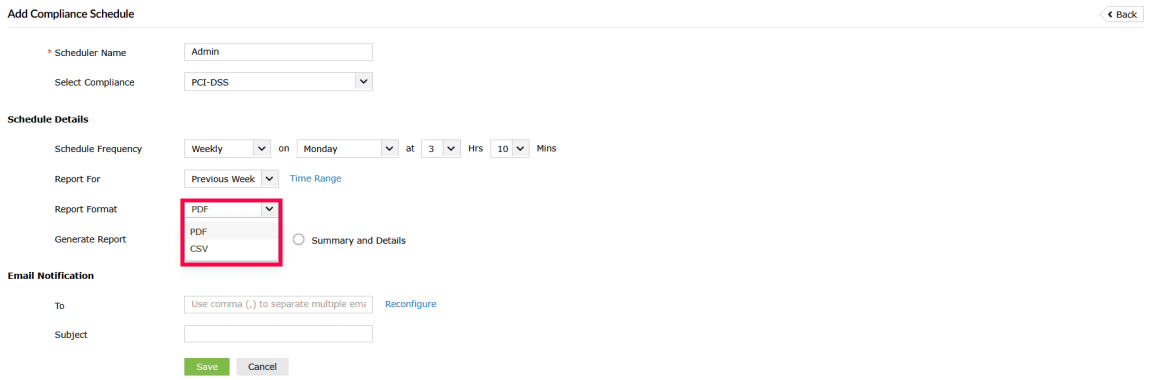


Figure 10: Configuring Schedule Details

- Choose whether to generate Only Summary or Summary and Details.

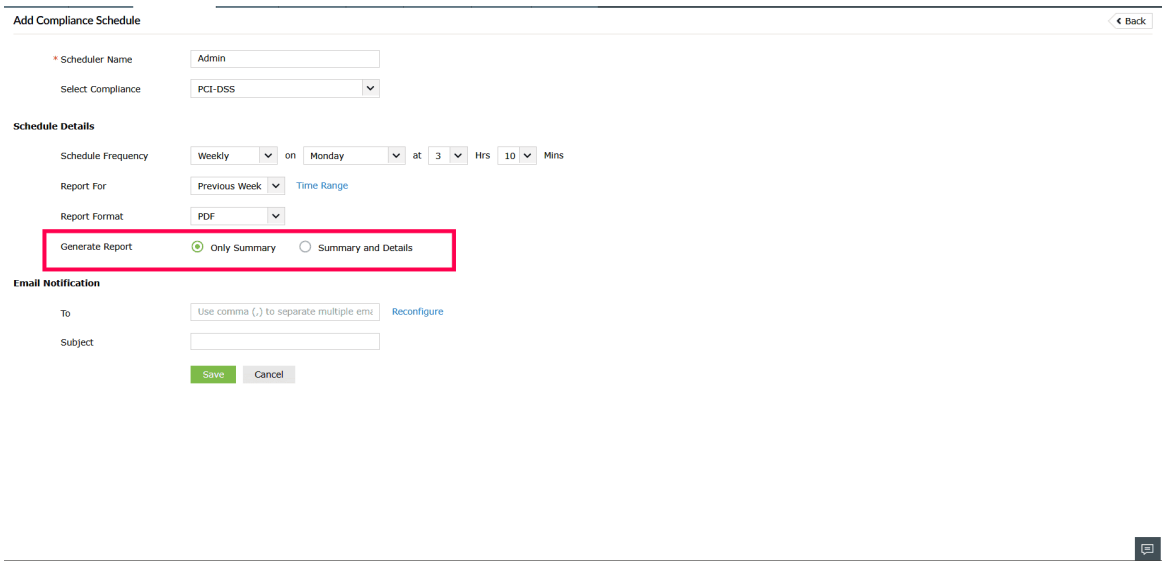


Figure 11: Configuring Schedule Details

  - In the Email Notification section, enter recipient email addresses in the To field (use commas to separate multiple addresses), and add a suitable Subject.
  - (Optional) Click Reconfigure to modify the email server settings if needed.

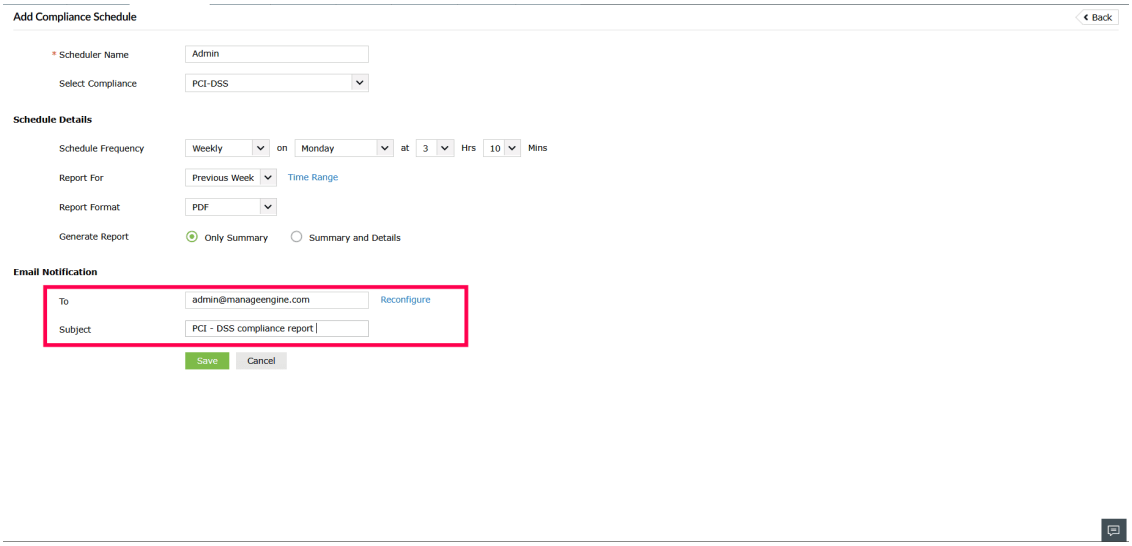


Figure 12: Configuring Email Notification

5. Click Save to confirm and activate the schedule.

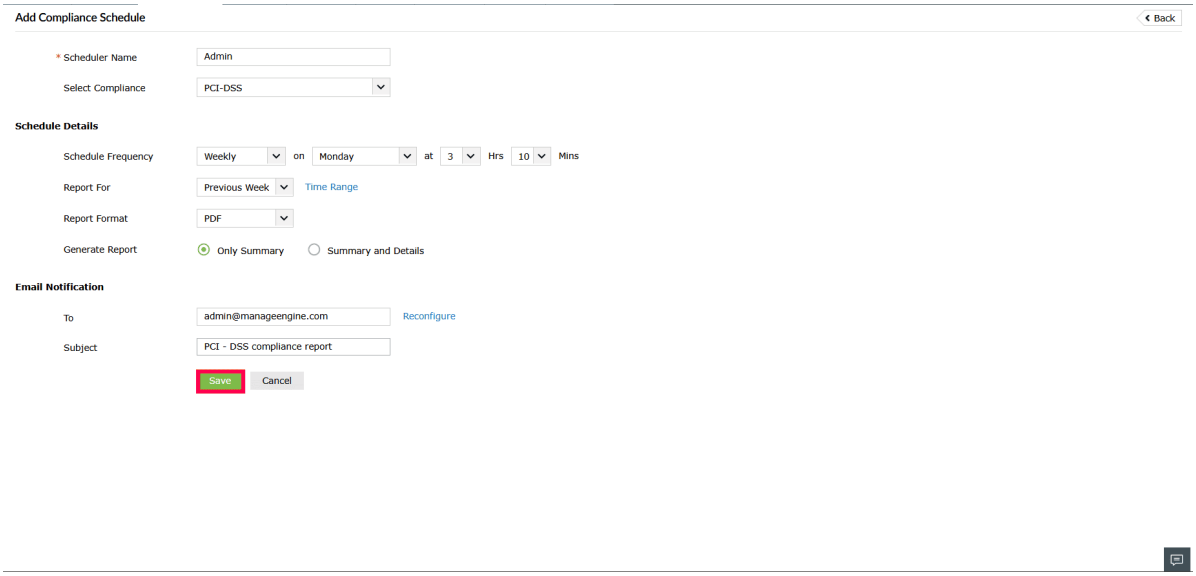


Figure 13: Scheduling compliance reports

Read also

This page explained about scheduling compliance reports. To learn how to manage and customize compliance reporting further, refer to the following documents:

- Managing compliance schedulers
- Viewing and managing compliance reports

8.4.5. Managing compliance schedulers

Last updated on: September 12, 2025

In this page

Overview

Searching compliance schedulers

Editing compliance schedulers

Enabling or disabling compliance schedulers

Deleting compliance schedulers

Overview

This page describes how to manage existing compliance report schedules in the product console. You can search for specific schedules, update their configurations, enable or disable them, or delete schedules as needed. These actions ensure that your compliance reporting workflows remain accurate and relevant to your operational needs.

Searching compliance schedulers

1. In the Schedule Compliance page, click the icon in the top-left corner to find a schedule by its name.

Editing compliance schedulers

1. Click the icon next to the schedule you want to update.

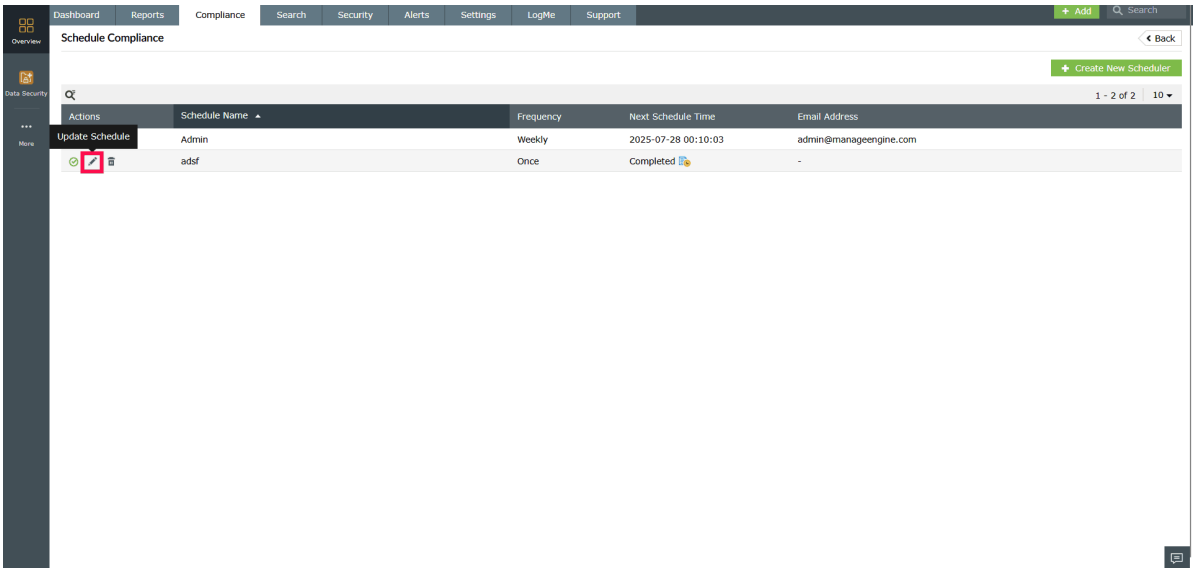


Figure 1: Editing a compliance scheduler

2. In the Edit Compliance Schedule window, make the required changes to the scheduler's configuration.

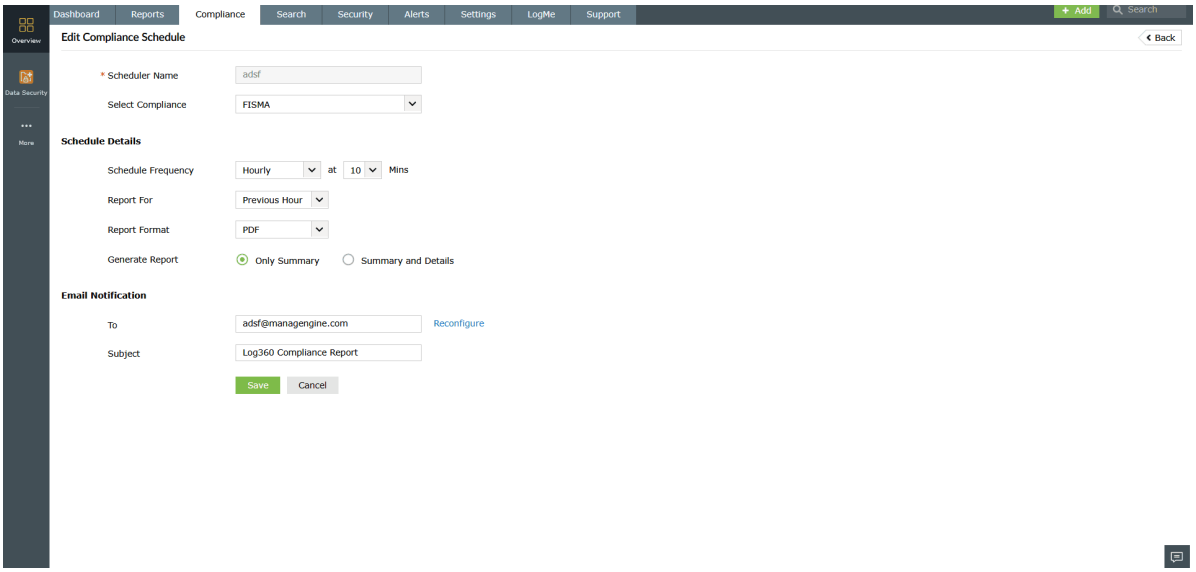


Figure 2: Editing a compliance scheduler

3. Click Save to apply the updates.

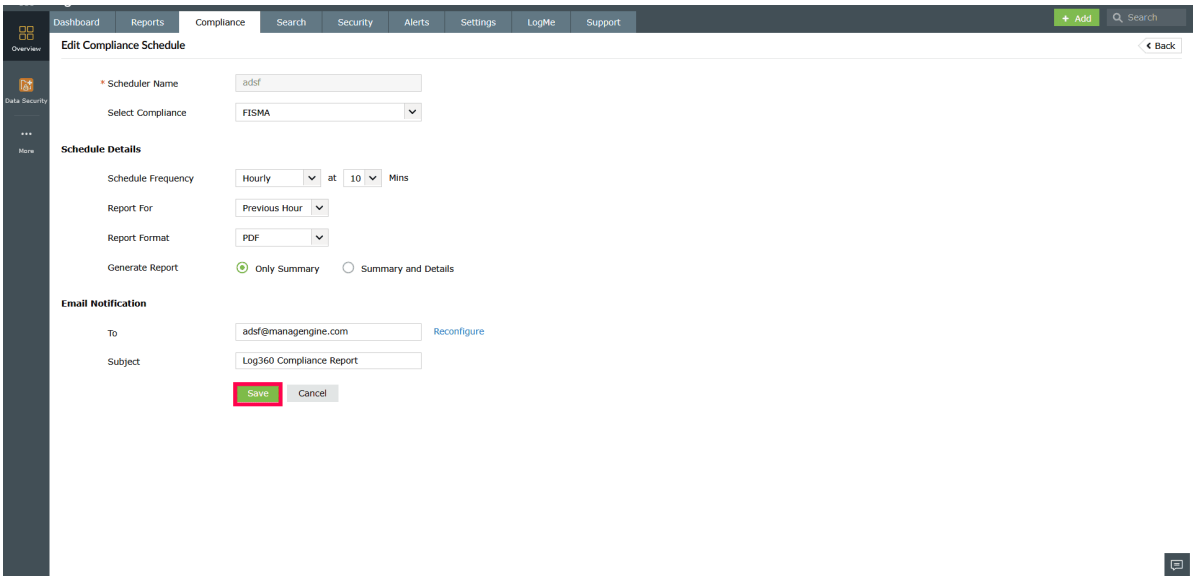


Figure 3: Editing a compliance scheduler

4. Hover over the Next Schedule Time timestamp to view the icon.

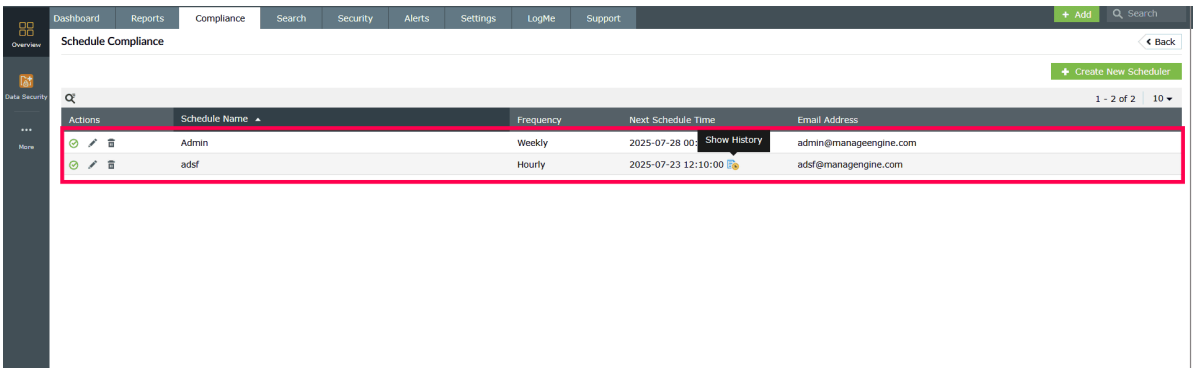


Figure 4: Accessing Show History

5. Clicking this icon displays a list of previously generated compliance reports along with their download links.

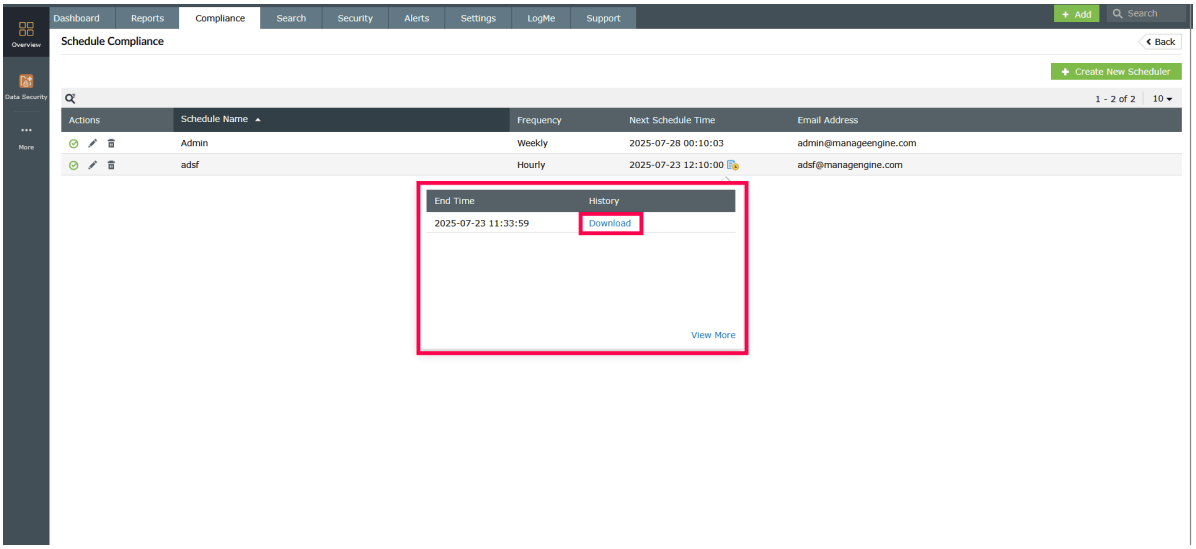


Figure 5: Downloading compliance reports

6. You can also click View More to see the complete history.

Enabling or disabling compliance schedulers

1. In the Schedule Compliance page, locate the relevant scheduler.
2. Click the icon to disable the schedule.

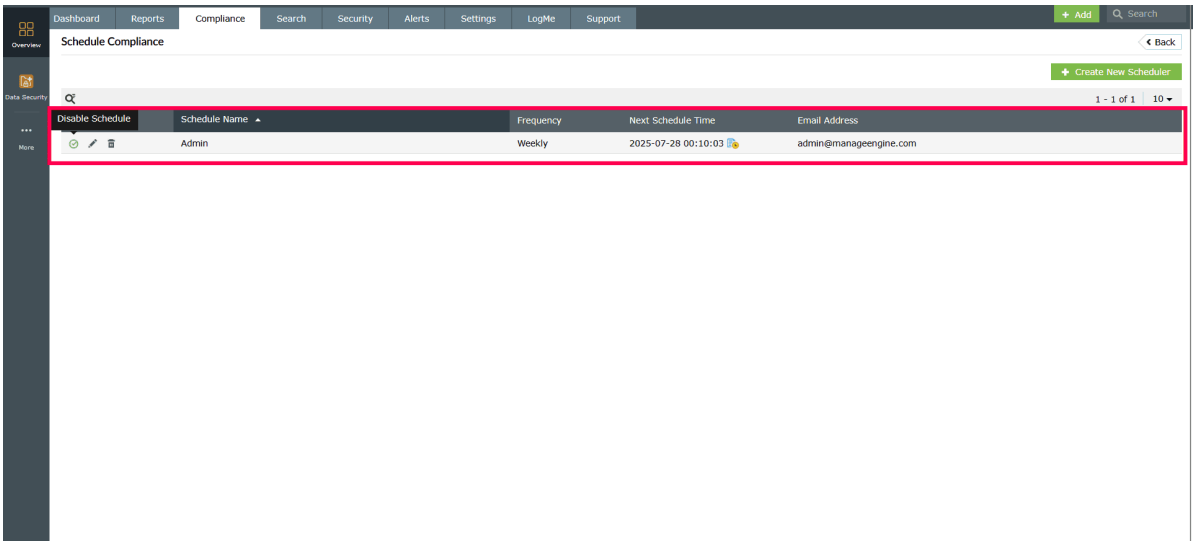


Figure 6: Disabling a compliance scheduler

Figure 6: Disabling a compliance scheduler

3. Click the ⊘ icon to re-enable the scheduler.

Deleting compliance schedulers

1. Click the 🗑 icon next to the schedule you want to remove.
2. In the confirmation dialog, click Yes to confirm and permanently delete the schedule.

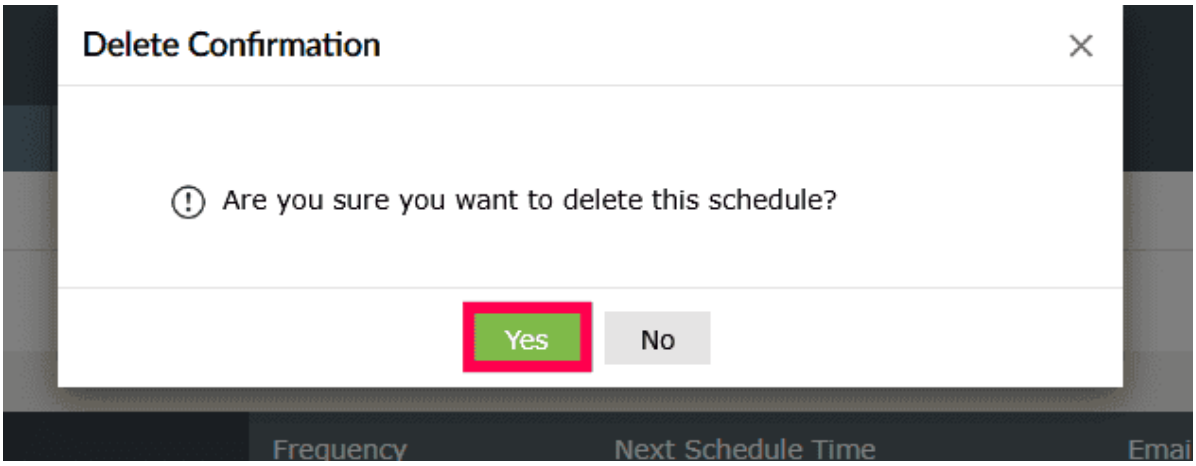


Figure 5: Deleting a compliance scheduler

Read also

This page detailed how to manage compliance schedulers, including searching, editing, enabling/disabling, and deleting schedules. To learn how to configure and schedule compliance reports, refer to the following articles:

- Configuring custom compliance reports
- Scheduling compliance reports

8.4.6. Viewing and managing compliance reports

Last updated on: September 12, 2025

In this page

Overview

Steps to view and manage compliance reports

Overview

This page explains how to view and manage compliance reports. You can view comprehensive audit data, export reports, and analyze device and user activity for detailed compliance insights.

Steps to view and manage compliance reports

1. Log in to your Log360 account.
2. Navigate to the Compliance tab.
3. Under the configured compliance mandates, click View Reports for the compliance standard you want to review.

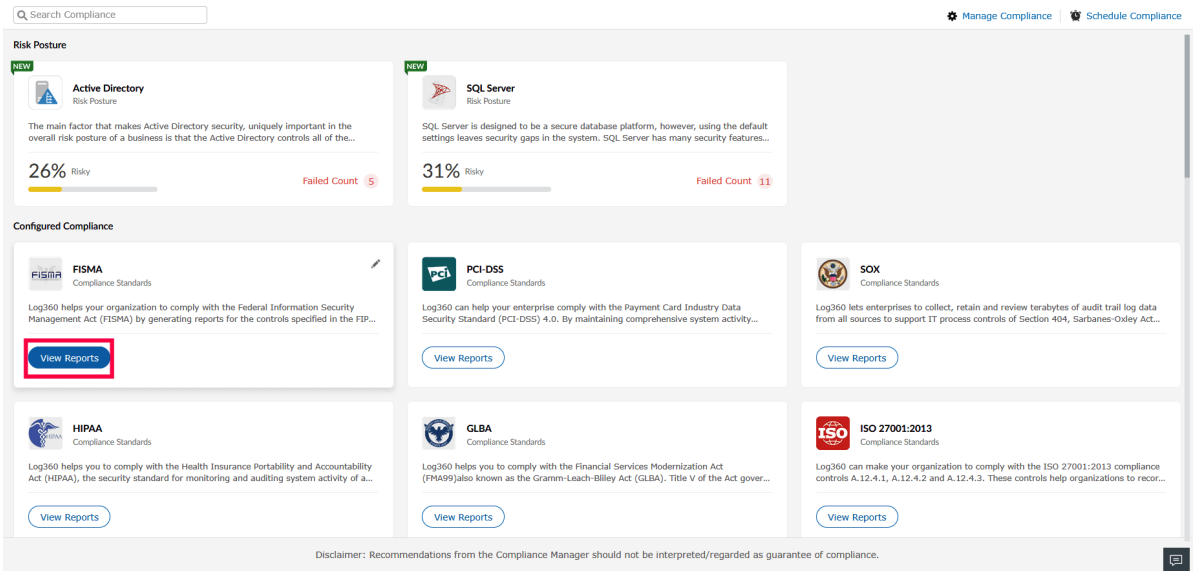
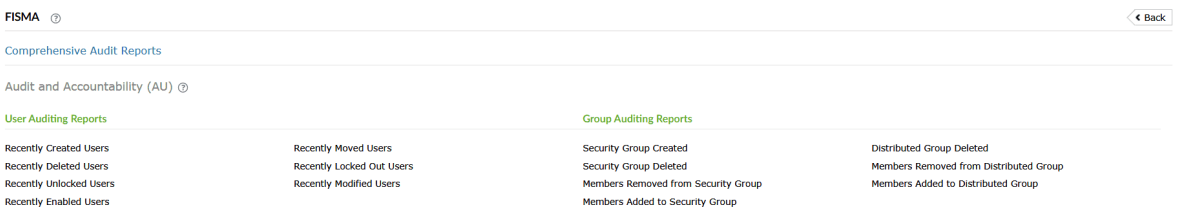


Figure 1: Viewing reports

4. The reports page displays a list of categories with detailed audit reports.



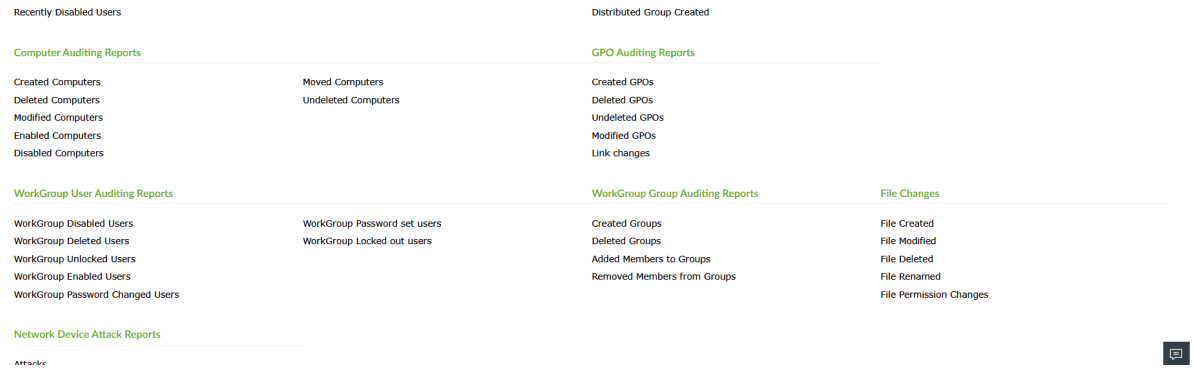


Figure 2: Viewing reports

5. To view detailed audit reports, click Comprehensive Audit Reports at the top of the page.

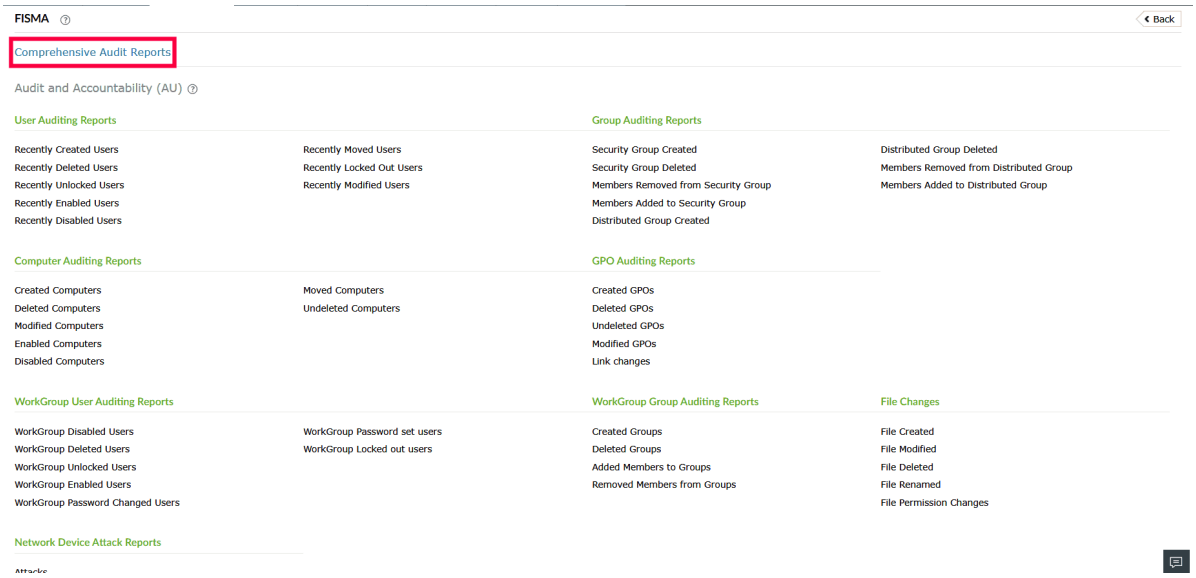


Figure 3: Viewing Comprehensive Audit Reports

6. To export reports for the selected compliance mandate, click Export As in the top-right corner.

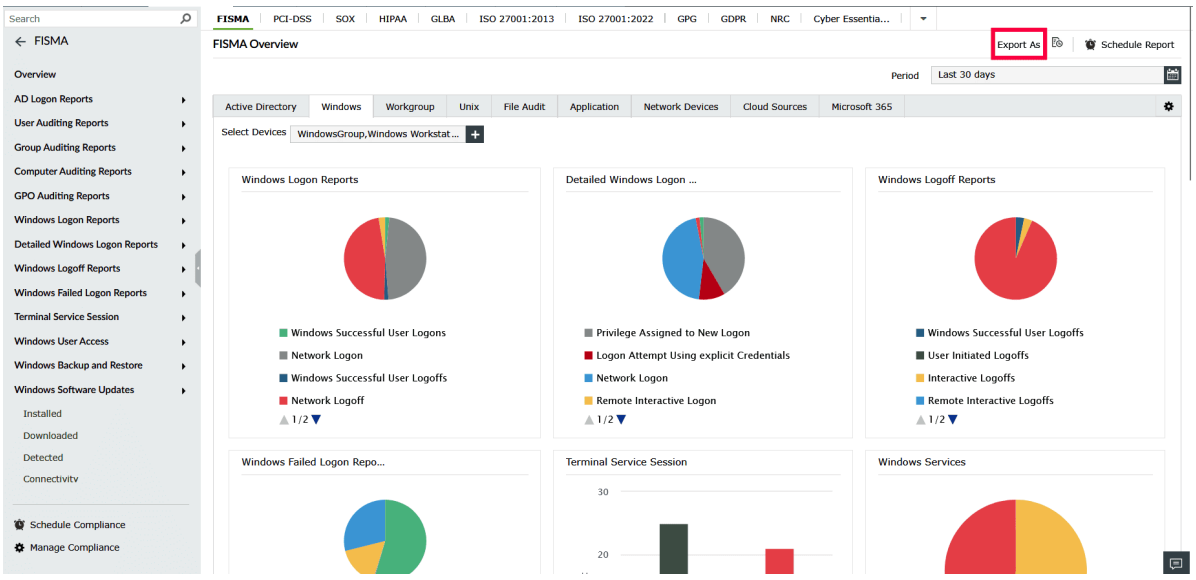


Figure 4: Exporting reports

7. In the export window, use the Export drop-down to choose the reports you want to export:
   - All Reports
   - All Overview Reports
   - Currently Viewed Reports
   - Select Reports

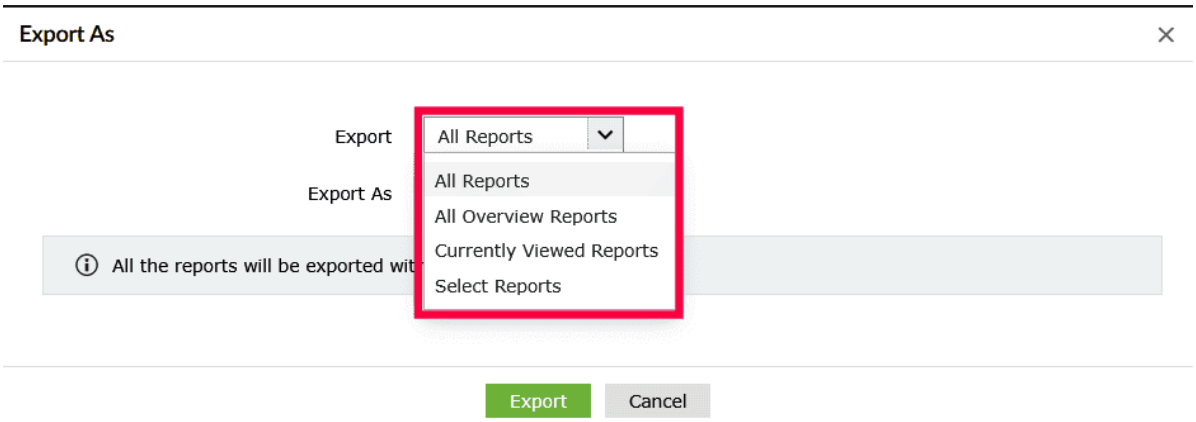


Figure 5: Exporting reports

8. From the Export As drop-down, choose the file format (PDF or CSV) and then click Export to download the reports.

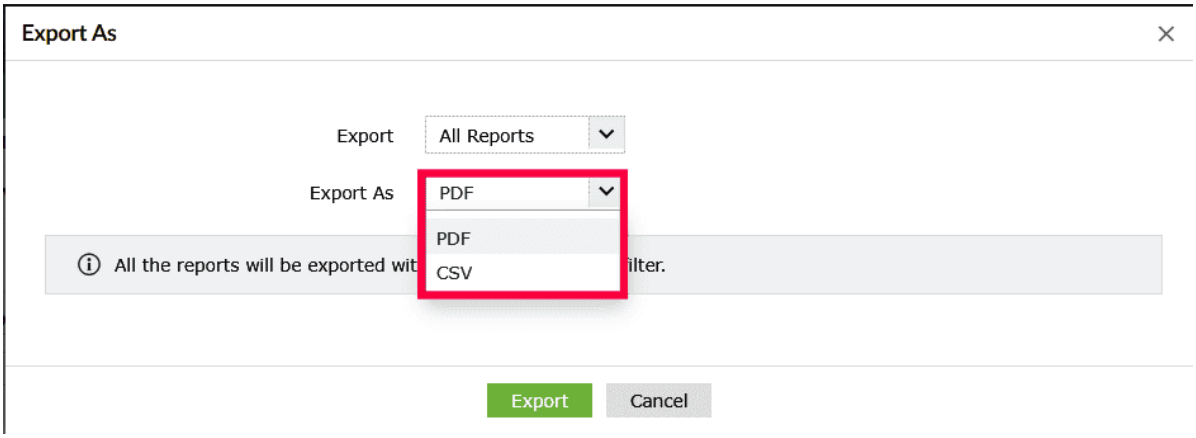
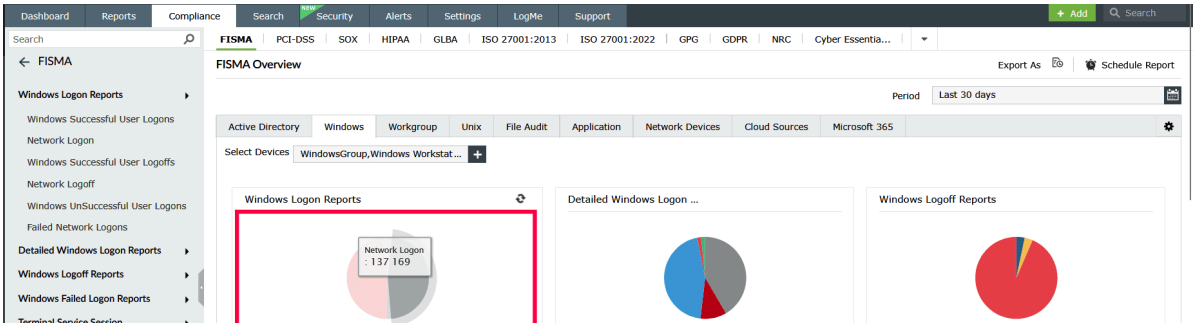


Figure 6: Exporting reports

9. To check past export history, click the icon.
10. Select a report from the list to view its details.



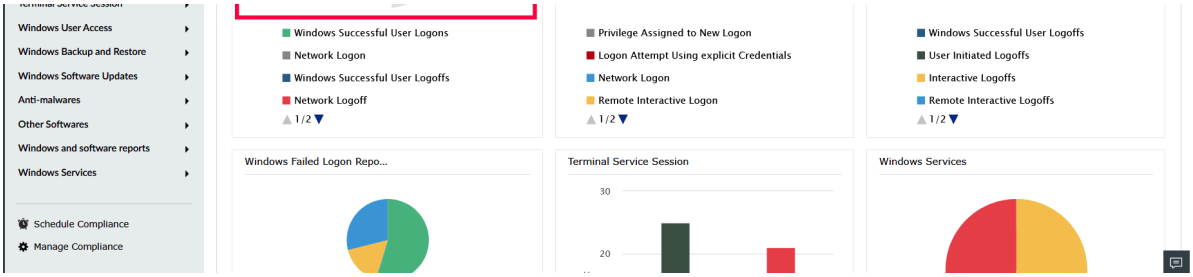


Figure 7: Selecting a report

11. To download the selected report, click Export As, choose the format (PDF or CSV).

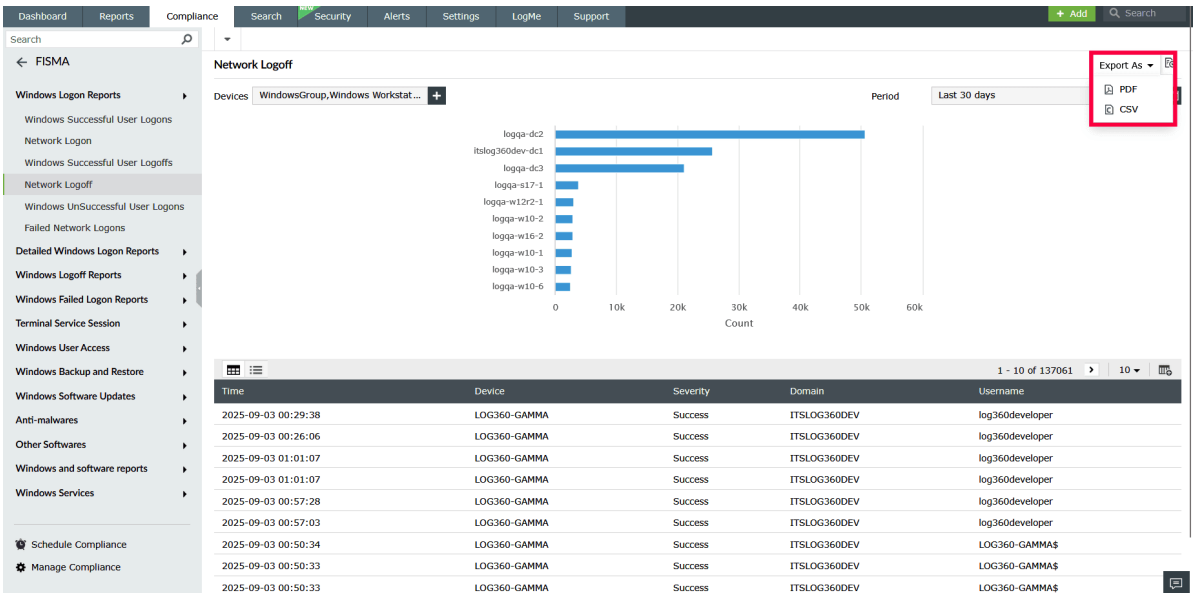


Figure 8: Exporting a report

12. Use the icon to locate a specific report.

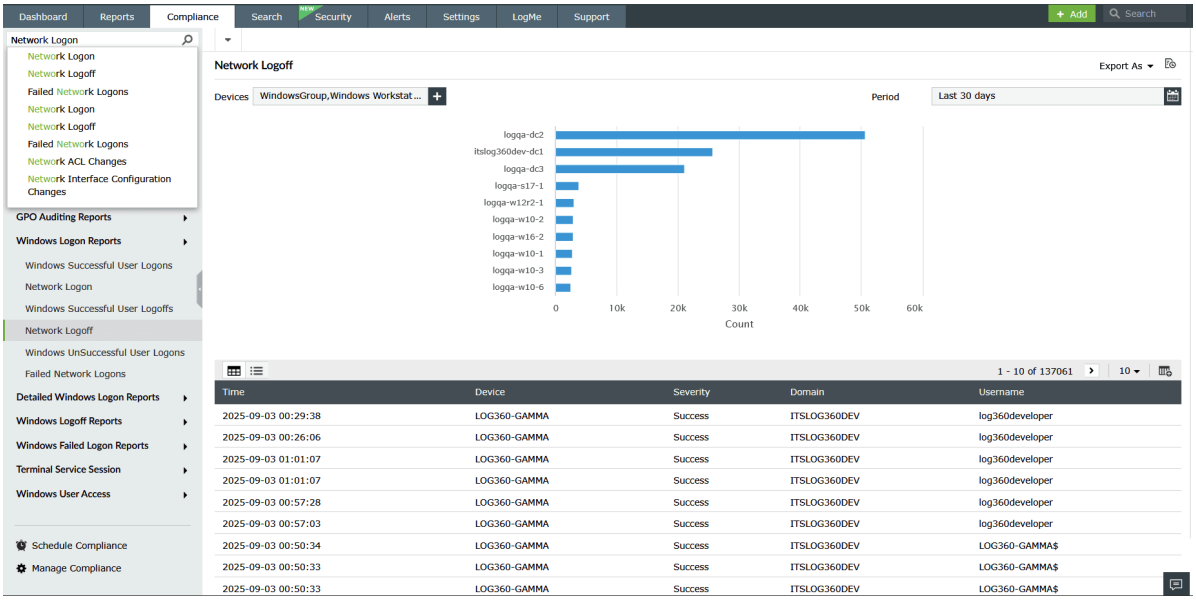


Figure 9: Searching for a report

13. In the report window:

- Click the icon to add or remove columns in the report view. From the list, select the required checkboxes and click Apply to add or remove columns.

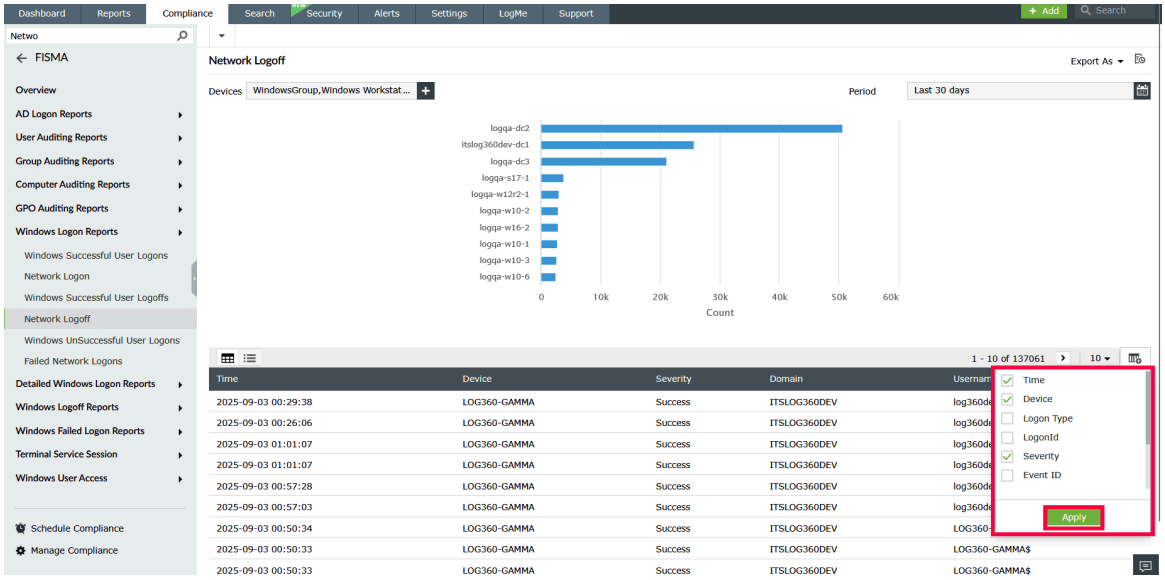


Figure 10: Adding/ removing columns

- Hover over the Device column and select a device.

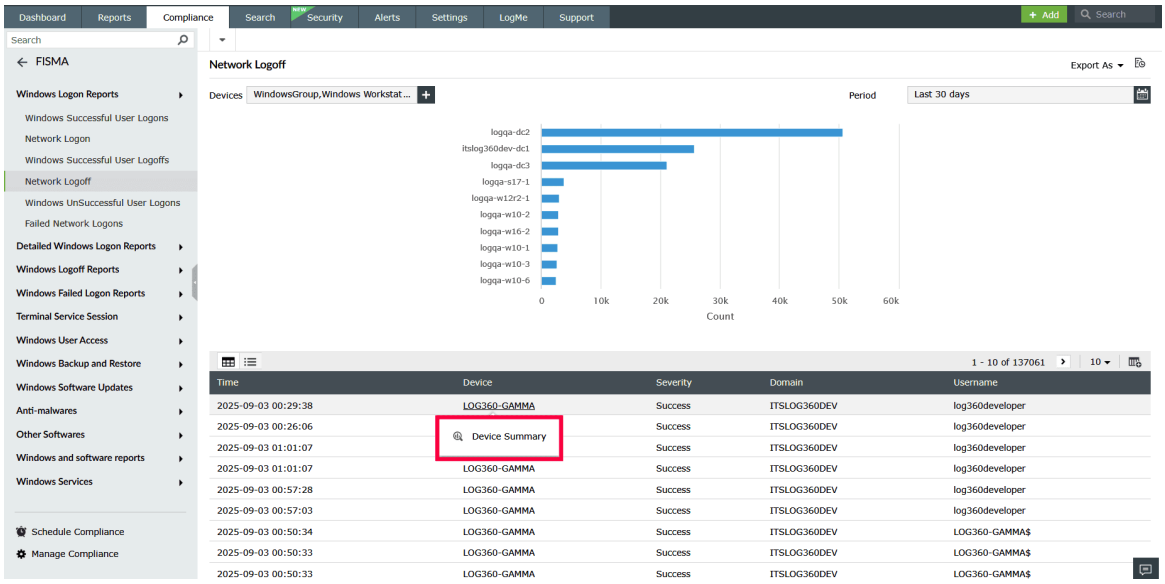
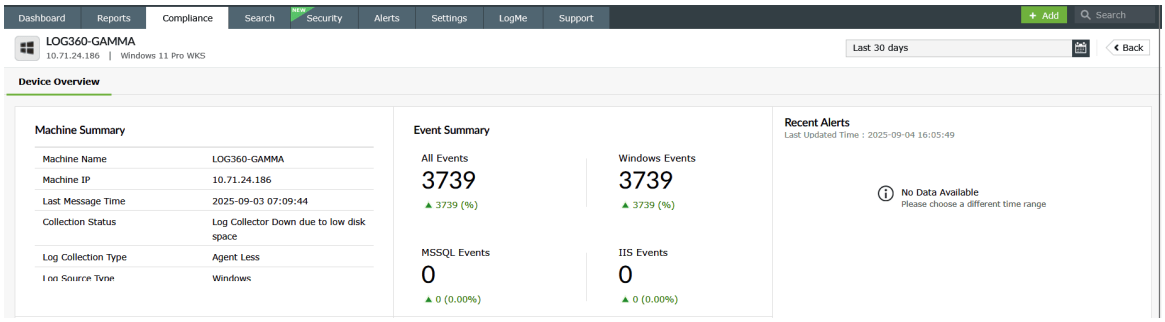


Figure 11: Viewing device summary

- Click Device Summary to view the device overview.



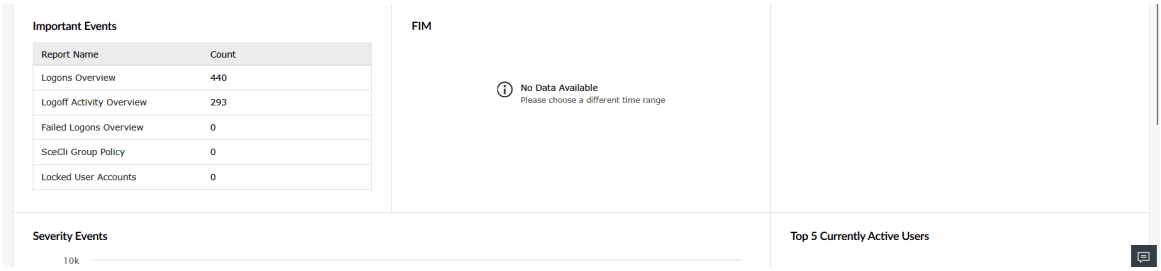


Figure 12: Viewing device overview

- Hover over the User Name column and select a user.

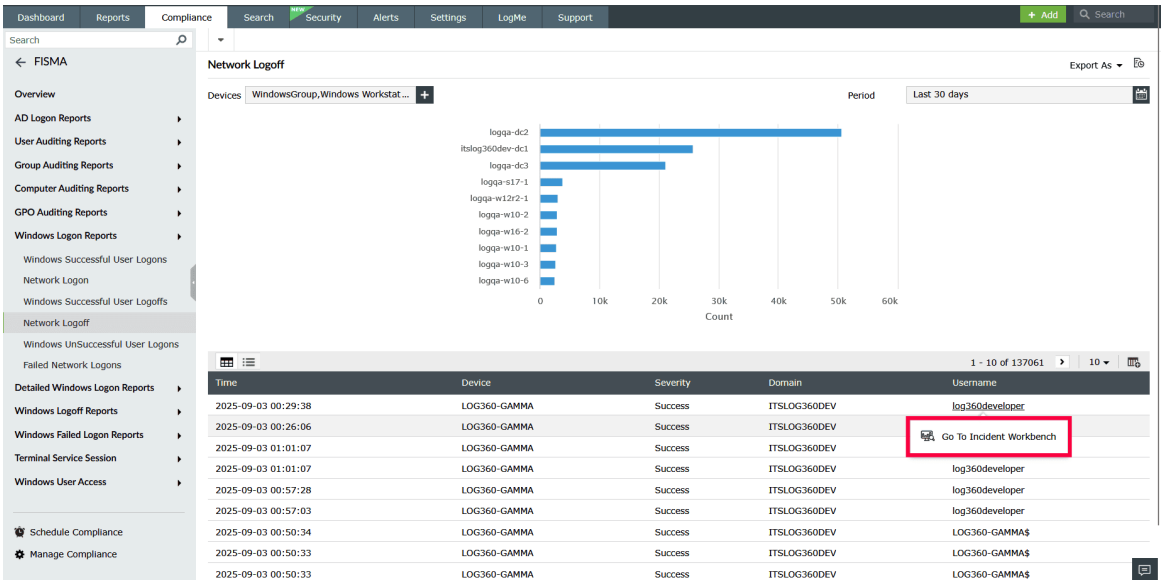


Figure 13: Viewing user activity

- Click Go to Incident Workbench to analyze user activity in detail.

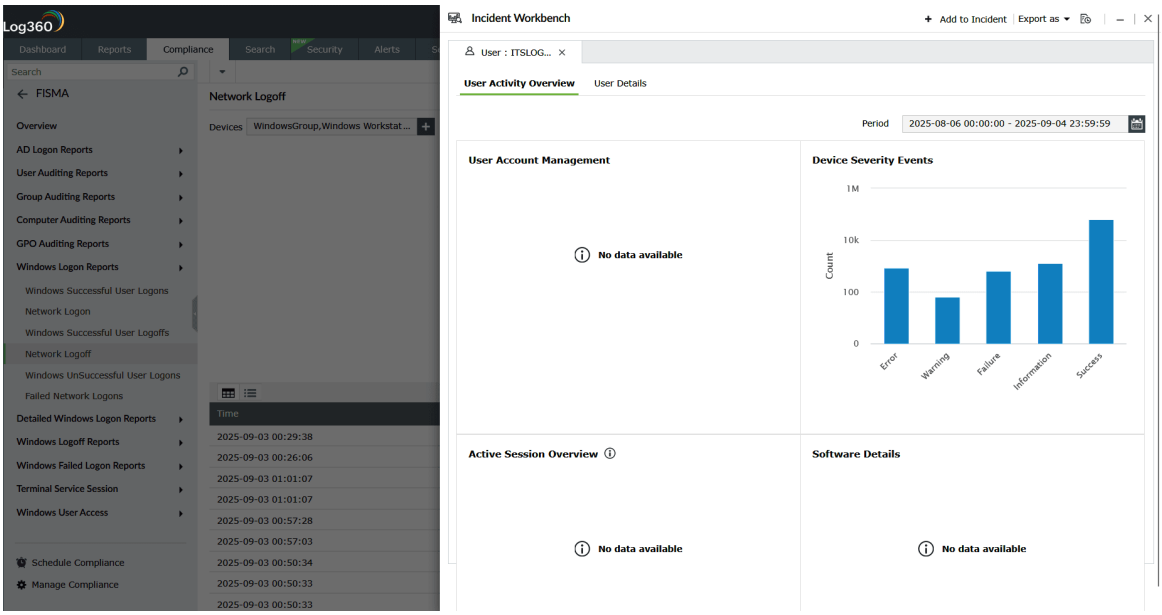


Figure 14: Viewing user activity and details

Read also

Read also

This document explained how to view and manage compliance reports, access comprehensive audit data, export reports, and analyze device and user activity. To learn how to schedule compliance and manage compliance schedulers, refer to the following articles:

- Scheduling compliance reports
- Managing compliance schedulers

8.4.6.1.1. Overview

Last updated on: September 12, 2025

In this page

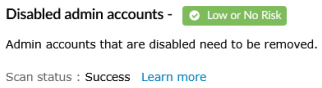
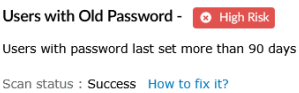
Understanding the working of risk posture

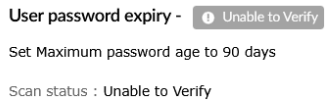
Risk posture describes an organization's overall ability to identify, assess, and respond to security risks. It requires a comprehensive review of the environment, including users, devices, network elements, configurations, and any stored information that could be exposed, along with an assessment of current security practices and software against known attack techniques.
Log360 currently supports risk posture assessments for the following sources:

- Active Directory
- SQL Server

Understanding the working of risk posture

Risk posture in Log360 is evaluated using pre-defined risk rules. These rules are derived from the CIS Benchmarks, which outline industry-accepted best practices for securing systems and applications. Each rule acts as a compliance criterion against which configurations of supported sources, such as Active Directory and SQL Server, are validated.
Each rule in risk posture is assigned a status that reflects whether the configuration complies with the defined baseline:

Status	Description	Example
Low/No Risk	This status informs that the selected source's configurations have met the recommended/user set compliance value as per their norms.	 Click Learn More to view associated vulnerability details, best practices, and recommendations.
High Risk	This status informs that the selected source's configurations have not met the recommended/pre-defined compliance standards set by the user or organization.	 Click How to fix it to see the identified vulnerability, review CIS best practices, and implement the suggested fix.
	This status informs that the Log360 server	

Status	Description	Example
Unable to Verify	was unable to fetch the required data needed for analyzing the specific rule. It can be due to the following reasons. • Insufficient domain details • Access denied for SYSVOL folder. • SQL Server down • Insufficient server details/user credentials	

Read also

This section explained how risk posture helps assess and monitor your organization's security configurations. To learn more about related capabilities, refer to the following articles:

- Risk analysis

8.4.6.1.2. Risk analysis

Last updated on: September 12, 2025

In this page

Overview

Steps to run a risk analysis

Scheduling risk analysis

Exporting analysis results

Overview

Running, scheduling, and exporting analysis evaluates your configured sources against defined risk posture rules to update their statuses (Low/No Risk, High Risk, Unable to Verify). This keeps the posture up to date, highlights misconfigurations that need attention, and provides time-stamped evidence for reporting and audits without requiring manual verification.
This page details how you can run and schedule analysis.

Steps to run a risk analysis

You can manually run an analysis at any time to view the updated risk posture results.

1. In your account, go to the Dashboard tab and click Risk Posture in the top-right corner.

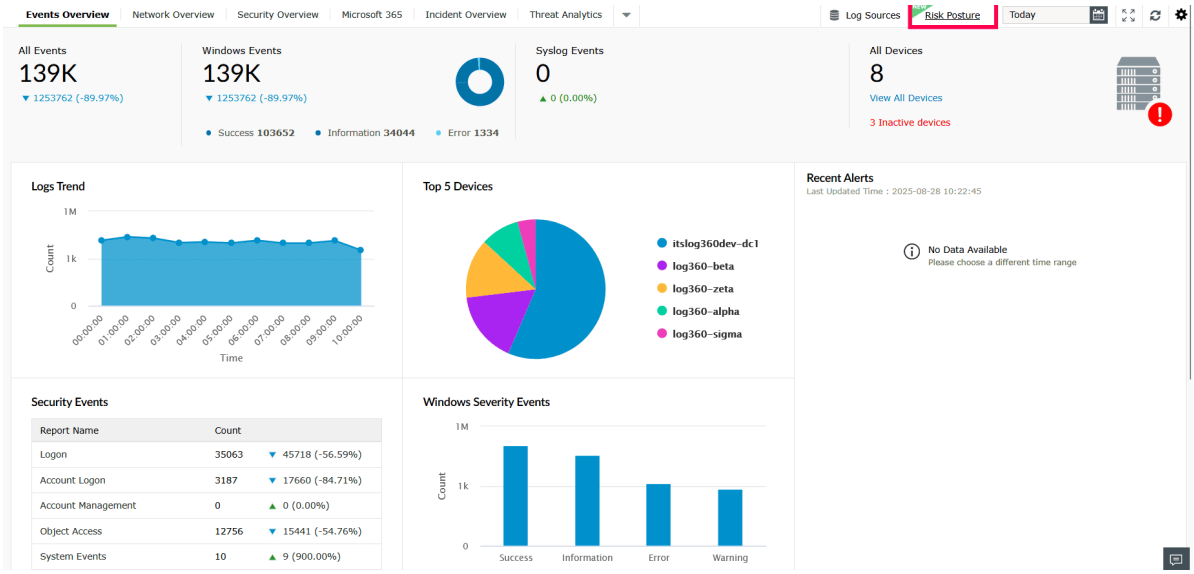


Figure 1: Navigating to Risk Posture

2. In the Risk Posture page, locate the source you want to analyze, and click Run Analysis at the top-right corner.

NOTE

You can access the same page by navigating to the Compliance tab.

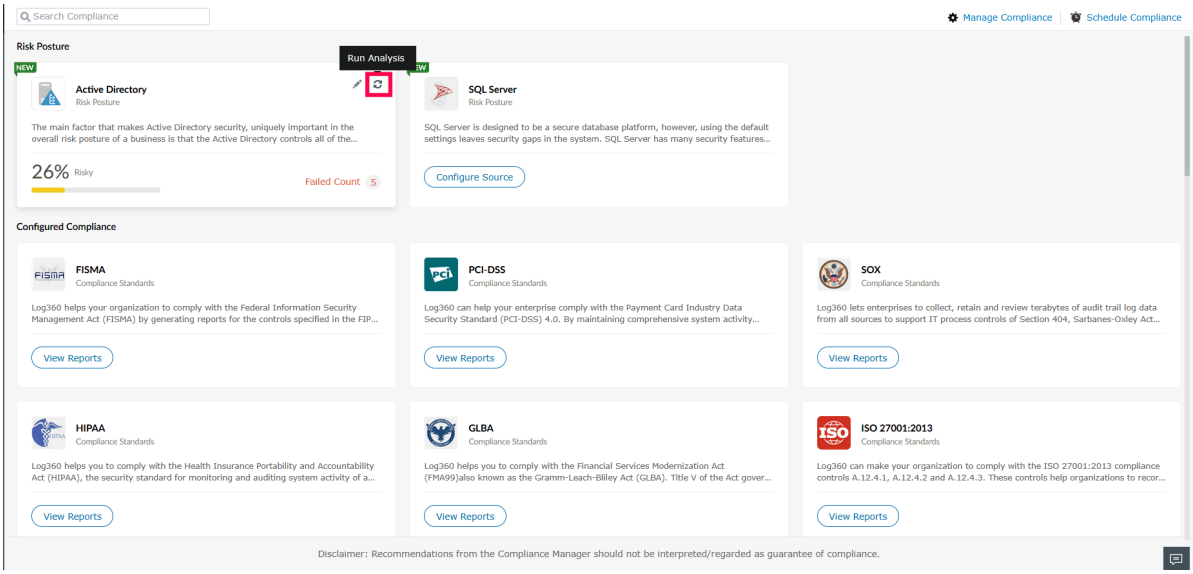


Figure 2: Running Analysis

3. You can also run an analysis by selecting a source and clicking Run Now.

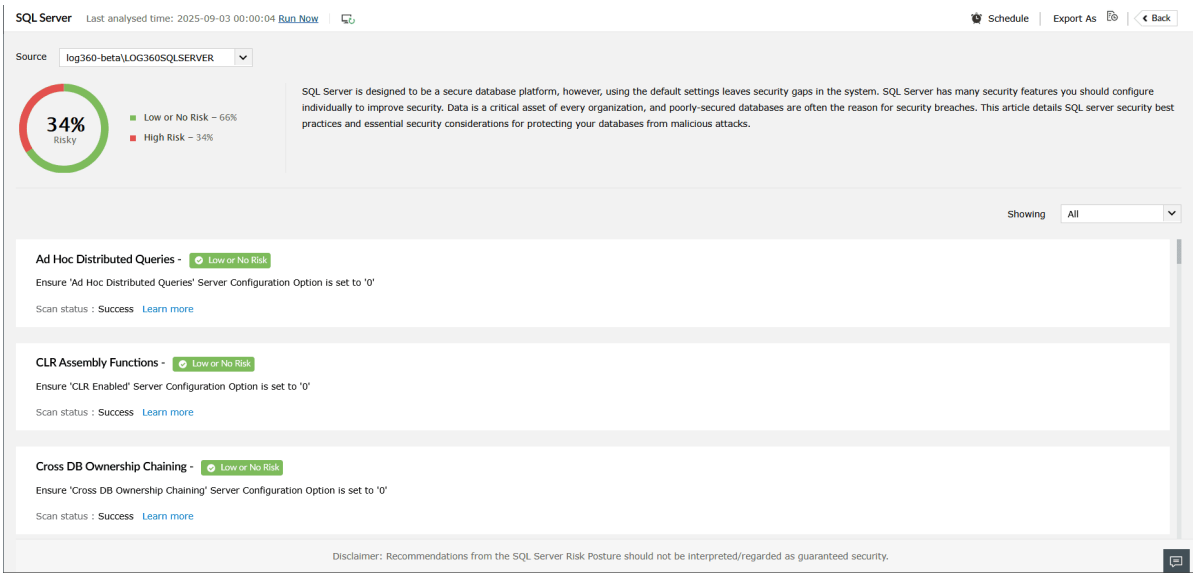


Figure 3: Running Analysis

Scheduling risk analysis

1. In your account, go to the Dashboard tab and click Risk Posture in the top-right corner.

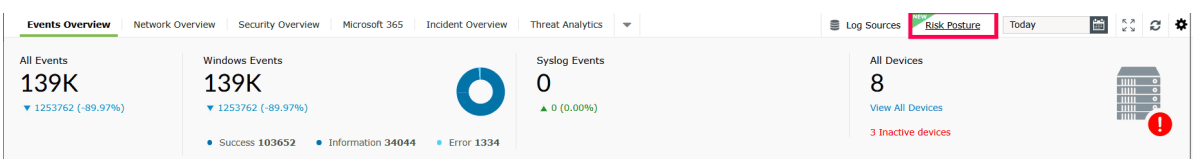




Figure 4: Running Analysis

2. On the Risk Posture page, locate and select the source you want to schedule the analysis for.

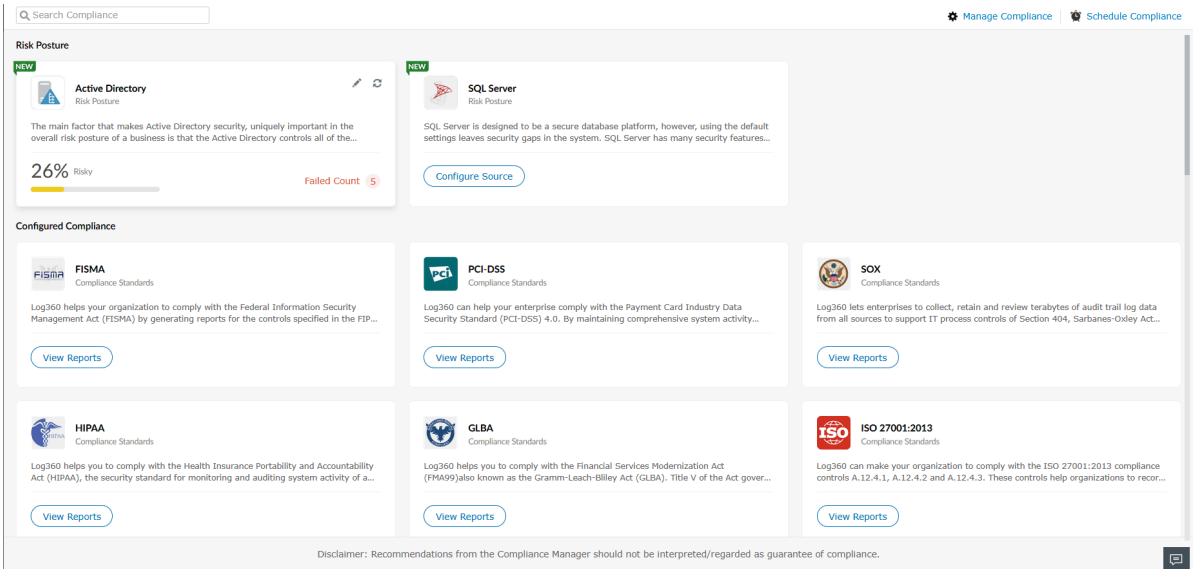
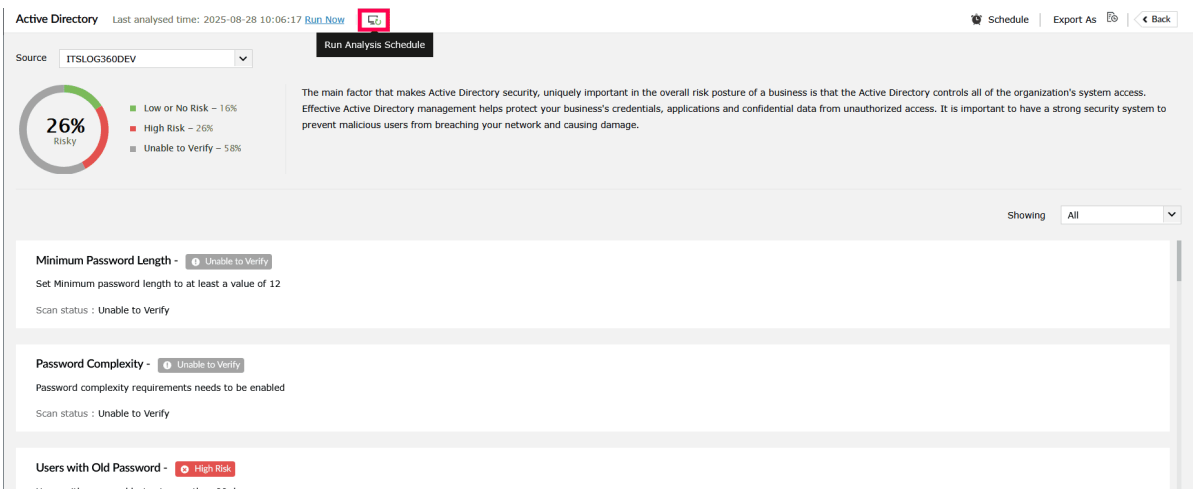


Figure 5: Selecting a source

3. Click the  icon.



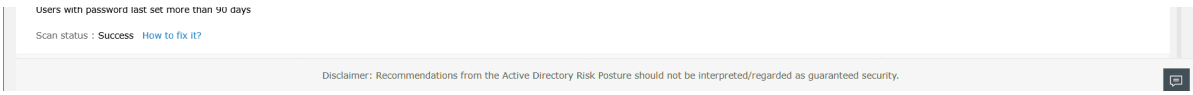


Figure 6: Scheduling run analysis

4. In the Run Analysis Schedule pop-up, set the frequency (Daily, Weekly, or Monthly) and specify the hours and minutes for the analysis to run.

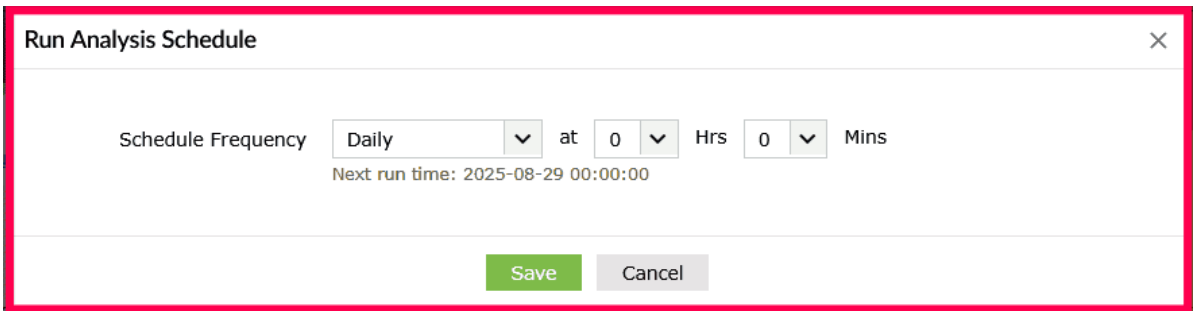


Figure 7: Setting the frequency for schedule analysis

5. If you select Weekly, choose a day from the dropdown. If you select Monthly, choose a month from the dropdown.
6. Click Save to apply the schedule.

Exporting an analysis

1. On the Risk Posture page, locate and select the source you want to export.

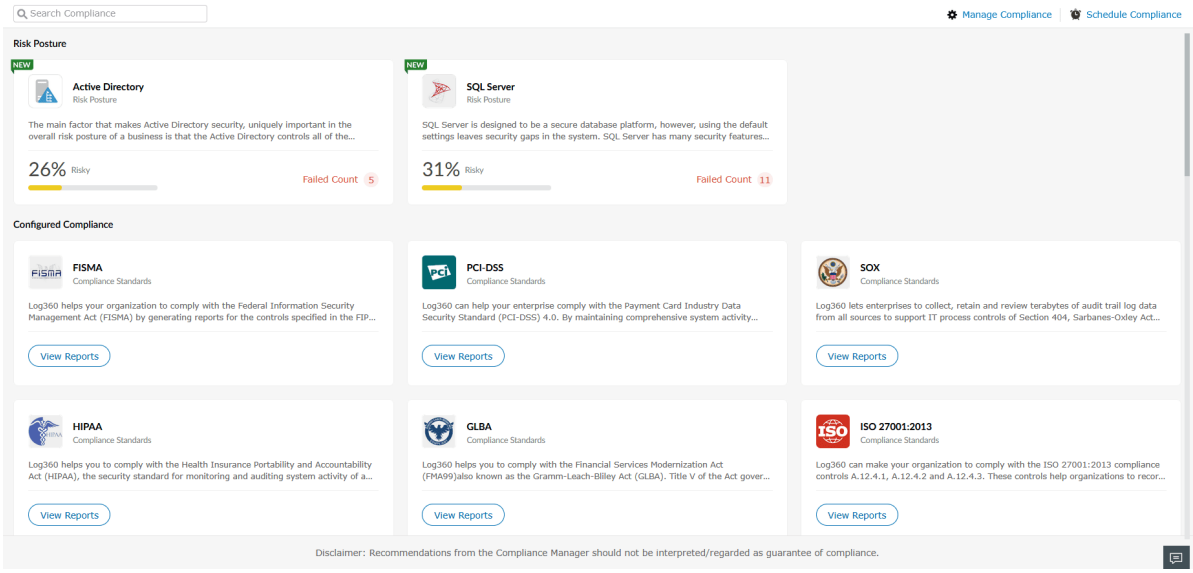
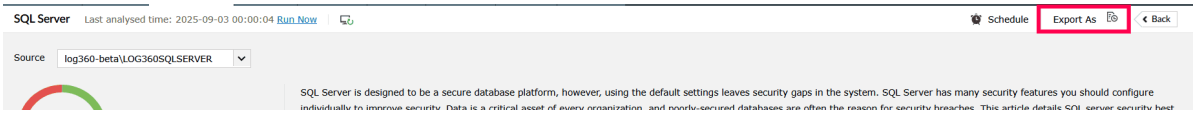


Figure 8: Selecting a source

2. Click Export As in the top-right corner.



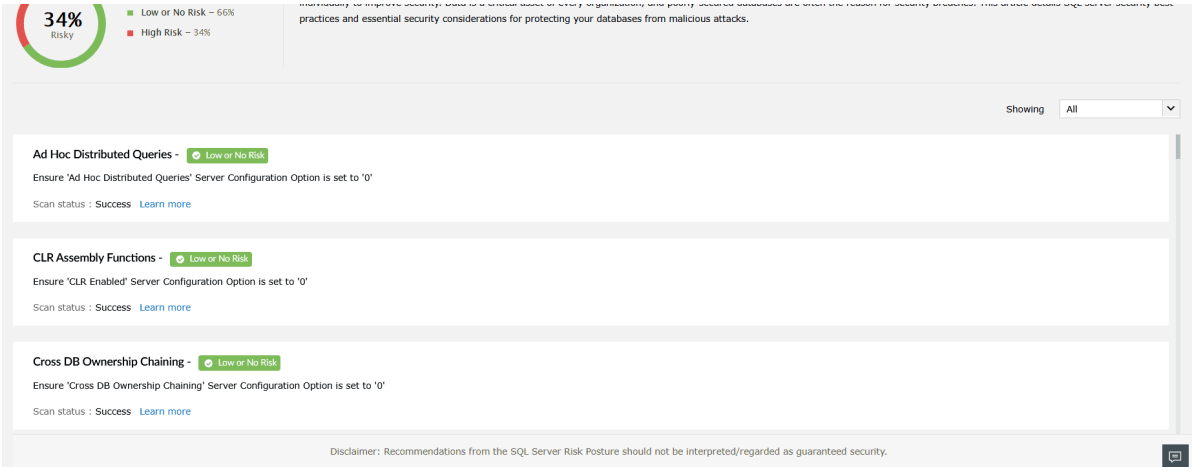


Figure 9: Exporting analysis results

3. In the Export dropdown, choose either Summary or Summary and Details.

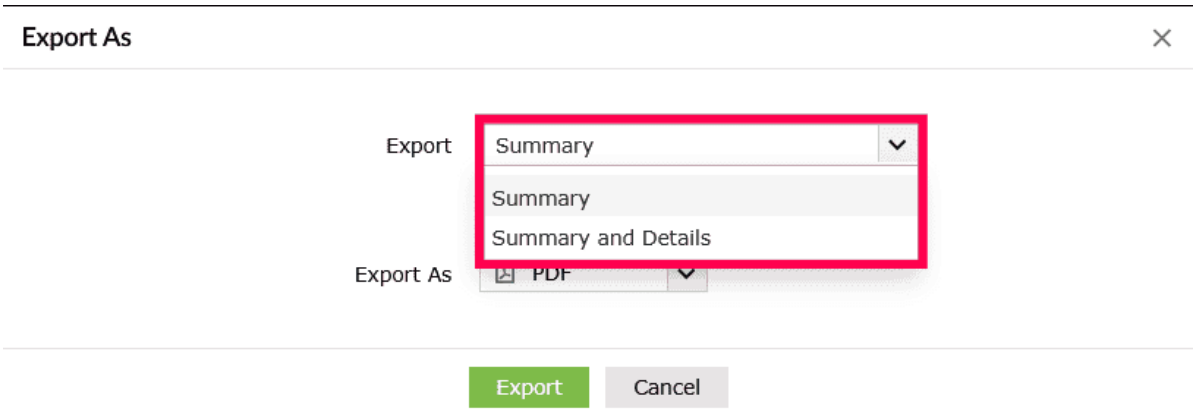


Figure 10: Exporting analysis results

4. (Optional) If you want to run a fresh analysis before exporting, select the Run Analysis before Export checkbox.

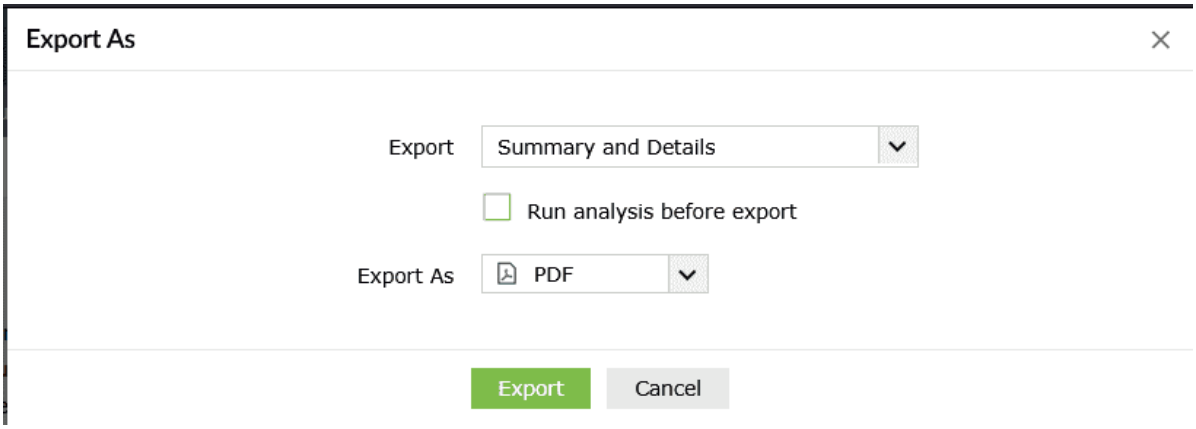
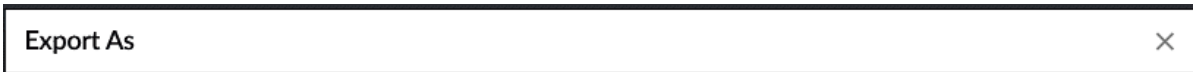


Figure 11: Exporting analysis results

5. In the Export As dropdown, choose the desired format: PDF or CSV.



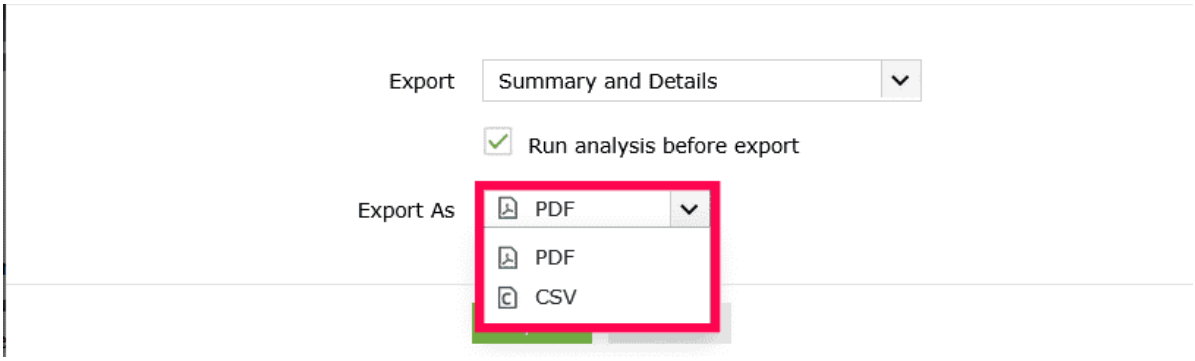


Figure 12: Exporting analysis results

6. Click Export to download the file.

Read also

This section explained how to run, schedule, and export an analysis to keep your risk posture updated. For details on the pre-defined rules available, see:

- Active Directory
- SQL Server

8.4.6.1.3. Active Directory

Last updated on: September 12, 2025

In this page

Overview

Pre-defined rules

Overview

Active Directory (AD) plays a central role in an organization's security posture, as it governs authentication and access to critical systems and resources. Effective AD security helps safeguard user credentials, applications, and confidential data against unauthorized access. Strengthening AD configurations reduces the risk of breaches and protects the business from potential damage caused by malicious actors.
This page explains the pre-defined risk posture rules for Active Directory that the product uses to evaluate configurations and highlight potential vulnerabilities.

Pre-defined rules

The following are the key pre-defined rules used to assess Active Directory configurations and identify potential security risks.

- Minimum Password Length
- Password Complexity
- Users with old password
- Disable Guest Account
- Disable Inactive Users
- Disable Local Administrative Account
- Kerberos User Logon Restriction
- Maximum Lifetime for Kerberos Service Ticket
- Account Lockout Threshold
- Account Lockout Duration
- Session Timeout Duration
- User Password Expiry
- Admin Accounts with old password
- Built-in Domain Administrator Account Usage
- Built-in Domain Administrator Account with Old Password
- Disabled Admin Accounts

- Inactive Enabled Admin Account
- Password Never Expired Users
- Enforce Password History

1. Minimum Password Length

Description:

This security rule determines the least number of characters that a password for a user account may contain. You can set a value between 1 to 14 characters, or you can establish that no password is required by setting the number of characters to 0.

Default:

- 7 on domain controllers.
- 0 on stand-alone servers.

Vulnerability:

Minimum password length policy setting determines the least number of characters that can make up a password for a user account. Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Possible Values:

- User-specified number of characters between 0 and 14 (If the number of characters is set to 0, no password is required)
- Not defined

Best Practice:

Set minimum password length to at least a value of 8. In most environments, an eight-character password is recommended because it's long enough to provide adequate security and still short enough for users to remember easily. A minimum password length greater than 14 isn't supported at the moment. This value will help provide adequate defense against a brute force attack. Adding complexity requirements will help reduce the possibility of a dictionary attack. For more info, see Password must meet complexity requirements.

Recommendation:

Using GUI,

- On your Domain Controller, open the Start Menu and go to Administrative Tools, then select Group Policy Management.
- In the console tree, expand Forest and then Domains, and select the domain where you want to configure the account policies.
- Double-click the domain to view the Group Policy Objects (GPOs) linked to it.
- Right-click Default Domain Policy and select Edit. The Group Policy Editor console will open

- Right-click Default Domain Policy and select Edit. The Group Policy Editor console will open.
- In the editor, navigate to Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy.
- Double-click Password Policy. To configure the minimum password length, right-click Minimum password length and select Properties, then define the desired policy setting.

2. Password Complexity

Description:

This security rule determines if passwords meet the complexity requirements. If this policy is enabled, passwords meet the following requirements: Not contain the user's account name or a part of the user's full name that exceeds two consecutive characters.

- Be at least six characters in length
- Contain characters from three of the following categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)

Complexity requirements are enforced when passwords are changed or created.

Default:

Enabled on domain controllers. Disabled on stand-alone servers.

Vulnerability:

Passwords that contain only alphanumeric characters are easy to discover with several publicly available tools.

Possible Values:

- Enabled
- Disabled
- Not defined

Best Practice:

Set Passwords must meet complexity requirements to Enabled. This policy setting, combined with a minimum password length of 8, ensures that there are at least 159,238,157,238,528 different possibilities for a single password. This setting makes a brute force attack difficult, but not impossible.

- Passwords may not contain the user's samAccountName (Account Name) value or entire displayName (Full Name value). Neither of these checks is case-sensitive.
- The password contains characters from three of the following categories:
  - Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
  - Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic

- Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) Currency symbols such as the Euro or British Pound aren't counted as special characters for this policy setting.
- Any Unicode character that's categorized as an alphabetic character but isn't uppercase or lowercase. This group includes Unicode characters from Asian languages.
- Short passwords that contain only alphanumeric characters are easy to compromise by using publicly available tools. To prevent this vulnerability, passwords should contain other characters and/or meet complexity requirements.

Recommendation:

- Using GUI,
- Open the Start Menu, go to Administrative Tools, and select Group Policy Management.
- In the console tree, expand Forest and then Domains, and select the domain where you want to configure account policies.
- Double-click the domain to view the Group Policy Objects (GPOs) linked to it.
- Right-click Default Domain Policy and select Edit. The Group Policy Editor console will open.
- In the editor, navigate to Computer Configuration, then Policies, followed by Windows Settings → Security Settings → Account Policies → Password Policy.
- Double-click Password Policy. To configure the complexity requirement, right-click Password must meet complexity requirements, select Properties, and enable the policy.

3. Users with old password

Description:

This security rule checks if all the users have changed their password over the past 90 days.

Default:

Enabled on domain controllers. Disabled on stand-alone servers.

Vulnerability:

The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password.

Best Practice:

Set maximum password age to a value between 30 and 90 days, depending on your environment. This way, an attacker has a limited amount of time to compromise a user's password and have access to your network resources.

Recommendation:

- Using GUI

- Using GUI,
- Open the Active Directory Users and Computers tool.
- In the directory tree, select the organizational unit (OU) that contains the account whose password you want to reset.
- Go to Accounts and select the account.
- Right-click the account name and choose Reset Password from the context menu.
- Enter the new password and click OK to apply the changes.
- Using Power Shell,
  - Change a specified account password

```
Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "<new password>" -Force)
```

- Set a password for an account using a distinguished name

```
Set-ADAccountPassword -Identity 'CN=<Common Name>,OU=<Organizational Unit>,DC=<Domain Component>,DC=<Domain Component>' -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "<new password>" -Force)
```

4. Disable Guest Account

Description:

This security setting determines whether the Guest account is enabled or disabled. This account allows unauthenticated network users to gain access to the system by signing in as a Guest with no password. Unauthorized users can access any resources that are accessible to the Guest account over the network. This privilege means that any network shared folders with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network. This accessibility can lead to the exposure or corruption of data.

Default:

Enabled on domain controllers. Disabled on stand-alone servers.

Vulnerability:

The default Guest account allows unauthenticated network users to sign in as a Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any shared folders with permissions that allow access to the Guest account, the Guests group, or the Everyone group are accessible over the network, which could lead to the exposure or corruption of data.

Possible Values:

- Enabled
- Disabled
- Not defined

Best Practice:

Set Guest account status to Disabled so that the built-in Guest account is no longer usable. All network users will have to authenticate before they can access shared resources on the system. If the Guest account is disabled and Network access: Sharing and security model for local accounts is set to Guest only, network logons, such as those logons performed by the SMB Service, will fail.
Recommendation:

- Using GUI,
  - Follow the below steps in GPO.
    - Configure the policy value for Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options.
    - Locate Accounts and set the Guest account status to Disabled.

5. Disable Inactive Users

Description:

This security rule determines if all the inactive Active Directory users were disabled.

Vulnerability:

Active Directory has an account for every user. Over time, users leave the organization, and those user accounts may not get removed from Active Directory. Stale user accounts are a significant security issue, as former employees and external attackers could use those accounts to attack the organization. Stale accounts also use up space in the directory database that could be reclaimed.

Best Practice:

You should carry out regular checks to look for any user accounts that have not changed their passwords in the last three months, and then disable and remove those accounts from Active Directory. Users who are inactive for a period of 90 days need to be removed from the organization.

Recommendation:

- Using GUI,
- Open the Active Directory Users and Computers tool.
- In the directory tree, select the organizational unit (OU) that contains the account you want to delete.
- Go to Accounts and select the account.
- Right-click the account name and choose Delete from the context menu.
- In the confirmation dialog box, click Yes to permanently delete the selected account.
- Using Power Shell,
  - Remove a specified account

- Remove a specified account

```
Remove-ADUser -Identity <account name>
```

- Remove an account by distinguished name

```
Remove-ADUser -Identity "CN=<Common Name>,OU=<Organizational Unit>,DC=
<Domain Component>,DC=<Domain Component>"
```

6. Disable Local Administrative Account

Description:

This security rule determines whether the local administrator account is enabled or disabled.

Default:

Disabled.

Vulnerability:

The built-in administrator account cannot be locked out no matter how many failed logons it accrues, making it a prime target for brute-force attacks that attempt to guess passwords.The account has a well-known Security Identifier (SID), and many non-Microsoft tools allow authentication by using only the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute-force attack by using the SID to log on.

Possible Values:

- Enabled
- Disabled

Best Practice:

It is best practice that the local administrator account is disabled.

Recommendation:

- Using GUI,
  - Follow the below steps in GPO.
    - In the Group Policy Editor, navigate to Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options.
    - Locate Accounts and set Administrator account status to Disabled.

7. Kerberos User Logon Restriction

Description:

This security rule determines if the Kerberos V5 Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the user account. Validation of each request for a session ticket is optional because the extra step takes time and it may slow network access to services.

Default:

Enabled.

Vulnerability:

If you disable this policy setting, users could receive session tickets for services that they no longer have the right to use because the right was removed after they logged on.

Possible Values:

- Enabled
- Disabled
- Not defined

Best Practice:

If this policy setting is disabled, users might be granted session tickets for services that they do not have the right to use. It is advisable to set Enforce user logon restrictions to Enabled.

Recommendation:

- Follow the below steps in GPO.
  - In the Group Policy Editor, navigate to Computer Configuration → Windows Settings → Security Settings → Account Policies → Kerberos Policy.
  - Locate Enforce user logon restrictions and set it to Enabled.

8. Maximum Lifetime for Kerberos Service Ticket

Description:

This security rule determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service. The setting must be greater than 10 minutes and less than or equal to the setting for the maximum lifetime for user ticket.

Default:

600 minutes (10 hours).

Vulnerability:

If you configure the value for the Maximum lifetime for service ticket setting too high, users might be able to access network resources outside their logon hours. In addition, users whose accounts have been disabled might be able to continue accessing network services by using valid service tickets that were issued before their account was disabled.

Possible Values:

- A user-defined number of minutes from 10 through 99,999, or 0 (in which case service tickets don't expire).
- Not defined

Best Practice:

It's advisable to set "Maximum lifetime for service ticket" to 600 minutes.

Recommendation:

- Follow the below steps in GPO.
  - In the Group Policy Editor, navigate to Computer Configuration → Windows Settings → Security Settings → Account Policies → Kerberos Policy.
  - Locate the Maximum lifetime for the service ticket and set it to 600 minutes.

9. Account Lockout Threshold

Description:

This security rule determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

Default: 0.

Vulnerability:

Brute force password attacks can be automated to try thousands or even millions of password combinations for any or all user accounts. Limiting the number of failed sign-ins that can be performed nearly eliminates the effectiveness of such attacks.

Possible Values:

- A user-defined number from 0 through 999
- Not defined

Best Practice:

The threshold that you select is a balance between operational efficiency and security, and it depends on your organization's risk level. To allow for user error and to thwart brute force attacks, Windows security baselines recommend a value of 5 could be an acceptable starting point for your organization.

Recommendation:

- From GUI
  - Follow the below steps in GPO.
- In the Group Policy Editor, go to Computer Configuration → Windows Settings → Security Settings → Account Policies → Account Lockout Policy.
- Set the Account lockout threshold to 5.

10. Account Lockout Duration

Description:

This security rule checks the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it.

Default:

None, because this policy setting only has meaning when an account lockout threshold is specified.

Vulnerability:

A Denial-of-Service (DoS) condition can be created if an attacker abuses the account lockout threshold policy setting and repeatedly attempts to sign in with a specific account. After you configure the account lockout threshold policy setting, the account will be locked out after the specified number of failed attempts.

Possible Values:

- A user-defined number of minutes from 0 through 99,999 (the Account lockout duration is set to 0, the account will remain locked until an administrator unlocks it manually.)
- Not defined

Best Practice:

It's advisable to set Account lockout duration to approximately 30 minutes.

Recommendation:

- Using GUI,
  - Follow the below steps in GPO.
    - In the Group Policy Editor, navigate to Computer Configuration → Windows Settings → Security Settings → Account Policies → Account Lockout Policy.
    - Set Account lockout duration to 30 minutes.

11. Session Timeout Duration

Description:

Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session.

Default:

Not enforced.

Vulnerability:

Long session time out makes un-attended systems a potential end point for attackers. This policy setting helps you prevent unauthorized access to devices under your control when the currently signed-in user leaves without

you prevent unauthorized access to devices under your control when the currently signed-in user leaves without deliberately locking the desktop.

Possible Values:

- The automatic lock of the device is set in elapsed seconds of inactivity, which can range from zero (0) to 599,940 seconds (166.65 hours).
- If the machine is locked after being set to zero (0) or has no value (blank), the policy setting is disabled, and a user sign-in session is never locked after any inactivity.

Best Practice:

Set the time for elapsed user-input inactivity based on the device's usage and location requirements. For example, if the device or device is in a public area, you might want to have the device automatically lock after a short period of inactivity to prevent unauthorized access. However, if the device is used by an individual or group of trusted individuals, such as in a restricted manufacturing area, automatically locking the device might hinder productivity. Setting the machine inactivity timeout seconds to 1000 is recommended.

Recommendation:

- Follow the below steps in GPO.
  - In the Group Policy Editor, navigate to Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options.
  - Set Interactive logon: Machine inactivity limit to 1000 seconds.

12. User Password Expiry

Description:

This security rule determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after multiple days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the minimum password age must be less than the maximum password age. If the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days.

Default: 42.

Vulnerability:

The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password. Configuring the maximum password age policy setting to 0 so that users are never required to change their passwords allows a compromised password to be used by the malicious user for as long as the valid user is authorized access.

Possible Values:

- User-specified number of days between 0 and 999 (Set 0, so that users are never required to change their passwords)
- Not defined

Best Practice:

Set the maximum password age to 90 days, depending on your environment. This way, an attacker has a limited amount of time in which to compromise a user's password and have access to your network resources.

Recommendation:

- Using GUI,
  - Follow the below steps in GPO.
    - In the Group Policy Editor, navigate to Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy.
    - Set Maximum password age to 90 days.

13. Admin Accounts with old password

Description:

This security rule checks if any admin accounts are with passwords that were last set more than 90 days.

Vulnerability:

The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the Admin, or by the Admin sharing the password.

Best Practice:

Reset the password once every 90 days. Use the below steps to reset the password.

Recommendation:

- Using GUI,
- Open the Active Directory Users and Computers tool.
- In the directory tree, select the organizational unit (OU) that contains the account for which you want to reset the password.
- Go to Accounts and select the account.
- Right-click the account name and choose Reset Password from the context menu.
- Enter the new password and click OK to apply the change.
- Using Power Shell,
  - Change a specified account password

```
Set-ADAccountPassword -Identity <account name> -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "<new password>" -Force)
```

  - Set a password for an account using a distinguished name

```
Set-ADAccountPassword -Identity "CN=<Common Name>,OU=<Organizational Unit>,DC
```

```
Set-ADAccountPassword -Identity 'CN=<Common Name>,OU=<Organizational Unit>,DC=
<Domain Component>,DC=<Domain Component>' -Reset -NewPassword (ConvertTo-
SecureString -AsPlainText "<new password>" -Force)
```

14. Built-in Domain Administrator Account Usage

Description:

This security rule determines if any built-in administrator accounts have been active over the last 14 days.

Vulnerability:

Active Directory has an Administrator account for several needs, but it should not be used regularly. If the administrator account is regularly used, it must be monitored. If any malicious activity is found, immediate action must be taken to prevent attackers from attacking the organization.

Best Practice:

You should carry out regular checks to look for any Administrator accounts that have been active within the last 2 weeks and ensure that the built-in Domain Administrator account is legitimate and accounted for. If not accounted for, a breach is likely to occur and should be investigated. Take action for those administrator accounts if any malicious activity is found.

15. Built-in Domain Administrator Account with Old Password

Description:

This security rule determines the period of time (in days) that a password can be used before the system requires the built-in administrator user to change it. You can set passwords to expire after multiple days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the minimum password age must be less than the maximum password age. If the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days.

Vulnerability:

The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the Administrator, or by the Administrator sharing the password.

Best Practice:

Reset the password once every 90 days.

Recommendation:

- Using GUI,
- Open the Active Directory Users and Computers tool.
- In the directory tree, select the organizational unit (OU) that contains the account whose password you want to reset.
- Go to Accounts and select the account.

- Right-click the account name and choose Reset Password from the context menu.
- Enter the new password and click OK to apply the change.
- Using Power Shell,
  - Change a specified account password

```
Set-ADAccountPassword -Identity <account name> -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "<new password>" -Force)
```

  - Set a password for an account using a distinguished name

```
Set-ADAccountPassword -Identity 'CN=<Common Name>,OU=<Organizational Unit>,DC=<Domain Component>,DC=<Domain Component>' -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "<new password>" -Force)
```

16. Disabled Admin Accounts

Description:

This security setting displays all the admin accounts that are disabled.

Vulnerability:

Admin user accounts which are disabled use up unwanted space in the directory database that could be removed from the database.

Best Practice:

You should carry out regular checks to look for privileged users who are all disabled and remove the disabled privilege users from Active Directory.

Recommendation:

- Using GUI,
- Open the Active Directory Users and Computers tool.
- In the directory tree, select the organizational unit (OU) that contains the account you want to delete.
- Go to Accounts and select the account.
- Right-click the account name and choose Delete from the context menu.
- In the confirmation dialog box, click Yes to delete the account permanently.
- Using Power Shell,
  - Remove a specified account

```
Remove-ADUser -Identity <account name>
```

```
Remove-ADUser -Identity <account name>
```

- Remove an account by distinguished name

```
Remove-ADUser -Identity "CN=<Common Name>,OU=<Organizational Unit>,DC=
<Domain Component>,DC=<Domain Component>"
```

17. Inactive Enabled Admin Account

Description:

This security rule checks if all the enabled admin accounts are active over a specified time period.

Vulnerability:

Inactive admin accounts are a significant security issue, as former employees and external attackers could use those accounts to attack the organization. Inactive admin accounts also use up space in the directory database that could be reclaimed.

Best Practice:

You should carry out regular checks to look for any admin accounts that have not been active for 90 days and remove those Admin accounts from Active Directory.
Recommendation:

- Using GUI,
- Open the Active Directory Users and Computers tool.
- In the directory tree, select the organizational unit (OU) that contains the account you want to delete.
- Go to Accounts and select the account.
- Right-click the account name and choose Delete from the context menu.
- In the confirmation dialog box, click Yes to delete the account permanently.
- Using Power Shell,
  - Remove a specified account

```
Remove-ADUser -Identity <account name>
```

  - Remove an account by distinguished name

```
Remove-ADUser -Identity "CN=<Common Name>,OU=<Organizational Unit>,DC=
<Domain Component>,DC=<Domain Component>"
```

18. Password Never Expired Users

Description:

This security rule checks if any users are configured with the Password Never Expires Option.

Vulnerability:

Enabling the "Password Never Expires" option could lead to being compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password.

Possible Values:

- Enabled
- Disabled

Best Practice:

Disable the Password never expires option. It is best practice to uncheck the "Password never expires" check box while creating the user account.
Recommendation:

- Using GUI,
  - Open the Active Directory Users and Computers tool.
  - In the directory tree, select the organizational unit (OU) containing the account you want to modify.
  - Go to Accounts and select the account.
  - Right-click the account name and choose Properties from the context menu.
  - In the Account tab, under Account Options, uncheck the Password never expires checkbox.
- Using Power Shell,
  - set-aduser <account name> -PasswordNeverExpires $false

19. Enforce Password History

Description

This security rule checks if the active directory was configured to prevent password reuse.

Vulnerability:

If password changes are required but password reuse isn't prevented, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users can use the same small number of passwords repeatedly.

Possible Values:

You can specify a number from 0 to 24

Best Practice:

Set Enforce password history to 24. This setting will help mitigate vulnerabilities that are caused by password reuse.
Recommendation:

Recommendation:

- Open the Start Menu, go to Administrative Tools, and select Group Policy Management.
- In the console tree, expand Forest and then Domains, and select the domain where you want to configure account policies.
- Double-click the domain to view the Group Policy Objects (GPOs) linked to it.
- Right-click Default Domain Policy and select Edit. The Group Policy Editor console will open.
- In the editor, navigate to Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy.
- Double-click Password Policy, right-click Enforce Password History, select Properties, and define the desired policy setting.

Read Also

This section details the pre-defined rules for Active Directory, including descriptions, default values, vulnerabilities, best practices, and recommendations. For more information, see:

- SQL Server

8.4.6.1.4. SQL Server

Last updated on: September 12, 2025

In this page

Overview

Pre-defined rules

Overview

SQL Server is designed as a secure database platform, but relying on default settings can leave security gaps. Its security features should be configured individually to ensure robust protection. Since organizational data is a critical asset, poorly secured databases are often a primary target for attacks.
This article outlines SQL Server security best practices and essential considerations to help safeguard your databases from unauthorized access, tampering, and other malicious activity.

Pre-defined rules

The following are the key pre-defined rules used to assess SQL Server configurations and identify potential security risks.

- Ad Hoc Distributed Queries
- CLR Assembly Functions
- Cross DB Ownership Chaining
- Database Mail XPs
- OLE Automation Procedures
- Remote Access
- Remote Admin Connections
- Scan For Startup Procedures
- Trustworthy Database Property
- SQL Mail XPs
- Standard Port
- Hide Instance
- Disable SA Login
- Rename SA Login
- XP CMDSHELL
- Auto Close
- Restrict SA Login

- Restrict SA Login
- CLR Strict Security
- Authentication Mode
- Guest Connect Permissions
- Orphaned Users
- Contained Database Authentication
- Public Default Permissions
- Built-in Group as Login
- Local Group as Login
- Agent Proxy Access for public role
- Check Password Expiration
- Check Password Policy
- Number of Error Log Files
- Default Trace
- Login Audit
- SQL Server Audit
- CLR Assembly Permission
- Symmetric Key Encryption Algorithm
- Asymmetric Key Size

1. Ad Hoc Distributed Queries

Description:

Ensure the 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0'

Vulnerability:

Enabling Ad Hoc Distributed Queries allows users to query data and execute statements on external data sources. This feature can be used to access remotely and exploit vulnerabilities on remote SQL Server instances and to run unsafe visual basic for application functions.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.
Recommendation:
Run the following T-SQL command:
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE;

EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE;
EXECUTE sp_configure 'Ad Hoc Distributed Queries', 0; RECONFIGURE;
GO
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;

2. CLR Assembly Functions

Description:

Ensure the 'CLR Enabled' Server Configuration Option is set to '0'

Vulnerability:

The CLR enabled option specifies whether user assemblies can be run by SQL Server. Enabling use of CLR assemblies widens the attack surface of SQL Server and puts it at risk from both inadvertent and malicious assemblies.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This functionality should be disabled if the 'clr strict security' option is set to 0. Note that this option is only available since SQL Server 2017. If clr strict security is set to 1 this recommendation is not applicable. By default, clr strict security is enabled and treats SAFE and EXTERNAL_ACCESS assemblies as if they were marked UNSAFE. Though not recommended, the clr strict security option can be disabled for backward compatibility. To check the status of 'clr strict security' option, run the following T-SQL command:

```
SELECT name, CAST(value as int) as value_configured, CAST(value_in_use as int) as
value_in_use FROM sys.configurations WHERE name = 'clr strict security';
```

Recommendation:

Run the following T-SQL command:

```
EXECUTE sp_configure 'clr enabled', 0; RECONFIGURE;
```

3. Cross DB Ownership Chaining

Description:

Ensure the 'Cross DB Ownership Chaining' Server Configuration Option is set to '0'

Vulnerability:

This option allows a member of the db_owner role in a database to gain access to objects owned by a login in any other database, causing an unnecessary information disclosure. Cross-database ownership chaining should only be enabled for the specific databases requiring it, instead of enabling it at the instance level for all databases by using the ALTER DATABASESET DB_CHAINING ON command. This database option may not be changed on the master, model, or tempdb system databases.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
EXECUTE sp_configure 'cross db ownership chaining', 0; RECONFIGURE; GO
```

4. Database Mail XPs

Description:

Ensure 'Database Mail XPs' Server Configuration Option is set to '0'

Vulnerability:

The Database Mail XPs option controls the ability to generate and transmit email messages from SQL Server.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'. Disabling the Database Mail XPs option reduces the SQL Server surface, eliminates a DOS attack vector and channel to exfiltrate data from the database server to a remote host.

Recommendation:

Run the following T-SQL command:
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'Database Mail XPs', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced

```
options', 0; RECONFIGURE;
```

5. OLE Automation Procedures

Description:

Ensure the 'Ole Automation Procedures' Server Configuration Option is set to '0'

Vulnerability:

The OLE Automation Procedures option controls whether OLE Automation objects can be instantiated within Transact-SQL batches. These are extended stored procedures that allow SQL Server users to execute functions external to SQL Server. Enabling this option will increase the attack surface of SQL Server and allow users to execute functions in the security context of SQL Server.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure
'Ole Automation Procedures', 0; RECONFIGURE;
GO
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;
```

6. Remote Access

Description:

Ensure the 'Remote Access' Server Configuration Option is set to '0'

Vulnerability:

The 'Remote Access' option controls the execution of local stored procedures on remote servers or remote stored procedures on local servers. This functionality can be abused to launch a Denial-of-Service (DoS) attack on remote servers by off-loading query processing to a target.

Possible Values:

- Enabled or '1'
- Disabled or '0'

- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure
'remote access', 0; RECONFIGURE;
GO
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;
```

> NOTE
>
> Restart the SQL Server service.

7. Remote Admin Connections

Description:

Ensure the 'Remote Admin Connections' Server Configuration Option is set to '0'

Vulnerability:

The remote admin connections option controls whether a client application on a remote computer can use the Dedicated Administrator Connection (DAC).The DAC lets an administrator access a running server to execute diagnostic functions or Transact-SQL statements, or to troubleshoot problems on the server, even when the server is locked or running in an abnormal state and not responding to a SQL Server Database Engine connection.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

In a cluster scenario, the administrator may not actually be logged on to the same node that is currently hosting the SQL Server instance and thus is considered "remote". Therefore, this setting should usually be enabled (1) for SQL Server failover clusters; otherwise, it should be disabled (0).

Recommendation:

Run the following T-SQL command:

```
EXECUTE sp_configure 'remote admin connections', 0; RECONFIGURE;
GO
```

8. Scan For Startup Procedures

Description:

Ensure the 'Scan For Startup Procs' Server Configuration Option is set to '0'

Vulnerability:

The scan for startup procedures option, if enabled, causes SQL Server to scan for and automatically run all stored procedures that are set to execute upon service startup. Setting Scan for Startup Procedures to 0 will prevent certain audit traces and other commonly used monitoring stored procedures from re-starting on start up. Additionally, replication requires this setting to be enabled (1) and will automatically change this setting if needed.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure
'scan for startup procs', 0; RECONFIGURE;
GO
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;
```

> NOTE
>
> Restart the SQL Server service.

9. Trustworthy Database Property

Description:

Ensure the 'Trustworthy' Database Property is set to 'Off'

Vulnerability:

The TRUSTWORTHY database option allows database objects to access objects in other databases under certain circumstances. Provides protection from maliciousnCLR assemblies or extended procedures.

Possible Values:

- Enabled or 'ON'
- Disabled or 'OFF'

Best Practice:

This configuration should be set to '0' except for msdb database which requires this to be 'ON'.

Recommendation:

Run the following T-SQL command for the databases where this property is turned on:

```
ALTER DATABASE [<database_name>] SET TRUSTWORTHY OFF;
```

10. SQL Mail XPs

Description:

Ensure the 'SQL Mail XPs' Server Configuration Option is set to '0'

Vulnerability:

SQL Mail provides a mechanism to send, receive, delete, and process e-mail messages using SQL Server in 2008 R2 or Before.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure
'SQL Mail XPs', 0; RECONFIGURE;
GO
```

```
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;
```

11. Standard Port

Description:

Using default port(1433) makes the server vulnerable to the attacks directed to the default port.

Vulnerability:

Enabling Ad Hoc Distributed Queries allows users to query data and execute statements on external data sources. This feature can be used to access remotely and exploit vulnerabilities on remote SQL Server instances and to run unsafe Visual Basic for Application functions.

Possible Values:

Any port available on the server.

Best Practice:

The port can be anything but the default 1433.

Recommendation:

Using GUI,

- Open SQL Server Configuration Manager
- In the console pane, expand SQL Server Network Configuration, expand Protocols for <InstanceName>, and then double click the TCP/IP protocol.
- In the TCP/IP Properties dialog box, on the IP Addresses tab, several IP addresses appear in the format IP1, IP2, up to IPAll. One of these is for the IP address of the loopback adapter, 127.0.0.1. Additional IP addresses appear for each IP address on the computer.
- Under IPAll, do one of the following:
  - Change the TCP Port field from 1433 to a non-standard port.
  - Or, leave the TCP Port field empty and set TCP Dynamic Ports to 0 to enable dynamic port assignment.
- Click OK to save changes.
- In the console pane, click SQL Server Services.
- In the details pane, right-click SQL Server (<InstanceName>) and select Restart to stop and restart SQL Server.

> NOTE
>
> The connection settings of any application that uses port number to communicate with the SQL server needs to be reconfigured while changing the port of SQL server.

Steps to reconfigure the port number of SQL server in EventLog Analyzer:

- Shut down the product.
- Open <EventLog Analyzer Home>\conf\database_params.conf
- Change existing port number to the required port number.
- Restart EventLog Analyzer for the changes to take effect.

12. Hide Instance

Description:

Ensure the 'Hide Instance' option is set to 'Yes' for Production SQL Server instances

Vulnerability:

Non-clustered SQL Server instances within production environments should be designated as hidden to prevent advertisements by the SQL Server Browser service. However, clustered instances may break if this option is selected. If you hide a clustered named instance, the cluster service may not be able to connect to the SQL Server.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '1'.

Recommendation:

Using GUI,

- Open SQL Server Configuration Manager
- Expand SQL Server Network Configuration, right-click Protocols for <InstanceName>, and then select Properties
- On the Flags tab, in the Hide Instance box, if Yes is selected, it is compliant.

Alternatively, run the following T-SQL command:

```
EXEC master.sys.xp_instance_regwrite @rootkey = N'HKEY_LOCAL_MACHINE', @key =
N'SOFTWARE\Microsoft\Microsoft SQL Server\MSSQLServer\SuperSocketNetLib',
@value_name = N'HideInstance', @type = N'REG_DWORD', @value = 1;
```

NOTE

- Restart the SQL Server service.

- Applications that use the SQL Browser service to discover SQL Server instances will not be able to discover the instance automatically if 'Hide Instance' is enabled. Either the 'Hide Instance' should be temporarily disabled or the port number should be used to connect to the SQL Server instance.

13. Disable SA Login

Description:

Ensure the 'SA' Login Account is set to 'Disabled'

Vulnerability:

The SA account is a widely known and often widely used SQL Server account with sysadmin privileges. This is the original login created during installation and always has the principal_id=1 and sid=0x01. Enforcing this control reduces the probability of an attacker executing brute force attacks against a well-known principal.

Possible Values:

- Enabled
- Disabled

Best Practice:

It is not a good security practice to code applications or scripts to use the sa account. However, if this has been done, disabling the sa account will prevent scripts and applications from authenticating to the database server and executing required tasks or functions.

Recommendation:

Run the following T-SQL command:

```
USE [master]
GO
DECLARE @tsql nvarchar(max) SET @tsql = 'ALTER LOGIN ' + SUSER_NAME(0x01) + '
DISABLE' EXEC (@tsql)
GO
```

NOTE

The applications which use SA login to authenticate SQL Server connection need to be reconfigured with a different user while altering the SA login.

14. Rename SA Login

14. Rename SA Login

Description:

Ensure the 'SA' Login Account has been renamed

Vulnerability:

It is easier to launch password-guessing and brute-force attacks against the sa login if the name is known.

Possible Values:

Any set of characters that are allowed by Microsoft SQL login name restrictions

Best Practice:

The SA Login should be renamed.

Recommendation:

Run the following T-SQL command:

```
ALTER LOGIN SA WITH NAME = <different_user>;
```

> NOTE
>
> The applications which use SA login to authenticate SQL Server connection need to be reconfigured with a different user while altering the SA login.

15. XP CMDSHELL

Description:

Ensure 'xp_cmdshell' Server Configuration Option is set to '0'

Vulnerability:

The xp_cmdshell option controls whether the xp_cmdshell extended stored procedure can be used by an authenticated SQL Server user to execute operating-system command shell commands and return results as rows within the SQL client.The xp_cmdshell procedure is commonly used by attackers to read or write data to/from the underlying Operating System of a database server.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure
'xp_cmdshell', 0; RECONFIGURE;
GO
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;
```

16. Auto Close

Description:

Ensure 'AUTO_CLOSE' is set to 'OFF' on contained databases

Vulnerability:

AUTO_CLOSE determines if a given database is closed or not after a connection terminates. If enabled, subsequent connections to the given database will require the database to be reopened and relevant procedure caches to be rebuilt.

Possible Values:

- Enabled or 'ON'
- Disabled or 'OFF'

Best Practice:

This configuration should be set to 'OFF'.

Recommendation:

Run the following T-SQL command for databases where this configuration is 'OFF':

```
ALTER DATABASE <database_name> SET AUTO_CLOSE OFF;
```

17. Restrict SA Login

Description:

Ensure no login exists with the name 'sa"

Vulnerability:

The SA login (e.g. principal) is a widely known and often widely used SQL Server account. Therefore, there should not be a login called SA even when the original SA login (principal_id = 1) has been renamed

should not be a login called SA even when the original SA login (principal_id = 1) has been renamed.

Possible Values:

Login names can be of any set of characters allowed by Microsoft SQL Login name guidelines.

Best Practice:

No Logins should be named as 'sa'.

Recommendation:

Run the following T-SQL command for logins where name is 'sa':

```
USE [master]
GO
ALTER LOGIN [sa] WITH NAME = <different_name>;
GO
```

> NOTE
>
> The applications which use the altered logins to authenticate the SQL Server connection need to be reconfigured by another user with equivalent privileges.

18. CLR Strict Security

Description:

Ensure 'clr strict security' Server Configuration Option is set to '1'

Vulnerability:

The clr strict security option specifies whether the engine applies the PERMISSION_SET on the assemblies in SQL Server 2017 and 2019.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '1'.

Recommendation:

Run the following T-SQL command:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure
'clr strict security', 1; RECONFIGURE;
GO
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;
```

19. Authentication Mode

Description:

Ensure the 'Server Authentication' Property is set to 'Windows Authentication Mode'

Vulnerability:

Windows provides a more robust authentication mechanism than SQL Server authentication.

Possible Values:

- SQL Server Authentication
- Windows Authentication
- Mixed Authentication

Best Practice:

This configuration should be set to 'Windows Authentication Mode'.

Recommendation:

Using GUI,

- Open SQL Server Management Studio.
- Open the Object Explorer tab and connect to the target SQL Server instance.
- Right click the instance name and select Properties.
- Select the Security page from the left menu.
- Set the Server authentication setting to Windows Authentication Mode.

Alternatively, run the following T-SQL command:

```
USE [master]
GO
EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
N'Software\Microsoft\MSSQLServer\MSSQLServer', N'LoginMode', REG_DWORD, 1
GO
```

NOTE

NOTE

Restart the SQL Server service.

20. Guest Connect Permissions

Description:

Ensure CONNECT permissions on the 'guest' user is Revoked within all SQL Server databases excluding the master, msdb and tempdb

Vulnerability:

A login assumes the identity of the guest user when a login has access to SQL Server but does not have access to a database through its own account and the database has a guest user account. Revoking the CONNECT permission for the guest user will ensure that a login is not able to access database information without explicit access to do so.

Possible Values:

The guest users might have or might not have CONNECT permissions.

Best Practice:

CONNECT permission for guest users must be revoked in all databases except for master, msdb and tempdb.

Recommendation:

Run the following T-SQL command for the databases with guest connect permission on:

```
USE <database_name>;
GO
REVOKE CONNECT FROM guest CASCADE;
```

21. Orphaned Users

Description:

Ensure 'Orphaned Users' are Dropped From SQL Server Databases

Vulnerability:

A database user for which the corresponding SQL Server login is undefined or is incorrectly defined on a server instance cannot log in to the instance and is referred to as orphaned and should be removed. Orphan users should be removed to avoid potential misuse of those broken users in any way.

Possible Values:

A Database might have or might not have any orphaned users

Best Practice:

No orphaned users must be present in a database server.

Recommendation:

Run the following T-SQL command for all the orphaned users:

```
USE <database_name>;
GO
DROP USER <username>;
```

> NOTE
>
> The orphaned users can be troubleshooted if possible. Refer Microsoft learn for further details.

22. Contained Database Authentication

Description:

Ensure SQL Authentication is not used in contained databases

Vulnerability:

Contained databases do not enforce password complexity rules for SQL Authenticated users. The absence of an enforced password policy may increase the likelihood of a weak credential being established in a contained database.

Possible Values:

- SQL Server Authentication
- Windows Authentication
- Mixed Authentication

Best Practice:

This configuration should be set to 'Windows Authentication Mode'.

Recommendation:

Leverage Windows Authenticated users in contained databases.

> NOTE
>
> Refer Microsoft learn for further details.

If required, use the following T-SQL command to drop logins:

```
USE <db_name>
GO
DROP USER <user_name>;
```

> NOTE
>
> Applications that use dropped logins to authenticate the SQL server need to be reconfigured with different logins.

23. Public Default Permissions

Description:

Ensure only the default permissions specified by Microsoft are granted to the public server role

Vulnerability:

The 'public' is a special fixed server role containing all logins. Unlike other fixed server roles, permissions can be changed for the public role. In keeping with the principle of least privileges, the public server role should not be used to grant permissions at the server scope as these would be inherited by all users. Every SQL Server login belongs to the public role and cannot be removed from this role. Therefore, any permissions granted to this role will be available to all logins unless they have been explicitly denied to specific logins or user-defined server roles. When the extraneous permissions are revoked from the public server role, access may be lost unless the permissions are granted to the explicit logins or to user-defined server roles containing the logins which require the access.

Possible Values:

Any number of permissions might be given to public roles.

Best Practice:

No extraneous permission must be given to the public role and should be removed if given and delegated to a user defined role if needed.

Recommendation:

Add the extraneous permissions found in the results to the specific logins to user-defined server roles that require the access.
Run the following T-SQL command for the permissions found:

```
USE [master]
GO
REVOKE <permission_name> FROM public;
GO
```

NOTE

For public roles, 'View any database' and 'Connect' are permissible.

24. Builtin Group as Login

Description:

Ensure Windows BUILTIN groups are not SQL Logins

Vulnerability:

The BUILTIN groups (Administrators, Everyone, Authenticated Users, Guests, etc.) generally contain extensive memberships, which would not meet the best practice of ensuring only the necessary users have been granted access to a SQL Server instance. These groups should not be used for any level of access into a SQL Server Database Engine instance.

Possible Values:

Any group, whether it be BUILTIN or user defined, can be SQL Logins.

Best Practice:

The Windows BUILTIN groups must be removed from SQL Logins. Note that before dropping the BUILTIN group logins, ensure that alternative AD Groups or Windows logins have been added with equivalent permissions. Otherwise, the SQL Server instance may become totally inaccessible.

Recommendation:

Using GUI,

- Open Computer Management.
- Click on Local Users and Groups. If needed, create a restrictive AD group containing only the required user accounts.
- Open SQL Server Management Studio → Connect to the database → Select New Login in the Left pane → Add the AD group or individual Windows accounts as a SQL Server login and grant it the permissions required.
- Drop the BUILTIN login using the syntax below after replacing <name>.

```
USE [master]
GO
```

```
GO
DROP LOGIN [<name>]
GO
```

25. Local Group as Login

Description:

Ensure Windows Local groups are not SQL Logins

Vulnerability:

Local Windows groups should not be used as logins for SQL Server instances. Allowing local Windows groups as SQL Logins provides a loophole whereby anyone with OS level administrator rights (and no SQL Server rights) could add users to the local Windows groups and give themselves or others access to the SQL Server instance.

Possible Values:

Any windows group can be SQL Login.

Best Practice:

The Windows Local groups must be removed from SQL Logins. Note that before dropping the Local group logins, ensure that alternative AD Groups or Windows logins have been added with equivalent permissions. Otherwise, the SQL Server instance may become totally inaccessible.

Recommendation:

Using GUI,

- Open Computer Management.
- Click on Local Users and Groups. If needed, create a restrictive AD group containing only the required user accounts.
- Open SQL Server Management Studio → Connect to the database → Select New Login in the Left pane → Add the AD group or individual Windows accounts as a SQL Server login and grant it the permissions required.
- Drop the Local group name logins using the syntax below after replacing <name>.

```
USE [master]
GO
DROP LOGIN [<name>]
GO
```

26. Agent Proxy Access for public role

Description:

Ensure the public role in the msdb database is not granted access to SQL Agent proxies

Vulnerability:

Granting access to SQL Agent proxies for the public role would allow all users to utilize the proxy, which may have high privileges. This would likely break the principle of least privileges.

Possible Values:

The public role might have access to any number of proxies.

Best Practice:

Revoke any agent proxy access to the public role. Before revoking the public role from the proxy, ensure that alternative logins or appropriate user-defined database roles have been added with equivalent permissions. Otherwise, SQL Agent job steps dependent upon this access will fail.

Recommendation:

Using GUI,

- Open SQL Server Management Studio → Connect to the database → Select Server SQL Agent → Select the proxy in interest → Right Click and select Properties → Add specific security principals which require access.
- Alternatively use sp_grant_login_to_proxy T-SQL.
  NOTE Refer Microsoft learn for further details.
- Revoke access to the <proxyname> from the public role using the following T-SQL command:

```
USE [msdb]
GO
EXEC dbo.sp_revoke_login_from_proxy @name = N'public', @proxy_name = N'<proxyname>';
GO
```

27. Check Password Expiration

Description:

Ensure the 'CHECK_EXPIRATION' option is set to 'ON' for all SQL Authenticated Logins Within the Sysadmin Role

Vulnerability:

Applies the same password expiration policy used in Windows to passwords used inside SQL Server if turned on. Else, the passwords in use might be weak.

Possible Values:

- Enabled or 'ON'
- Disabled or 'OFF'

Disabled or 'OFF'

Best Practice:

This option should be set to 'ON'. This is a mitigating recommendation for systems which cannot follow the recommendation to use only Windows Authenticated logins.

Recommendation:

Run the following T-SQL command for the login names where check expiration is set to 'OFF':

```
ALTER LOGIN [<login_name>] WITH CHECK_EXPIRATION = ON;
```

28. Check Password Policy

Description:

Ensure the 'CHECK_POLICY' Option is set to 'ON' for All SQL Authenticated Logins

Vulnerability:

Applies the same password complexity policy used in Windows to passwords used inside SQL Server if turned on. Else, the passwords in use might be weak.

Possible Values:

- Enabled or 'ON'
- Disabled or 'OFF'

Best Practice:

This option should be set to 'ON'. The setting is only enforced when the password is changed. This setting does not force existing weak passwords to be changed. Thus existing passwords need to be changed manually.

Recommendation:

Run the following T-SQL command for the login names where check policy is set to 'OFF':

```
ALTER LOGIN [<login_name>] WITH CHECK_POLICY = ON;
```

29. Number of Error Log Files

Description:

Ensure 'Maximum number of error log files' is set to greater than or equal to '12'

Vulnerability:

SQL Server error log files must be protected from loss. The log files must be backed up before they are

overwritten. Retaining more error logs helps prevent loss from frequent recycling before backups can occur.

Possible Values:

All positive numerical values

Best Practice:

This option should be set to greater than or equal to 12.

Recommendation:

Using GUI,

- Open SQL Server Management Studio.
- Open Object Explorer and connect to the target instance.
- Navigate to the Management tab in Object Explorer and expand. Right click on the SQL Server Logs file and select Configure.
- Verify the Limit the number of error log files before they are recycled checkbox is checked.
- Verify the Maximum number of error log files is greater than or equal to 12.

Alternatively, run the following T-SQL command replacing <NumberGreaterThanOrEqualTo12>:

```
EXEC master.sys.xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
N'Software\Microsoft\MSSQLServer\MSSQLServer', N'NumErrorLogs', REG_DWORD,
<NumberGreaterThanOrEqualTo12>;
```

30. Default Trace

Description:

Ensure the 'Default Trace Enabled' Server Configuration Option is set to '1'

Vulnerability:

The default trace provides audit logging of database activity including account creations, privilege elevation and execution of DBCC commands.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '1'.

Recommendation:

Run the following T-SQL command:

Run the following T-SQL command:

```
EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure
'default trace enabled', 1; RECONFIGURE;
GO
EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;
```

31. Login Audit

Description:

Ensure 'Login Auditing' is set to 'failed logins'

Vulnerability:

This setting will record failed authentication attempts for SQL Server logins to the SQL Server Error-log. Capturing failed logins provides key information that can be used to detect or confirm password guessing attacks. Capturing successful login attempts can be used to confirm server access during forensic investigations, however, using this audit level setting to also capture successful logins creates excessive noise in the SQL Server Error-log which can hamper a DBA trying to troubleshoot problems.

Possible Values:

- None
- Failed
- Successful
- Both Failed and Successful

Best Practice:

This configuration should be set to 'failure'.

Recommendation:

Using GUI,

- Open SQL Server Management Studio.
- Right click the target instance and select Properties and navigate to the Security tab.
- Select the option Failed logins only under the Login Auditing section and click OK.

Alternatively, run the following T-SQL command:

```
EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 2
```

NOTE: Restart SQL Server service.

32. SQL Server Audit

Vulnerability:

SQL Server Audit is capable of capturing both failed and successful logins and writing them to one of three places: the application event log, the security event log, or the file system. By utilizing Audit instead of the traditional setting under the security tab to capture successful logins, we reduce the noise in the ERRORLOG.

Possible Values:

Any number of Server Audits might be present in a Server with Audit Action Type of AUDIT_CHANGE_GROUP, FAILED_LOGIN_GROUP and SUCCESSFUL_LOGIN_GROUP.

Best Practice:

There should be atleast one Server Audit specification must be created/present with following audit names:

- AUDIT_CHANGE_GROUP
- FAILED_LOGIN_GROUP
- SUCCESSFUL_LOGIN_GROUP

Recommendation:

Using GUI,

- Open SQL Server Management Studio.
- Expand the SQL Server in Object Explorer.
- Expand the Security Folder.
- Right-click on the Audits folder and choose New Audit.
- Specify a name for the Server Audit.
- Specify the audit destination details and then click OK to save the Server Audit.
- Right-click on Server Audit Specifications and choose New Server Audit Specification.
- Name the Server Audit Specification.
- Select the created Server Audit in the Audit drop-down selection.
- Click the drop-down under Audit Action Type and select AUDIT_CHANGE_GROUP.
- Click the new drop-down Audit Action Type and select FAILED_LOGIN_GROUP.
- Click the new drop-down under Audit Action Type and select SUCCESSFUL_LOGIN_GROUP.
- Click OK to save the Server Audit Specification.
- Right-click on the new Server Audit Specification and select Enable Server Audit Specification.
- Right-click on the new Server Audit and select Enable Server Audit.

Alternatively, run the following T-SQL command replacing <Enter audit name here> and <Enter audit spec name

Alternatively, run the following T-SQL command replacing <Enter audit name here> and <Enter audit spec name here>:

```
USE master
GO
CREATE SERVER AUDIT <Enter audit name here> TO APPLICATION_LOG;
GO
CREATE SERVER AUDIT SPECIFICATION <Enter audit spec name here> FOR SERVER
AUDIT <Enter audit name here> ADD (FAILED_LOGIN_GROUP), ADD
(SUCCESSFUL_LOGIN_GROUP), ADD (AUDIT_CHANGE_GROUP), ADD
(SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP), ADD
(FAILED_DATABASE_AUTHENTICATION_GROUP) WITH (STATE = ON);
GO
ALTER SERVER AUDIT <Enter audit name here> WITH (STATE = ON);
GO
```

33. CLR Assembly Permission

Description:

Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies

Vulnerability:

Setting CLR Assembly Permission Sets to SAFE_ACCESS will prevent assemblies from accessing external system resources such as files, the network, environment variables, or the registry. Assemblies with EXTERNAL_ACCESS or UNSAFE permission sets can be used to access sensitive areas of the operating system, steal and/or transmit data and alter the state and other protection measures of the underlying Windows Operating System.

Possible Values:

- SAFE_ACCESS
- EXTERNAL_ACCESS
- UNSAFE

Best Practice:

All CLR Assemblies should have the permission set to 'SAFE_ACCESS' except for those which are Microsoft-created (is_user_defined = 0) are excluded from this check as they are required for overall system functionality. The remediation measure should first be tested within a test environment before production to ensure the assembly still functions as designed with SAFE permission setting.

Recommendation:

Run the following T-SQL command:

```
USE <database_name>;
GO
ALTER ASSEMBLY <assembly_name> WITH PERMISSION_SET = SAFE;
```

Symmetric Key Encryption Algorithm

Description:

Ensure 'Symmetric Key Encryption algorithm' is set to 'AES_128' or higher in non-system databases

Vulnerability:

As per the Microsoft Best Practices, only the SQL Server AES algorithm options, AES_128, AES_192, and AES_256, should be used for a symmetric key encryption algorithm. The following algorithms (as referred to by SQL Server) are considered weak or deprecated and should no longer be used in SQL Server: DES, DESX, RC2, RC4, RC4_128.

Possible Values:

- DES
- Triple DES
- TRIPLE_DES_3KEY
- RC2
- RC4
- 128-bit RC4
- DESX
- 128-bit AES
- 192-bit AES
- 256-bit AES

Best Practice:

All Symmetric keys in the database must use 'AES_128' or higher as encryption algorithm.

Recommendation:

NOTE: Refer Microsoft learn to know more about Altering symmetric key.
If required, use the following T-SQL command to drop symmetric keys:

```
USE <database_name>
GO
DROP SYMMETRIC KEY <key_name>;
```

35. Asymmetric Key Size

Description:

Ensure Asymmetric Key Size is set to 'greater than or equal to 2048' in non-system databases

Vulnerability:

Microsoft Best Practices recommend using at least a 2048-bit encryption algorithm for asymmetric keys. The RSA_2048 encryption algorithm for asymmetric keys in SQL Server is the highest bit-level provided and therefore the most secure available choice.

Possible Values:

- 512 bit
- 1024 bit
- 2048 bit

Best Practice:

Asymmetric key size should be set to greater than or equal to 2048 bits.

Recommendation:

NOTE: Refer Microsoft learn to know more about Altering asymmetric key.
If required, use the following T-SQL command to drop asymmetric keys:

```
USE <database_name>
GO
DROP ASYMMETRIC KEY <key_name>;
```

Read Also
This section details the pre-defined rules for SQL Server, including descriptions, default values, vulnerabilities, best practices, and recommendations. For more information, see:

- Active Directory

8.5.1. Log Search in EventLog Analyzer

Last updated on: September 12, 2025

In this page

How to search: Basic and Advanced

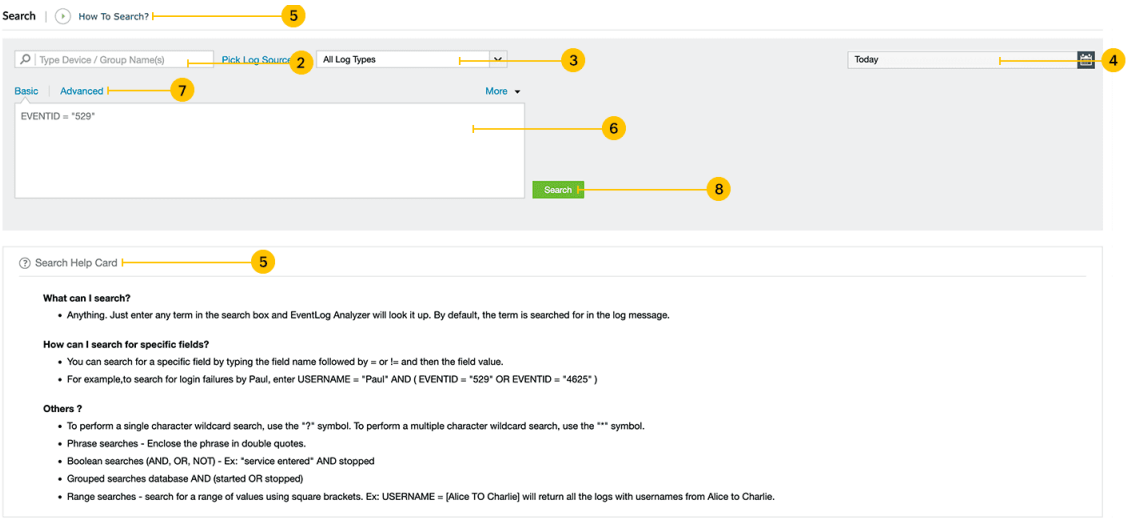
Types of basic search queries

Elasticsearch - Unarchive status

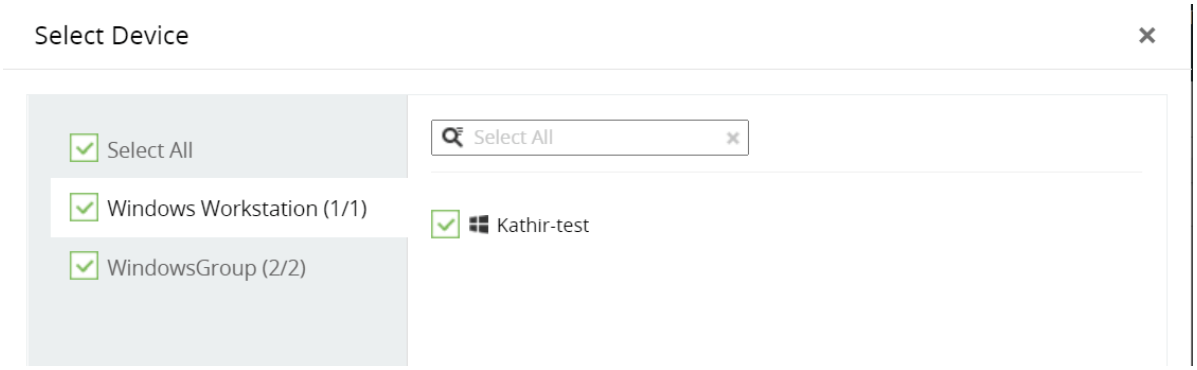
EventLog Analyzer provides a robust search engine to help you retrive log data during investigations. You can search raw logs collected by the server and detect events of interest such as misconfigurations, viruses, unauthorized access, unusual logons, applications errors, and more.
EventLog Analyzer provides basic and advanced search functionalities. Types of search queries supported are wild-card, phrase, boolean, grouped searches.

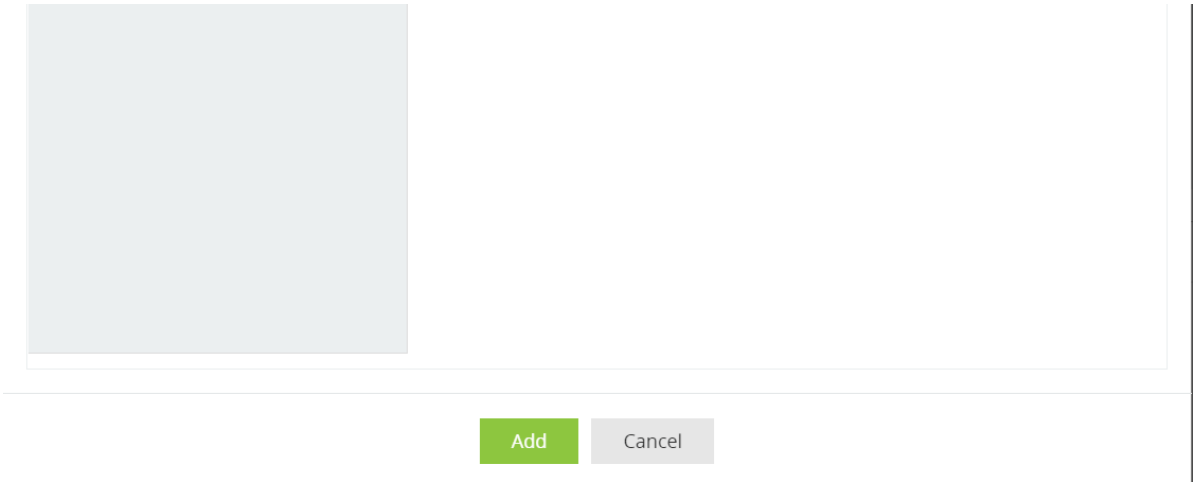
How to search: Basic and Advanced

1. Go to the Search tab.

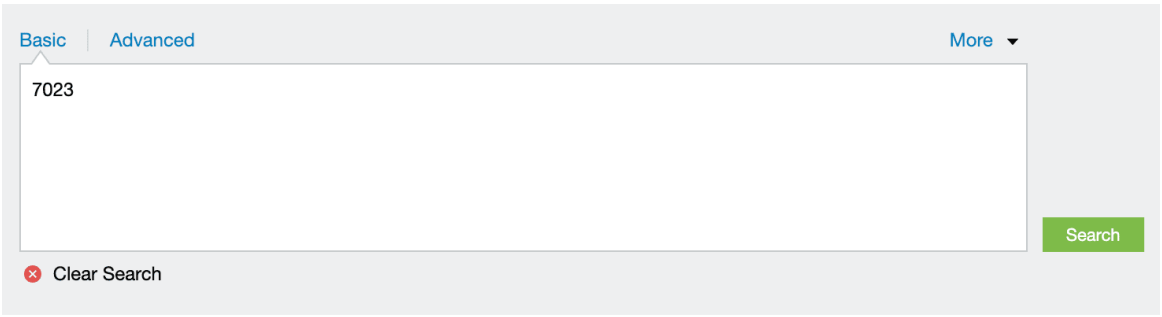


2. Click Pick device and select the devices across which you want to search. Click Add. If nothing is specified in this field, log search will be carried out across all available devices.

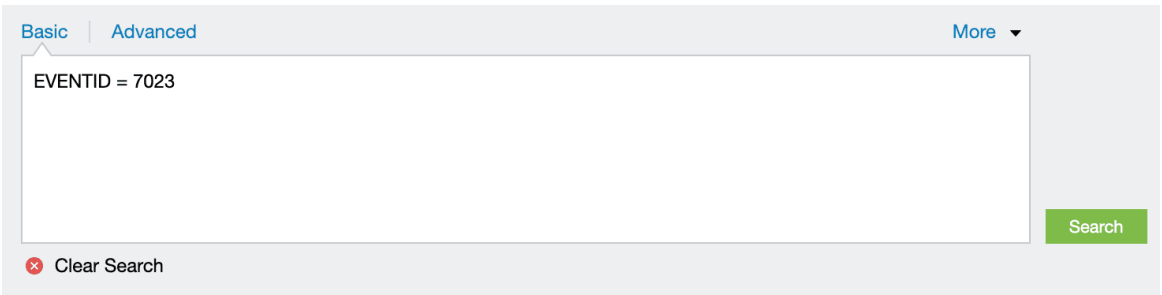




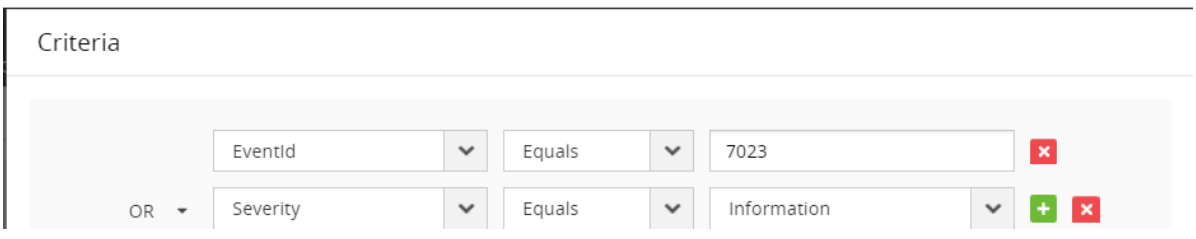
3. Select log type from the drop-down box. By default the selection is All Log Types, and the search is carried out across all log types.
4. Select the period as required.
5. Search Help Card is a built-in guide that lists the types of search queries you can perform in the search box. You can also watch how to search tutorials.
6. Use Basic search to enter your own search string/search criteria.
   - Type the field value into the Search box.

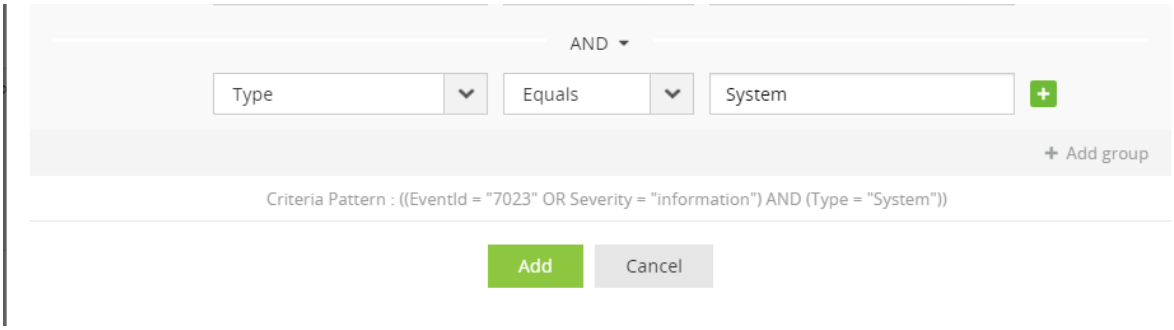


   - Type the field name and value into the Search box.



7. To build complex search expressions with the interactive search builder, click Advanced.





- Specify field values for your search criteria.
- Click '+' to add a field. Click '□' to remove a field.
- Select logical operator 'AND' and 'OR' between the fields.
- Click Add group to construct a new set of field values.
- Click Add.

8. Click Search to see the results and result graph.

> **Note**
>
> The result graph is displayed for a period of two weeks only.

Types of basic search queries

Using boolean operators:

You can use the following boolean operators: AND, OR, NOT.
Syntax: <field name>=<field value> <boolean> <field name>=<field value>.
Example: HOSTNAME = 192.168.117.59 AND USERNAME = guest

Comparison operators:

You can use the following comparison operators: =, !=, >, <, >=, <=.
Syntax: <field name> <comparison operator> <field value>.
Example: HOSTNAME = 192.168.117.59

Wild-card characters:

You can use the following wild-card characters: ? for a single character, * for multiple characters.
Syntax: <field name> = <partial field value> <wild-card character>
Example: HOSTNAME = 192.*

Phrases:

Use double quotes ("") to specify a phrase as the field value.
Syntax: <field name> = "<partial field value>"
Example: MESSAGE = "session"

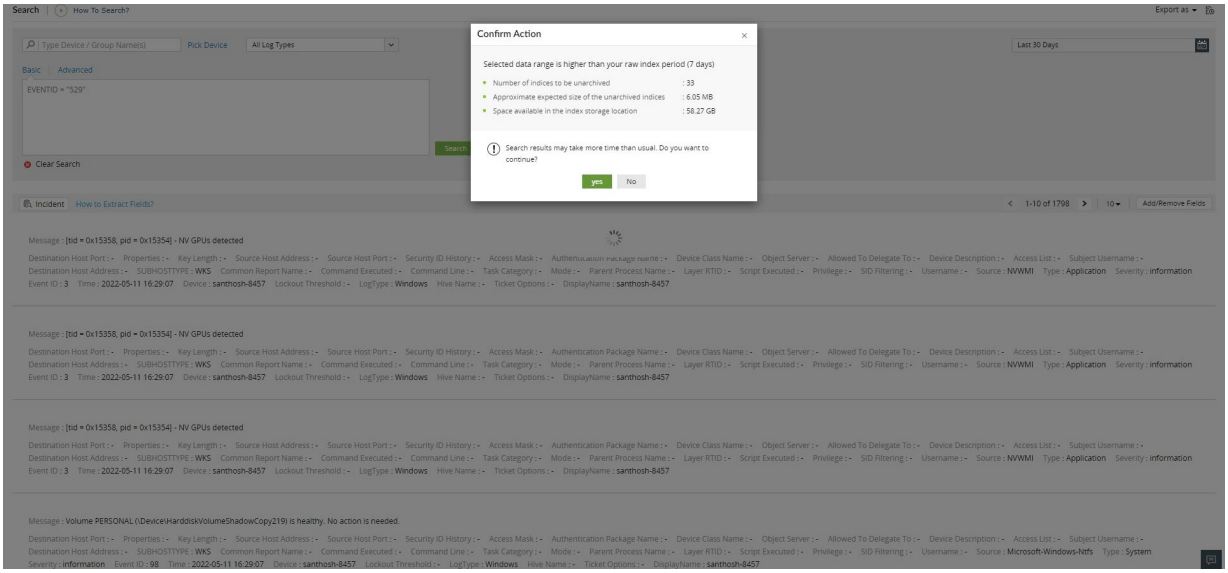
Example: MESSAGE = "session"

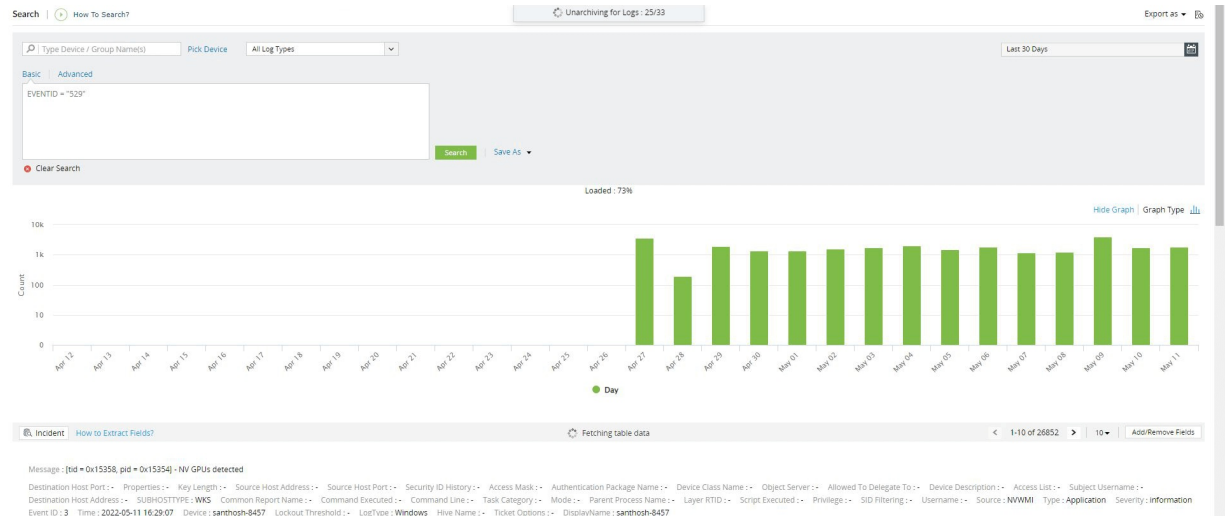
Using grouped fields:

Use round brackets () to enclose groups of search criteria and relate them to other groups or search criteria using boolean operators.
Syntax: (<search criteria group>) <boolean operator> <search criterion>
Example: (SEVERITY = debug OR FACILITY = user) and HOSTNAME = 192.168.117.59

Elasticsearch - Unarchive status

Logs stored in Eventlog Analyzer's Elasticsearch have a retention period that is customizable, and all logs beyond this period will be deleted. Apart from this, there is also an archive period beyond which, the logs will be archived and stored as a zip file. This is done to enhance memory utilization.
For example, if the archive period is set to 30 days and the retention period 90 days, logs less than 30 days old will be available for searching. And, logs older than 30 days but less than 90 days will be archived.
To search for logs beyond the archive period (30 days in this case), these archived logs need to be unarchived first before they can be made available for searching. This process takes some time depending on the log size. The log data will be available as and when a zip file gets unarchived.







Note

1. When logs beyond the archive period are being searched, a prompt is displayed with the following details:
   Free space, Expected unarchive size, Number of zip, and whether the user wants to proceed with unarchiving or cancel the option and return to normal search.
2. This flow for unarchiving logs is the same for all the other tabs of EventLog Analyzer such as Dashboard, Reports, Compliance, Correlation, and Alerts.

8.5.2. Custom Log Parser

Last updated on: September 12, 2025

In this page

How to extract additional fields using EventLog Analyzer?

Specifying custom field values

Regex method

Adding prefix and suffix

Validating the pattern

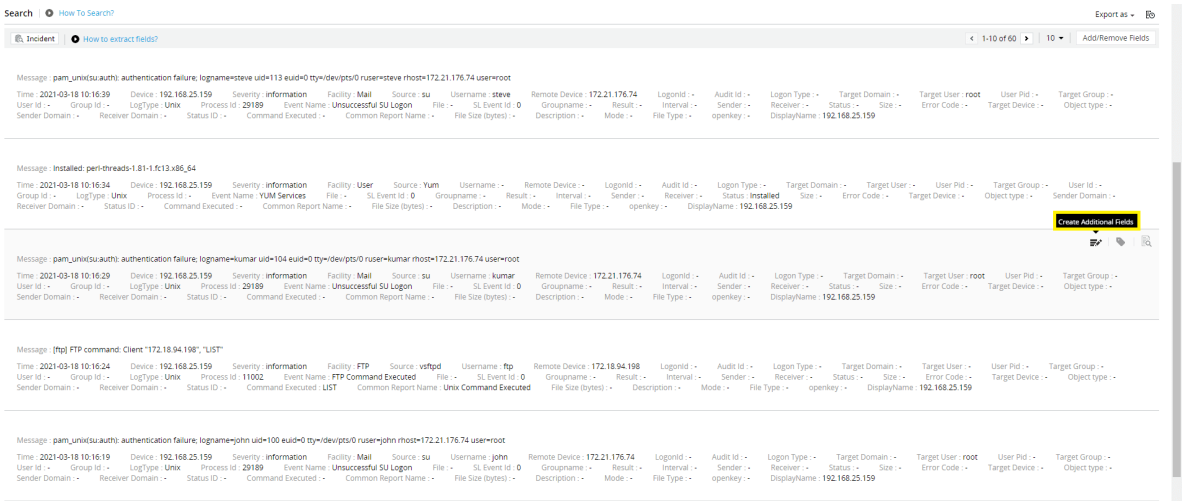
Delimiter method

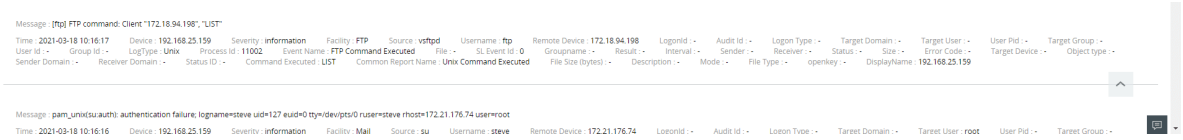
Network administrators are always in need of more information and insights from their log data. There are times when an IT administrator would identify some log information which is useful and would like to have it indexed automatically as a new field. Having more fields being indexed makes your log data more useful while conducting log forensics analysis and creating network security reports.
EventLog Analyzer allows administrators to create custom (new) fields or extract fields from raw logs by using the interactive Field Extraction UI to create regular expression (RegEx) patterns to help EventLog Analyzer to identify, parse and index these custom fields from new logs it receives from network systems and applications.

How to extract additional fields using EventLog Analyzer?

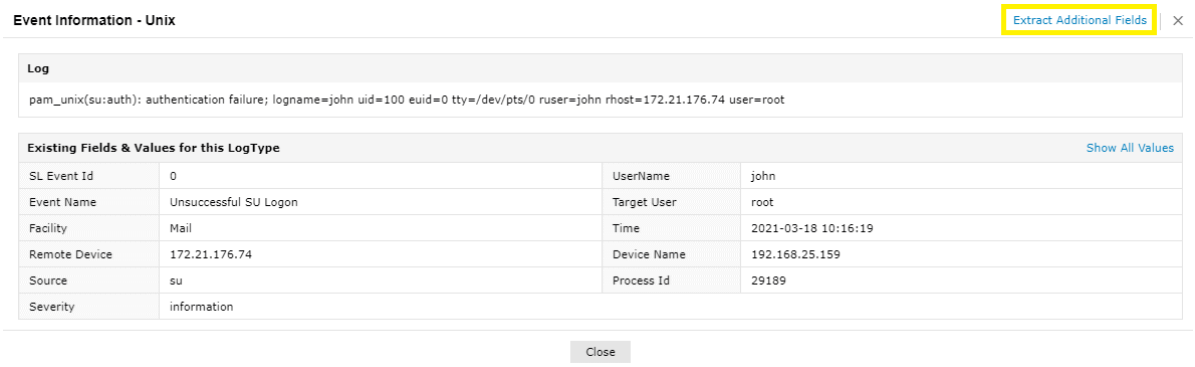
- Navigate to the Search tab and search for the logs from which fields need to be extracted. Click Create Additional Fields to view and extract fields.

> **Note**
>
> Alternatively, you can also extract additional fields while importing the log file.





- You can view the extracted field details in the Event Information window. If the required value is not parsed, you can extract further fields by clicking the Extract Additional Fields.



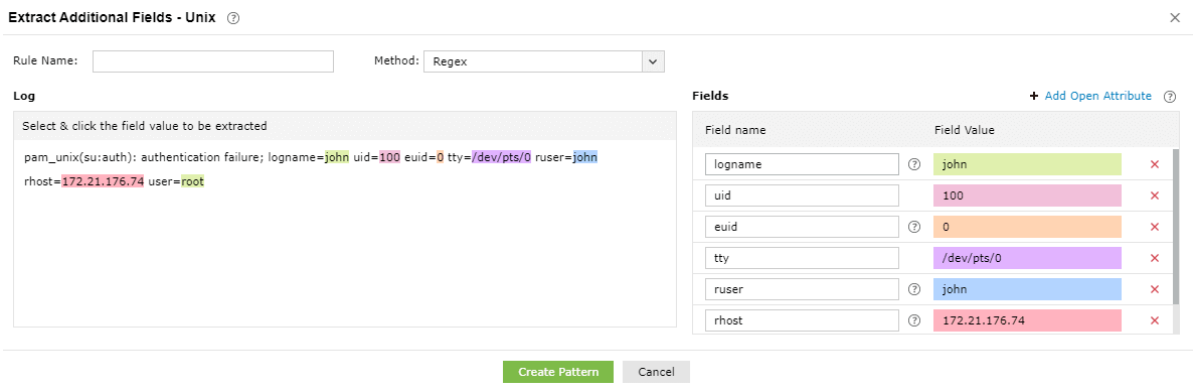
Specifying custom field values

There are two methods by which custom fields can be specified viz.

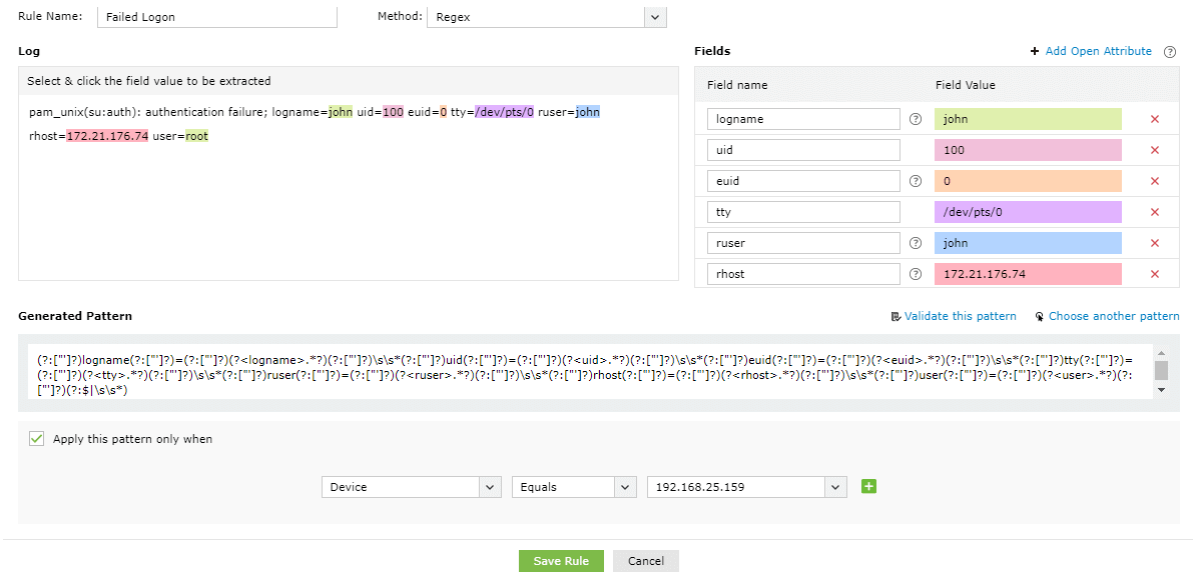
- Regex method
- Delimiter method

Regex method

- Provide a rule name.
- Select and click the word(s) in the message, to be extracted as a field.
- You can use the Auto Identify option to identify the fields automatically.



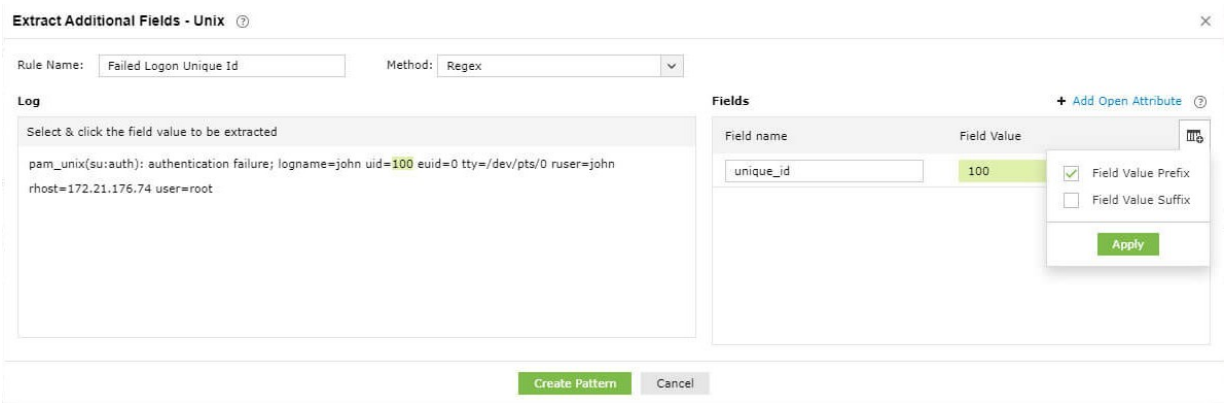
- Provide a name for this field. Optionally, specify the prefix and suffix to the field value.
- Click on Create Pattern to generate a parser rule pattern.



Adding prefix and suffix

- You can also include the prefix and/or suffix of a field value to improve precision. To include a prefix and/or suffix, click on the icon in the right corner of the Fields table and select the required option. Click Apply.
- For instance, consider the message : Successful Network Logon: User Name: sylvian Domain: ADVENTNET Logon ID: (0x0,0x6D51131) Logon Type: 3 Logon Process: NtLmSsp Authentication Package: NTLM Workstation Name: SYLVIAN Logon GUID: - Caller User Name: - Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address: 192.168.113.97 Source Port: 0 22873
- The prefix Logon Type can be a static value as most of the logs will have the exact word as Logon Type where as Source Network Address can be dynamic as the logs may have different word(s) like, Source IP Address, Source Address, but with the same pattern.
- If the prefix and suffix are defined with exact match, the field extraction will be precise.

  Note: An open attribute will not have a prefix or suffix.



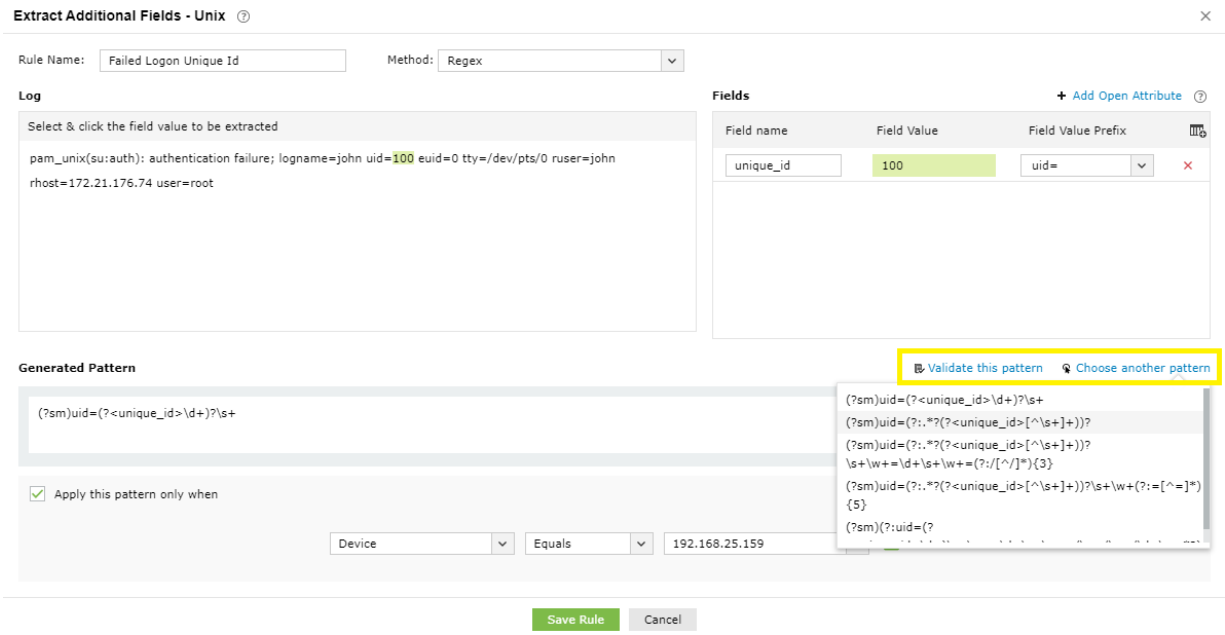
Validating the pattern

A parser rule pattern is created using the field definition. You can edit the generated pattern manually, if you are

A parser rule pattern is created using the field definition. You can edit the generated pattern manually, if you are familiar with regular expressions.

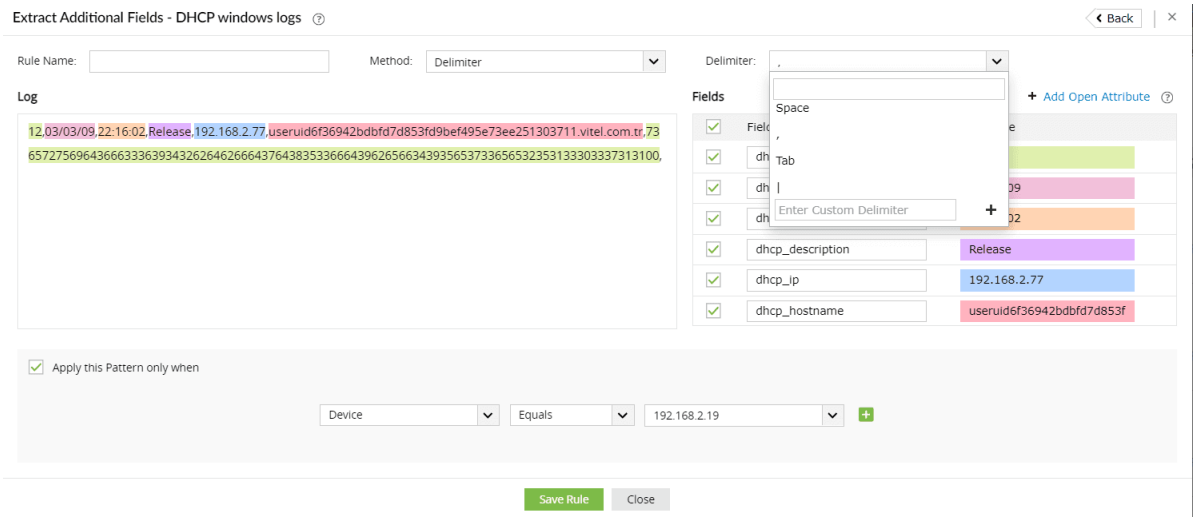
Validate link is used to test the generated pattern against the previous search results. You can manually check the suitability of the pattern by analyzing the 'Matched Log Messages' and 'Unmatched Log Messages' displayed.

- Click on Choose another pattern to choose a pattern from the list of patterns generated by the application.
- You can define any existing field matching criteria to apply the pattern for this specific log type.
- Save the pattern to extract the field(s) from the upcoming logs.



Delimiter method

- Provide a rule name.
- You can use the Delimiter to extract fields using delimiters such as Space, Comma, Tab, or Pipe.



- To save the created rule, click Save rule.

8.5.3. Saving search and exporting search results

Last updated on: September 12, 2025

In this page

How to save search?

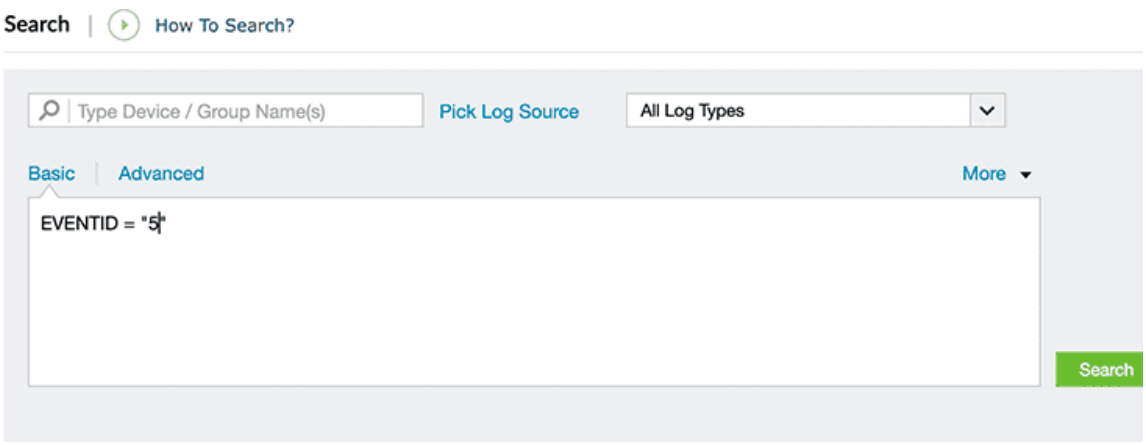
How to export search?

Enhancements

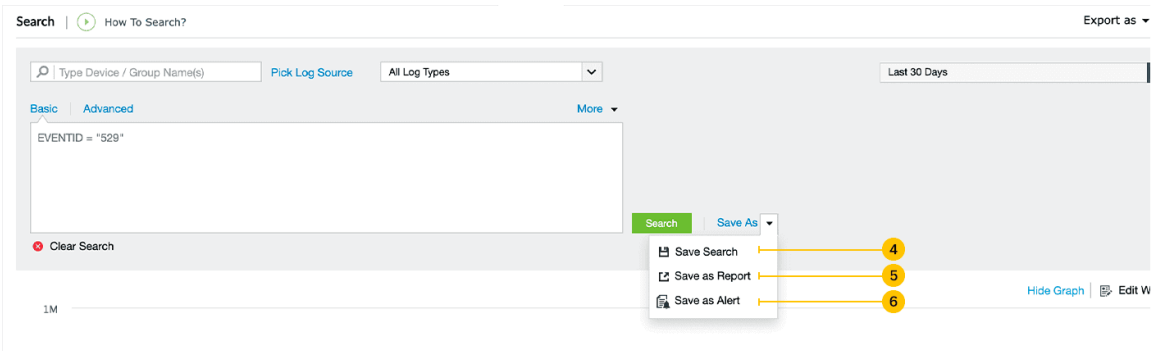
EventLog Analyzer drills down to the raw logs when retrieving results for your search query. The results can be saved, or used to create report and alert profiles.

How to save search?

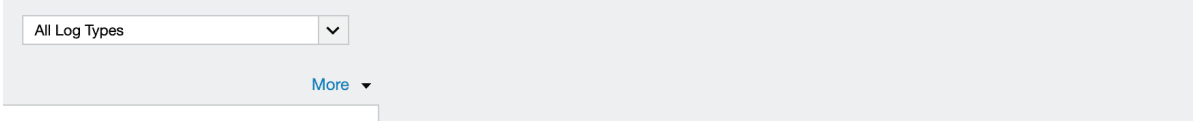
1. Go to the Search tab and enter the search criteria as required (see how to search).
2. Click Search for the results.

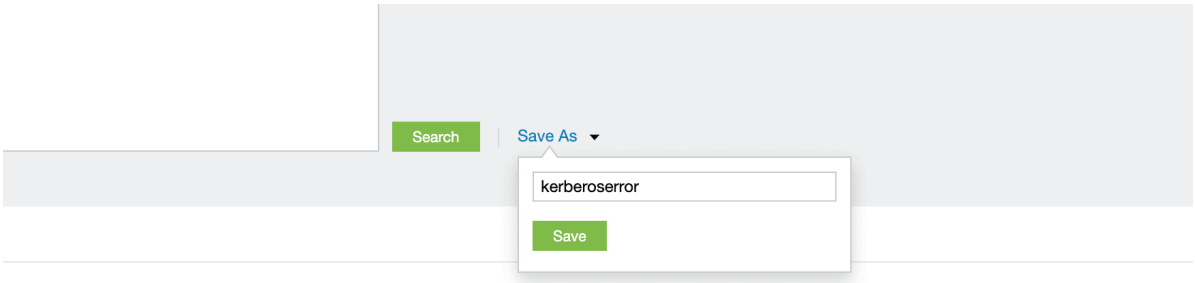


3. You can save the search criteria as search, reports or alerts.

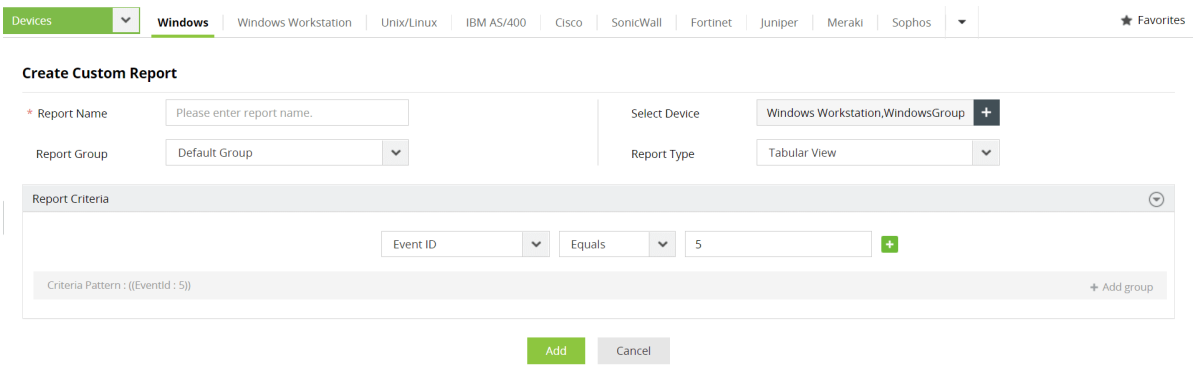


4. To save as search, click Save Search. Enter a name without space. Click Save.





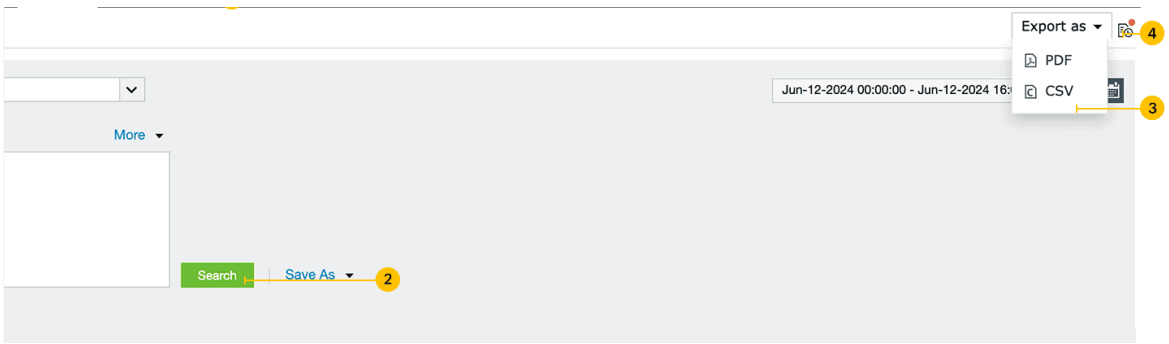
5. To save as report, click Save as Report. Enter Report name and click Add (see create reports).



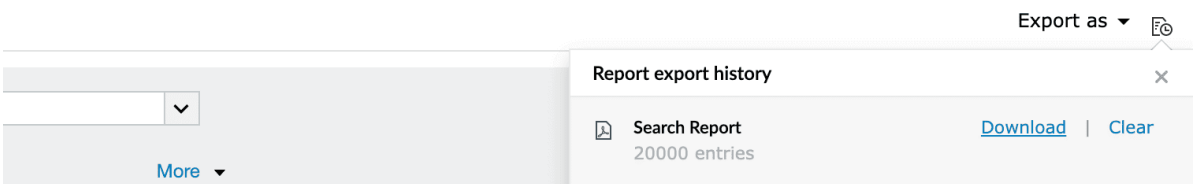
6. To save as an alert, click Save as Alert. In the window that opens, click Save (see Create alert profile).

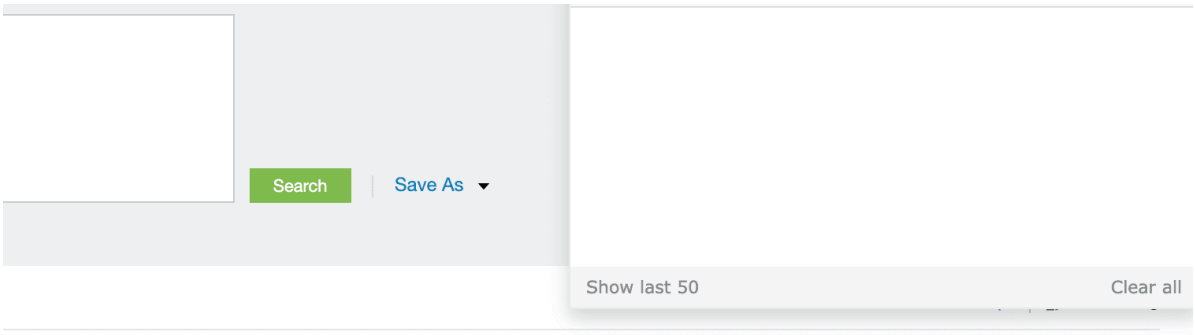
How to export search?

1. Go to Search and enter the search criteria.
2. Click Search.



3. Click Export as on the top-right corner. Select the format.
4. View the report export history by clicking on the icon, which can then be downloaded if required.

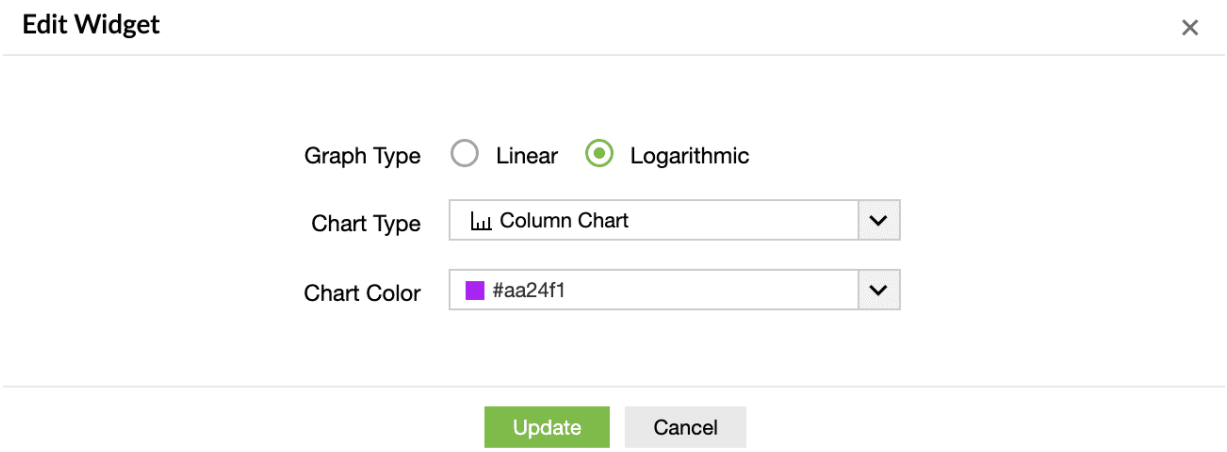




Enhancements

Edit graph:

After clicking on Edit Widget, you can choose Graph Type, Chart Type, and Graph Color, and the changes will be reflected accordingly.

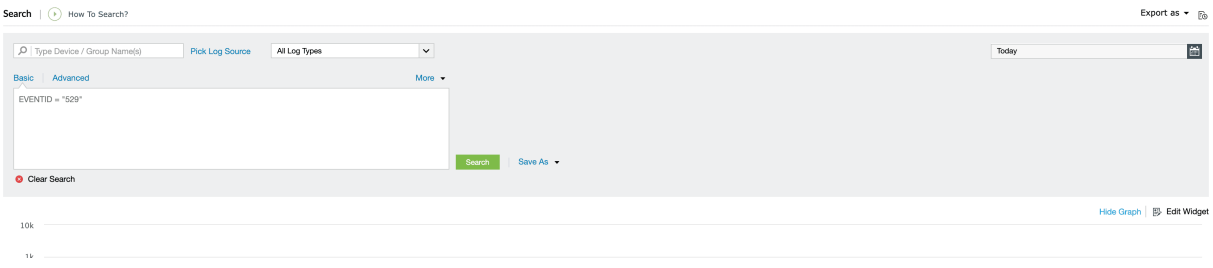


Graph drill down:

To drill down to a specific time range, simply click on a point on the graph. When you do this, the calendar will automatically adjust to display the corresponding time period. Both the table and the graph will also dynamically update to reflect the selected time range.

Graph selection:

When you choose a specific section of the graph by dragging the cursor, the table will automatically adjust to show data within that time range, and the graph will be highlighted according to its chart type. You'll also notice an option to clear the selection becomes available. It's important to note that in this case, the chosen time range will not be updated in the calendar.





As you drag your cursor over a specific area of the graph, that portion will be highlighted, and the logs within that time range will be displayed.

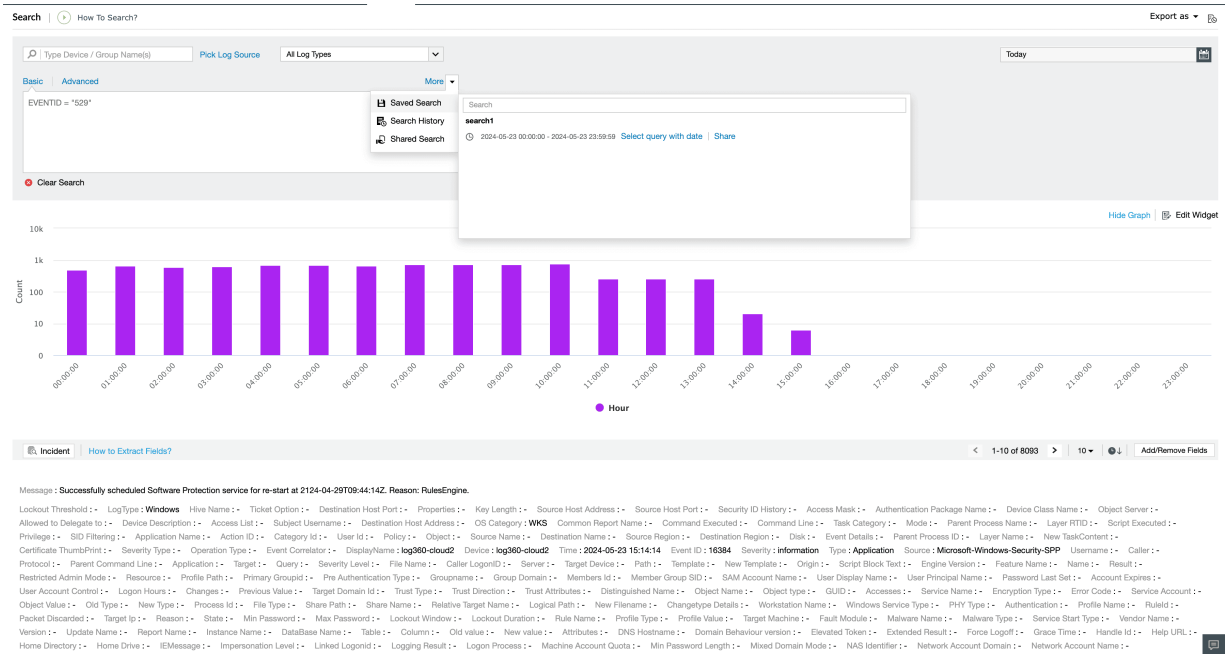
How to use Saved Search

After your search parameters have been successfully saved, if you ever need to reuse the same parameters for a future search, simply follow these steps:

- Click on More to reveal a drop-down menu.
- Select Saved Search.
- Pick the saved search containing the desired parameters.

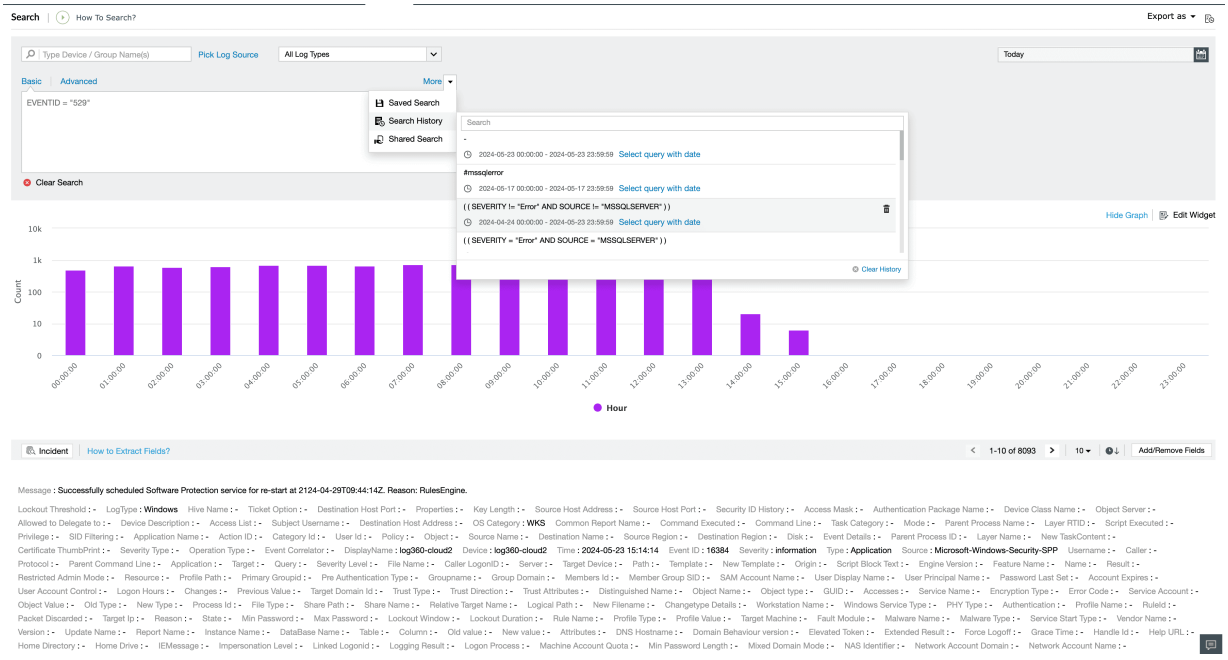
If you require an exact time range, you can utilize the Select query with date option.

> **Note**
>
> Under Saved Search, a maximum of 20 searches can be saved.



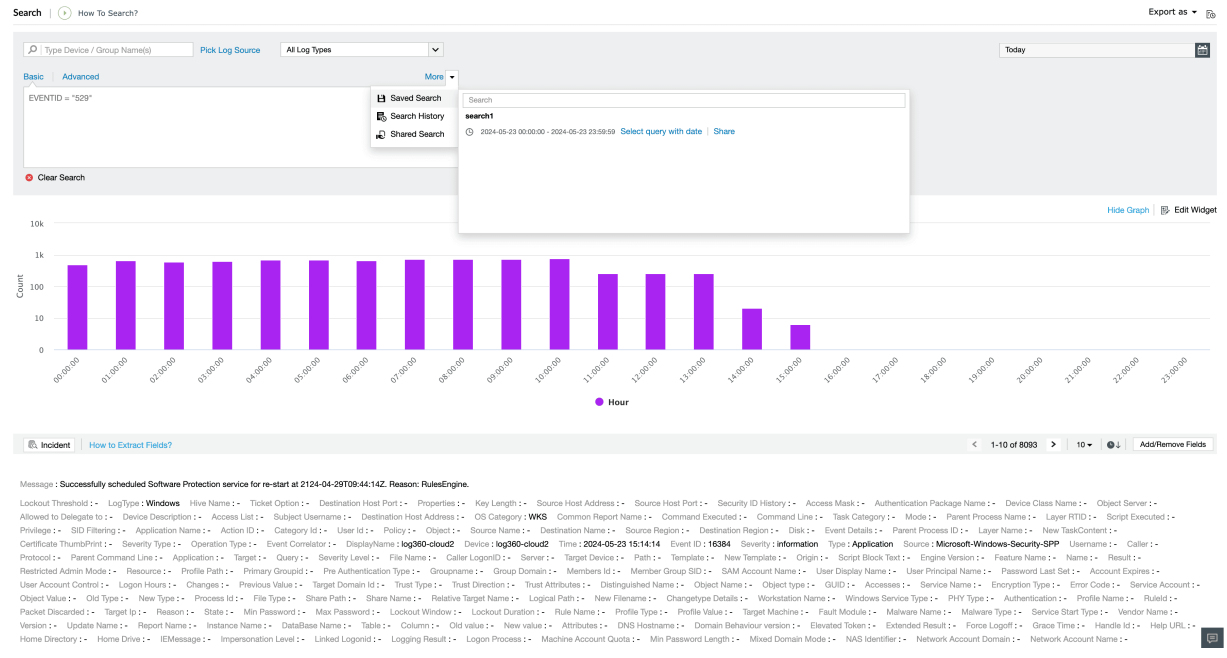
Search History:

Search requests will be saved in your browser's local storage and displayed as a Search History list. This list can contain up to 50 entries. When the limit is reached, older entries will be deleted to accommodate new ones. If you perform a search with the same criteria as an existing entry in the search history, the new query will replace the previous one.



Share search:

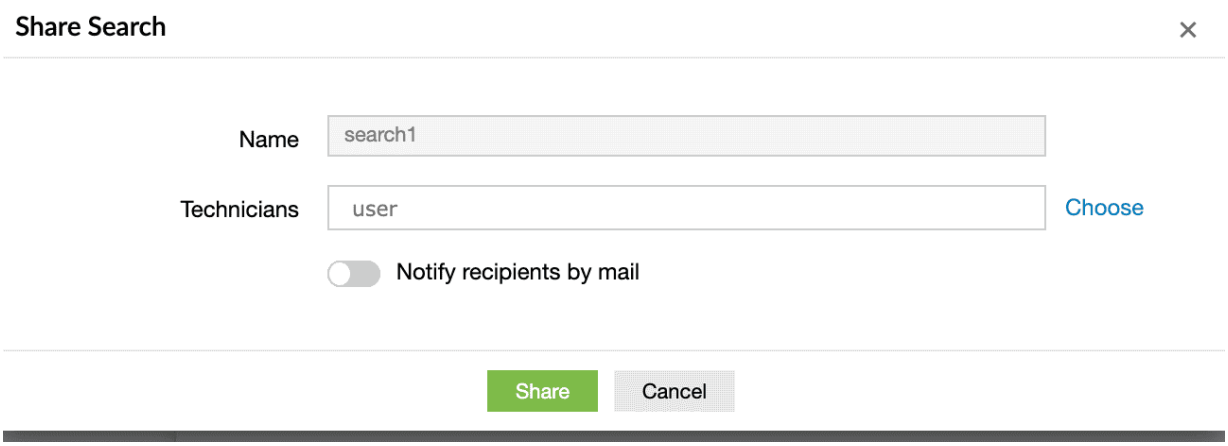
You can share saved searches with other technicians within your organization. When you share a saved search, all the associated data will be accessible to the shared user.



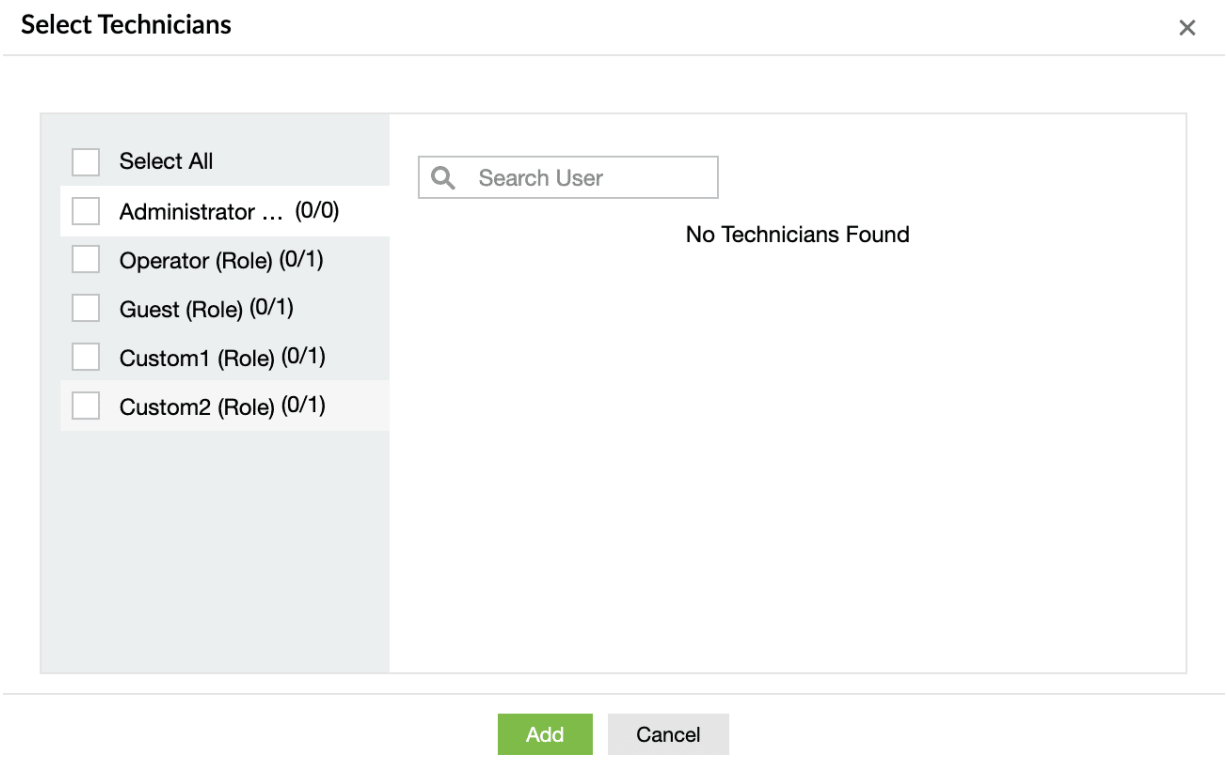
To share a search with other technicians, select the Saved Search option from the More dropdown menu and then click Share.

Note

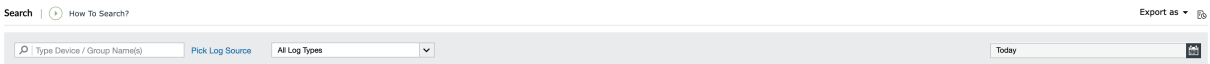
When a search is shared to a role, they won't have the ability to delete the shared search. The same applies for the guest users too.

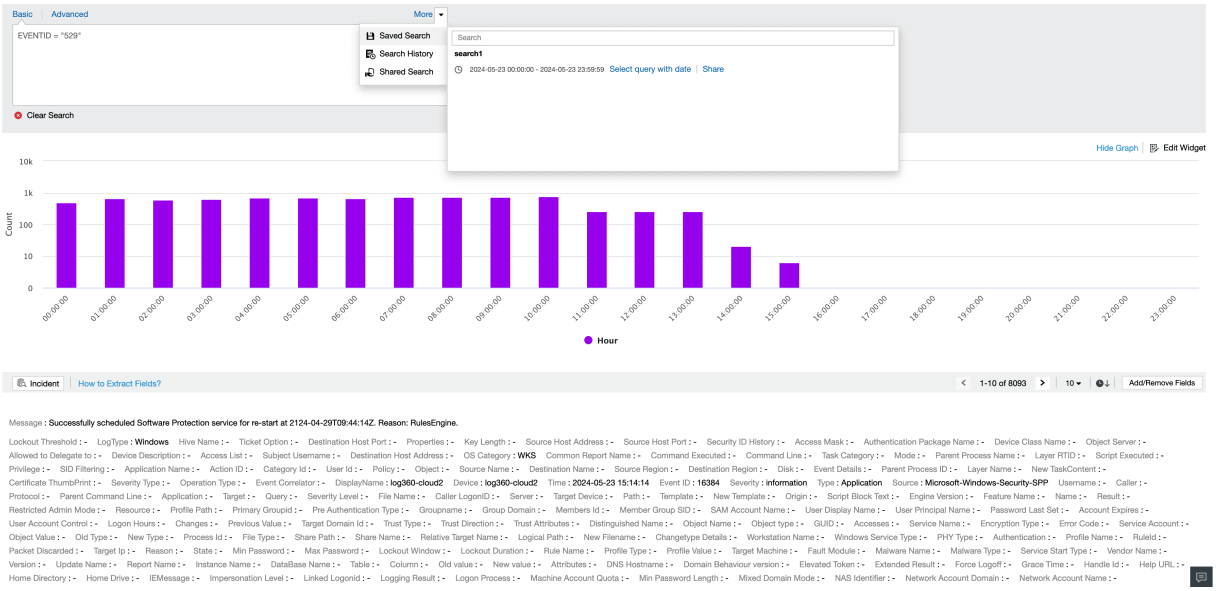


After clicking the Share option, you can select technicians to notify via email by toggling the Notify recipients via mail button.



Alternatively, you can also click on Choose, which will redirect you to the following page where all the technician names along with their role can be seen.





After sharing a search, you can modify the list of technicians or withdraw the shared search from selected technicians. To make changes, select the Edit Share button. To remove all technicians, use the Revoke button.

8.5.4. Tagging tool

Last updated on: September 12, 2025

In this page

How to create a tag?

How to edit a tag

How to perform log search using a tag

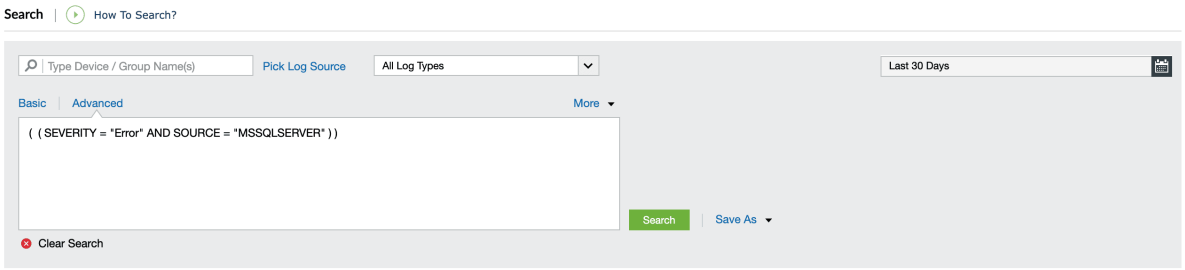
How to delete a tag

EventLog Analyzer's tagging tool bookmarks your logs and complex search queries using hashes, helping you view searches across different sources. You can also add troubleshooting tips or notes along with your tag.

How to create a tag?

To create a tag, go to Search tab and follow the below steps:

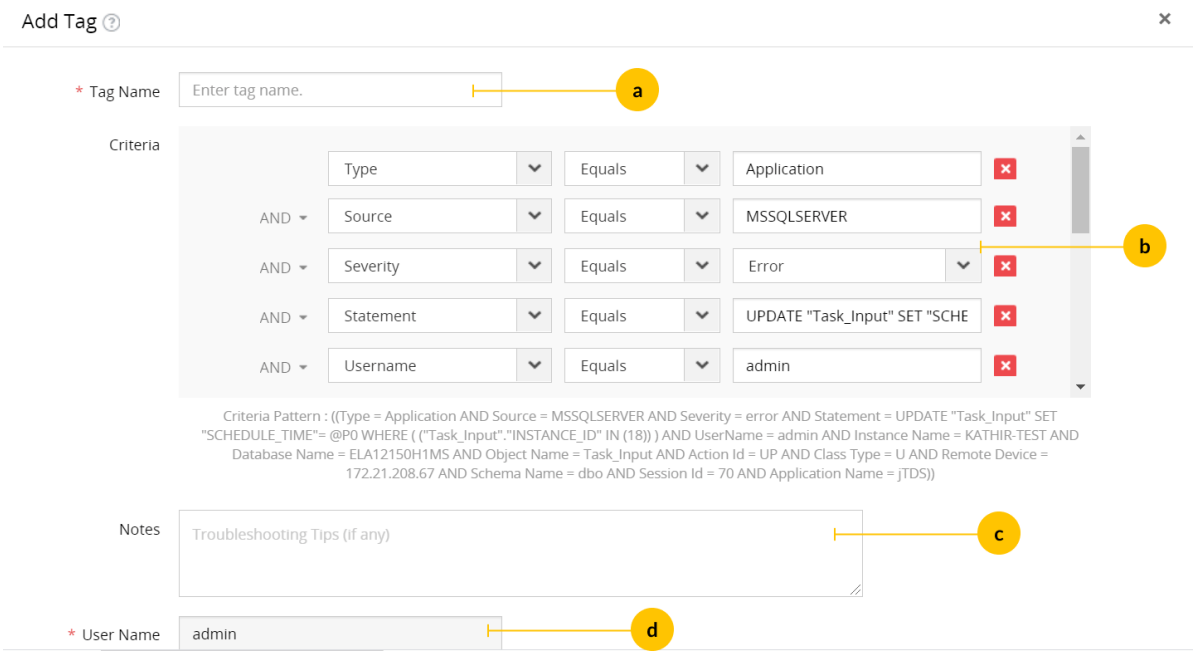
1. Specify all the search criteria which you wish to associate with your new tag and click Search.



2. Click on the tag icon on the right side of any log entry in the displayed search result.



3. Fill the required details in the Add Tag pop-up:

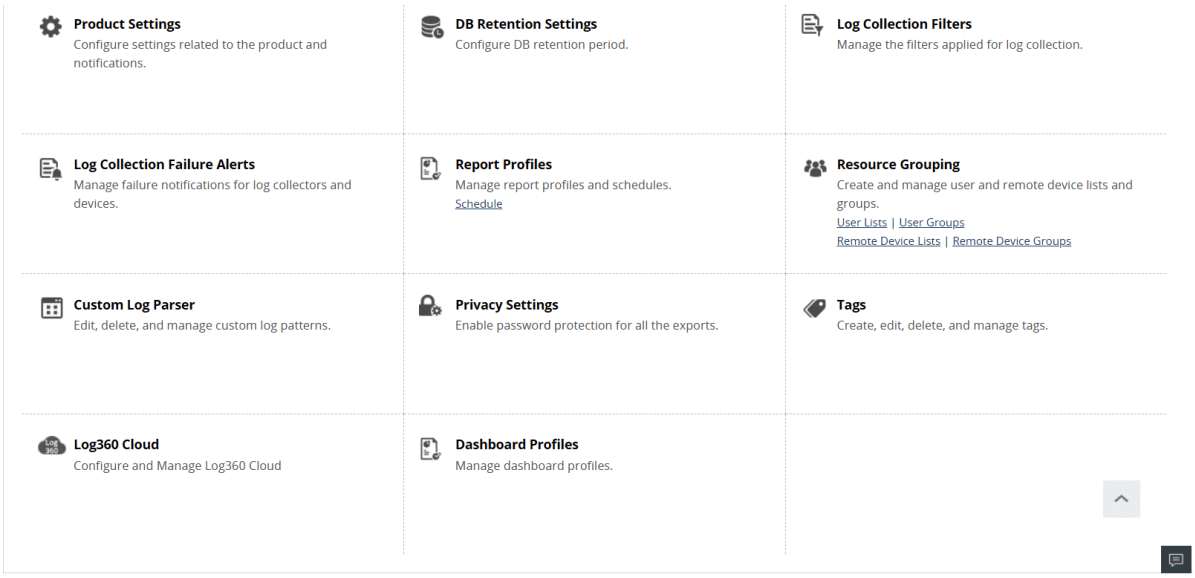


- Provide the name of the tag.
- Select the tag criteria from the predefined list. The list is based on the fields available in the search result. If it does not have the field you are looking for, then add those fields to the search results using the column selector at the top-right corner of the search results.
- Provide troubleshooting tips/notes for the tag, if any.
- Specify the user name. By default, the current user name (logged on to the EventLog Analyzer web client), is displayed.

4. Click Apply to save the tag.

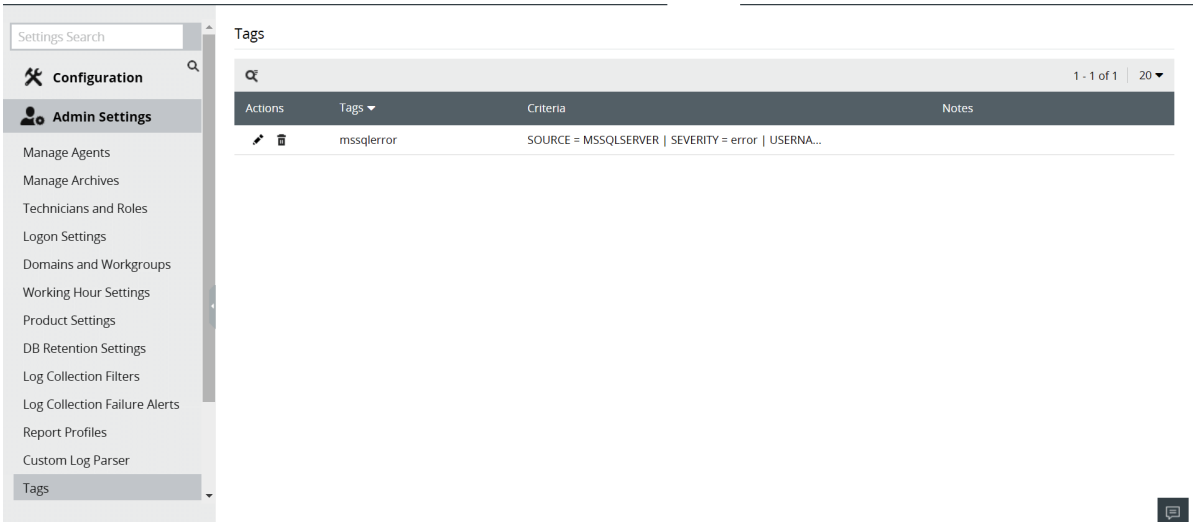
How to edit a tag

1. Navigate to Settings > Admin settings > Tags.

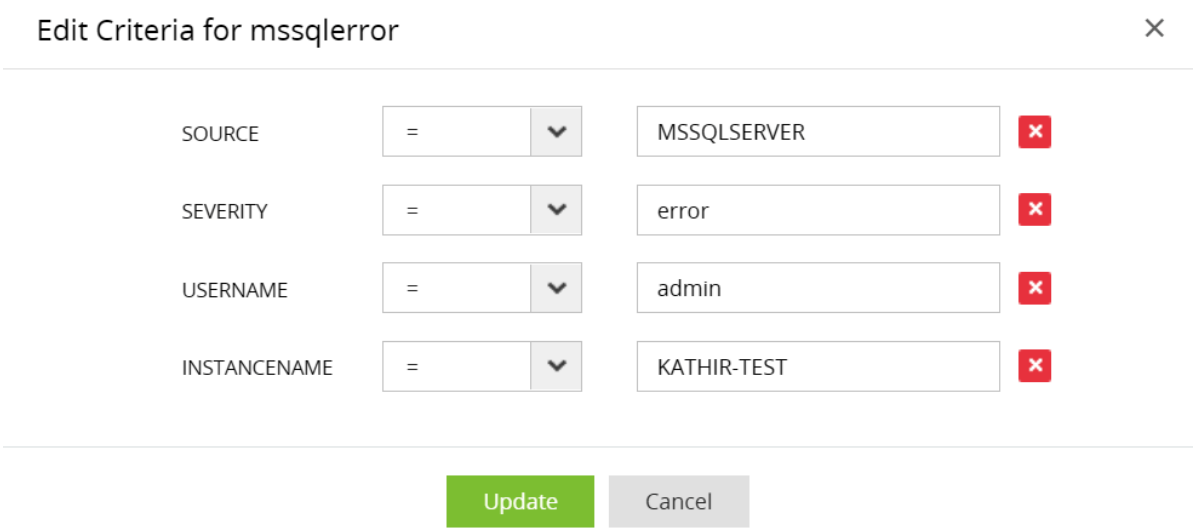


2. Click the edit icon next to the tag

2. Click the edit icon next to the tag.



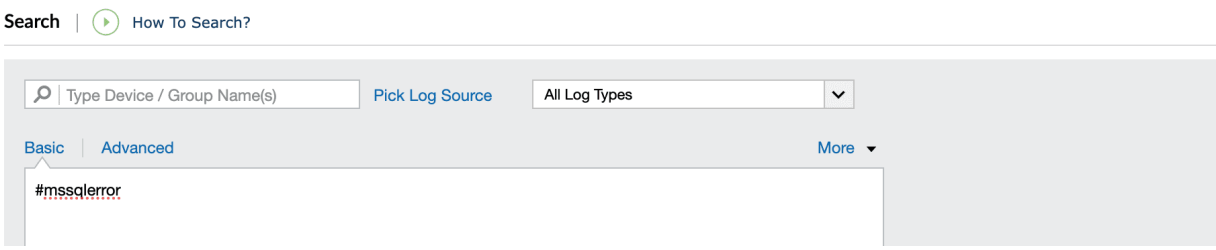
3. Modify the tag criteria.

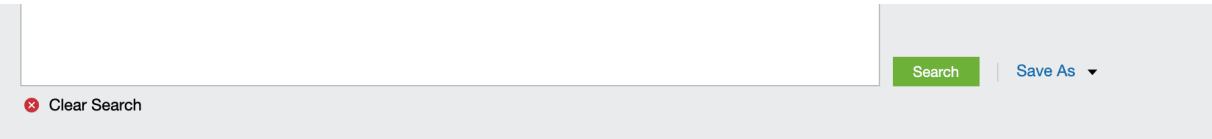


> **Note**
>
> You can also edit tags on the search results page by clicking the edit icon below the tag name.

How to perform log search using a tag

You can search for tags by their name, prefixed with #, in the search query text box.

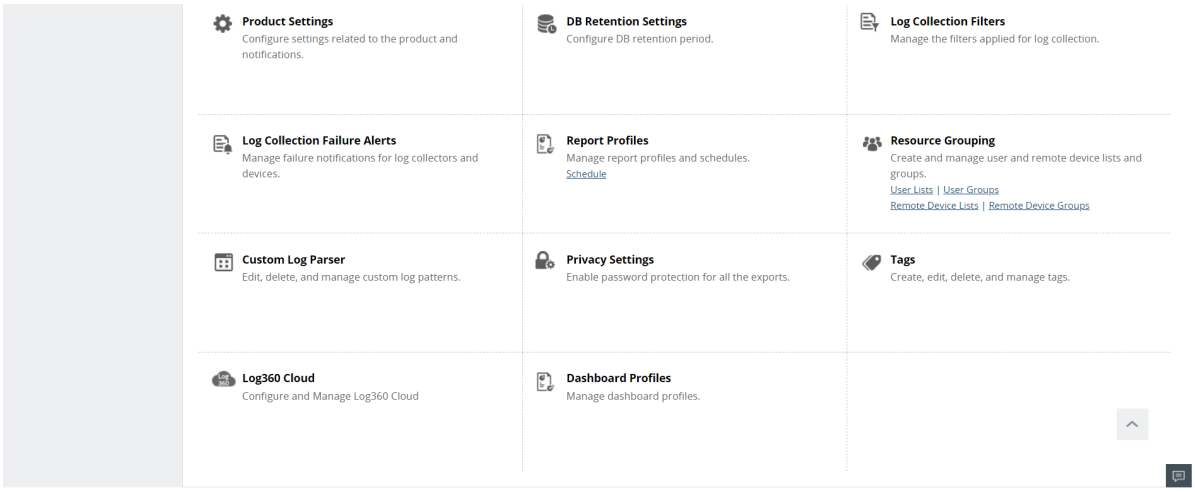




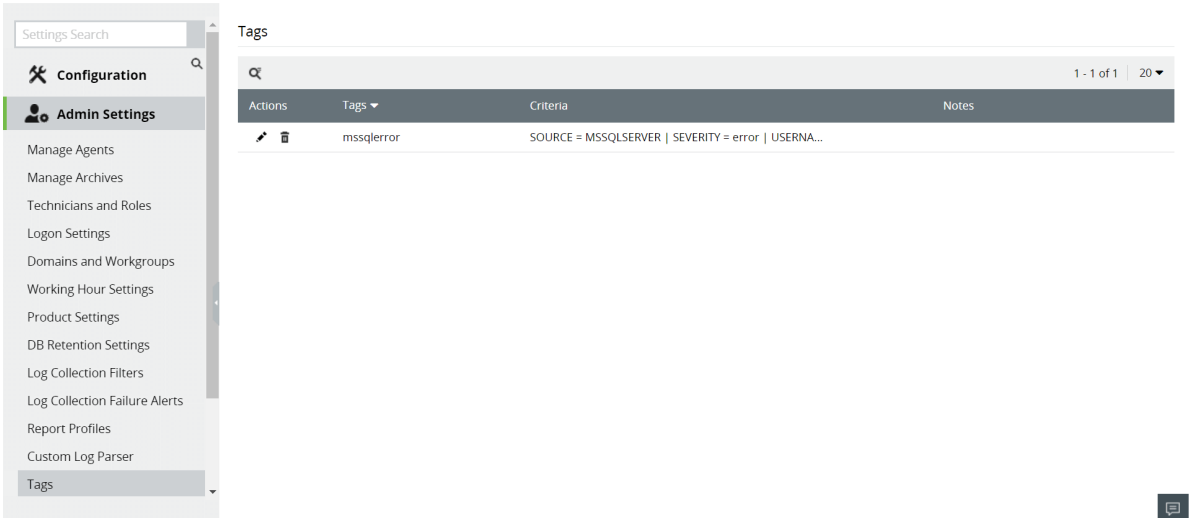
> **Note**
>
> Typing # provides you with a list of all created tags for ease of selection.

How to delete a tag

1. Navigate to Settings > Admin settings > Tags.



2. Click on the delete icon beside the tag name in the tag table. Click Yes in the pop-up.



> - The tag name and the notes added to the tag should contain only alphanumeric characters.
> - Tag criteria can be edited only by the user who created the tag and EventLog Analyzer users with

Administrative privilege.

- Any user of EventLog Analyzer can add a note to a tag, irrespective of the creator of the tag.

8.6.1. Alerts overview

Last updated on: September 12, 2025

In this page

Overview

Event alerts

Core capabilities

Remediation and response integration

Working architecture

Use cases

Overview

This page elaborates on how alerts notify you about security events, compliance issues, and critical file changes in real time. you can create predefined or custom alert profiles, set severity levels, and receive notifications. alerts can also trigger automated actions through playbooks for faster response.

Event alerts

Stay informed about critical security events through real-time alerting. The system analyzes audit logs for indicators of compromise (IoCs) and notifies you via SMS or email when necessary.
Alerts are classified into three severity levels as attention, trouble, and critical, helping you prioritize and respond efficiently.

Core capabilities

- Real-time security alerts, including those from imported logs
- Compliance-specific alerts for regulatory monitoring
- File integrity monitoring (FIM) alerts to flag critical changes in sensitive files or folders
- Predefined & custom alert profiles

Choose from over 1,000 predefined alerting criteria to cover a wide range of threat scenarios. You can also build custom alert profiles tailored to your organization’s needs, applying parameters like thresholds and time ranges for precise control.

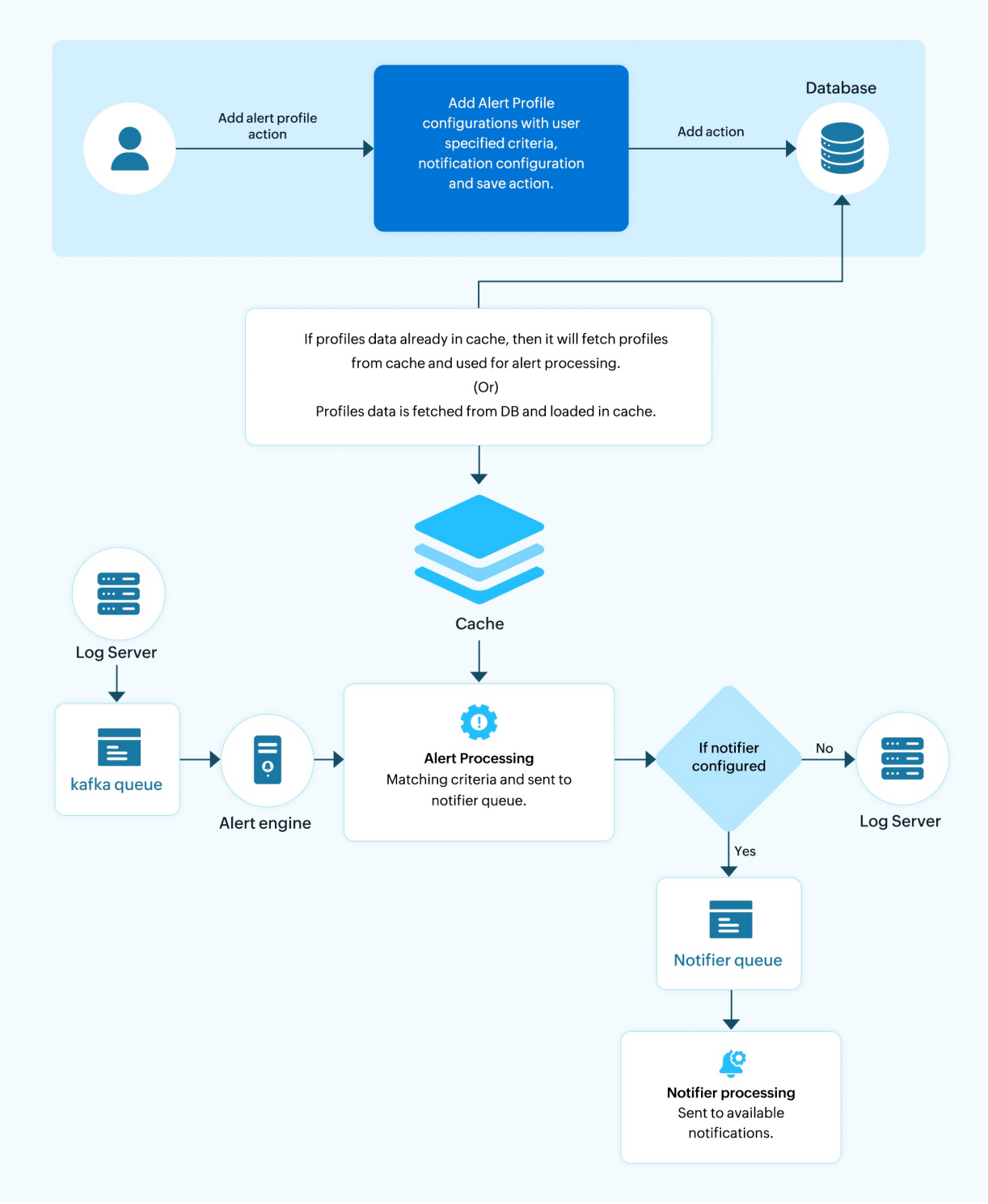
Remediation and response integration

- When an alert is triggered, you can handle incidents directly within the console or escalate them through

external ticketing tools for enhanced accountability.

- For a faster, automated response, you can assign a playbook to instantly perform actions such as disabling compromised accounts, shutting down a system, or terminating suspicious processes.
- View all triggered alerts under the alerts tab in the interface.

Working architecture



Use cases

1. Securing sensitive configuration files

Use case A finance department configuration file containing critical transaction settings is modified after hours, raising suspicion of tampering.
With alerts A FIM (File Integrity Monitoring) alert triggers immediately. The playbook supports rapid response by executing actions such as restoring the last clean version of the file, logging the incident, and notifying the security team by minimizing risk and preserving system integrity.

2. Detecting unauthorized login patterns

Use caseA series of failed login attempts from an employee’s account over a short period suggests possible credential misuse.
With alertsA security alert is generated in real time. The response system escalates the incident via a ticketing tool and optionally executes a playbook that temporarily locks the account and notifies administrators, containing potential damage while ensuring a speedy investigation.

Read also

This page outlined how alerts can enhance your organization's threat detection and remediation measures. Read more about creating alert profiles, configuring notifications, and monitoring events to strengthen security and compliance.

- Create Alert Profile
- Manage alert Profiles
- Alert Notification & Remediation

8.6.2. Create alert profiles

Last updated on: September 12, 2025

In this page

Overview

Configuring alert profiles

Creating an alert profile

Overview

This page explains how to create and manage alert profiles. it covers setting predefined or custom criteria, choosing log sources, defining severity levels, and configuring notifications. you can also enable playbooks to automate actions for faster incident response.

Configuring alert profiles

1. In the product dashboard, navigate to the Alerts tab as highlighted in the below image.

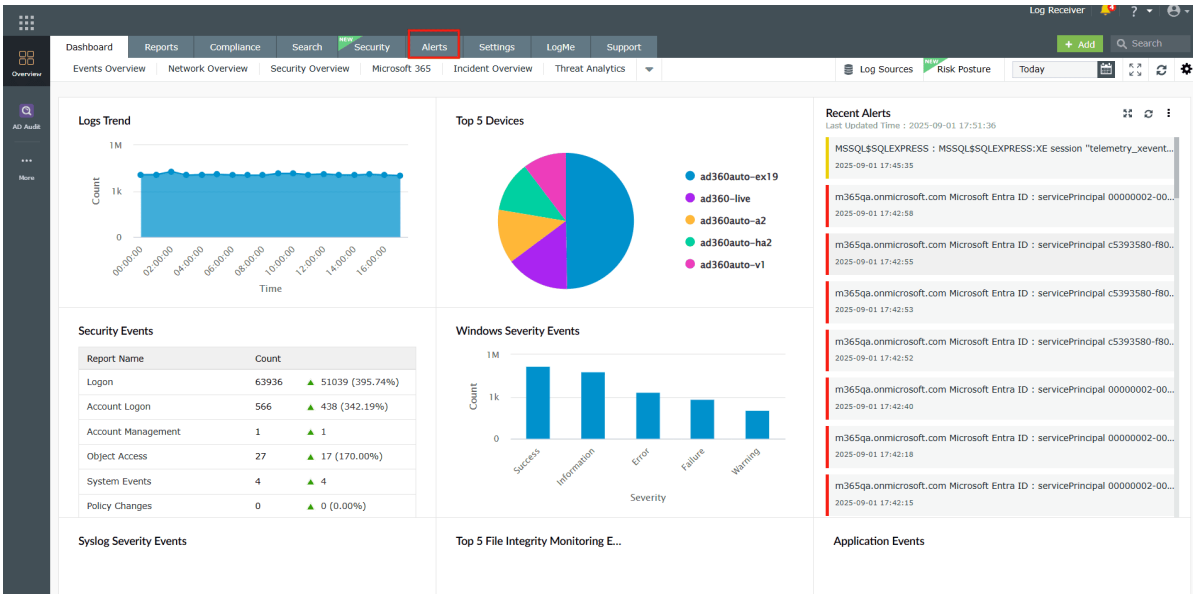
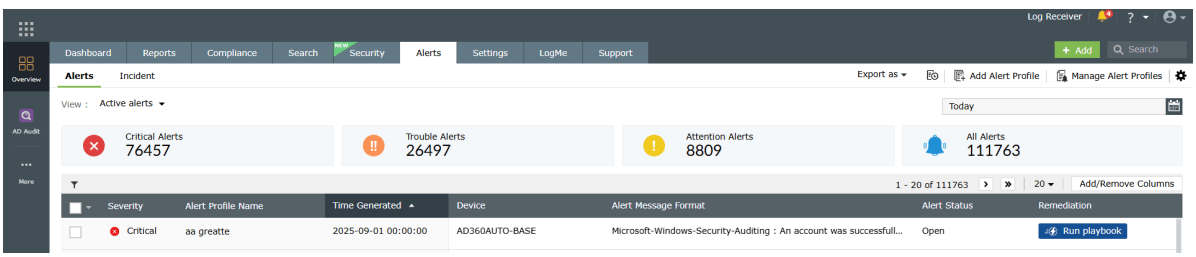


Image 1: Alerts tab in the dashboard

2. You will be taken to the Alerts module.



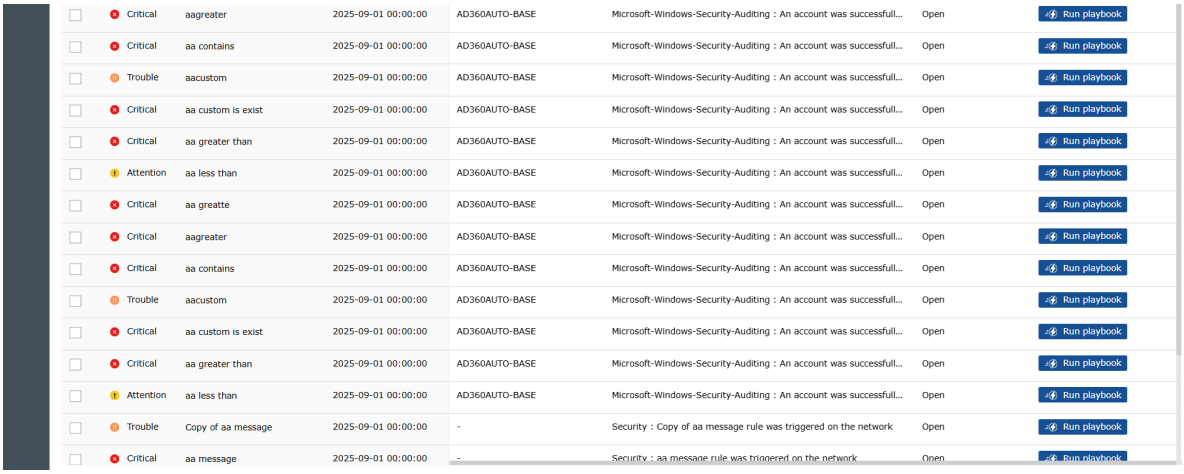


Image 2: Alerts module via the dashboard

From this module, you can create, manage, and configure alert profiles

Creating an alert profile

You can choose from the available predefined alert profiles and the also define customized criteria for specific requirements.

Steps to create an alert profile

1. In the product console, navigate to the Alerts tab and click on the Add Alert Profile button at the top-right corner of the page as highlighted in the below image.

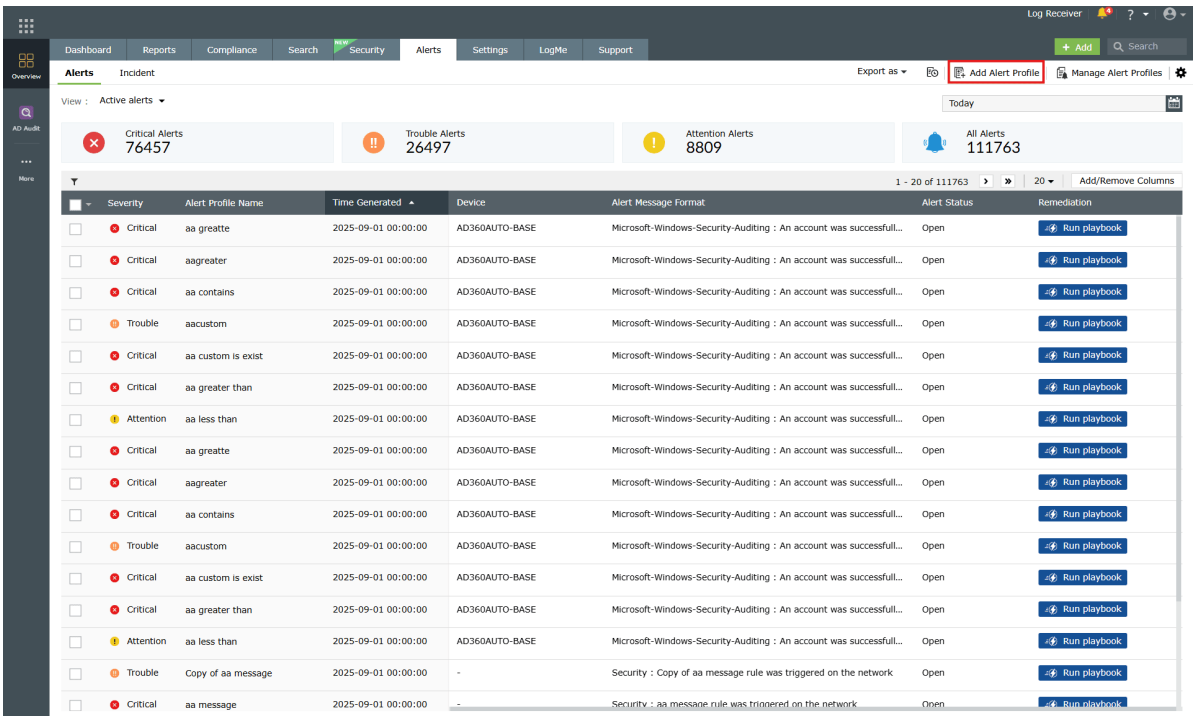


Image 3: Add Alert Profile button in the Alerts tab

2. The Add Alert Profile page opens. Enter a unique name for the alert profile in the Name field.

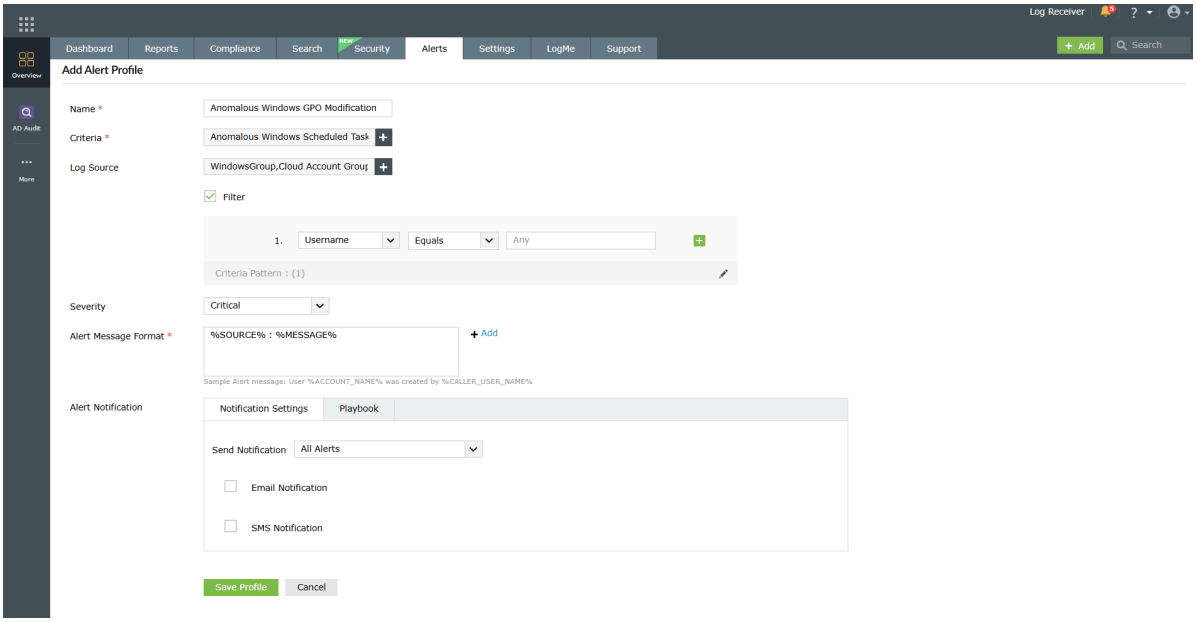


Image 4: Add alert profile module

3. In the Criteria field, click on the + icon to define the alert conditions. This opens the Alert Criteria Builder window. There are 4 sub-tabs available in the Alert Criteria Builder:
   - Predefined Alert Criteria
   - Rules
   - Compliance Alert Criteria
   - Custom Alert Criteria

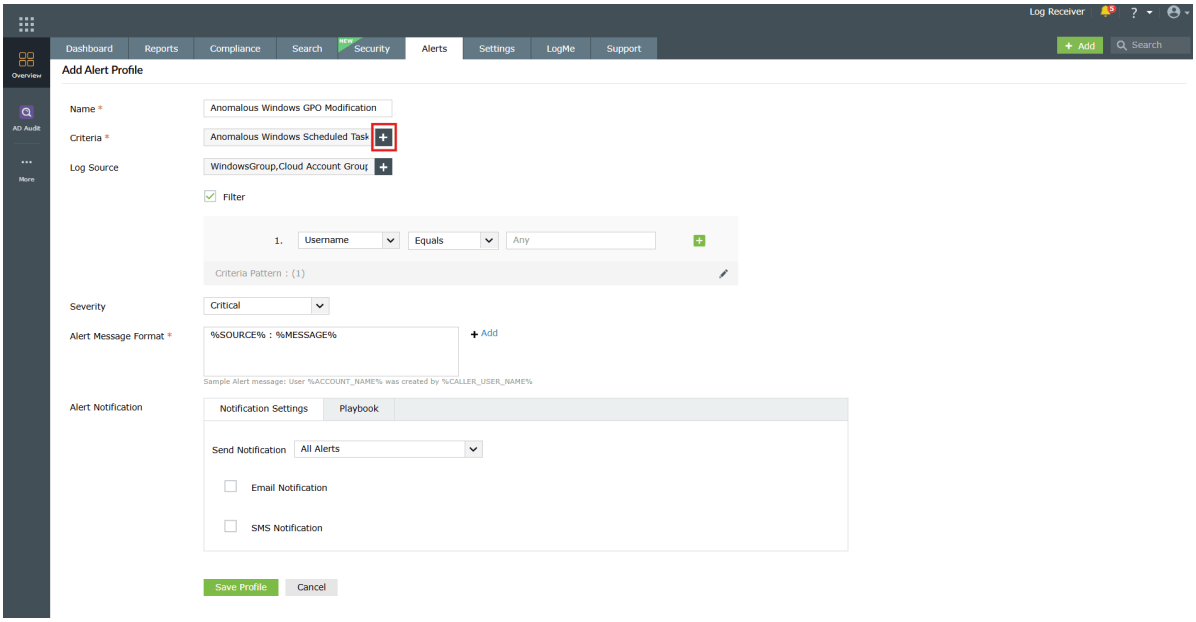


Image 5: Alerts criteria configuration

4. Defining alert criteria: When adding alert criteria, you can choose from four categories in the Alert Criteria Builder window.
   - Predefined Alerts

- Select Predefined Alert Criteria in the criteria builder.
- You can also now add custom filter criteria using the Filter option, which replaces the earlier + Add Criteria button for easier access.
- Choose a log type from the Group drop-down and select the required category.
- Pick the desired alert condition by clicking the radio button next to it.
- This option allows you to quickly select from a wide collection of predefined alert conditions, saving time and effort.

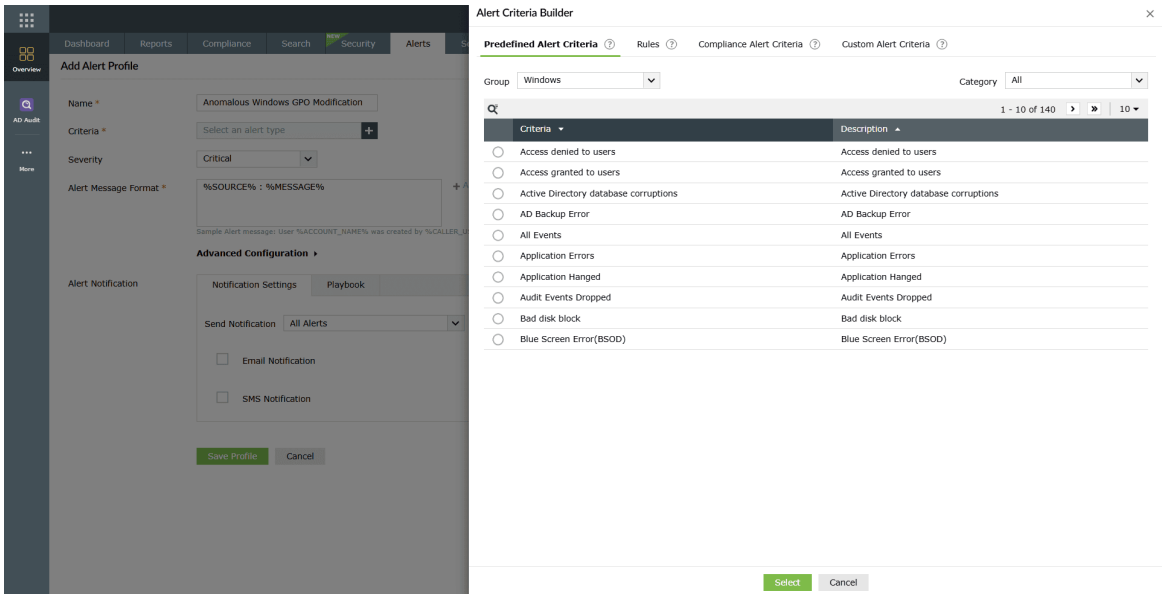
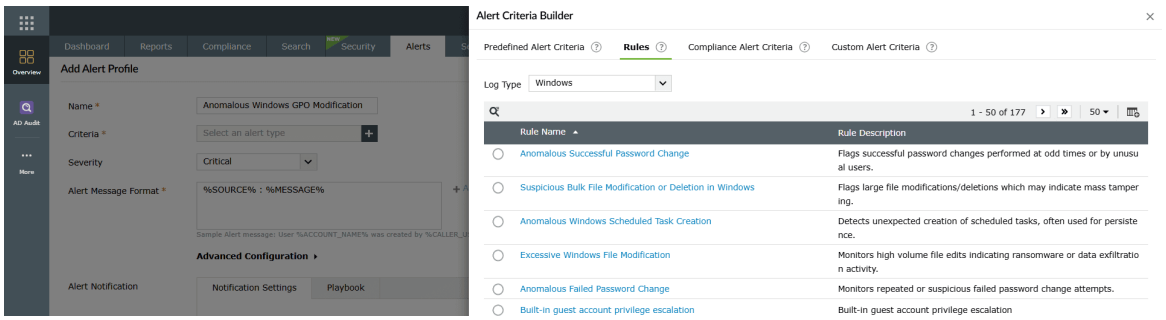


Image 6: Predefined Alert Criteria options in the criteria builder

- Rules
  - Select the Rules sub-tab in the criteria builder.
  - Browse through predefined, security-focused alert rules mapped to common threat patterns and anomalous activities.
  - Choose from a wide range of rule-based detections across supported log types such as Windows, firewalls, databases, and more.
  - Each rule is designed to surface suspicious activity, for example, unusual password changes, bulk file modifications, failed logons, privilege escalations, or unexpected system shutdowns.
  - Enable the required rules to detect automatically and alert on activities that may indicate insider threats, ransomware, brute force attempts, or other security risks.



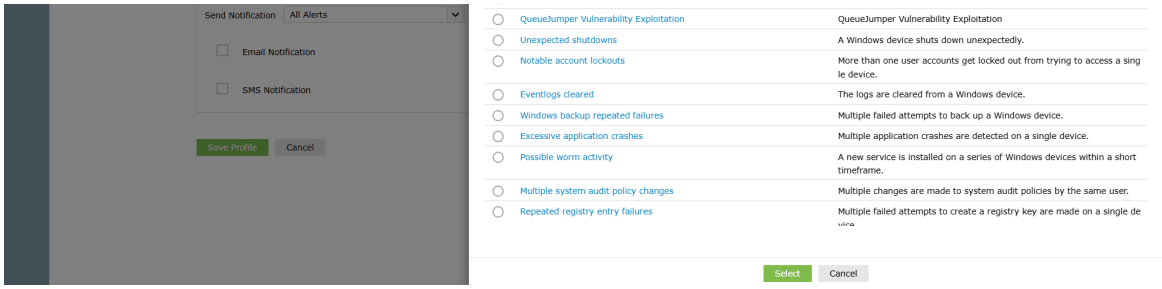


Image 7: Rule-based Alert Criteria options in the criteria builder

- Compliance Alerts
  - Select Compliance Alert Criteria in the criteria builder.
  - Browse through compliance-related alerting criteria designed to detect violations of IT regulations such as PCI DSS, SOX, HIPAA, GLBA, PDPA, NIST, CCPA, GDPR, and ISO 27001:2013.
  - Select the required compliance alert condition.
  - Compliance alerts help you monitor anomalies such as policy changes, privilege escalations, unauthorized logons, and sensitive file access or modification.

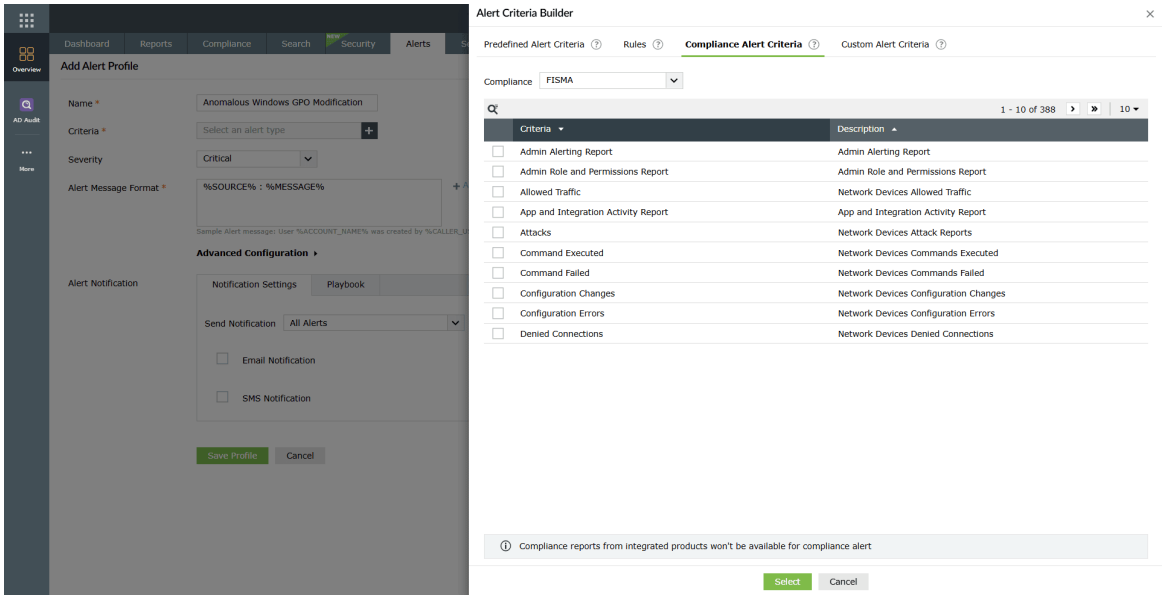


Image 8: Predefined Alert Criteria options in the criteria builder

- Custom Alerts
  - Select Custom Alert Criteria in the criteria builder.
  - Define one or more alert conditions using attributes, comparators, and values.
  - Group or ungroup conditions using AND/OR operators.
  - Optionally, configure alerts for imported logs such as Oracle, Microsoft SQL, IIS, or Print Servers by selecting the custom extracted fields.

> NOTE
>
> To add multiple custom extracted fields, click on the + icon in the criteria builder

To add multiple custom extracted fields, click on the + icon in the criteria builder.

- Vulnerability and Misconfiguration Comparators (available when integrated with Endpoint Central):
- Is Vulnerable – Detect devices tagged as vulnerable.
- Vulnerable To – Identify devices exposed to specific CVEs.
- Misconfigured For – Detect devices with misconfigurations (e.g., Windows Credential Guard disabled).

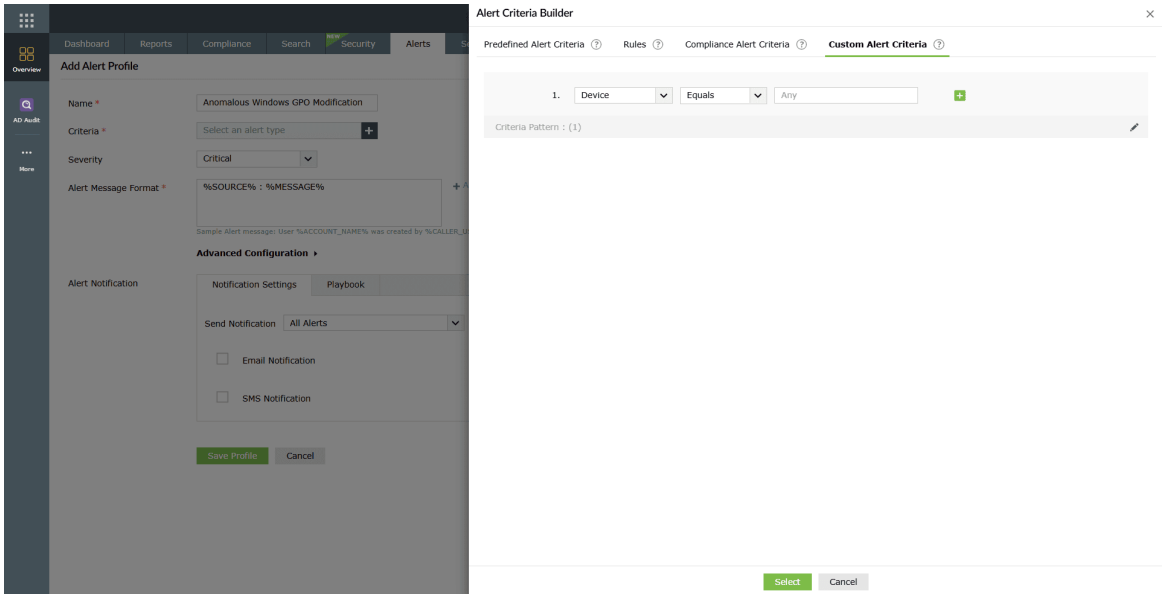


Image 9: Alert Criteria Builder window

5. Choose the Log Source(s) to be configured under this alert profile.

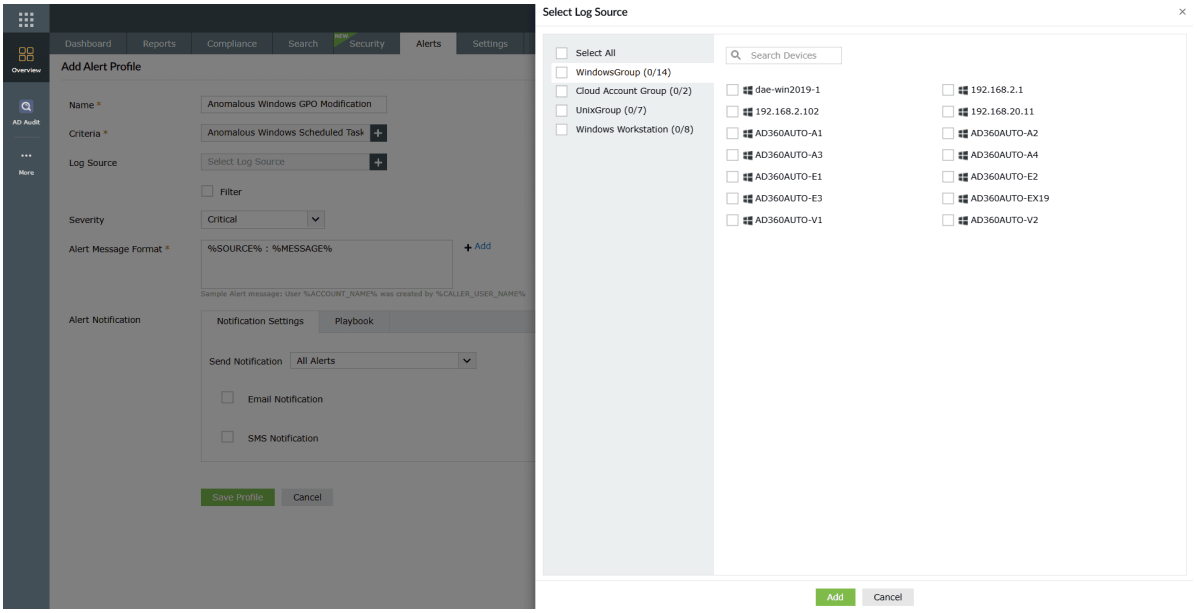


Image 10: Log source configuration

6. (Optional) Click on the checkbox to enable Filter for this alert profile. For configuring users and groups under this alert profile, refer to the Object Filter help document.

> **NOTE**
>
> Additional custom filter criteria can now be added using the Filter option. Earlier, this functionality was provided as a + Add Criteria button within the alert profile view, but it has now been moved outside for easier access.

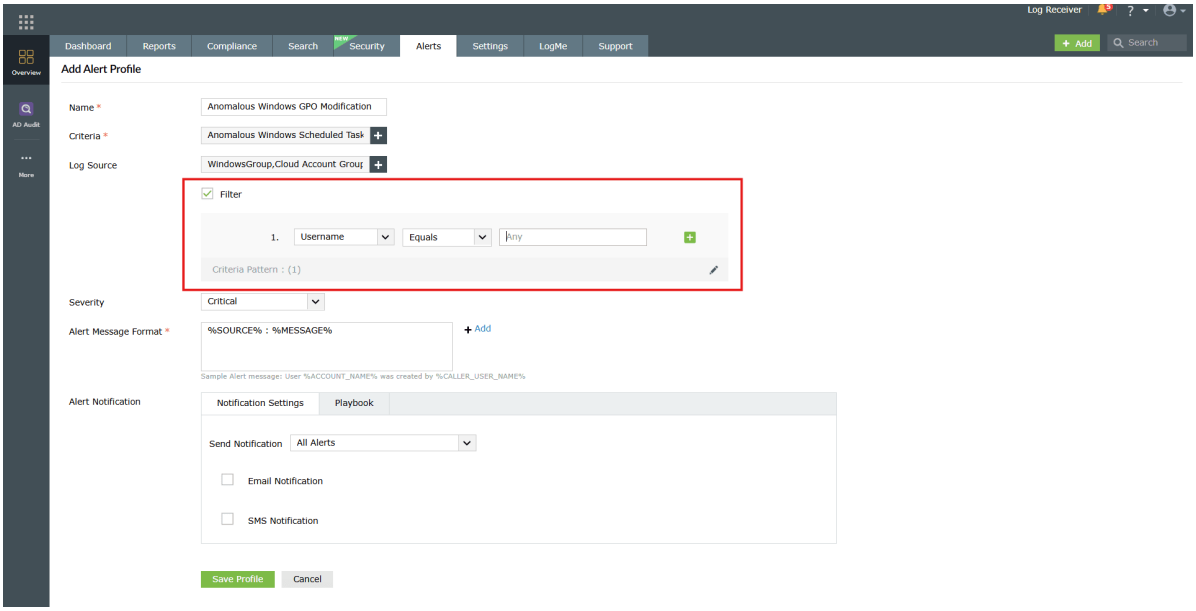


Image 11: Configuring filter for log source

7. Choose the severity level for the alerts generated by this profile from the Severity drop-down. Available options are:
   - Critical
   - Trouble
   - Attention
8. In the Alert Message Format field, customize the alert message. Click on +Add to insert variables such as account name, source, and message into the message format.

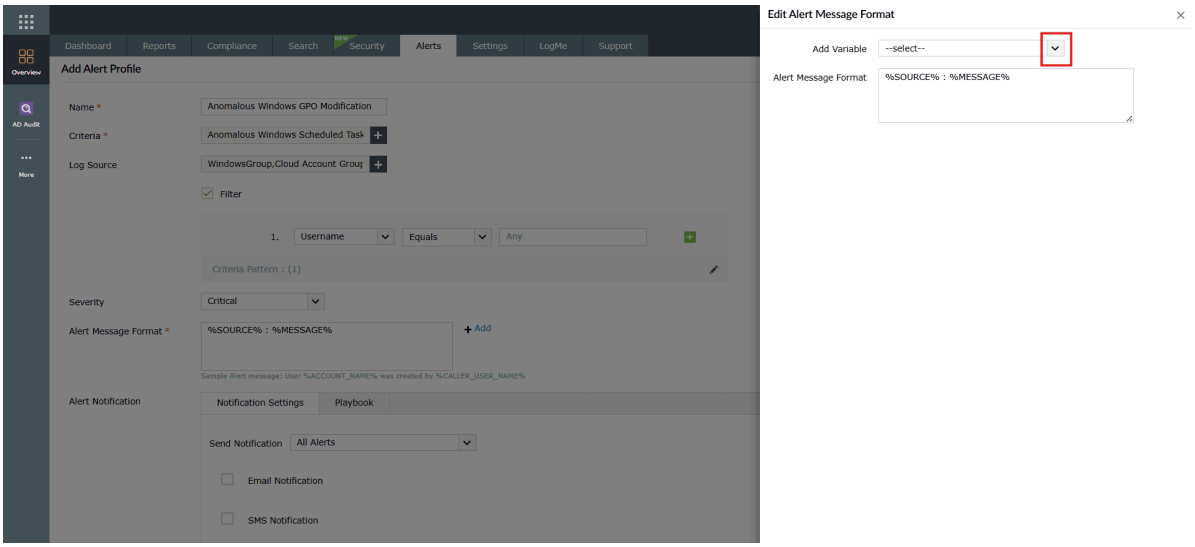




Image 12: Alert Message Format customization

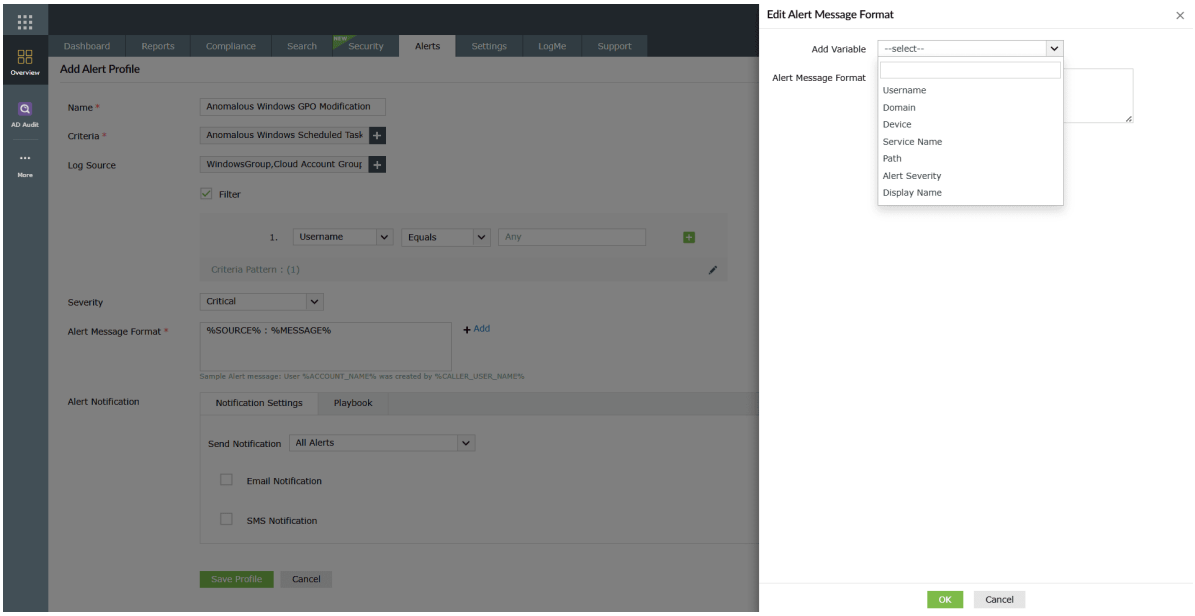


Image 13: Alert Message Format customization

9. Expand the Advanced Configuration section to refine alert trigger conditions:

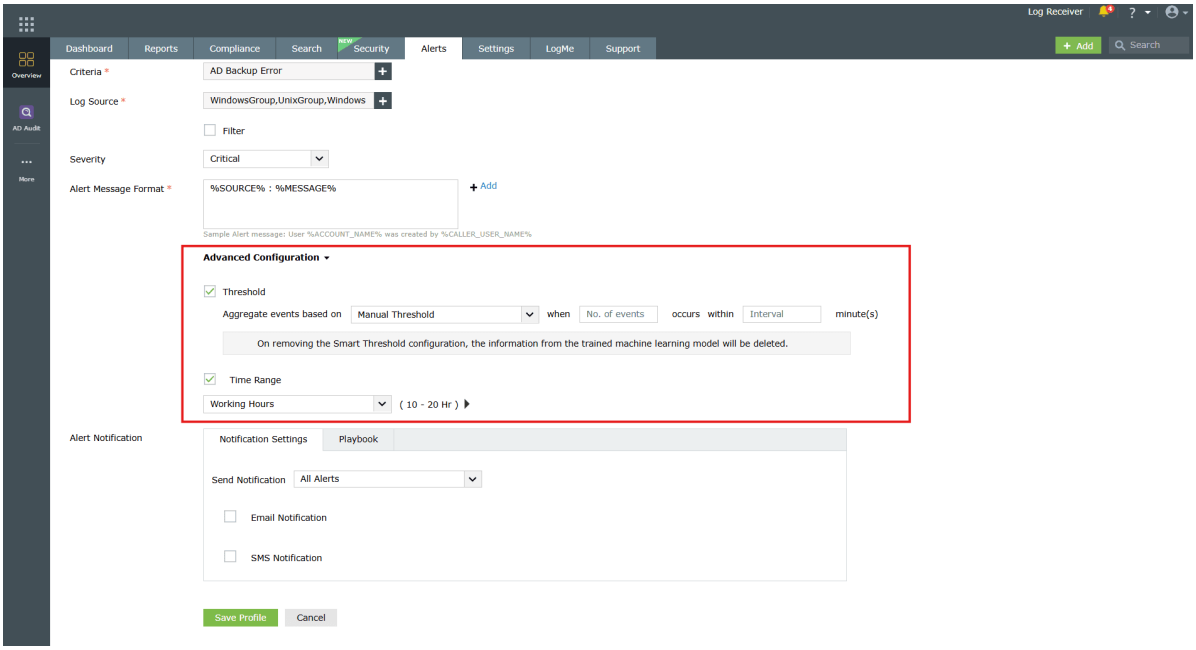


Image 14: Advanced Configuration options

- Threshold
  - Manual Threshold: Define the number of event occurrences and the time interval (in minutes).
  - Smart Threshold: Enter the time interval, and the optimal event count will be automatically determined using ML algorithms to reduce false positives.

- Time Range: Specify working hours during which the alert profile should be active.

10. Under Alert Notification, configure notifications and playbooks for the alert profile:

- Notification Settings:
  - Select the Notification Settings tab while creating an alert profile.

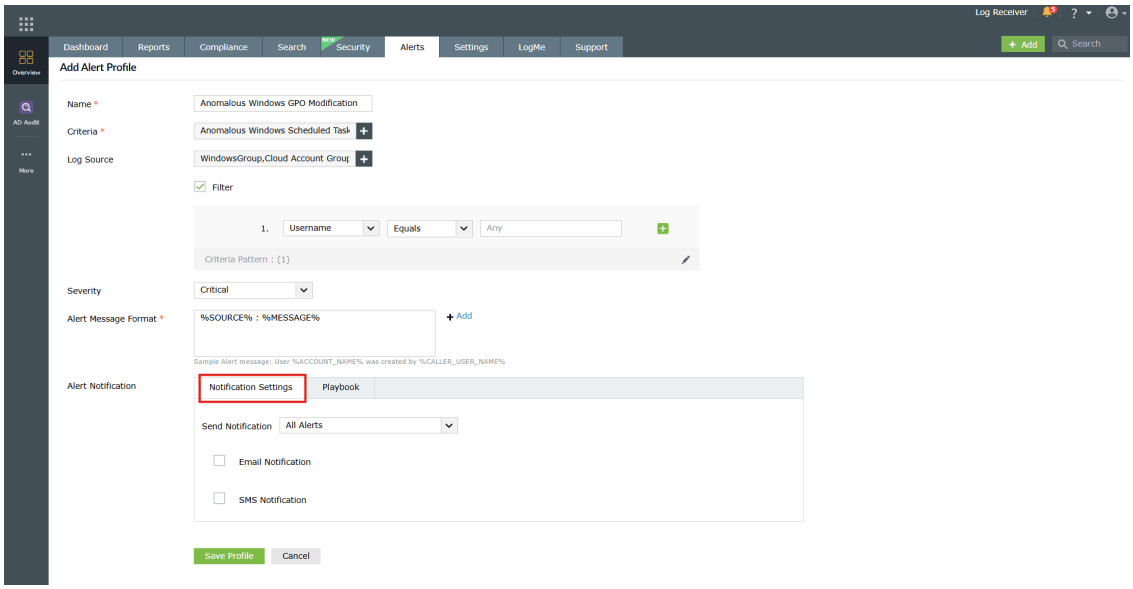


Image 15: Notification settings configuration

  - Choose whether notifications should be sent for all alerts continuously or paused for a specific duration after a notification is triggered.

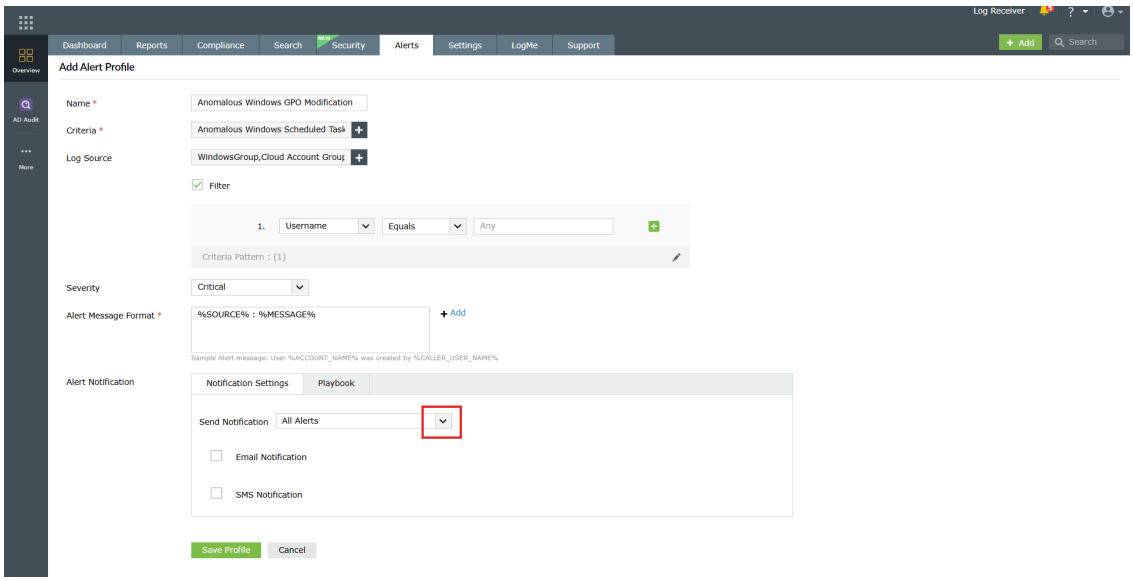
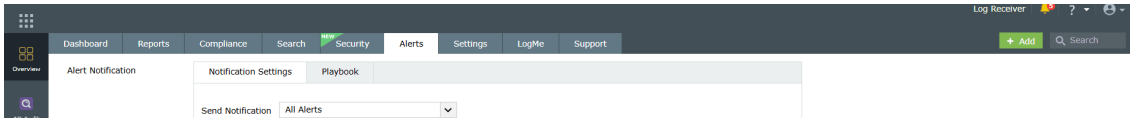


Image 16: Notification settings configuration

  - Configure Email Notifications by specifying recipients, subject lines, and message templates with dynamic macros after enabling it by clicking on the checkbox.



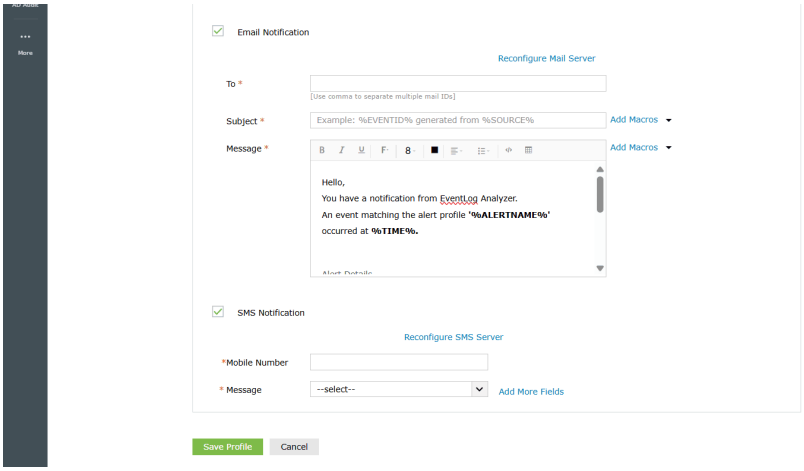


Image 17: Email notification settings configuration

- Enable SMS Notifications by entering mobile numbers and predefined message formats.
- These notifications ensure that critical alerts are immediately communicated to administrators and security teams, enabling quicker response to potential threats.
- To learn more about configuring the alert notifications, refer to the Alert Notification and Remediation help document.

- Playbook
  - Enable automated playbook remediations for the alert profile by navigating to the Playbook sub-tab and configuring the required playbook.

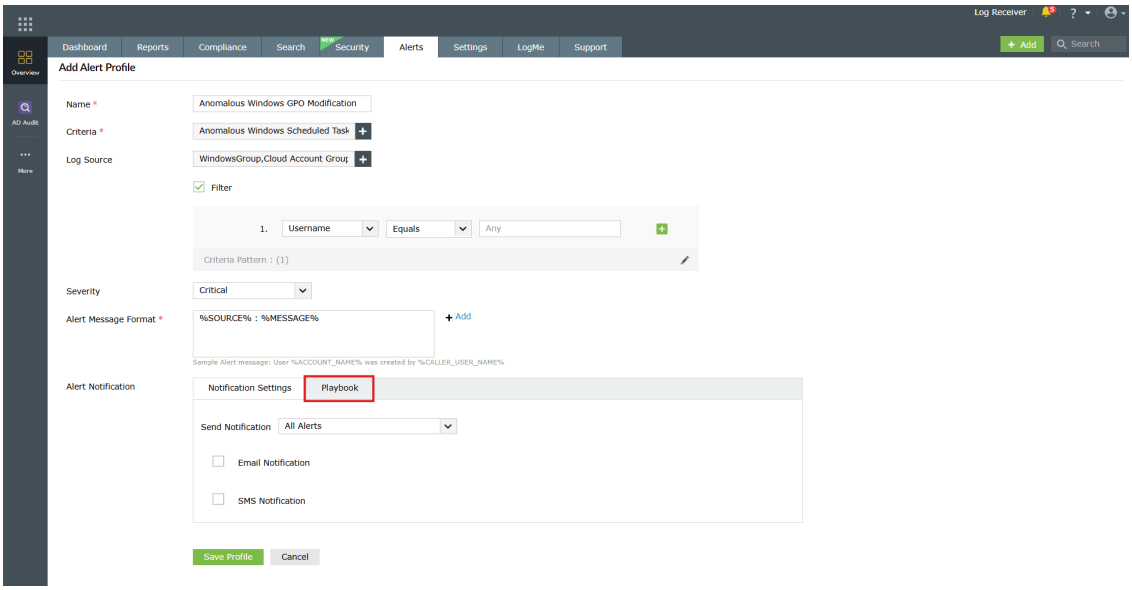
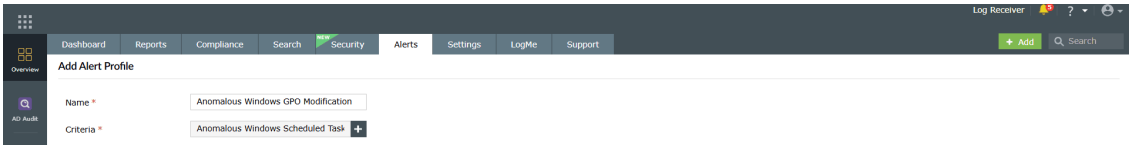


Image 18: Playbook remediation configuration

  - Check the Enable Playbook box to select or add a predefined playbook that should run automatically when the alert is triggered.



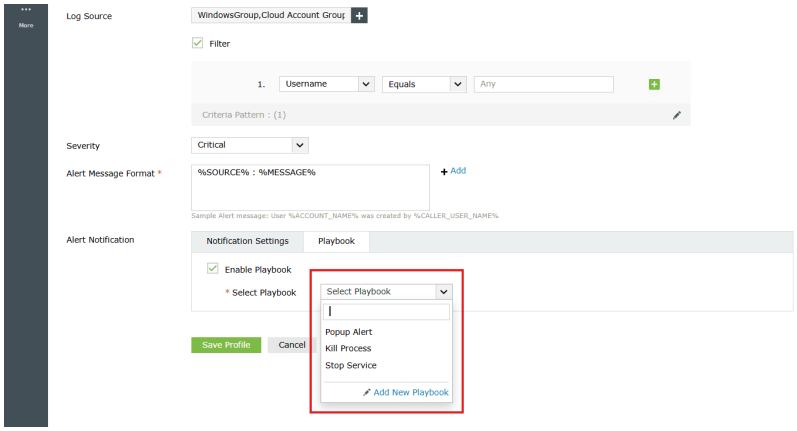
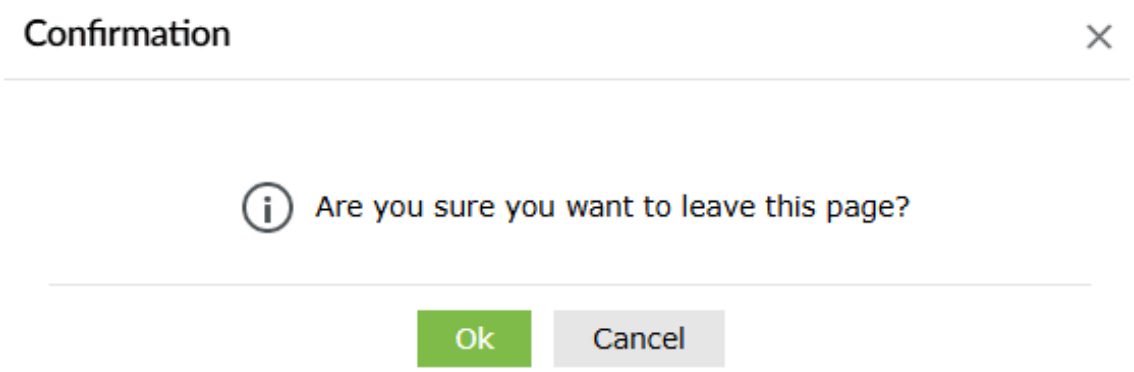


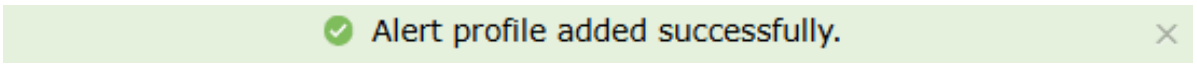
Image 19: Alert Notification settings with Playbook option

- You can configure a new playbook by clicking on the Add New Playbook option. A pop-up appears asking for a confirmation. Click on Ok.



- You will be taken to the Manage Playbooks module. To learn more about playbooks and how to configure them, refer to the Playbook management help document.playbooks and how to configure them, refer to the Playbook management help document.

11. Once all configurations are complete, click on Save Profile. Upon successful completion of the action, the below pop-up appears, and the alert profile is now created and listed on the Manage Alert Profiles page.



Read also

This page gave a step-by-step guide on how to create new alert profiles. Read more about configuring alert notifications, using playbooks, and managing alert profiles to streamline monitoring and response from the below help pages.

- Overview
- Manage alert Profiles
- Alert Notification & Remediation

8.6.3. Manage alert profiles

Last updated on: September 12, 2025

In this page

- Overview
- Managing alert profiles
  - Enable/Disable
  - Delete
  - Edit
  - Clone an alert profile
  - Bulk Actions
  - Filter alert profiles
  - More Options
    - Import
    - Export

Overview

The manage alerts section provides an overview of all configured alert profiles along with their severity, associated log sources, and notification settings. Based on the Created By type, alert profiles can be edited, deleted, copied, or toggled on/off. Similarly, few alert profiles, however, can only be enabled, disabled, or duplicated and cannot be edited or deleted.

There are three types of alert profiles based on the “Created by” column:

- Log360
  - These are the default, built-in alert profiles.
  - They are not fully modifiable.
  - Users can only do limited actions such as: enable/disable, clone, and update specific configurations (like log sources and notification settings).
  - But users cannot delete or fully edit them.
- Users
  - These are the custom alert profiles created manually by technicians/users.
  - They are fully modifiable.
  - Meaning: you can perform all actions — enable/disable, delete, update completely, and clone.
  - Exception: If it’s a rule-based alert under “Users,” then it behaves like Log360/Extension ones (i.e., only partially modifiable).

- Extension
  - These are alert profiles that come from extensions installed through the Marketplace.
  - Same as Log360 profiles, they are not fully modifiable.
  - Users can only enable/disable, clone, and update specific configurations (log sources & notifications).

Managing alert profiles

1. In the console, navigate to the Alerts tab.

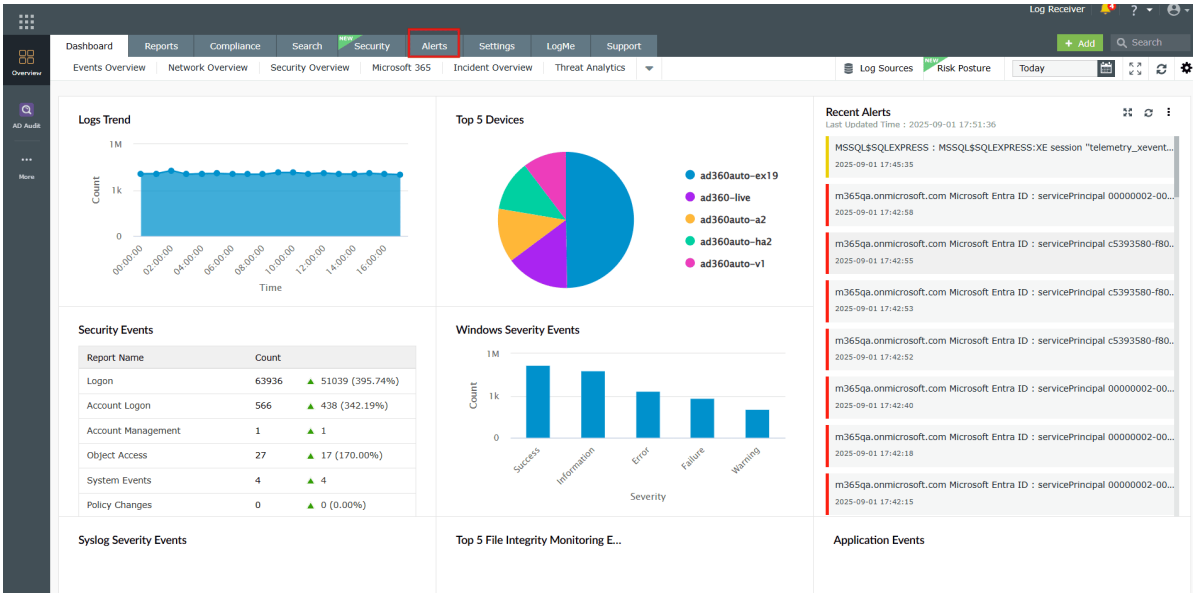


Image 1: Alerts tab in the dashboard

2. You will be taken to the Alerts module. Click on Manage Alert Profiles as highlighted in the below image.

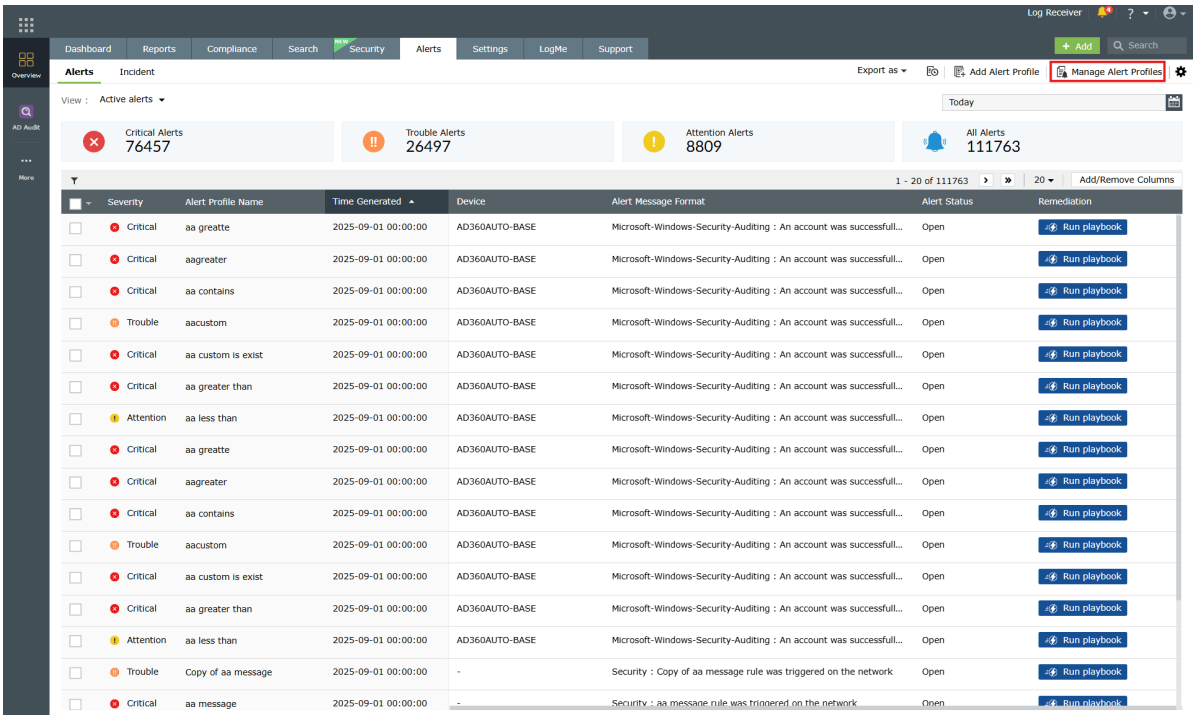


Image 2: Alerts module via the dashboard

3. The Manage Profiles page displays the list of all alerts, their profile types, creators, and log sources.

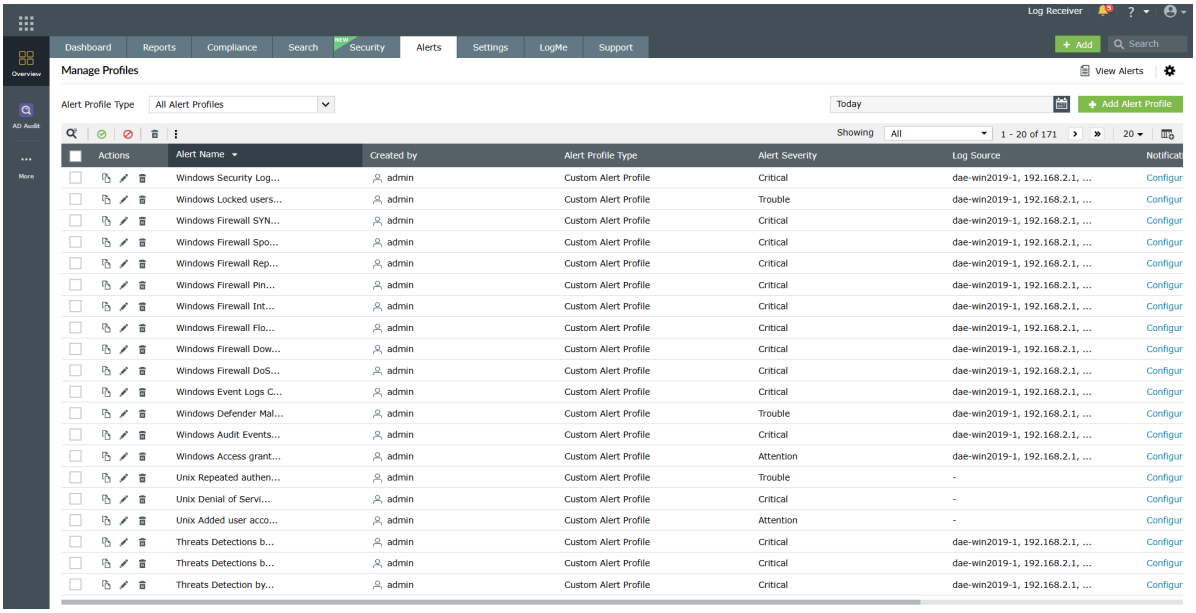


Image 3: Manage alert profiles module

You can:

- Enable/disable
- Delete
- Edit
- Copy an alert profile
- Perform bulk actions
- Filter and sort alerts

4. You can also add a new alert profile by clicking on the Add Alert Profile button as highlighted below. To learn more about creating new alert profiles, refer to the Create Alert Profiles help document.

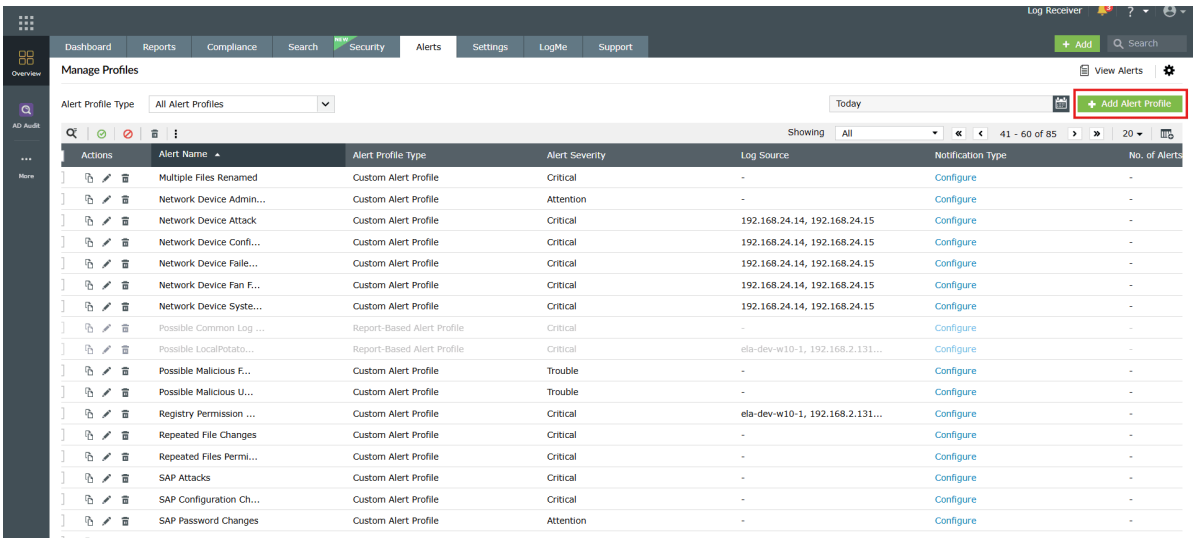


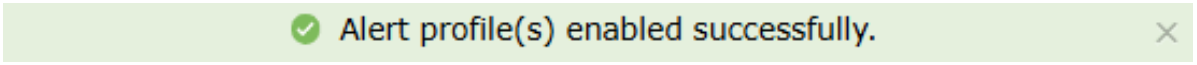


Image 4: Add alert profile option via manage alert profiles module

Enable/disable an alert profile

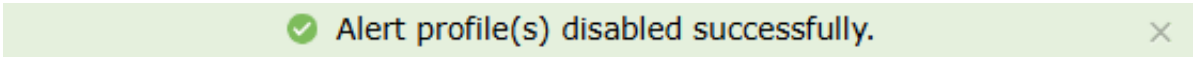
Enabling an alert profile

1. Click on the enable icon present in the ribbon to enable the alert.
2. The alert is now enabled, and a confirmation pop-up briefly appears.



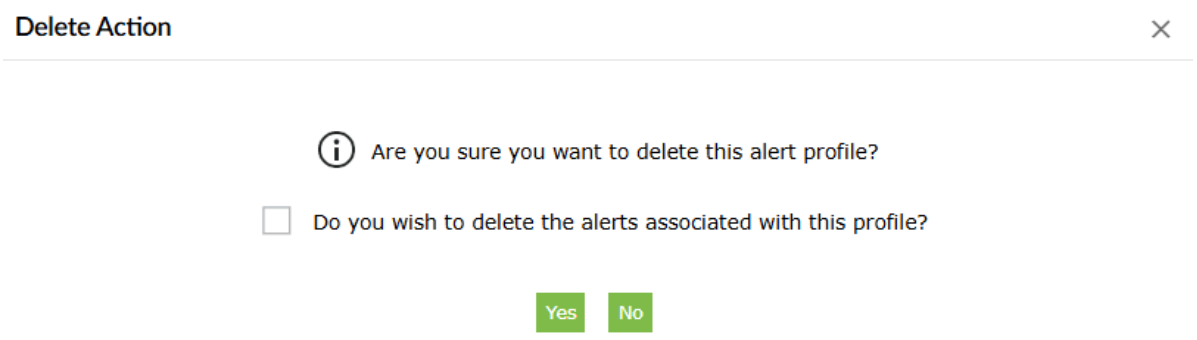
Disabling an alert profile

1. Click on the disable icon present in the ribbon to disable the alert.
2. The alert is now disabled, and a confirmation pop-up briefly appears.



Delete an alert profile

1. Click on the Delete icon under the Actions column to delete the alert.
2. A Delete Action pop-up appears for confirmation. Click on the checkbox and Yes to proceed.



3. Once completed, a success confirmation pop-up appears.



NOTE

Only applicable alert profiles based on the Created By type can be deleted. Similarly the rest of the

types can only be enabled, disabled, or copied.

Edit an alert profile

1. Click on the Edit icon under the Actions column to modify the respective alert profile.
2. You will be taken to the Edit Alert Profile module. Make the necessary changes to the criteria, severity, or notification settings, and click on Update.

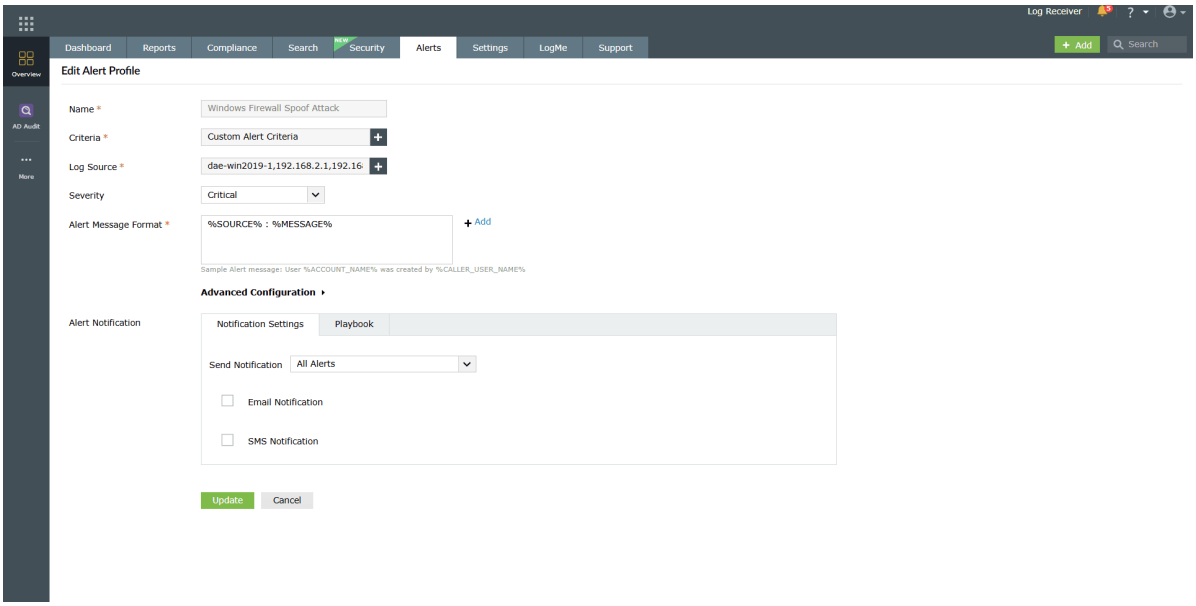


Image 5: Edit alert profile via manage alert profiles module

3. Upon successful completion of the action, the below pop-up appears, and the alert is saved instantly, and you are redirected back to the Manage Alerts module with the updated alert listed.



Clone an alert profile

1. Click on the Clone icon under the Actions column to duplicate the respective alert profile.
2. The alert is instantly duplicated, and you will be instantly taken to the Add Alert Profile module where you can edit the cloned alert profile based on your requirements and save that version on the cloned alert profile.

Bulk actions

1. Select the checkboxes next to the alerts you want to manage.
2. Use the toolbar at the top of the alert list to perform actions in bulk, such as clicking on the Enable, Disable, or Delete icons to perform the desired bulk action.

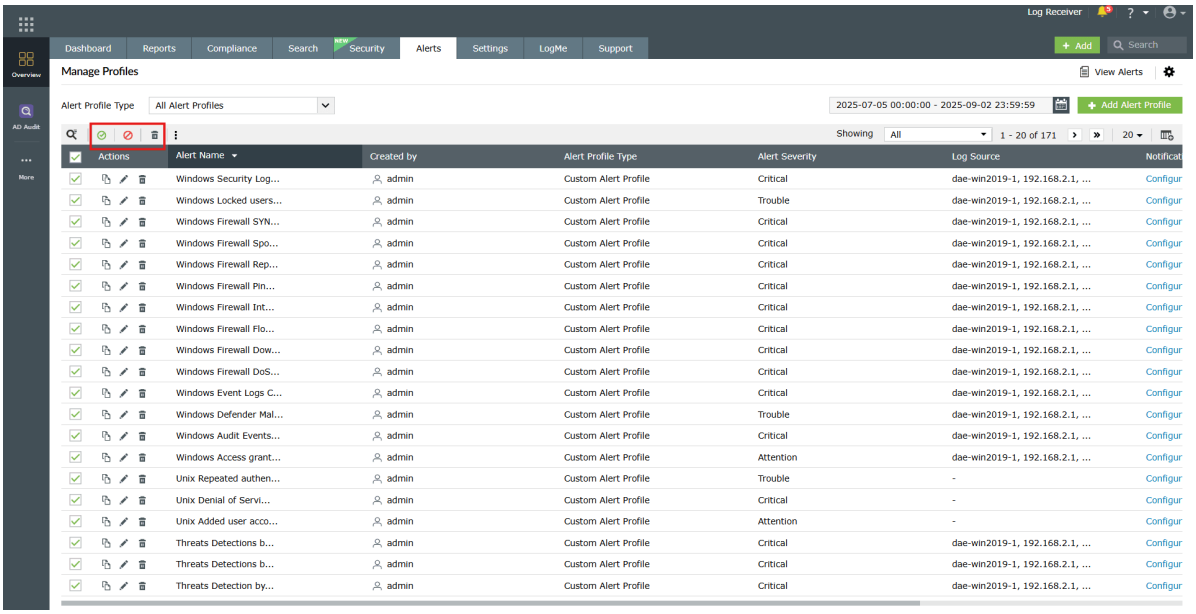
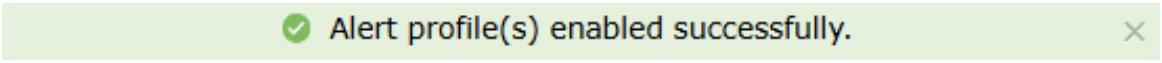


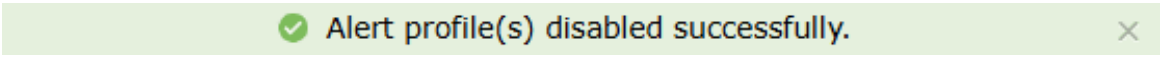
Image 6: Bulk enable/disable or delete alerts

3. Upon successful completion of the action, the following confirmation pop-up appears:

- When enabled successfully:



- When disabled successfully:



- When deleted successfully:

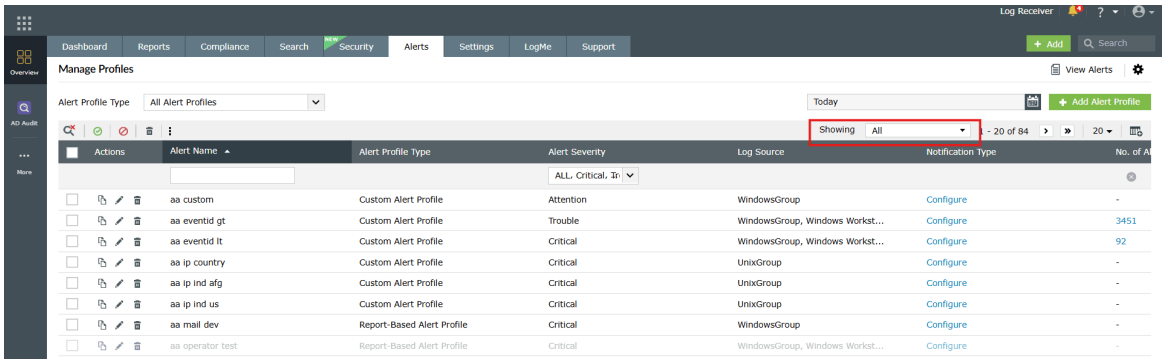


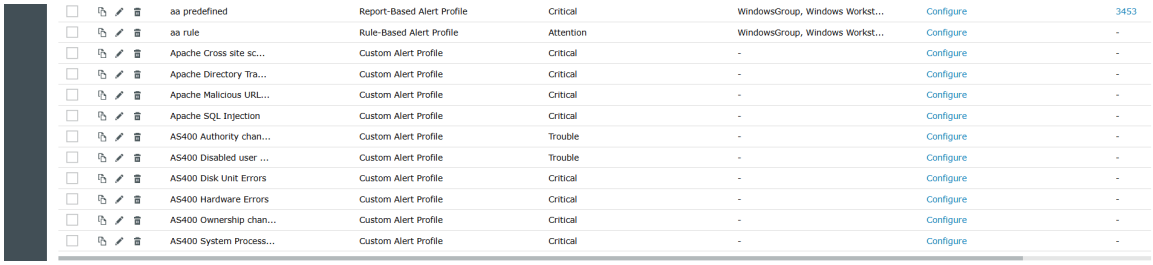
Filtering alert profiles

You can filter alert profiles in the following ways:

1. Based on status (enabled/disabled)

- Use the filter option above the alerts list to view only enabled or only disabled alert profiles.





aa predefined	Report-Based Alert Profile	Critical	WindowsGroup, Windows Workst...	Configure	3453
aa rule	Rule-Based Alert Profile	Attention	WindowsGroup, Windows Workst...	Configure	-
Apache Cross site sc...	Custom Alert Profile	Critical	-	Configure	-
Apache Directory Tra...	Custom Alert Profile	Critical	-	Configure	-
Apache Malicious URL...	Custom Alert Profile	Critical	-	Configure	-
Apache SQL Injection	Custom Alert Profile	Critical	-	Configure	-
AS400 Authority chan...	Custom Alert Profile	Trouble	-	Configure	-
AS400 Disabled user ...	Custom Alert Profile	Trouble	-	Configure	-
AS400 Disk Unit Errors	Custom Alert Profile	Critical	-	Configure	-
AS400 Hardware Errors	Custom Alert Profile	Critical	-	Configure	-
AS400 Ownership chan...	Custom Alert Profile	Critical	-	Configure	-
AS400 System Process...	Custom Alert Profile	Critical	-	Configure	-

Image 7: Filtering alert profiles via manage alert profiles module

- This helps you quickly identify active alerts versus those that are turned off.

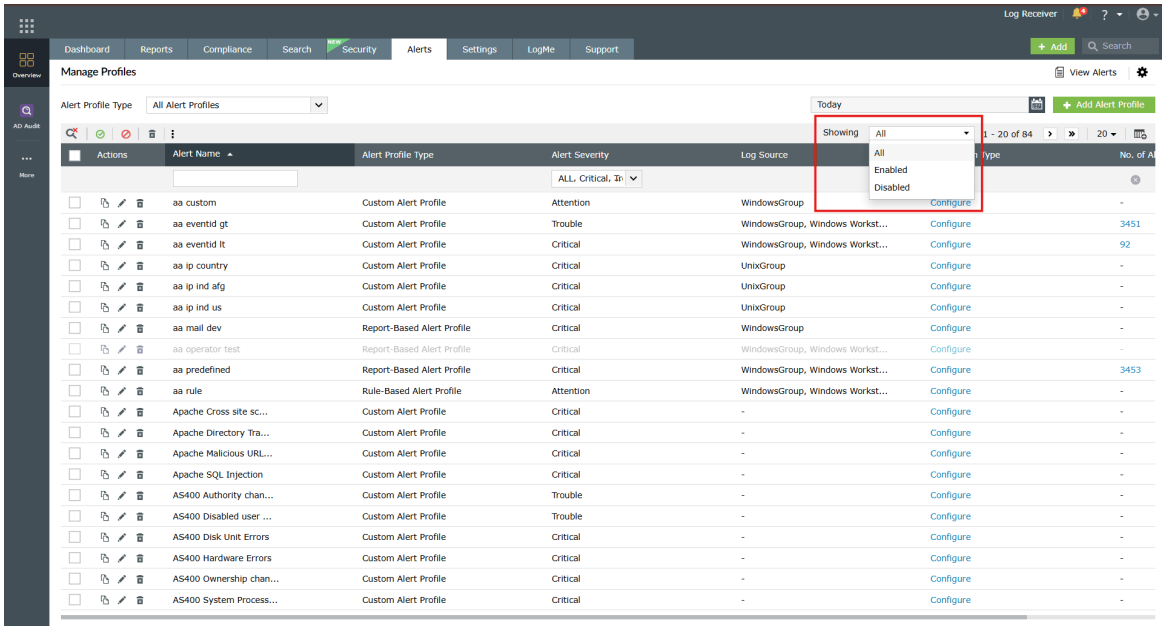


Image 8: Filtering alert profiles via manage alert profiles module

2. Calendar-based filtering

- Click on the calendar icon in the filter options.

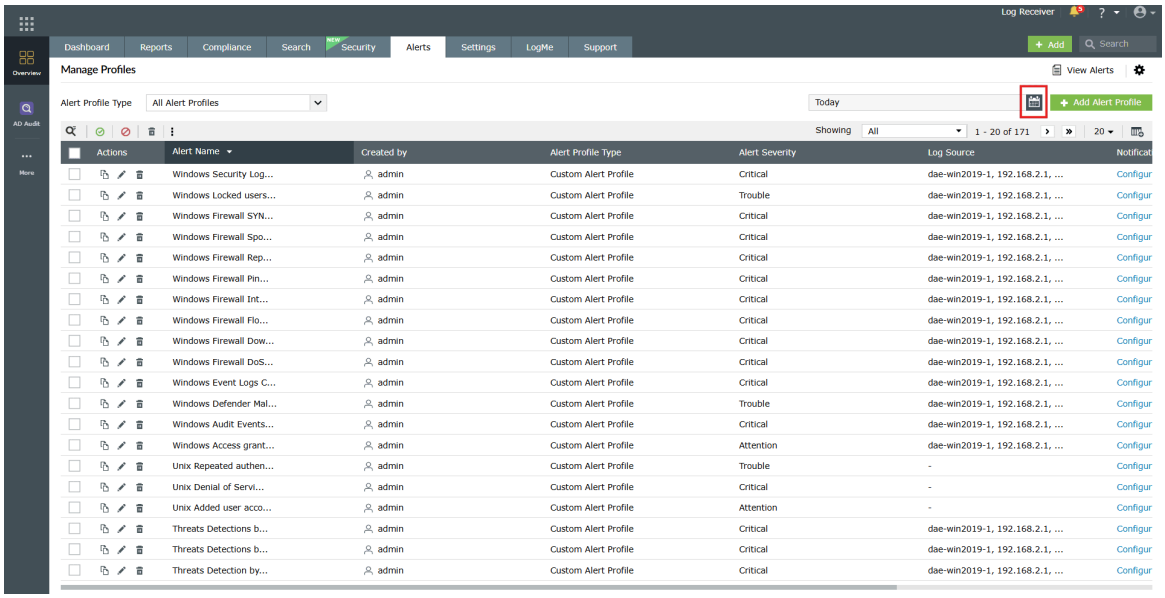


Image 9: Filtering alert profiles for a time range

- The action opens a calendar view along with predefined time ranges for you to choose from. You can also view the count of all triggered alerts based on the time range.

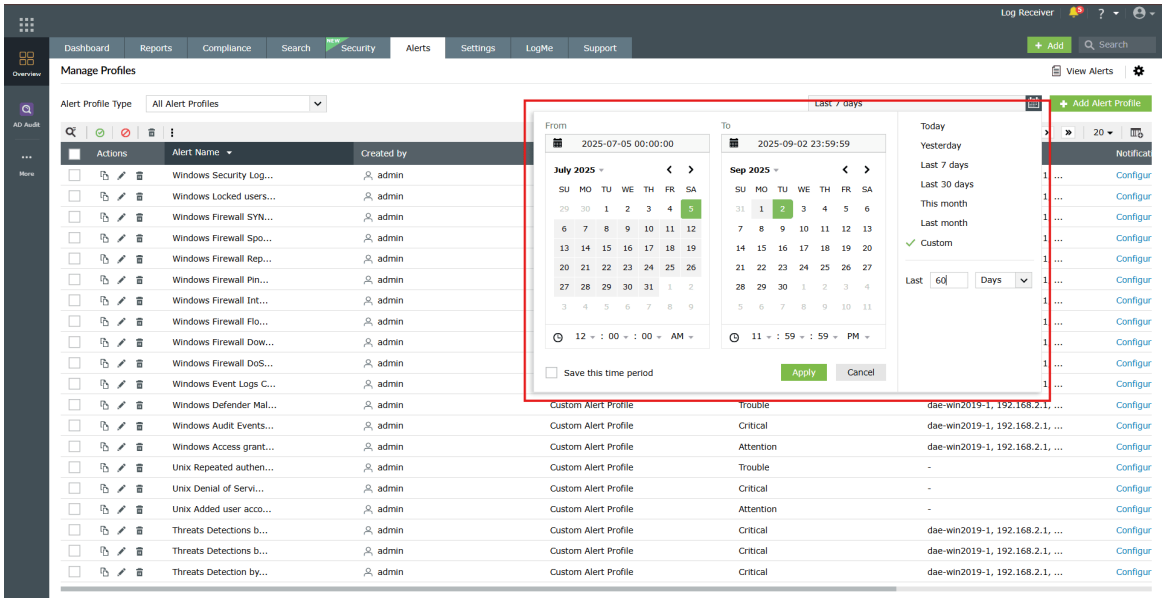
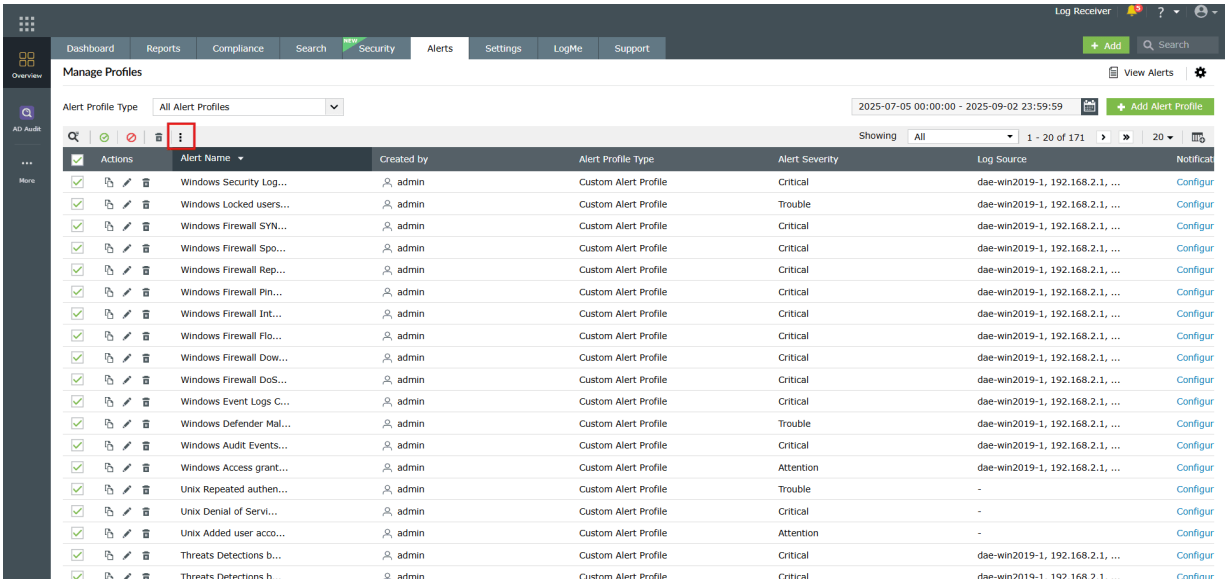


Image 10: Filtering alert profiles for a time range

  - Click on any of the predefined time ranges available that best suits your requirement.
  - Click on Custom range and enter a number in the box provided to represent the past number of days' worth of alerts you wish to view.
- Click on Apply.
- Upon completion, the alerts list will continue to display all available profiles. However, the alert counts will be filtered and updated based on the selected time range.

More Options

Click on the More Options icon as highlighted below to view the Import and Export actions.



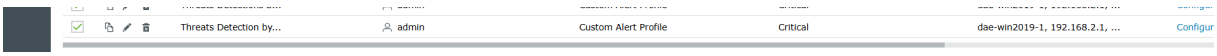
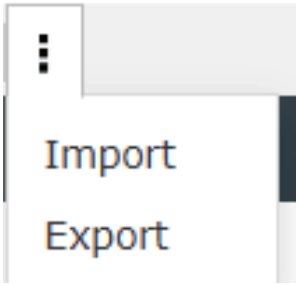


Image 11: More options for managing alert profiles



Import alert profiles

- Click on the Import option in the options list.
- Browse and select the file that contains the alert profiles you wish to import.
- If the imported alert profile matches an existing one, you will be prompted to overwrite the existing profile. Select the required profile and click Import.

Export alert profiles

- Select the required alert profiles using the checkbox(es).
- Click on the Export option in the options list.

> NOTE
>
> Default, extension-based and Rule-based alert profiles cannot be exported.

Read also

This page elaborated a detailed guide on managing alert profiles efficiently. Read more about creating alert profiles, configuring alert notifications, and using playbooks for automated response and monitoring from the below guides:

- Overview
- Create Alert Profile
- Alert Notification & Remediation

8.6.4. Alert notification and remediation

Last updated on: September 12, 2025

In this page

Overview

Notification settings

Playbook remediation

Overview

The Alert notification and remediation section enables you to configure how alerts are communicated and remediated. Notifications ensure that administrators and security teams are informed in real time, while playbooks provide automated remediation for faster response to threats.

> NOTE
>
> The remediation section referring to playbook management is applicable only for EventLog Analyzer

Notification settings

1. Navigate to the Alerts tab and select the required alert profile.

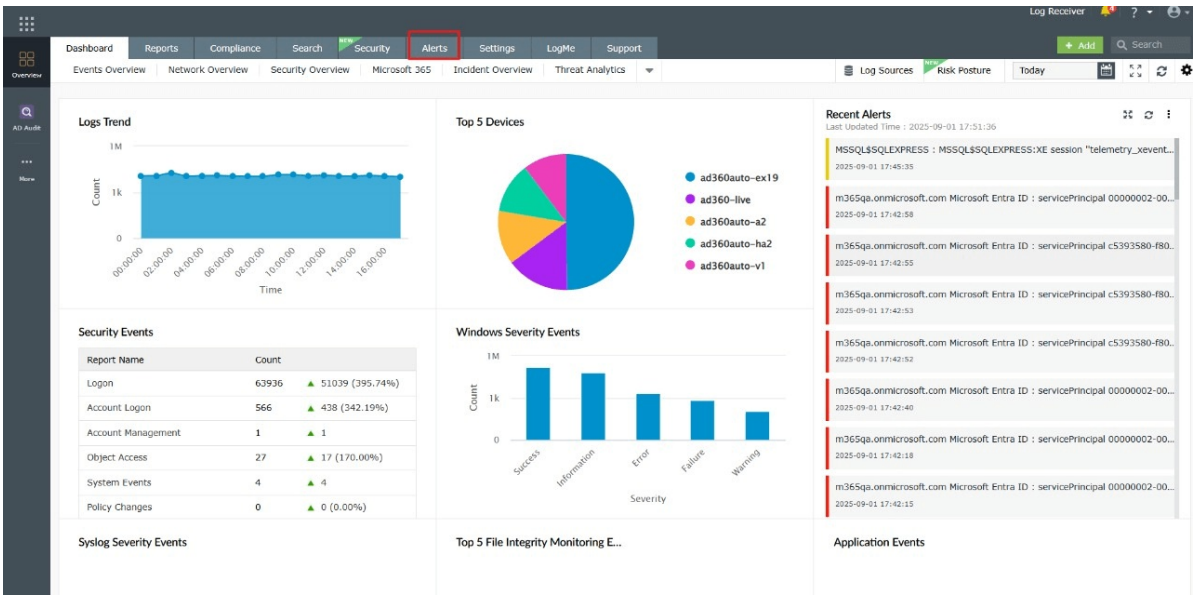


Image 1: Alerts module via the dashboard

2. Under the Notification Settings tab, you can configure how notifications should be delivered

2. Under the Notification Settings tab, you can configure how notifications should be delivered.

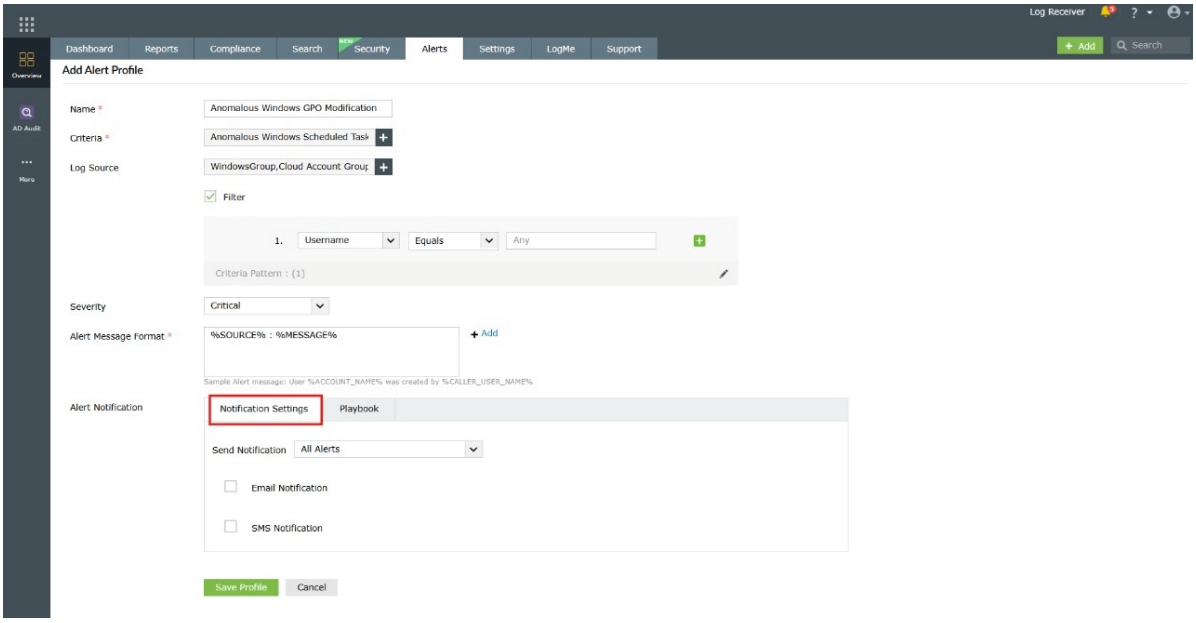


Image 2: Notification settings configuration

Options available:

- Send Notification drop-down: Choose whether notifications should be sent for all alerts continuously or paused for a specific duration after a notification is triggered.

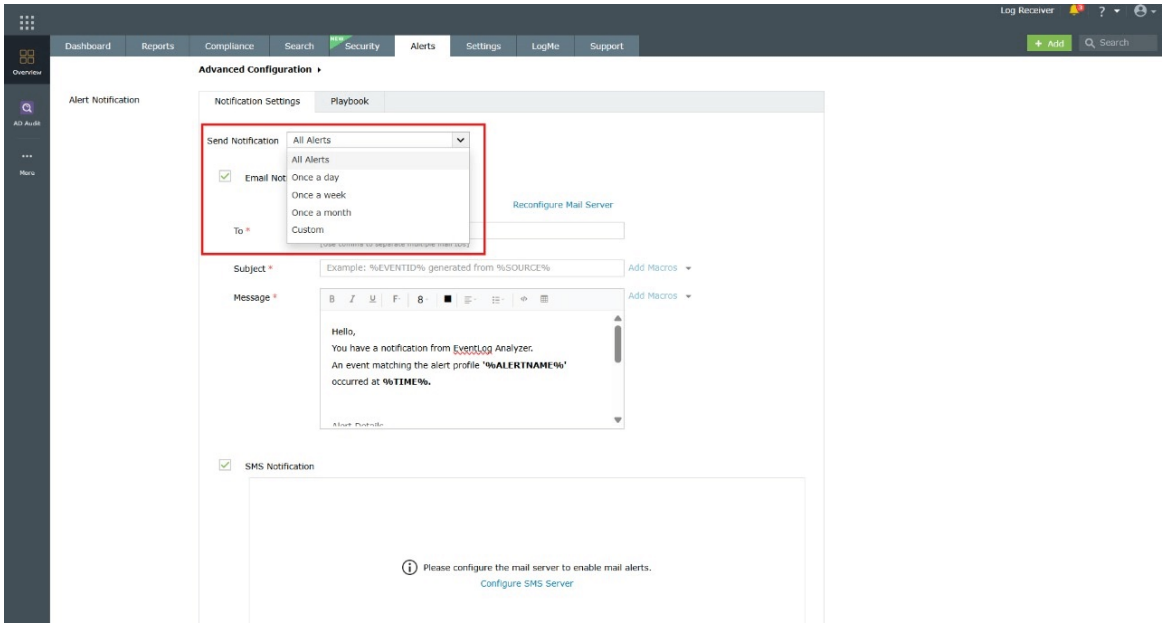
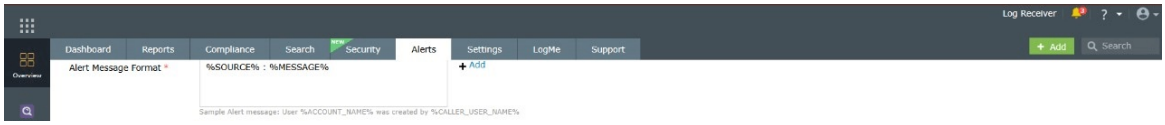


Image 3: Notification settings configuration

- Email notifications: Enable email alerts by entering recipients, subject lines, and customizable message templates with dynamic macros.



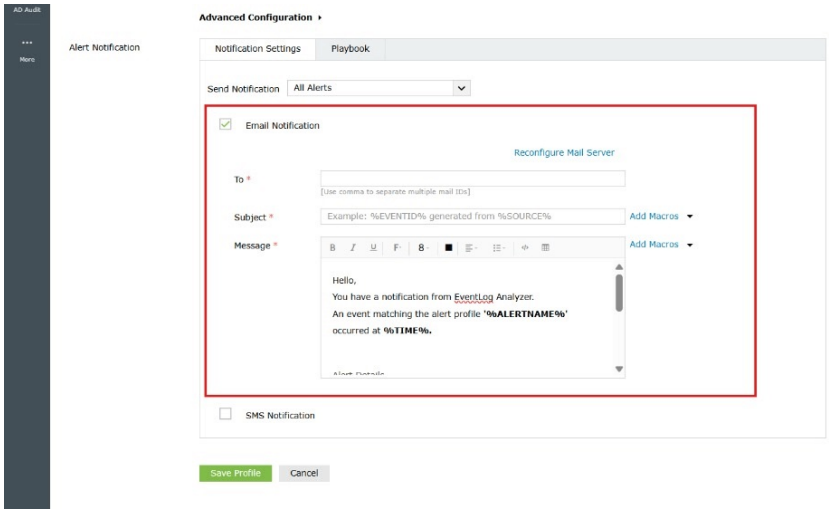
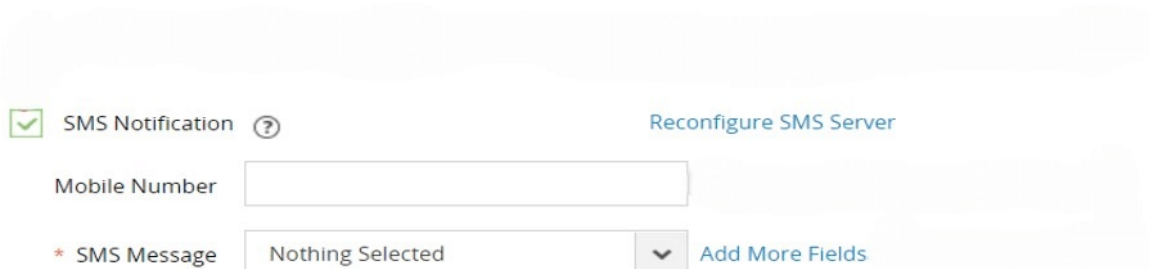


Image 4: Email notification settings configuration

- When you select Email Notification, the following fields can be configured:
  - To: Enter the recipient email addresses. Multiple addresses can be added by separating them with commas. Example: admin@example.com, soc@example.com
  - Subject: Define the subject line of the email notification. You can use macros to insert dynamic values such as %EVENTID%, %SOURCE%, or %ALERTNAME%. Example: Alert: %EVENTID% generated from %SOURCE%
  - Message: Customize the body of the notification email. A default message is provided, but you can edit it to include relevant alert details and instructions. Macros can also be inserted here for dynamic data.
  - Macros: The Add Macros option allows you to insert system variables dynamically. Common macros include:
    - %SOURCE% → The source generating the event
    - %EVENTID% → The event identifier
    - %ALERTNAME% → The name of the triggered alert profile
    - %TIME% → The time at which the event occurred
    - %MESSAGE% → The detailed event message
  - Reconfigure Mail Server
    If email notifications fail, ensure that the mail server is correctly configured. Use the Reconfigure Mail Server option to update mail server settings.
- SMS notifications: Enable SMS alerts by adding mobile numbers and predefined message formats.



Notifications provide instant visibility of critical alerts, enabling IT and security teams to detect and respond quickly, even when not logged into the console.

Playbook remediation

1. Navigate to the Playbook tab within the alert profile.

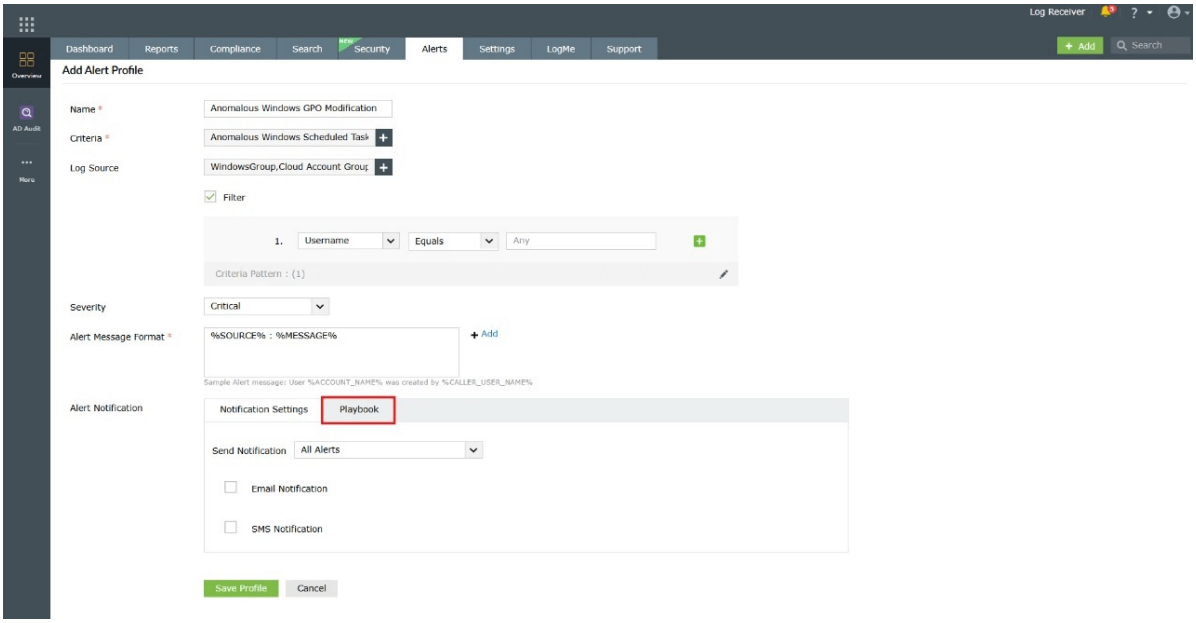


Image 5: Playbook remediations configuration

2. Check the Enable Playbook option.

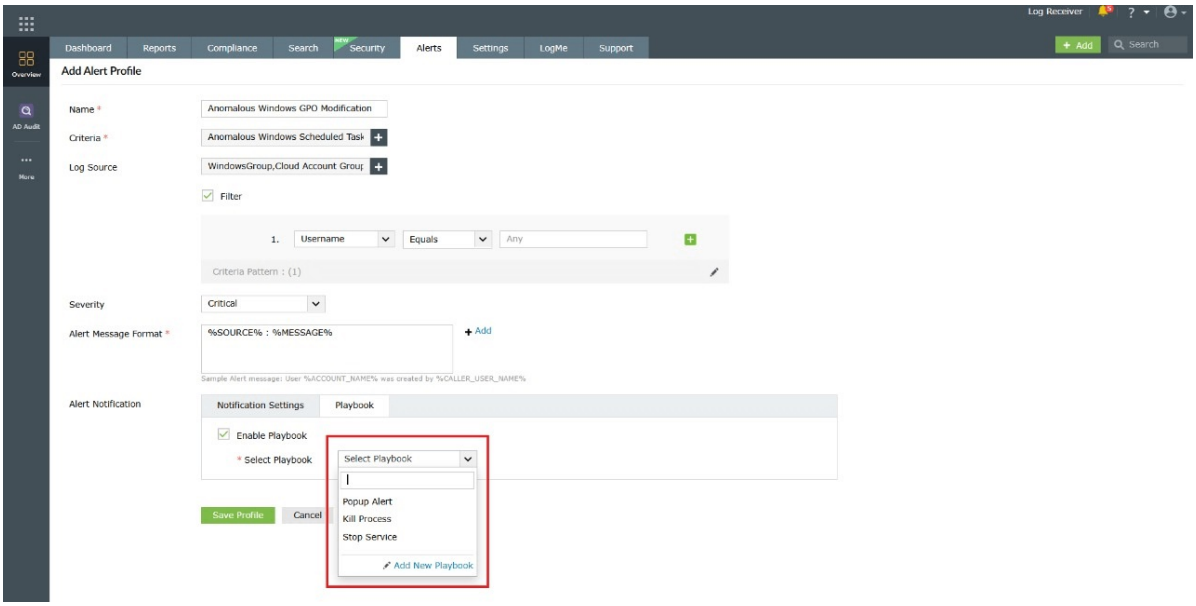


Image 6: Playbook remediations configuration

3. From here, you can:

- Select from predefined playbooks to automate standard remediation steps.

- Click Add New Playbook to create a custom playbook. A confirmation pop-up will appear. Select OK to continue.
- You will be redirected to the Manage Playbooks module to configure the new playbook.

Examples of playbook actions include:

- Disabling compromised user accounts.
- Blocking malicious IP addresses.
- Killing suspicious processes.

Once configured, the selected playbook executes automatically whenever the alert profile is triggered, reducing response time and minimizing manual intervention.
To learn more about configuring playbooks, refer to the Playbook Management help document.

Read also

This page explained how to configure alert notifications and remediations for the threats detected. Read more about configuring notifications, enabling playbooks, and managing alerts to streamline response and reduce manual effort.

- Overview
- Create Alert Profile
- Manage alert Profiles

9.1.1. Administration Settings

Last updated on: September 12, 2025

- Log360 Integration
- Auto Update
- Manage Technicians
- Logon Settings
- Reverse Proxy
- Device allocation management

9.1.2. Device Group Management

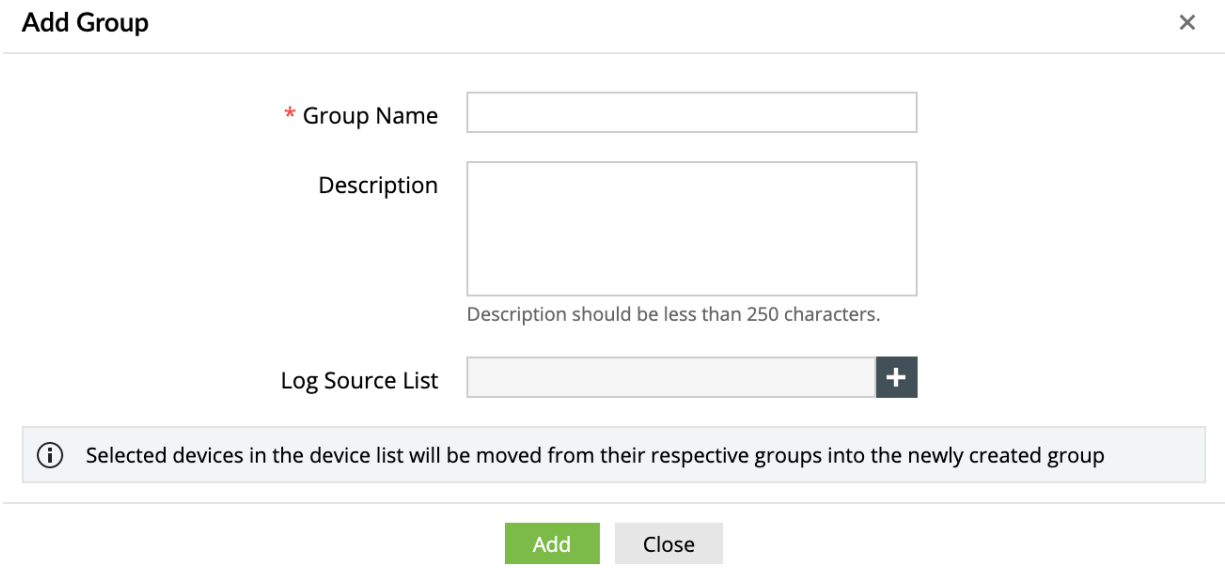
Last updated on: September 12, 2025

Device groups allow you to perform initial configuration for multiple devices simultaneously with the help of configuration templates, schedule maintenance and downtime for multiple devices, suppress events on multiple devices, etc.

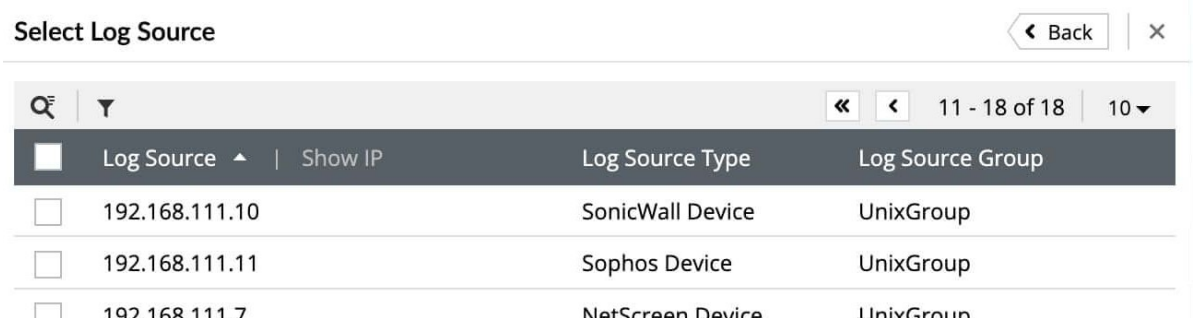
How to add a device group?

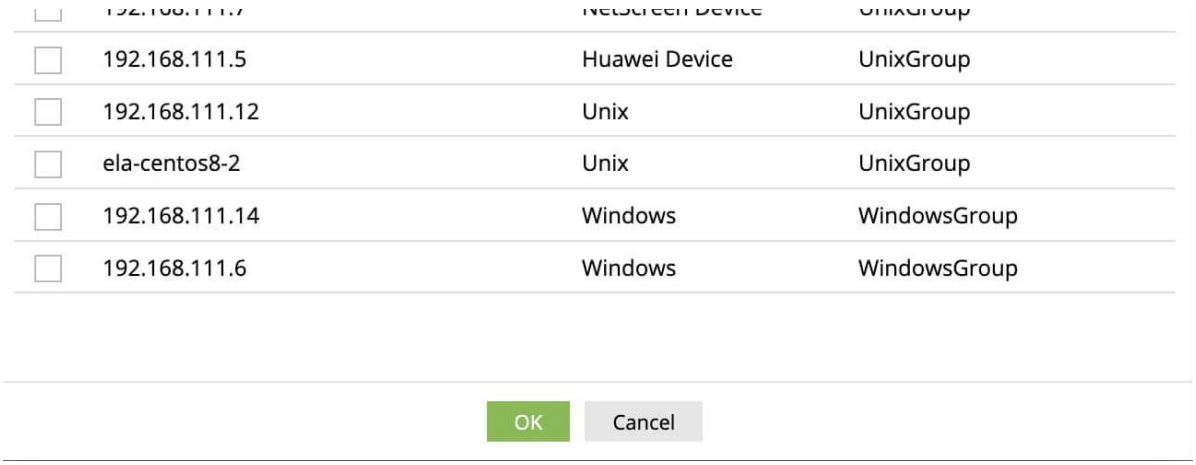
You can add a new device group using the following menu option:

- Settings tab → Admin Settings → Device Groups → +Add Group



1. Enter a unique name for the device group to be added.
2. Write a description for the device group.
3. Click on the +Add Device(s) button to add devices to this device group. You can then select the devices you wish to add by clicking on the respective check box(es).
4. Click OK.
5. Click on the + Add Device(s) button to add devices to this device group, and select the devices by clicking on the respective check box(es). Click OK to complete adding the required devices.





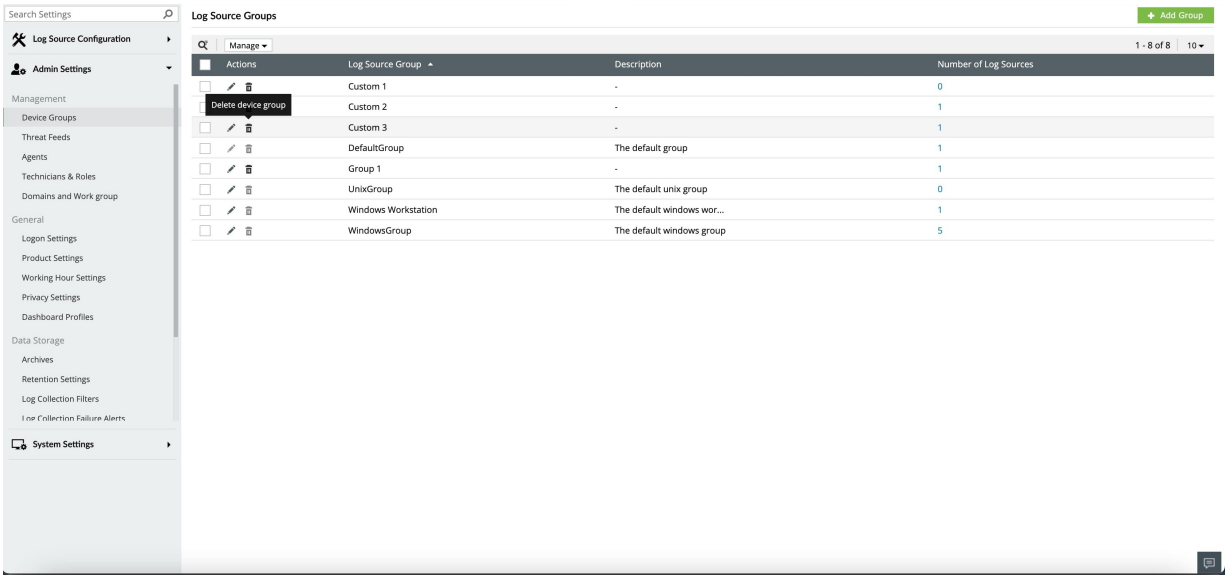
6. Click the Add button to create the device group with the devices listed.

How to edit a device group?

On the table row of a specific device group, Update icon is available to edit the selected device group. Here, you can edit the Group Name, Description, and Device List.

How to delete a device group?

On the table row of a specific device group, the Delete icon will delete the selected device group.



Device Groups

In the Device Groups table, all the device groups added to EventLog Analyzer are displayed with description and number of devices.

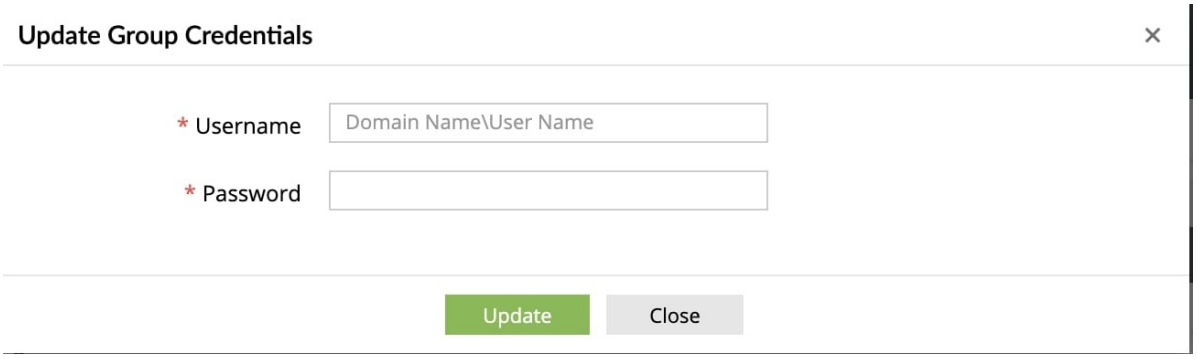
By clicking on the number under the Number of Devices link, you can view all the devices present in the device group.

The More Options drop down menu allows you to:

- Change Monitor Interval



- Update Credentials



9.1.3. Archive

Last updated on: September 12, 2025

In this page

Viewing Archived Logs

Loading Archived Files

Deleting Archived Files

How to configure group based/device based archive settings

View configured Policy

Edit the priority of the policies

Check to which policy applies to a specific device

How to check the server status and storage occupied?

Archive troubleshooting cases

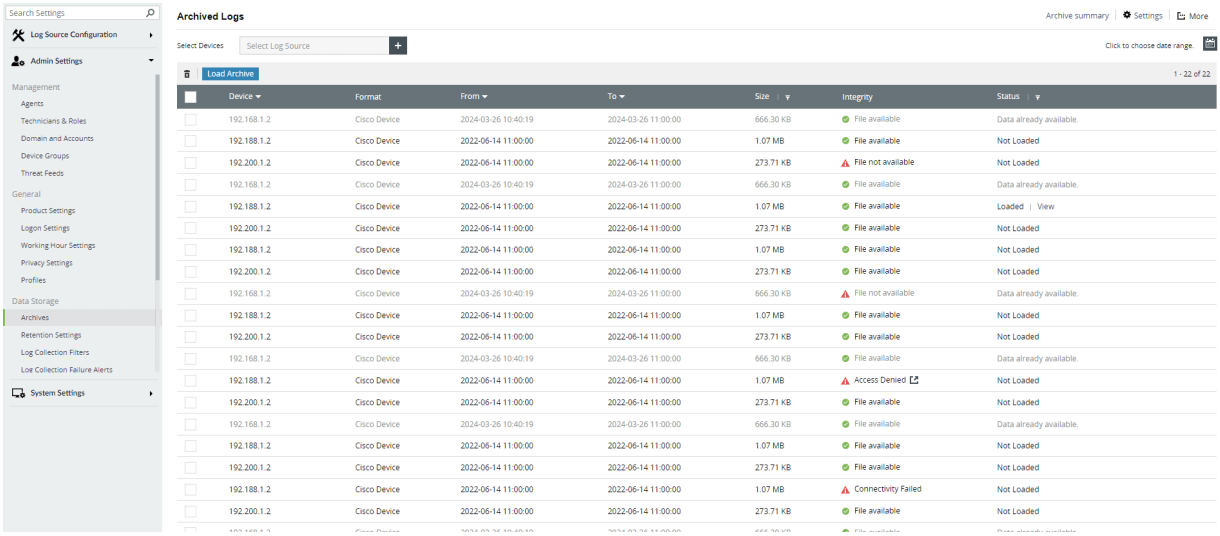
The log files processed by EventLog Analyzer are archived periodically for internal, forensic, and compliance audits. You can configure the following as per your requirements:

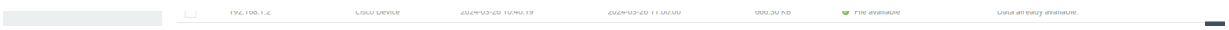
- Archiving interval
- Type of logs that need to be archived
- Storage location of the archived files
- Retention period

The archived files can be encrypted and time-stamped to make them secure and tamper-proof.

How to view archived logs ?

To view your archived log data, go to the Settings tab in EventLog Analyzer and navigate to Admin Settings > Data Storage > Archives





The Archived Logs page contains the following information:

- Device - List of devices from which the logs are being collected
- Format - Device type
- From and To - The time frame denotes the time period during which the logs were collected and archived by EventLog Analyzer.
- Size - Size of the archived log data collected from each device.
- Integrity - The integrity of the archived files, whether they are intact or have been tampered with, is denoted by the following states:
  - Verified - Archived logs are intact.
  - Archive file is missing - When the flat file is not found during the compression/zipping process.
  - Archive file not found - When an archived file is not available in the location where it was originally stored in the DB.
  - Archive file is tampered - When the original archive file is edited/some part of the file is deleted externally.

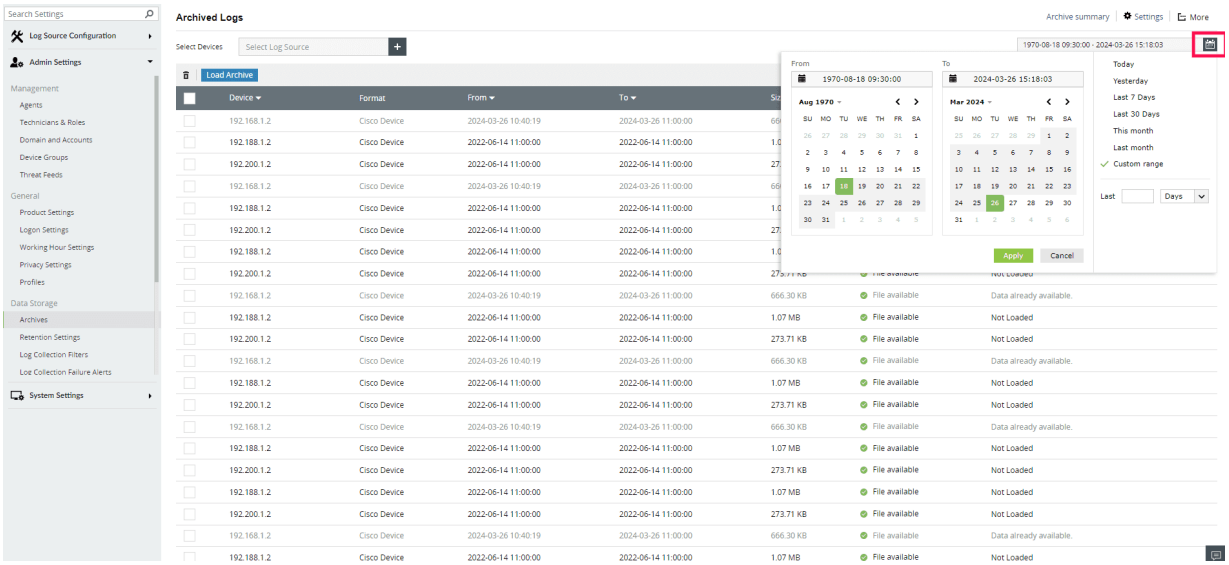
    > **Note**
    >
    > In case a file has been deleted or tampered with, an email notification will be sent immediately containing the message "Archive file is tampered".

  - Archive file available - When the archive integrity check is disabled, both the verified and tampered files will carry this status.
  - Archive file not available - When the archive integrity check is disabled and the archive file is either missing or not found in the original location, this status will be shown.
  - Access Denied - When the remote location can't be accessed where the archives are stored
  - Connectivity failed - When the Amazon S3 bucket is not accessible due to network connectivity where archives are stored
- The status of the archival is indicated by the following four different states:
  - Loaded - The archived files are already loaded to the database. Click View to view the file
  - Data already available - If the archive file is in Elastic Search database
  - Data partially available - If some of the archive data is in ElasticSearch database
  - Not Loaded - If the archive file is not in ElasticSearch database.
  - File yet to be uploaded - If the archive file is not transferred to the specified zip location

How to view a specific archival file?

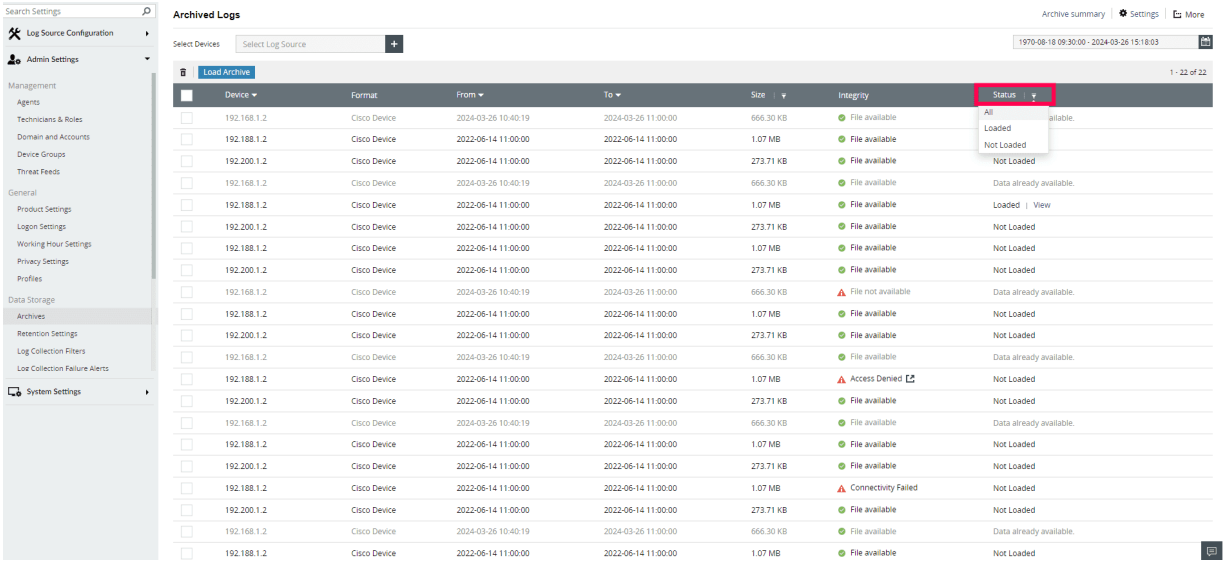
- To view a specific archival file, click on the check box corresponding to Device.
- To view the log files that were archived during a specific time, click on the calendar icon in the top right corner

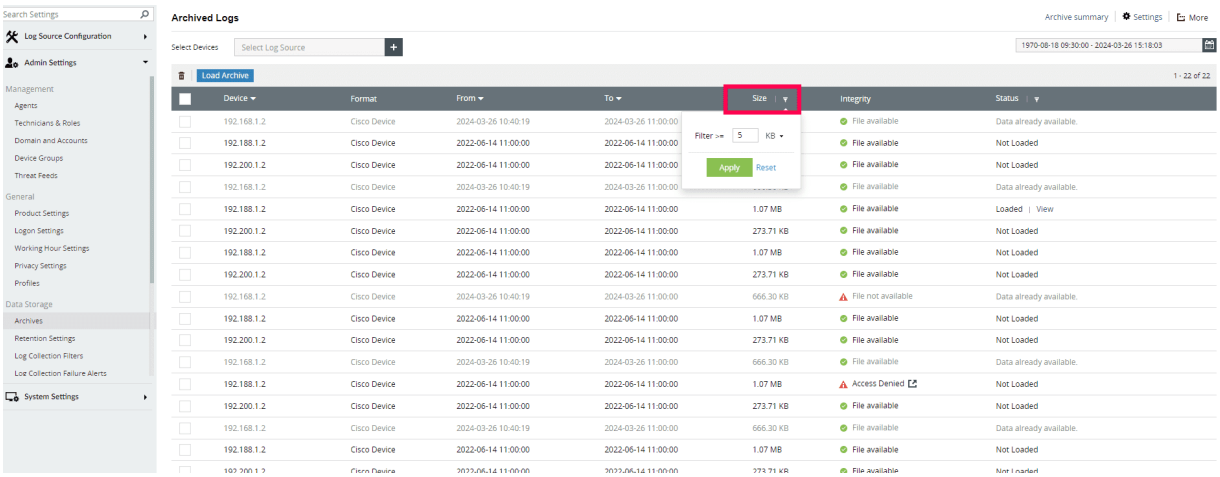
of the page and select the desired period.

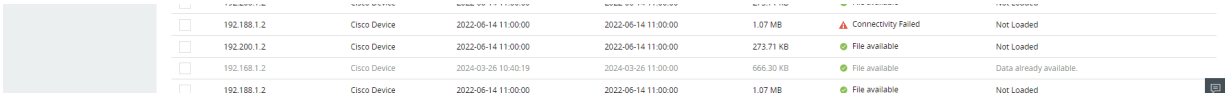


How to filter and view a set of archive files?

To view files based on the size or status of the archive data, click on the filter icon next to Size or Status and set the appropriate values. The files will be filtered based on the given values.

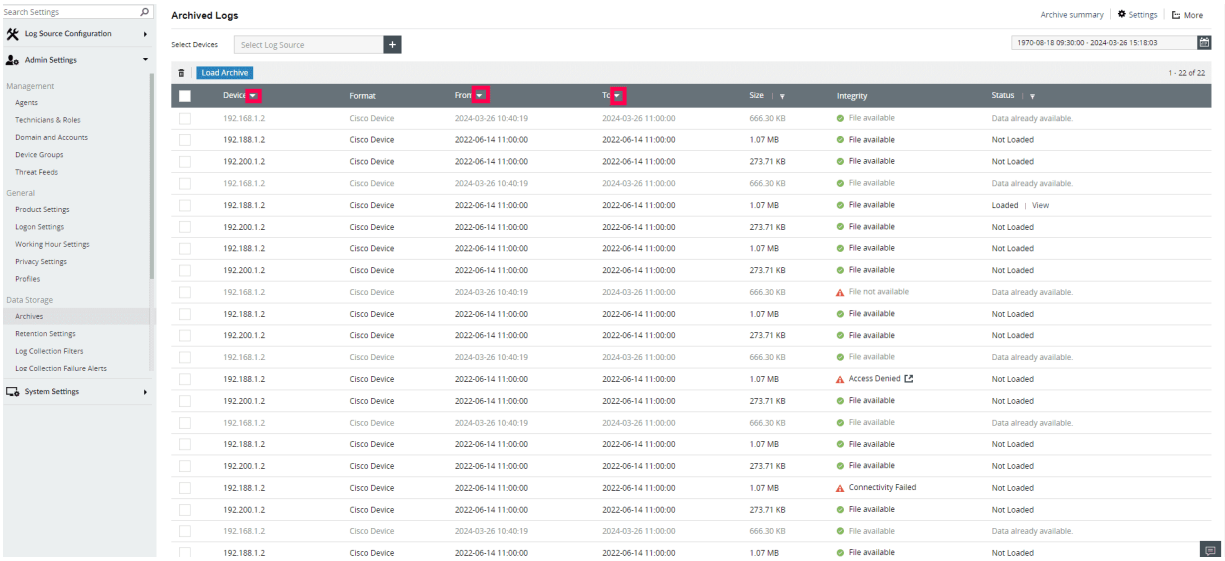






How to sort the list of archive files?

Click on the drop down icon next to Device/From/To, to sort the list in ascending order based on the respective column values. By clicking again, the list will be sorted in descending order.

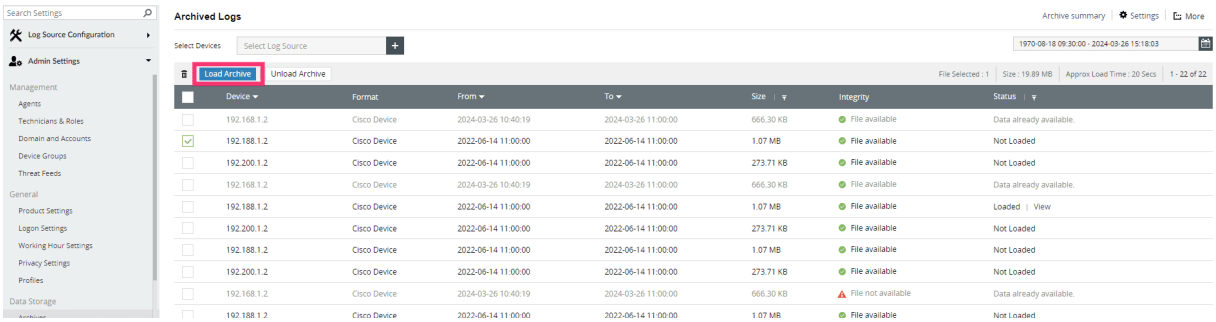


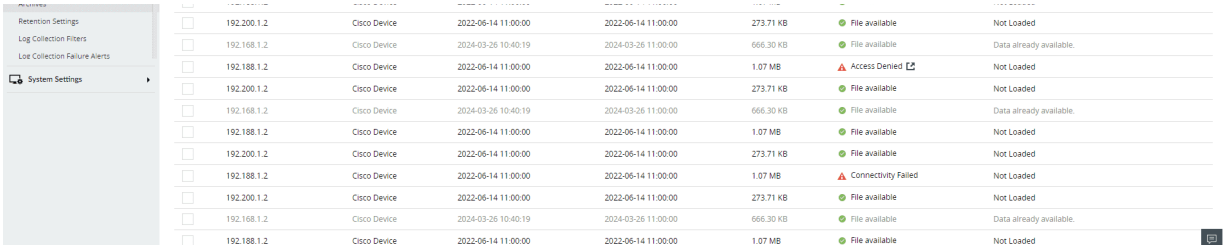
How to load archive files?

To load your archived files, go to the Settings page in EventLog Analyzer and navigate to Admin Settings > Data Storage > Archives

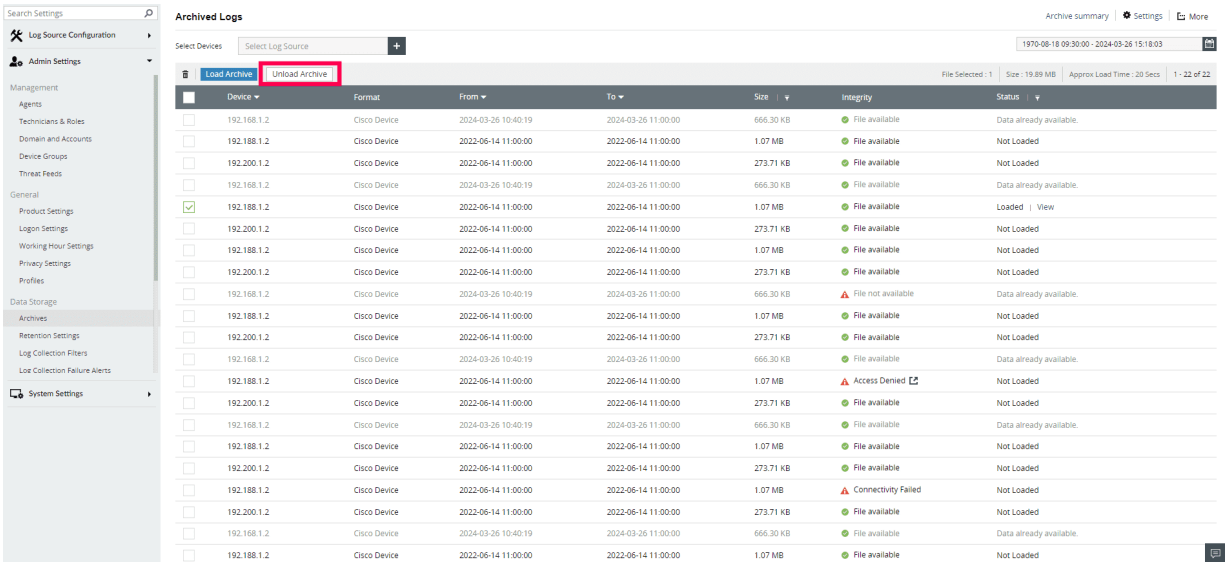
1. Check the status of the archived file corresponding to the device. If it shows Not Loaded, click on the Load Archive button to load the files to the database.
2. Once the status of the file changes to Loaded, click on the corresponding View button to view the files.

> **Note**
>
> Archives stored in shared storage and S3 buckets will be downloaded to local storage and loading will be initiated.

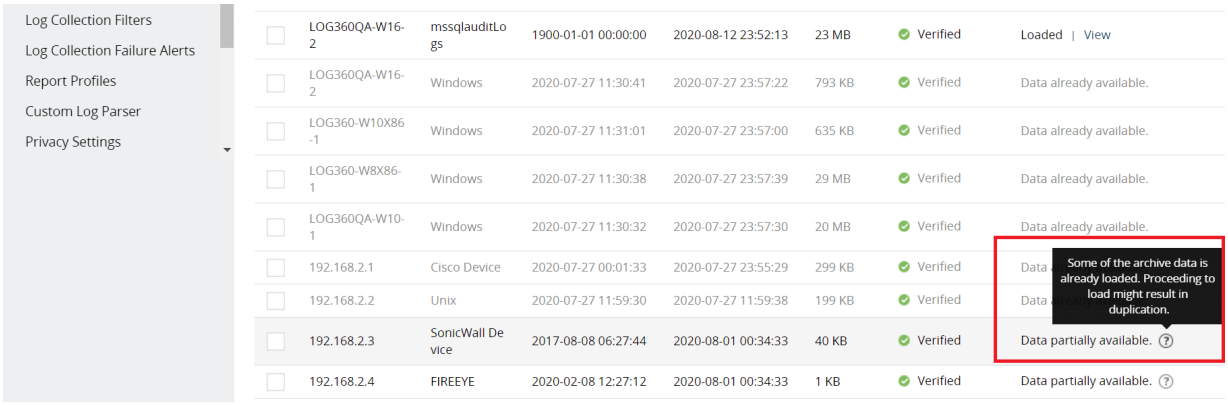




> **Note**
>
> To unload a file, select the file and click on the Unload Archive button.



> **Note**
>
> If the status of the file says Data partially available and if you proceed to load the archive, there could be a duplication of the data.

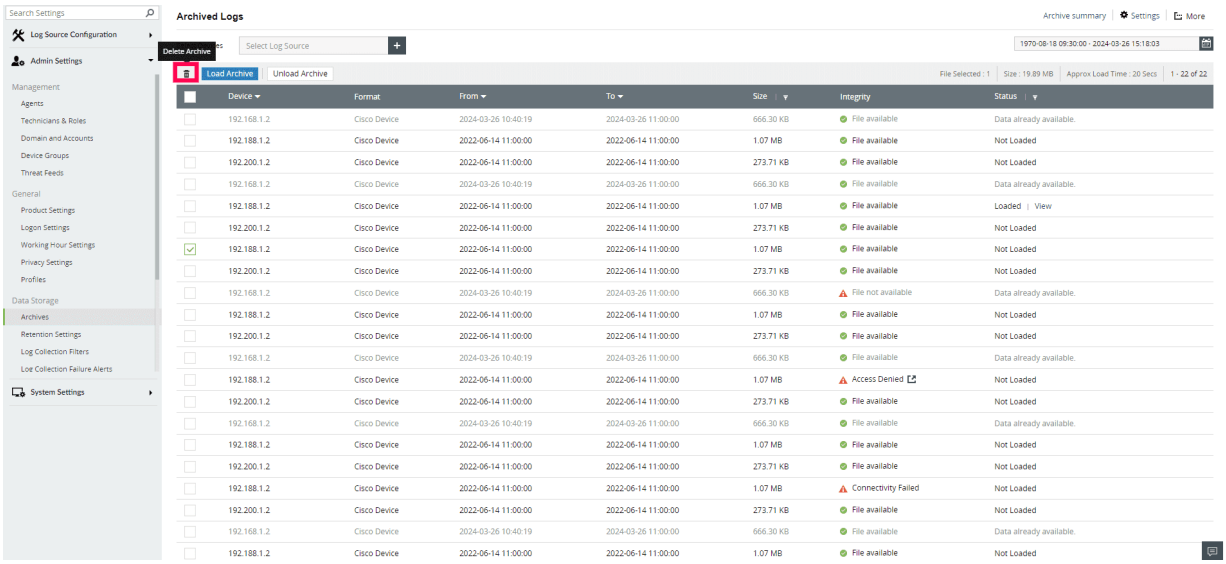


How to delete archive files ?

To delete your archived files, go to the Settings page in EventLog Analyzer and navigate to Admin Settings > Data Storage > Archives.

1. Select the archived file(s) by selecting the respective check box(es).
2. Delete the archived file(s) by clicking on the Delete icon.

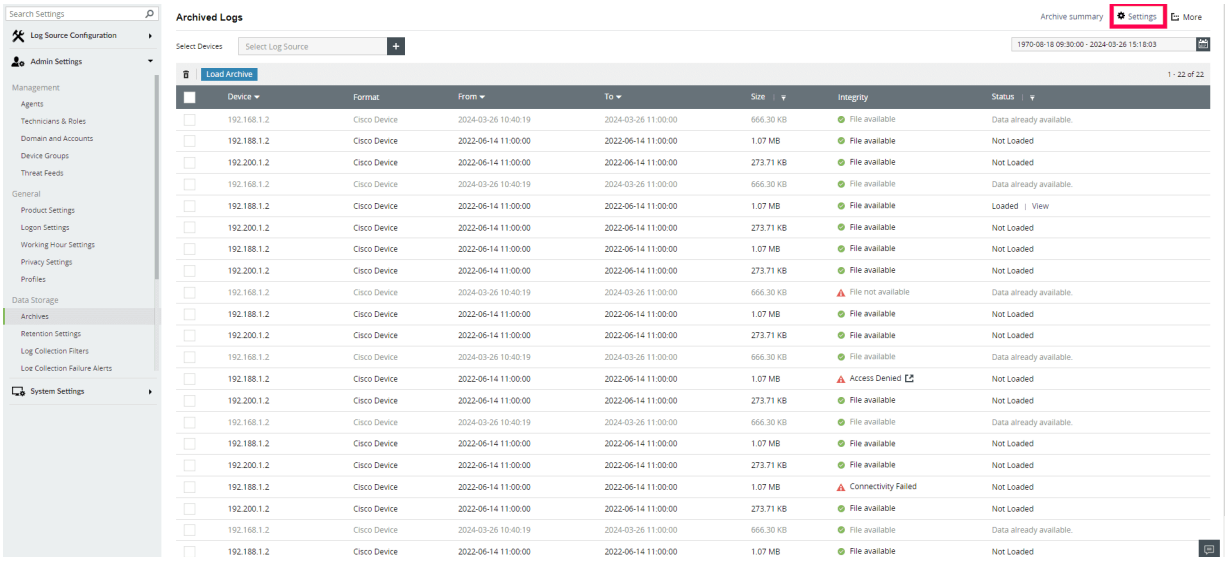
> **Note**
>
> Deleting a host from the manage device page removes corresponding archive entries from the UI, but the physical files remain stored if you need to retrieve them in the future. If these archives are no longer needed, ensure to delete the files manually to free up space.
> Archives that are in yet-to-be-uploaded status can also be deleted. It will delete the file which is stored in the local temp location

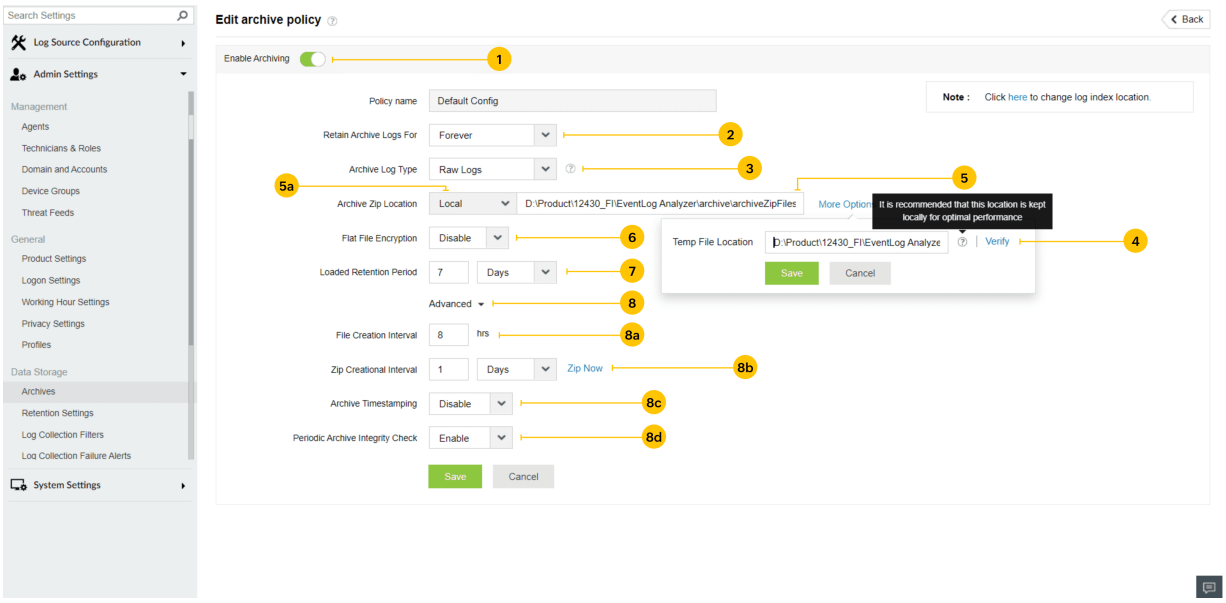


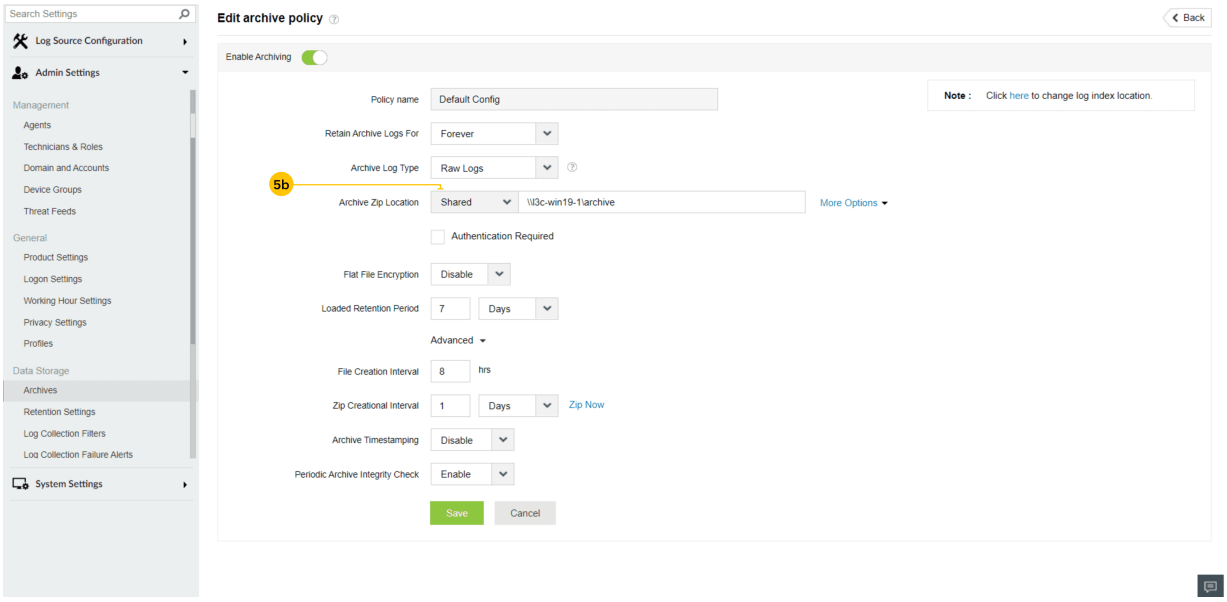
How to configure group based/device based archive settings ?

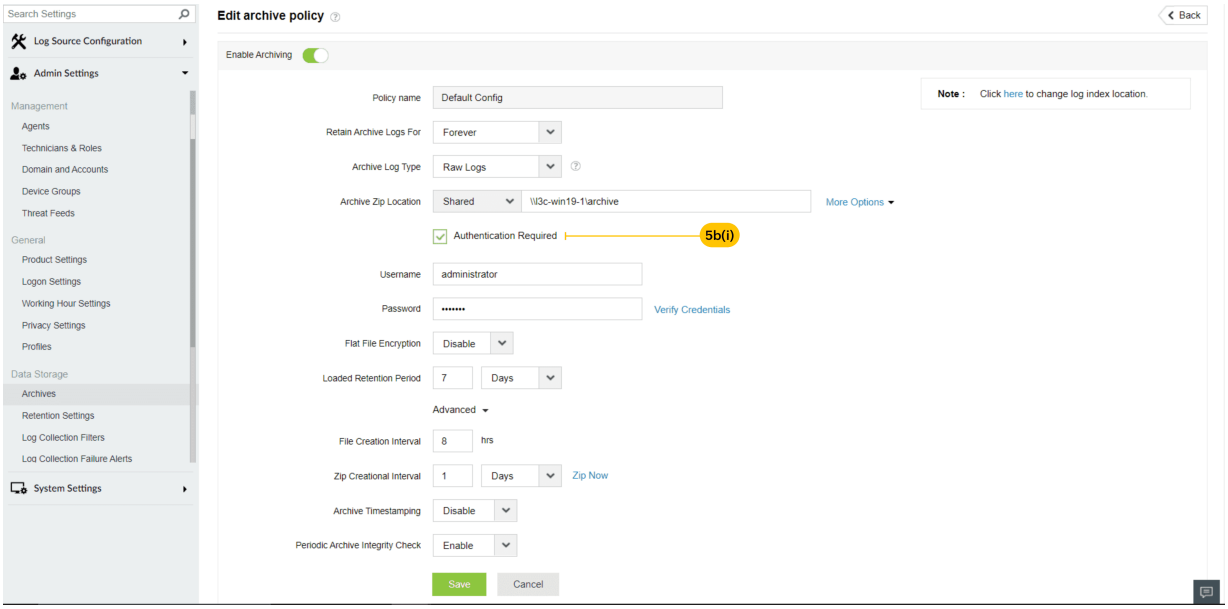
To configure archival settings, click on Settings in the top right corner of the screen.
Configure the archive interval, retention period, encryption, time-stamp of the archive files, location to save the archive files and the index files.

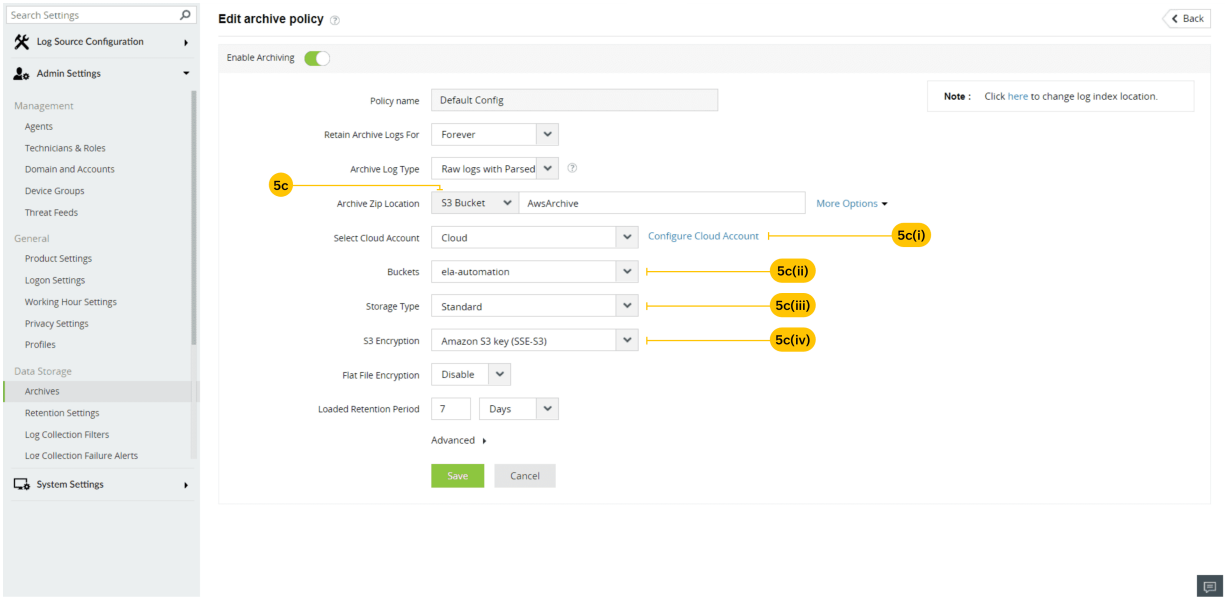
> **Note**
>
> The archive and database storage are asynchronus operations. These operations are unrelated.


Archived Logs
Archive summary
Settings
More
Select Devices
Select Log Source
1970-08-18 09:30:00 - 2024-03-26 15:18:03
Load Archive
1 - 22 of 22
Device
Format
From
To
Size
Integrity
Status
Log Source Configuration
Admin Settings
Management
Agents
Technicians & Roles
Domain and Accounts
Device Groups
Threat Feeds
General
Product Settings
Logon Settings
Working Hour Settings
Privacy Settings
Profiles
Data Storage
Archives
Retention Settings
Log Collection Filters
Log Collection Failure Alerts
System Settings

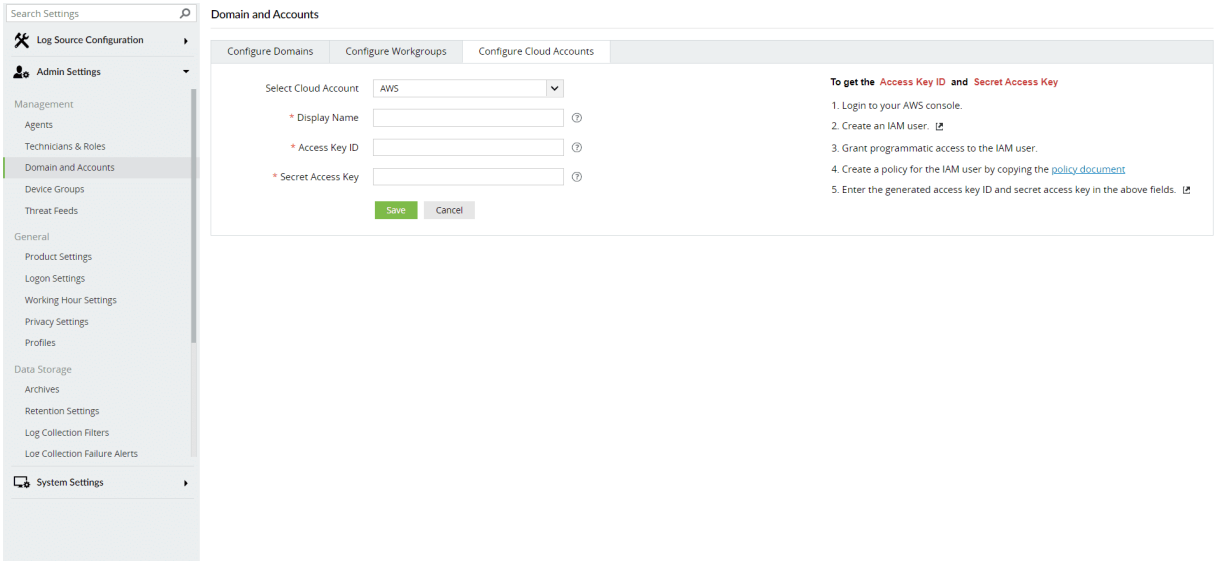

Edit archive policy
Back
Enable Archiving
Policy name
Default Config
Note : Click here to change log index location.
Retain Archive Logs For
Forever
Archive Log Type
Raw Logs
Archive Zip Location
Local
D:\Product\12430_FI\EventLog Analyzer\archive\archiveZipFiles
More Options
It is recommended that this location is kept locally for optimal performance
Temp File Location
D:\Product\12430_FI\EventLog Analyze
Verify
Save
Cancel
Flat File Encryption
Disable
Loaded Retention Period
7
Days
Advanced
File Creation Interval
8
hrs
Zip Creational Interval
1
Days
Zip Now
Archive Timestamping
Disable
Periodic Archive Integrity Check
Enable
Save
Cancel
1
2
3
4
5
5a
6
7
8
8a
8b
8c
8d


Edit archive policy
Back
Enable Archiving
Policy name
Default Config
Note : Click here to change log index location.
Retain Archive Logs For
Forever
Archive Log Type
Raw Logs
Archive Zip Location
Shared
\\l3c-win19-1\archive
More Options
Authentication Required
Flat File Encryption
Disable
Loaded Retention Period
7
Days
Advanced
File Creation Interval
8
hrs
Zip Creational Interval
1
Days
Zip Now
Archive Timestamping
Disable
Periodic Archive Integrity Check
Enable
Save
Cancel
5b





Configure Cloud Account:



1. Ensure that archiving is enabled. By default, it is enabled.Use the toggle button to disable archiving.
2. Enter the Archive retention period for the archived files. The default period is forever.
3. Logs can be archived in two formats - Raw Logs with Parsed Fields and Raw Logs. Logs will be stored with metadata on selecting the former, and without metadata for the latter.

> Note
>
> The storage space for Raw Logs will be lesser but only basic reports can be generated using this data.

4. Enter the storage location for Flat file location in the Temp File Location field.Click on Verify to validate the location.

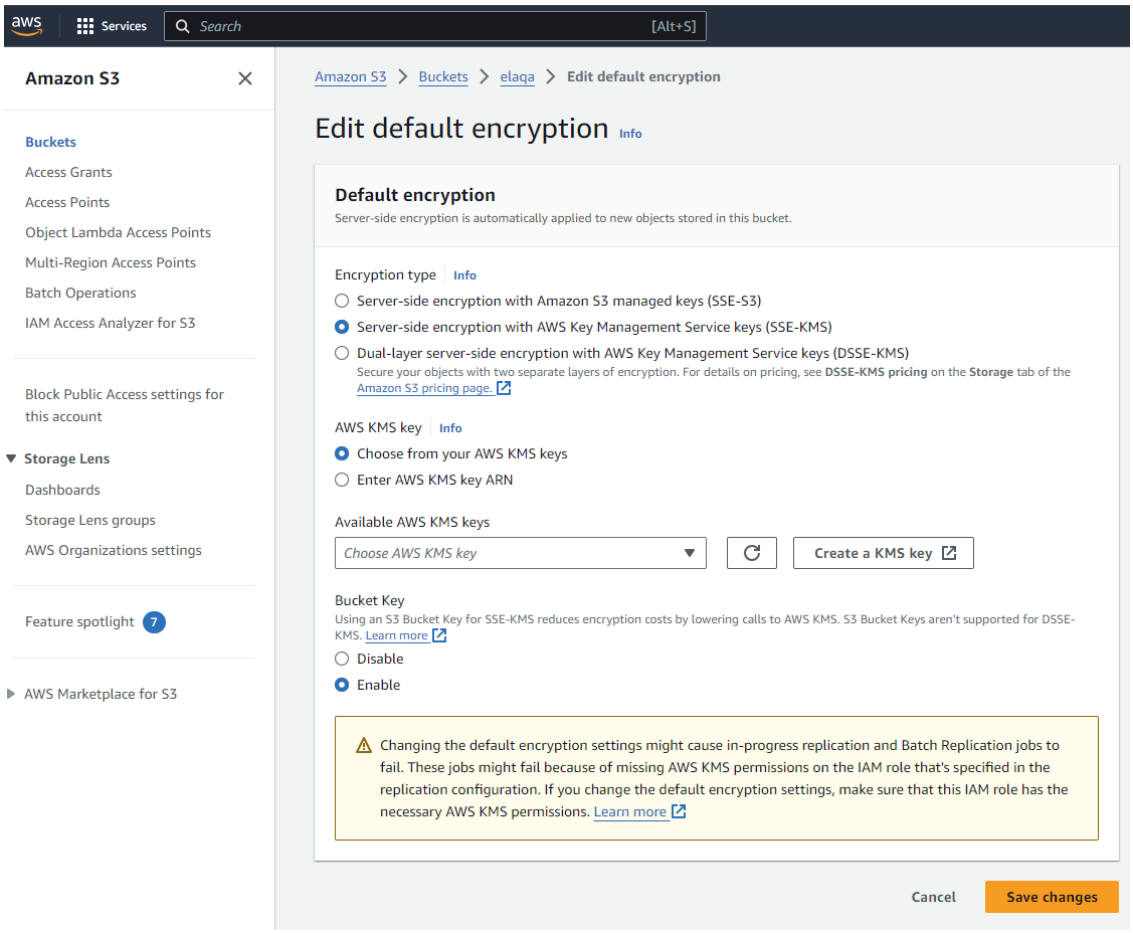
> Note
>
> : By default, the location is set to local for optimal performance.

5. Enter the storage location for the archived files in the Archive Zip Location field.
    1. Local - To store archives in a local location, choose local from the dropdown and enter the storage location
    2. Shared - To store archives in a shared location, select 'Shared' from the dropdown menu and enter the storage location.
        - By clicking on the authentication check box, you will need to enter the credentials to access the shared location. Unchecking it would make the path accessible to everyone with share access.
        - Ensure that the remote machine is available and it has sufficient read and write permissions for the share.
    3. S3 Bucket - To store archives in S3 Bucket, choose S3 Bucket from the dropdown and enter the folder name. By default the folder name will be "AwsArchive"
        1. Cloud account - Displays the configured cloud accounts.Select the respective cloud account from the dropdown. To configure the cloud account, click on "Configure Cloud Account" - This will configure AWS cloud account without a cloud trial. To configure the cloud account with cloud trial refer this document.

        > Note
        >
        > Cloud accounts configured through Domain and Accounts or from Archives can only be listed here

        2. Buckets - Displays the configured buckets associated with the respective cloud account. Select the

respective bucket from the dropdown. Ensure that your bucket has the sufficient permissions. To create a new bucket,enter the bucket name in the input field and click on the "+" icon. By default, the bucket type is General Purpose, and it is in home region. Ensure that bucketname follows this naming convention rules, If the archives stored in these buckets are to be encrypted, Ensure that the buckets have " Bucket Key Enabled " permission. By default, KMS keys will be disabled when creating a bucket. To provide the permissions , navigate to Amazon S3 → Buckets → (Bucketname) → Properties → Default Encryption → Bucket Key



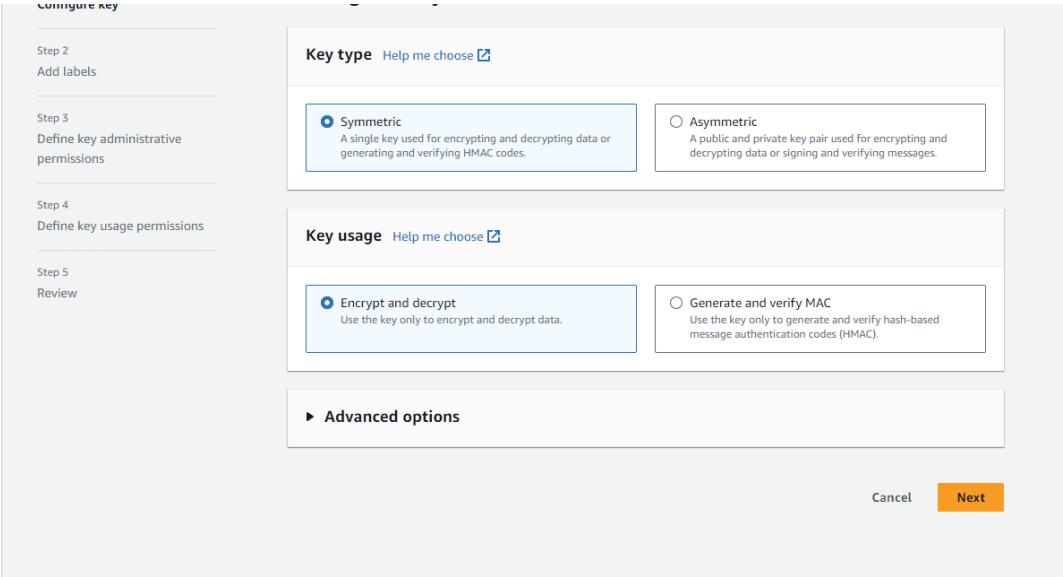
3. Storage Type - Displays the S3 Storage Classes. The default storage type utilized is S3 Standard, which comes at no cost. However, additional storage types include pricing based on the amount of storage utilized. AWS Storage Pricing and Permissions

4. S3 Encryption - Displays the encryptions for the bucket.The default encryption is Amazon S3 managed keys (SSE-S3) as the base level of encryption.

   AWS Key Management Service (AWS KMS) and Dual-layer server-side encryption with AWS KMS keys (DSSE-KMS) can be configured if the respective KMS keys are already present.If no keys are available, you can generate KMS key in the AWS console.
   Creating a KMS Key:

   1. AWS console → Services → All Services → Key Management Service → Create key.





Permissions:

- To list the configured kms keys for your cloud account , provide "kms:ListKeys" policy permission to your IAM user.
- To encrypt the archives using KMS key , provide "kms:GenerateDataKey" policy permission to your kms key (key ARN) . Refer this document for KMS key permissions

Pricing :

There are no additional charges for using default encryption for S3 buckets

For SSE-KMS and DSSE-KMS, AWS KMS charges apply and are listed at AWS KMS pricing.

6. To secure the archival logs, enable flat file encryption. By default, it will be disabled.
7. Enter the log retention period for the loaded archive files. The default period is 7 days.
8. Click on Advanced and fill in the following fields:
    1. Choose the time interval for file creation. The logs will be written to flat files at the specified time period.

> **Note**
>
> The default interval is 8 hours.

    2. Choose the required time interval for creating a zip file. The flat files will be compressed (40:1 ratio) and zip files are created at the specified time period.

> **Note**
>
> The default interval is 1 day.

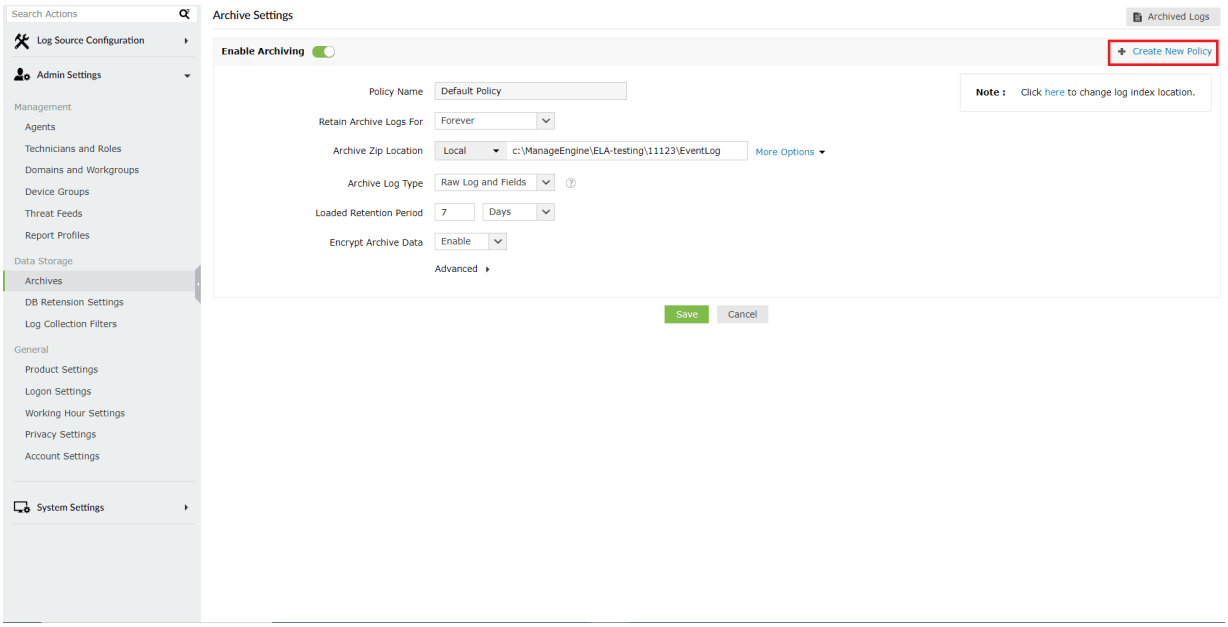
    3. Enable Archive Timestamping if required. By default, it is disabled.
    4. The Periodic Archive Integrity Check is enabled by default.

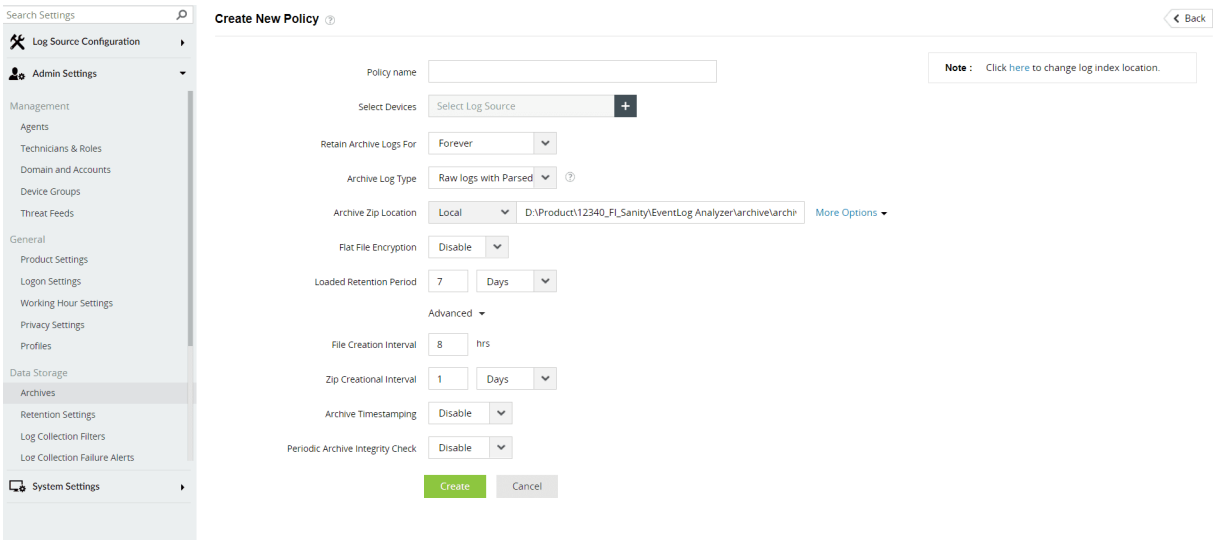
> **Note**
>
> The default interval is 1 day.

9. Save the settings and close the window. For instant archiving, click the Zip Now button next to Zip Creational Interval.

> **Note**
>
> Files will be zipped locally and will be transferred to the destination location, so additional disk space will be required. Ensure that you have sufficient storage in the system(Size).To know about the disk space required in the local storage, calculate using the tuning guide

Configure multiple archive settings by clicking on Create New Policy in the top right corner.

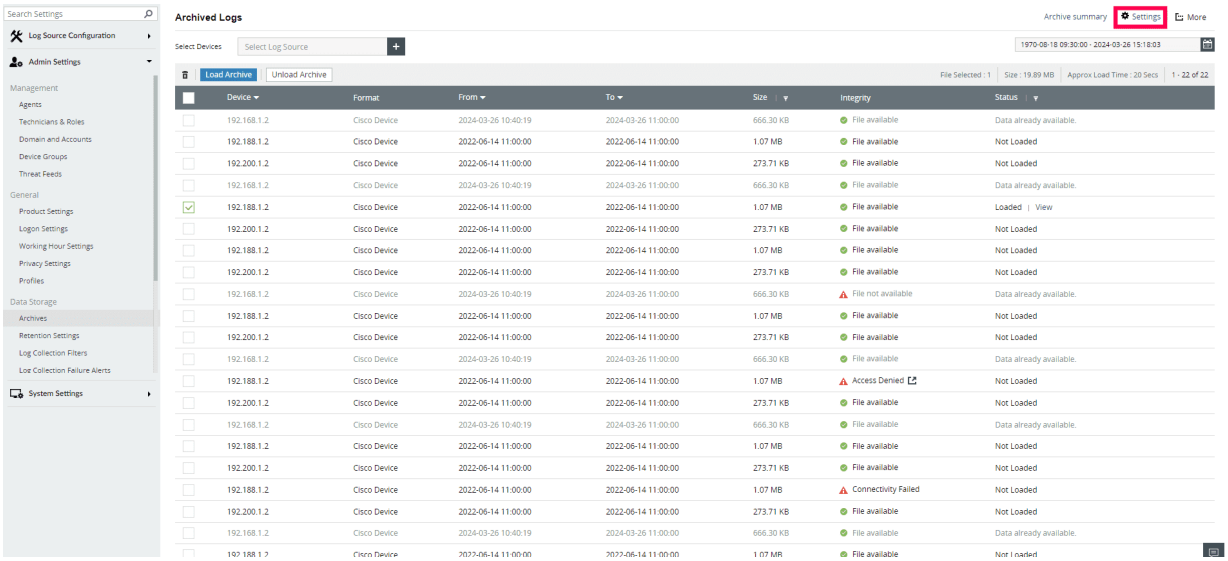


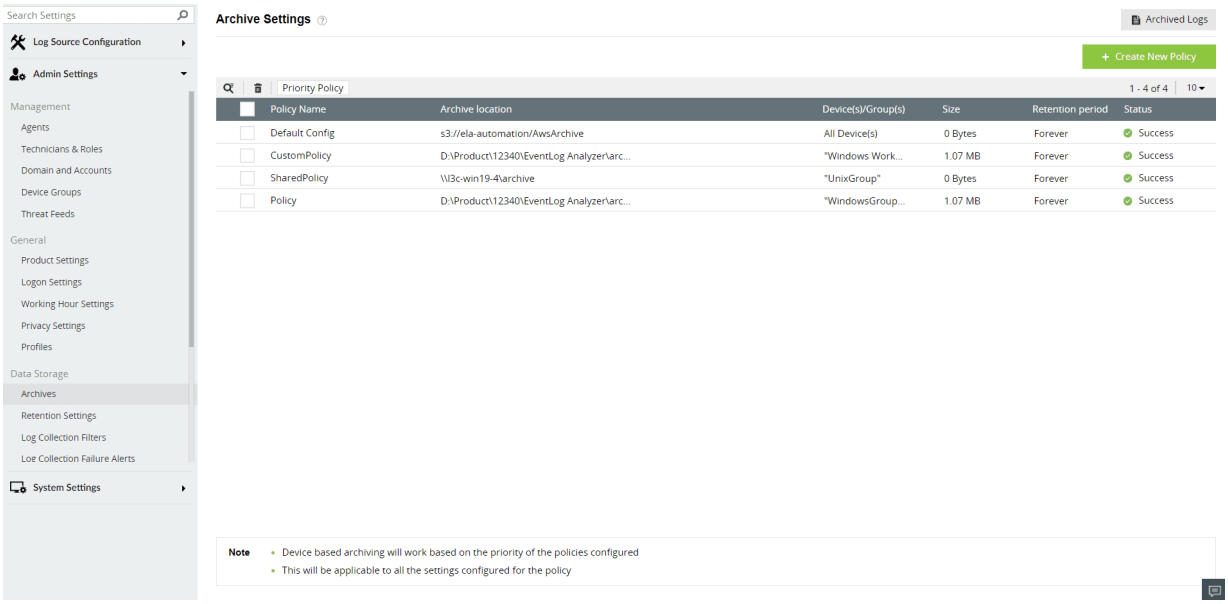


Additional configuration - Select the devices/groups for which the policy will be applied.

How to view configured Policy ?

Click on Settings at the top right corner of the screen. This will lead to the Archive Settings page which contains all the configured policies.

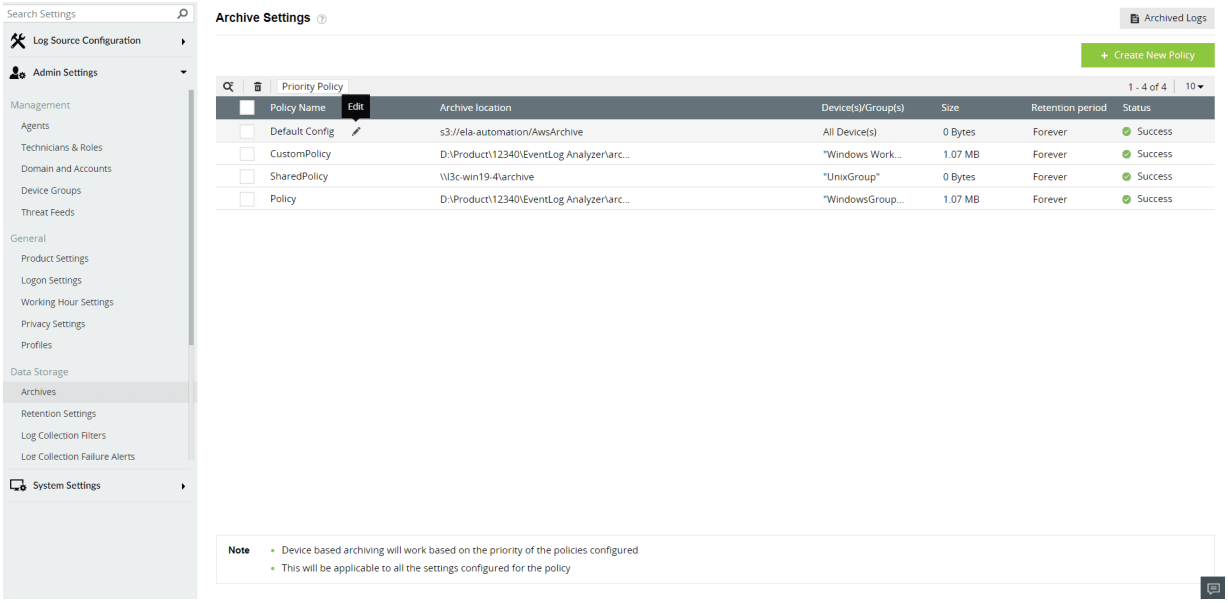




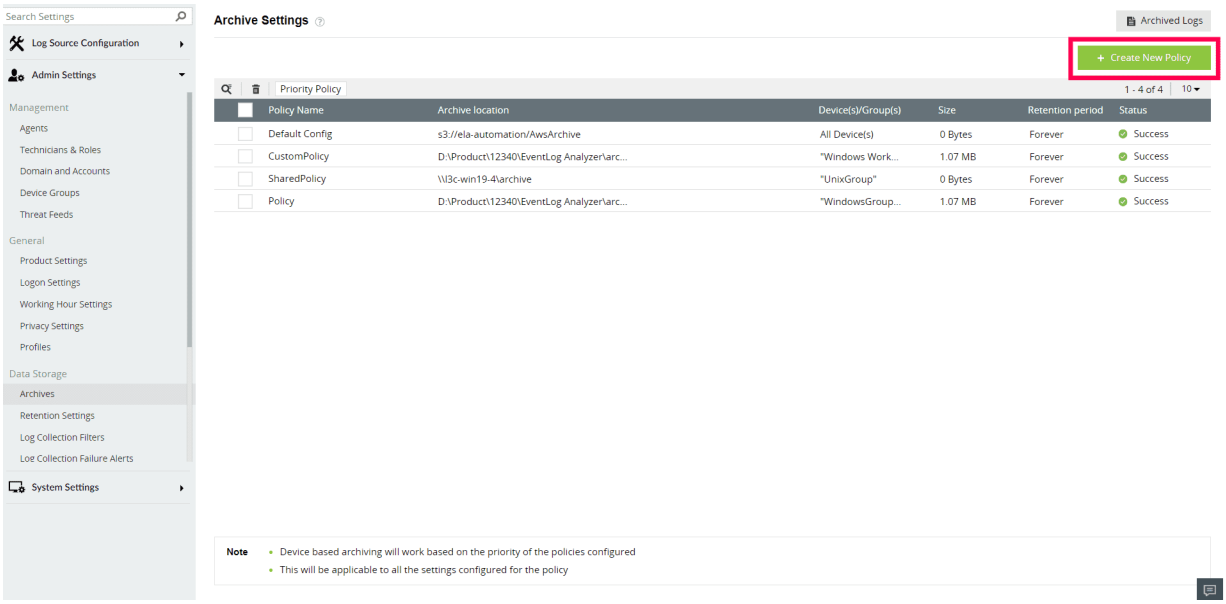
- Policy Name - Specifies the name of the policy.
- Archive Location - Shows the zip location of the policy.
- Devices/Groups - Shows all the devices and groups added in the policy.
- Size - Total size of archive of all the devices/groups added in the policy.

- Retention period - Log retention period of the policy.
- Status - Shows the status of the archival. The status will either be Success or Archiving Disabled.

Click on Edit by hovering on the policy to edit the configured settings.



You can also add a new policy by clicking on the Create New Policy button in the top right corner in archive settings page.

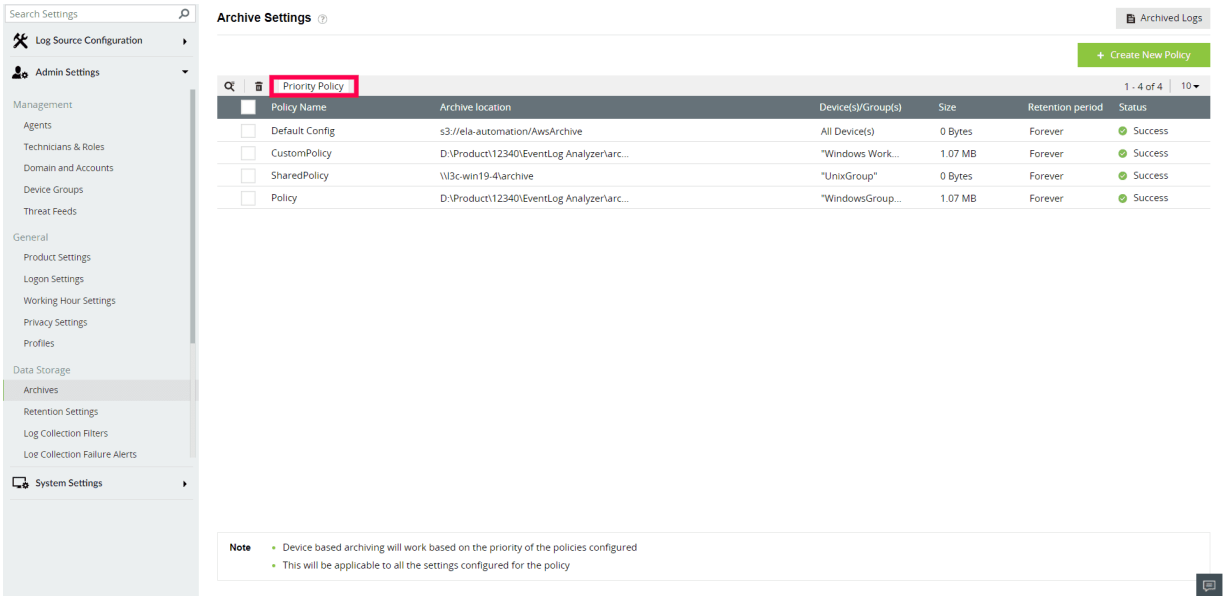


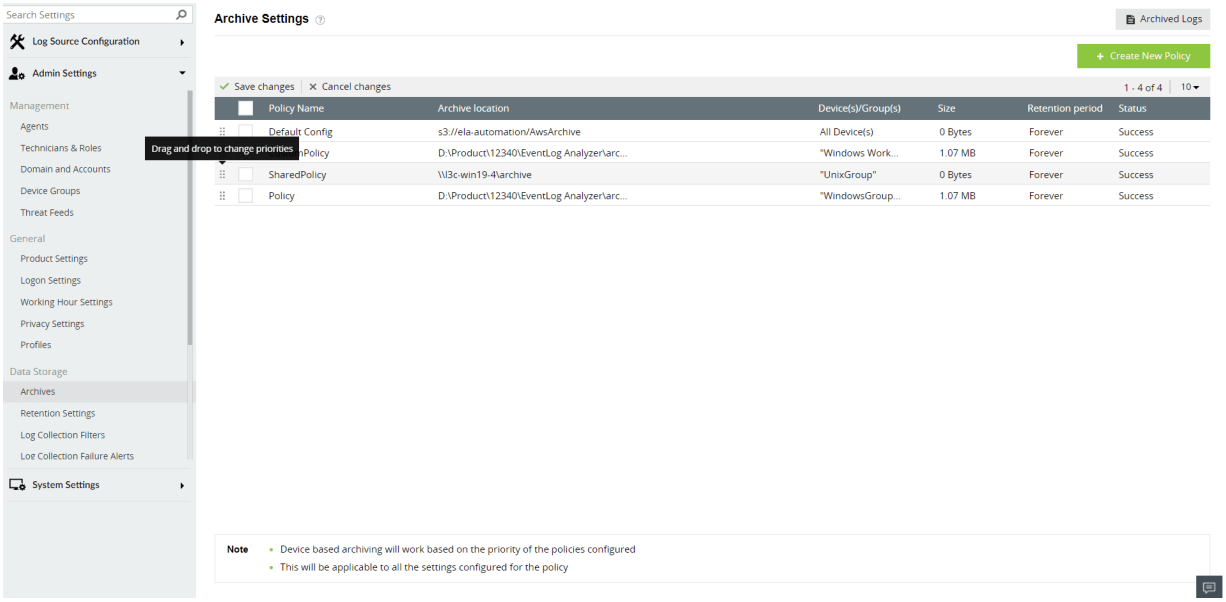
How to edit the priority of the policies?

To change the priority of the policies, click on Priority Policy, rearrange the policies by dragging and dropping them, and save.

Note

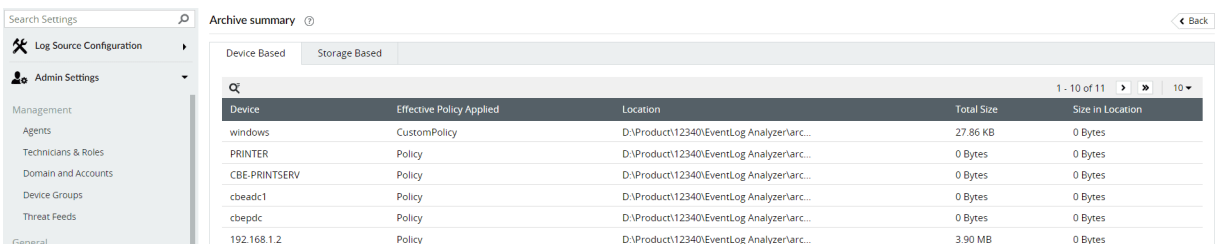
If a device/group has been added under multiple policies, the archive settings of the policy with the highest priority will be applied to that particular device/group.

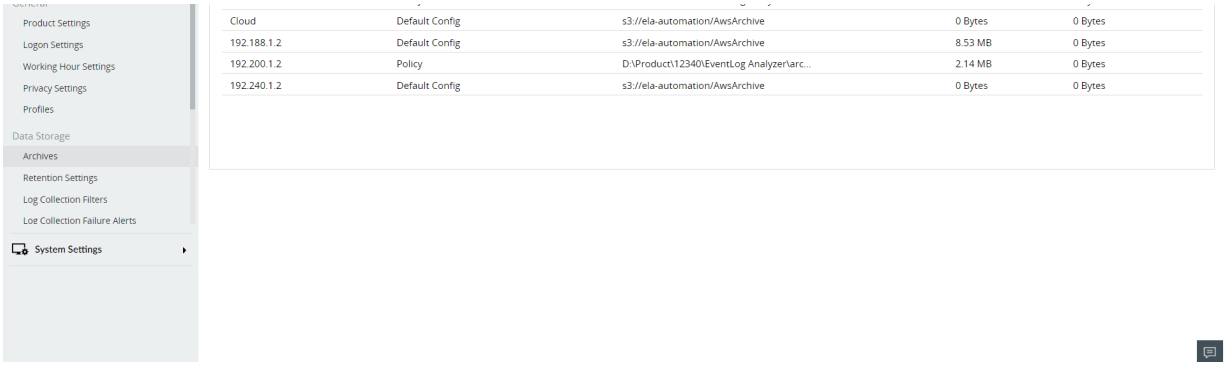




How to check to which policy applies to a specific device?

In the Settings tab of EventLog Analyzer, navigate to Admin Settings > Data Storage > Archives > Settings > Archive Summary



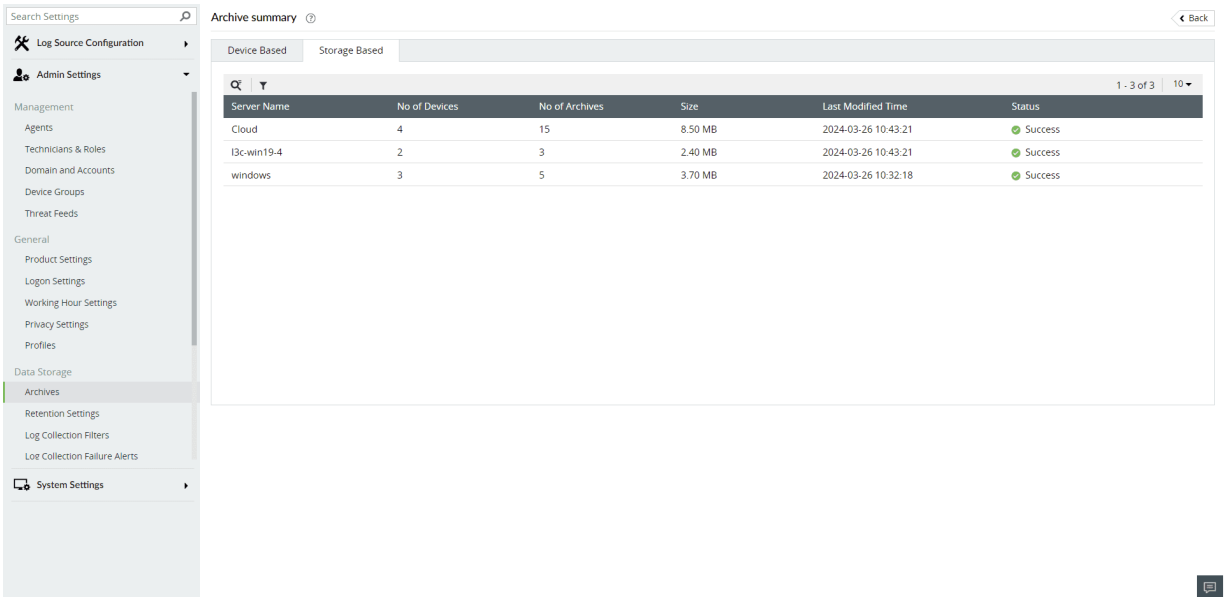


- Device - Shows the list of devices that are added in one or more policies
- Effective Policy Applied - Shows the policy which is applied to that particular device.
- Location - Shows the zip location of the policy.
- Total size - Shows the total size of archives for that particular device.
- Size in location - Shows the size of the device archives collected under that specific policy.

How to check the server status and storage occupied?

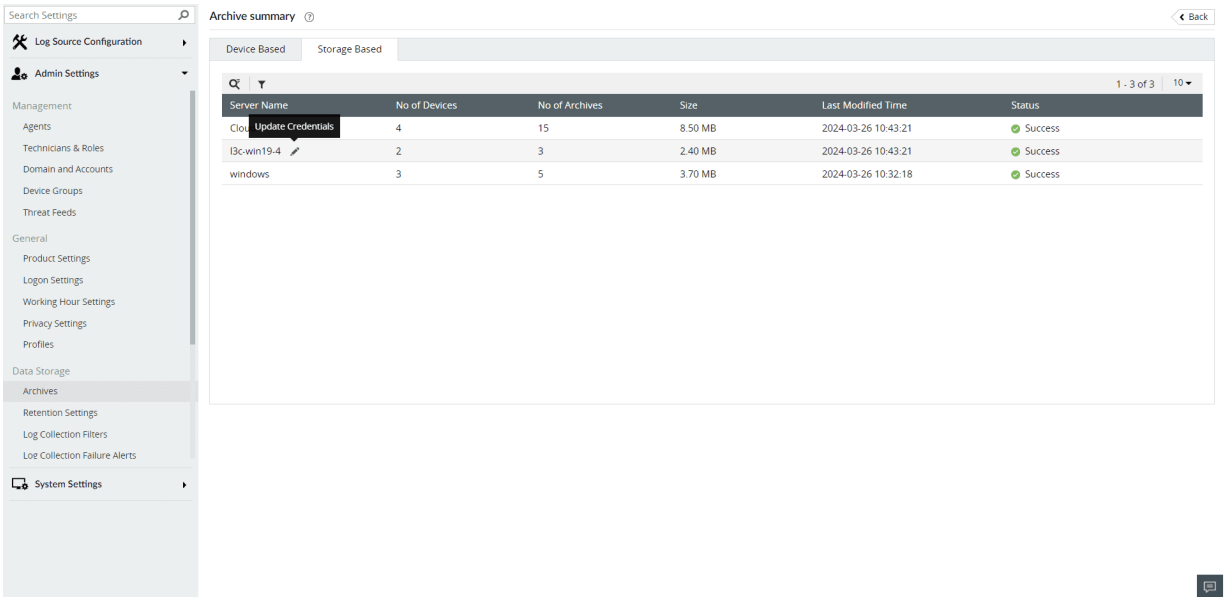
Storage Summary:

In the Settings tab of EventLog Analyzer, navigate to Admin Settings > Data Storage > Archives > Archive Summary > Storage Based

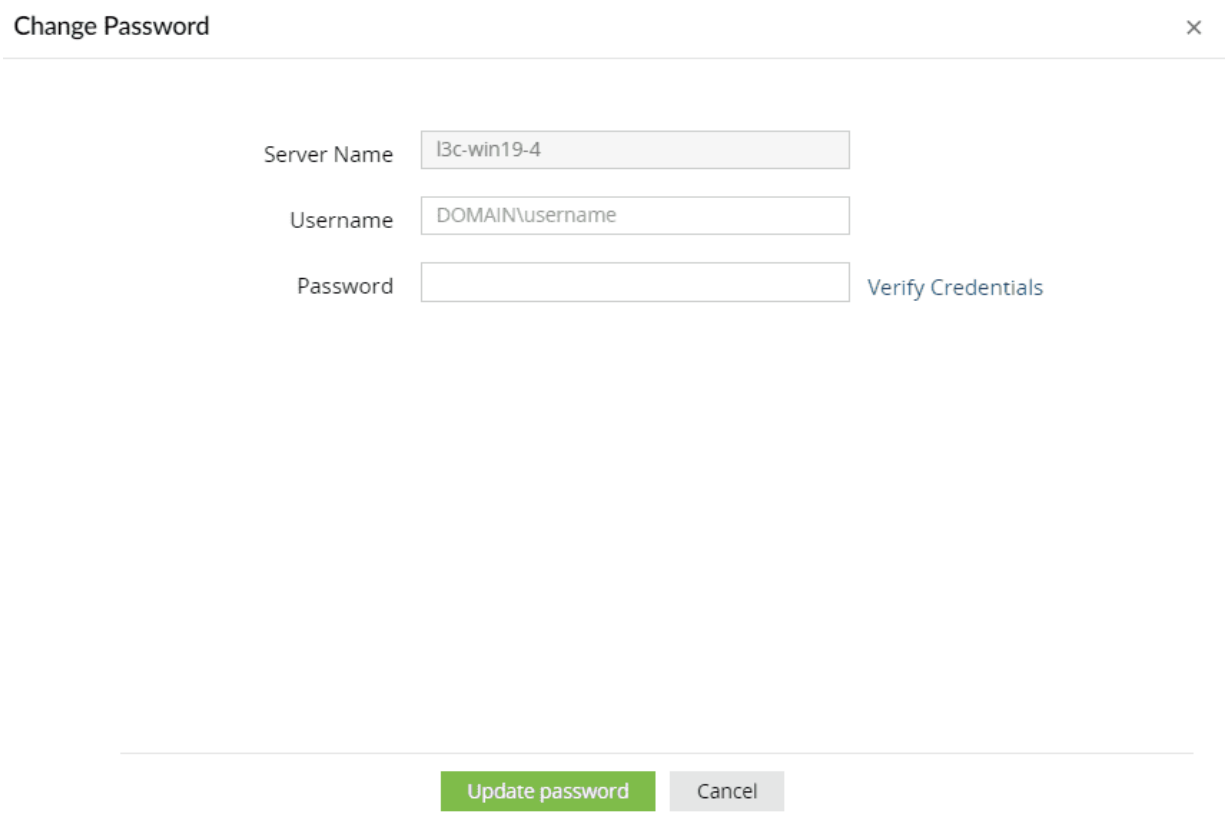


- ServerName - Displays the list of servers configured in archive policies and archives
- No of Devices - Displays the number of devices associated with the server
- No of Archives - Displays the no of Archives present for the respective server
- Size - Displays the total size of the archives in the server
- Last Modified Time - Displays the Last password updated time for the server

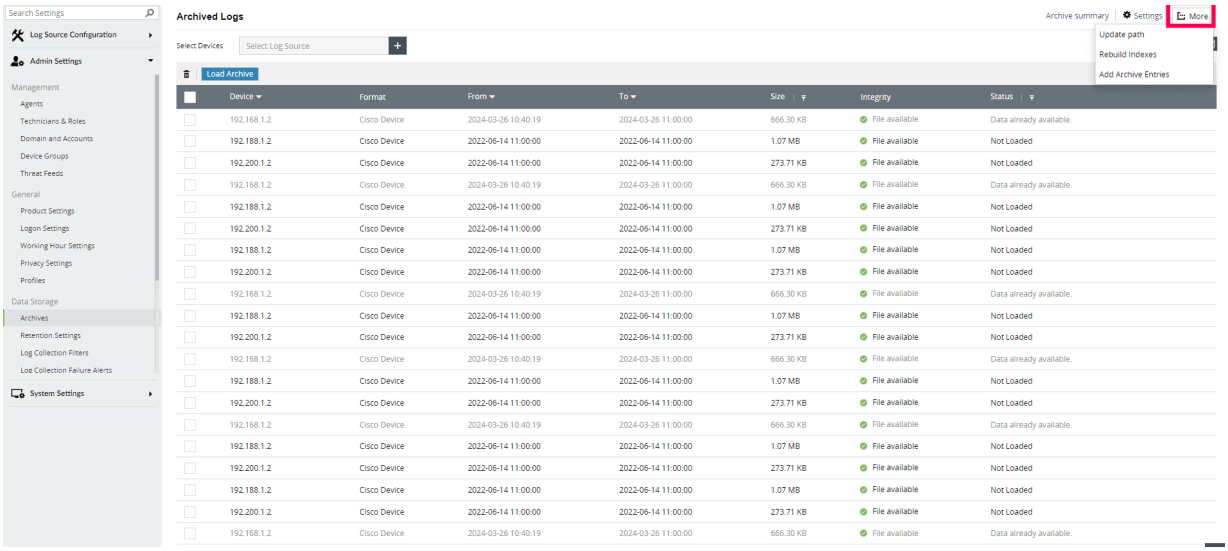
- Last Modified Time - Displays the Last password updated time for the server
- Status - Displays the reachability status of the server
  - Access Denied - When the server is unavailable or it doesn't have the necessary permissions
  - Connectivity failed - When the cloud is not reachable due to internet disconnection
- Edit icon - Update Credentials - Update the new credentials in case of password change for the server (Applicable only for shared server)



Update the username and password for the server



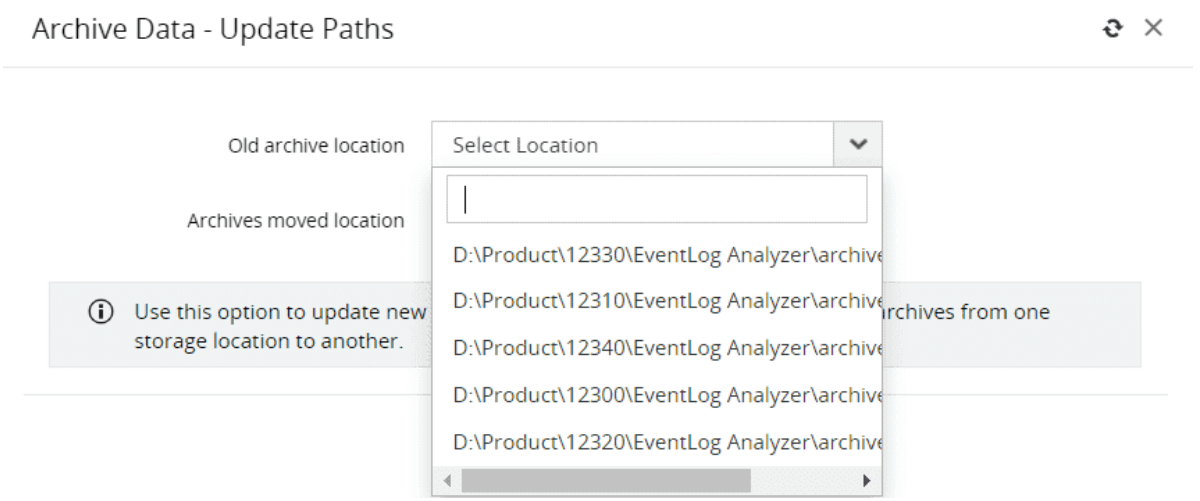
Archive troubleshooting cases



1. Update path

   - Goto Settings > Admin Settings > Data Storage > Archives > More in the top right corner > Update path
   - Select the old archive location in the dropdown and enter the new location where archives are moved or present in Archives moved location and click on Update.

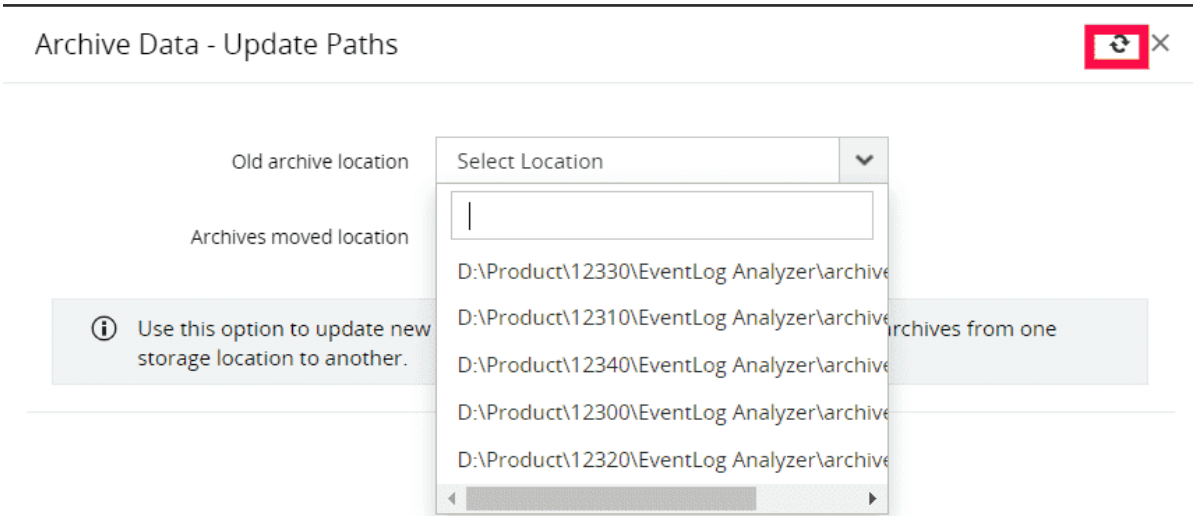
> **Note**
>
> : Update path is only applicable for local and shared locations



2. Update archive file integrity

   - Goto Settings > Admin Settings > Data Storage > Archives > More > Update path.
   - Click the refresh button in the top right corner to update the integrity status of the files.

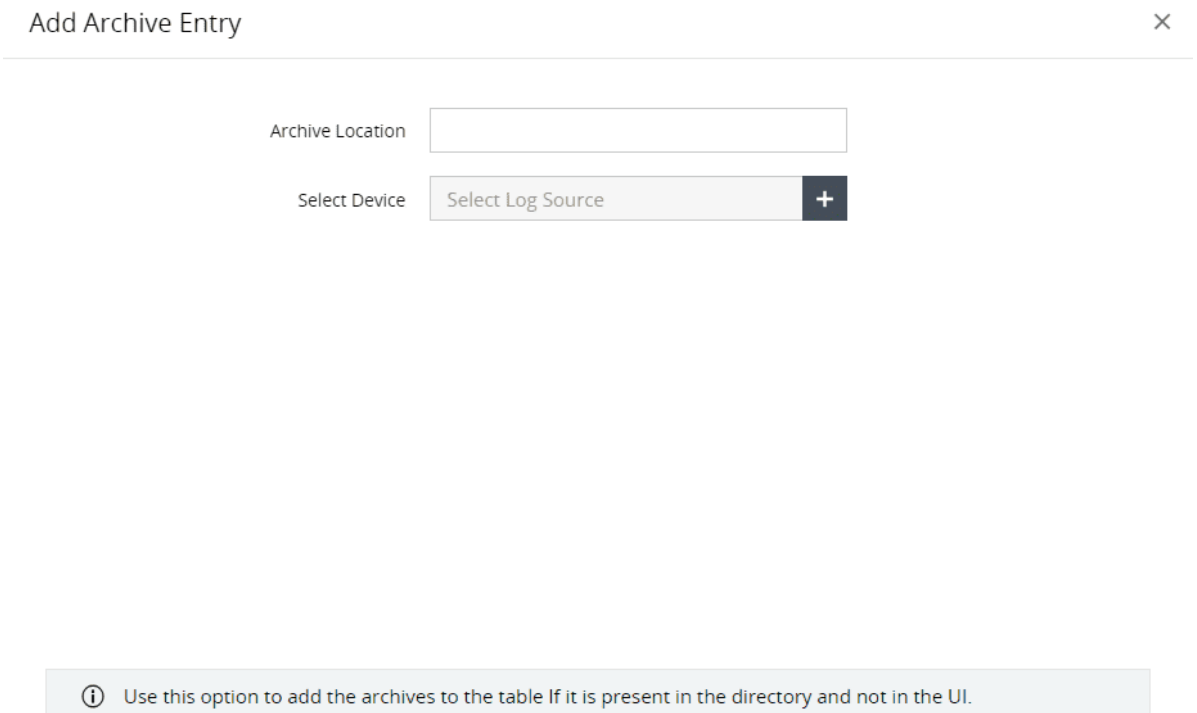
The File not Found status will change to Verified, if the file is present in the directory as specified in DB. This will also change the status from Tampered Files to Verified.
Integrity Status like Access denied and Connectivity failed will be updated to Verified, if the file is present in the respective location

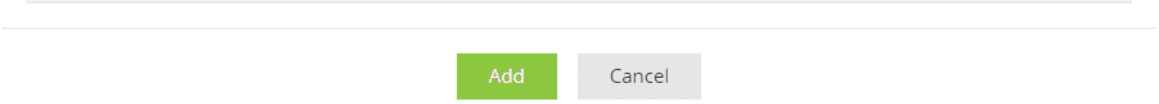


3. To add archives in DB

- Goto Settings > Admin Settings > Data Storage > Archives > More > Add Archive Entries .
- Enter the location where the archives are present.If needed, select Device and add the archives of a particular device.

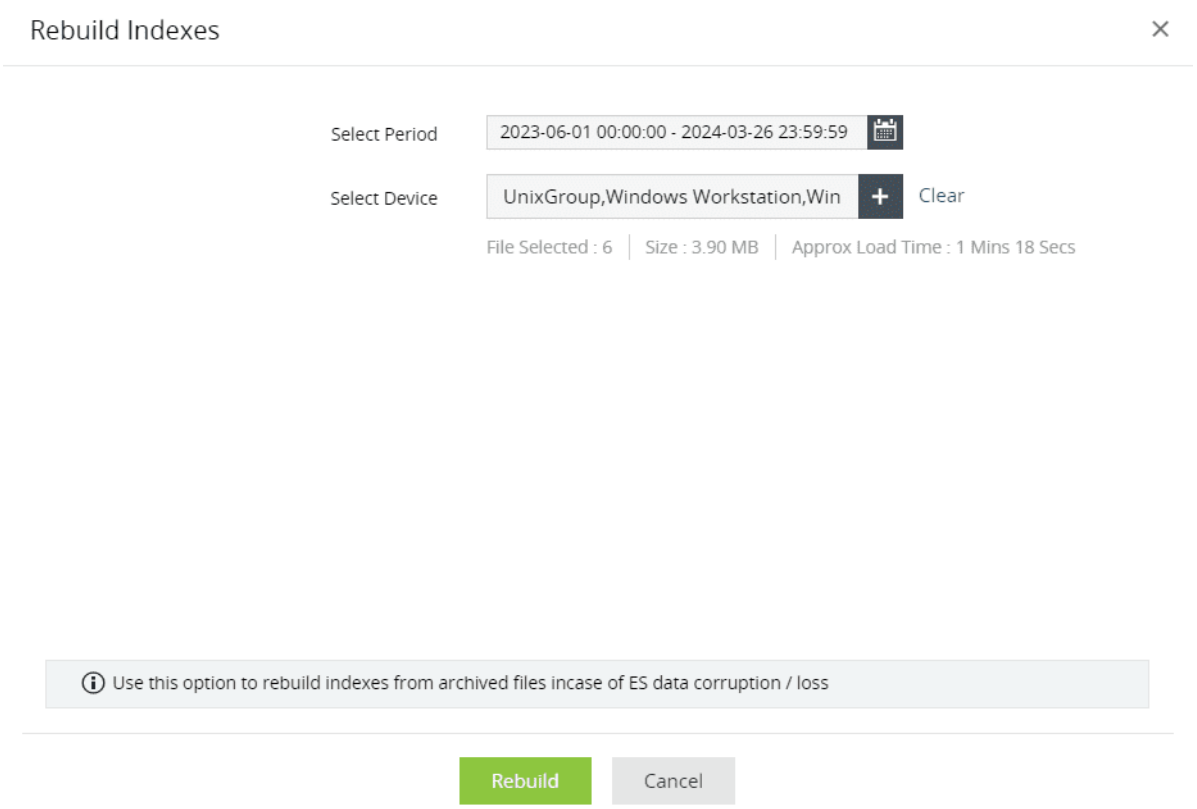
> Note
>
> : Add Archive Entry is only applicable for local and shared locations





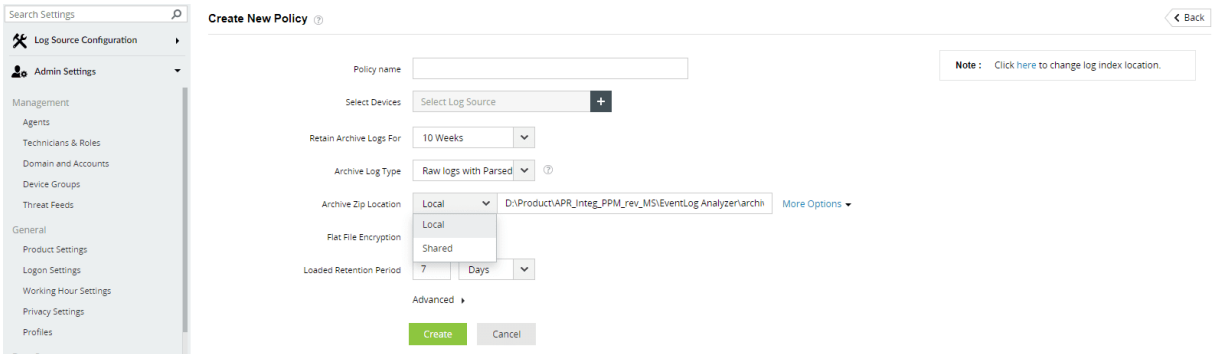
4. If ES/data lost or corrupted

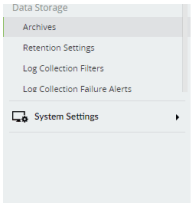
- Goto Settings > Admin Settings > Data Storage > Archives > More > Rebuild Indexes.
- Select the date range and the device for which the logs need to be indexed in ES from Archives.Click on Rebuild.



Centralized Archiving:

If centralized archiving is enabled in the Admin Server. In that case, the S3 bucket option will not be displayed for new policies in Manage Server. For existing S3 bucket configured policies, file transfers will continue to upload in S3 locations. Files will be downloaded locally and then transferred to the Admin Server. Ensure that you have sufficient storage, also make sure to change the location to local if centralized archiving is enabled for optimal performance.




Data Storage
Archives
Retention Settings
Log Collection Filters
Log Collection Failure Alerts
System Settings

9.1.4. Privacy Settings

Last updated on: September 12, 2025

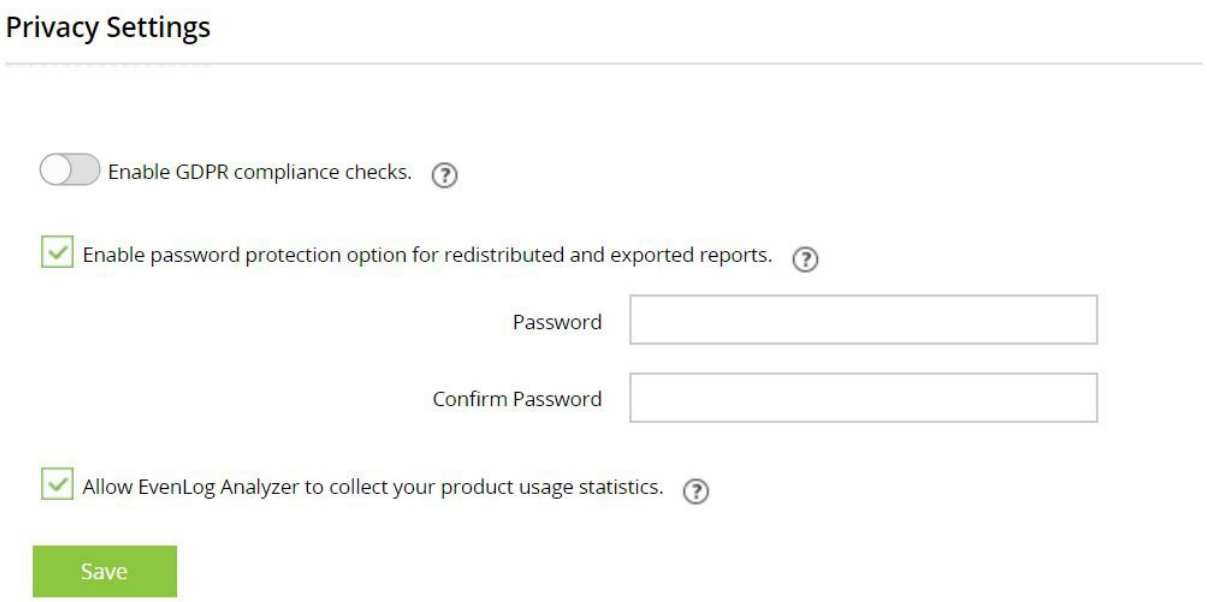
In this page

GDPR configuration settings.

Password protection settings for exported reports.

Product usage statistics collection settings.

Using Privacy Settings, you can enable or disable the GDPR configuration settings, enable or disable password protection for exported reports and allow or deny permission for EventLog Analyzer to collect your product usage statistics.



GDPR Configuration settings.

To enable or disable the GDPR configuration settings,

1. Go to Settings > Admin Settings > Enable GDPR compliance checks.
2. Click on Save.

Password protection settings for exported reports.

To enable password protection for exported reports,

1. Go to Settings > Admin Settings > check on the "Enable password protection option for redistributed and exported reports" checkbox.
2. Enter the desired password in the "Password" and "Confirm Password" box.

3. Click on Save.

To disable the password protection for exported reports,

1. Go to Settings > Admin Settings > uncheck on the "Enable password protection option for redistributed and exported reports" checkbox.
2. Click on Save.

Product usage statistics collection settings.

To allow or deny permission for EventLog Analyzer to collect your product usage statistics,

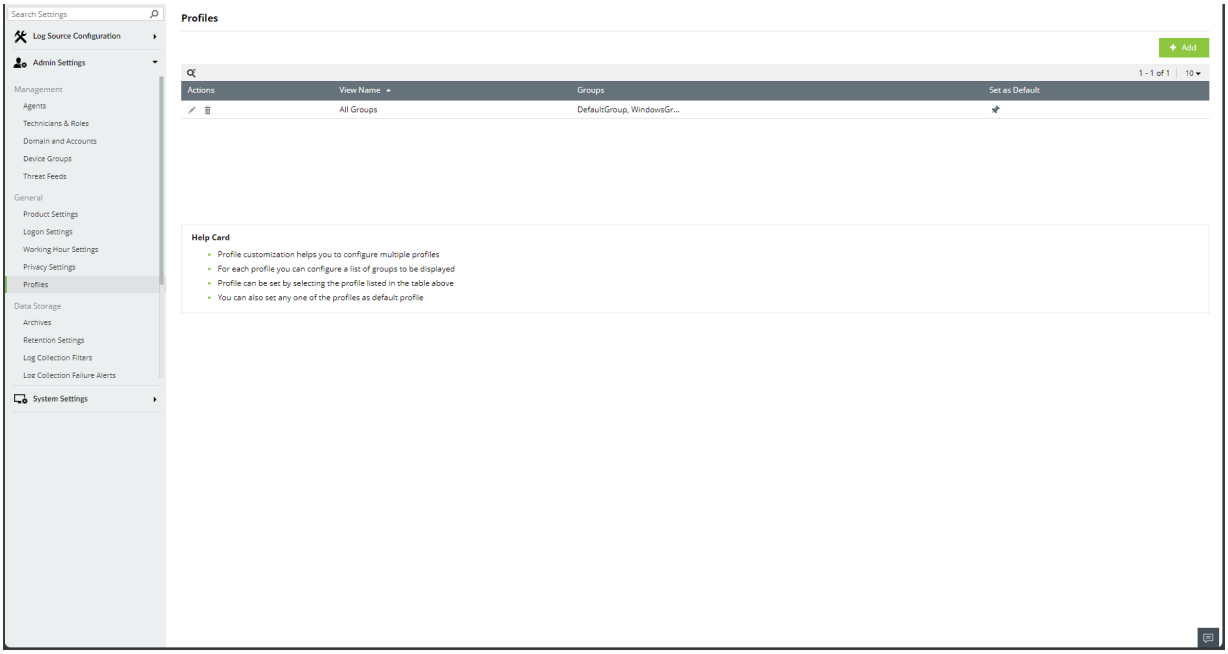
1. Go to Settings > Admin Settings > check or uncheck the Allow EvenLog Analyzer to collect your product usage statistics checkbox and click on Save.

9.1.5. Profiles

Last updated on: September 12, 2025

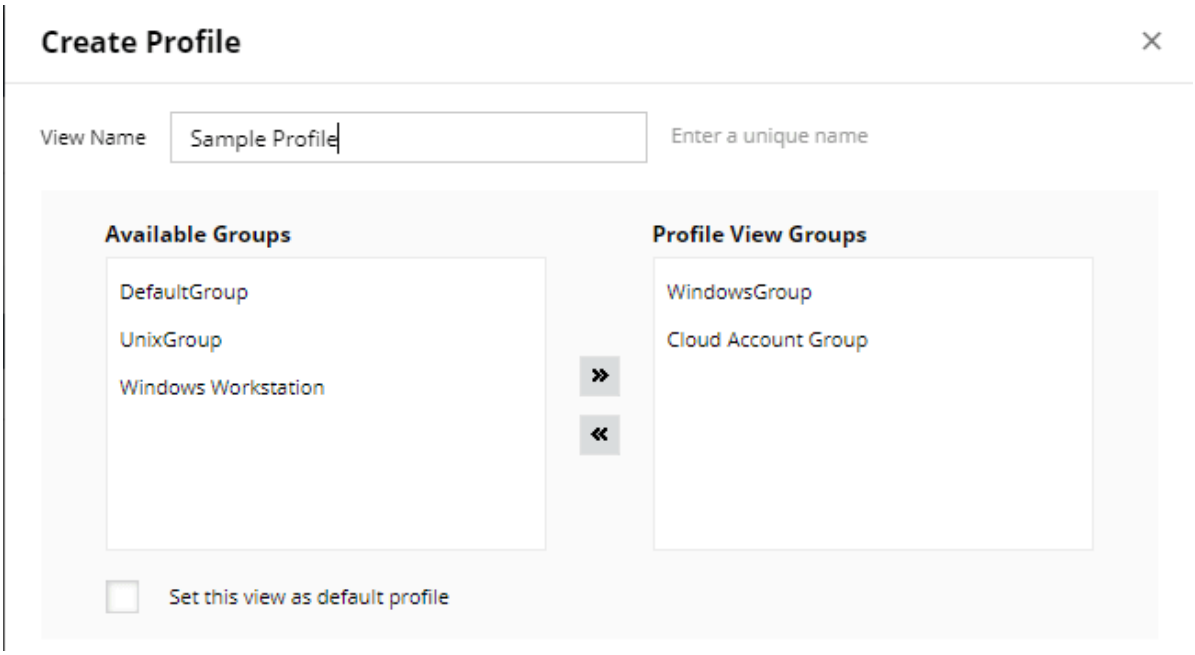
EventLog Analyzer gives you the option of selecting the default devices whose logs will be used to populate the module. The profiles allow you to accumulate devices groups into profiles and select one of them as the default profile to form the basis of the product.

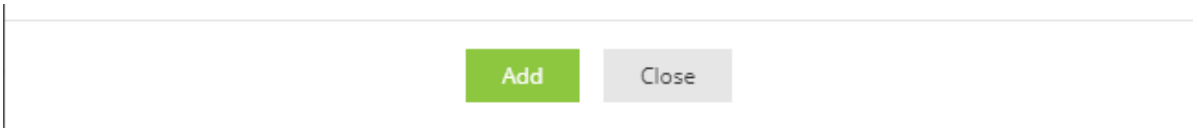
To view, create, edit, or delete profiles, navigate to Settings > Admin Settings > General > Profiles. You can see a list of existing profiles.



Creating profiles

- Click Add at the top of the page.





- Enter a name for the profile and select the groups that should constitute it. To know how to add a new device group, click here.
- If you want to set that as the default profile, check the Set this view as default profile box.
- Finally, click Add.

Setting default profile

The default profile is the one based on which the product will be built. There can only be one default profile at a time.

To set a profile as default,

- Select the Default icon corresponding to the profile of your choice.
- In the pop-up box that appears, click Yes.

Editing profile

- Click the edit icon corresponding to the profile you want to edit.
- Update the necessary details and click Update.

Deleting profiles

- Click the delete icon corresponding to the profile you want to delete.
- In the pop-up box that appears, click Yes.

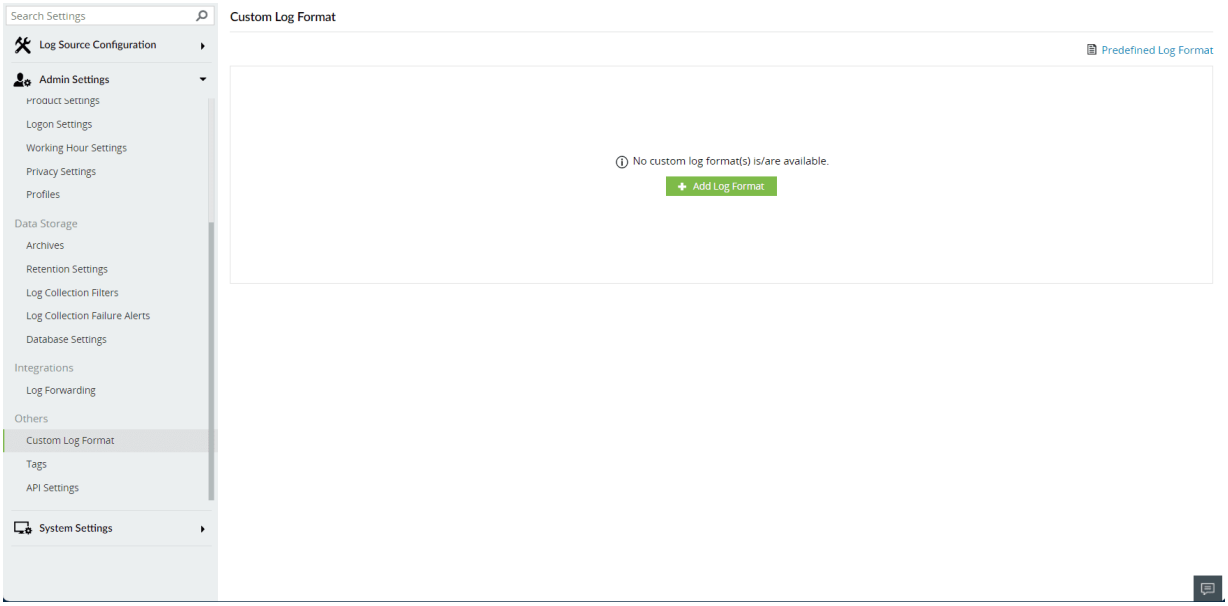
9.1.6. Custom log parsing

Last updated on: September 12, 2025

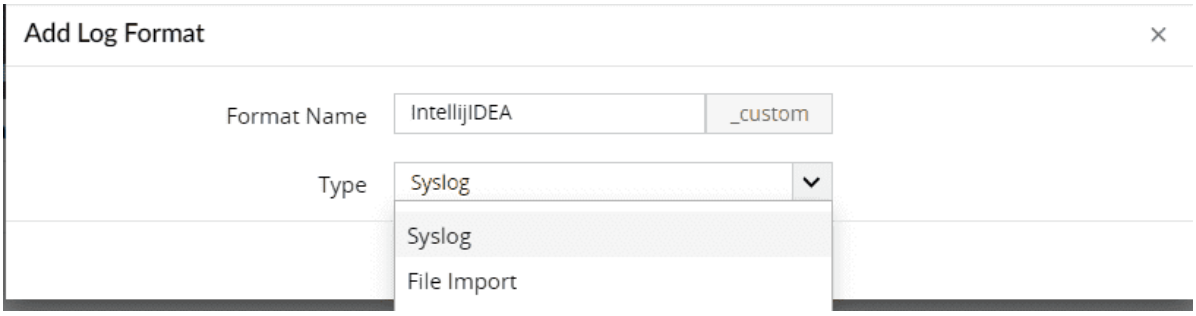
EventLog Analyzer's custom log parsing enables users to extract additional fields from logs by defining parser rules. This feature also allows the creation of custom formats and the definition of parser rules for the newly created formats.

1. Creating custom log formats

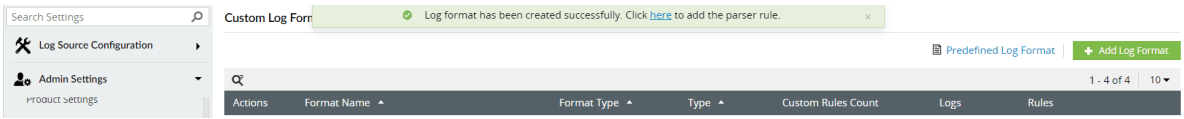
Navigate to Settings > Admin Settings > Custom Log Format.

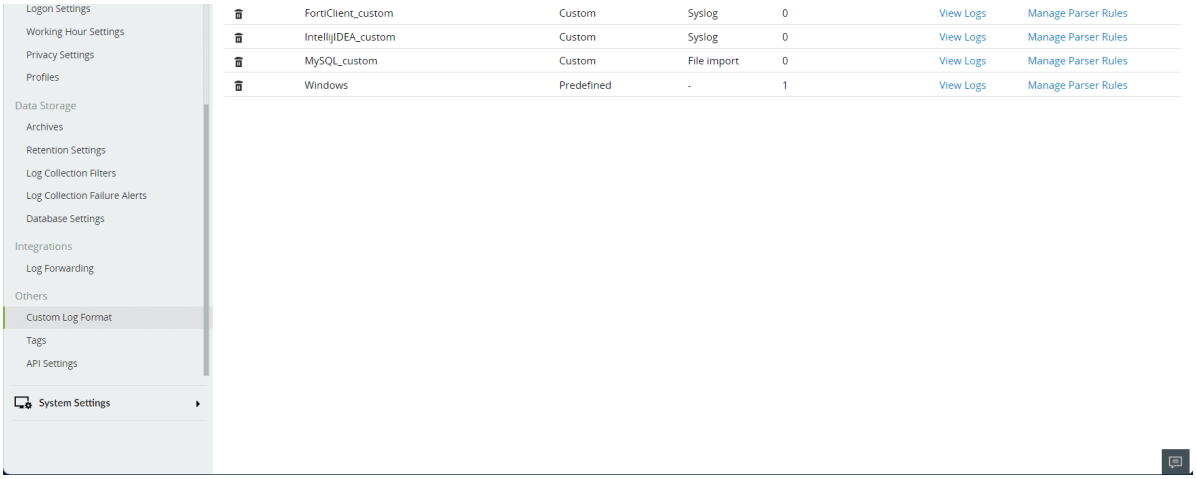


- To create a new format, click Add Log Format.
- A dialog box will appear; enter the new custom format name in the Format Name text box.
- This will create a new log format based on the syslog type. File import type is also supported.

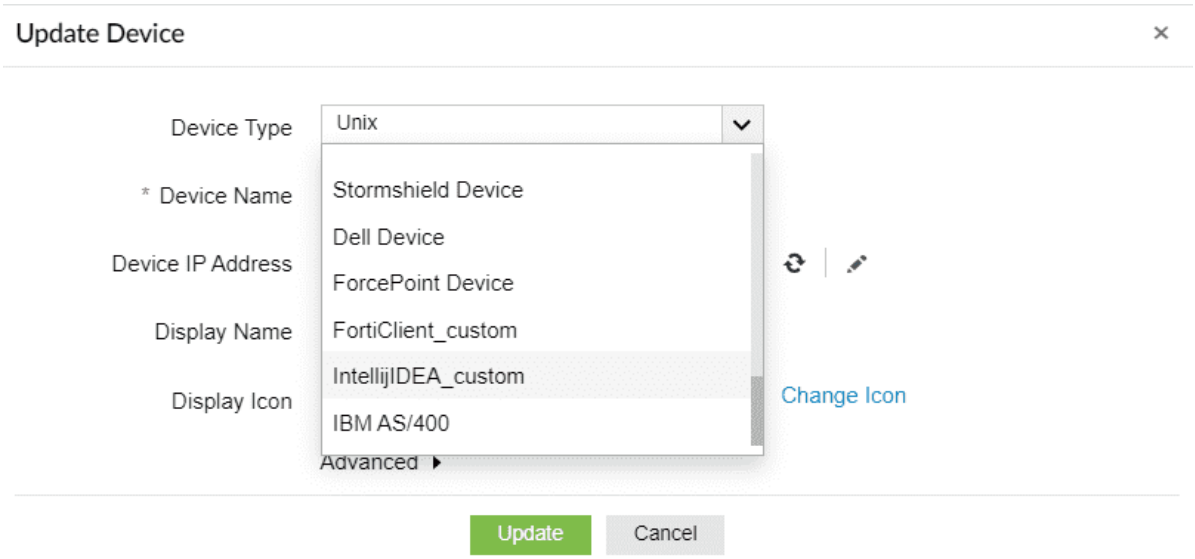


- After creating the custom log format, a confirmation box will appear, providing options to create parser rules for the newly created format or navigate to "Manage Parser Rules" for creating new parser rules.

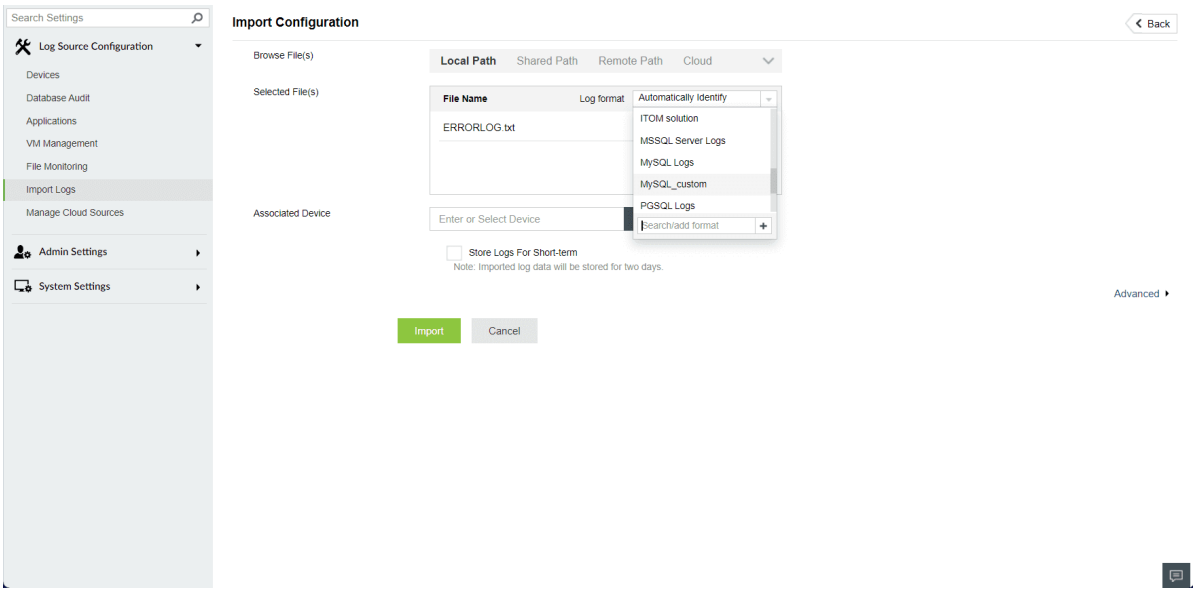




- The newly created "Syslog" based format can be assigned to any syslog devices. This can be done by navigating to Settings > Devices > Syslog devices > Update > Device Type and update to newly created format.



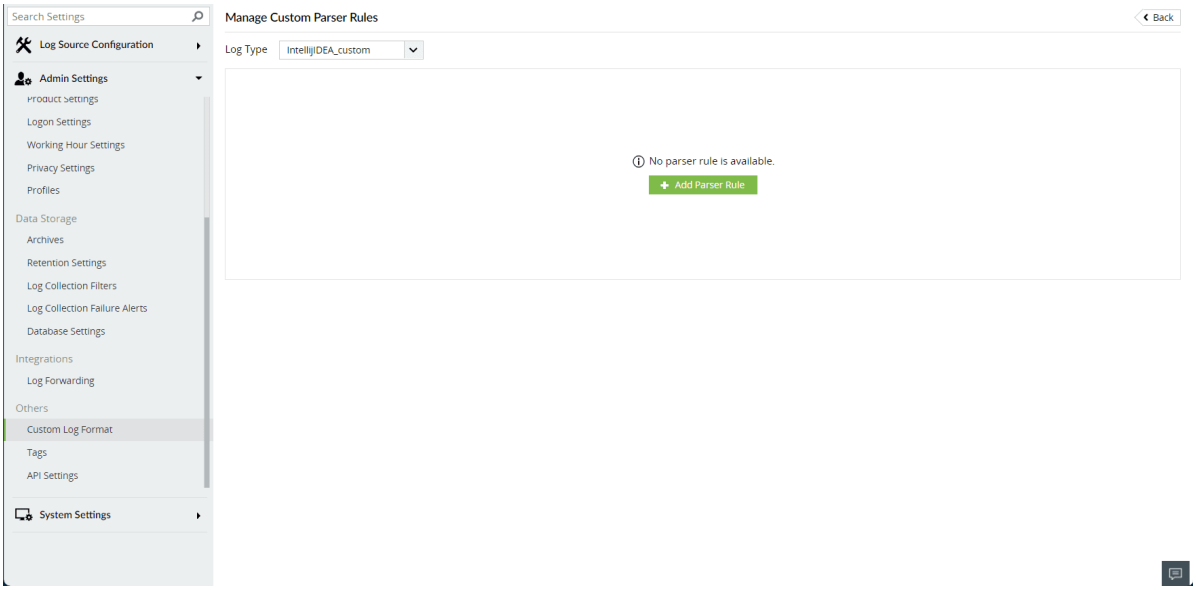
- The newly created "File import" based format can be assigned during file import.



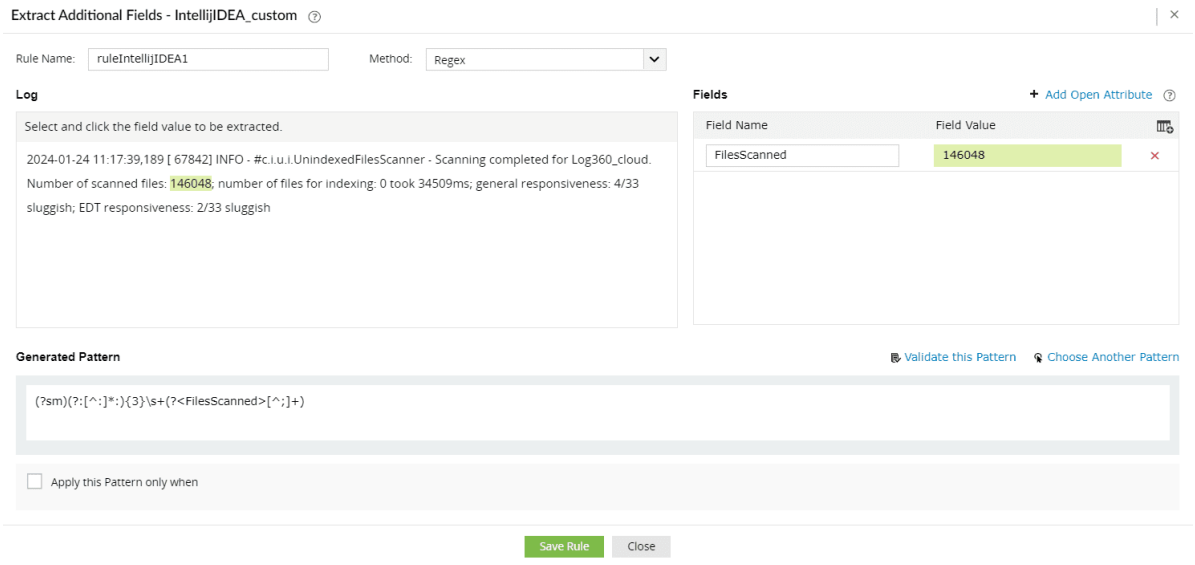
> **Note**
>
> A custom log format can be assigned to devices for log collection. When the format is deleted, the parsed fields and values are no longer accessible in the logs, and only the default fields remain available. This applies to archived logs as well.

2. Creating parser rules for log formats

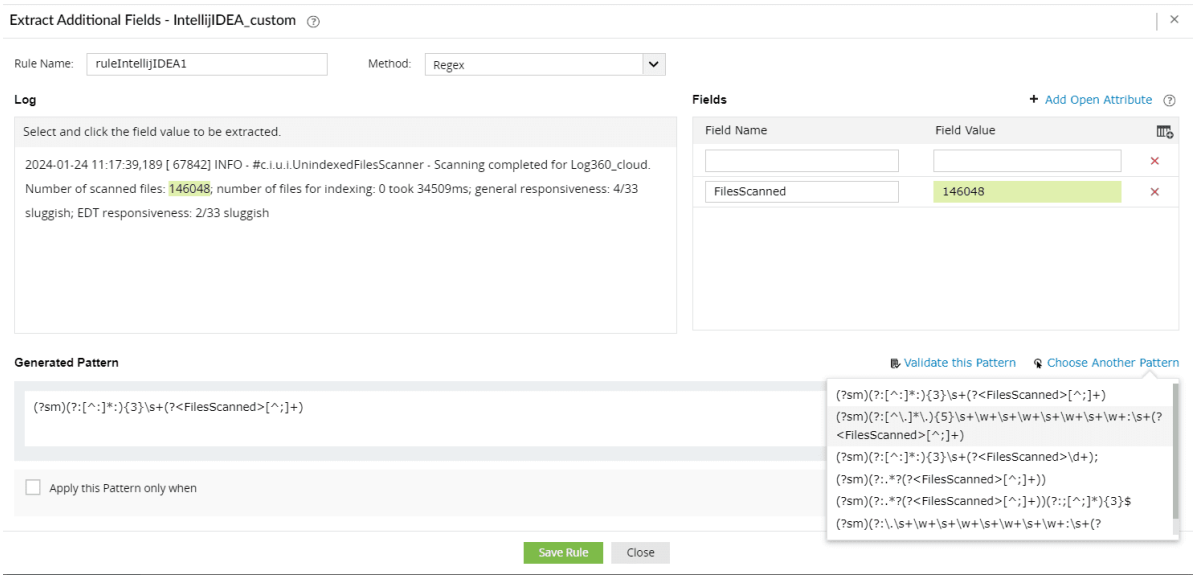
- To create a parser rule, click on Add Parser Rule.



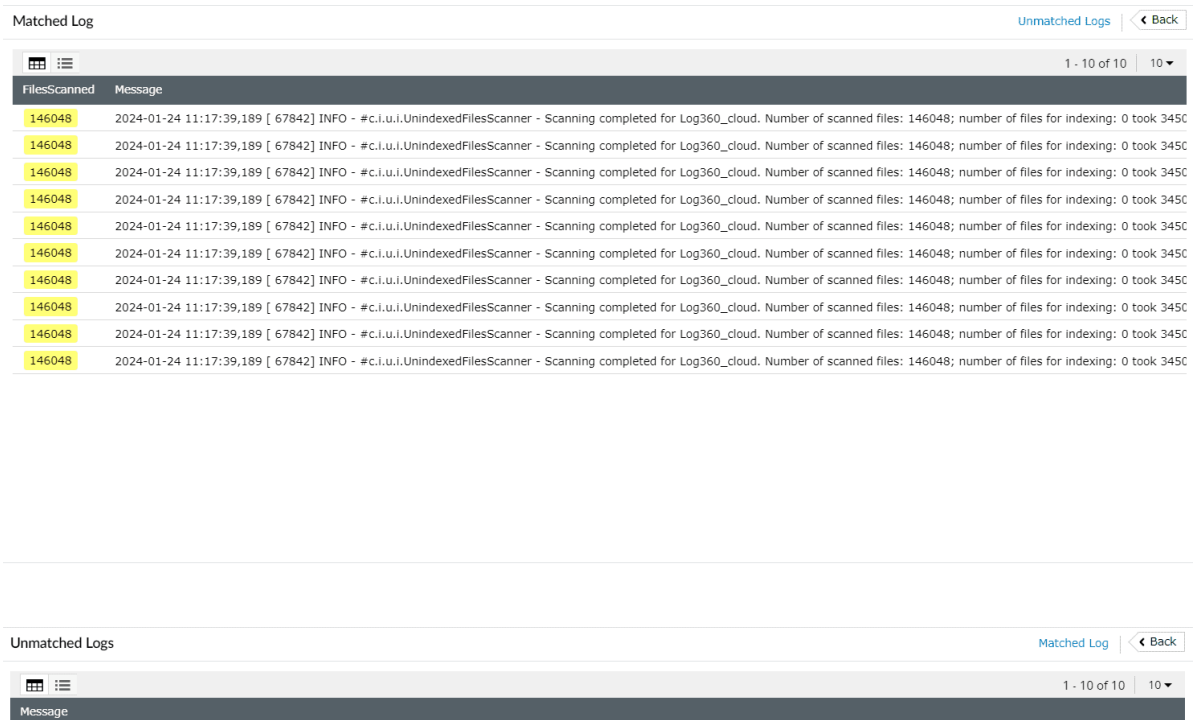
- There are two methods available to extract the field: Regex and Delimiter.
- Paste the log, click Save Changes, and select the field values to be extracted.
- Provide a rule name and field name for the parser rule.



- Utilize the 'Auto Identify' icon to recognize common fields and choose from appropriate working fields.
- By clicking Add Open Attribute, you can enter both the field name and its value, making it easier for future searches.
- A regular expression (regex) pattern will be generated, and this pattern is used to extract the field from the log.
- The option Choose Another Pattern shows a different pattern generated to extract the given field.
- Specify "apply this pattern only when" criteria for when to apply this parser rule.

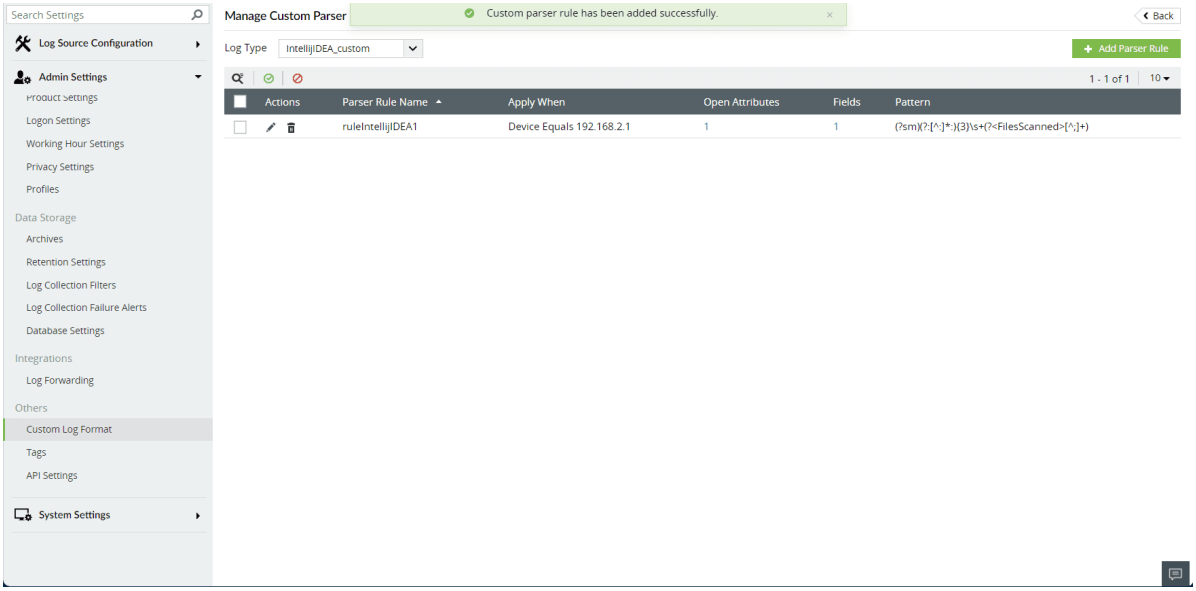


- Verify whether the generated pattern is extracting the field correctly by clicking Validate this pattern.
- Clicking Validate this pattern opens a new window to verify the generated pattern with the recently collected 50 logs, matching it. If the pattern does not match, the logs will be categorized as unmatched. If the pattern proves ineffective, select a different pattern by clicking Choose another pattern and attempt to validate the pattern.

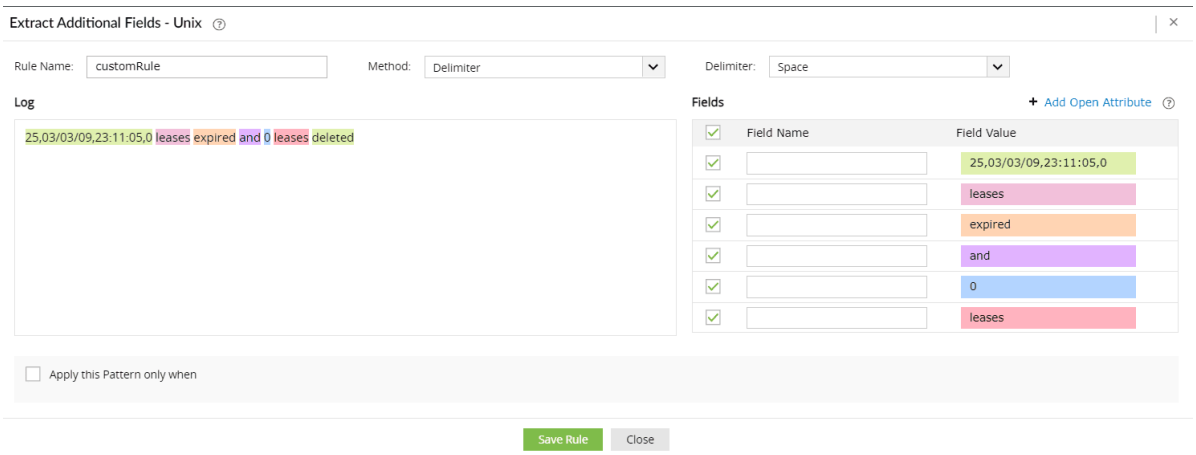


```
2024-01-19 13:53:56,049 [ 772] INFO - #c.i.i.p.PluginManager - Plugin PluginDescriptor(name=Groovy, id=org.intellij.groovy, descriptorPath=plugin.xml, path=~\AppData\Local\Programs\IntelliJ IDEA Comm
2024-01-19 13:53:56,049 [ 772] INFO - #c.i.i.p.PluginManager - Plugin PluginDescriptor(name=Groovy, id=org.intellij.groovy, descriptorPath=plugin.xml, path=~\AppData\Local\Programs\IntelliJ IDEA Comm
2024-01-19 13:53:56,049 [ 772] INFO - #c.i.i.p.PluginManager - Plugin PluginDescriptor(name=Groovy, id=org.intellij.groovy, descriptorPath=plugin.xml, path=~\AppData\Local\Programs\IntelliJ IDEA Comm
2024-01-19 13:53:56,049 [ 772] INFO - #c.i.i.p.PluginManager - Plugin PluginDescriptor(name=Groovy, id=org.intellij.groovy, descriptorPath=plugin.xml, path=~\AppData\Local\Programs\IntelliJ IDEA Comm
2024-01-19 13:53:56,049 [ 772] INFO - #c.i.i.p.PluginManager - Plugin PluginDescriptor(name=Groovy, id=org.intellij.groovy, descriptorPath=plugin.xml, path=~\AppData\Local\Programs\IntelliJ IDEA Comm
2024-01-19 13:53:55,856 [ 579] INFO - #c.i.p.i.b.AppStarter - Enabling system properties after restart: [intellij.first.ide.session]
2024-01-19 13:53:55,856 [ 579] INFO - #c.i.p.i.b.AppStarter - Enabling system properties after restart: [intellij.first.ide.session]
2024-01-19 13:53:55,856 [ 579] INFO - #c.i.p.i.b.AppStarter - Enabling system properties after restart: [intellij.first.ide.session]
2024-01-19 13:53:55,856 [ 579] INFO - #c.i.p.i.b.AppStarter - Enabling system properties after restart: [intellij.first.ide.session]
2024-01-19 13:53:55,856 [ 579] INFO - #c.i.p.i.b.AppStarter - Enabling system properties after restart: [intellij.first.ide.session]
```

- Click Save Rule to save the rule.



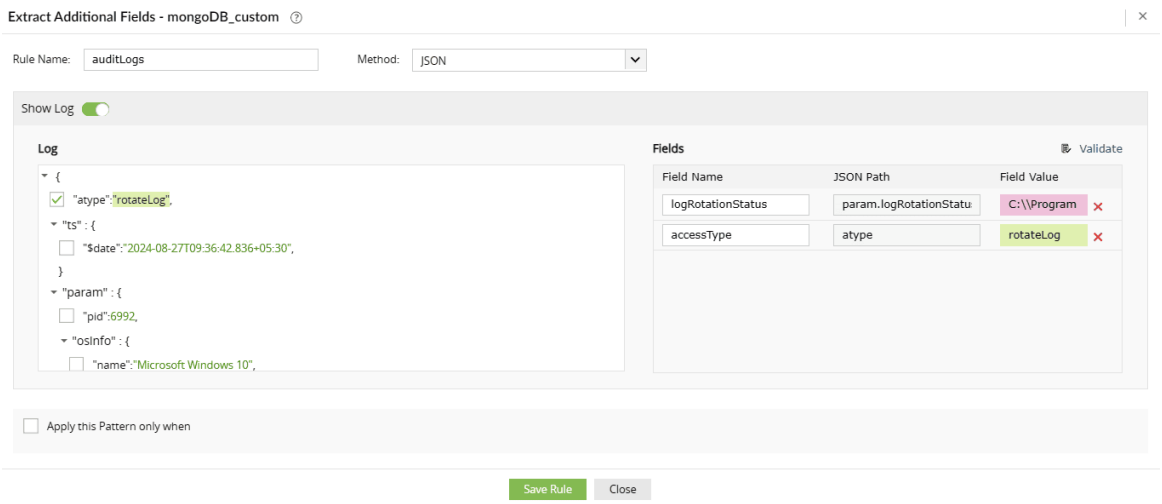
- Fields can also be extracted by changing the method to Delimiter. Users can specify the delimiter between each word, such as space, comma, tab, pipe, or enter a custom delimiter to extract the fields. Custom delimiter should be entered as symbols and not words. If the extracted fields work well for the log, users can provide a field name and save the rule.



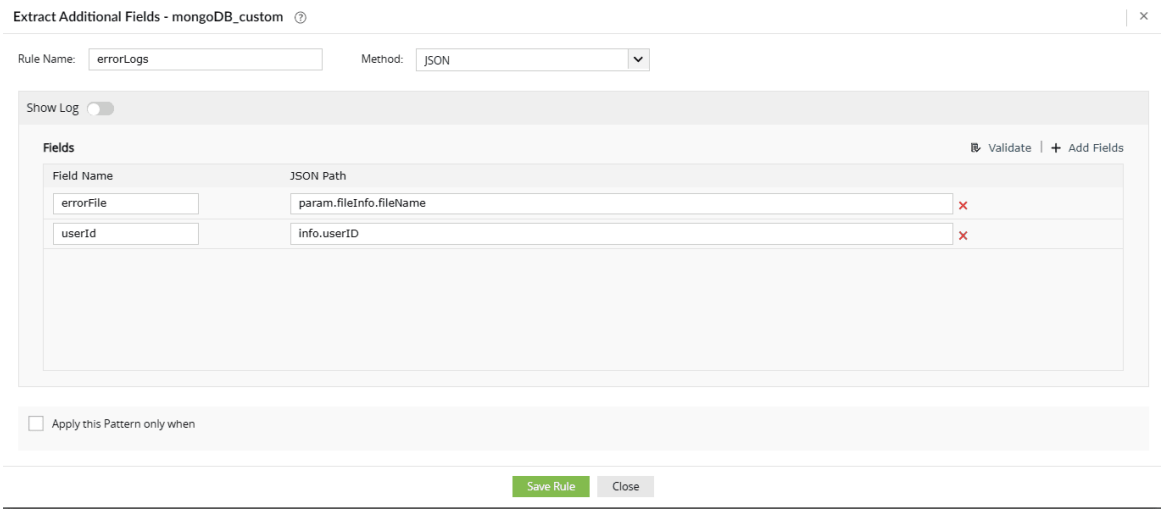
- For JSON format logs, users can extract fields by specifying the JSON path to target specific fields in the

log. Each field is defined by assigning a field name and mapping it to its corresponding JSON path. It's important to note that the JSON path should accurately reference the key or nested structure within the JSON log.

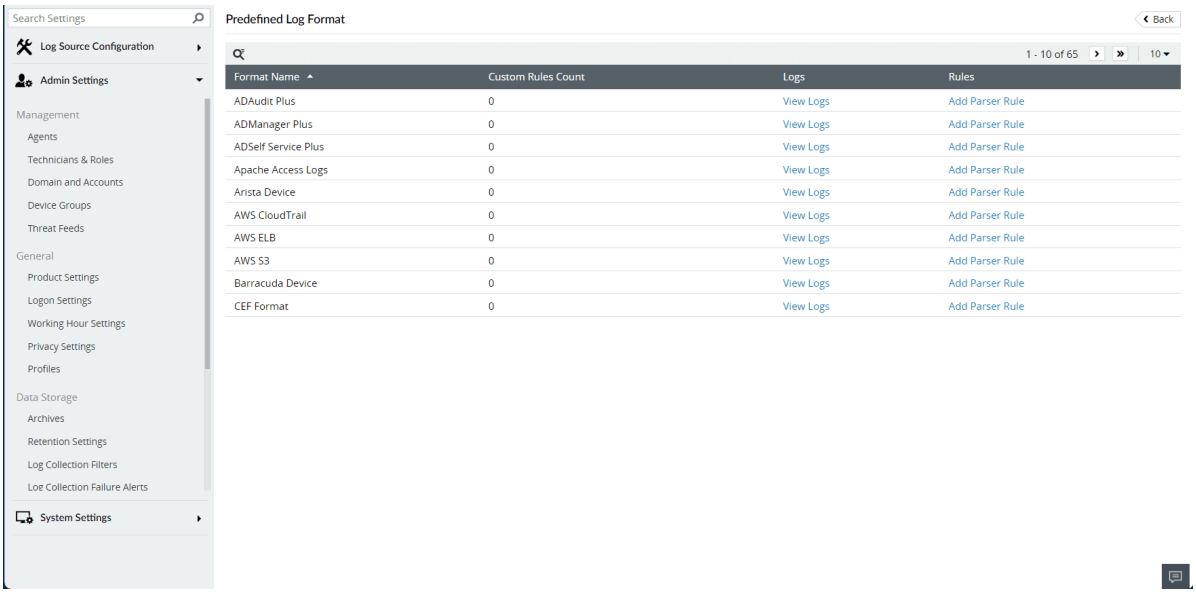
- JSON field extraction can be configured only for the File Import custom log format. Users can create JSON extraction rules in the following two ways:
  - With a Sample Log:



    - Provide a valid JSON log.
    - Select the required fields from the JSON tree.
    - Assign field names for the corresponding JSON paths.
  - Without a Sample Log:

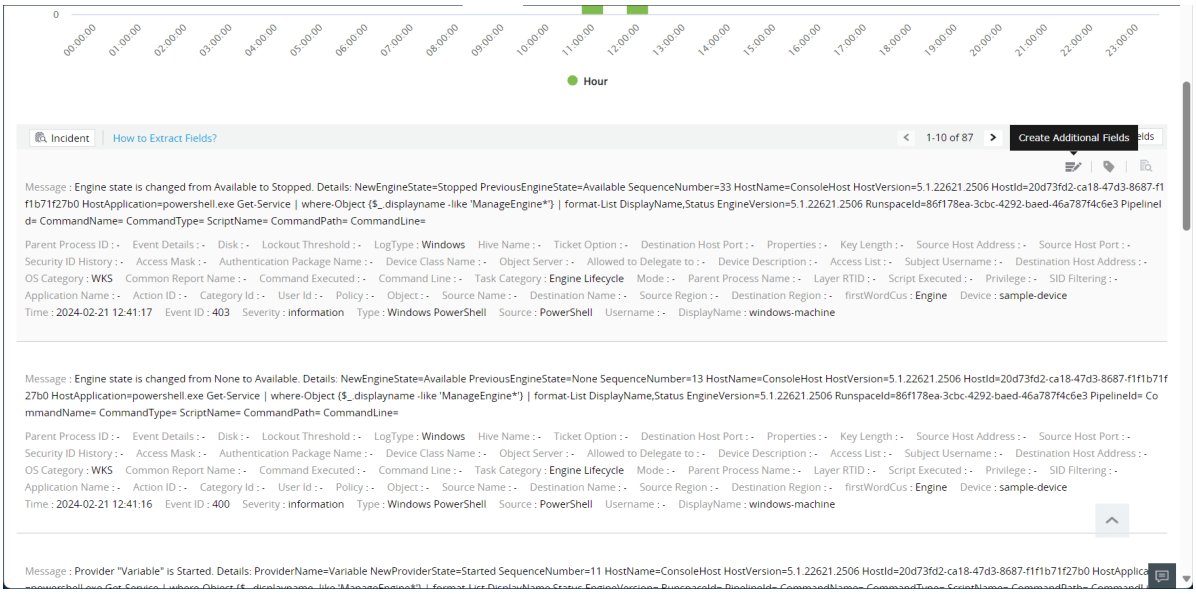


    - Manually specify the JSON path to target specific fields.
    - Ensure the JSON path matches the log structure.
- View the fields and open attributes associated with a specific parser rule, along with the option to disable or enable that rule. Edit the parser rule as needed and delete it if necessary.
- To add a parser rule for the predefined format, navigate to Settings > Custom Log Format > Predefined log format.

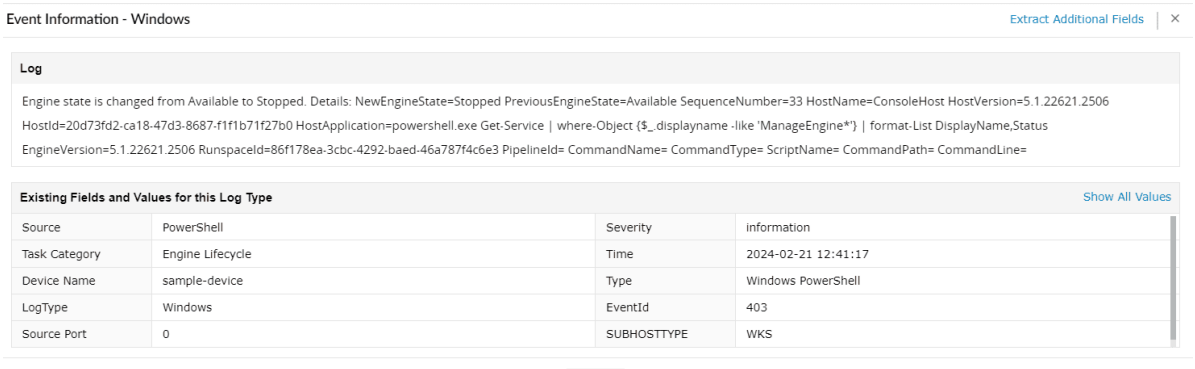


3. Extracting fields by creating custom parser rules from the search tab

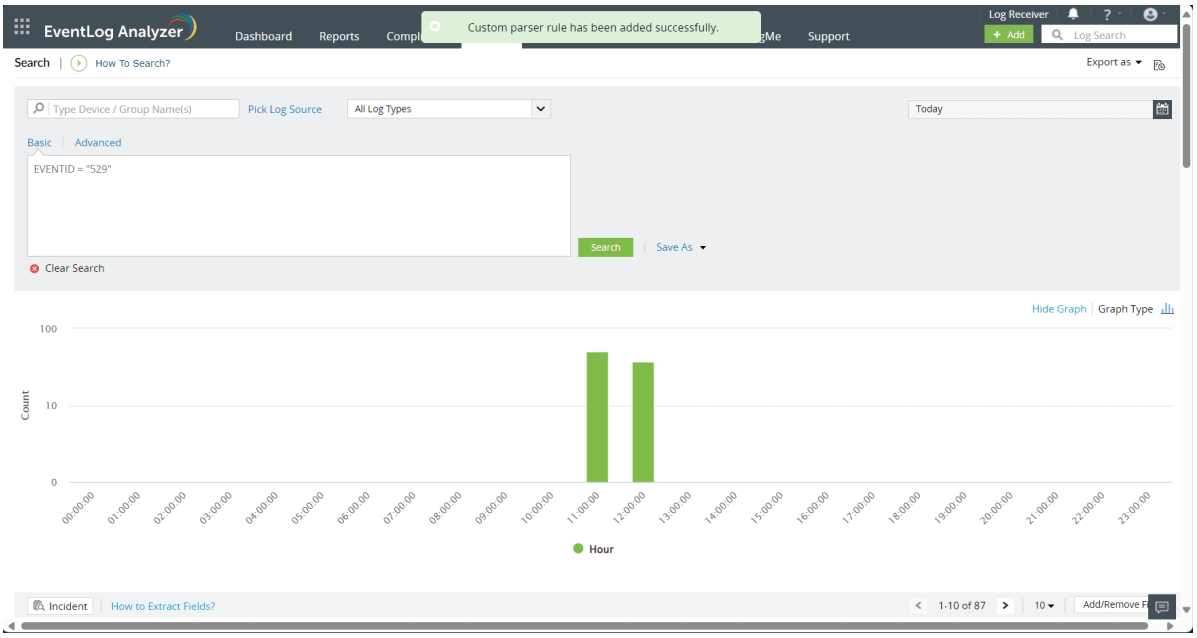
- Extract additional fields directly from the search tab. Locate the Create Additional Fields icon on the right side of each log and click it.



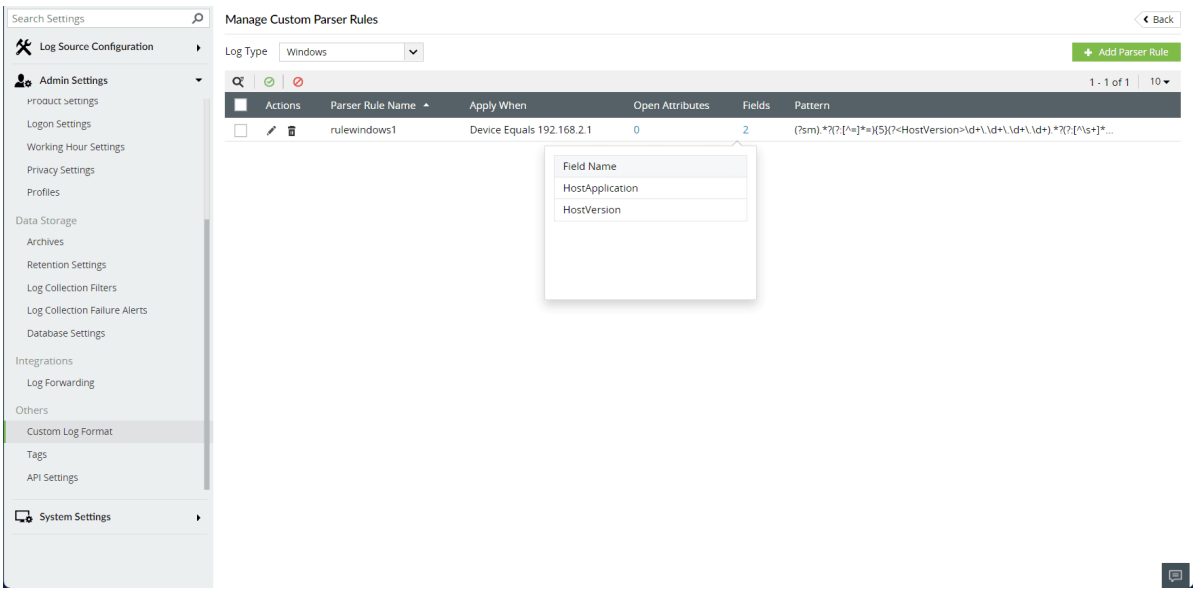
- The details of the log are displayed, and then select Extract Additional Fields.



- Follow the steps mentioned in the above section for creating a parser rule.



- The created parser rule can be viewed from the settings page.



> **Note**
>
> Fields can be extracted using two ways for both predefined and custom formats: via search and via settings.

9.1.7. Retention Settings

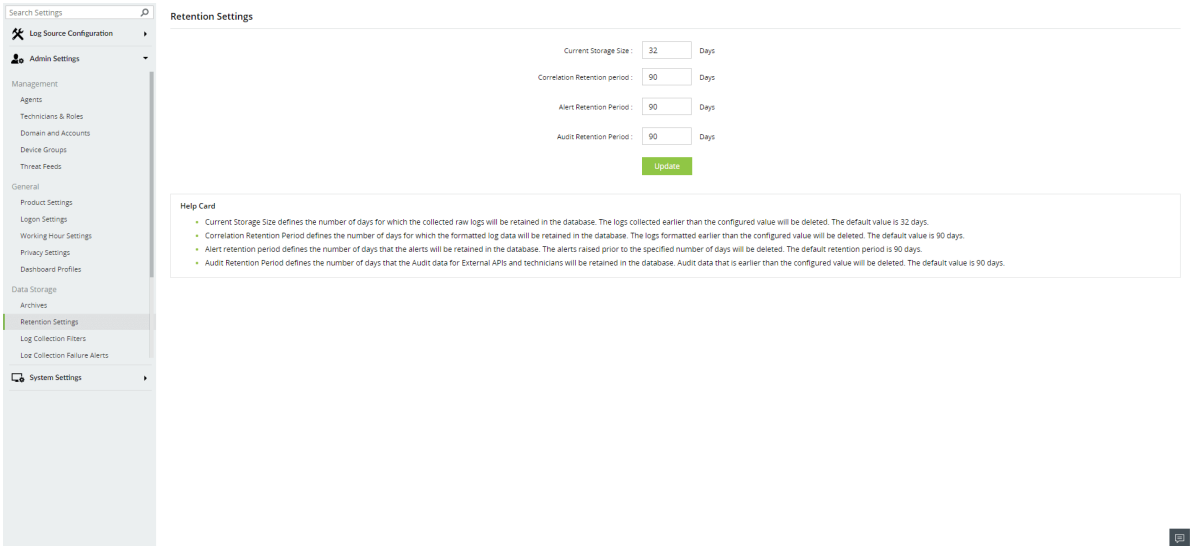
Last updated on: September 12, 2025

EventLog Analyzer retains log data in its database for a customizable time period. The database contains two sets of log data: raw logs and formatted logs. You can customize separate time periods for both the log data. After this period, the data will be permanently deleted from the database. Keeping the logs in the database forever will consume memory and increase overhead costs.

> **Note**
>
> The archive and database storage are asynchronous operations i.e. they are unrelated.

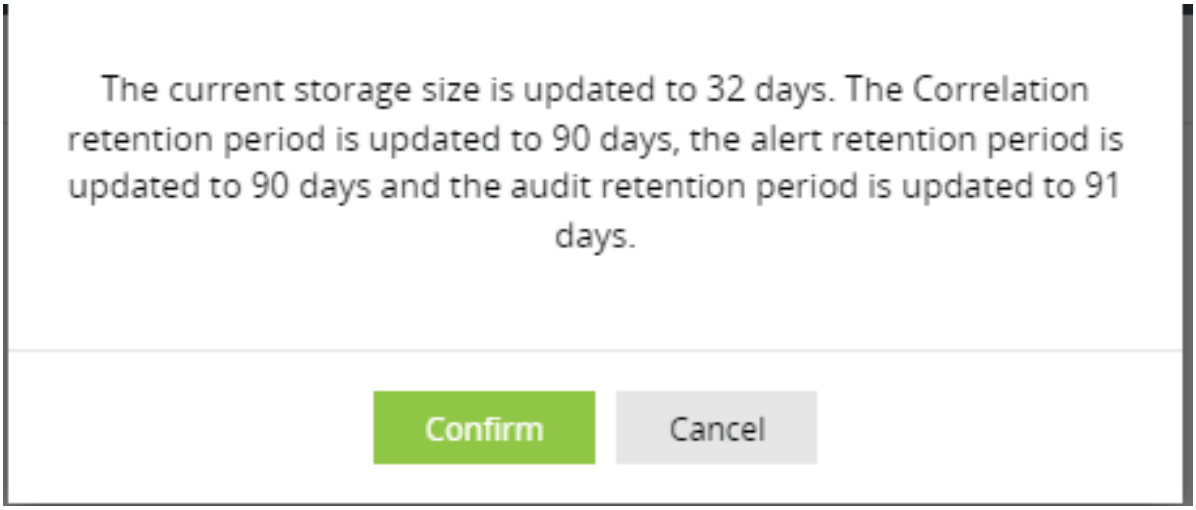
To customize retention settings,

- In the Settings tab, navigate to Admin Settings > Data Storage > Retention Settings.



- In the Current Storage Size box, enter the number of days for which the raw logs need to be retained in the database. The default value is 32 days.
- In the Correlation Retention Period box, enter the number of days for which the formatted logs need to be retained in the database. The default value is 90 days.
- In the Alert Retention Period box enter the number of days for which the alerts need to be retained in the database. The default value is 90 days.
- In the Audit Retention Period box enter the number of days for which Audit data for External APIs and technicians will be retained in the database. The default value is 90 days.
- After having entered all the values, click Update to save settings.





The Confirm Action box will appear. Click on Confirm.

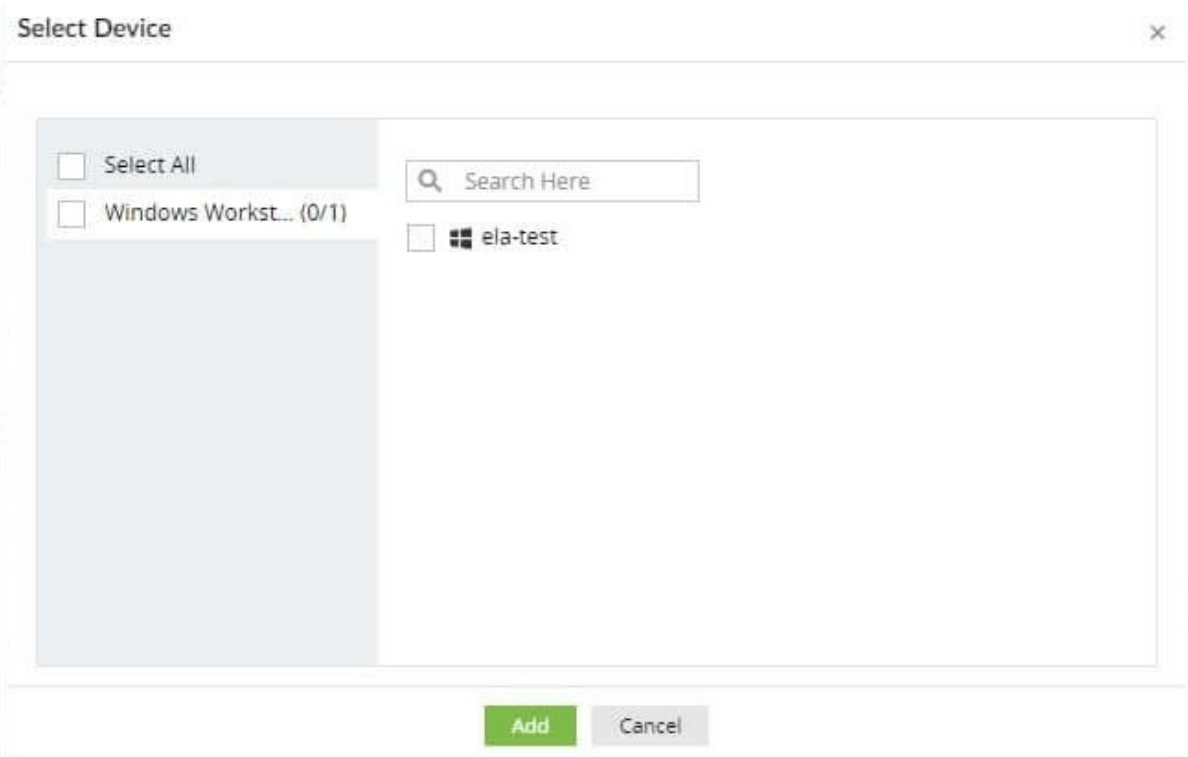
9.1.8. Log Collection Filter

Last updated on: September 12, 2025

EventLog Analyzer allows you to collect and process only the necessary logs by configuring log collection filters.

Steps to create a log collection filter

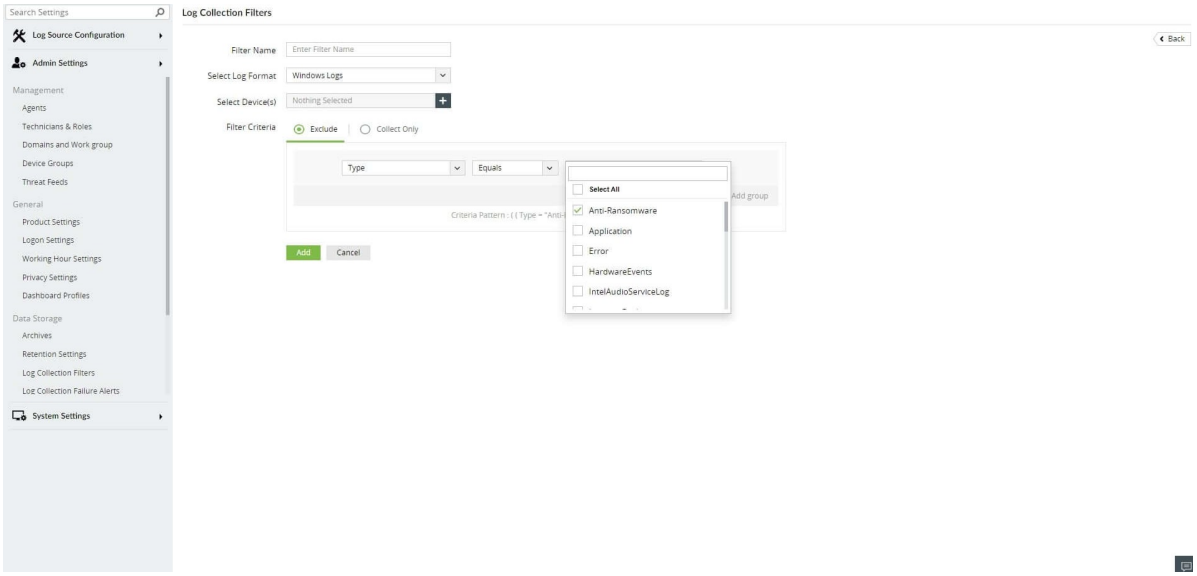
1. In EventLog Analyzer, navigate to Settings → Admin Settings → Log Collection Filters.
2. Click on the +Add Filter button.
3. Enter a unique name for your filter in the Filter Name field.
4. Select the log format from the Select Log Format drop-down menu. Choose any one of the following log formats displayed:
   - Windows Logs
   - Syslogs
   - IBM AS/400 Logs.
5. Click on the + button present in the Select Device(s) field to select a device group.



6. In the Select Device pop-up menu, you can either search and select particular devices in your network to apply the filter to or select entire device groups by selecting the respective check boxes on the left pane and clicking on Add.
7. In the Filter Criteria box, you will see the Exclude and Collect Only drop-down menus to configure a filter to perform either of the following actions:

- Exclude all the logs that satisfy the specified filter criteria.
- Collect only the logs that satisfy the specified filter criteria.

> **Note**
>
> You can configure a filter to perform only one action. You need to create separate filters to collect and exclude logs for the same set of devices or device groups.

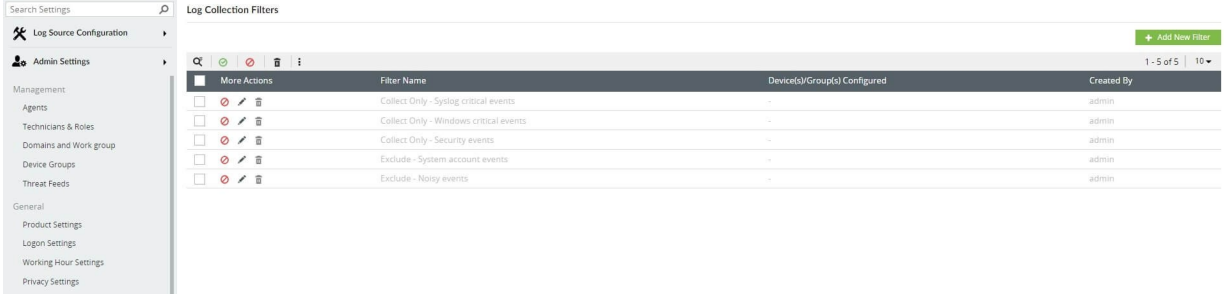


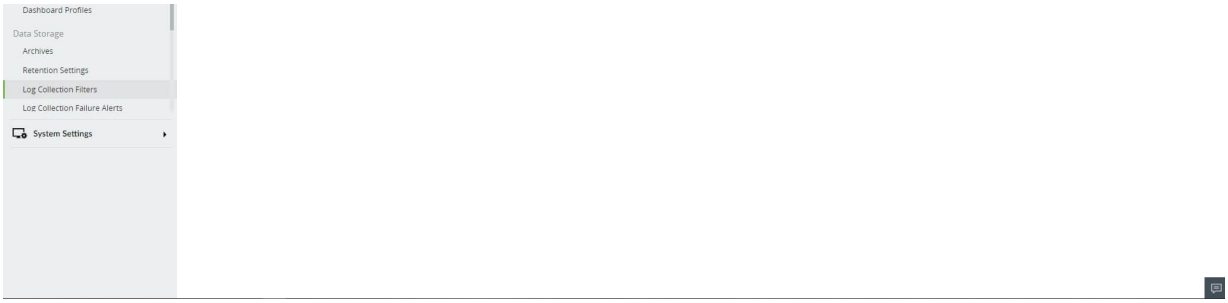
8. Click on the + sign to add multiple filter criteria by using conditional operators such as AND and OR.
9. You can also configure multiple filter groups by clicking on +Add Group and link them using AND or OR operators to create a high-level filter.
10. Click on Finish to save the created filter.

Viewing and managing log collection filters

You can view, enable or disable, edit, and delete all the created filters in the Log Collection Filters page by clicking on the respective icons provided. Please note that the default filters present in this page can only be disabled and not deleted.

You can see the list of devices associated with a particular filter by hovering your mouse pointer over the Device(s)/Group(s) Configured section. The More Actions drop-down menu allows you to select and enable, disable, export, and import multiple filter profiles.





Note

The list of all the sources for which the log collection filter option is available is provided below:

- Windows logs.
- IBM/400 logs.
- Only Unix, Cisco, SonicWall, Juniper, PaloAlto, Fortinet, CheckPoint Device, NetScreen, WatchGuard, Sophos, Brracuda, Huawei, Meraki, HP, Syslog, PfSense, FirePower, F5, Stormshield, Dell, ForcePoint, Topsec and sangfor under Syslog log format.
- Only Sysmons, IIS Server (event viewer logs only), Oracle, Terminal, Printer, MSSQL Server Logs(event viewer logs only) and Syslog Application under Application log format.
- Only AWS and SalesForce under Cloud Sources log format.

9.1.9. Log Collection Failure Alerts

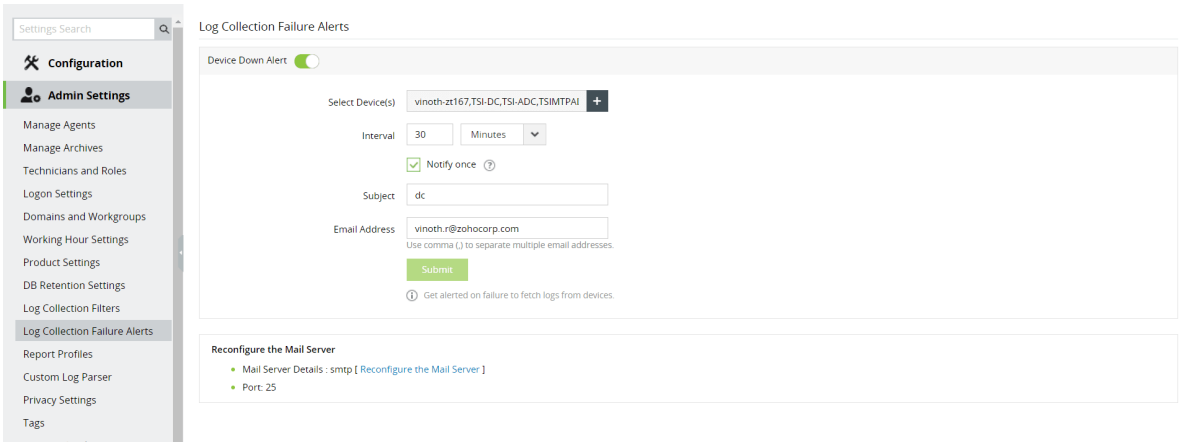
Last updated on: September 12, 2025

You can configure EventLog Analyzer to generate alerts when a device is down.

Device Down

To configure alerts to notify users about devices not sending logs,

- In the Settings tab, navigate to Admin Settings → Log Collection Failure Alerts → Device Down Alert.

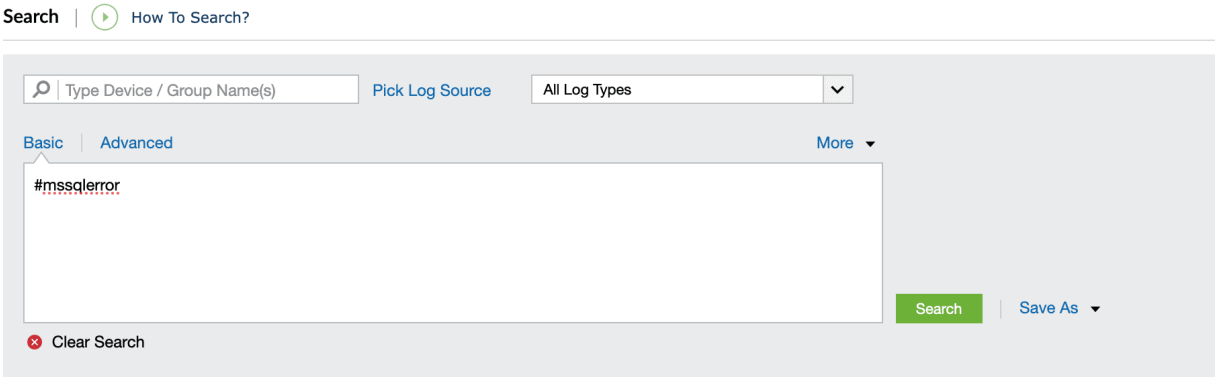


- If the alert is not enabled by default, click the toggle button to enable it.
- Select the device(s) or device group(s) for which alerts are to be generated when the device goes down.
- Select the time interval (minutes, hours, days) at which you want to be notified via email.
- In the Subject box, enter the subject of the email that will be sent to users.
- In the Email Address box, enter the email IDs of users to whom the alert emails should be sent.
- Click Submit to complete configuring log collection failure alerts.

9.1.10. Tags

Last updated on: September 12, 2025

In this section, you can manage the tags assigned in log search. You can view all the tags created, criteria specified, and notes for the tag. You can also edit criteria or delete the tag. To create a tag, refer to Tagging Tool. Navigate to Settings > Admin Settings > Tags.



How to edit a tag?

To edit the critieria of the tag, click the edit icon next to the tag. You can update the criteria of the tag here.

How to delete a tag?

To delete a tag, click the delete icon next to the tag.

9.1.11. Auto Update

Last updated on: September 12, 2025

- Navigate to Admin → Administration → Auto Backup/Update → Auto Update.
- To enable auto update for a particular component, click on the icon located in the action column of the particular component.
- To disable auto update for a particular component, click on the icon located in the action column of the particular component.
- To edit the update scheduler for a particular component, click on the icon located in the action column of the component.
- In Check for Update option, select whether you want to check for updates daily, weekly, or monthly.
- Selecting the option Automatically Download and update Log360 will download and install any available updates automatically.
- You can also choose to receive notifications about available updates by selecting the options under Notify me.
  - When updates are available: Notifications will be sent when updates are available.
  - After installing the update: Notifications will be sent after the updates have been downloaded and installed.
- Click Save.
- Furthermore, you can use the Update History link to view all the installed updates.

Alternatively, you can also configure the auto update settings by following the steps listed below:

- Navigate to Support tab.
- Click on Check for updates box at the top right corner of the page.
- Click Settings link in the pop-up that appears, then click on Auto Update tab.
- Select the check box against Enable Auto Update to enable auto update.
- In Check for Update option, select whether you want to check for updates daily, weekly, or monthly.
- Selecting the option Automatically Download and update Log360 will download and install any available updates automatically.
- You can also choose to receive notifications about available updates by selecting the options under Notify me.
  - When updates are available: Notifications will be sent when updates are available.
  - After installing the update: Notifications will be sent after the updates have been downloaded and installed.
- Click Save.

9.1.12.1. Overview

Last updated on: September 12, 2025

In this page

Pre-requisites

The Log360 agent collects log data from devices and forwards it to the Log360 server for centralized monitoring and analysis.
The agent is required in the following scenarios:

- To monitor files on Windows file servers.
- When there are RPC connectivity issues between the log source and the product console's server.
- Windows agent installation is mandatory to collect Windows event logs when the product console's server is deployed on Linux.

The agent can be deployed on devices using multiple methods:

- Using the product console - Direct installation from the product interface.
- Using Group Policy Objects (GPOs) - Automates agent installation across multiple Windows devices in Active Directory.
- Using SCCM or similar software deployment tools - Supports silent installation for Windows and Linux devices.
- Using Endpoint Central - Create and deploy a software package for bulk agent installation.

  NOTE

  Silent installation allows the agent to be installed in the background without displaying any installation prompts or dialogs. This is especially useful when deploying the agent on multiple devices or using software deployment tools like SCCM, GPO, or Endpoint Central.

- Manual installation - For single devices or cases where automated deployment is not possible.

Pre-requisites

Before installing the Log360 agent, ensure that the target devices meet the following requirements:

1. Supported Operating Systems:
   - Windows Client OS: Windows XP and later
   - Windows Server OS: Windows Server 2003 and later
   - Linux OS: RedHat (RHEL), SuSE, Fedora, CentOS, Ubuntu, Debian
2. User Privileges:
   - Windows devices: The installation account must have administrator privileges.

- Linux devices: The user must have sudo or root access.

> NOTE
>
> For additional information on the prerequisites and requirements for Windows agent installation, refer to this help document.

Read also

This document explained how and when to install the agent, along with supported deployment methods and pre-requisites. To learn how to install and manage agents, refer to the following documents:

- Agent installation
- Managing agents

9.1.12.2. Agent installation

Last updated on: September 12, 2025

In this page

Overview

Using product console

Using GPO

Using SCCM

Via Endpoint Central

Manual installation

Overview

This page explains how the agent can be installed using the product console, GPOs, SCCM, Endpoint Central, or manually, depending on your deployment needs.

Agent installation using the product console

1. Log in to your account.
2. Navigate to the Settings tab, and under Admin Settings, select Collectors/Agents.

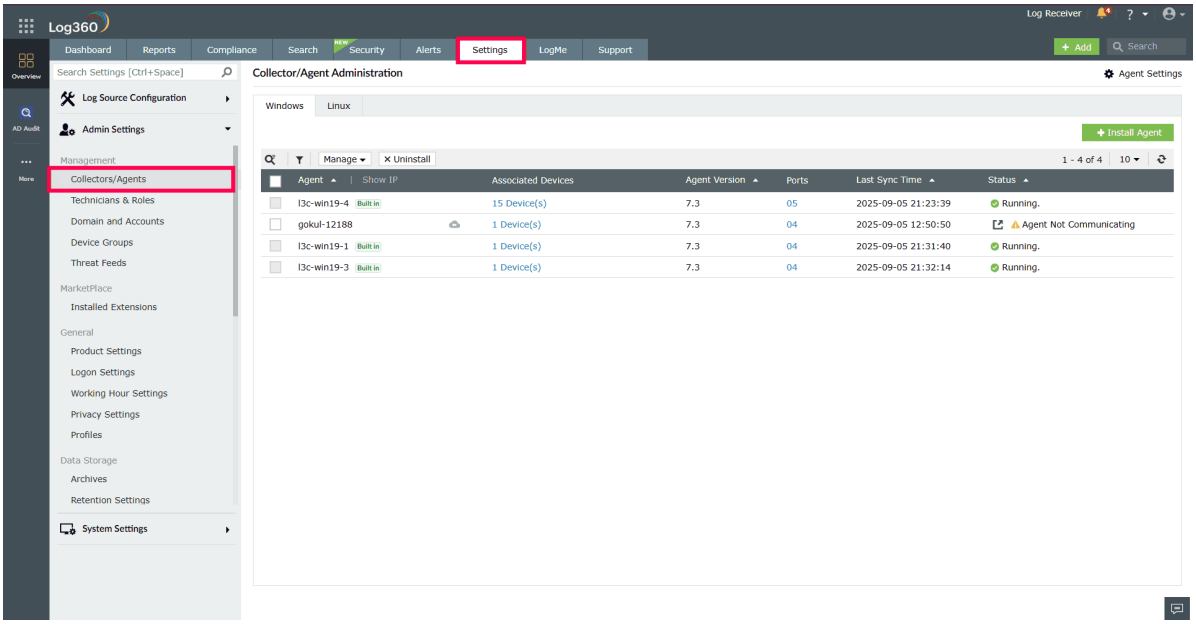


Figure 1: Navigating to Collectors/ Agents

3. Click + Install Agent and then the icon corresponding to Device(s).
4. Select the devices on which you want to install the agent.

5. Enter the Username and Password for the device(s).This account must have administrator privileges.

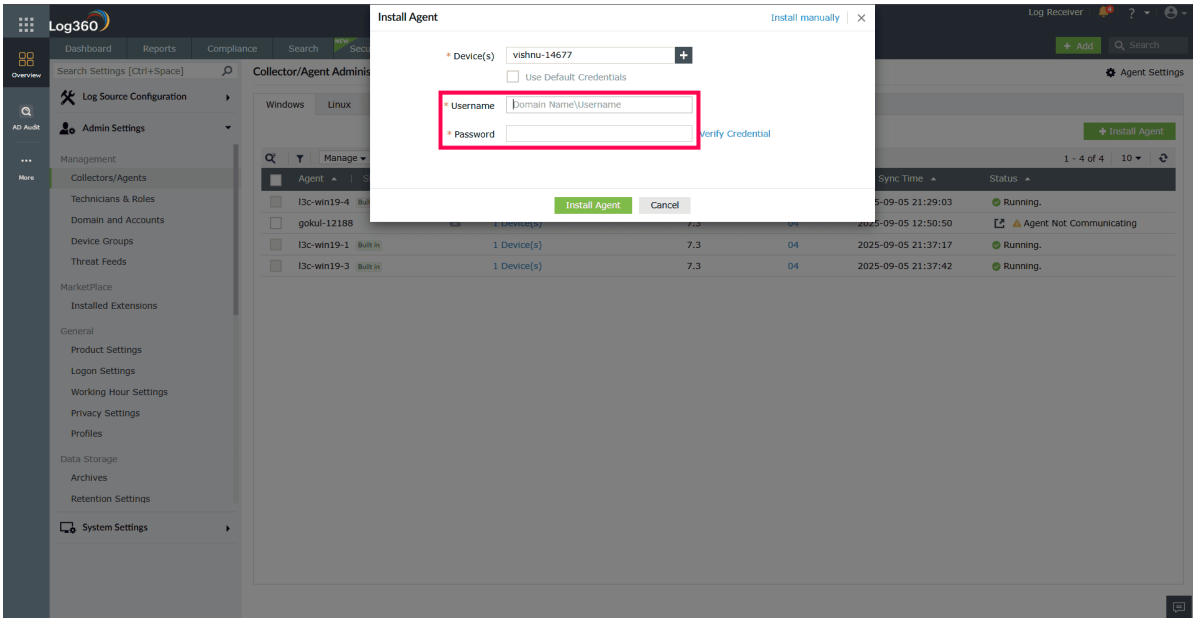


Figure 2: Entering username and password

6. Click Verify Credential to validate the credentials entered.
7. Alternatively, you can choose Use Default Credentials by selecting the checkbox next to it.

> NOTE
>
> If multiple devices are selected, ensure that the credentials are valid for all devices.

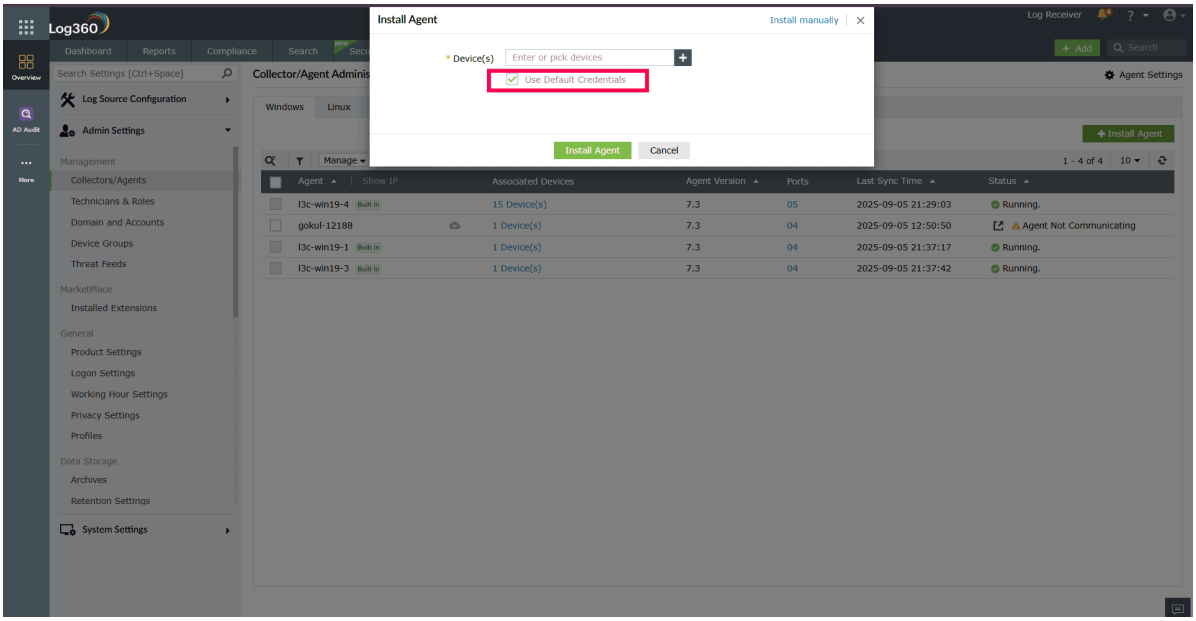


Figure 3: Using default credentials

Agent installation using GPOs

Before installing the agent using Group Policy Objects (GPOs), place the following files in a network-shared folder on the server:

- InstallLog360Agent.vbs (Path:<InstallationDirectory>\ManageEngine\Log360\tools\scripts)
- Log360Agent.exe (download from the Manage Agents page).

The installation process comprises the following steps:

- Creating a GPO
- Configuring script settings
- Configuring Administrative Template Settings
- Applying the GPO

Creating a GPO

1. Open Group Policy Management.
2. In the left pane, right-click Group Policy Objects and select New.

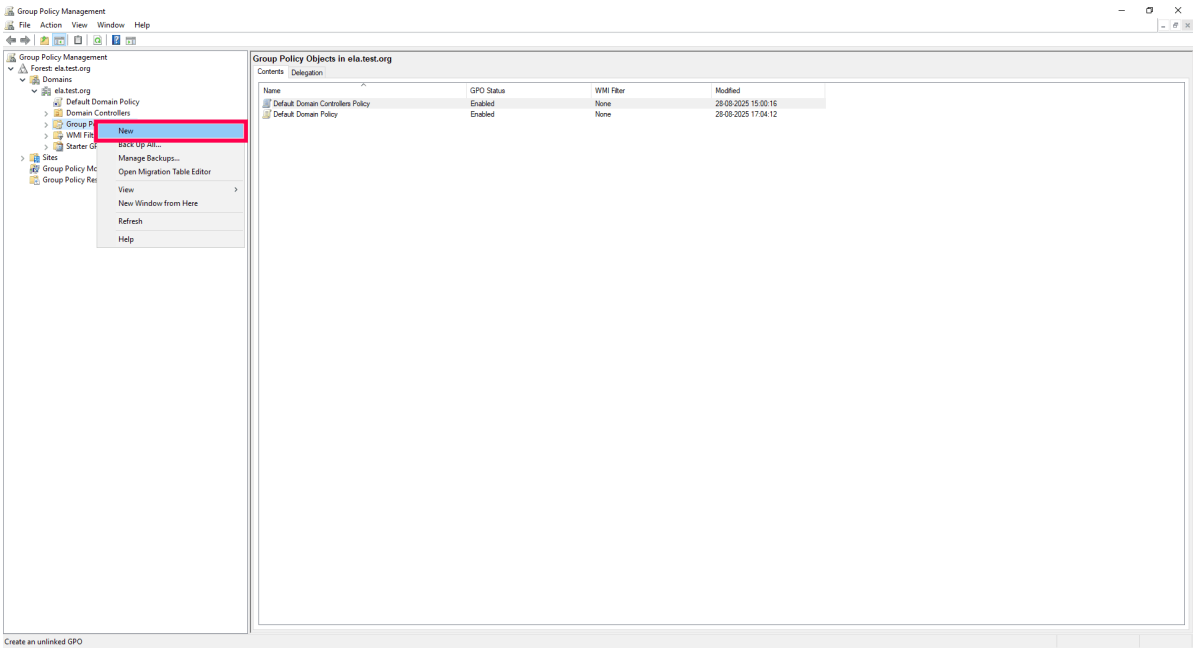
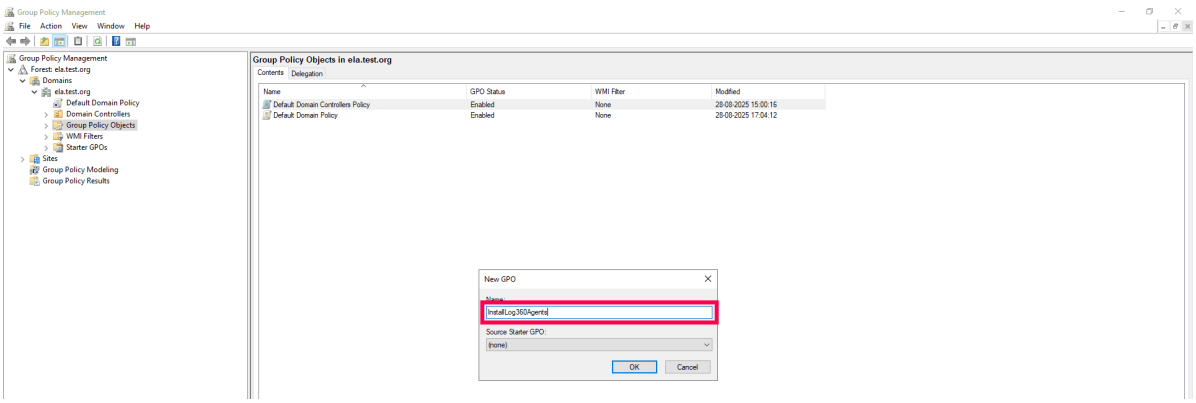


Figure 4: Creating a new group policy object

3. Enter a suitable name for the GPO and click OK.



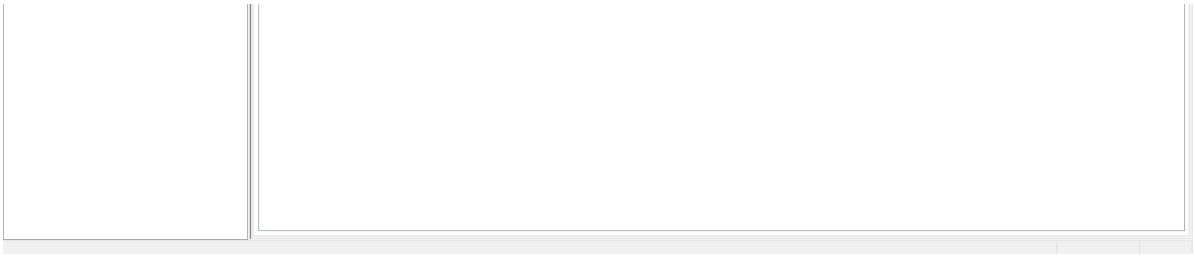


Figure 5: Naming the GPO

Configuring script settings

1. Right-click the newly created GPO and select Edit.

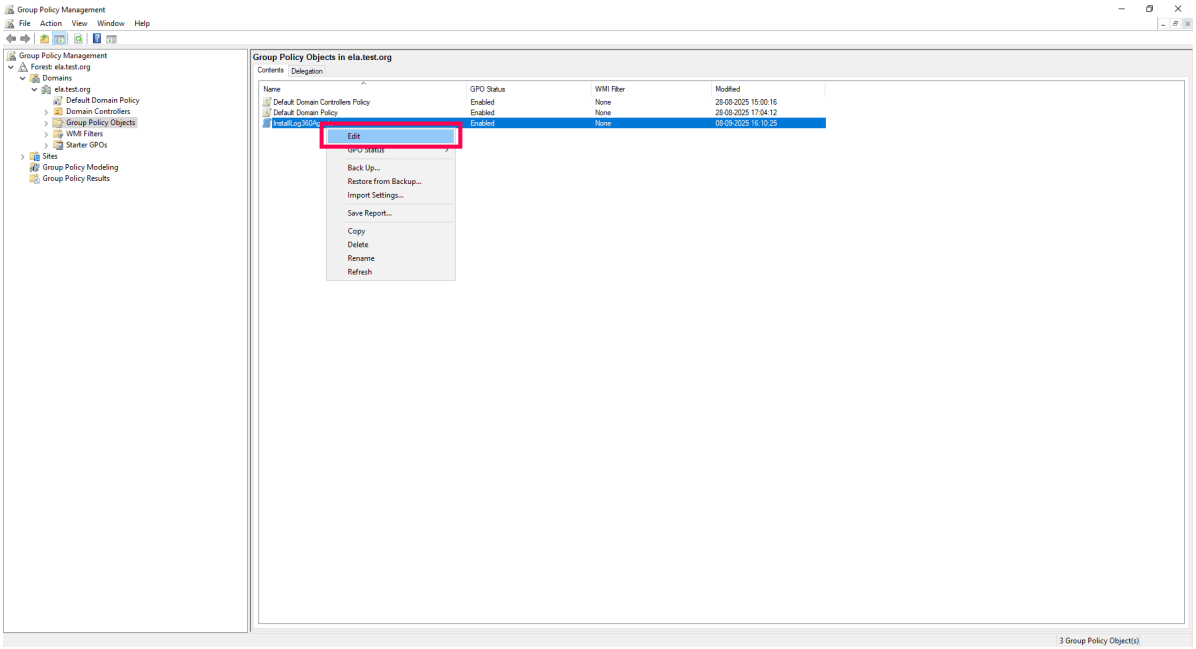
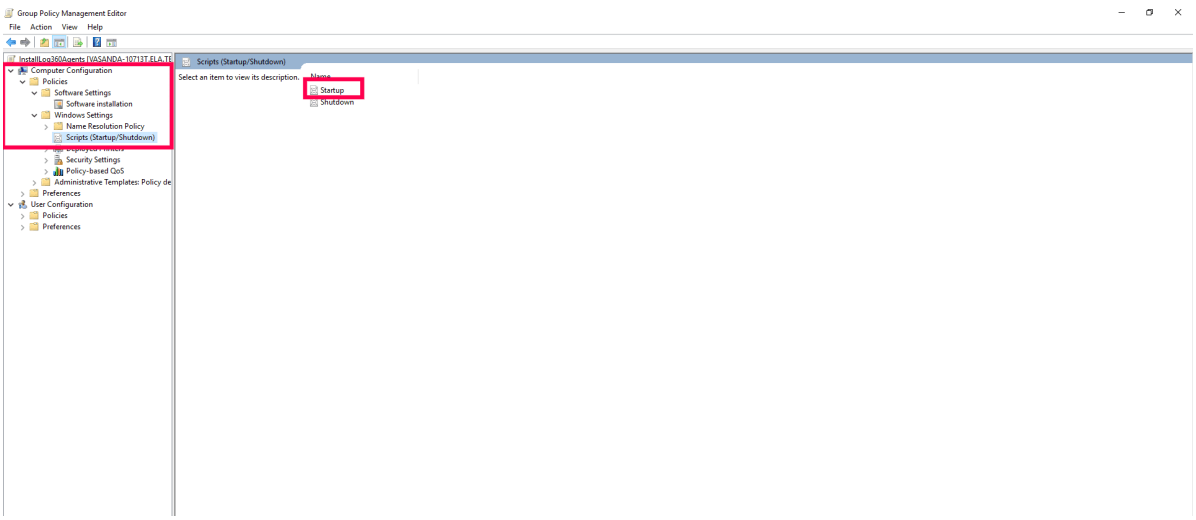


Figure 6: Editing GPO

2. For Windows Server 2003, navigate to: Computer Configuration> Windows Settings> Scripts (Startup/Shutdown)> Startup.
3. For Windows Server 2008 and later, navigate to: Computer Configuration> Policies> Windows Settings> Scripts (Startup/Shutdown)> Startup.



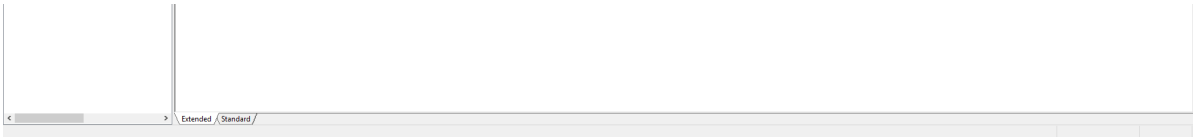


Figure 7: Configuring script settings

4. Right-click Startup, and in the dialog box that appears, click Add.
5. In the Add Script dialog box, click Browse and select InstallLog360Agent.vbs from the shared location.

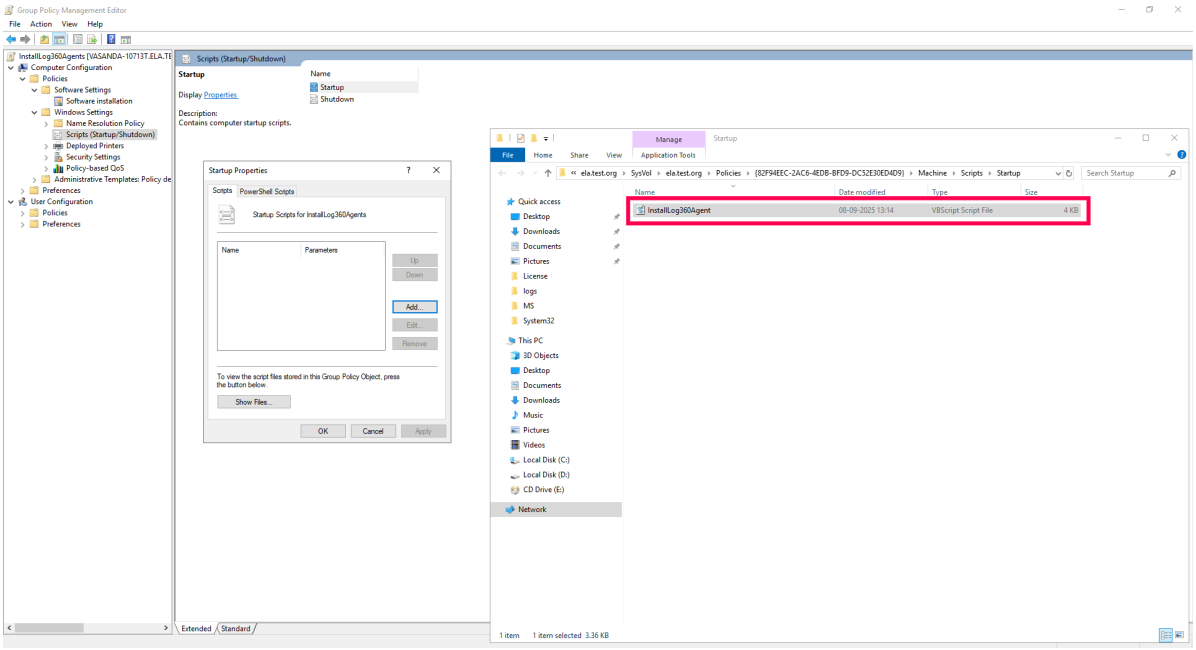
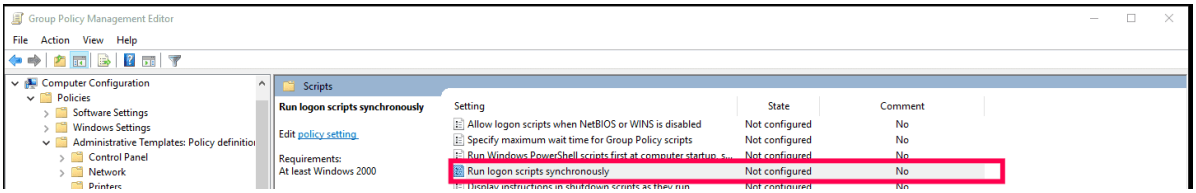


Figure 8: Installing agent

6. n the Script Parameters field, enter the following parameters:
   /INSTALLERPATH:"<share path of Log360Agent.exe">
   Example:
   .\InstallLog360Agent.vbs /INSTALLERPATH:"\\Agent-shared\Log360Agent\Log360Agent.exe"
7. Click OK to return to the Startup Properties dialog box.
8. Click Apply and then OK.

Configuring Administrative Template Settings

1. In the Group Policy Management Editor, navigate to Computer Configuration > Administrative Templates > System.
2. Under System, select Scripts.
3. In the right pane, double-click Run logon scripts synchronously and enable it.
4. Click Apply and then OK.



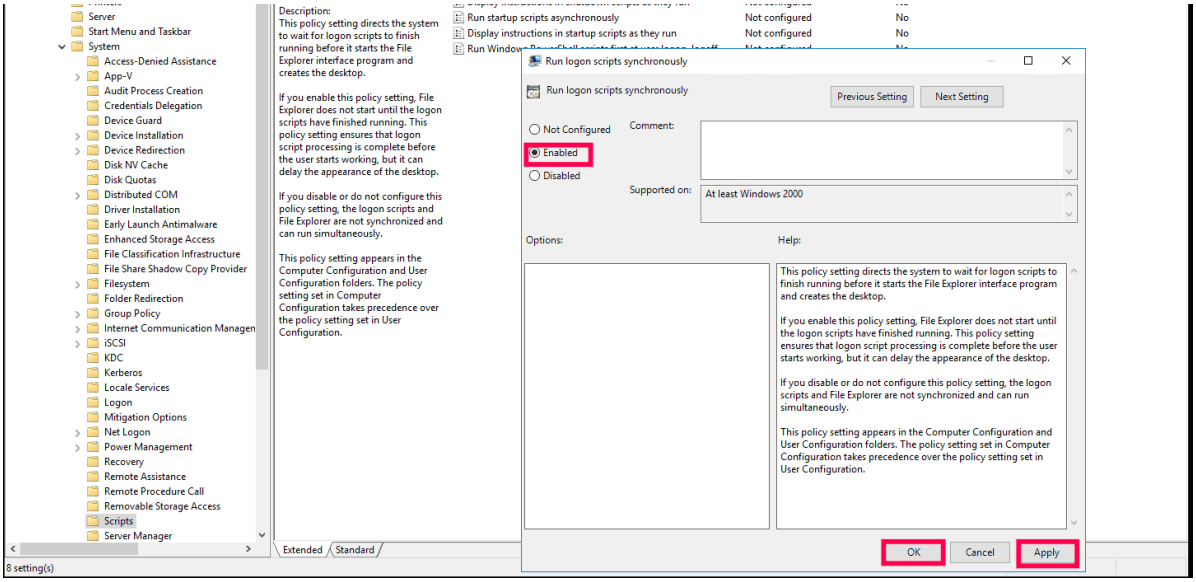


Figure 9: Enabling run logon scripts

5. Similarly, enable Maximum wait time for Group Policy scripts.
6. In the left pane, navigate to System and select Logon.
7. Double-click Always wait for the network at startup and logon and enable it.
8. Click Apply and then OK.

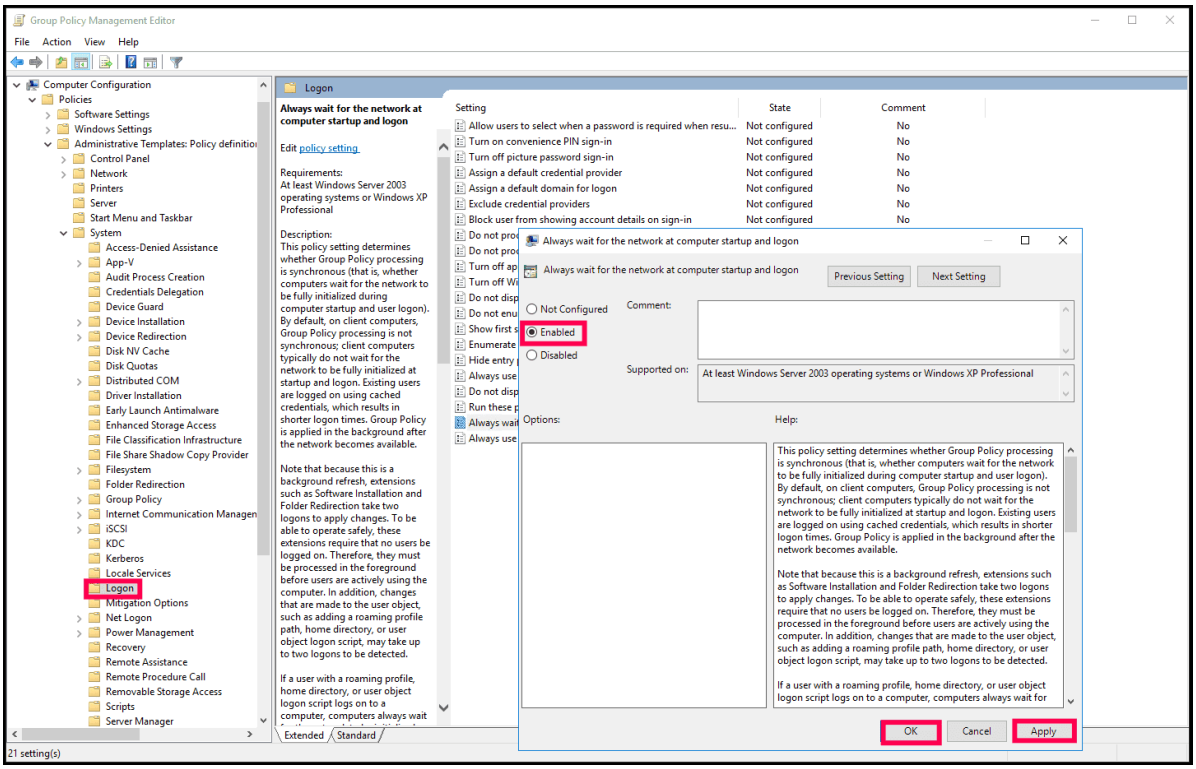


Figure 10: Configuring logon setting

9. In the left pane, navigate to System and select Group Policy.
10. Double-click Group Policy slow link detection and enable it.
11. Click Apply and then OK.

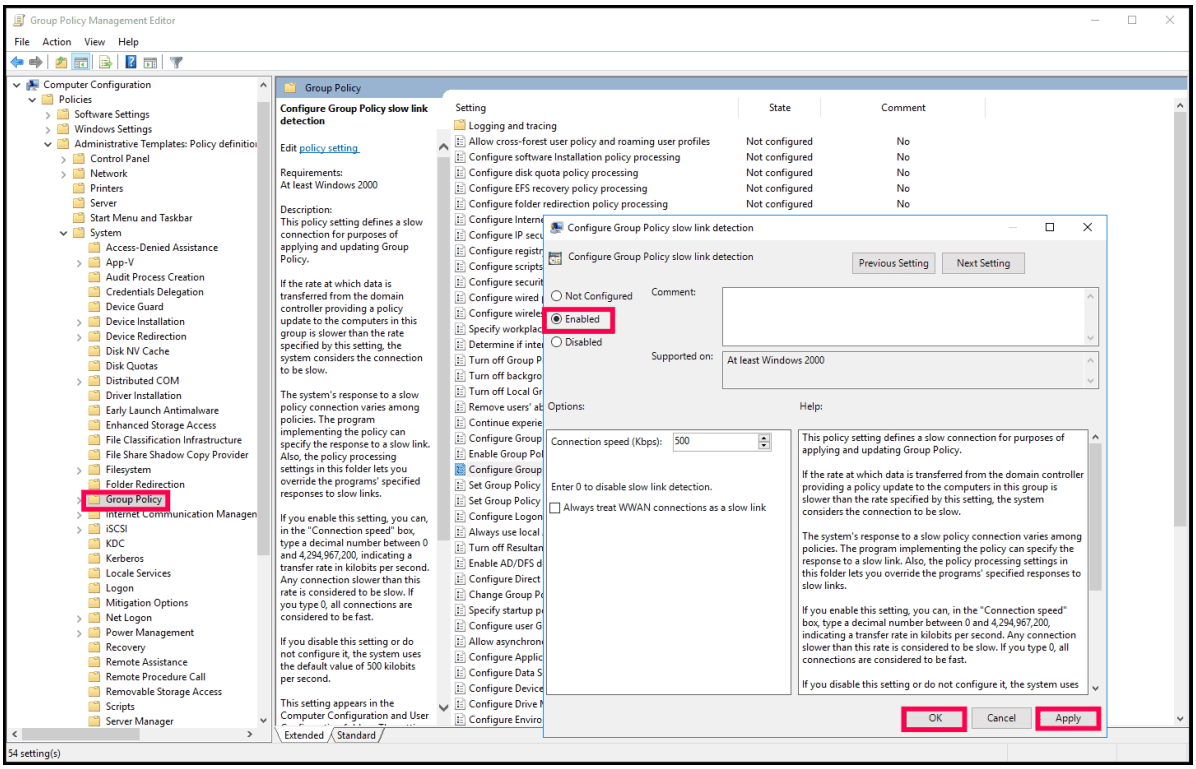


Figure 11: Configuring group policy settings

Applying the GPO

NOTE To install the agent on multiple computers simultaneously, create an AD group and add all the required computers to that group. Then, apply the GPO to the group.

1. In Group Policy Management Editor, right-click the GPO and select Properties.
2. Navigate to the Security tab and unselect the Apply Group Policy permissions for Authenticated Users.
3. Click Add, then in the dialog box, select Object Types.
   - To apply the GPO to computers directly, ensure Computers is selected.
   - To apply it to a group, ensure Groups is selected.
   - Click OK to save and apply the changes.

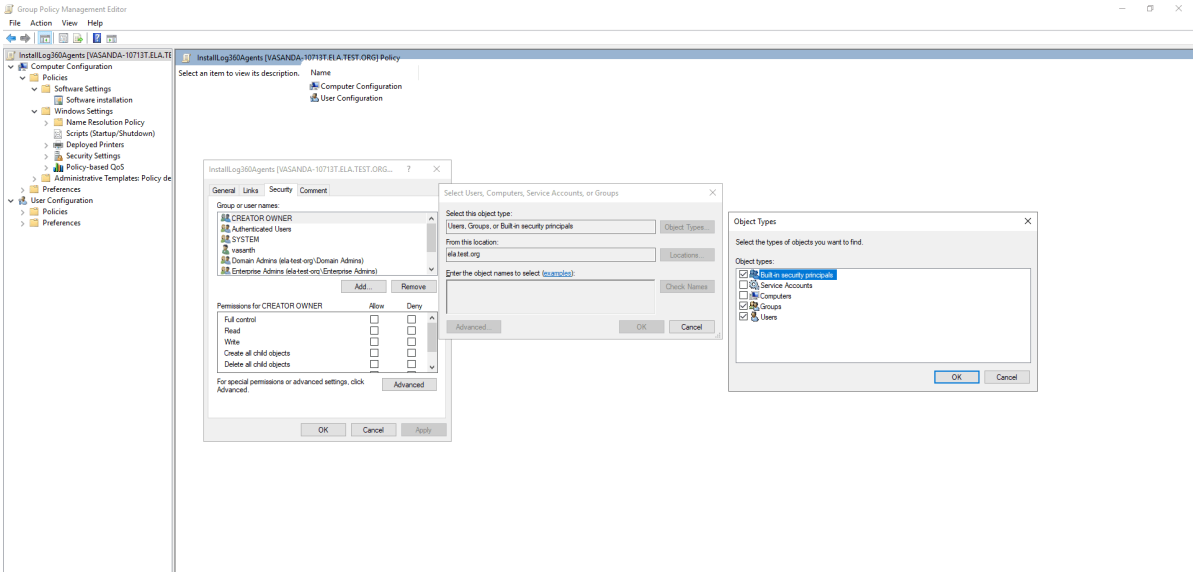




Figure 12: Selecting object types

4. Enter the name of the desired computer(s) or group(s), then click Check Names.
5. Select the correct object(s) and click OK to return to the properties dialog box.

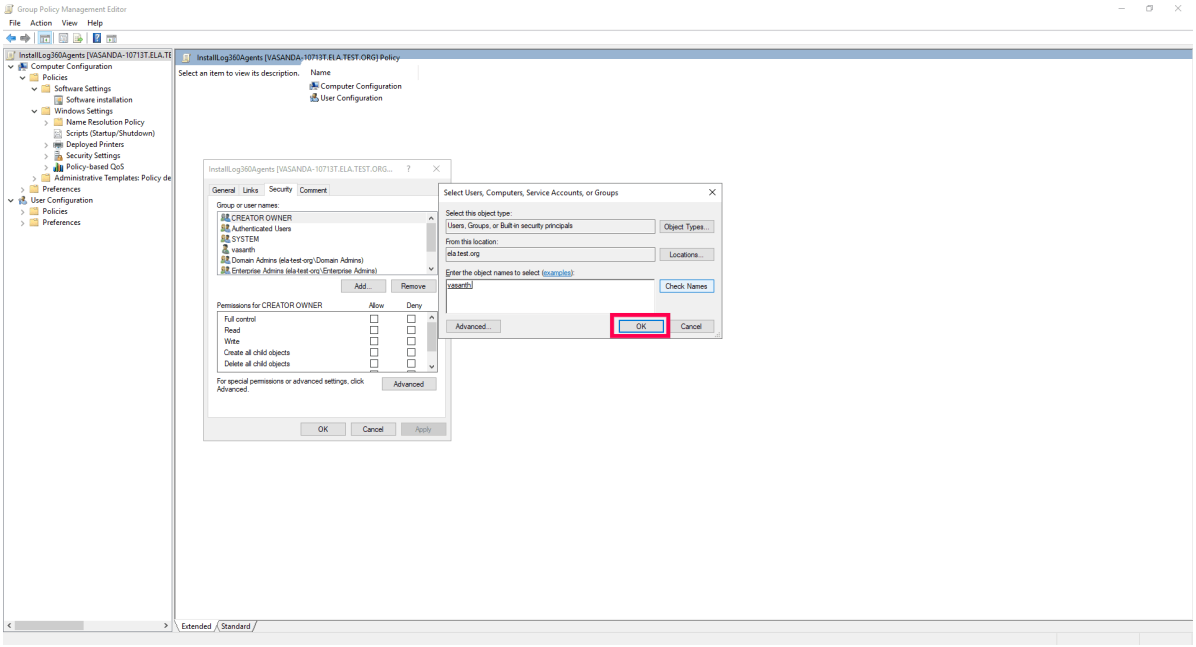
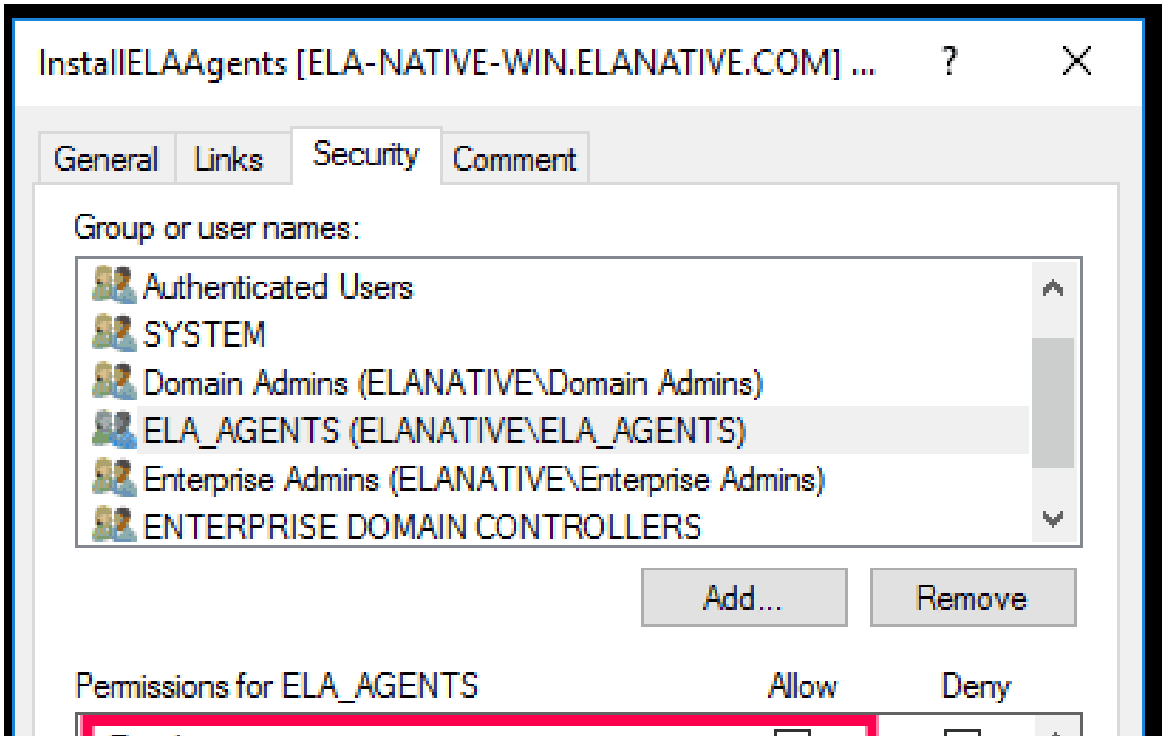


Figure 13: Selecting object types

6. In the Security tab, assign the following permissions to the selected computer(s) or group(s):
   - Read: Allow
   - Apply Group Policy: Allow



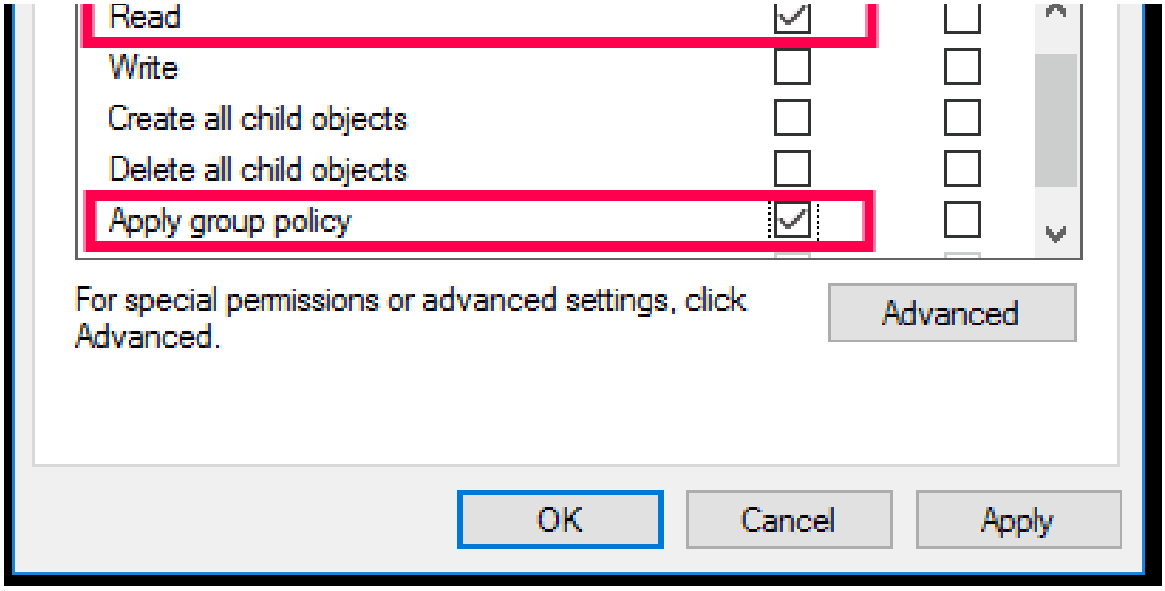


Figure 14: Configuring permissions

- Click Apply, then OK.
- In the Group Policy Management Console, right-click the Domain and select Link an Existing GPO.

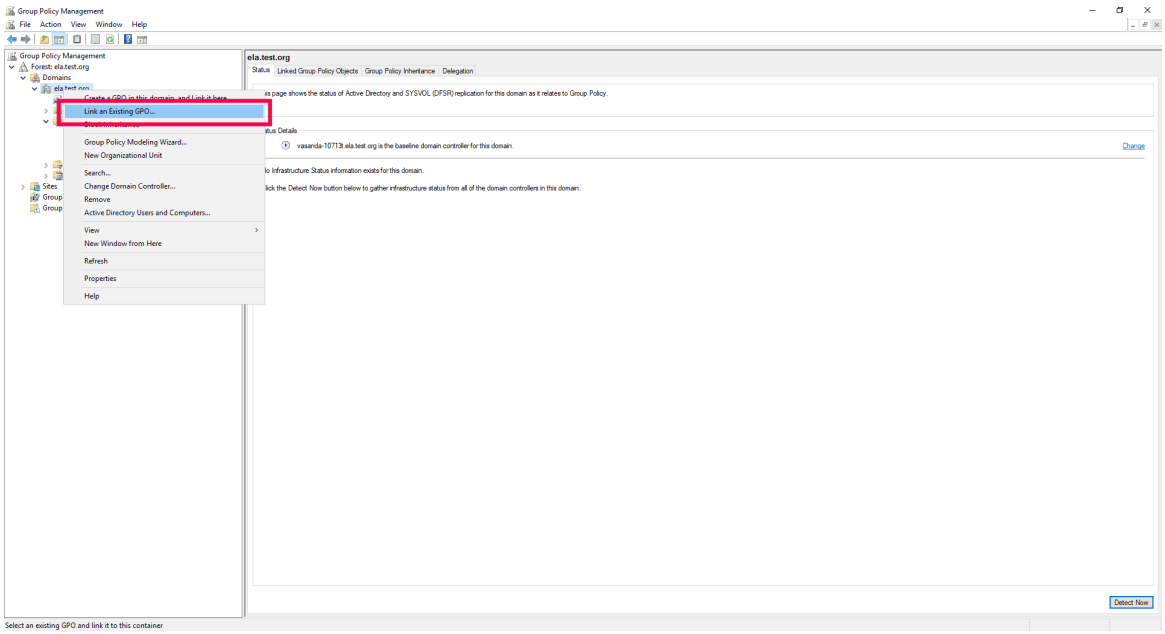
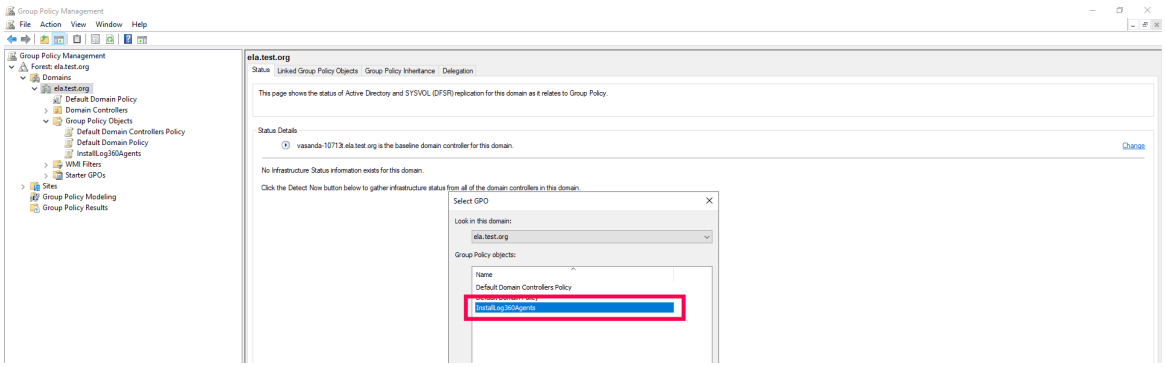


Figure 15: Linking an existing GPO

- Choose the GPO you created, then click OK.



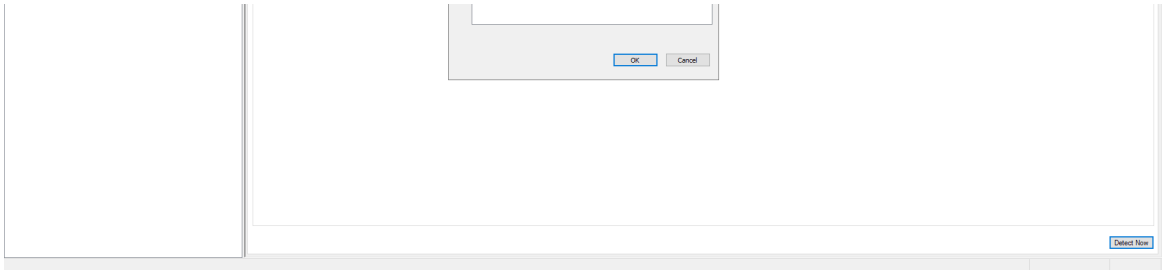


Figure 16: Selecting GPO

- Restart the computers to apply the GPO settings and wait for the reset password / unlock account link to appear on the Windows logon screen.

> NOTE: After installation, disable or delete the GPO to prevent the script from running at every startup.

Using Microsoft System Center Configuration Manager (SCCM) or similar deployment tools

1. Place the appropriate installer file in a network-shared folder:
   - Windows: Log360Agent.exe
   - Linux: EventLogAgent_<Arch>.bin
2. On the target devices, run the following command to install the agent:
   - For Windows:
     "Log360Agent.exe" SILENT_INSTALL /hide_progress /hide_splash
   - For Linux:
     ./EventLogAgent_64.bin > ./ELAAgent_InstallationLog.log 2>&1

Agent installation via Endpoint Central

Follow these steps to install the agent using Endpoint Central:

1. Create an EXE package
2. Deploy the package

Create an EXE package

> NOTE
>
> EXE (Executable Installer) is a vital file format in the Windows environment, primarily used for software installation and management.

- Log in to the Endpoint Central console as an administrator.
- Navigate to the Software Deployment tab, select Packages, and click Add Package.
- From the Add Package dropdown, select Windows.

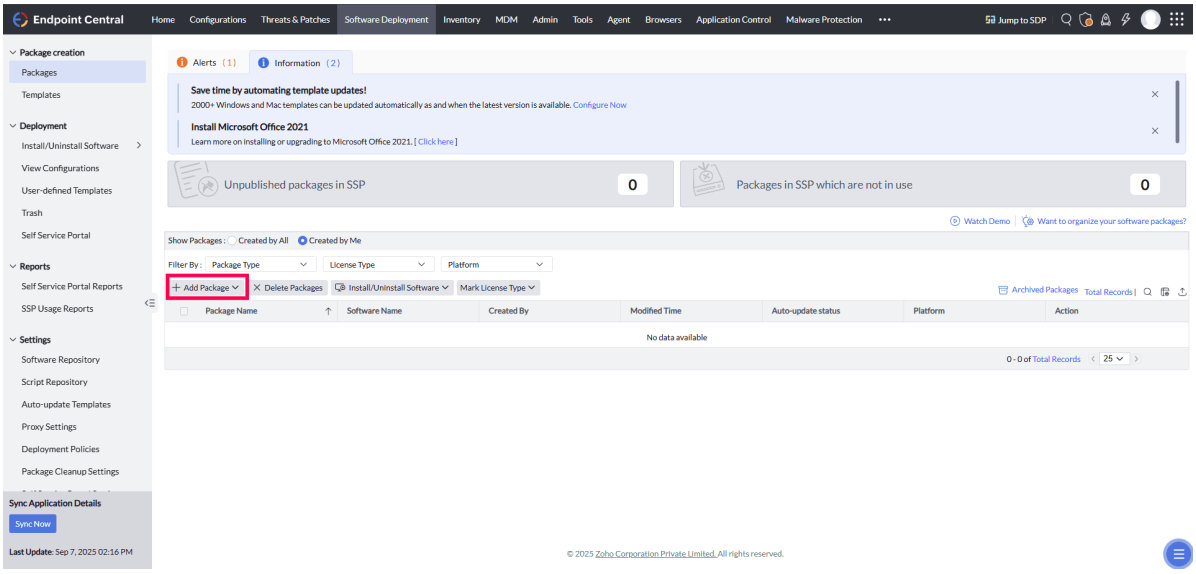
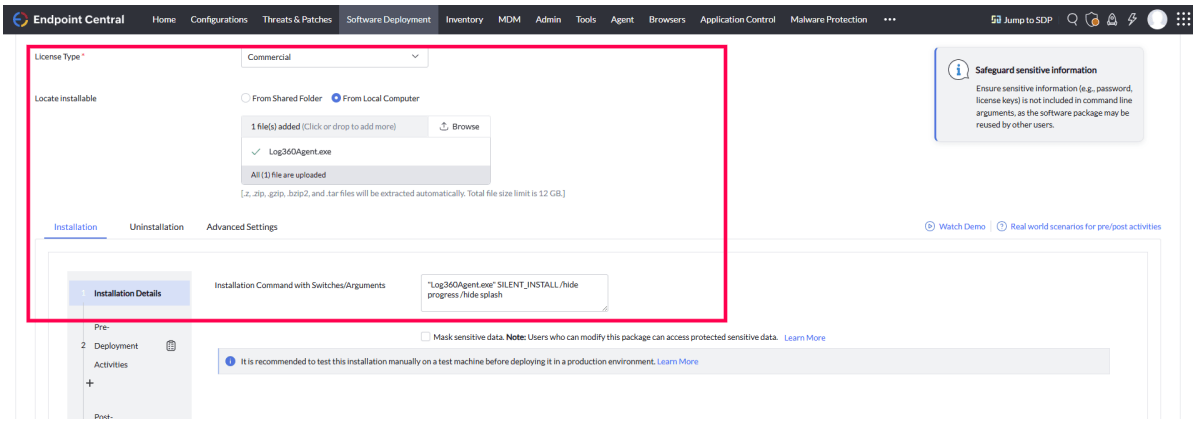


Figure 17: Adding a package

- Fill out the package details:
  - Package Name: Enter a name, for example, Log360 Agent.
  - Package Type: Select EXE / APPX / MSIEXEC / MSU.
  - License Type: Select Commercial from the drop-down.
  - Locate Installable: To install Log360Agent.exe, choose the Local Computer option to upload the file directly or opt for the Shared Folder option and ensure the Log360Agent.exe file is placed in the shared location.

> **NOTE**
>
> The product console includes .exe files for Windows and .bin files for Linux systems.



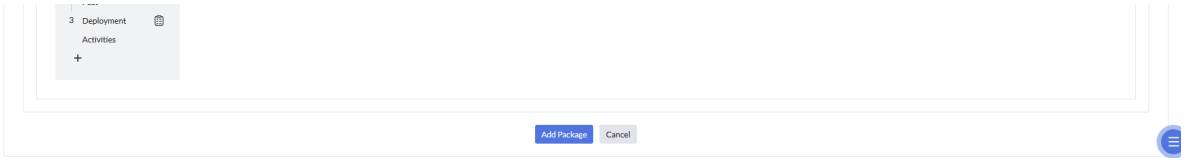


Figure 18: Configuring package details

- Update and enter the following text in the Installation Command with Switches/Arguments field. Log360Agent.exe SILENT_INSTALL /hide_progress /hide_splash
- Click Add Package to save the changes.

Deploy the package

After creating the EXE package, follow these steps to install the agent using Software Deployment:

- Navigate to the Software Deployment tab, select Deployment, and click Install/Uninstall Software.

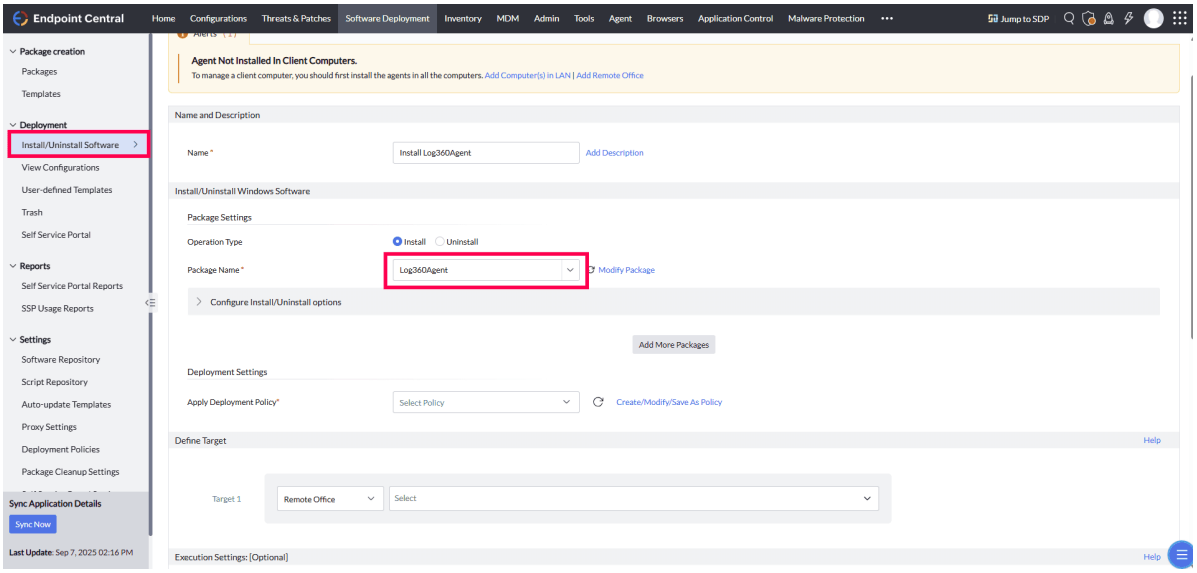


Figure 19: Installing the agent

- Provide a name for the installation, for example, Install Log360 Agent, and add an optional description if needed.
- Select Install as the Operation Type, and from the Package Name dropdown, choose the package created earlier.
- Configure the required options under Deployment Settings:
  - Configure additional install/uninstall options if needed.
  - Specify when the deployment should occur.
- Under Define Target, select the computers or domains where the package should be deployed.

> NOTE
>
> If needed, configure Retry options in Execution Settings to handle installation failures.

- Click Deploy to initiate the installation.

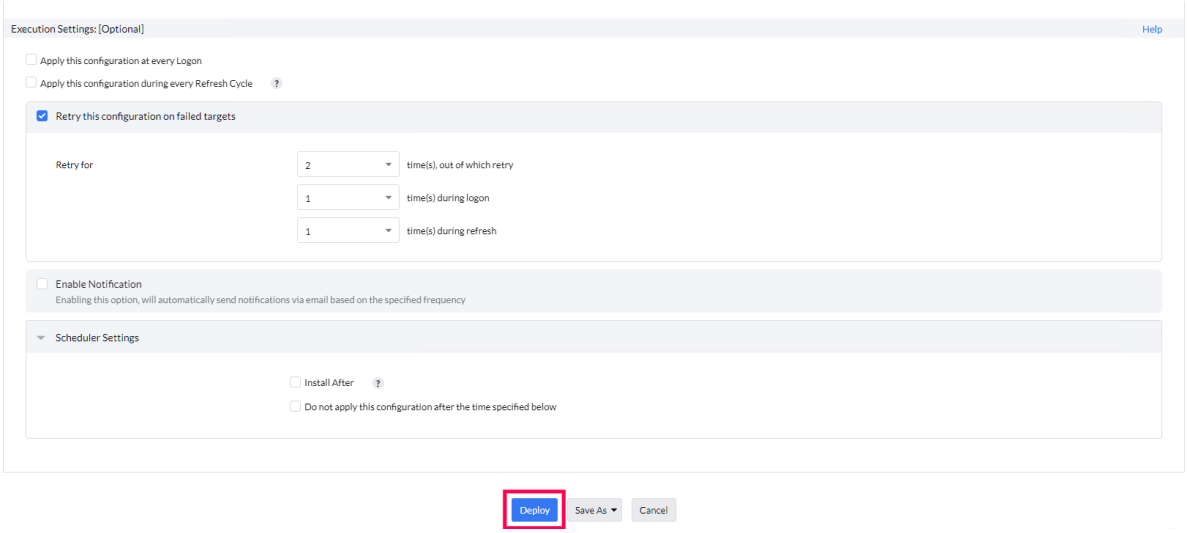


Figure 20: Initiating the installation

- Track the deployment progress and status under Deployment > View Configurations.

Manual installation

You can also install the agent manually by downloading it from the console and running the installer on the required devices.

For Windows devices

1. Log in to your account and go to the Settings tab.
2. Under Admin Settings, select Collectors/Agents.
3. Click Install Agent in the top-right corner.

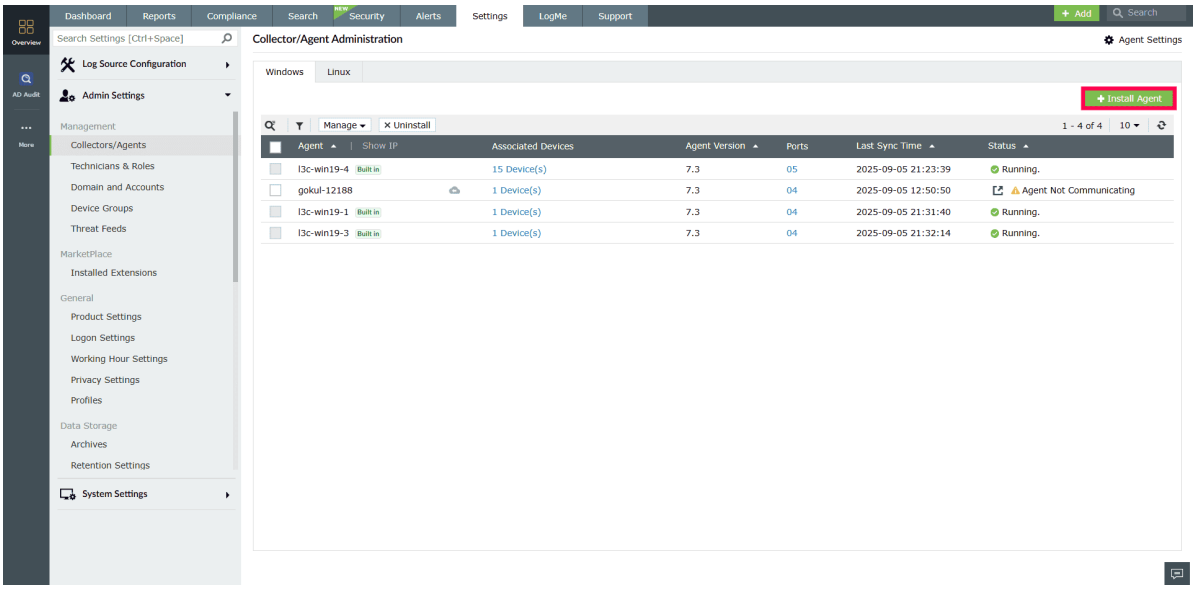


Figure 21: Installing agent

4. In the installation window, select Install Manually to download the agent package.

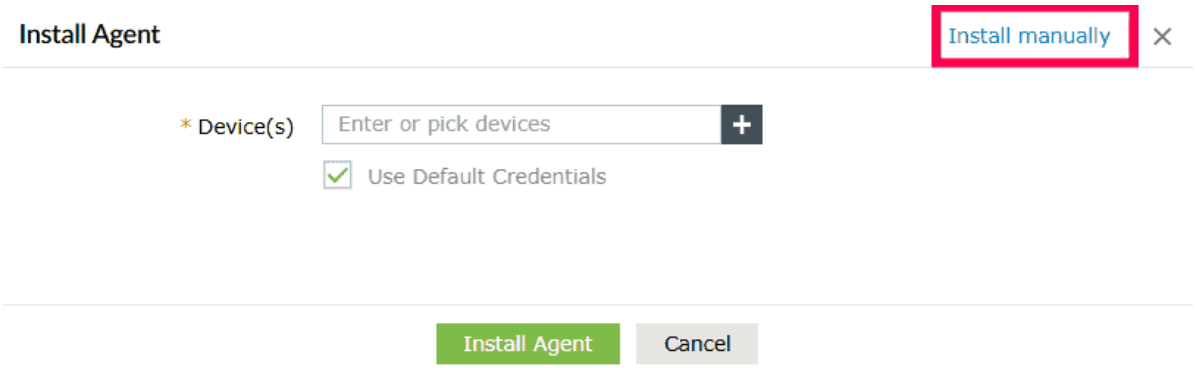


Figure 22: Installing manually

5. Run the downloaded installer on the target device.

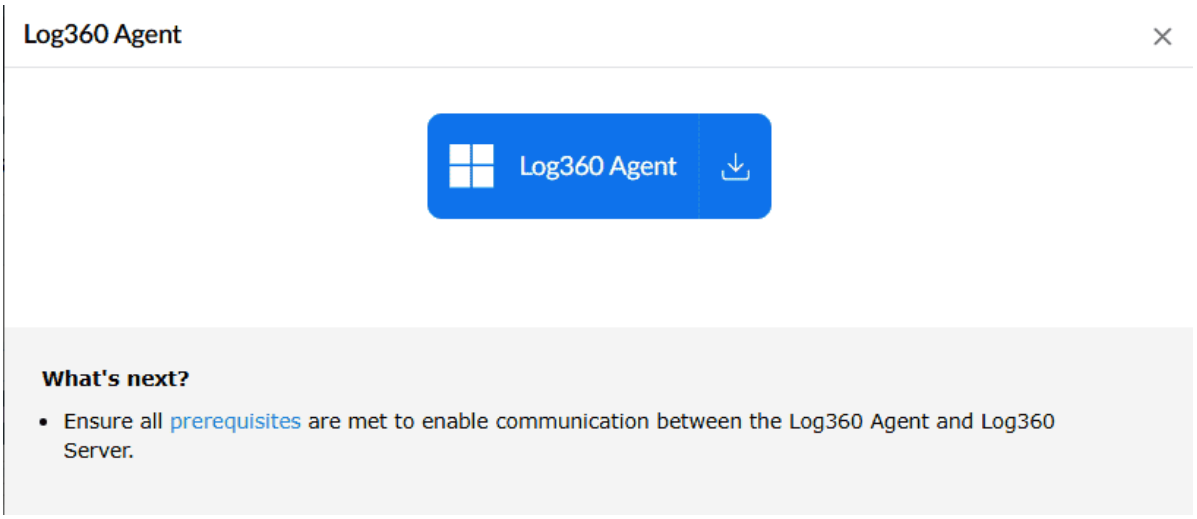


Figure 23: Downloading the installer

Read also

This document explained when and how to install the Log360 agent using different deployment methods. To learn how to manage agents, refer to the following document:

- Managing agents

9.1.12.3. Managing agents

Last updated on: September 12, 2025

In this page

Overview

Updating an agent

Uninstalling an agent

Force restart an agent

Associate devices to an agent

Stop an agent

Overview

This page explains how to manage agents, which includes updating agent configurations, uninstalling agents, force restarting them, associating devices, and stopping agents.

Updating an agent

1. Log in to your account.
2. Navigate to the Settings tab, and under Admin Settings, select Collectors/Agents.
3. Hover over the agent you want to update and click the ✎ icon that appears.

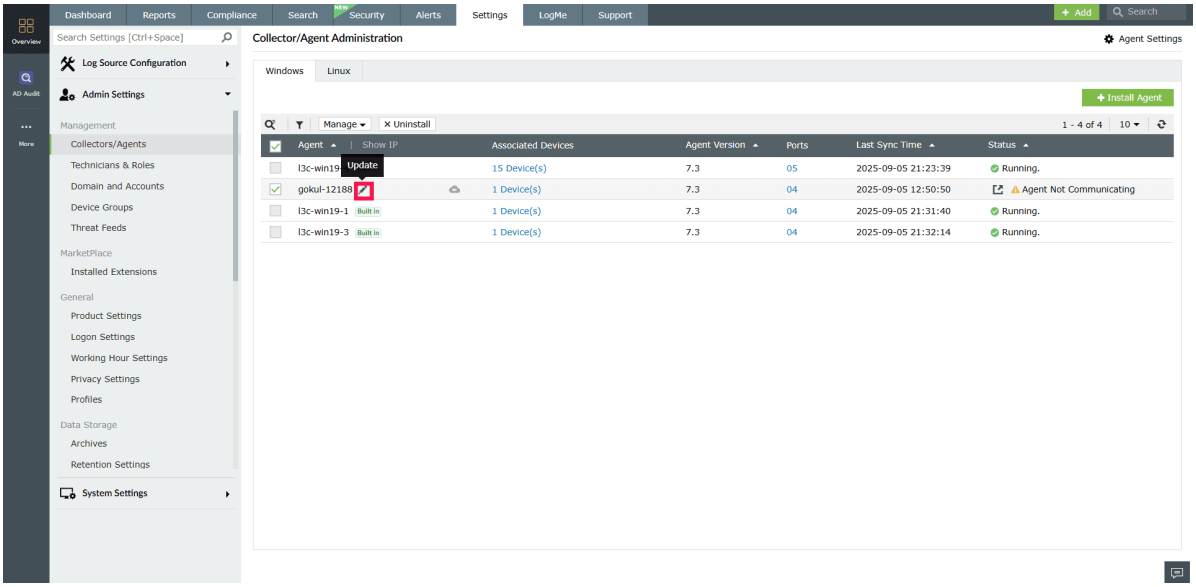


Figure 1: Updating an agent

4. In the pop-up window, make the necessary changes to the agent configuration.

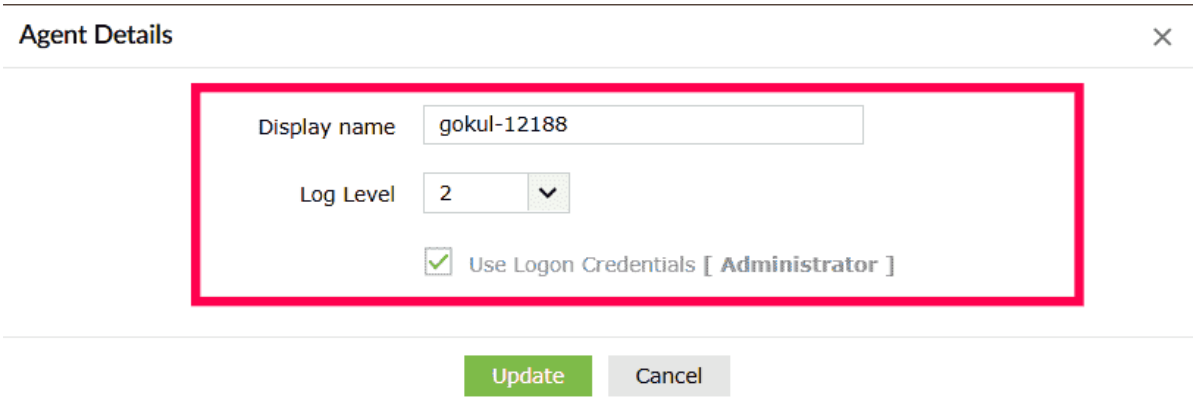


Figure 2: Updating an agent

5. Once you have made the required updates, click Update to save the changes.

Uninstalling an agent

1. On the Collection/Agent Administration page, select the checkbox next to the agent you want to uninstall.
2. Click the X Uninstall button.

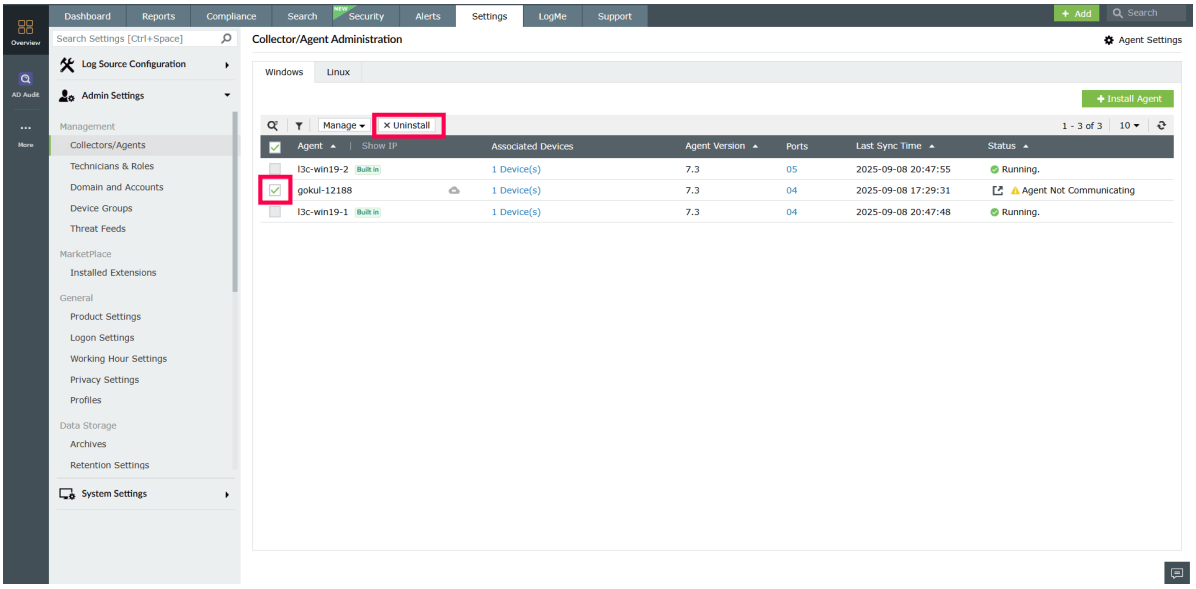


Figure 3: Updating an agent

3. In the confirmation pop-up, click Yes to complete the uninstallation.

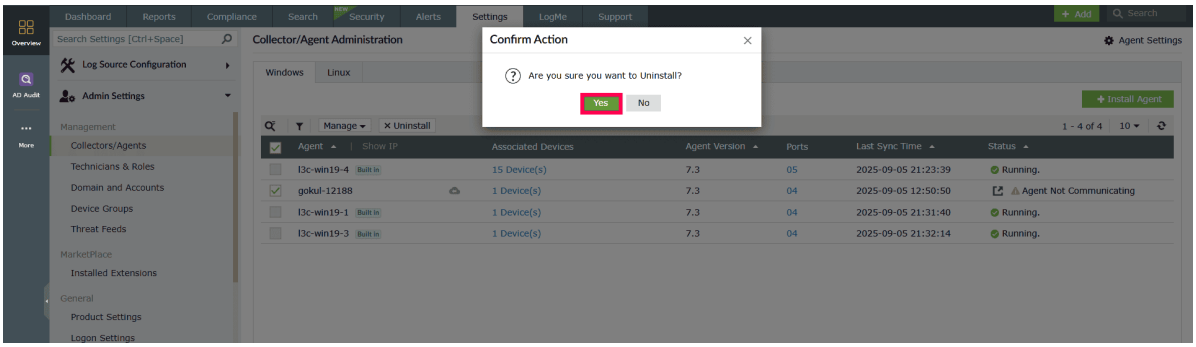




Figure 4: Updating an agent

Force restart an agent

1. On the Collection/Agent Administration page, select the agent(s) you want to restart by ticking the checkbox next to the agent name.
2. Click Manage and choose Force Restart from the drop-down menu.

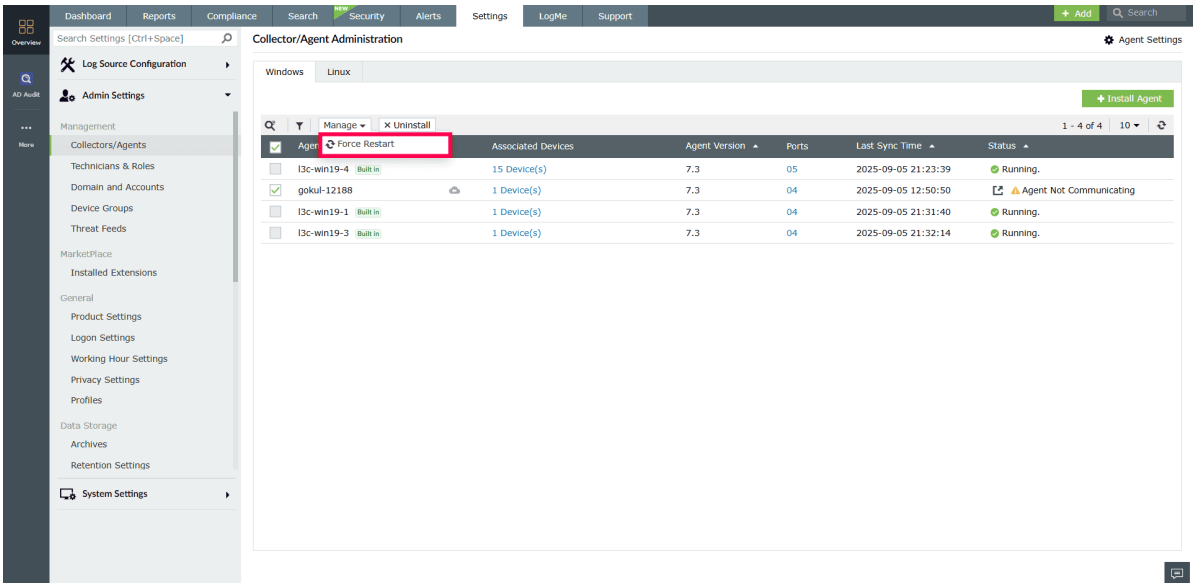
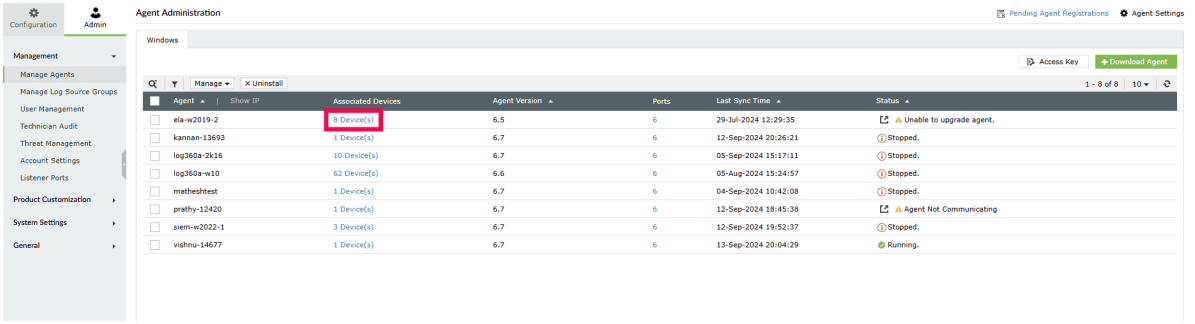


Figure 5: Force restarting an agent

3. Confirm the action by clicking Yes. The selected agent(s) will now be force restarted.

Associate devices to an agent

1. On the Collection/Agent Administration page, click the Associated Device(s) column for the desired agent.



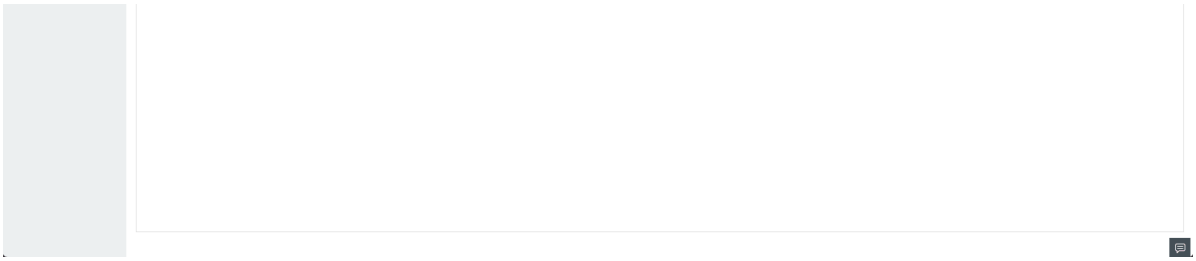


Figure 6: Selecting a device

2. In the pop-up window:

- To remove a device, hover over it, click the delete icon, and confirm by selecting Yes.

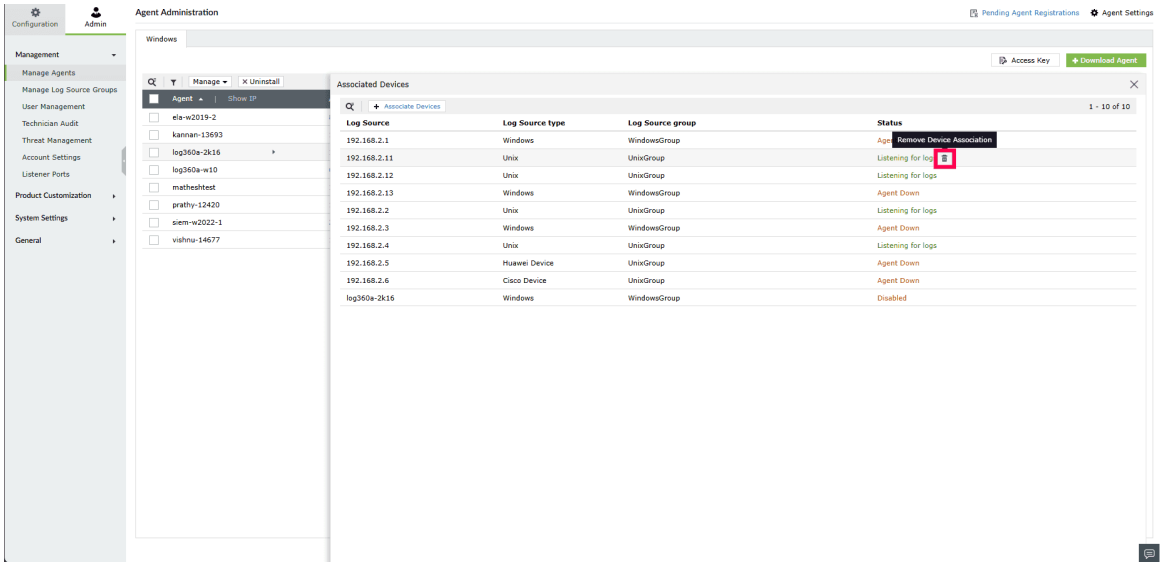


Figure 7: Deleting a device

- To add devices, click + Associate Device(s), select the desired devices, and click Add.

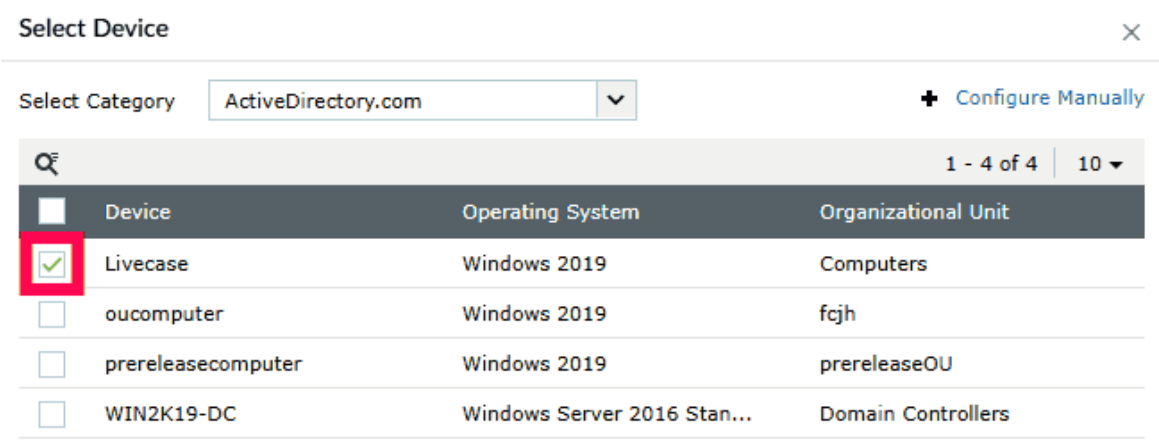




Figure 8: Associating a device

Stop an agent

1. On the Collection/Agent Administration page, hover over the agent's Status column and click Stop.

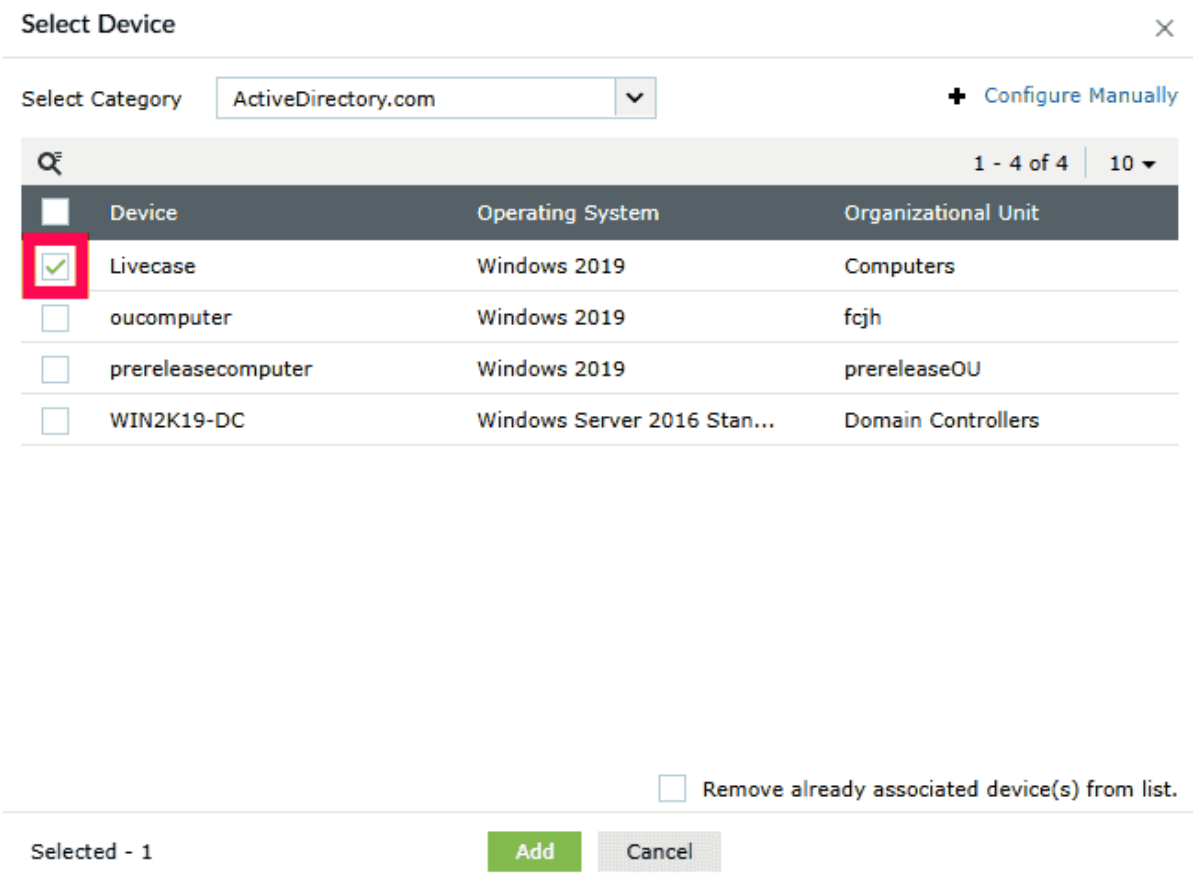


Figure 9: Stopping an agent

Read also

This page explained how to manage agents in Log360, including updating, uninstalling, force restarting, associating devices, and stopping agents. To learn how to install agents and configure agent settings, refer to the following document:

- Agent installation
- Agent settings

9.1.12.4. Agent settings

Last updated on: September 12, 2025

In this page

Overview

Settings configuration

Overview

This page details how to configure agent settings for offline log collection and communication ports. These settings ensure reliable log collection and secure communication with the server.

Offline log collection

When the agent is disconnected from the network, unable to upload logs, or when storage capacity is exhausted, logs can be temporarily stored locally.

- You can set a maximum limit for this local storage.
- Once the limit is reached, the agent will stop collecting logs until the connection is restored.
- Collected logs will be uploaded automatically once communication with the server resumes.

Configuration	Default value	Description
Maximum size of data directory, when agent is unable to send data to server or storage is full	0	If disabled, log collection stops when the agent cannot send data. When enabled, logs are stored locally up to the configured size (in GB). These logs are later uploaded once the connection is re-established.

Agent communication port

You can configure the port used by the agent to communicate with the server.

- Use default HTTPS port: The agent communicates over the standard HTTPS port.
- Use a custom HTTPS port: Specify a port number for agent-server communication.

> NOTE
>
> All communication occurs over HTTPS, ensuring secure transmission of data.

Settings configuration

1. Log in to your account.
2. Go to the Settings tab.
3. Under Admin Settings, select Collectors/Agents.
4. In the Collectors/Agents administration page, click Agent Settings in the top-right corner.
5. To enable offline log collection:
   - Toggle Enable Offline log collection.
   - Enter the maximum size of the data directory (in GB).

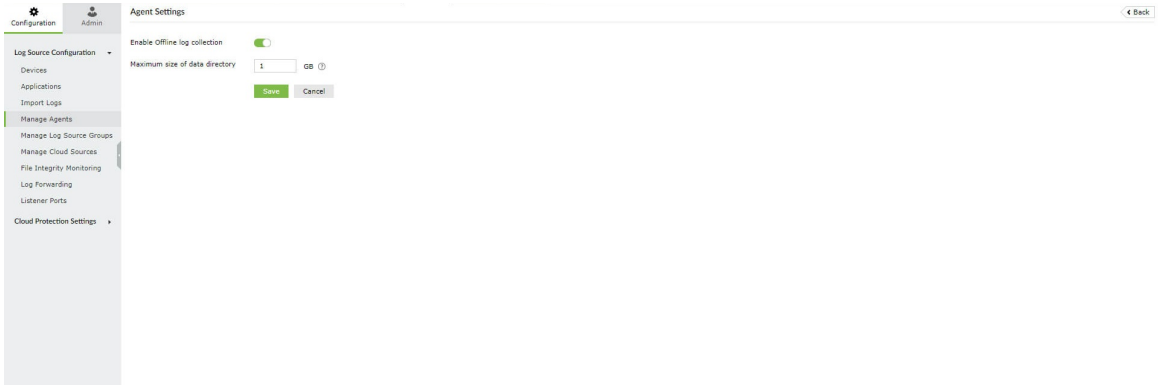


Figure 1: Enabling offline log collection

6. To configure the communication port:
   - Choose either Use default HTTPS port or Use a custom HTTPS port.
   - If custom, enter the port number.

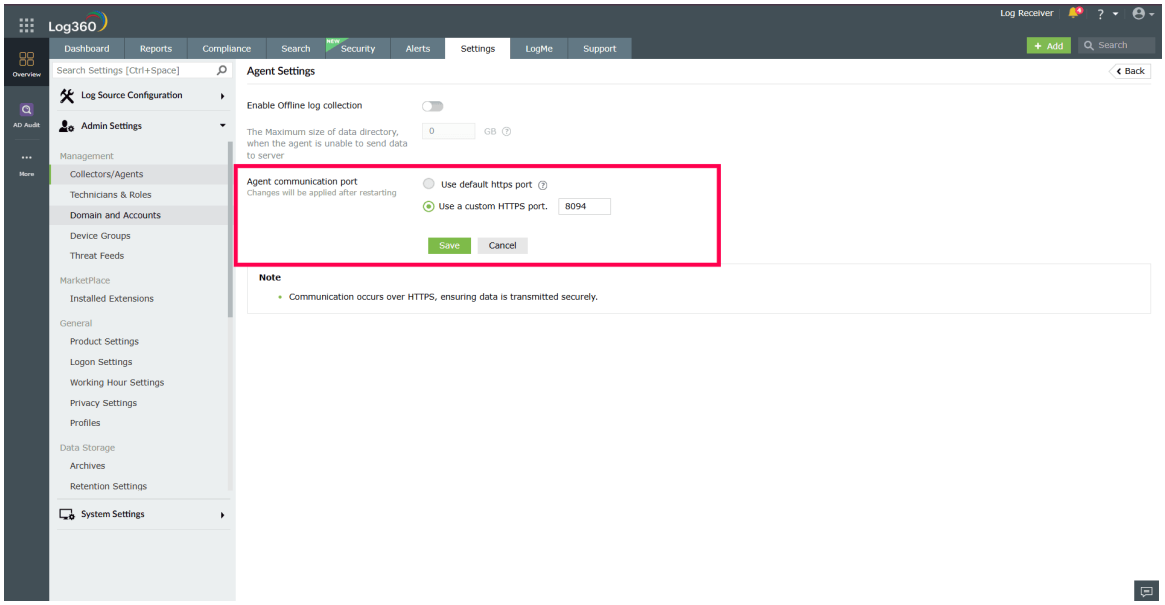


Figure 2: Configuring communication port

NOTE

Any changes to the agent communication port will take effect only after restarting.

7. Click Save to apply changes.

Read also

This page explained how to configure agent settings in Log360, including offline log collection and communication ports. To learn how to install and manage agents, refer to the following documents:

- Agent installation
- Managing agents

9.1.13.1. About Centralized Technician Management Log360

Last updated on: September 12, 2025

In this page

Use cases

Pre-requisites

Delegation and permission inheritance

Centralized Technician Management (CTM) in Log360 enables users to manage technician roles and permissions for all integrated components from a single console. The supported integrations include:

- ADAudit Plus
- Cloud Security Plus
- Exchange Reporter Plus
- DataSecurity Plus
- Log360 UEBA
- ADManager Plus
- M365 Manager Plus

> NOTE
>
> To view and manage technicians and their roles centrally in Log360, all individual product instances must be integrated with Log360.

When a user is configured as a technician, they are granted permissions to perform actions, access, and manage tabs of the product console and its components. A technician can be assigned to one or multiple domains, based on organizational requirements.
The console provides three default technician roles as below.

- Admin - Complete control over the application.
- Operator - Limited privileges, allowing create and delete operations on assigned resources.
- Guest - Read-only access to assigned security resources (device groups).

In addition to these roles, you can also create custom roles to assign more permissions to users.
The CTM system of Log360 supports group-based delegation using Active Directory (AD) security groups or Organizational Units (OUs). This simplifies permission management for multiple users. When a user is added to or removed from an AD group or OU, the changes are automatically applied in the console.

Use cases

1. Unified access management

Managing technicians separately in multiple product consoles can lead to inconsistent permissions and added overhead.
By leveraging CTM: Access levels and permissions can be configured in Log360 and applied across all supported child components. This eliminates the need to log in to each component individually, ensuring uniform access control and reducing user complexity.

2. Role assignment and granular control

Assigning roles to each technician individually can be time-consuming in large environments, especially when different levels of access are required.
By leveraging CTM: Roles can be assigned to Active Directory security groups or OUs in the console. Users who belong to these groups automatically inherit the assigned roles upon login. This not only simplifies delegation but also ensures granular control by allowing administrators to define precise permissions for multiple components, domains, and groups from a single console.

3. Updating multiple technicians

Making the same changes individually for each technician can be time-consuming, especially in large environments.
By leveraging CTM:Users can update settings for multiple technicians at once from a single console. This centralization saves time, ensures consistency across accounts, and reduces the risk of manual errors.

Pre-requisites

Ensure the following before using CTM:

1. All integrated components are updated to the required build versions or above:
    - ADAudit Plus - 7009
    - Cloud Security Plus - 4130
    - Exchange Reporter Plus - 5615
    - DataSecurity Plus - 6061
    - Log360 UEBA - 4033
    - M365 Manager Plus - 4502
    - ADManager Plus - 7130
2. PAM360 does not support this feature.
3. In the limited versions of M365 Manager Plus, Exchange Reporter Plus, and Active Directory reporting component (Limited version of ADManager Plus), available for integration with Log360 only select roles such as Operator Extended, Log360User, and Super Admin Limited are available for assignment, respectively. To access additional roles and features, you need to upgrade to the full versions of these products:
    - M365 Manager Plus
    - Exchange Reporter Plus

- ADManager Plus

4. The limited version of ADManager Plus restricts the number of technician accounts to 25. To increase this limit, upgrading to the full version is required.

Delegation and permission inheritance

When technicians are created from a configured technician group (Security Group or OU), their permissions, roles, and delegations are inherited from that group.
The following scenarios explain how inheritance works in group-based delegation.

Editing a technician configured under a group/OU

When a technician from a group/OU is edited, the user will be configured as an individual technician in Log360.

Sync behavior with child components

Group or Organizational Unit (OU) configurations for technicians in Log360 are not directly mirrored in the child components (CC). Instead, the synchronization works as follows:

1. User already exists in the child component
   - If a user already exists in the child component before logging into Log360, that user will be recognized in the child component as an individual technician.
   - During synchronization, the existing individual technician in the child component is detected and reflected in Log360.
2. User does not exist in the child component
   - If the user does not exist in the child component before logging into Log360, the user will be configured under the assigned Group/OU in Log360.
   - This configuration is then synced to the child component, but as an individual technician, not as part of the Group/OU.

Groups and OUs are managed only within Log360 and are not synced with the child components.

Technicians assigned to multiple groups

If a user belongs to more than one group with different roles and delegations:

- In Log360 and ADManager Plus, the user inherits roles and delegations from all groups.
- In other components, only the configuration of the first group the user was added to is applied.

Inheritance scenarios

In each case, assume User 1 is a member of Group 1.

1. User 1 is already configured as a technician
   - Outcome: If User 1 is already configured as a technician, only their individual roles are retained. Roles assigned through the group are not applied.
2. User 1 is removed from Group 1
   - Outcome: If User 1 is removed from Group 1 in Active Directory, they can log in only if they are directly

configured as a technician. Any roles and delegations that were assigned through the group will no longer be available.

3. Group 1 is disabled in the technicians list
   - Outcome: User 1 is disabled.
4. Group 1 is deleted from the technicians list
   - Outcome: User 1 is deleted.
5. Group 1 is deleted from Active Directory
   - Outcome: User 1 can log in only if directly configured as a technician.
6. User 1 is modified
   - Outcome: User 1 is removed from the group and configured as an individual technician.

> NOTE
>
> In Log360 and ADManager Plus, any individual technician can be a part of multiple technician groups.

Read also

This document provides an overview of Centralized Technician Management, including its use cases and prerequisites. For more related functionalities, refer to the following articles:

- Adding technicians
- Managing technicians

9.1.13.2. Adding technicians

Last updated on: September 12, 2025

In this page

Overview

Adding a centralized technician

Using product authentication

Using Active Directory (AD) authentication

Adding a centralized technician group/ OU

Overview

Centralized Technician Management in Log360 allows you to create and manage technician accounts from a unified console. Instead of configuring technicians individually in each child component, you can integrate them in the product console and delegate access across supported components.
This section guides you through adding technicians using either product authentication or Active Directory (AD) authentication, with roles and access permissions applied centrally. You can also create technician groups by importing users from AD groups or OUs to streamline delegation.

Adding a Centralized Technician

You can add technicians in Log360 either using product authentication or Active Directory (AD) authentication. Once added, roles and access permissions can be delegated across supported components from the same interface.

Using product authentication

1. In your account, navigate to the Settings tab.
2. Under Admin Settings, select Technicians & Roles.

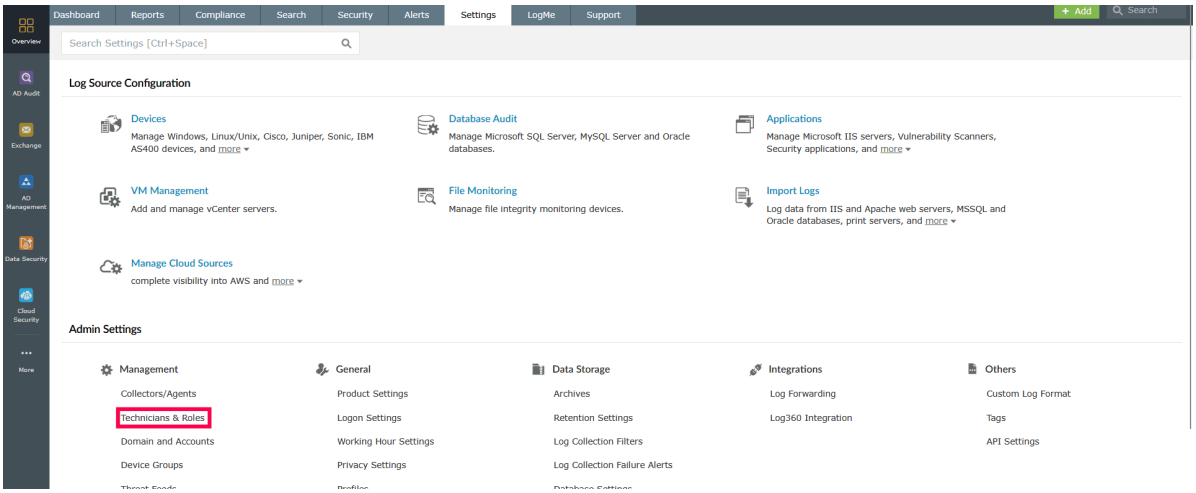




Figure 1: Navigating to Technicians and Roles

3. Click the + Add Technician at the top-right corner.

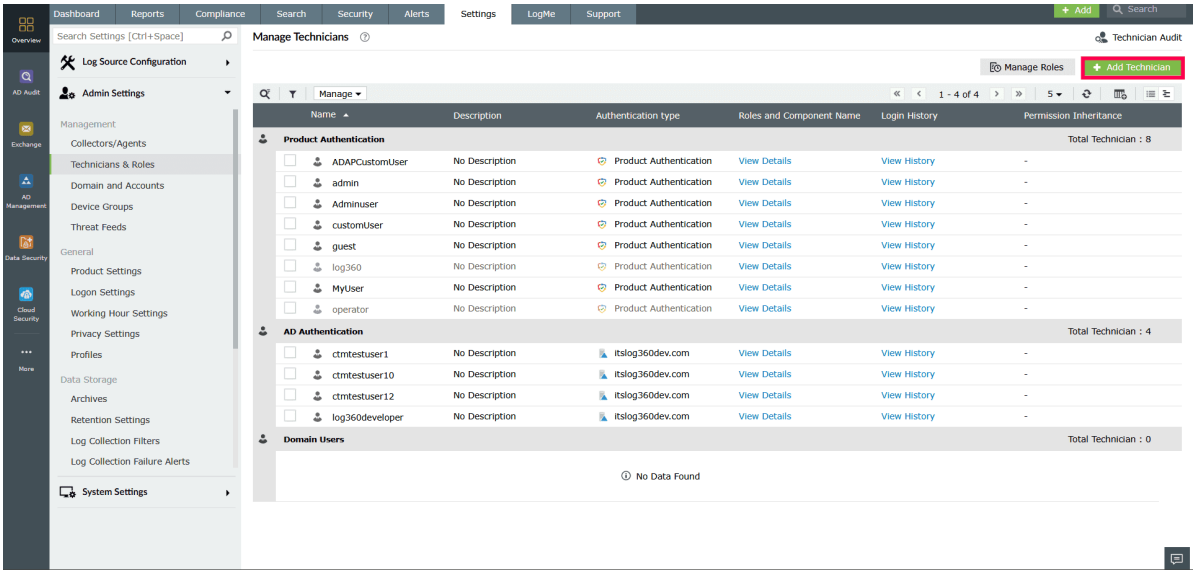


Figure 2: Adding a centralized technician

4. In the Authentication Type dropdown, select Product Authentication.

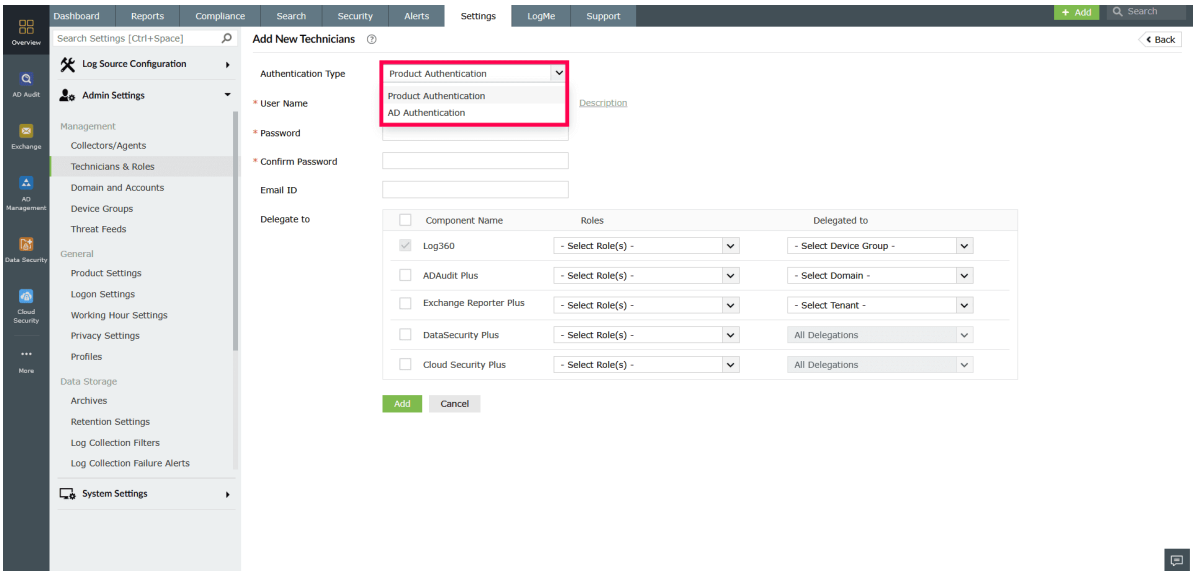
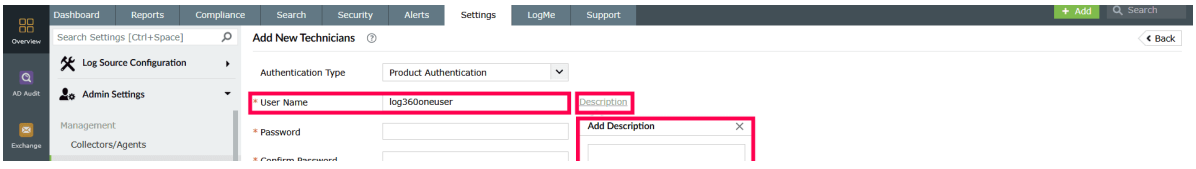


Figure 3: Selecting Authentication Type

5. In the User Name field, enter a name for the technician. You can optionally add a description using the Description button.



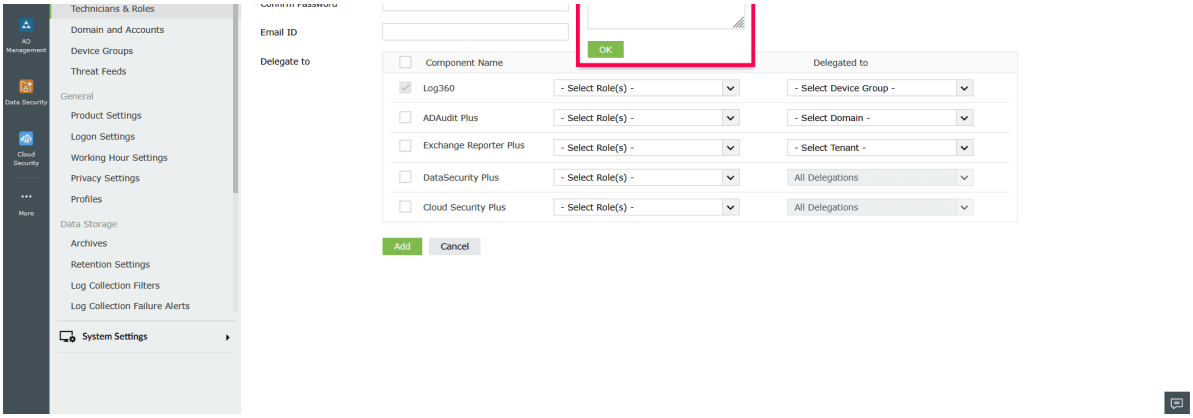


Figure 4: Configuring Technician settings

6. Enter and confirm a new password in the respective fields.

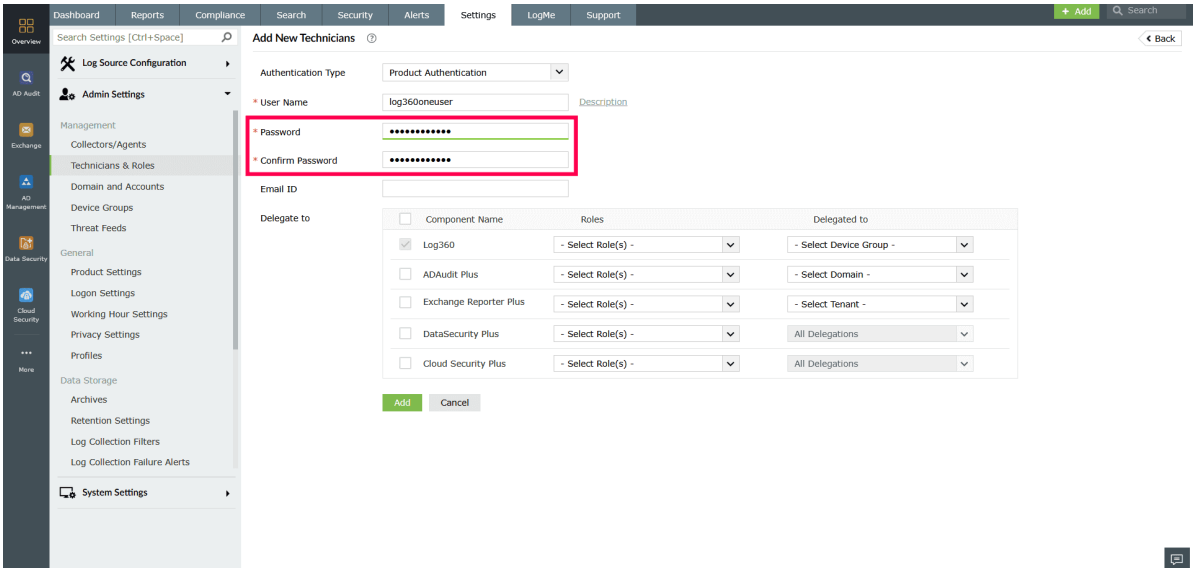


Figure 5: Configuring Technician settings

7. Provide a valid email address of the technician in the Email ID field. This is an optional field.

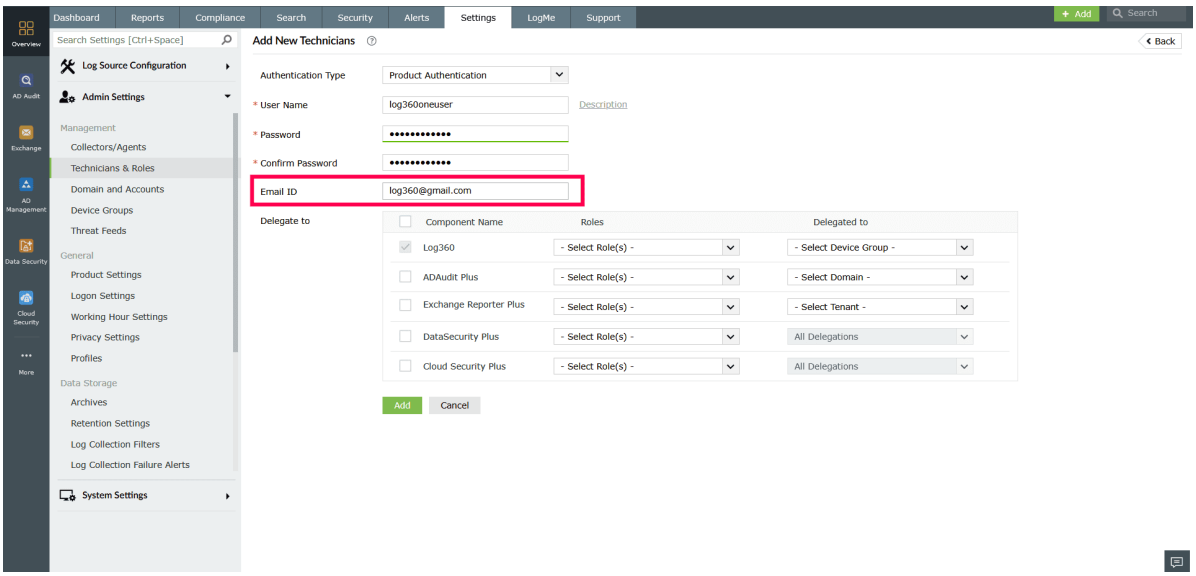


Figure 6: Configuring Technician settings

Figure 6: Configuring Technician settings

8. To assign roles for Log360:

- Use the Roles dropdown to assign the technician's role.

> NOTE
>
> Refer to this section to create and manage roles

- Use the Device groups dropdown to specify the groups the technician should have access to. Once done, click Add.

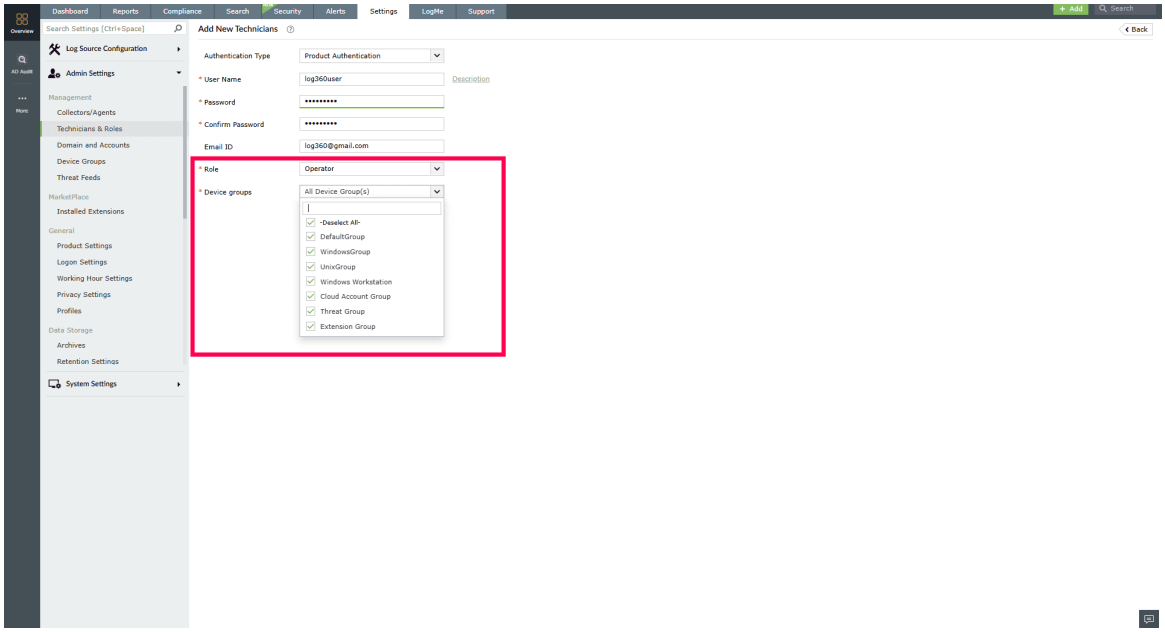


Figure 7: Selecting device groups

9. If components are integrated, you can delegate access to specific roles and entities in each component:

- In the Delegate to section, select the checkbox next to the components you want the technician to access.

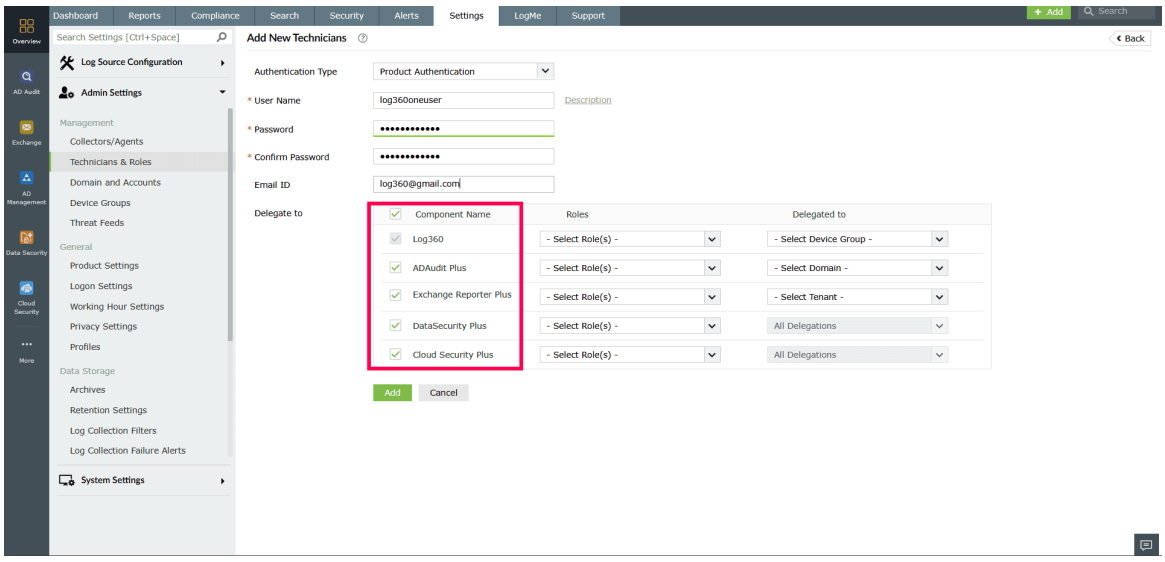


Figure 8: Selecting components

- For each selected component:
  - Assign the Role by selecting the role from the Roles drop-down
  - Specify the delegated entity using the appropriate dropdowns provided for each component.

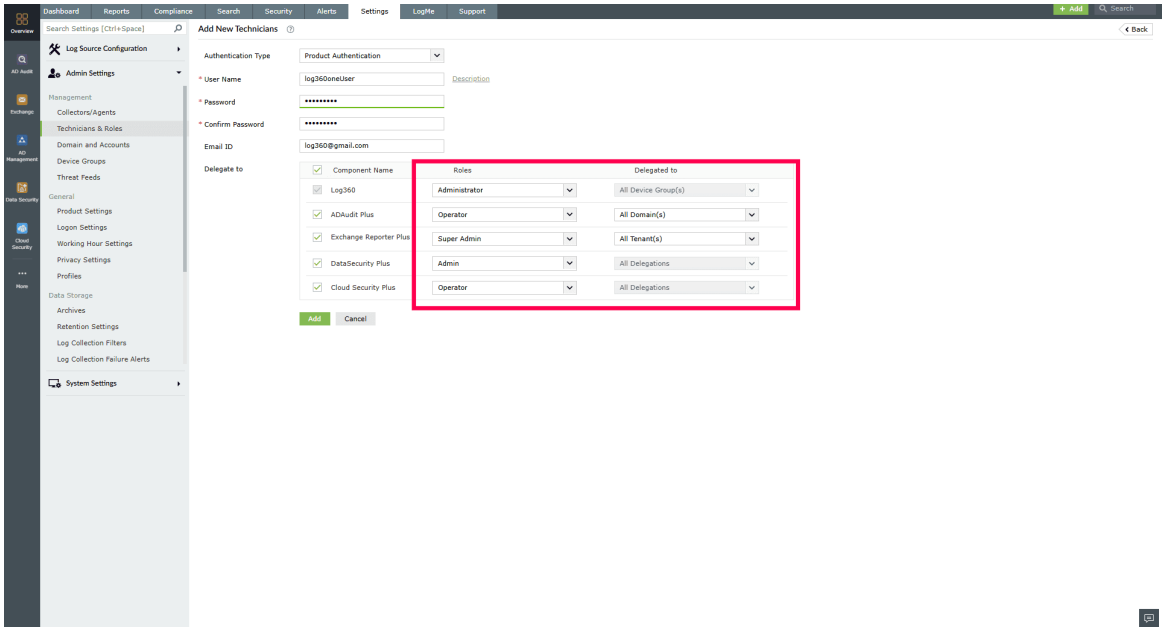


Figure 9: Assigning roles and delegations for integrated components

> NOTE
>
> To integrate components with the product, refer to this help document.

10. Once done, click Add to complete the technician setup.

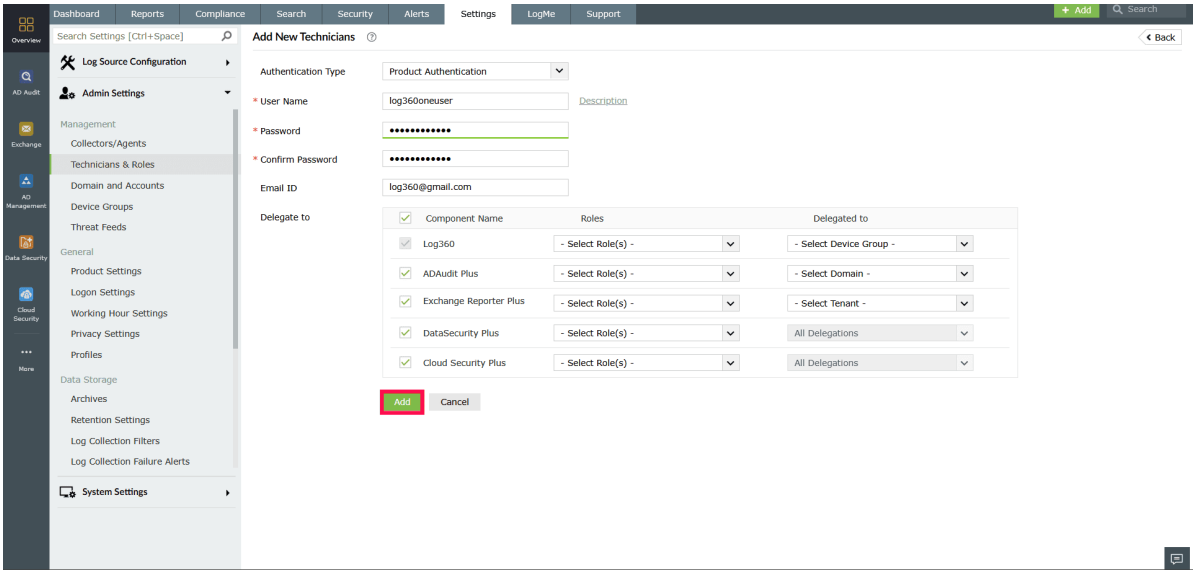


Figure 10: Adding a new technician

Using Active Directory (AD) authentication

1. In the Add New Technicians page, from the Authentication Type dropdown, select AD Authentication.

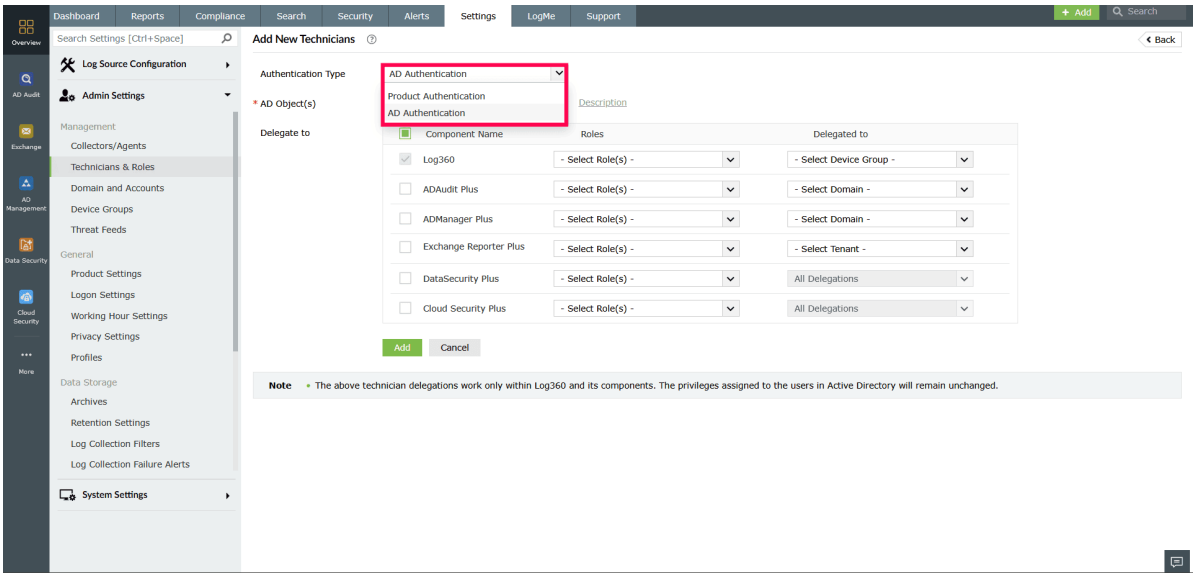


Figure 11: Selecting Authentication Type

2. In the AD Object(s) field, select the required user(s) from Active Directory. Use the + icon to add users after selection. You can optionally add a description using the Description button.

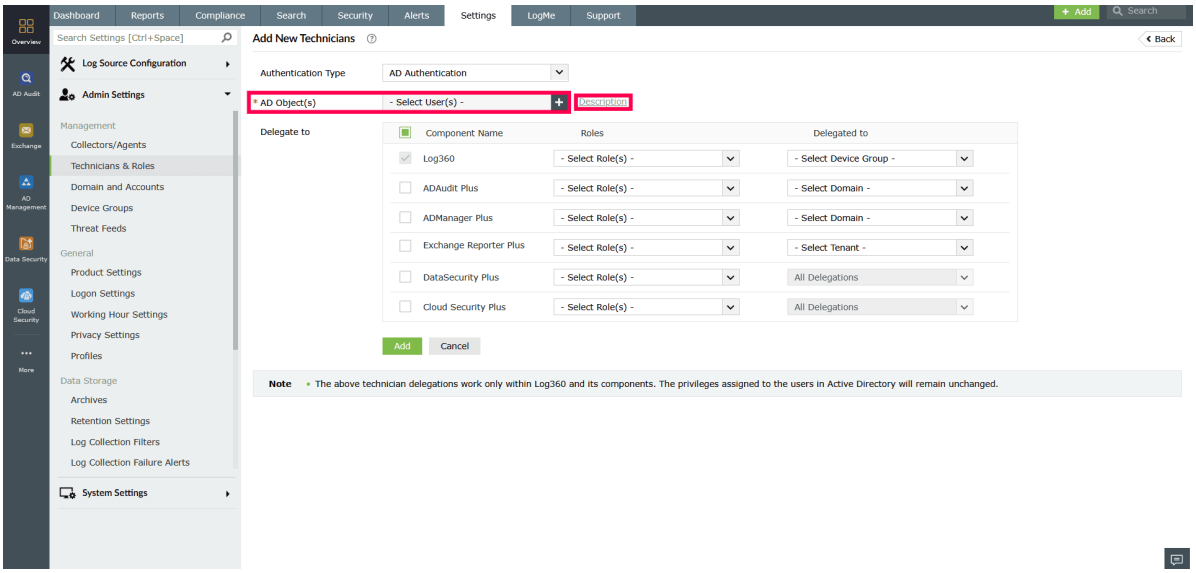
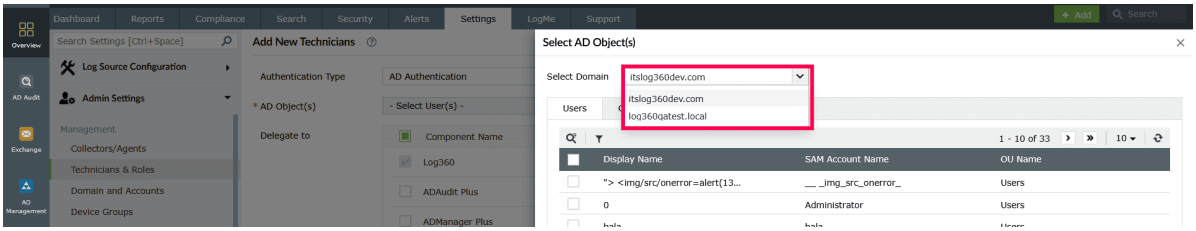


Figure 12: Configuring Technician settings

3. In the Select AD Object(s) window, use the Select Domain drop-down to choose the AD domain from which you want to assign users as technicians.



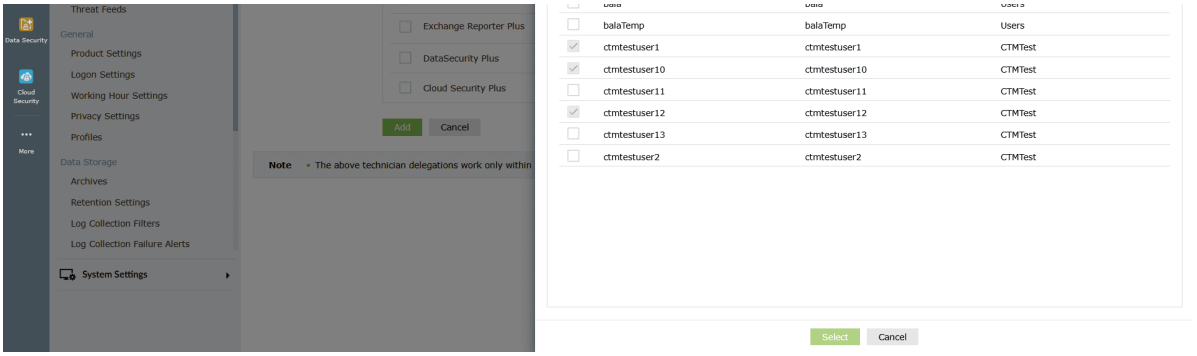


Figure 13: Selecting a domain

4. In the Users tab, select the user(s) of your choice by selecting the checkbox(es) under the Display Name field.

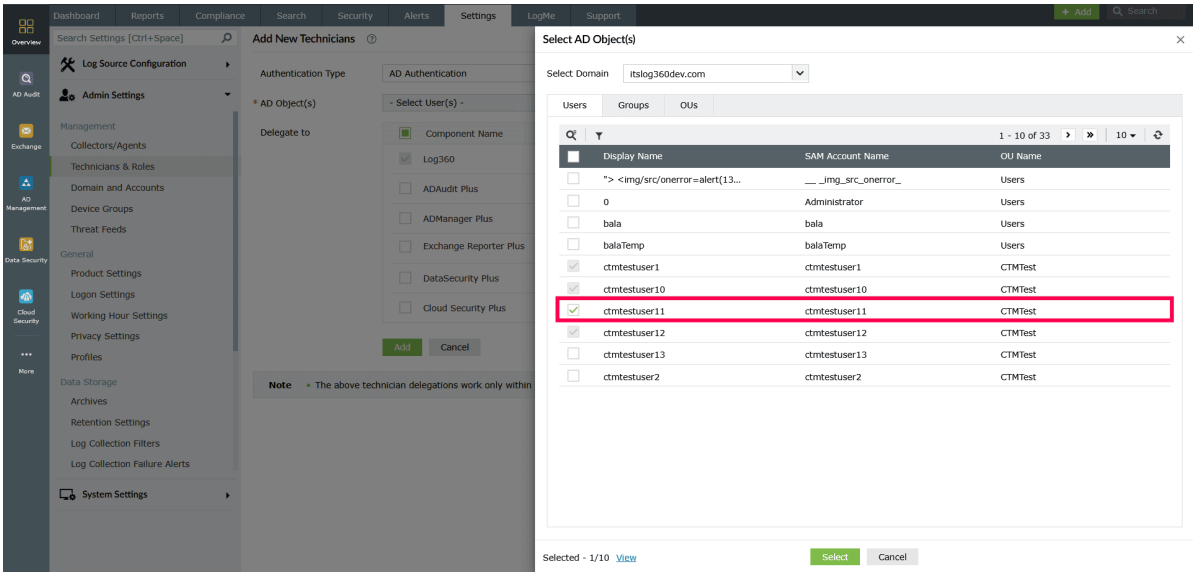


Figure 14: Selecting user(s)

5. You can also use the icon to locate specific users.

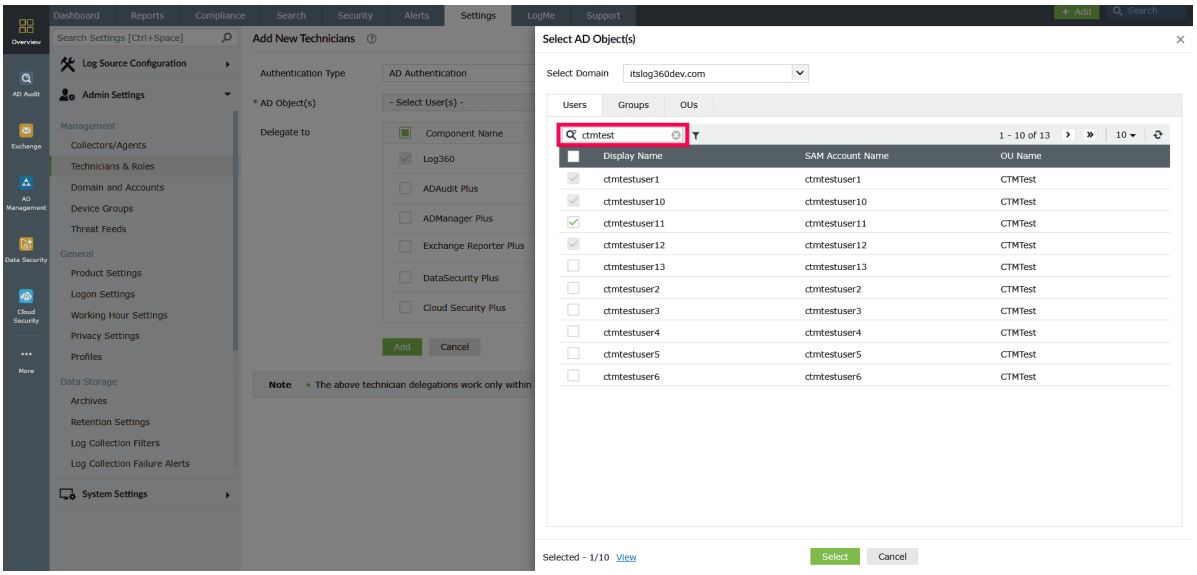


Figure 15: Search option for finding specific AD users

6. Use the ▼ icon to refine user selection.
7. Once you click the ▼ icon, an OU structure window appears.
8. In the OU tree, check the box next to the specific OU that contains the users you wish to assign as technicians. Click Apply to save the changes.

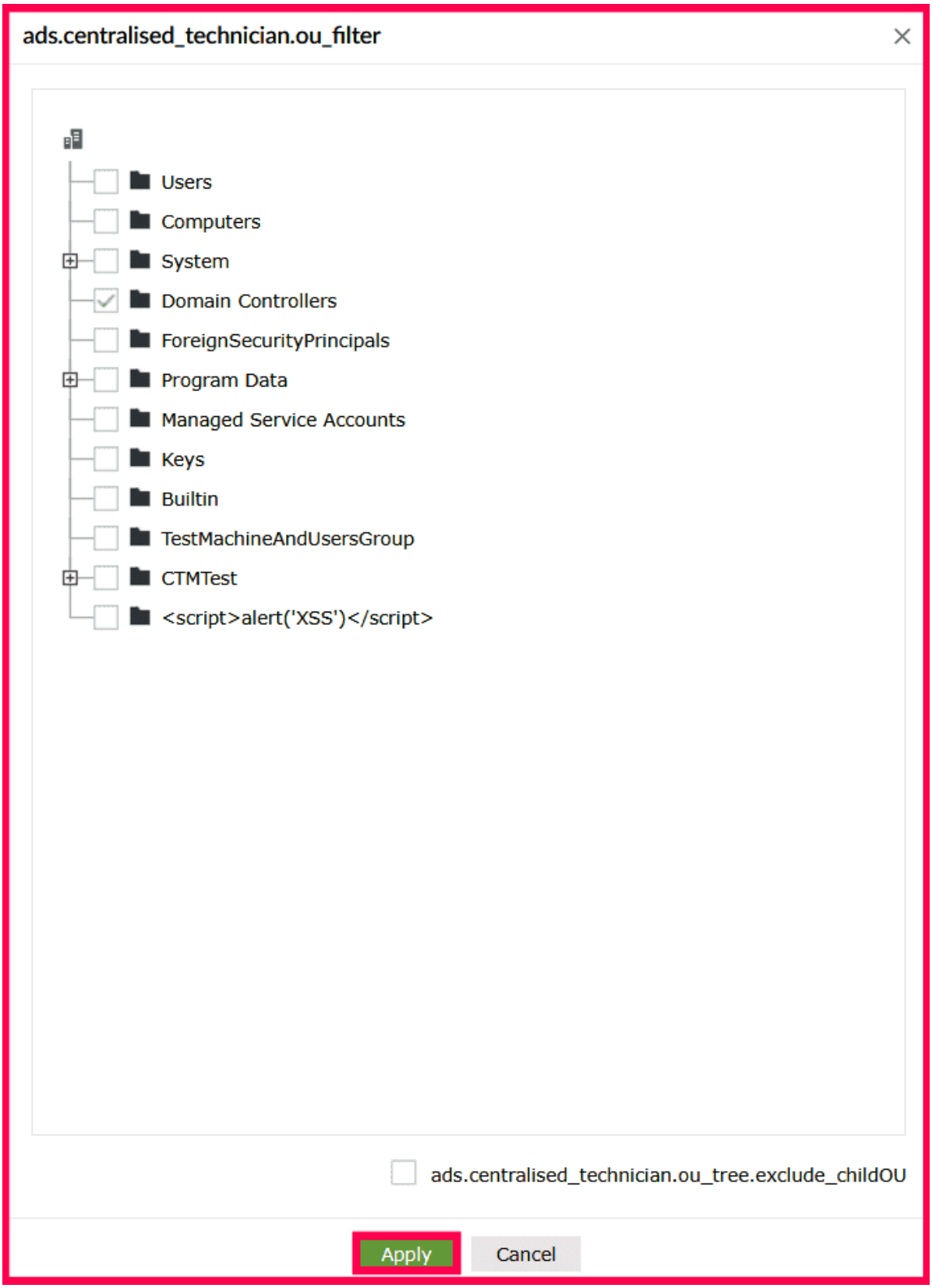


Figure 16: Filter option to refine the list of AD users

NOTE

- Some OUs include child OUs. For example, selecting the Program Data OU also includes its child OU, such as Microsoft, and all users within both.

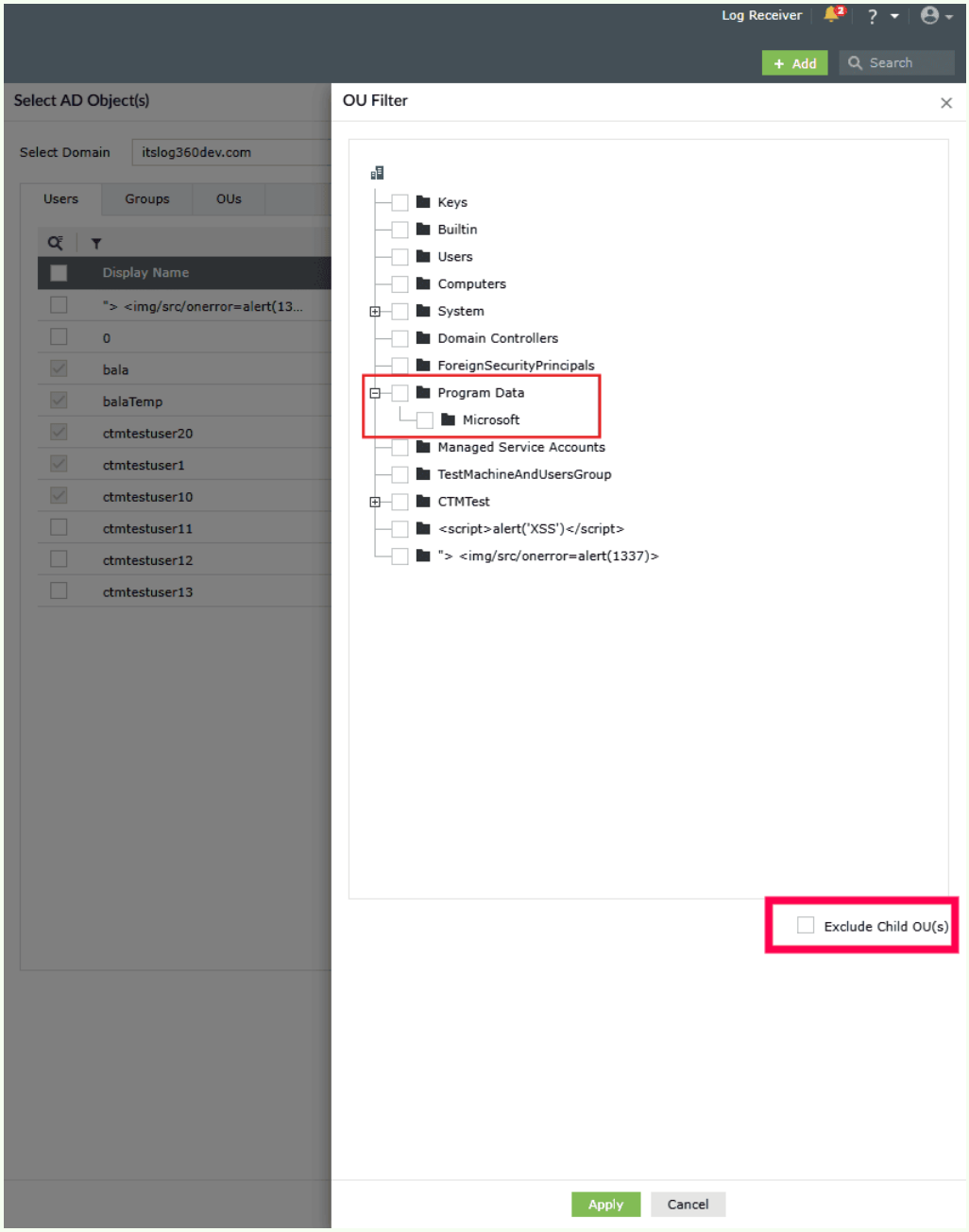


Figure 17: Auto-inclusion of OU and its Child OU

- If you want to exclude these child OUs, select the checkbox next to Exclude Child OU(s) at the bottom of the OU tree.

9. In the Select AD Object(s) page, click Select to add the chosen user(s).



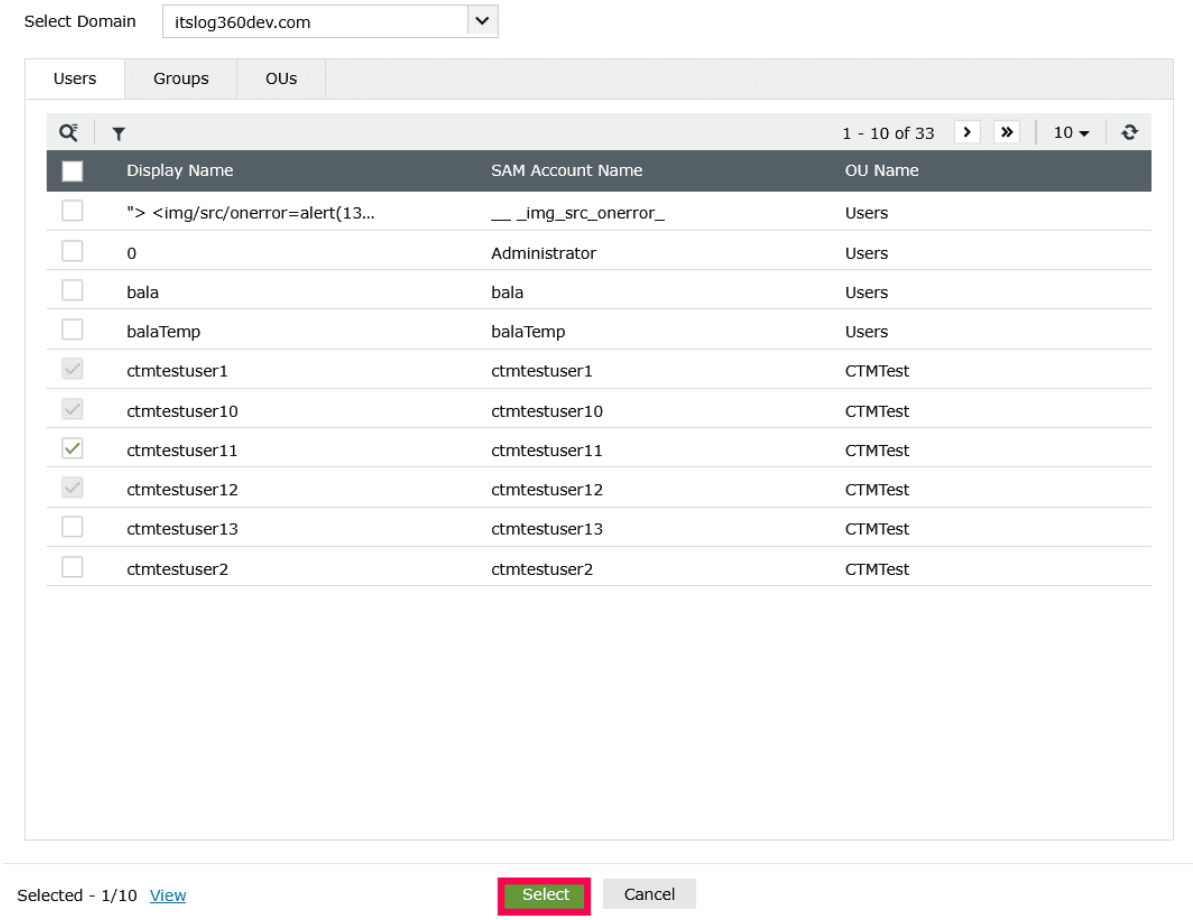


Figure 18: Selecting AD Object(s)

10. Follow the same steps outlined in steps 8- 10 of the previous section to assign roles and delegate entities.

Adding a centralized technician group/ OU

1. In the Add New Technicians page, from the Authentication Type dropdown, select AD Authentication.

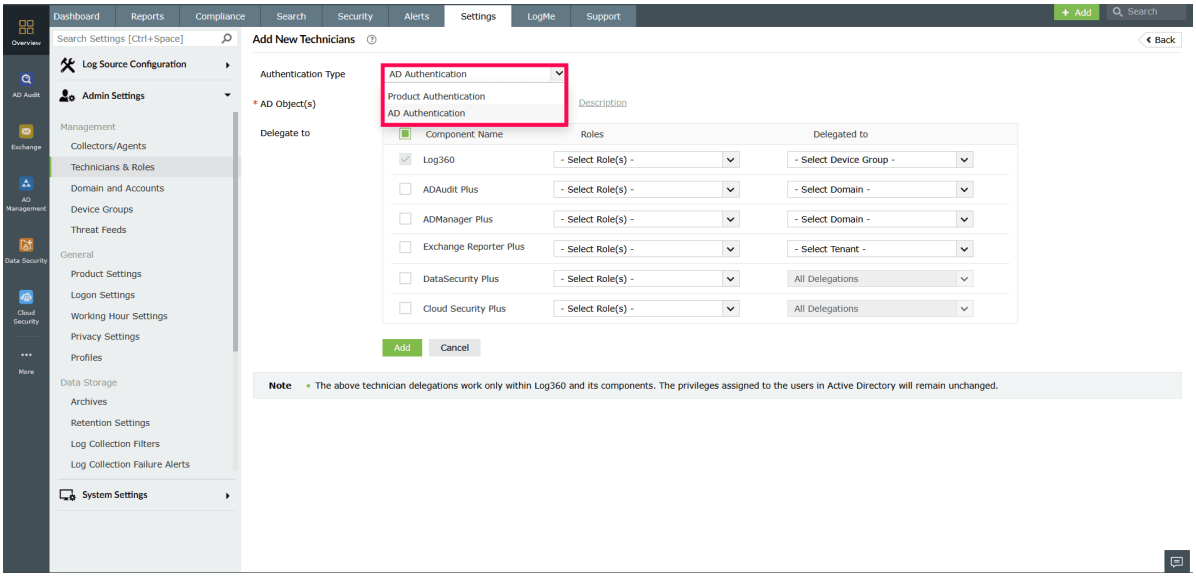


Figure 19: Selecting authentication type

2. In the AD Object(s) field, select the required user(s) from Active Directory. Use the icon to add users after selection. You can optionally add a description using the Description button.

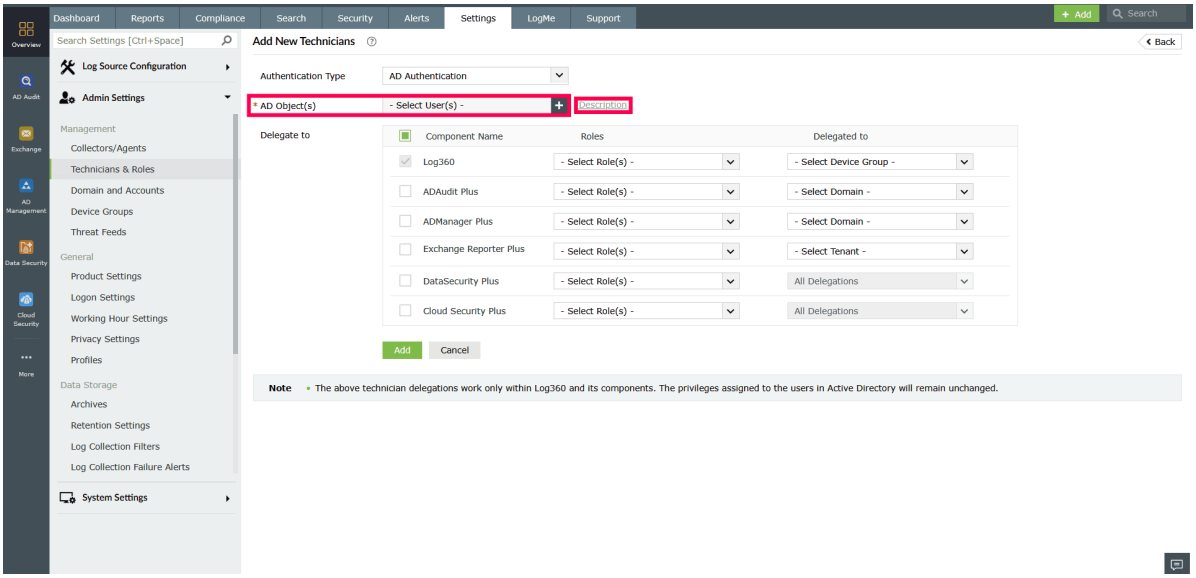


Figure 20: Configuring Technician settings

3. In the Select AD Object(s) window, use the Select Domain drop-down to choose the AD domain from which you want to assign users as technicians.

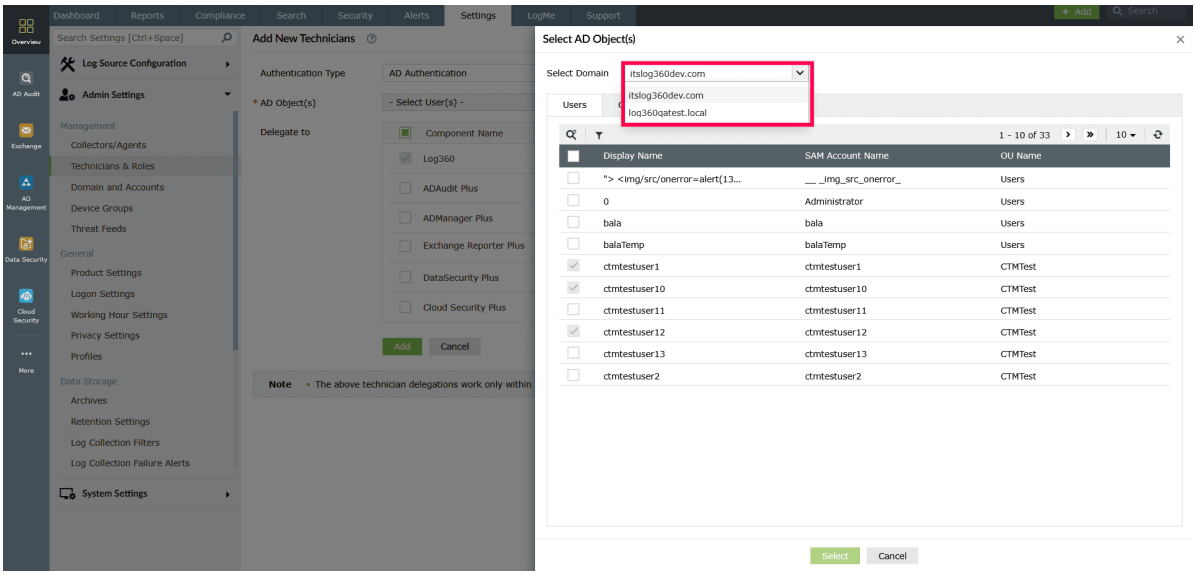


Figure 21: Selecting a domain

4. The Groups tab displays all AD groups in a tabular format along with their descriptions. You can use the search icon to locate a specific group.
NOTE If an Active Directory (AD) user belongs to a configured group or OU, they will be recognized under that group when logging into the Log360 console. However, the user will not be able to log in directly to any of the child components.



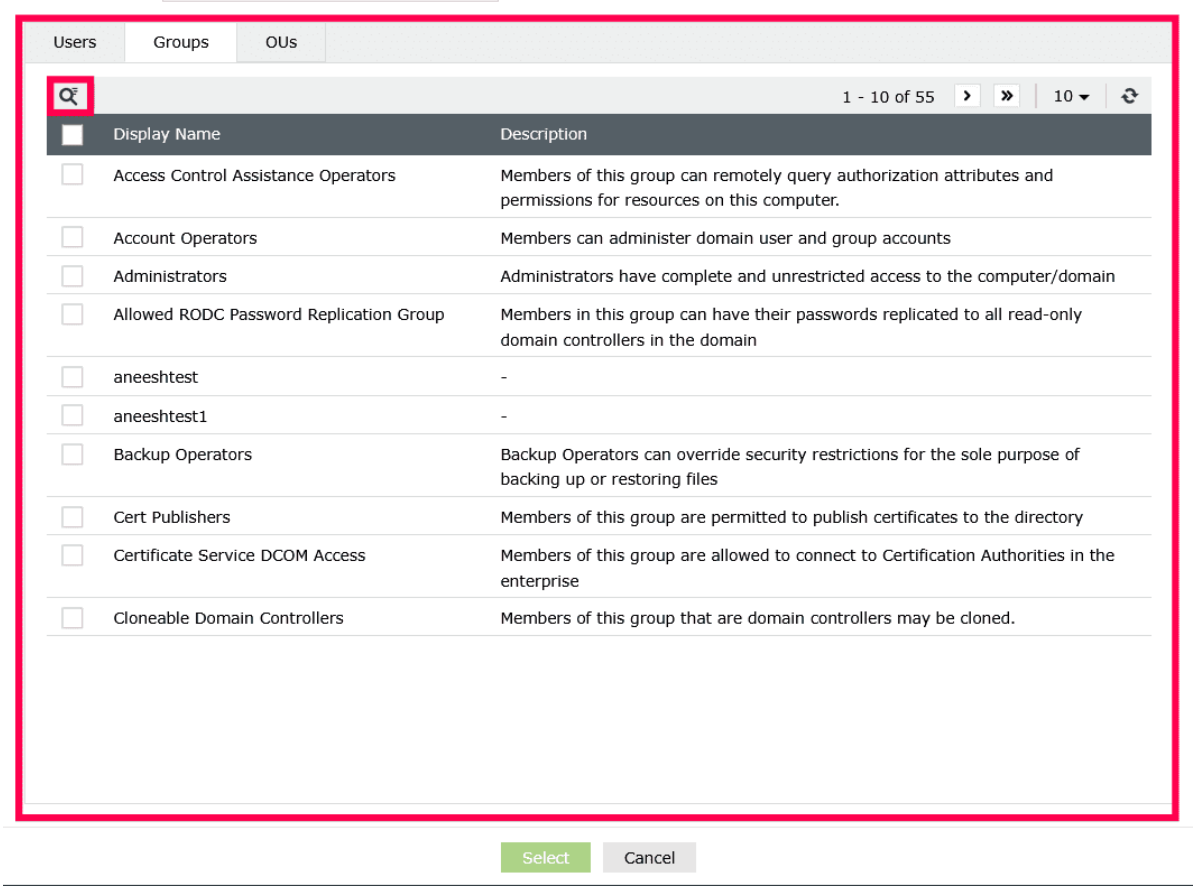
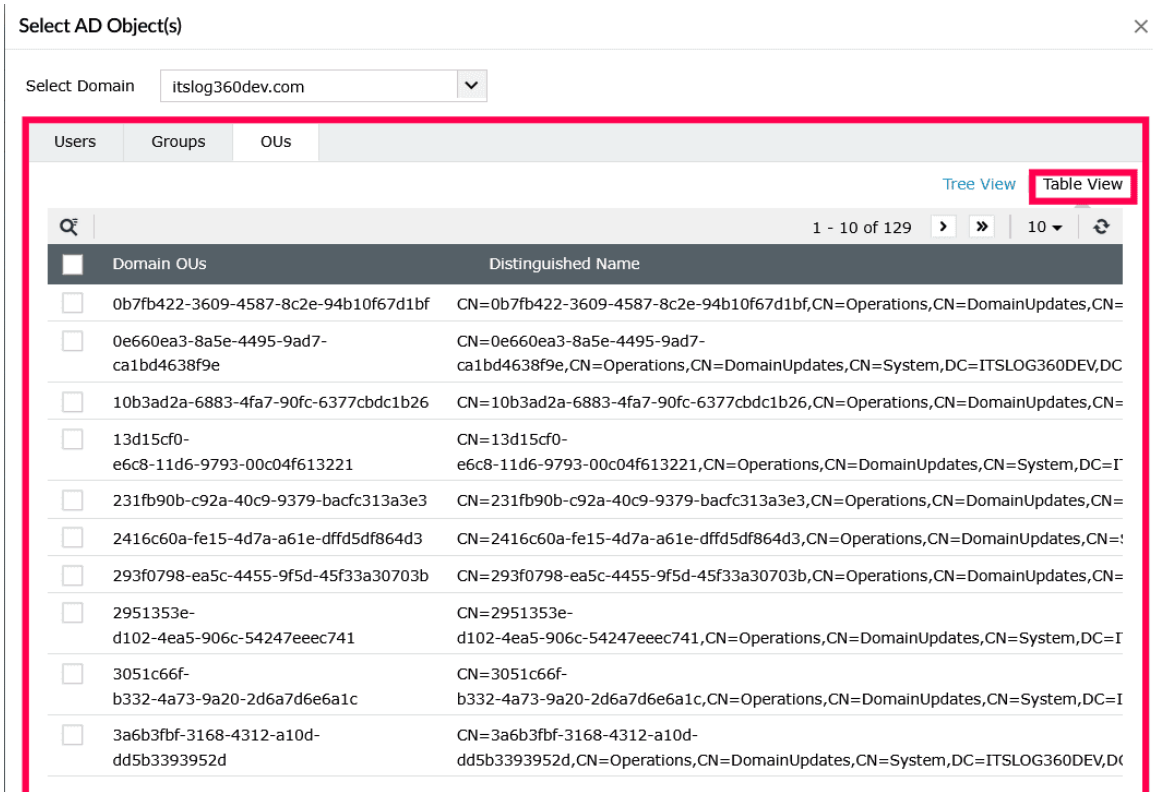


Figure 22: Group tab settings

5. The OUs tab lists all Organizational Units in either:

- Click Table View which displays OUs in a list with their distinguished names. Use the icon to find an OU.



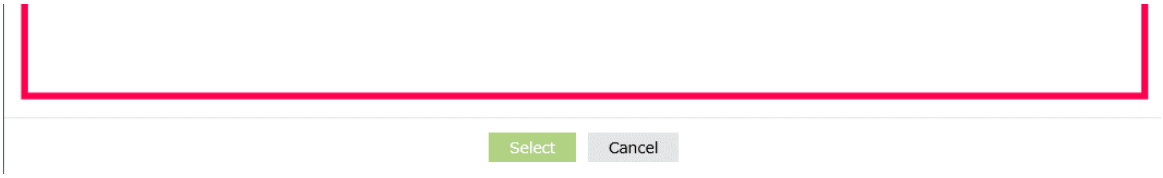


Figure 23: Table view of OU tab

- Click Tree View which displays OUs in a hierarchical tree structure.

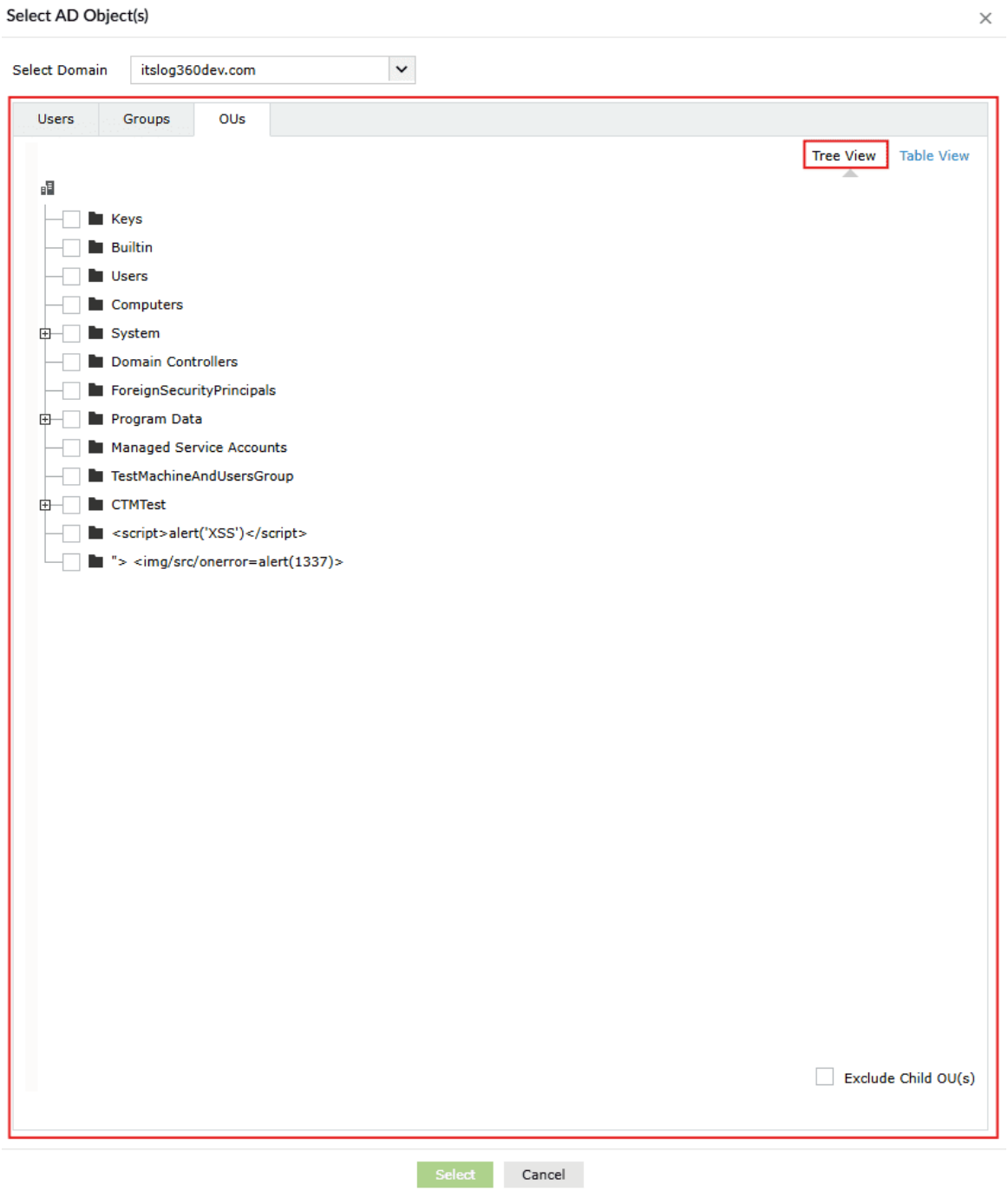


Figure 24: Tree view of OU tab

- You can exclude all child components of a selected OU by checking the Exclude Child OU at the bottom of the tree.

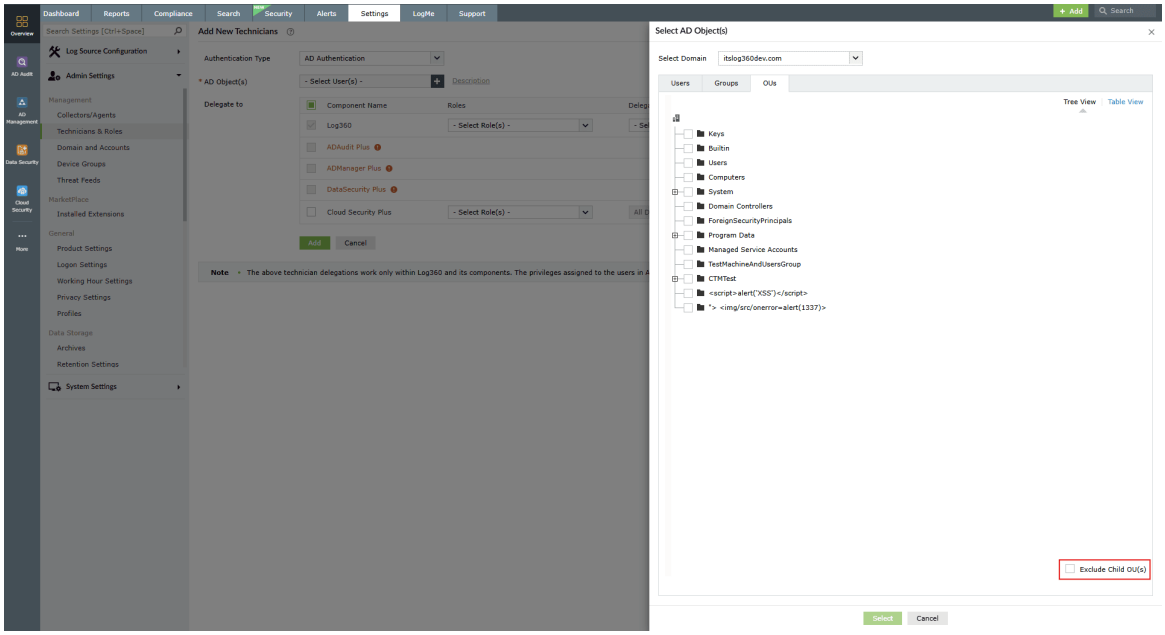


Figure 25: Excluding Child OU

6. Select the checkbox next to required group or OU and click Select to add it.
7. Follow the same steps outlined in steps 8- 10 of this section to assign roles and delegate entities.

Read also

This section detailed how to add technicians individually or by importing technician groups and Organizational Units (OUs) using Active Directory authentication. To learn more about managing technicians, creating and managing roles, refer to the following articles:

- Managing technicians
- Creating and managing roles

9.1.13.3. Managing technicians

Last updated on: September 12, 2025

In this page

Overview

Viewing and managing technician details

Editing technician settings

Editing settings for multiple technicians

Enabling or disabling technicians

Deleting technicians

Overview

Centralized Technician Management offers a centralized interface for administrators to manage technician accounts from a single console. This section details how you can view, edit, delete, and update multiple technician details from the product console.

Viewing and managing technician details

1. In your account, navigate to the Settings tab.
2. Under Admin Settings, select Technicians and Roles.

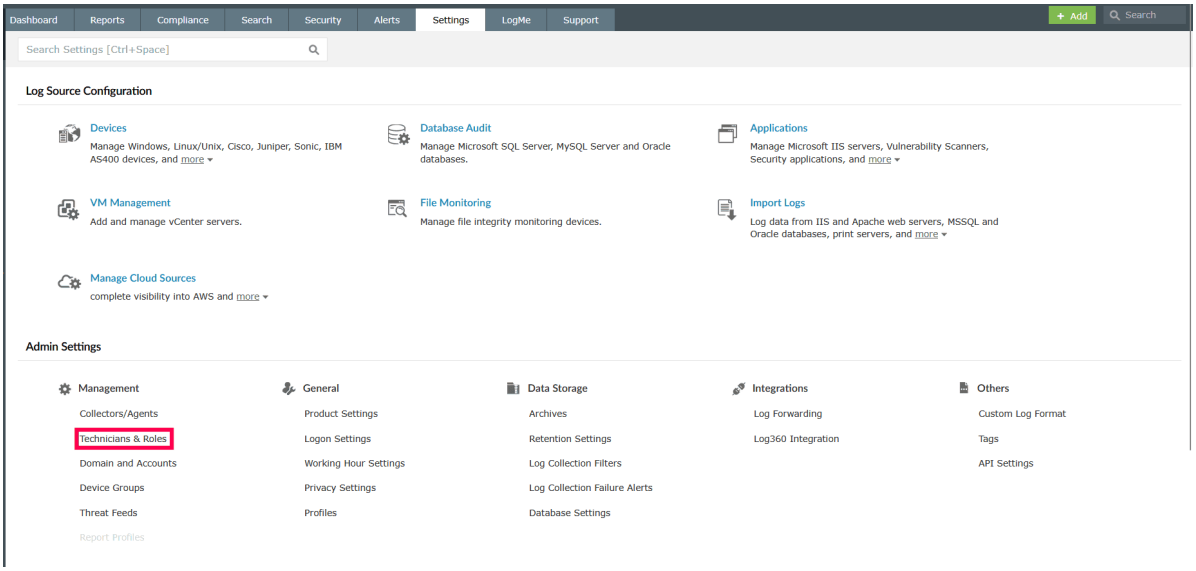


Figure 1: Navigating to Technicians and Roles

3. On the Manage Technicians page, click View Details for the desired technician.

> **NOTE**
>
> In the group view, individual technicians are listed under Product Authentication and AD Authentication, while users belonging to groups appear under their respective groups.

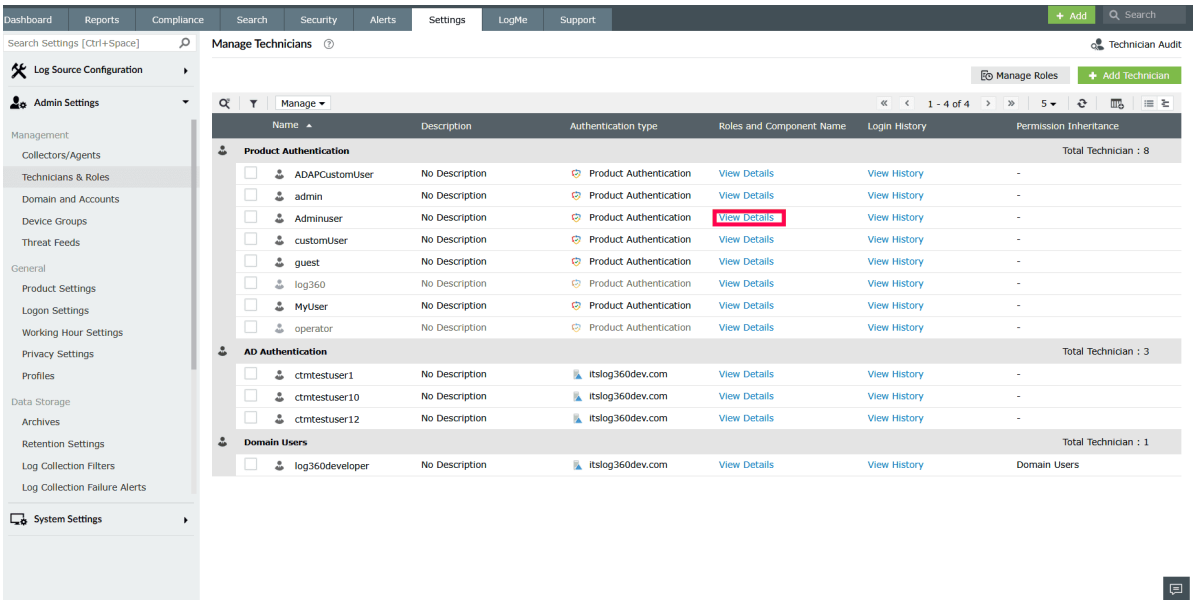


Figure 2: Viewing role and component details

4. In the details window, click icon next to any assigned component to disable.

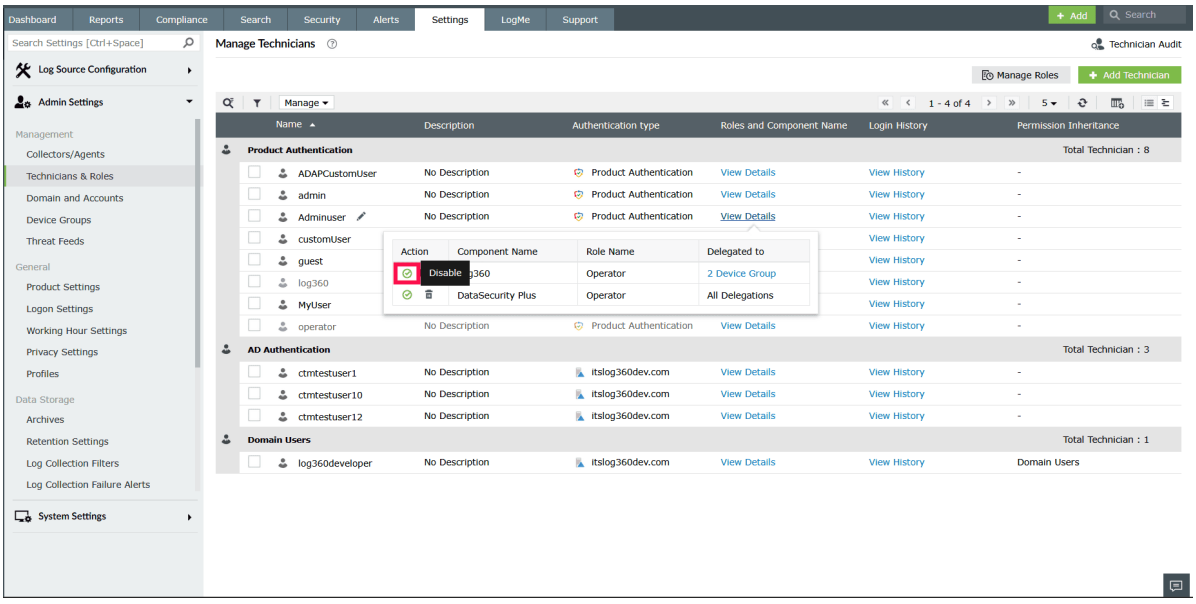


Figure 3: Disabling a component

5. In the confirmation pop-up, click Yes to disable.



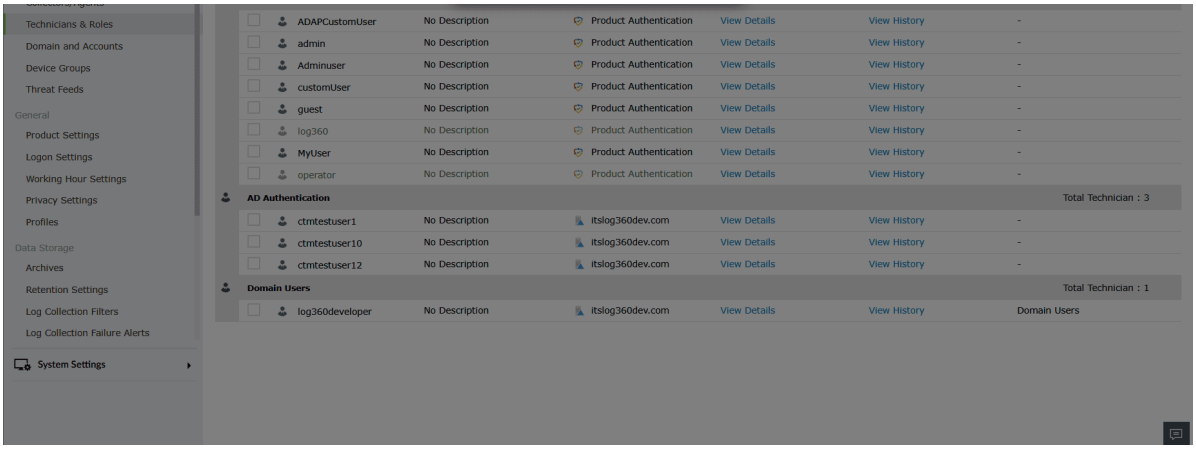


Figure 4: Disabling a component

6. To re-enable, click the icon to reassign the component to the technician.

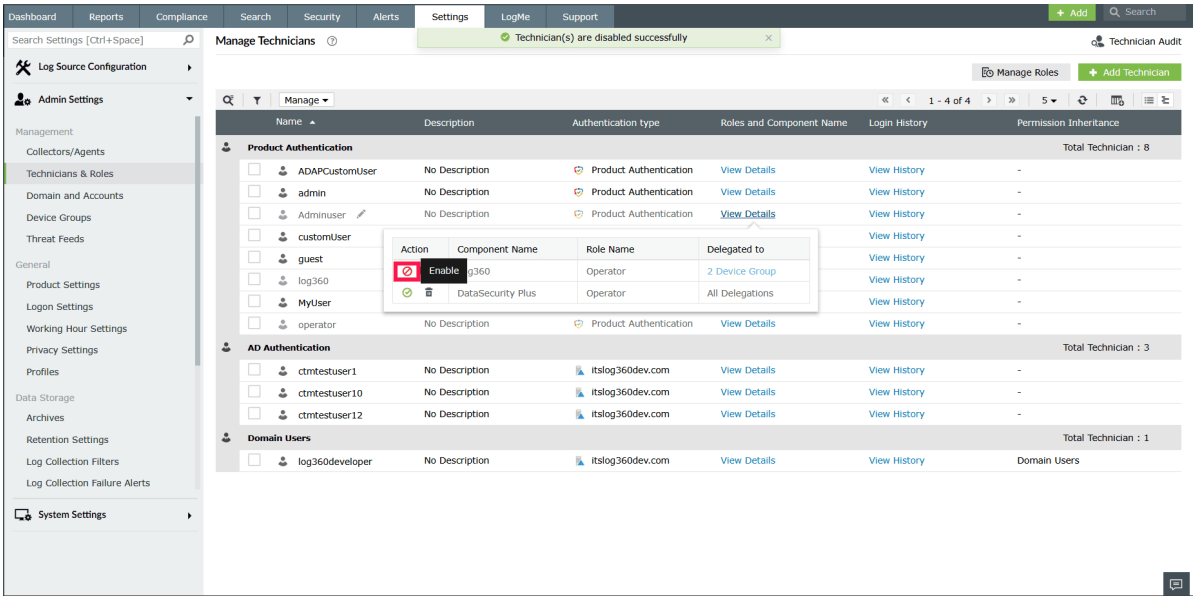


Figure 5: Enabling a component

7. Click the delete icon next to the component you want to remove.

   NOTE Technicians created in Log360 can only be deleted after they have been removed as technicians from all the integrated components.

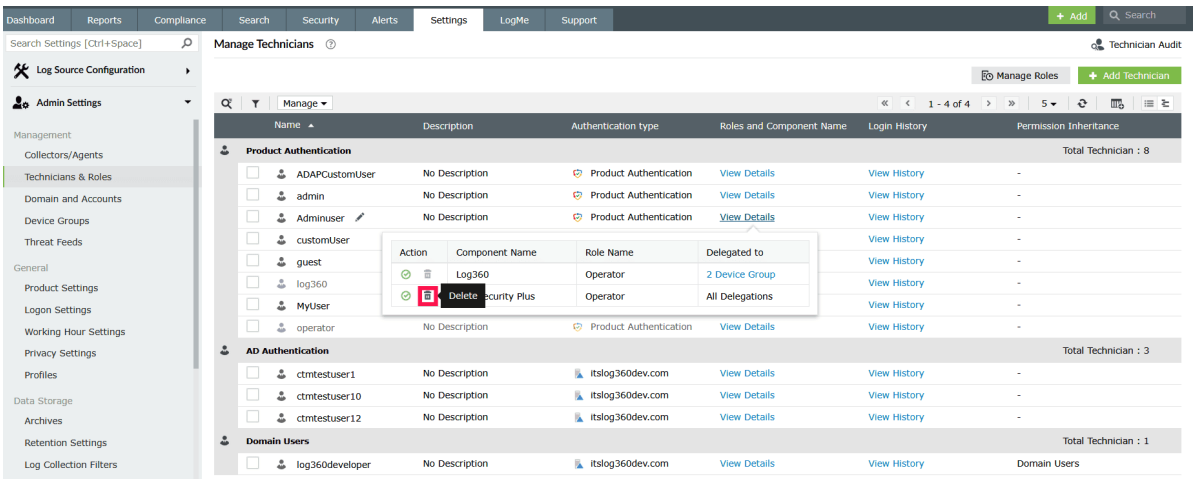




Figure 6: Deleting a component

8. Confirm the deletion in the pop-up by clicking Yes.

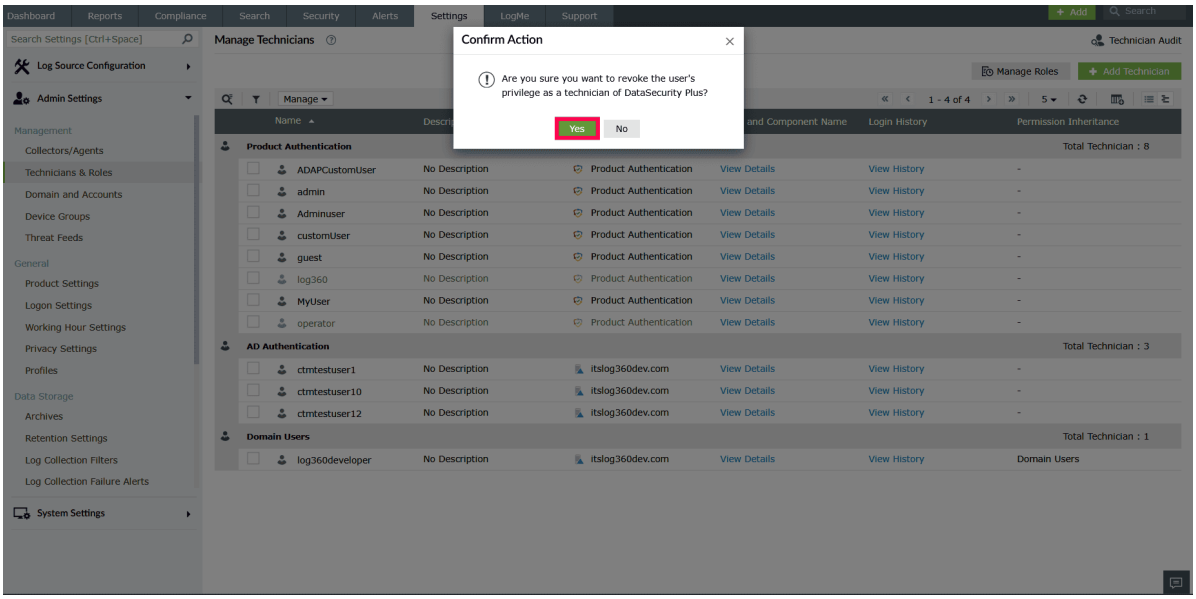


Figure 7: Confirming deletion

9. Click the device group hyperlink (for example, 2 Device Group) to open a list of all device groups assigned to the technician.

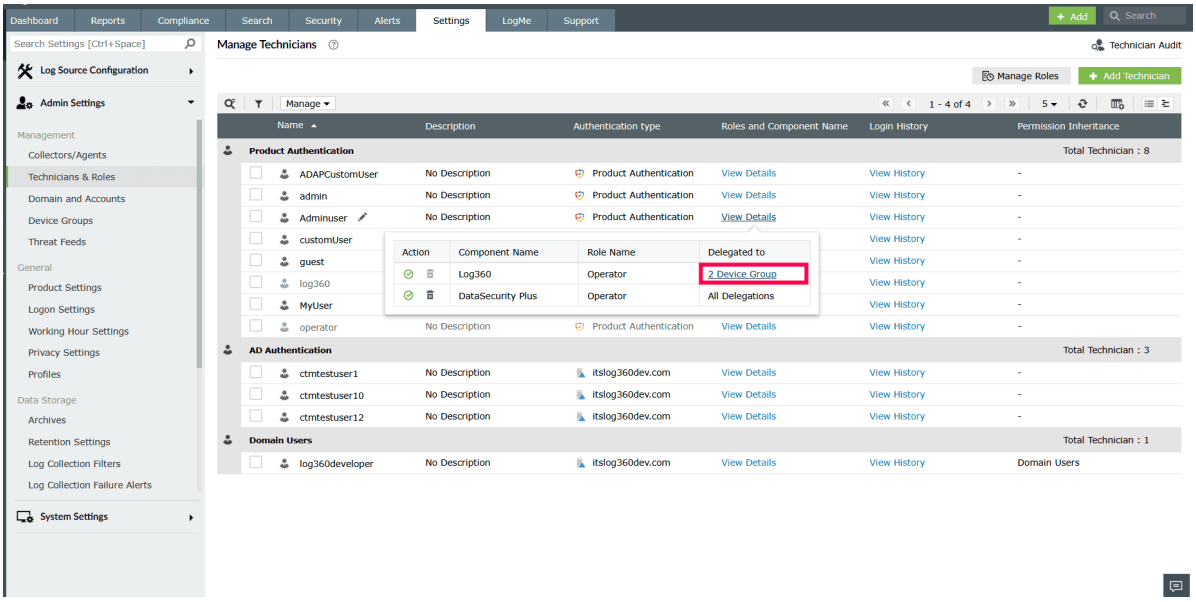


Figure 8: Viewing delegations

10. The window displays each group and the devices within it. You can also use the Search Device field to locate a device by name.



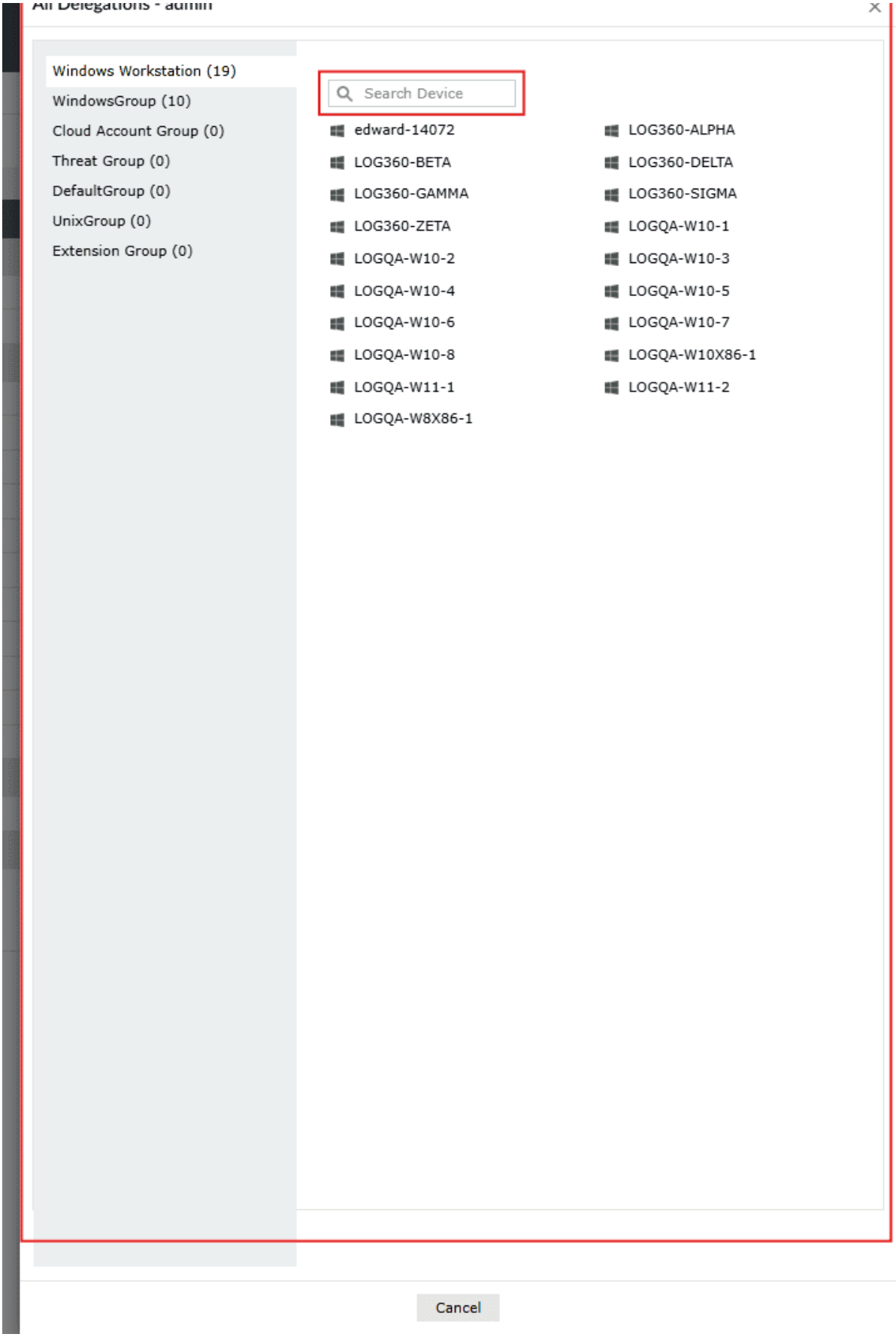


Figure 9: Viewing device groups

11. Under Login History, click View History to see detailed records of the technician's login activity, including logon and logoff times.

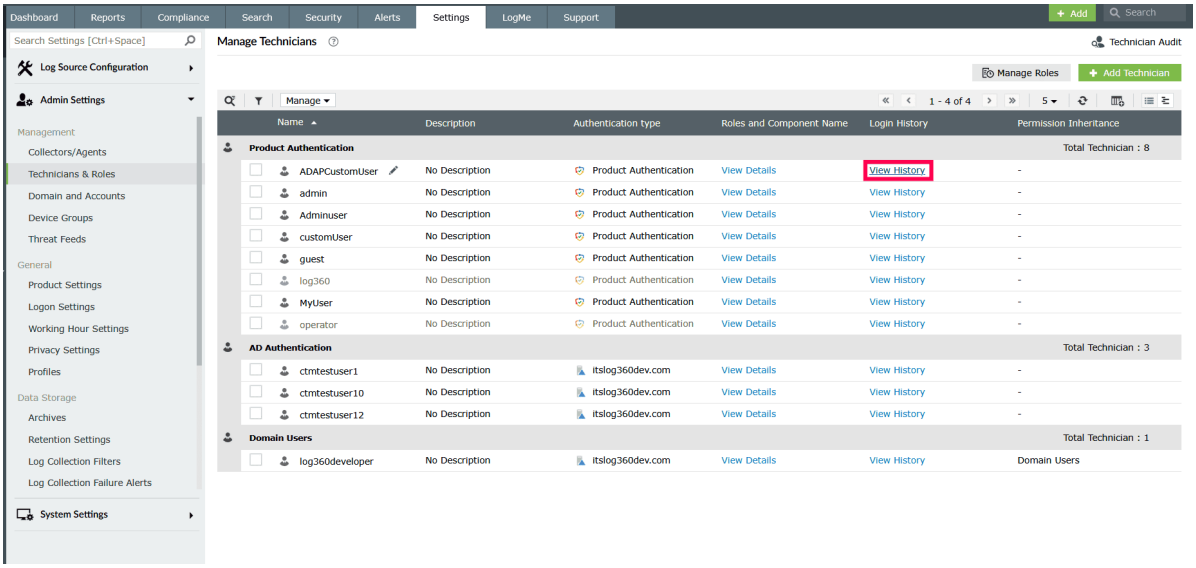


Figure 10: Viewing login history

12. You can also click the icon to locate devices by their IP address.

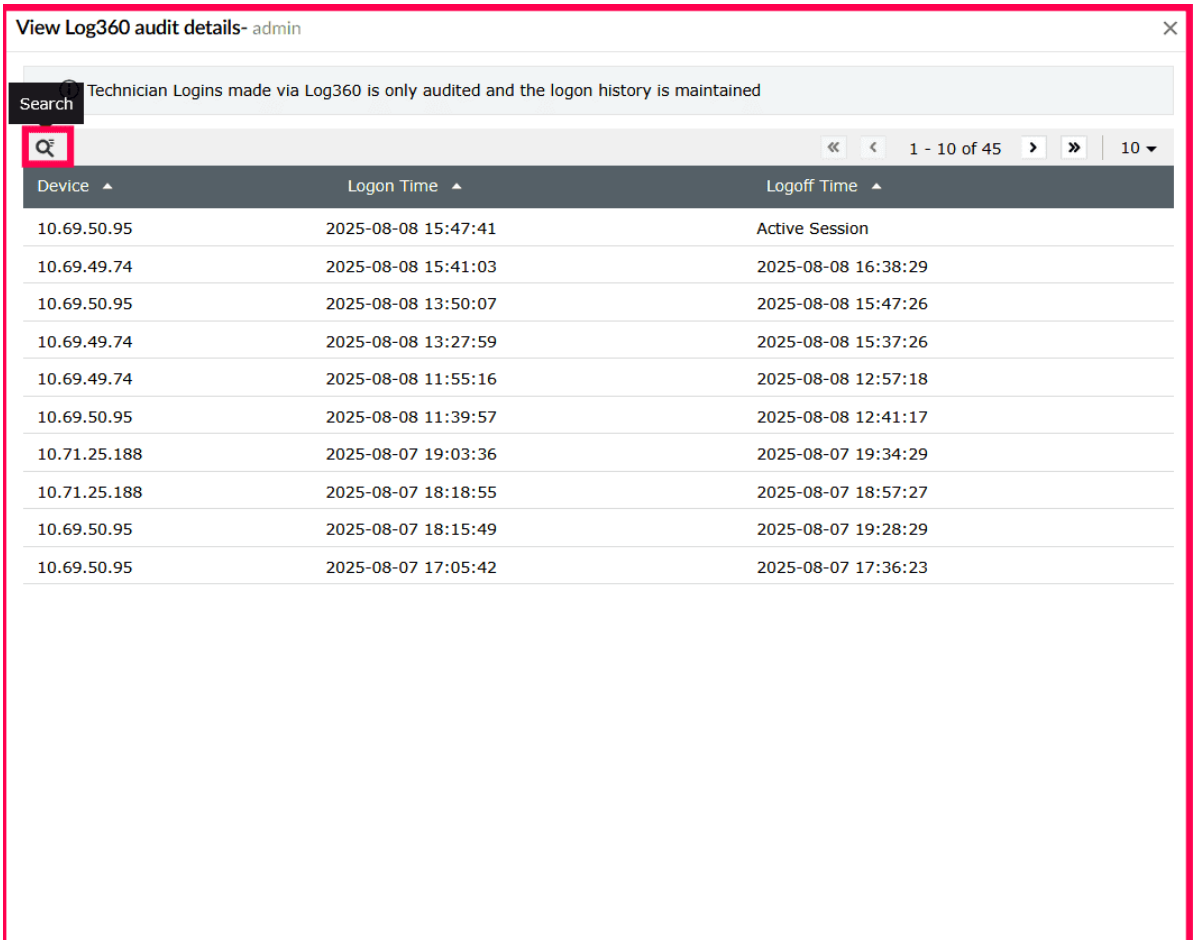


Figure 11: Searching devices using IP address

13. The Permission Inheritance column applies only to users belonging to a group or OU and indicates the specific group or OU from which their delegation, role, or permissions are inherited.

14. Click the icon to add or remove columns. Select the checkboxes for the columns you want to display, then

click Apply to save your changes.

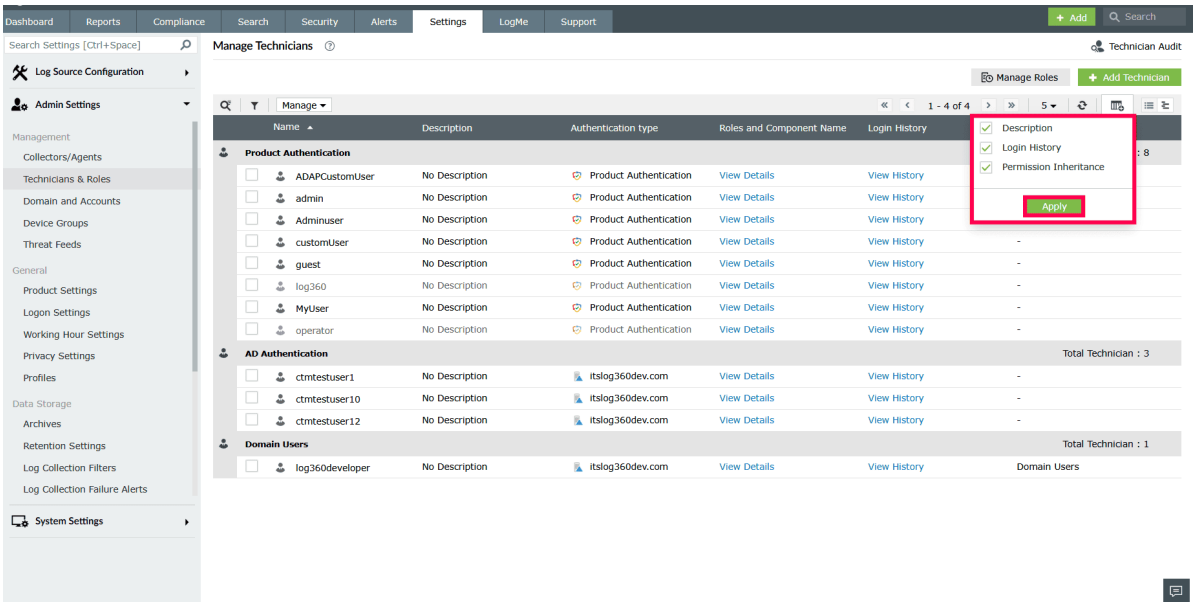


Figure 12: Adding or removing columns

15. In the top right corner, click this icon to switch to group view, and this icon to switch to table view.

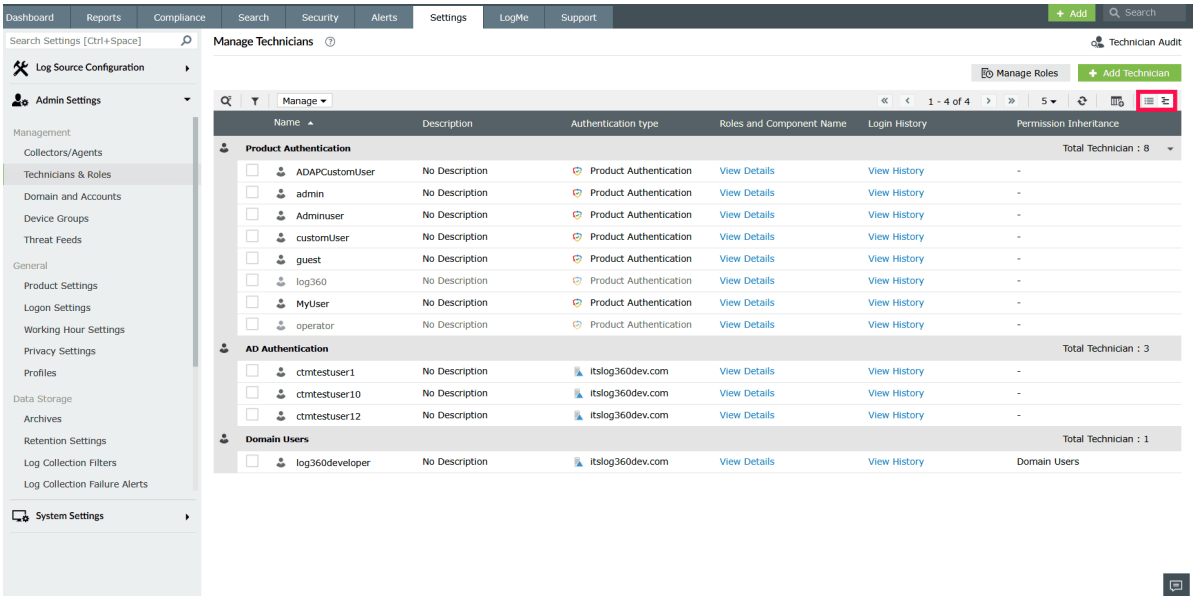


Figure 13: Table view and group view

16. In the Manage Technicians page, use the icon in the top-left corner to find a technician by name.
17. Click the icon to narrow down the technician list.
18. In the first dropdown, select the attribute you want to filter by:
    - Name
    - Authentication Type
    - Log360 Roles
    - Object Type

- Status

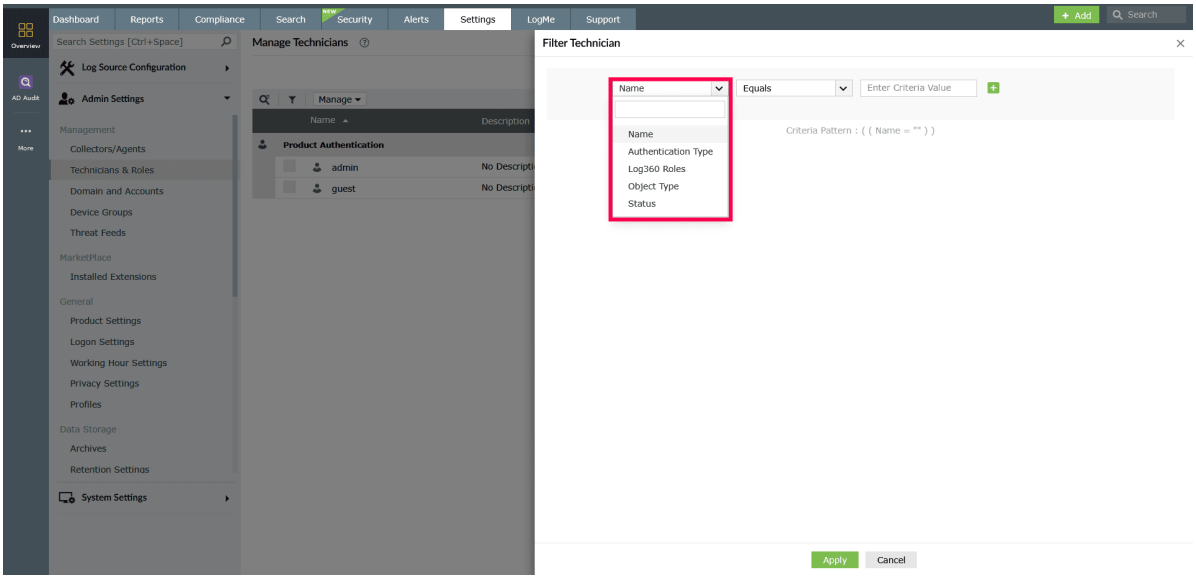


Figure 14: Filtering technicians

19. The available matching conditions vary based on the selected attribute:
    - Name: Equals, Not Equals, Contains, Not Contains, Starts With, Ends With
    - Authentication Type, Log360 Roles, Object Type, Status: Equals, Not Equals
20. In the next field, enter or select the desired criteria value.
21. To add more than one filter condition, click the + icon and choose whether the additional condition should be applied using AND (both conditions must match) or OR (either condition can match).

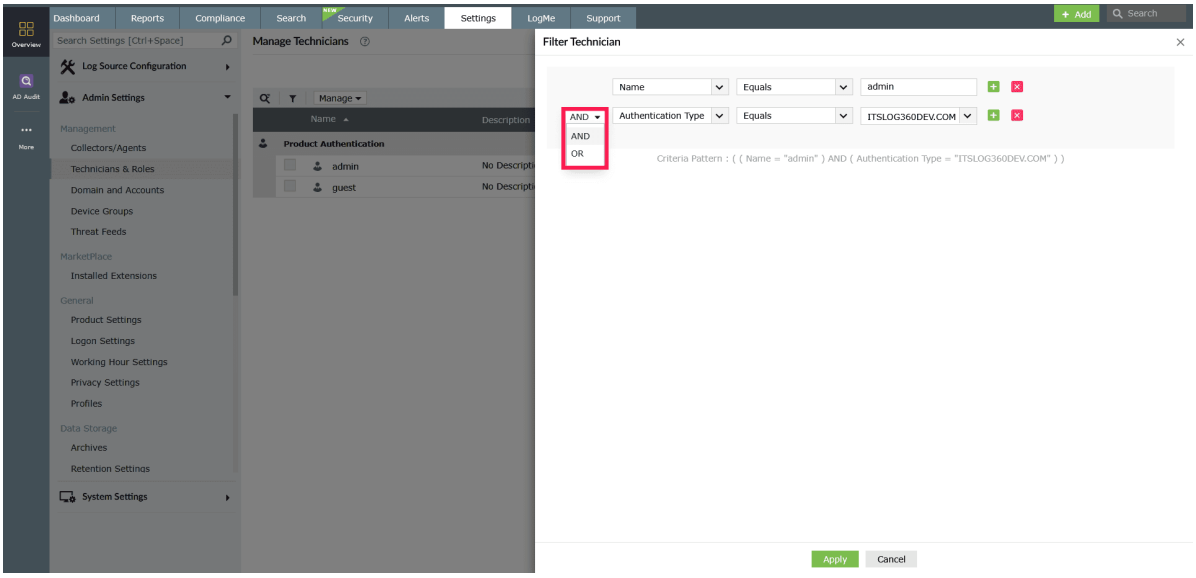


Figure 15: Filtering technicians

22. To remove a condition, click the ✕ icon next to it.
23. Click Apply to filter the list of technicians based on your chosen criteria.

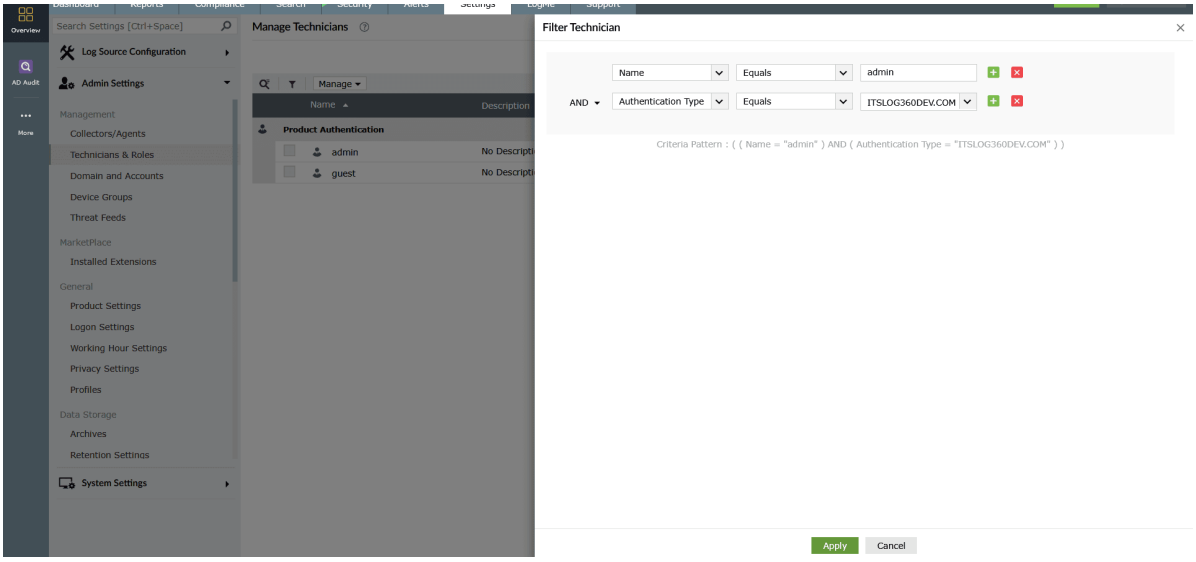


Figure 16: Filtering technicians

Editing technician settings

1. In the Manage Technicians page, hover over the technician's name and click the icon to modify the technician's settings.

> **NOTE**
>
> Changes to technician's roles, permissions, and delegations made directly in a child component's console will be synchronized with Log360. However, password changes are not synced.

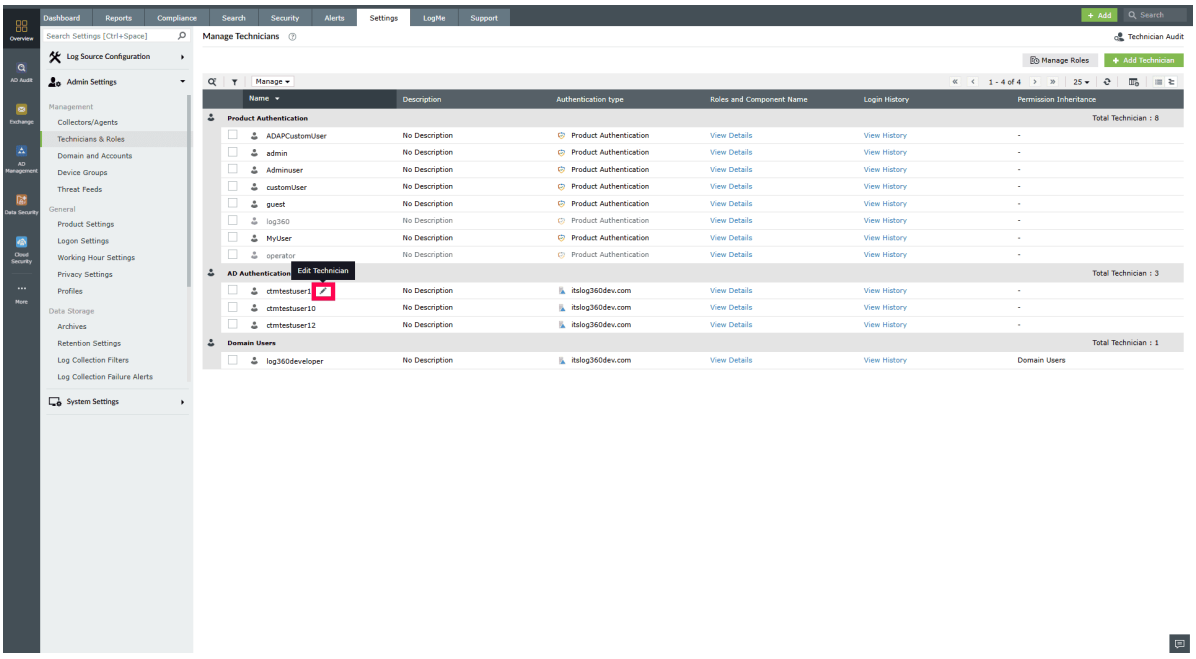


Figure 17: Editing technician settings

Figure 17: Editing technician settings

2. In the Edit Technician page, make the required changes.

> **NOTE**
>
> If you add a new component to an existing technician, you must reset the password.

3. Click Update to save the changes.

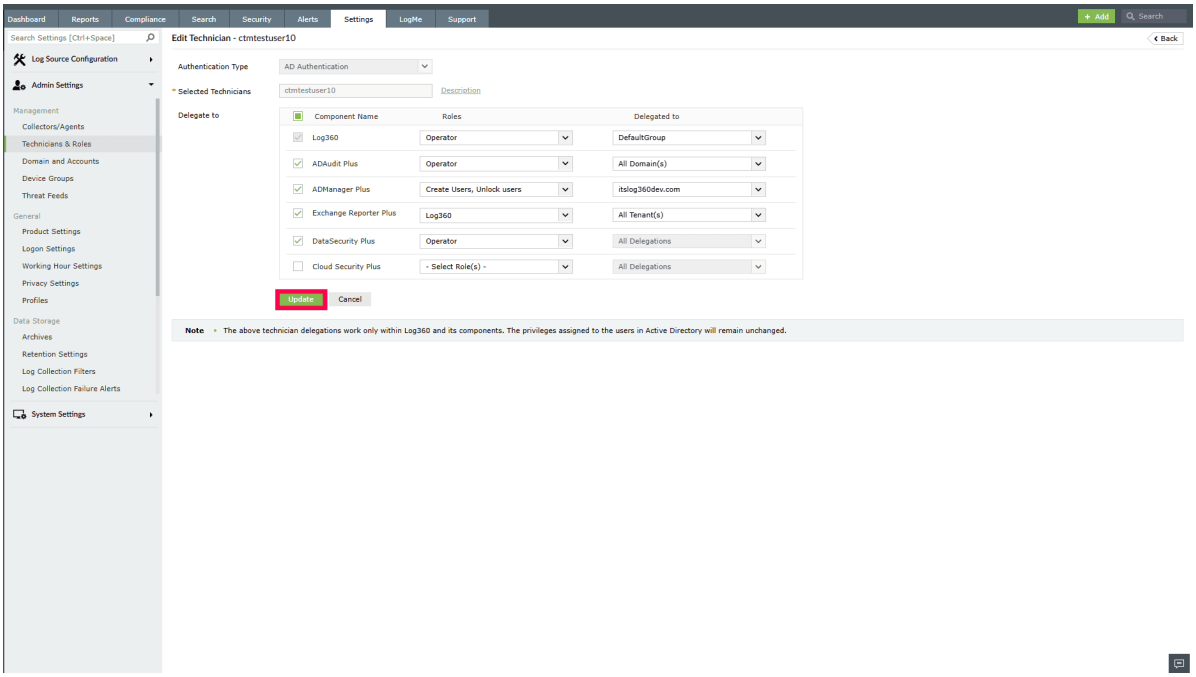
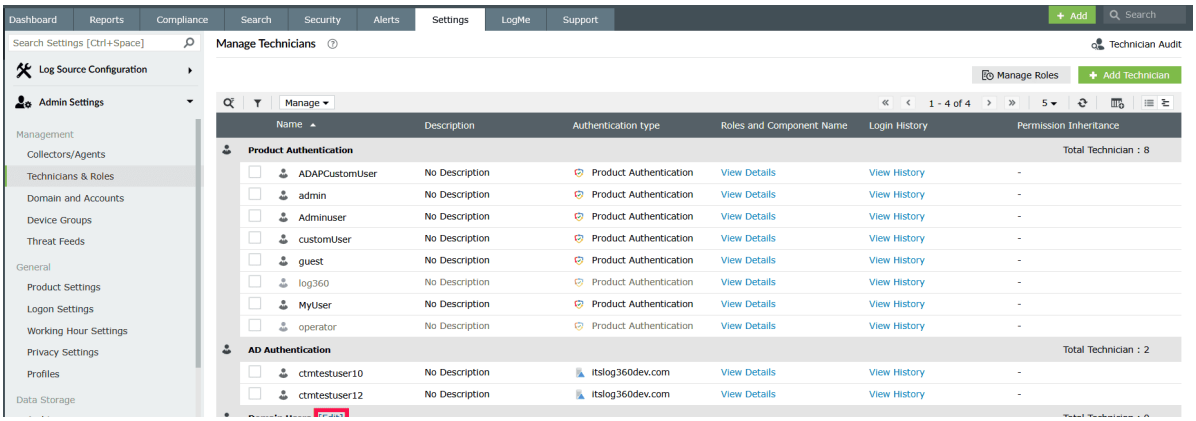


Figure 18: Updating technician settings

4. To edit a group, hover over its name and click Edit.

> **NOTE**
>
> If a technician who belongs to an AD group is edited, they will be removed from that group and appear as an individual technician under AD Authentication in the grouped view.



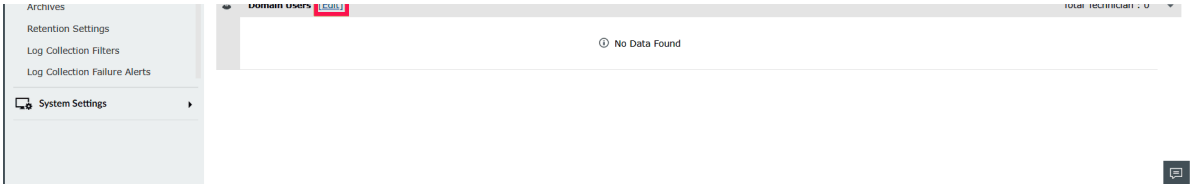


Figure 19: Modifying group settings

5. In the Edit Technician page, make the required changes and click Update to save the changes.

Editing settings for multiple technicians

> **NOTE**
>
> Editing multiple technicians at once is not supported for default technicians or for the currently logged-in user.

1. On the Manage Technicians page, select the checkboxes next to the technicians you want to edit.

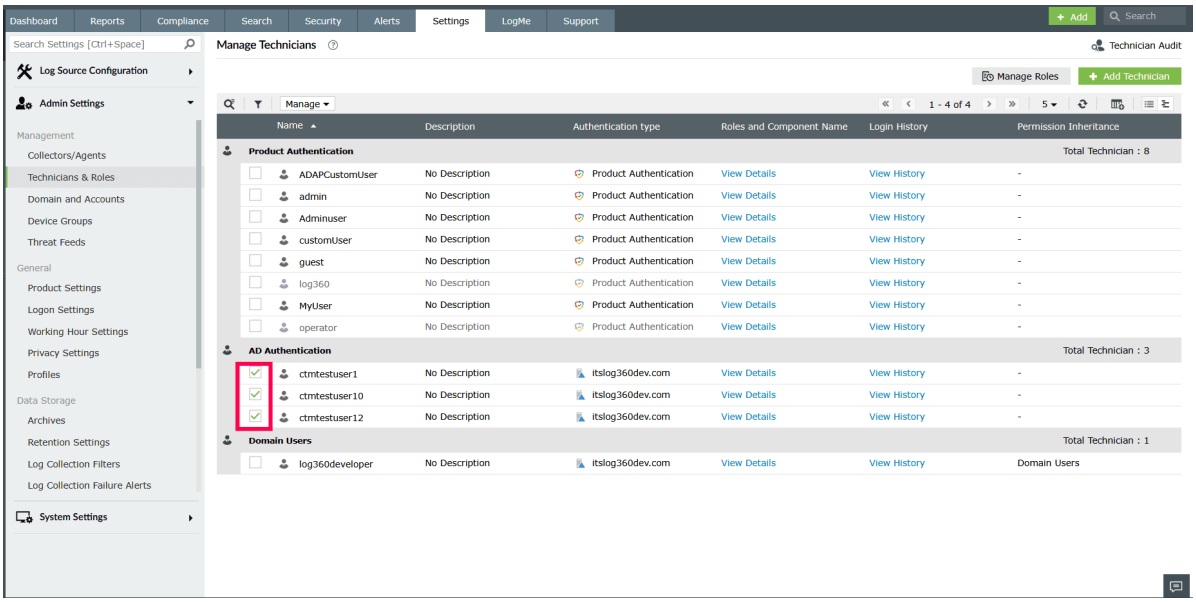
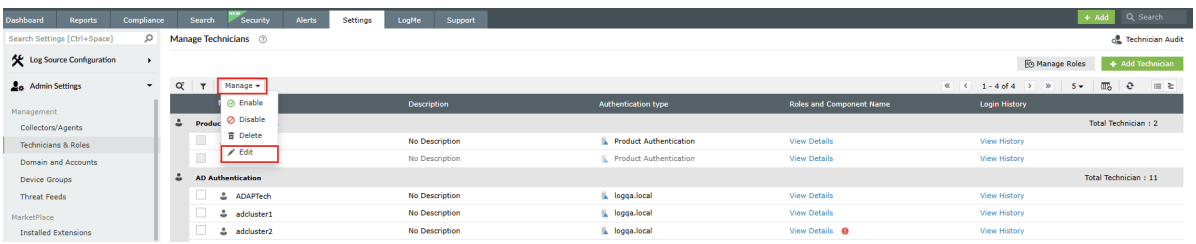


Figure 20: Selecting technicians

2. Click the Manage drop-down menu.
3. From the menu, click Edit to update settings for multiple technicians.



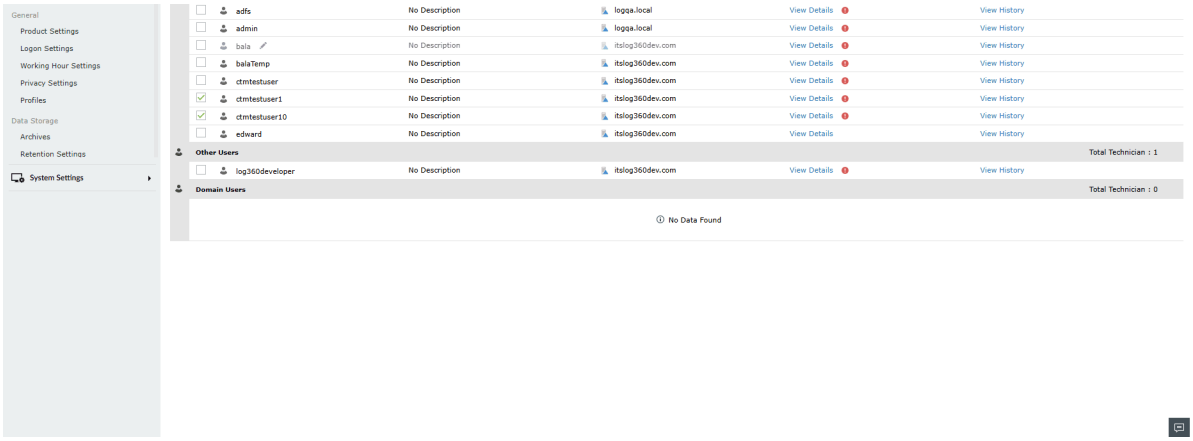


Figure 21: Editing settings for multiple technicians

4. Make the required changes to the selected technicians.
5. Click Update to apply the changes.

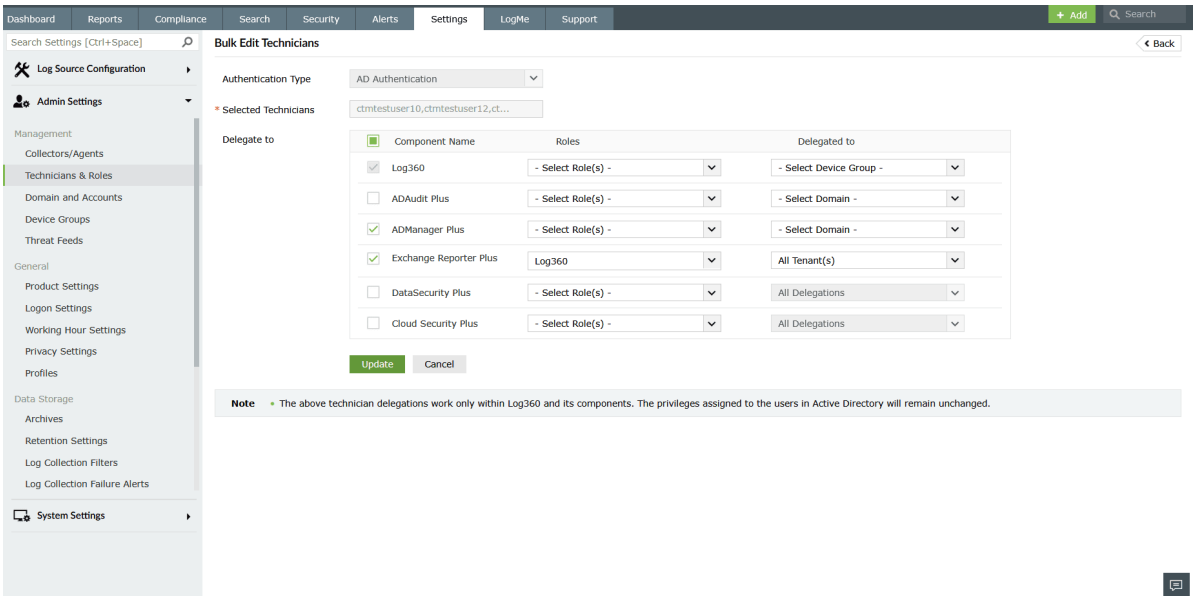
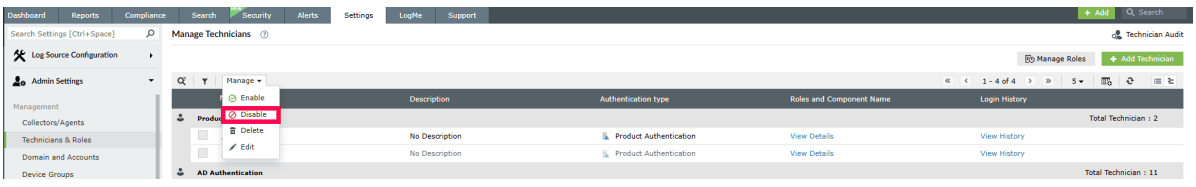


Figure 22: Updating technician settings

Enabling or disabling technicians

To disable technicians

1. On the Manage Technicians page, select the checkboxes next to the technicians you want to disable.
2. Click the Manage drop-down menu.
3. Select Disable from the list.



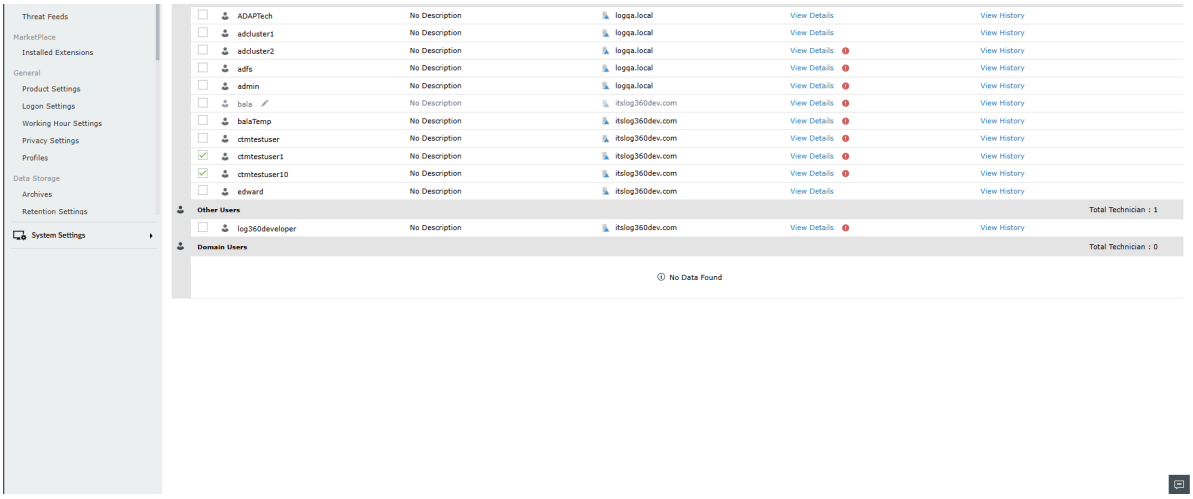


Figure 23: Disabling technicians

4. In the confirmation pop-up, click Yes to proceed.

> NOTE
>
> Disabled technicians cannot log in or perform any assigned actions until they are enabled again.

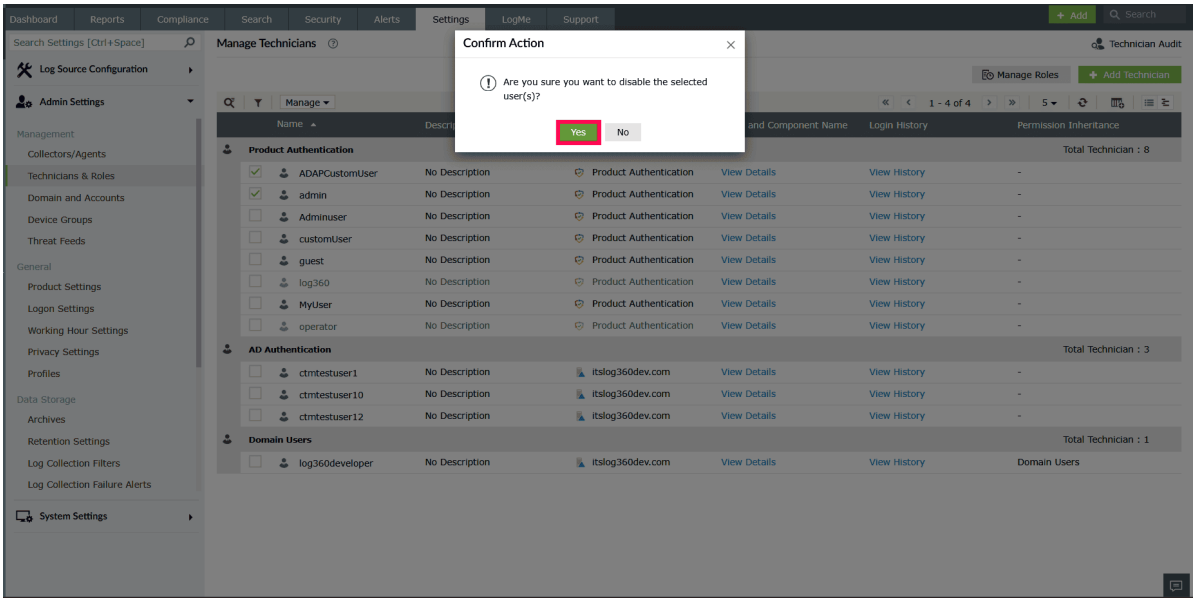
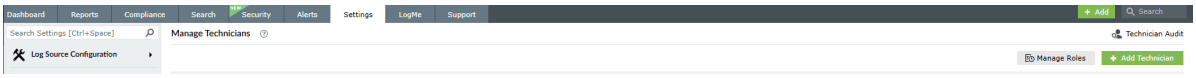


Figure 24: Disabling technicians

To enable technicians

1. On the Manage Technicians page, select the checkboxes next to the technicians you want to enable.
2. Click the Manage drop-down menu.
3. Select Enable from the list.



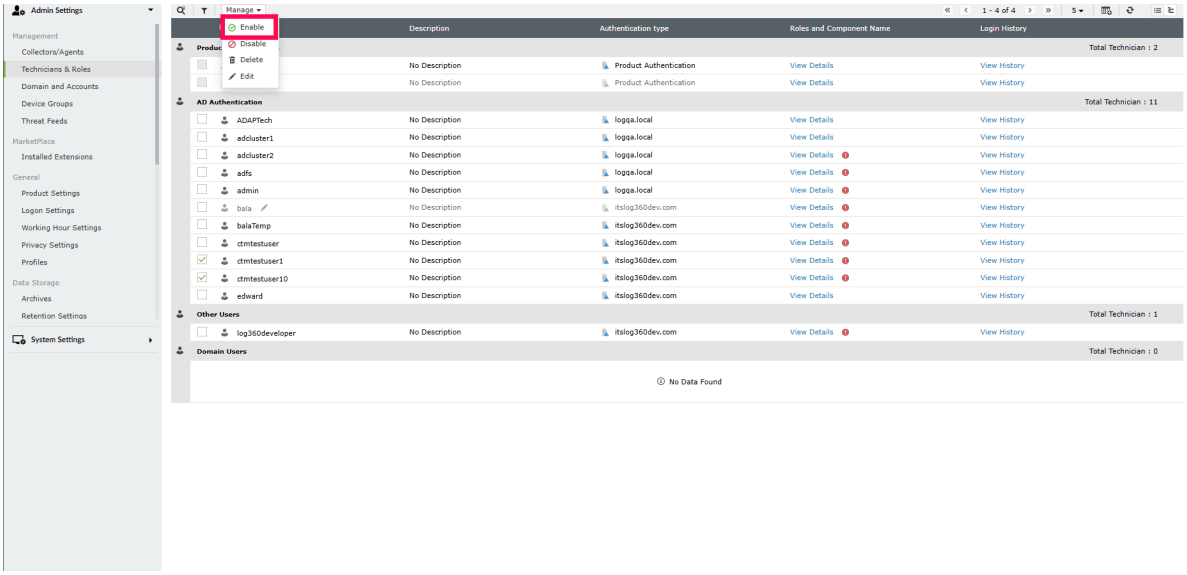


Figure 25: Enabling technicians

Deleting technicians

1. On the Manage Technicians page, select the checkboxes next to the technicians you want to delete.

> NOTE
>
> If an AD group is deleted, any technician who was part of that group will be converted to an individual technician and placed in the Others group.

2. Click the Manage drop-down menu.
3. Select Delete from the list.

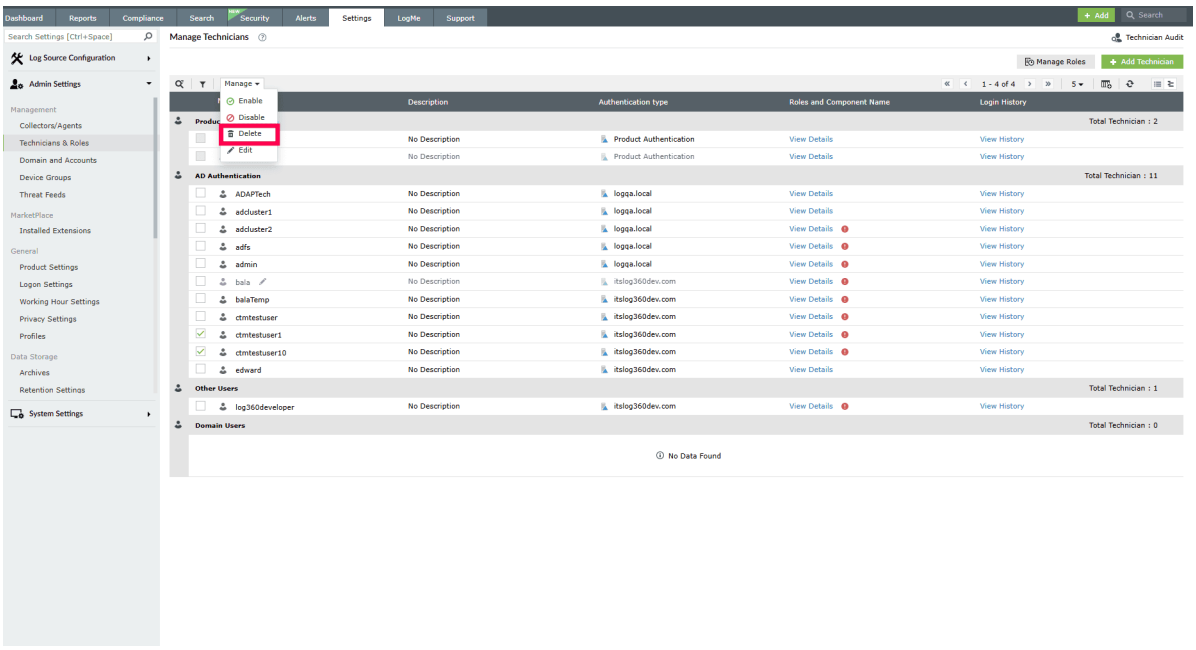


Figure 26: Deleting a technician

4. In the confirmation pop-up, click Yes to proceed.

> NOTE
>
> You cannot delete default technicians or the currently logged-in user.

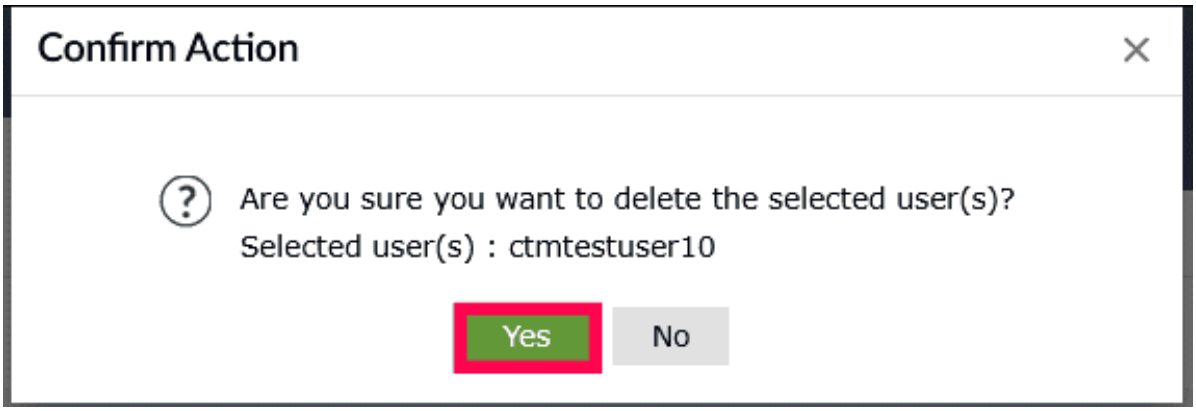


Figure 27: Deleting a technician

Read also

This page elaborated on viewing, editing, updating multiple technicians, enabling/disabling, and deleting technicians. For more related functionalities, refer to the following article:

- Creating and managing roles

9.1.13.4. Creating and managing roles

Last updated on: September 12, 2025

In this page

Overview

Creating a role

Managing roles

Overview

Roles define the set of permissions assigned to a user or a group of users in the product console. They determine what actions a user can perform and what data they can access. By creating and managing roles effectively, you can ensure that each user has the appropriate level of access, maintaining both operational efficiency and data security. This page elaborates on how to create new roles and manage existing ones.

Creating a role

1. In your account, navigate to the Settings tab.
2. Under Admin Settings, select Technicians and Roles.

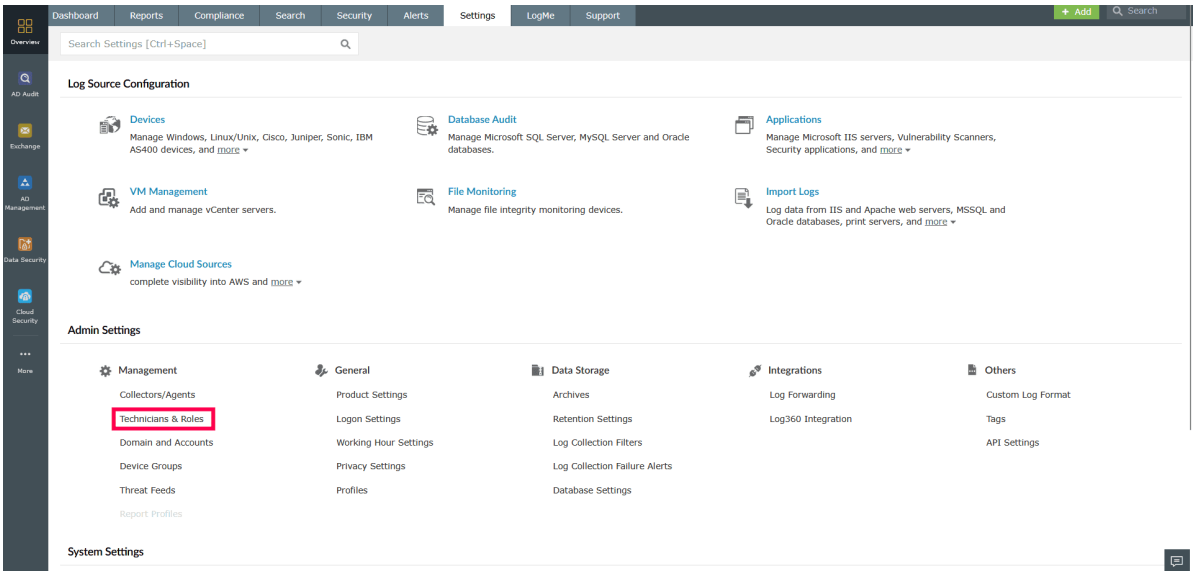
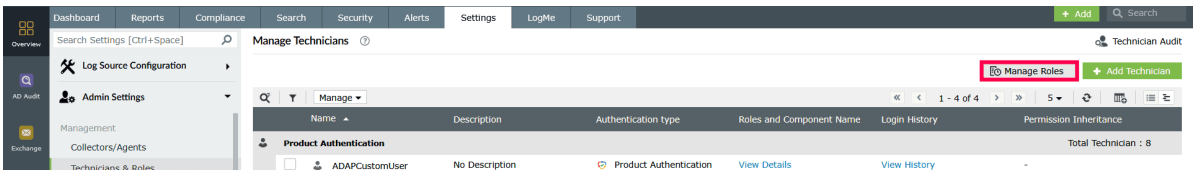


Figure 1: Navigating to Technicians and Roles

3. On the Manage Technicians page, click Manage Roles.



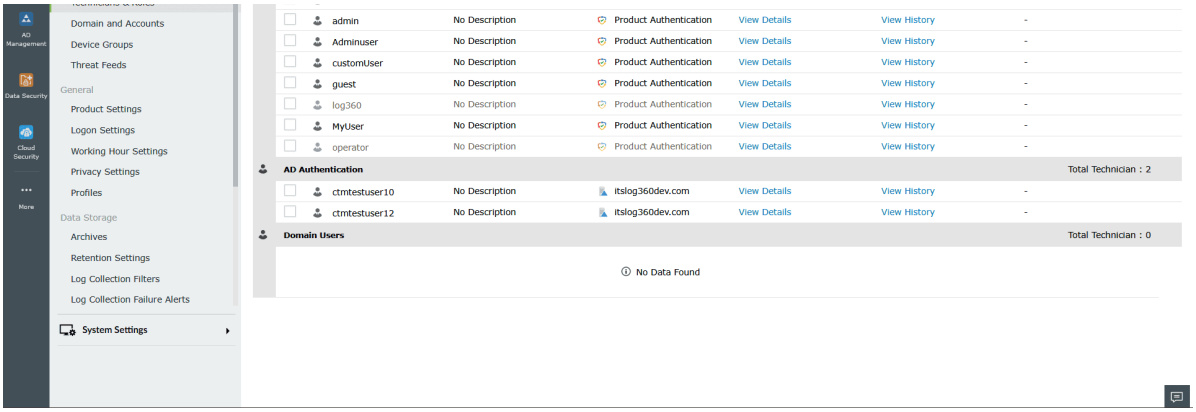


Figure 2: Navigating to Manage Roles

4. In the top-right corner, click Create New Role.

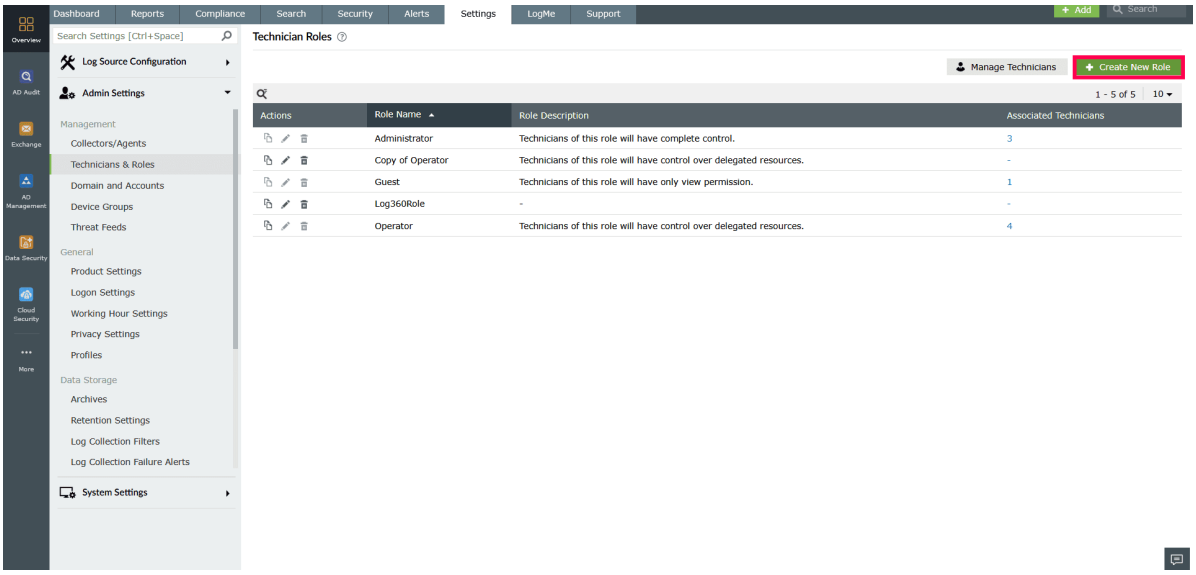


Figure 3: Creating a new role

5. Enter a Role Name. You may also provide a Description (optional).

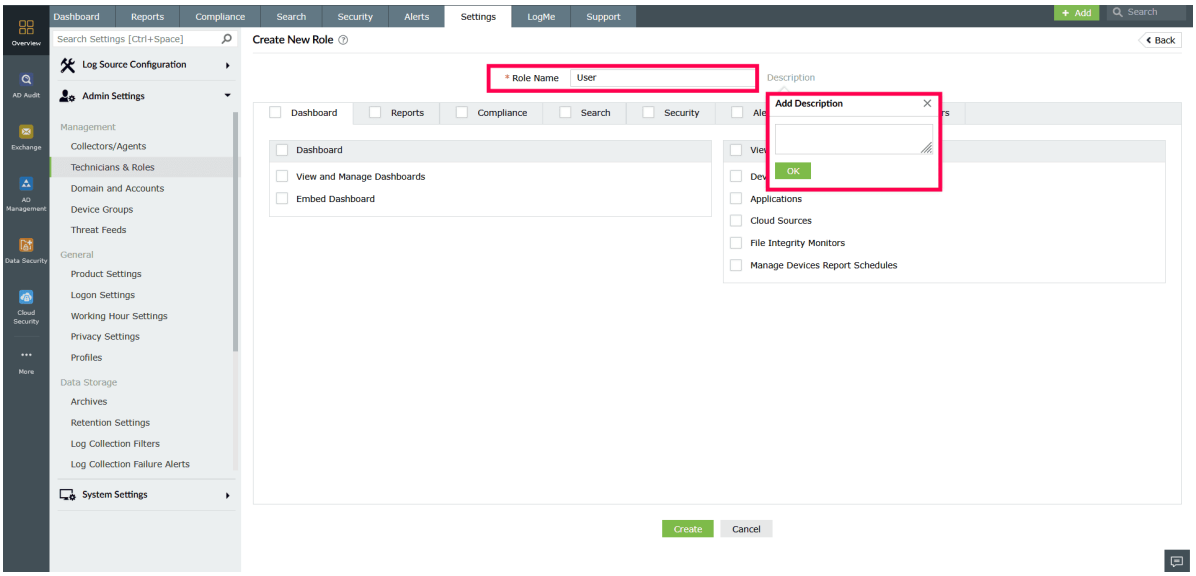


Figure 4: Adding role name and description

6. The available permissions are grouped under these tabs: Home, Reports, Compliance, Search, Security, Correlation, Alerts, Settings, and Others.
7. Select the checkbox beside a tab to grant all permissions under that tab.

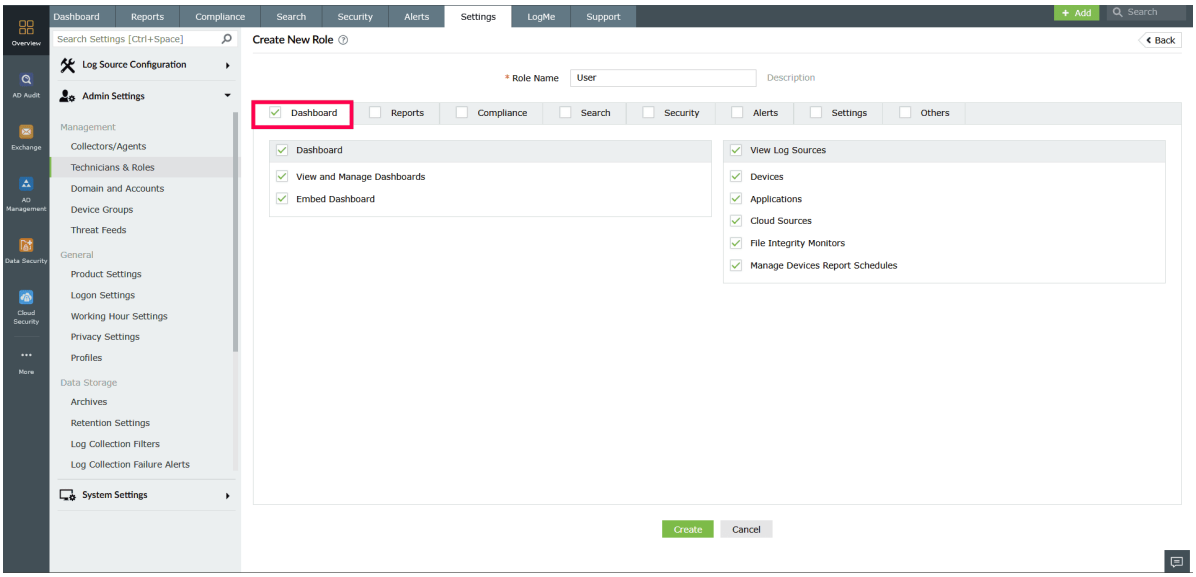


Figure 5: Configuring permissions

8. You can also click the tab to select individual permissions. The tabs and their permissions are as follows:
   - Dashboard:
     - Dashboard: Allow users to view, create, and manage dashboards.
     - View the Log Sources: Assign permissions to view device, application, and file integrity monitoring logs.
     - Use the section-level checkbox to select all options at once.

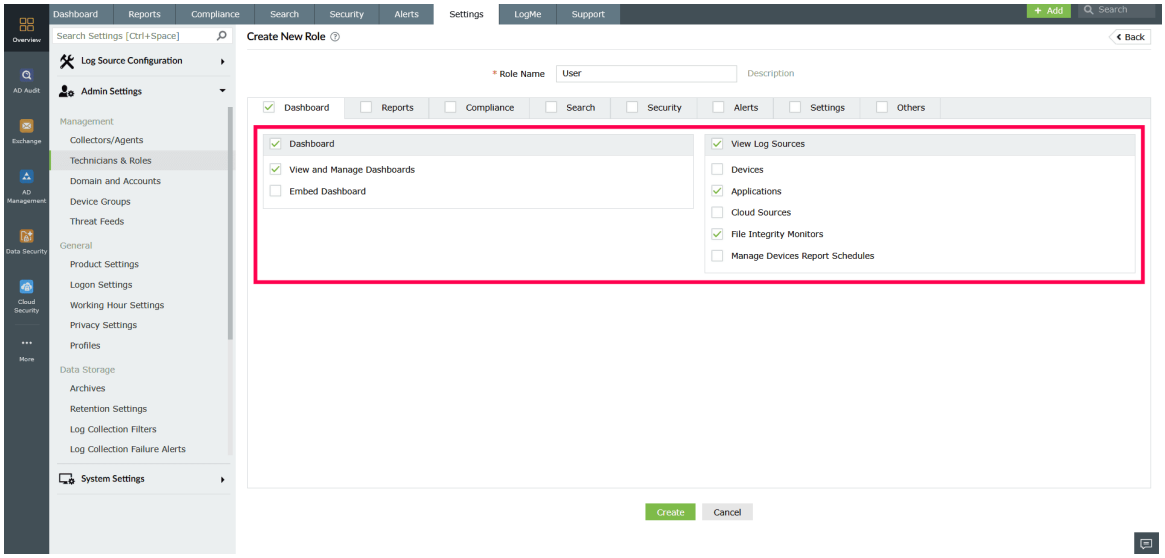


Figure 6: Configuring permissions in the Home tab

   - Reports:

- Choose whether users can view, schedule, and create reports.
- Select General to grant all permissions under this tab.

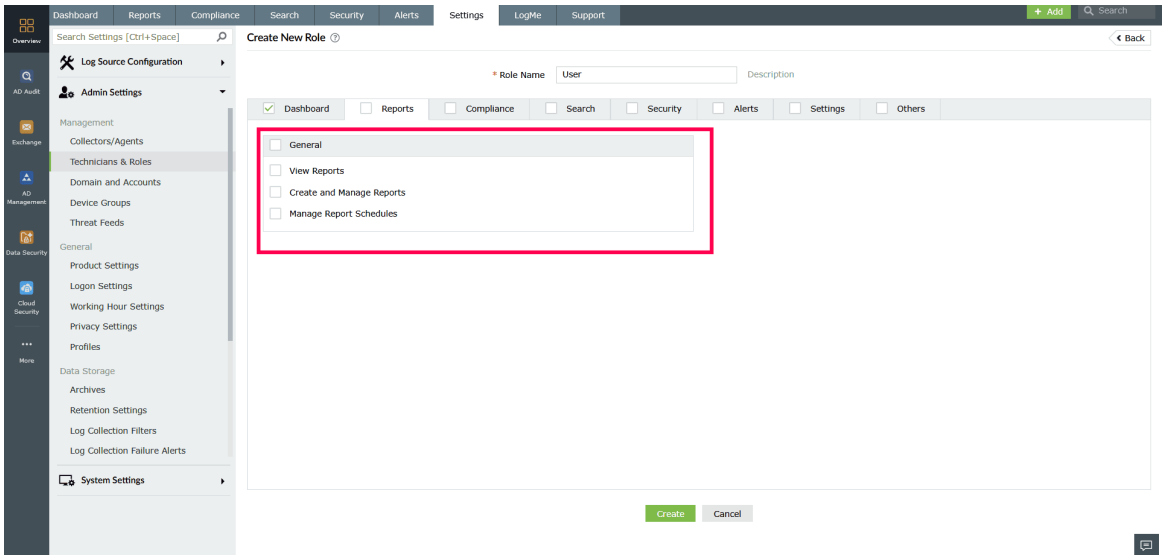


Figure 7: Configuring permissions in the Reports tab

- Compliance
  - Allow viewing, creating, and scheduling of compliance reports.
  - Use General to assign all compliance permissions.

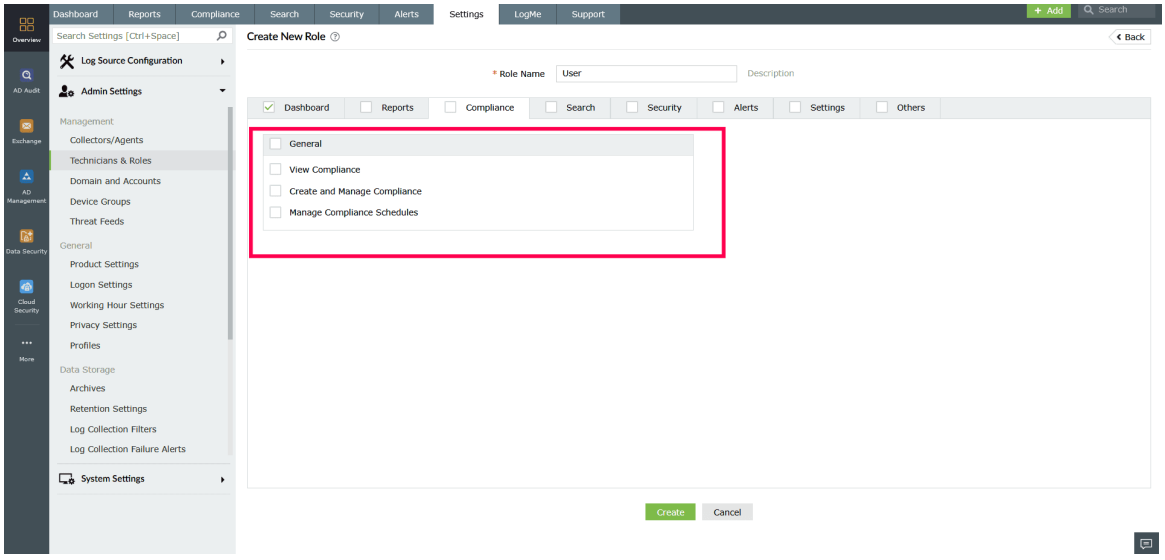
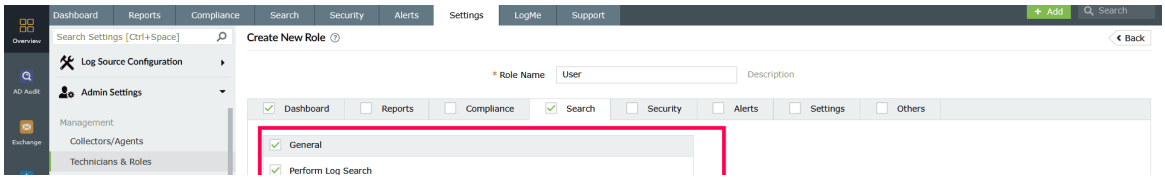


Figure 8: Configuring permissions in the Compliance tab

- Search
  - Allow or restrict the ability to search collected logs.



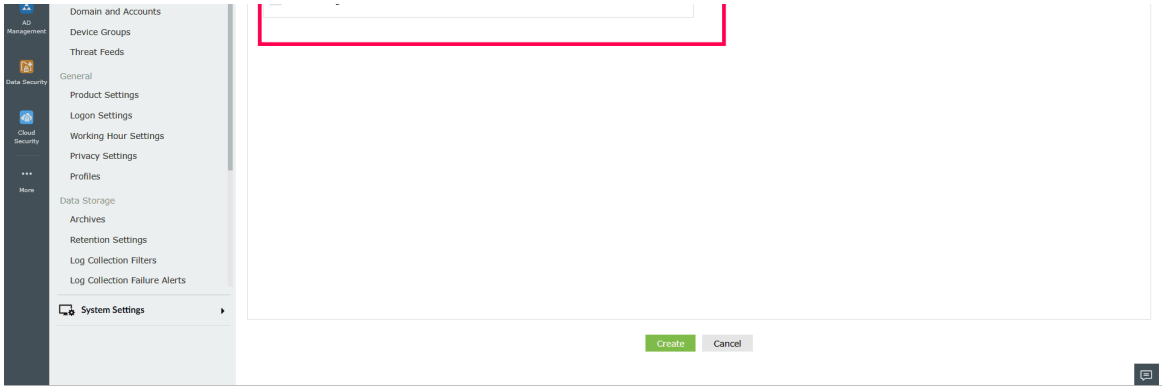


Figure 9: Configuring permissions in the Search tab

- Security
  - Security: View security reports, manage security rules, create and manage security actions, manage report schedules, and create security rules. Includes permission for accessing the security dashboard.
  - Activity Monitoring: View reports, create and manage rules, and schedule activity monitoring reports.

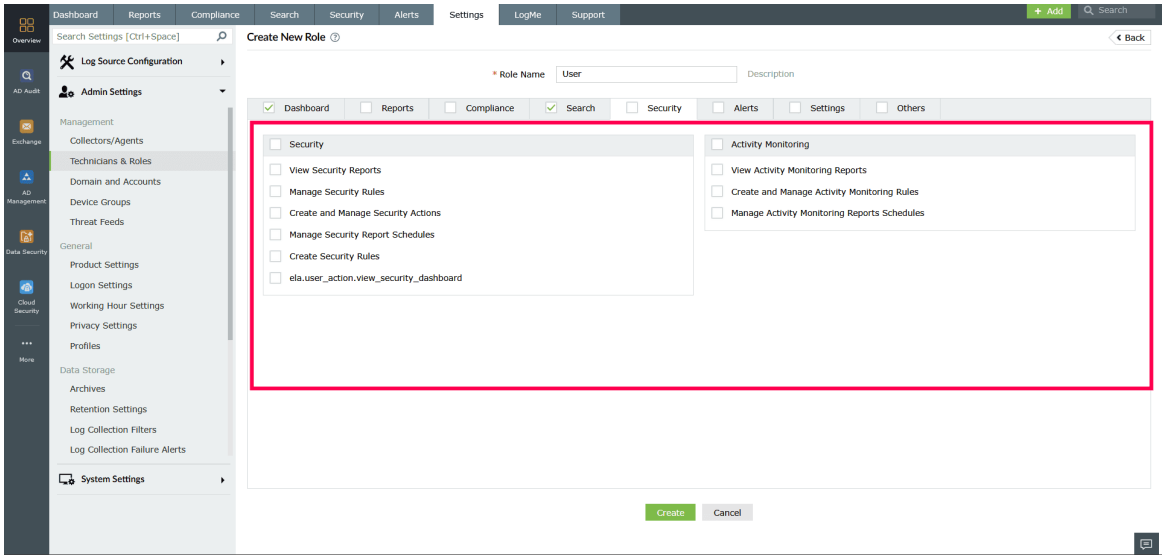
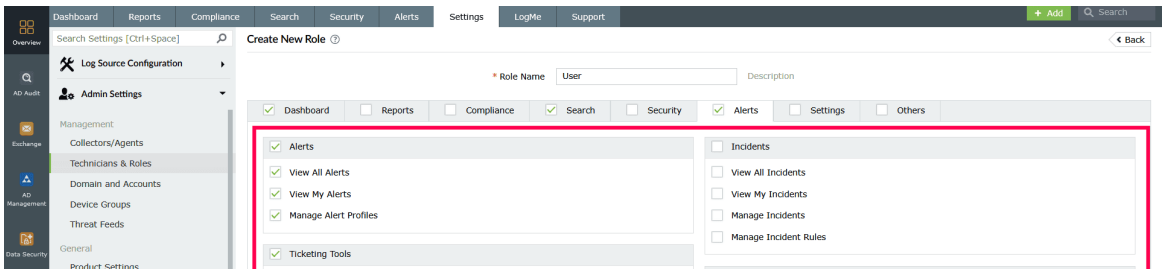


Figure 10: Configuring permissions in the Security tab

- Alerts
  - Alerts: View all or personal alerts, manage alert profiles, and assign alert rules.
  - Incidents: View all or personal incidents, manage incidents, and manage incident rules.
  - Ticketing Tools: Configure ticketing integrations, create tickets, and view tickets.
  - Incident Workflows: Manage workflows for incident handling.



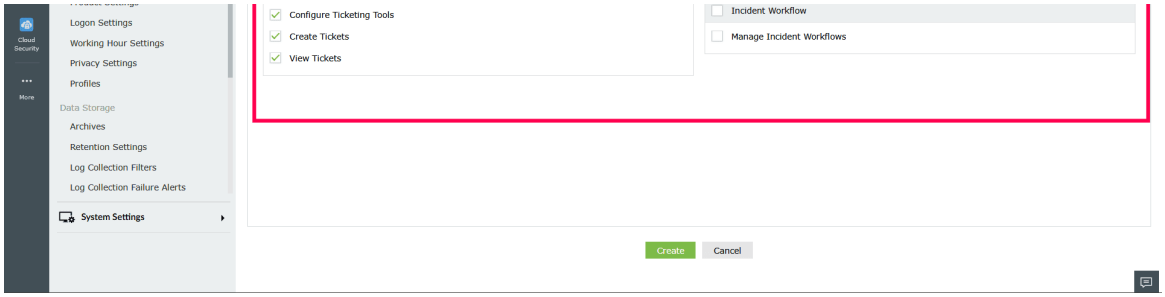


Figure 11: Configuring permissions in the Alerts tab

- Settings
  - Log Source Configuration: Configure and manage devices, applications, databases, virtual machines, file integrity monitoring, manage cloud sources, and import logs.
  - Admin Settings: Manage device groups, threat feeds, report profiles, log archives, log retention settings, database settings, log collection filters, log collection failure alerts, privacy settings, profiles, log forwarder, Log360 integrations, custom log parsing rules, and tags.
  - System Settings: Manage general and system-level configurations.

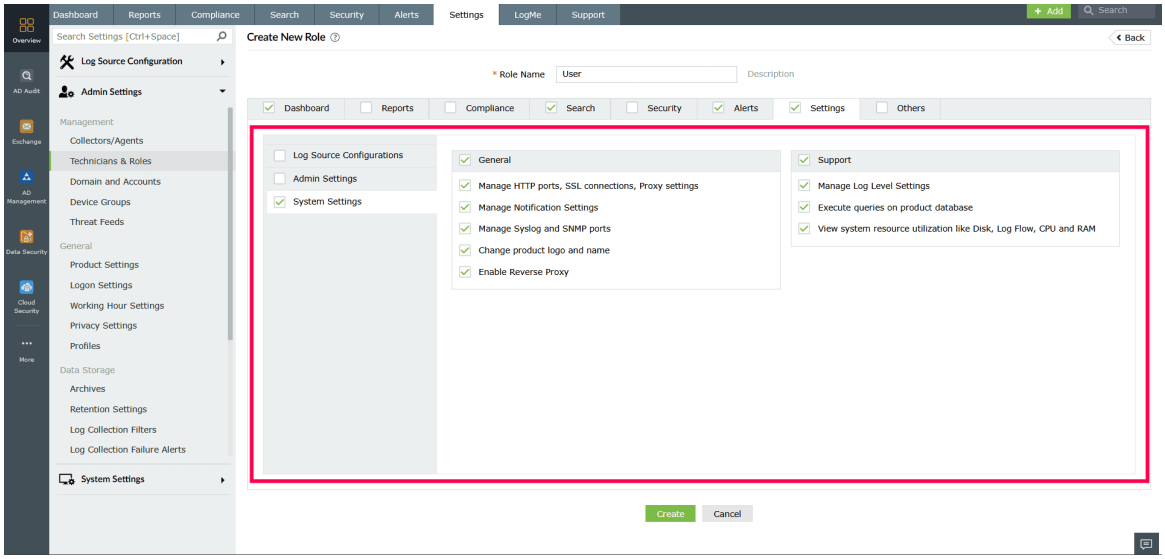
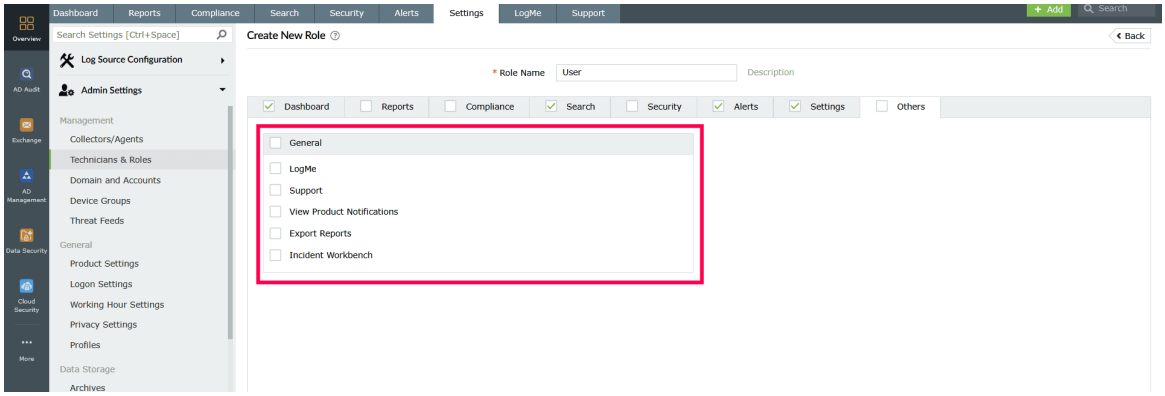


Figure 12: Configuring permissions in the Settings tab

- Others
  - Grant access to view product support information, supported log sources, and notifications.



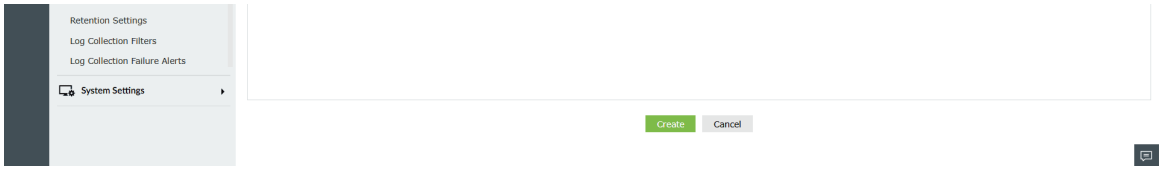


Figure 13: Configuring permissions in the Others tab

9. After selecting all required permissions, click Create to save the role.

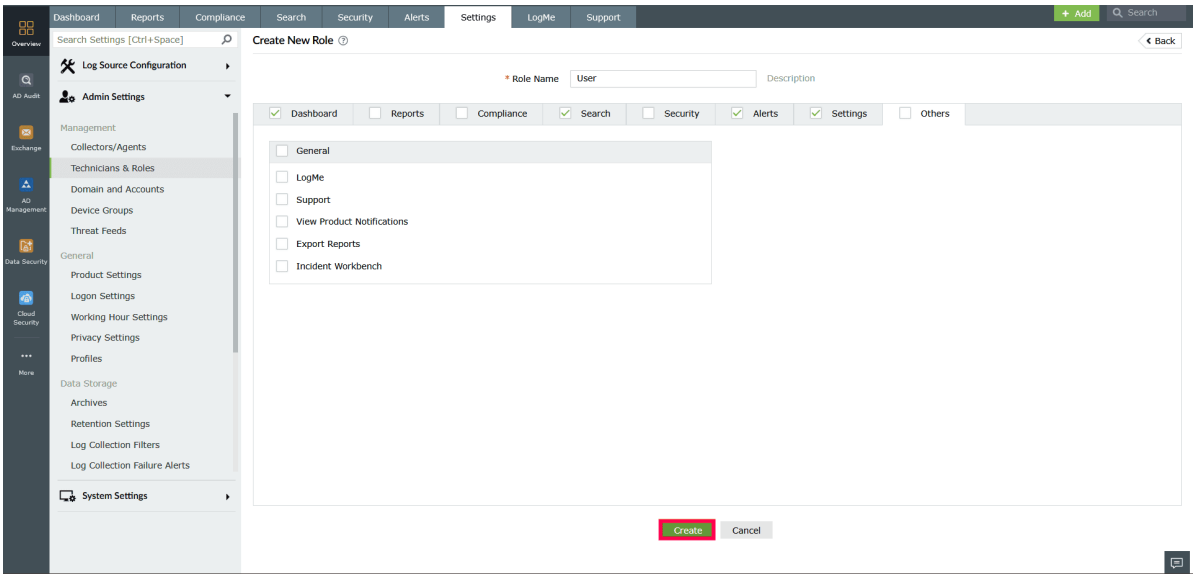


Figure 14: Creating a new role

Managing roles

1. Click the  icon to create a duplicate of an existing role.

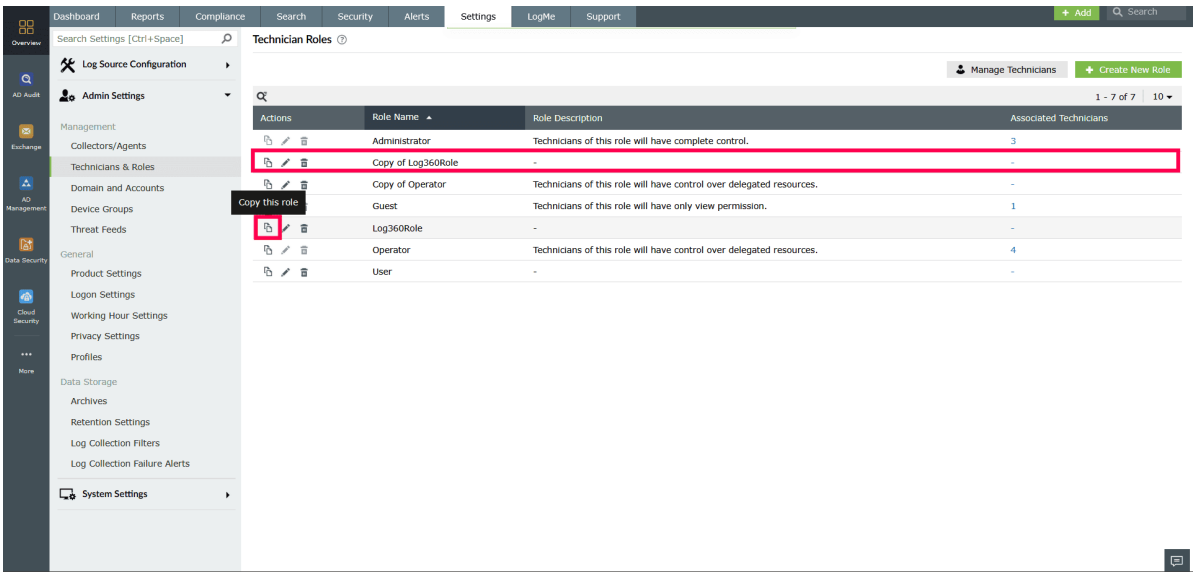


Figure 15: Making a copy of a role

> **NOTE**
>
> Default roles such as Guest, Admin, and Operator cannot be edited or modified.

2. Click the icon to modify the permissions of a role.

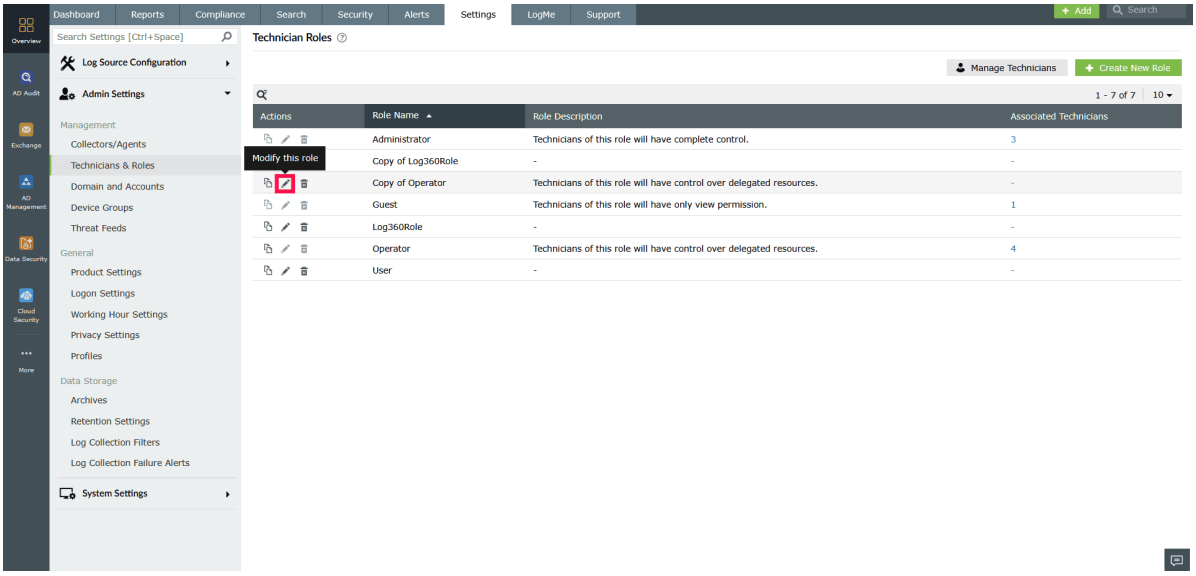


Figure 16: Modifying a role

3. This opens the Modify Role page where you can change permissions.

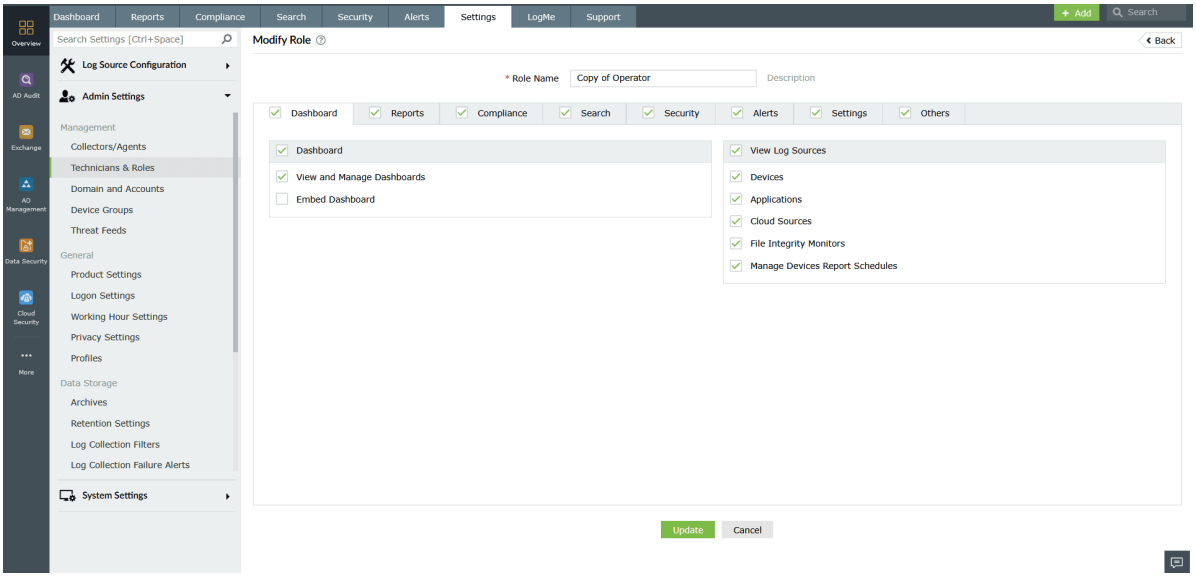


Figure 17: Modifying a role

4. Click the icon to remove a role.



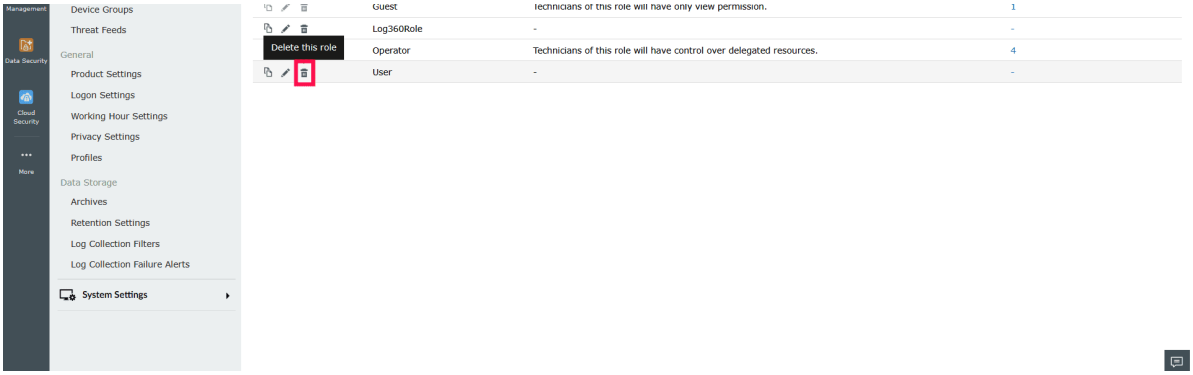


Figure 18: Deleting a role

5. In the confirmation popup, click Yes to confirm deletion.

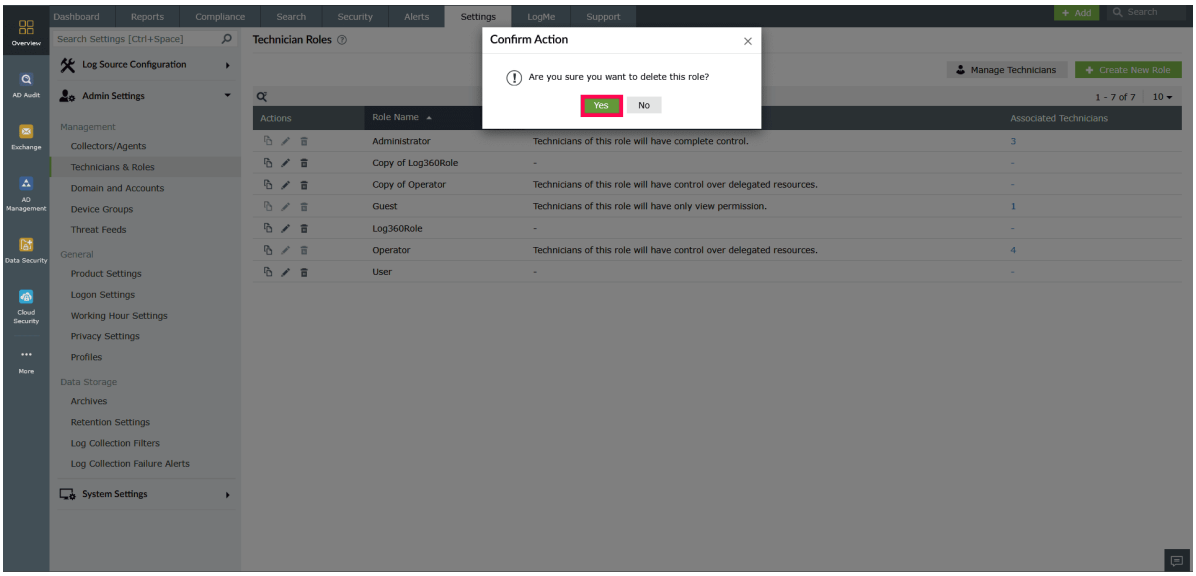


Figure 19: Deleting a role

6. Use the icon to find roles by their name.

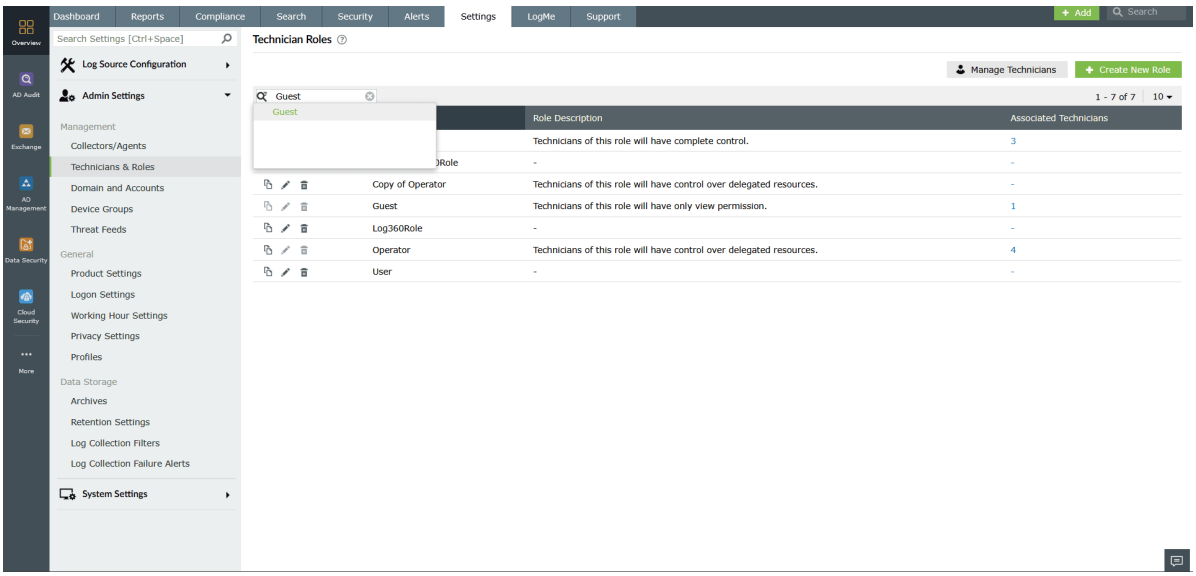


Figure 20: Searching for a role

7. To view the technicians associated with each role, click the number shown under the Associate Technician column.

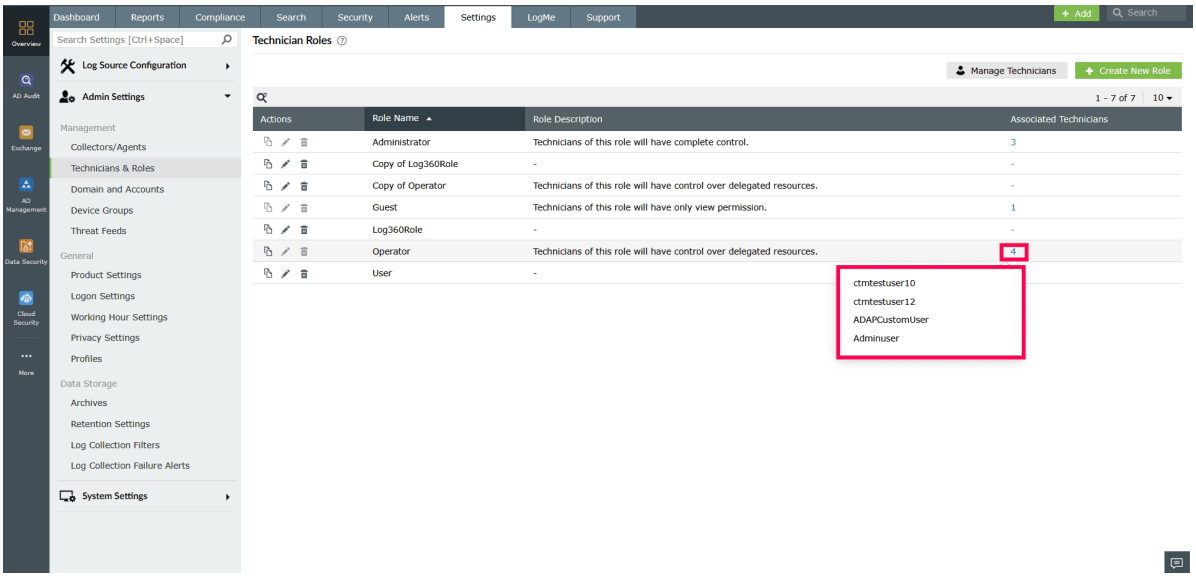


Figure 21: Viewing associated technicians

Read also

This page explained how to create and manage roles. For more details on the feature, see the articles below:

- About Centralized Technician Management
- Adding technicians

9.2.1. Product Settings

Last updated on: September 12, 2025

You can change the following settings of Log360 from this tab.

- Connection Type
- Security Hardening
- General

Connection Type

1. Choose your connection type. You can choose to use either http or https.
2. Specify the port number of your choice after choosing they type of connection.
   - Default ports - HTTP : 8095, HTTPS : 8458.
3. To enable LDAP SSL, mark the check-box against the Enable LDAP SSL field.
4. Click Save to store the configured settings.

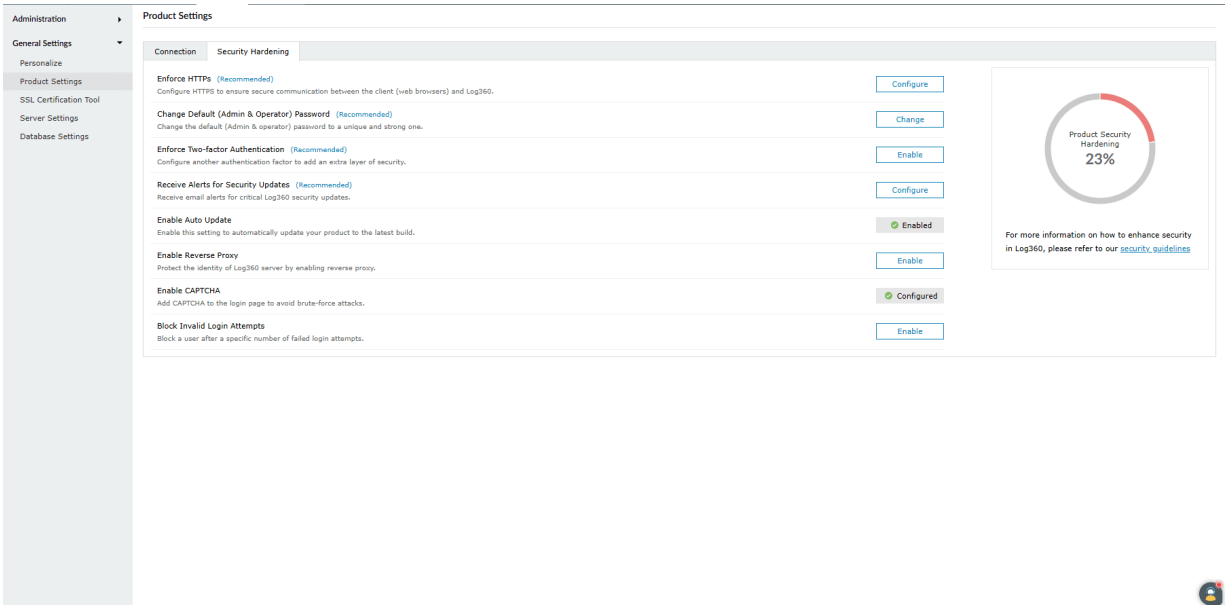
General

1. Be alerted when the available disk space falls below a pre-defined level (1 GB, 2 GB or 5 GB), by selecting the appropriate value from the drop-down box.
2. Select the Session Expiry Time, which is the time for which a user session would last, from the drop-down box.
3. Select the level of logs that is to be collected by the product. The default working mode for Log360 is Normal with minimal set of debugging information. Select Debug to collect detailed log reports.
4. Enable or disable collection of anonymous usage statistics gathering to be sent to us.
5. Click Save to store the configured settings.

9.2.2. Security Hardening

Last updated on: September 12, 2025

Security hardening feature helps you manage and configure the security settings of Log360. This tab also displays a security score which is calculated based upon the weightage given to each configuration.
To manage individual settings, click the Configure or Enable option corresponding to that security setting and make the required changes. Once configured, the setting will have a green ticked Configured/Enabled icon next to it, as shown in the image below.



We recommend you to configure all the settings and ensure your product security score is 100%. The security settings alert will be displayed in the notification center (icon on the top-right corner) until a security score of 100% is reached.

> **Note**
>
> For licensed customers, the alert will also be displayed after every successful login until all the mandatory security configurations (marked with * under List of security settings) are done.

List of security settings:

1. Enforce HTTPS*
   Configuring HTTPS helps you secure connection between the web browser and the Log360 server. See how to enable HTTPS.
2. Change Default (Admin & Operator) Password*
   It is recommended to use a strong password to access Log360 dashboard. Use this setting to change both the admin and operator password.
3. Enforce Two-factor Authentication*
   Two-factor authentication adds an additional layer of security. See how to configure two-factor authentication

Two-factor authentication adds an additional layer of security. See how to configure two-factor authentication.

4. Receive Alerts for Security Updates*
   Configuring this setting allows you to receive email notifications on the release of important security patches. This ensures that you are well-informed about important security updates for the product, enabling you to update it as soon as possible.
5. Enable Auto Update
   Enable this setting to automatically update your product to the latest build. Click on Configure to navigate to the auto-update settings tab. See how to enable auto-update.
6. Enable Reverse Proxy
   Enabling reverse proxy helps protect the identity of Log360 server. Click on Configure to navigate to the reverse proxy settings tab. See how to enable reverse proxy settings.
7. Enable CAPTCHA
   This setting adds captcha to the login page to avoid brute-force attacks. See how to add captcha.
8. Block Invalid Login Attempts
   This setting allows you to block a specific user who fails to login after a specific number of attempts. See how to block invalid login attempts.

> **Note**
>
> The first three settings given in the above list are mandatory for Log360.

9.3.1. General logon settings and password policy

Last updated on: September 12, 2025

In this page

Logon settings

General logon settings

CAPTCHA Settings

Block Users Settings

Other Settings

Password Policy logon settings

Overview

The logon settings module helps you secure user access with options like CAPTCHA, account lockout, password reset visibility, and password policies. It includes six sub-tabs—General, Password Policy, Two-Factor Authentication, External Authentication, Allow/Restrict IPs, and Smartcard Authentication—allowing you to customize authentication and strengthen account protection.

Logon settings

1. In the product console, navigate to the Settings tab and click on Logon settings listed under Admin Settings as shown in the below image.

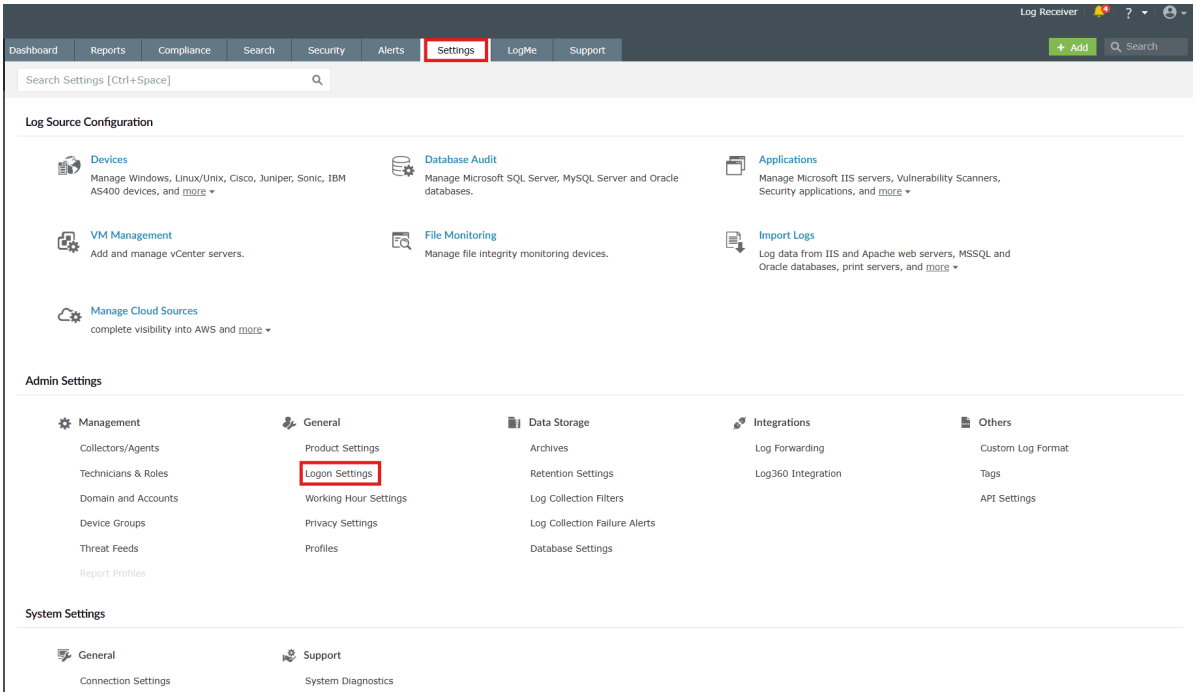


Image 1: Logon settings via the settings tab

2. You will be taken to the Logon Settings module.

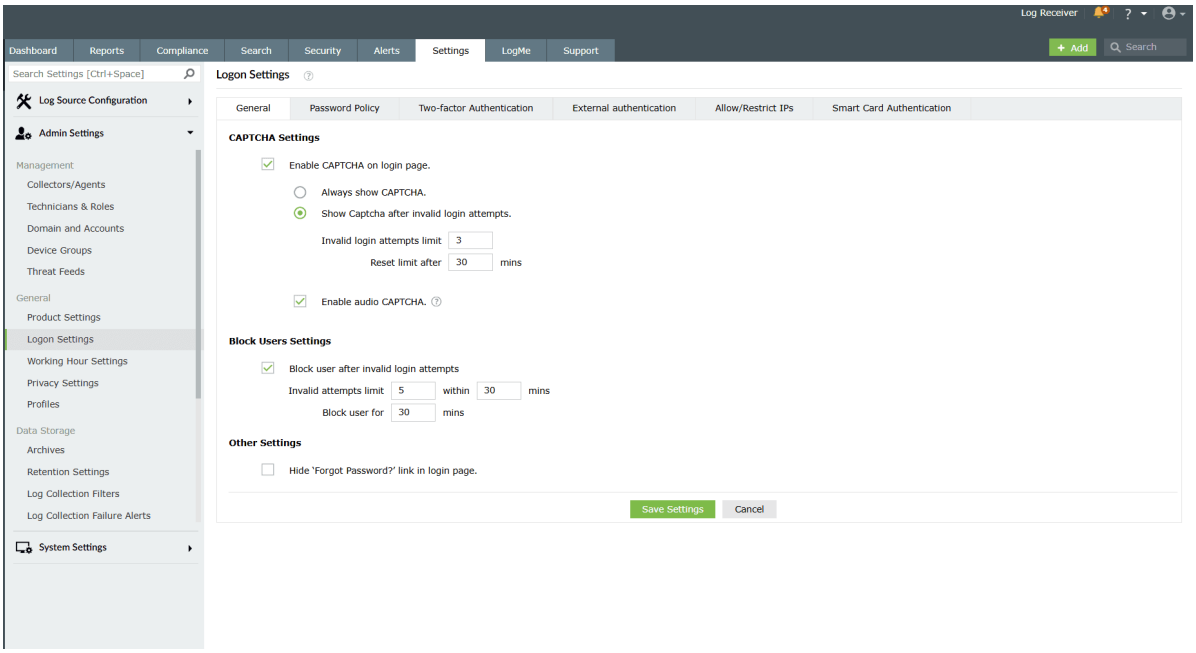


Image 2: General logon settings via the settings tab

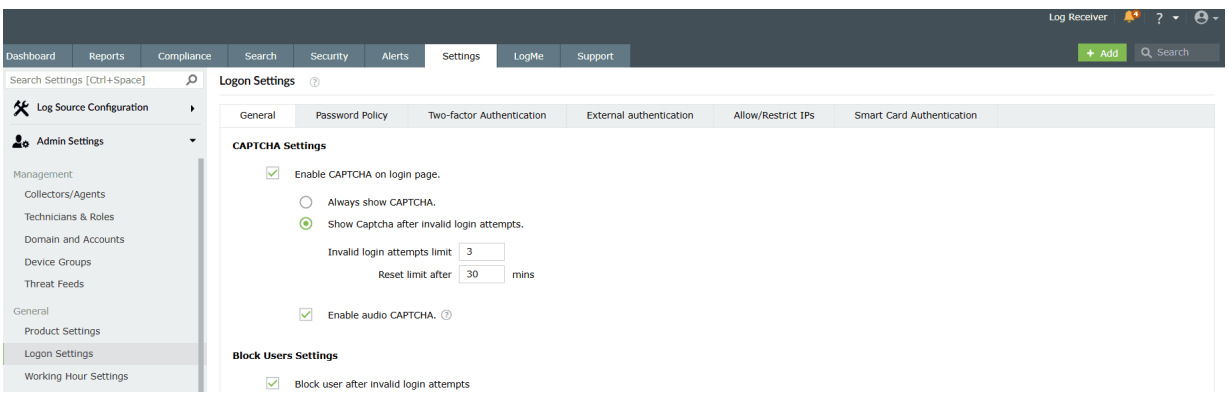
The Logon Settings module further contains 6 sub-tabs:

- General
- Password Policy
- Two-factor Authentication
- External authentication
- Allow/Restrict IPs
- Smart Card Authentication

Read further to learn more about these logon settings.

General logon settings

This setting provides options to manage login security features like CAPTCHA, account lockout, and password reset visibility.



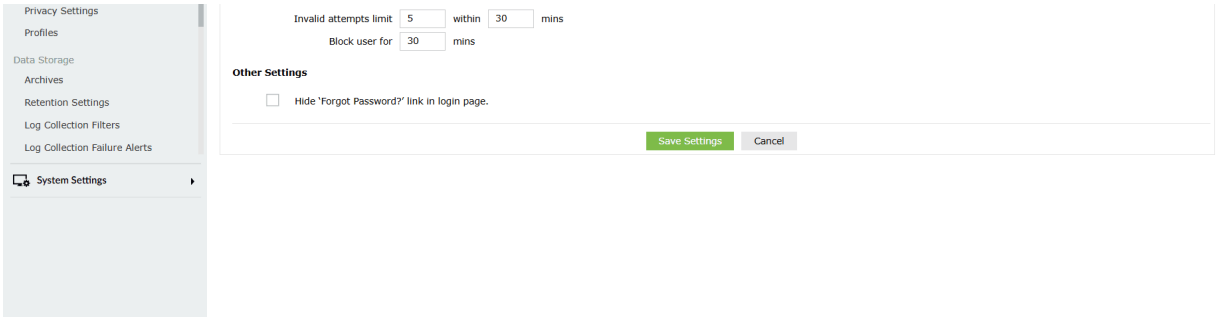


Image 3: General logon settings sub-tab via the settings tab

The General sub-tab contains the below configurations:

1. CAPTCHA settings

Shows a CAPTCHA challenge during login to prevent automated access attempts. This setting- Enable CAPTCHA on login page, is enabled by default. Click on the checkbox to empty it and disable this setting. With the CAPTCHA enabled, you can choose to either-

- Always show CAPTCHA: Displays CAPTCHA for every login attempt, regardless of success or failure history. Or,
- Show CAPTCHA after invalid login attempts: Displays CAPTCHA only after a set number of failed login attempts. You can set the requirement for CAPTCHA to the user by configuring the Invalid login attempts limit (default value is 3)-set the number of invalid login attempts limit after which a CAPTCHA verification will be required for the user to login and a time interval for Reset limit after (default value is 30 mins)-set a time interval in minutes for the corresponding invalid logon attempts.
- Enable audio CAPTCHA: This is an additional optional configuration which is also enabled by default. When audio CAPTCHA is enabled, only digits will be shown in the CAPTCHA image. If a browser doesn't support audio CAPTCHA, then the default CAPTCHA image (with letters and digits) will be shown.

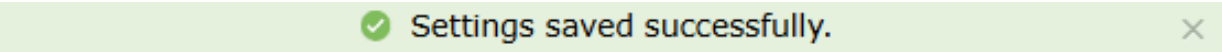
2. Block Users settings

This setting- Block user after invalid login attempts, is enabled by default. Click on the checkbox to empty it and disable this setting. This option locks the account for a set time if failed login attempts exceed the configured limit. In this setting, you can configure the number of invalid login attempts from a user within a period of time, after which the user will be automatically blocked for a certain period of time. You can set the values for the same under:

- Invalid attempts limit: A numeric value (default value is 5)
- Within: Value in minutes (default value is 30 mins)
- Block user for: Value in minutes (default value is 30 mins)

3. Other settings

This setting- Hide 'Forgot Password?" link in login page, is disabled by default. If you want to hide the "Forgot Password?" link in the login page, then enable this setting by clicking on the empty checkbox. When enabled successfully, this setting removes the password reset link from the login page for added security.
After all the necessary configurations are made, click on Save Settings. Upon successful completion of action, the below pop-up appears.



Password Policy logon settings

This setting defines rules for password strength, change frequency, and reuse restrictions to enhance account security.

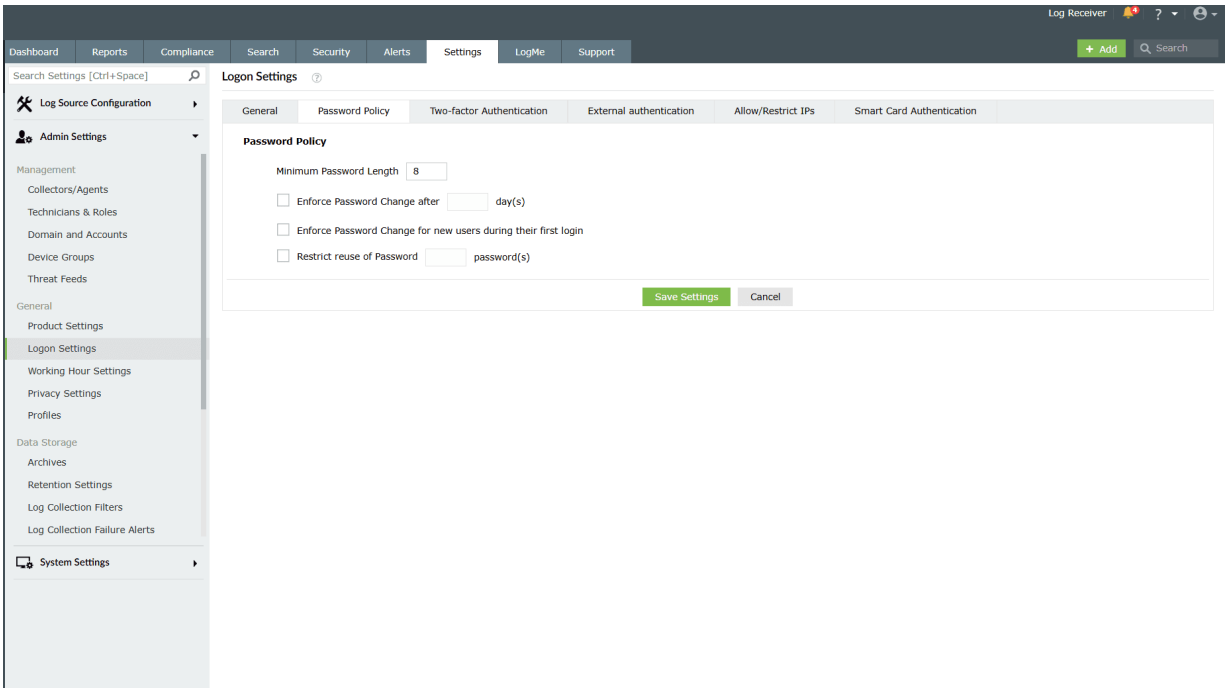
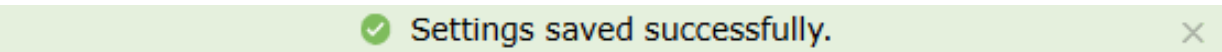


Image 4: Password policy logon settings sub-tab via the settings tab

The Password Policy sub-tab contains the below configurations:

1. 1. Minimum Password Length: Specifies the minimum number of characters required in the password. The default value is set to 8 characters.
2. 2. Enforce Password Change after: Requires users to change their password after a set number of days. Enter the desired value in days to enable this option. This setting is disabled by default. Click on the empty checkbox to enable this setting.
3. 3. Enforce Password Change for new users during their first login: Forces new users to change their password upon first login for better security. This setting is disabled by default. Click on the empty checkbox to enable this setting.
4. 4. Restrict reuse of Password: Prevents users from reusing the specified number of their most recent passwords. Enter the number of passwords to restrict in the provided field. This setting is disabled by default. Click on the empty checkbox to enable this setting.

After all the necessary configurations are made, click on Save Settings. Upon successful completion of action, the below pop-up appears.



Read also

This document explained how to configure CAPTCHA, block users after invalid login attempts, and hide the “Forgot Password?” link, and set password rules like length, expiry, and reuse restrictions. For more understanding, refer to the below help documents:

- Two-factor authentication
- Allow/restrict IP addresses
- Smartcard authentication

9.3.2. Two-factor authentication

Last updated on: September 12, 2025

In this page

Overview

Two-Factor Authentication

Email Verification

SMS Verification

Google Authenticator

RSA SecurID

Duo Security

Microsoft Authenticator

Custom TOTP Authenticator

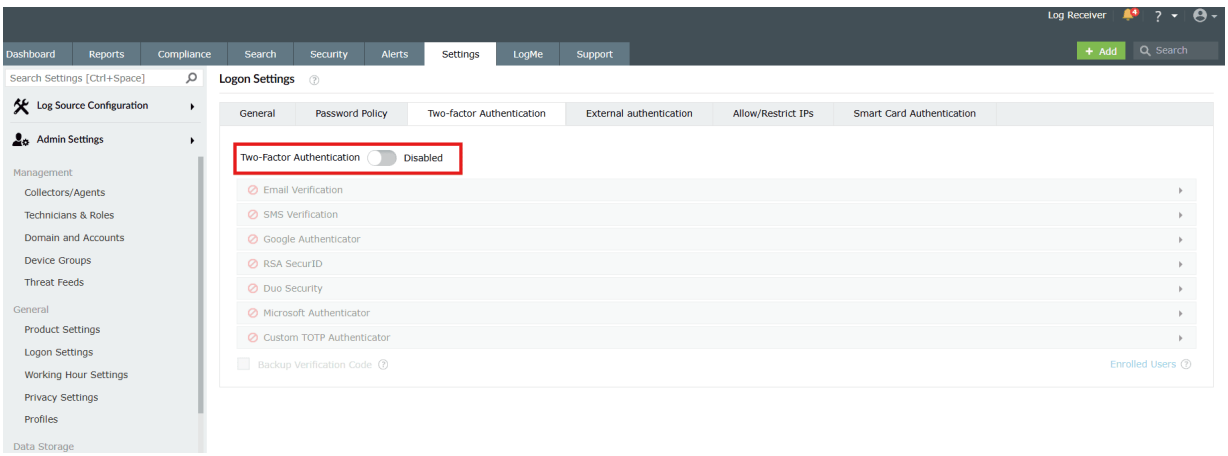
Backup Verification Codes

Overview

Two-Factor Authentication (2FA) adds an extra layer of login security by requiring users to verify their identity with a second factor in addition to their password. You can choose from multiple authentication methods such as email, SMS, authenticator apps, RSA SecurID, Duo Security, or backup codes. At least one method must be enabled for 2FA to work.

Two-Factor authentication

To strengthen user logon security, the product supports two-factor authentication. Two-Factor Authentication (2FA) requires a user to provide two different types of authentication factors to verify their identity. This makes sure the person logging in is really who they claim to be, even if their password is stolen.
By default, this setting and the methods under it are in a disabled state.



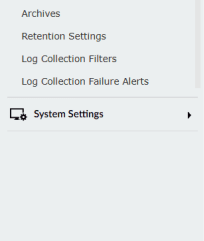


Image 1: Two-factor authentication logon settings via the settings tab

You must enable the toggle as highlighted in the above image in order to configure the Two-Factor Authentication settings. Additionally, authentication methods must also be enabled to be able to access their respective configurations.

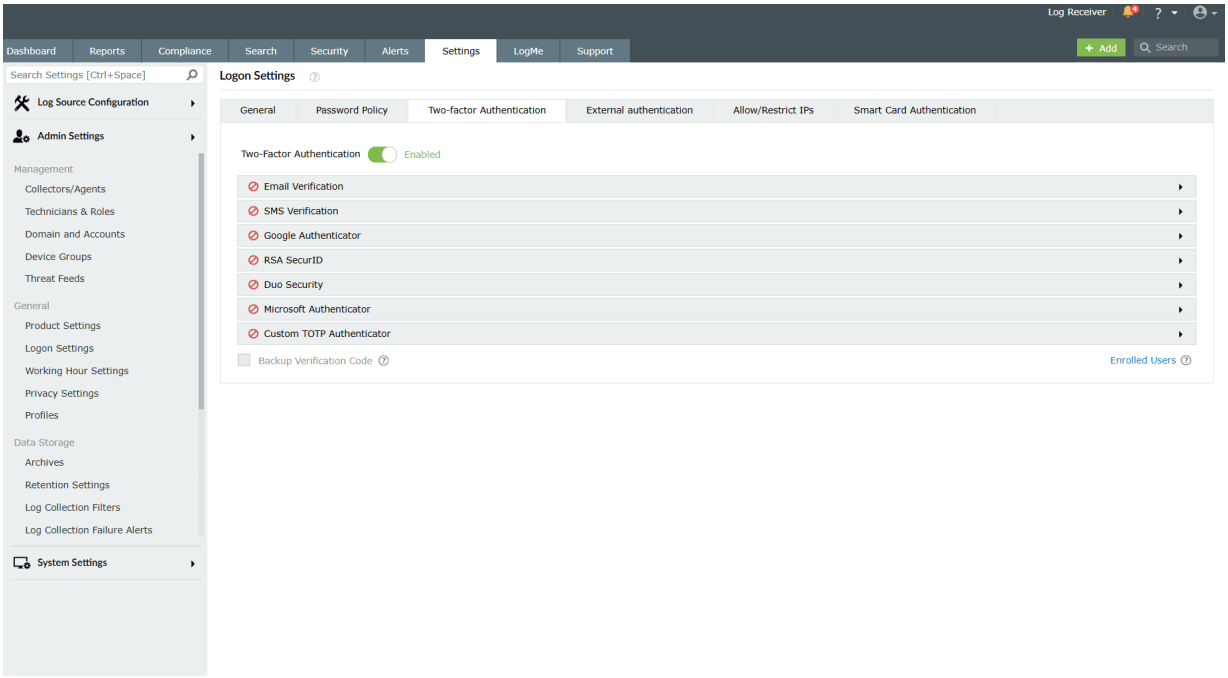


Image 2: Enabling two-factor authentication logon settings via the settings tab

> NOTE
>
> - You must configure at least one authentication mode to successfully enable two-factor authentication.
> - If multiple authentication options are enabled, then the user will be asked to choose one at the time of logging in.

Once enabled, users need to authenticate using one of the authentication mechanisms below in addition to the Active Directory credentials whenever they log in. Click on the arrow icons to expand each authentication mode's configuration fields. Below is a detailed guide for the various authentication methods available under this logon setting.

Email Verification

When this option is selected, the product sends a verification code via email to the user's email address. The user has to enter the verification code to login successfully.

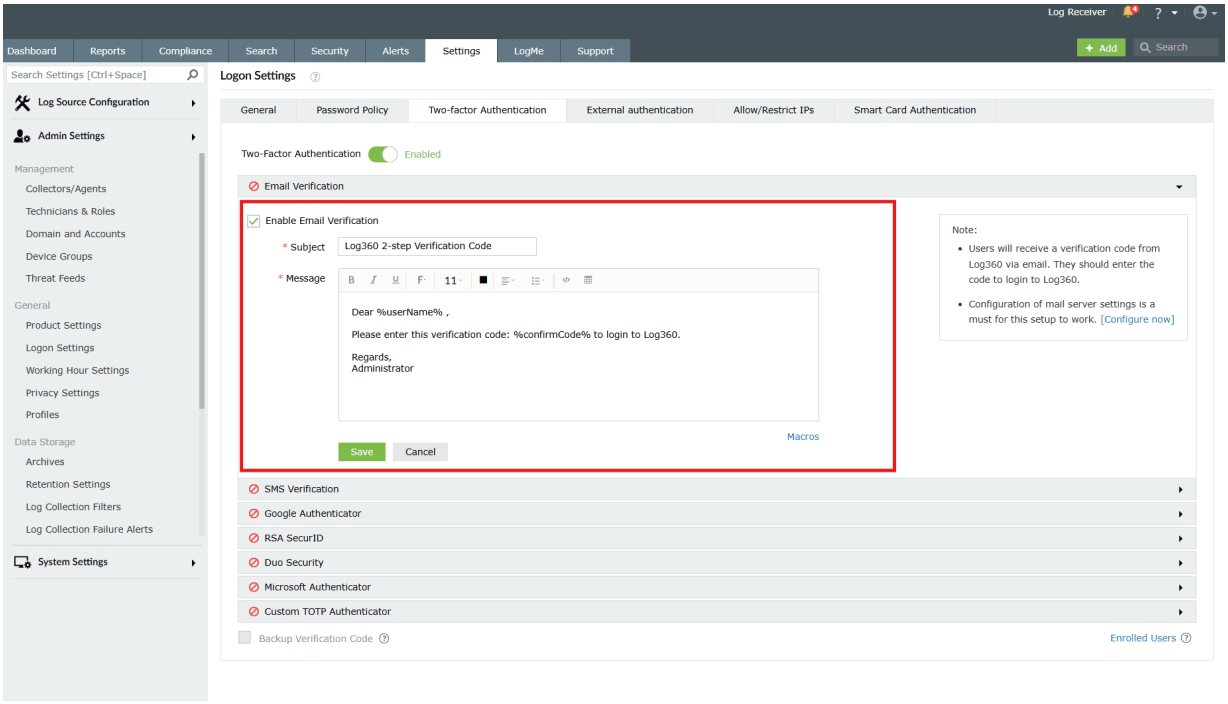
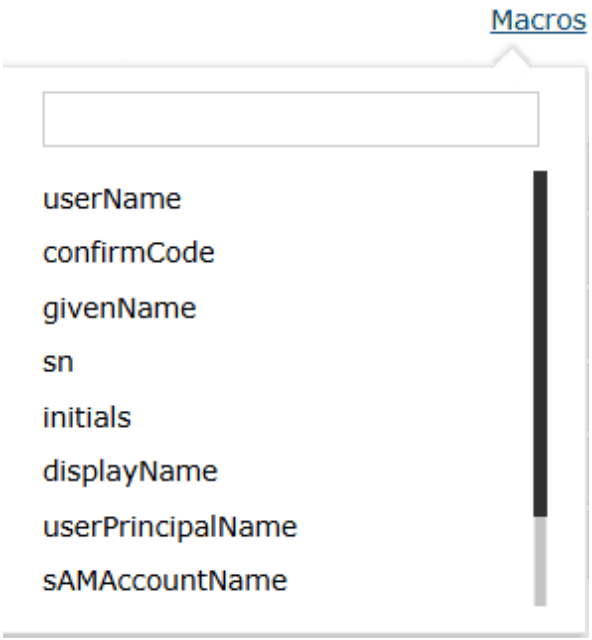


Image 3: Email verification two-factor authentication logon settings

- Subject: Enter a subject for the email.
- Message: Enter the message in the box provided.
- Click the Macros link at the bottom to insert them in the email message. The message and subject can be modified as per user requirements with the help of available macros. The macro %confirmCode% must be present in the message.



- After the necessary configurations are made, click on Save.

SMS Verification

When this option is selected, a verification code is sent via SMS to the user's mobile number. The user has to enter the verification code to login successfully.

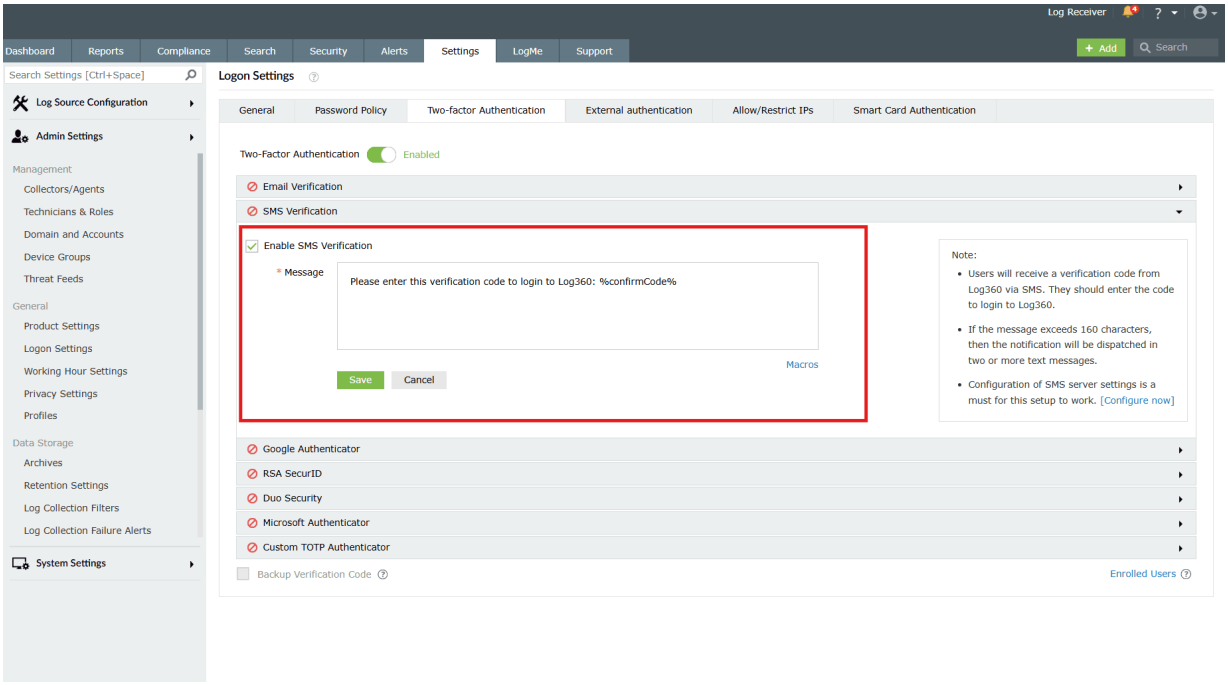
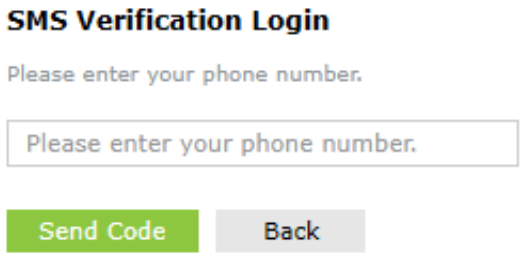


Image 4: SMS verification two-factor authentication logon settings

- Enter the Message in the box provided.
- Click the Macros link at the bottom to insert them in the SMS.
- After the configurations are made, click on Save.

Once enabled, users will be asked to enroll for two-factor authentication by entering their mobile number during login.



Google Authenticator

Google Authenticator is a mobile app that generates TOTP (Time-based One-Time Passwords) for 2FA (Two-Factor Authentication). It enhances security by requiring a second verification step when logging into the product. Once enabled, users will be required to enter a six-digit security code generated by the Google Authenticator

app for identity verification.

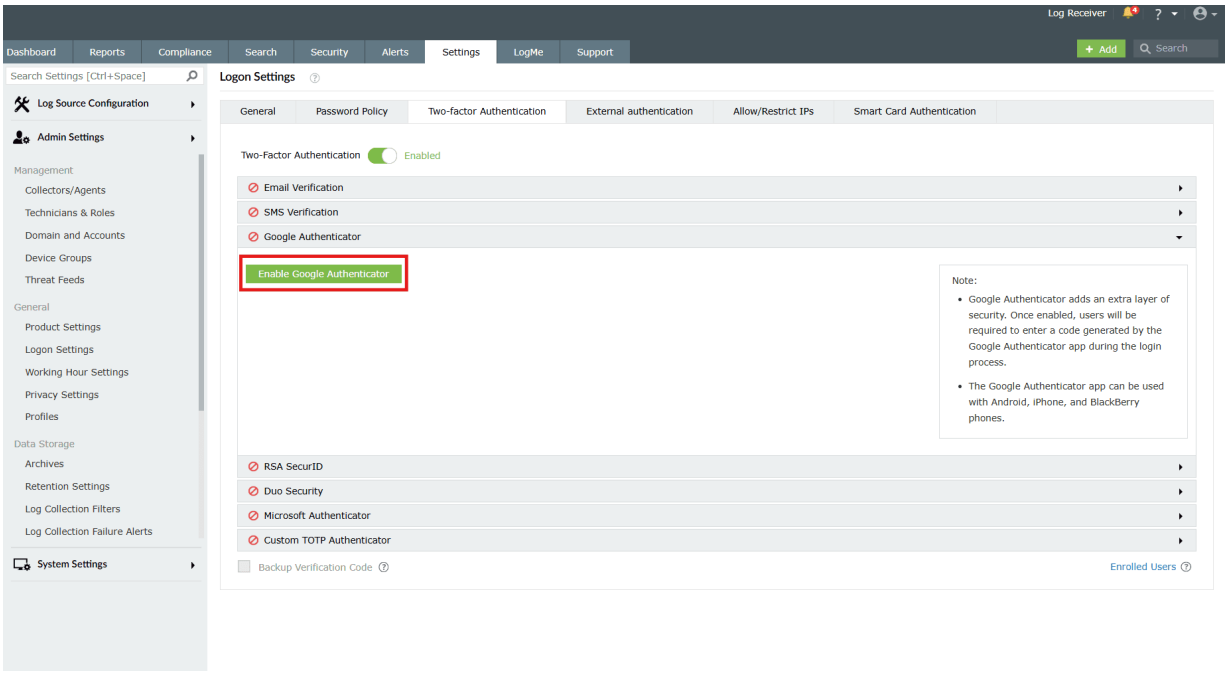
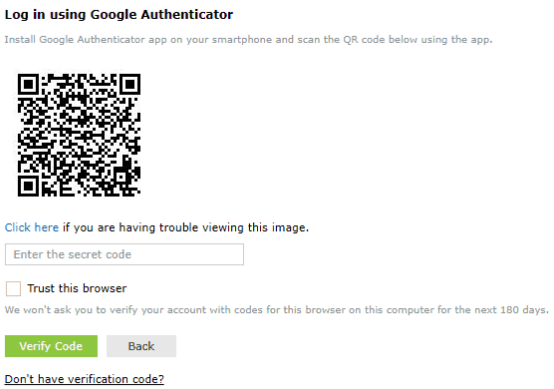


Image 5: Google authenticator two-factor authentication logon settings

- Just click on Enable Google Authenticator.
- Click on Save.

After enabling successfully, users can enroll themselves for two-factor authentication using the Google Authenticator app during login.

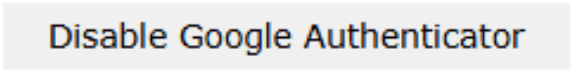
- After entering the password and logging in, the product asks to setup Google Authenticator.
- A QR will be shown which can be scanned using Google Authenticator app.



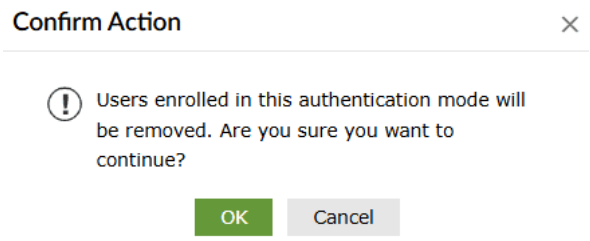
- Enter the time based 6 digit code that's generated in the Google Authenticator app to Enter the secret code box.
- Trust this browser option can be selected to go code-free for 180 days.
- Click Verify Code.

To disable Google Authenticator

1. Simply click on the Disable Google Authenticator button available.



2. A Confirm Action pop-up box appears. Click on OK.



3. Google Authenticator is now disabled, and the button shows the option to enable it now.

RSA SecurID

RSA SecurID is a mechanism developed for performing two-factor authentication for a user to a network resource. Users can use the security codes generated by the RSA SecurID mobile app, hardware tokens, or tokens received via mail or SMS to log in to the product.

Prerequisites

- For SDK integration: RSA Authentication Manager 8.0 or higher.
- For REST API integration: RSA Authentication Manager 8.2 SP1 or higher.
- Ensure that the product server is added as an authentication agent in the RSA admin console before configuring RSA SecurID in the product.

Steps to configure the product server as an authentication agent

- Log in to your RSA admin console (e.g., https://product-rsa.testdomain.com/sc).
- Navigate to Access > Authentication Agents > Add New .

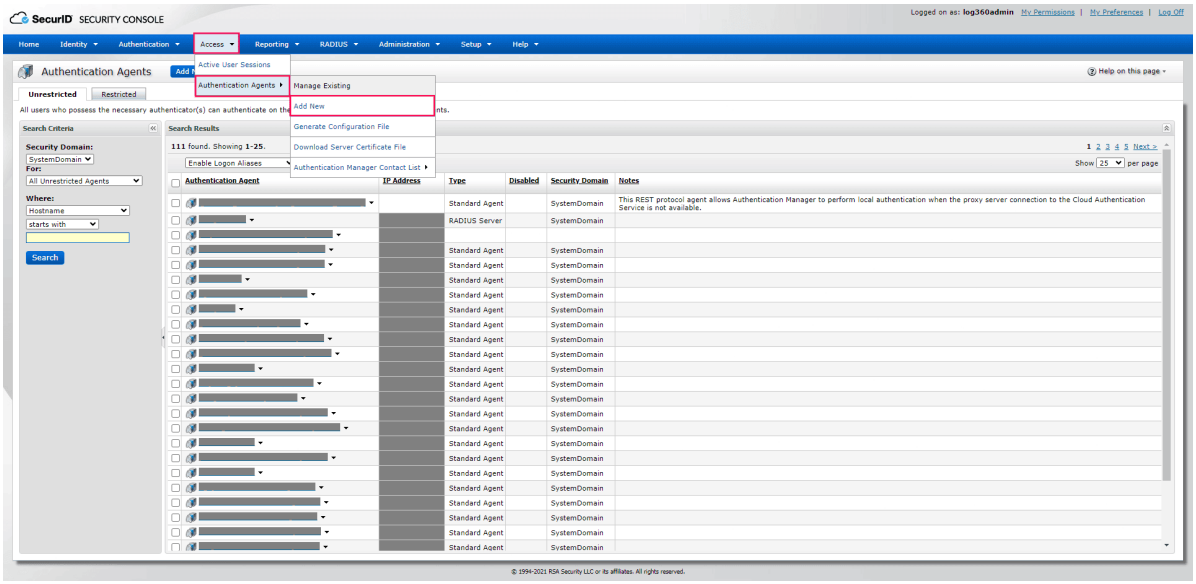


Image 6: RSA SecurID console configuration

- Enter the product server hostname in the Hostname field and click Resolve IP.
- Click Save to add the product server as an authentication agent.

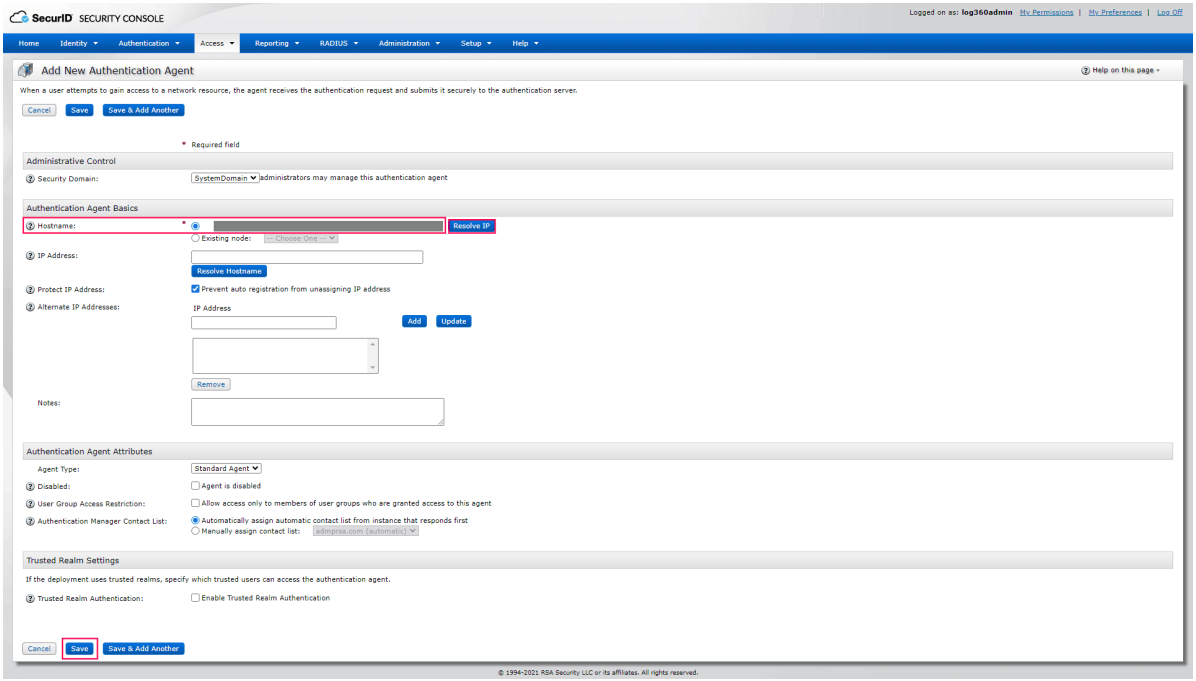


Image 7: Authentication agent in RSA SecurID console

SDK Integration (Legacy)

1. Ensure that the following JAR files are present in the <product name_install_directory>/lib folder:
   - authapi-8.6.jar
   - log4j-1.2.12rsa-1.jar
   - cryptojcommon-6.1.3.3.jar
   - JcmFIPS-6.1.3.3.jar
   - cryptojce-6.1.3.3.jar

   > **NOTE**
   >
   > These files are part of the Authentication Agent SDK for Java (v8.6). If they are missing, obtain the latest JAR files from RSA SecurID and place them in the directory.

2. In the RSA admin console, go to Access > Authentication Agents > Generate Configuration File.
3. Download AM_Config.zip and extract the sdconf.rec file.
4. In the product console, navigate to RSA SecurID.



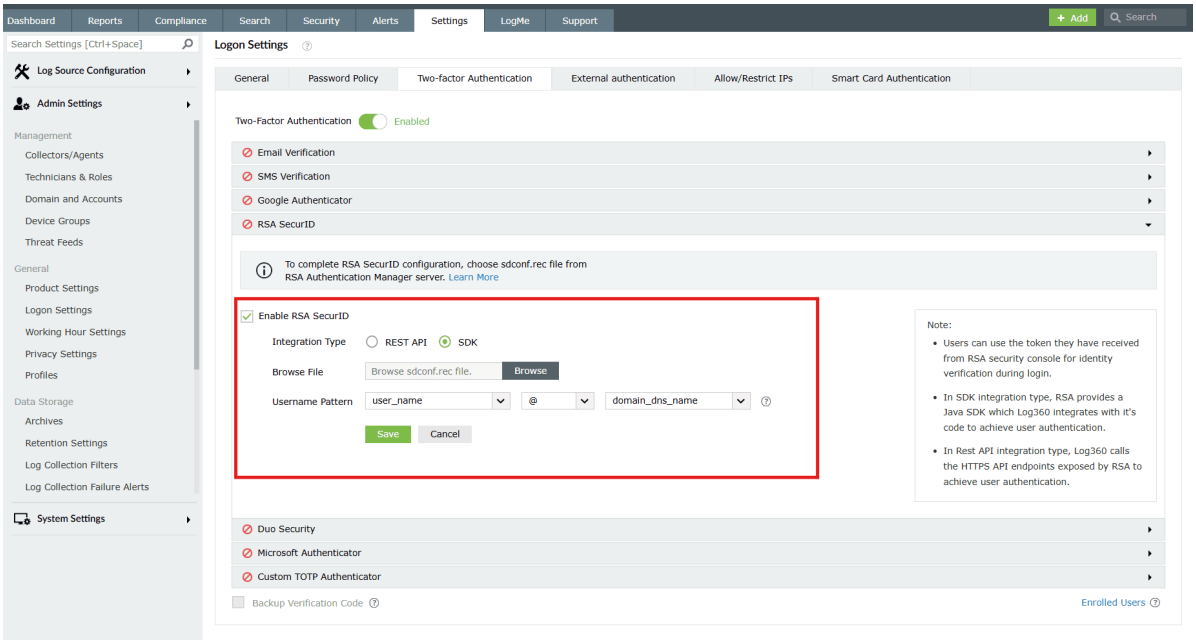
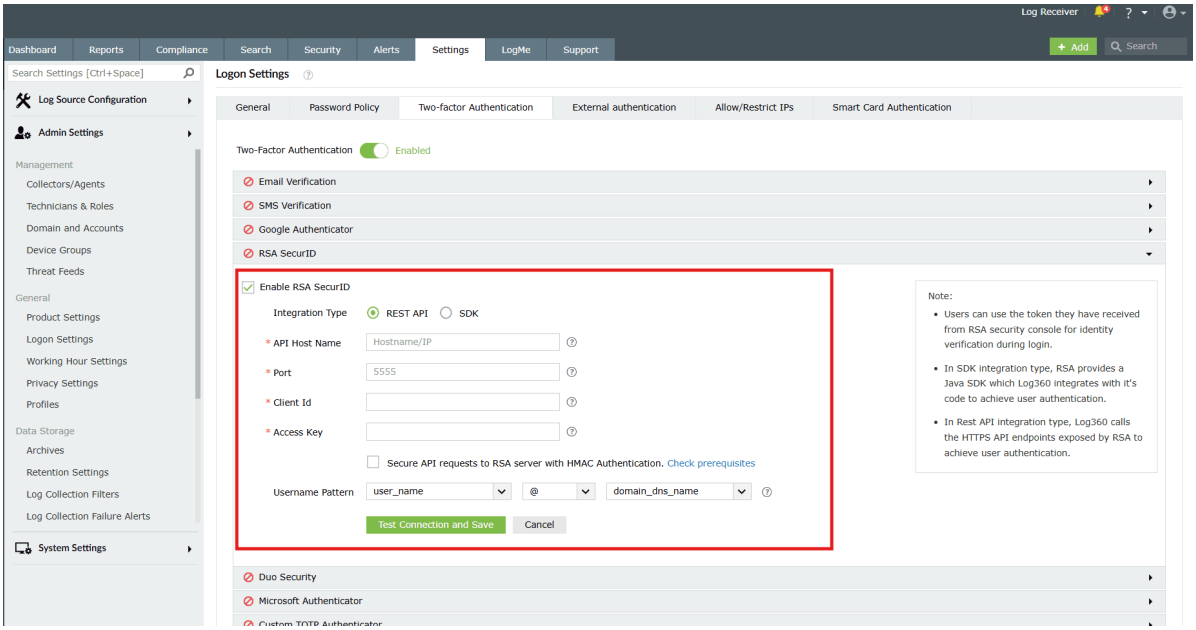


Image 8: Configuring RSA SecurID in the product console

5. Check the Enable RSA SecurID box.
6. For Integration Type, select SDK.
7. Click Browse and upload the sdconf.rec file.
8. Click Save. Once enabled, users will be prompted to authenticate with their RSA SecurID token passcodes during login.

REST API Integration (Recommended)

1. In the RSA admin console, navigate to Setup > System Settings > Authentication Settings > RSA SecurID Authentication API.
2. Copy the Access ID, Access Key, and Communication Port details.
3. In the product console, navigate to RSA SecurID.



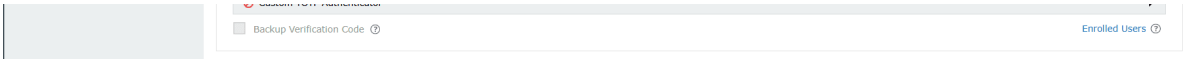


Image 9: Configuring RSA SecurID REST API in the product console

4. Check the Enable RSA SecurID box.
5. For Integration Type, select REST API.
6. Configure the following fields:
   - API Host Name: Hostname/IP of RSA Authentication Manager.
   - Port: Communication port number obtained in Step 2.
   - Client Id: Hostname of the product server (authentication agent).
   - Access Key: Key obtained in Step 2.
   - Access Id: ID obtained in Step 2.
7. (Optional) Check Secure API requests to RSA server with HMAC Authentication.

> NOTE
>
> Before enabling HMAC, ensure HMAC prerequisites are configured on the RSA server.

8. Click Test Connection and then Save.

HMAC Prerequisites

Hash-based message authentication code (HMAC) ensures the integrity of authentication requests exchanged between authentication agents and the RSA SecurID Authentication API.

1. Log on to the appliance with SSH, or access it via VMware vSphere Client / Hyper-V Manager.
2. To enable HMAC verification of requests, run:
   ./rsautil store -a update_config
   auth_manager.rest_service.authorization.mode 1 GLOBAL 501
3. To disable HMAC and use only the RSA SecurID Authentication API's access key for authentication, run:
   ./rsautil store -a update_config
   auth_manager.rest_service.authorization.mode 0 GLOBAL 501

Duo Security

If your organization uses Duo Security for two-factor authentication, it can be integrated with the product to secure logins. Users can approve or deny the product login requests using a push notification or by entering the six-digit security code generated by the Duo mobile app. Authentication via Duo Security can be configured in two ways: Web v2 SDK and Web v4 SDK.

- Web v2 SDK: Uses a traditional Duo prompt which will be displayed in an iframe in the product.
- Web v4 SDK: Uses Duo's OIDC-based universal prompt with a redesigned UI that redirects users to Duo for authentication.

NOTE

- Duo Security has phased out Web v2 SDK, so it is recommended to switch to Web v4 SDK, which features the new Universal Prompt.
- Enable HTTPS to ensure proper functioning of Web v4 SDK.

Prerequisite

Add the API hostname and admin console (e.g., https://admin-325d33c0.duosecurity.com) as a trusted site or intranet site in the users' machine if they are using older versions of Internet Explorer.

NOTE

Duo Security has phased out Web v2 SDK, so it is recommended to switch to Web v4 SDK, which features the new Universal Prompt.

Web v4 SDK configuration steps

1. Log in to your Duo Security account (e.g., https://admin-325d33c0.duosecurity.com) or sign up for a new account and log in.
2. Go to Applications and click on Protect an Application.

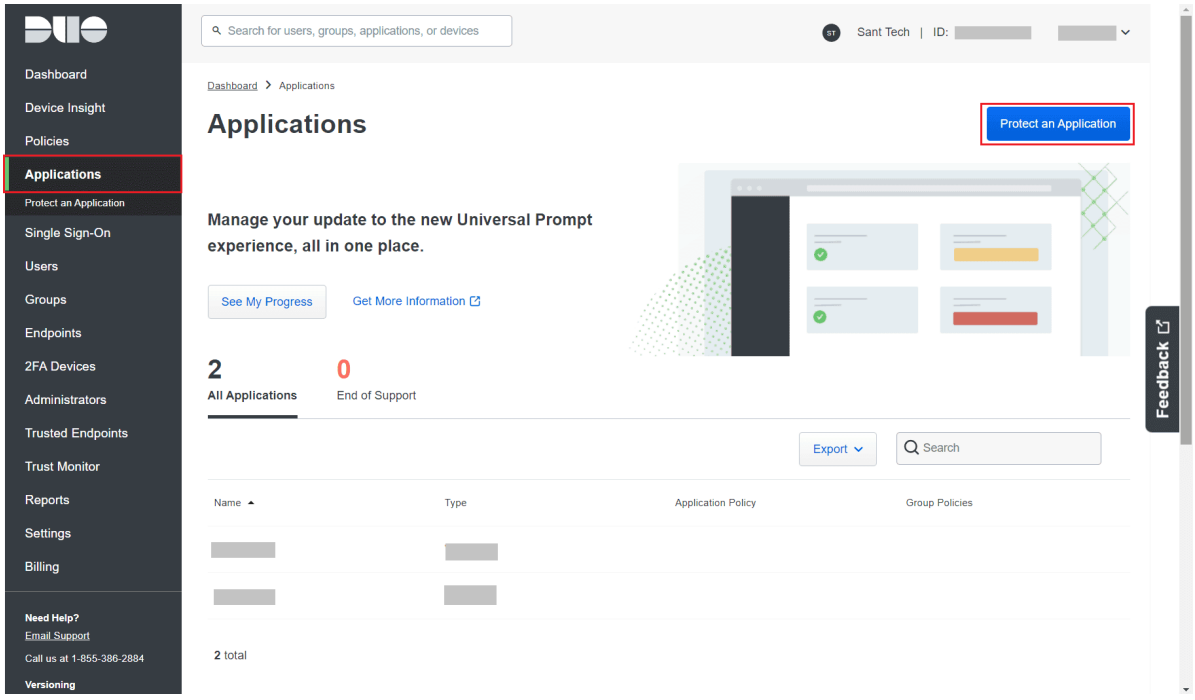


Image 10 : Protect an Application from Duo Security account

3. Search for Web SDK and click Protect.



Image 11: Web SDK from Duo Security account

4. Copy the Client ID, Client secret, and API hostname values.

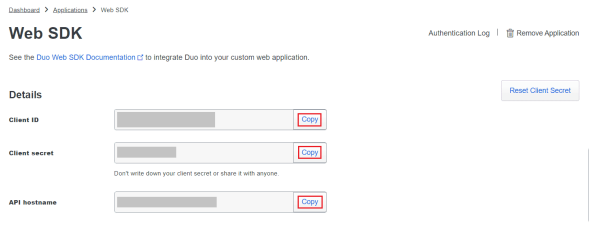


Image 12: Web Sdk configuration from Duo Security account

5. In the product console, navigate to the Duo Security module with Web v4 SDK as integration type.

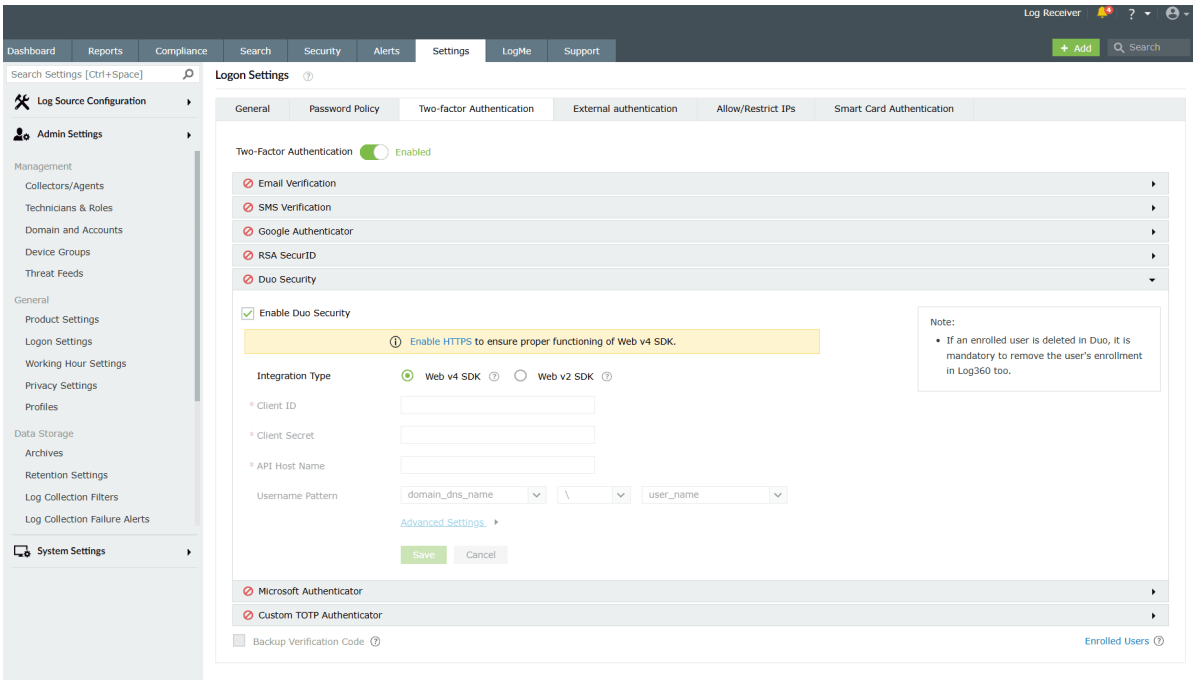
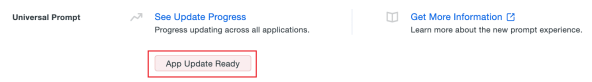


Image 13: Configuring Duo Security two-factor authentication in the product console

6. In the respective fields, paste the Client ID, Client secret, and API hostname obtained from the Duo Admin Panel.
7. Click on Save.

Migrating from Web v2 SDK to Web v4 SDK

1. In the Duo Admin Panel, select the Web SDK application, which was previously configured for the product, and copy the Integration key, Secret key and API hostname values.
2. Scroll down to the Universal Prompt section. The App Update Ready message will be displayed, indicating that Universal Prompt can now be activated for the product.



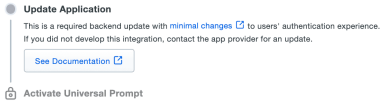


Image 14: App update ready to activate universal prompt in Duo Security console

3. In the Web v4 SDK fields in the product, paste the Integration key, Secret key, and API Host Name values in the Client ID, Client Secret, and API Host name fields respectively.
4. Once the Web v4 SDK is configured in the product and a user authenticates through the frameless Duo v4 SDK, the App Update Ready message in Duo Admin Panel will be updated and the New Prompt Ready message will be displayed.

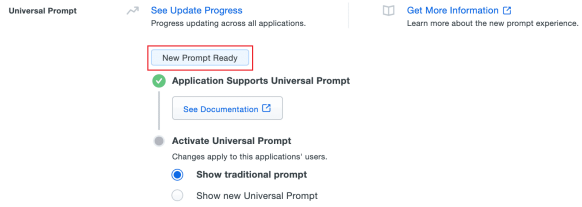


Image 15: Activating Universal Prompt for product console from Duo Security console

5. Select Show new Universal Prompt to activate the universal prompt for the product.

Microsoft Authenticator

Microsoft Authenticator is a mobile app that generates TOTP for 2FA, which not only enhances security but is also useful in forgot password scenarios. Its working is similar to that of Google Authenticator. This configuration too can be helpful in offline cases where there is no internet connection.

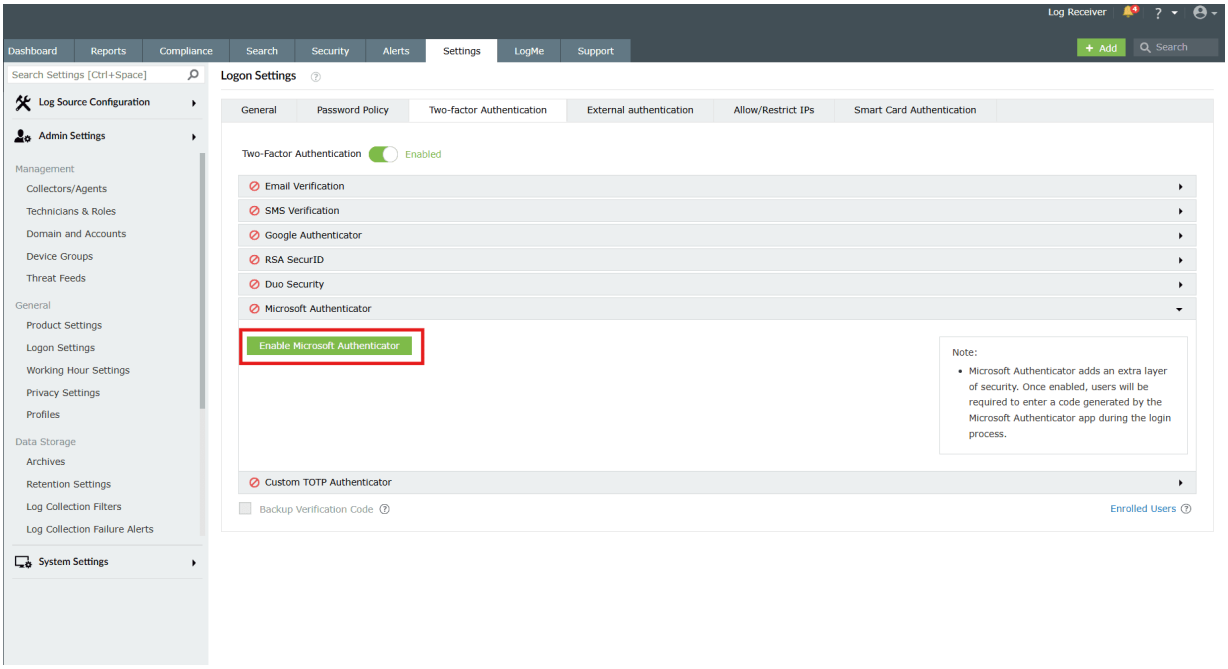
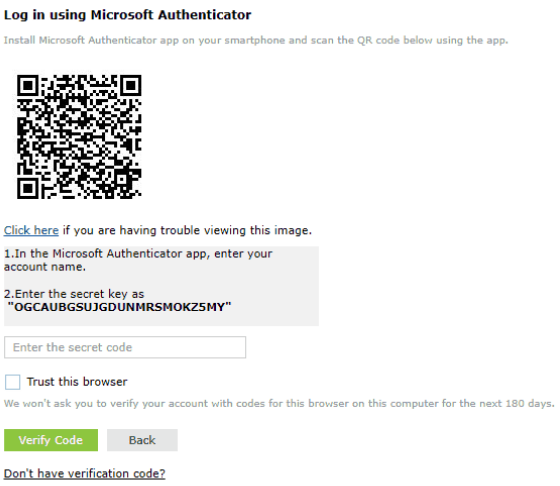


Image 16: Microsoft authenticator in two-factor authentication

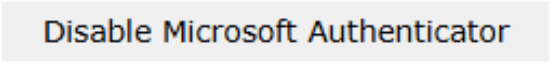
- Just click on Enable Microsoft Authenticator.
- Once enabled, users can enroll themselves for two-factor authentication using the Microsoft Authenticator app during login.
- After entering the password and logging in, the product asks to setup Microsoft Authenticator.
- A QR will be shown which can be scanned using the Microsoft Authenticator app.



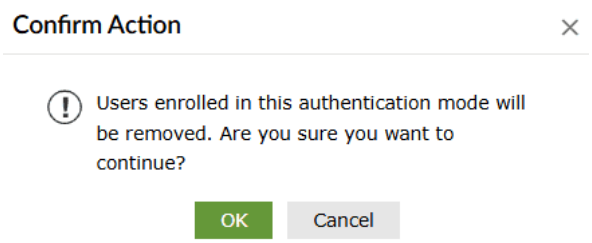
- Enter the time-based 6 digit code that's generated in the Microsoft Authenticator app to Enter the secret code box.
- Trust this browser option can be selected, and no code will be asked for 180 days.
- Click Verify Code.

To disable Microsoft Authenticator

1. Simply click on the Disable Microsoft Authenticator button available.



2. A Confirm Action pop-up box appears. Click on OK.



3. Microsoft Authenticator is now disabled, and the button shows the option to enable it now.

Custom TOTP Authenticator

In addition to the authenticators mentioned above, you can also add a custom TOTP (Time-based One-Time Password) authenticator as a means of verifying identities, provided the application satisfies the following

criteria:

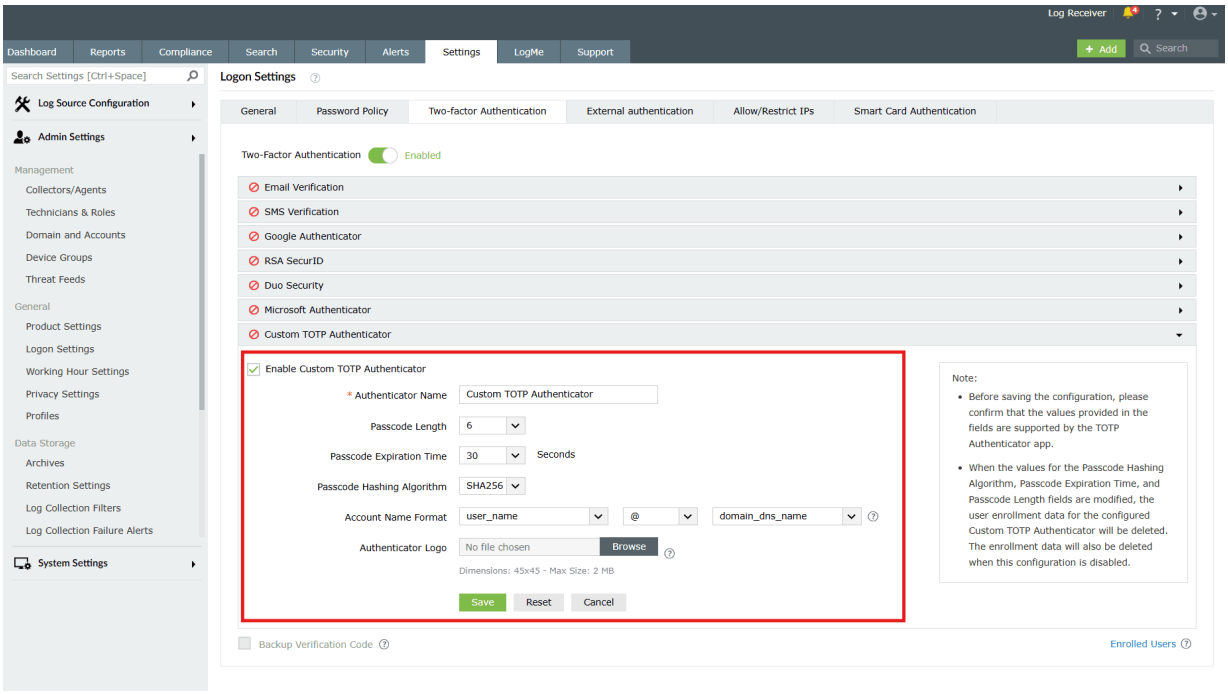


Image 17: Custom TOTP authenticator in two-factor authentication

1. Fill in the field values for the below:
   - Authenticator Name: Enter the name of the authenticator application.
   - Passcode Length: Fix a limit for passcode length. The application can provide passcodes of varying lengths- 6, 7, or 8 characters.
   - Passcode Expiration Time: Set an expiry for the passcode (in seconds.)
   - Passcode Hashing Algorithm: Choose a hashing algorithm for your passcode. The application supports any password hashing algorithm that the product utilizes- SHA1, SHA256, and SHA512.
   - Account Name Format: This format decides how the username will be displayed in the TOTP app during configuration and passcode generation. The supported formats for the image are PNG, JPG, JPEG, BMP, and GIF. Please ensure the dimensions of the logo do not exceed 45x45 pixels and the size is less than 2MB.
2. Click on the Reset button to reset and re-configure all the above fields.
3. Click on Save after entering the field values.

Backup Verification Code

Backup verification codes allow users to log in when they don't have access to their phone or face issues with one of the two-factor authentication methods. When enabled, a total of five codes will be generated. A code once used will become obsolete and cannot be used again. Users also have the option to generate new codes.

Enabling backup verification code

To enable the backup verification code, simply put a check against the Backup Verification Code box.



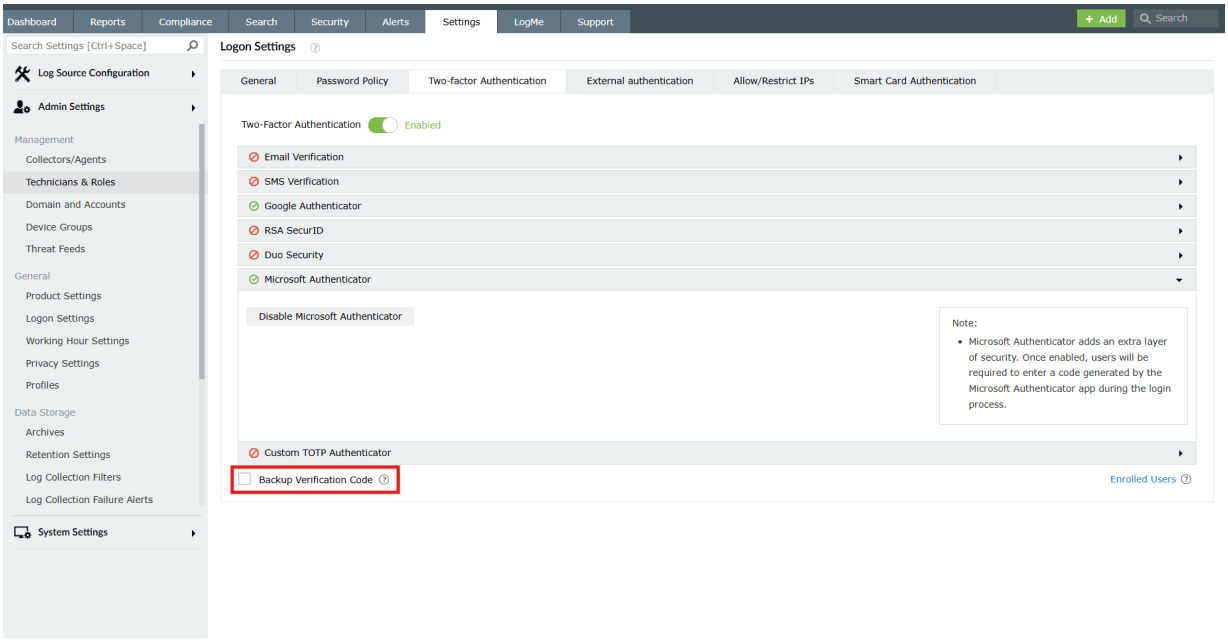
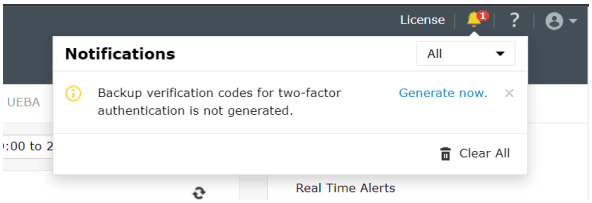


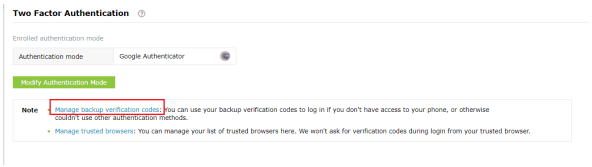
Image 18: Enabling backup verification code in two-factor authentication

What happens after enabling?

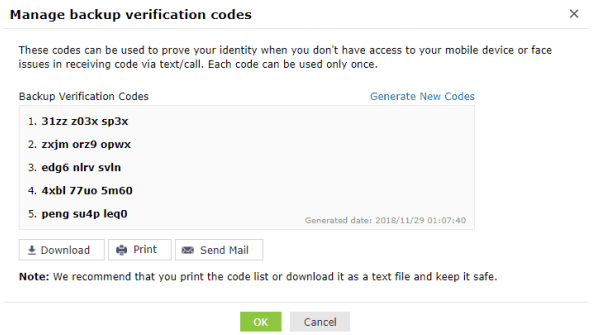
- Once enabled, users will be notified to configure their codes when they log in to the product console. On clicking Configure Now, they will be taken to the two-factor authentication settings page.



- Users need to click the Manage Backup Verification Codes link to view the codes.

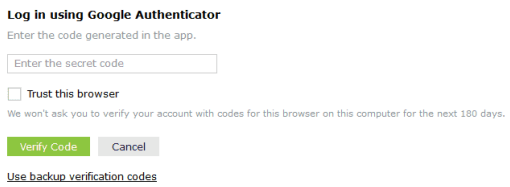


- Users can also download the codes as a text file, print them, get them delivered to their personal email address, or generate new codes.

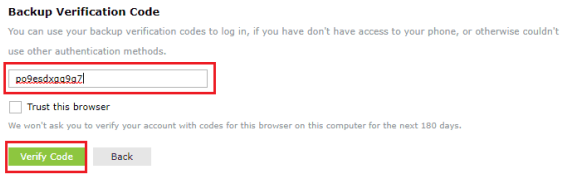


Using the backup verification code to login

- To use backup verification codes during login, users need to click the Use backup verification codes link in the second-factor authentication page.



- In the backup verification code page, they need to enter one of their backup verification codes and click Verify Code to login.



Read also

This document explained how to enable and configure different two-factor authentication methods such as email, SMS, authenticator apps, RSA SecurID, Duo Security, custom TOTP, and backup verification codes. For more understanding, refer to the below help documents:

- General logon settings
- Allow/restrict IP addresses
- Smartcard authentication

9.3.3. Single Sign-On

Last updated on: September 12, 2025

In this page

SAML Authentication

NTLM Authentication

You can set up single sign-on - through SAML or NTLM authentication.

SAML Authentication

You can set up single sign-on for technicians and admins using AD authentication to access the product through any of these popular identity providers:

- Okta
- OneLogin
- Ping Identity
- AD FS
- Custom identity provider

Configuring single sign-on using Okta

Step 1: Configure the product in Okta

1. Log in to the Okta portal as Admin.
2. Under the Application tab, click Applications and select Create App Integration.
3. Choose Sign on method as SAML 2.0 and click Next.
4. In General Settings, enter the SAML application name, say EventLog Analyzer, in the App name field. Upload a logo for the application if needed, then click Next.
5. In the Configure SAML section, enter the values for:
   - Single sign-on URL
   - Audience URI

   > **Note**
   >
   > The values for these two fields can be obtained from EventLog Analyzer→ Settings→ Admin Settings → General → Logon Settings → Single Sign-On → SAML Authentication. Copy the ACS/Recipient URL value and paste it in the single sign-on URL field. Copy the Entity ID value and paste it in the Audience URL field.

6. Select Application username that matches with userPrincipleName or samAccountName or Username of

6. Select Application username that matches with userPrincipleName or samAccountName or Username of Active Directory user.
7. If you want to encrypt SAML Assertion, Click Show Advanced Settings and Select Encrypted in Assertion Encryption. Leave other encryption options as it is.
8. Upload the Encryption Certificate, CA-signed or Self-Signed (Downloaded from Settings→Admin Settings → General → Logon Settings→ Single Sign-On → SAML Authentication → Advanced Settings → Encryption Configuration → Download Self-Signed Certificate).

   > Note
   >
   > If you want to configure multiple ACS url , add the Access urls in Other Requestable SSO URLs

   For example, if you have another access url: eventloganalyzer-server-1:8445
   Navigate to Settings → Admin Settings → General → Logon Settings → Single Sign-On → SAML Authentication
   ACS url shown in configuration page:
   https://eventloganalyzer.com:8445/samlLogin/XXXXXXXXXXXXXXXXXXXXXXXX
   you need to enter as https://eventloganalyzer-server-1:8445/samlLogin/XXXXXXXXXXXXXXXXXXXXXXXX
9. Leave the other settings as they are.
10. Click Finish.
11. Once the configuration is complete, navigate to the Sign on tab to download the Identity Provider metadata file.

Step 2: Configuring Okta in the product

1. Log in to EventLog Analyzer as an administrator.
2. Navigate to Settings→ Admin Settings → General → Logon Settings → Single Sign-On → SAML Authentication.
3. Mark the checkbox against Enable Single Sign-on with Active Directory.
4. Select Okta from the Identity Provider (IdP) drop-down.
5. For SAML Configuration Mode option, select Upload Metadata File.
6. Click Browse and upload the metadata file obtained in Step 11 (1).
7. In Advanced Settings, Select SAML response as Signed and SAML Assertion as Signed.
8. Select Signature Algorithm as SHA256.
9. In Encryption Configuration, Configure Assertion Encryption if Assertion is encrypted.
10. Click Save to complete the configuration.

Configuring single sign-on - using OneLogin

Step 1: Configure the product in OneLogin

1. Log in to the OneLogin portal.
2. Click Administration and Select Applications → Applications..
3. Click Apps tab and search for SAML Test Connector (IdP) and select it.
4. Enter the Display Name and upload the icon for the application. Click Save.
5. Under Configuration tab, enter the values for ACS (Consumer) URL Validator and ACS (Consumer) URL.

   > **Note**
   >
   > The values for these two fields can be obtained from EventLog Analyzer → Settings → Admin Settings → General → Logon Settings → Single Sign-On → SAML Authentication → Identity Provider (IdP) → OneLogin. Copy the ACS/Recipient URL value and paste it in these two fields.

   If you have multiple ACS url you may need to enter the regex for multiple ACS url in the ACS (Consumer) URL Validator . For example, if you have another access url: eventloganalyzer-server-1:8445
   ACS url shown in configuration page:
   https://eventloganalyzer.com:8445/samlLogin/XXXXXXXXXXXXXXXXXXXXXX
   you need to enter as ^(https://eventloganalyzer.com:8445)|(https://eventloganalyzer-server-1:8445)/samlLogin/XXXXXXXXXXXXXXXXXXXXXX
6. Select the SAML nameID format that matches with userPrincipleName or SamAccountName or Username of Active Directory User.
7. Click Save to complete the configuration in OneLogin.
8. Click More Actions in the top panel and click SAML Metadata to download the metadata file.

Step 2: Configure OneLogin in the product

1. Log in to EventLog Analyzer as an administrator.
2. Navigate to Settings→ Admin Settings → General → Logon Settings → Single Sign-On.
3. Mark the checkbox against Enable Single Sign-On.
4. Select OneLogin from the Identity Provider (IdP) drop-down.
5. For SAML Configuration Mode option, select Upload Metadata File.
6. Click Browse and upload the metadata file obtained in Step 8 (1).
7. Click Advanced Settings
8. Select SAML Response as Unsigned.
9. Select SAML Assertion as Signed.
10. Select Signature Algorithm which you have configured in OneLogin IDP.
11. Select Assertion Encryption unencrypted

11. Select Assertion Encryption unencrypted.
12. Click Save to complete the configuration.

Configuring single sign-on using Ping Identity

Step 1: Configure the product Ping Identity

1. Logon to the Ping Identity portal.
2. Click Applications -> My Applications -> Add Application -> Application Type->SAML Application .
3. Enter the application name, description, and logo, then click Configure.
4. To auto-populate the configuration details of EventLog Analyzer, you can upload the metadata file which can be downloaded by navigating to Settings→ Admin Settings → General → Logon Settings → Single Sign-On → SAML Authentication -> Ping Identity -> Download SP Metadata.
5. The alternative option is to enter the ACS URL and entity ID which can be obtained by navigating to Settings→ Admin Settings → General → Logon Settings → Single Sign-On → SAML Authentication -> Ping Identity -> ACS/Recipient URL.
6. Click Save.
7. Go to configuration page, if you want to configure multiple ACS url , click Add below ACS URLs and enter the Access url.
   For example, if you have another access url: eventloganalyzer-server-1:8445
   Navigate to Settings → Admin Settings → General → Logon Settings → Single Sign-On → SAML Authentication.
   ACS url shown in configuration page:
   https://eventloganalyzer.com:8445/samlLogin/XXXXXXXXXXXXXXXXXXXXXX
   you need to enter as https://eventloganalyzer-server-1:8445/samlLogin/XXXXXXXXXXXXXXXXXXXXXX
8. If you want to encrypt SAML Assertion, Check Encryption Enable.
9. Upload the Encryption Certificate, CA-signed or Self-Signed (Downloaded from Settings→Admin Settings → General → Logon Settings→ Single Sign-On → SAML Authentication → Advanced Settings → Encryption Configuration → Download Self-Signed Certificate).
10. If you want to sign SAML request , check Enable in Enforce Signed Authentication Request.
11. In Overview, Click Attributes, Select saml_subject that matches with userPrincipleName or SamAccountName or Username of Active Directory User.
12. Once the configuration is complete, the metadata file can be downloaded.

Step 2: Configure Ping Identity in the product

1. Logon to EventLog Analyzer.
2. Navigate to Settings→ Admin Settings → General → Logon Settings → Single Sign-On.
3. Select Ping Identity from the drop-down list.
4. Upload the metadata file obtained in Step 4 (1)

4. Upload the metadata file obtained in Step 4 (1).
5. Click Save to complete the configuration.

Configuring single sign-on using AD FS

To configure AD FS for identity verification, you need the following components:

1. You need to install the AD FS server. The detailed steps for installing and configuring AD FS can be found in this Microsoft article.
2. An SSL certificate to sign your AD FS login page and the fingerprint for that certificate.

AD FS Configuration steps:

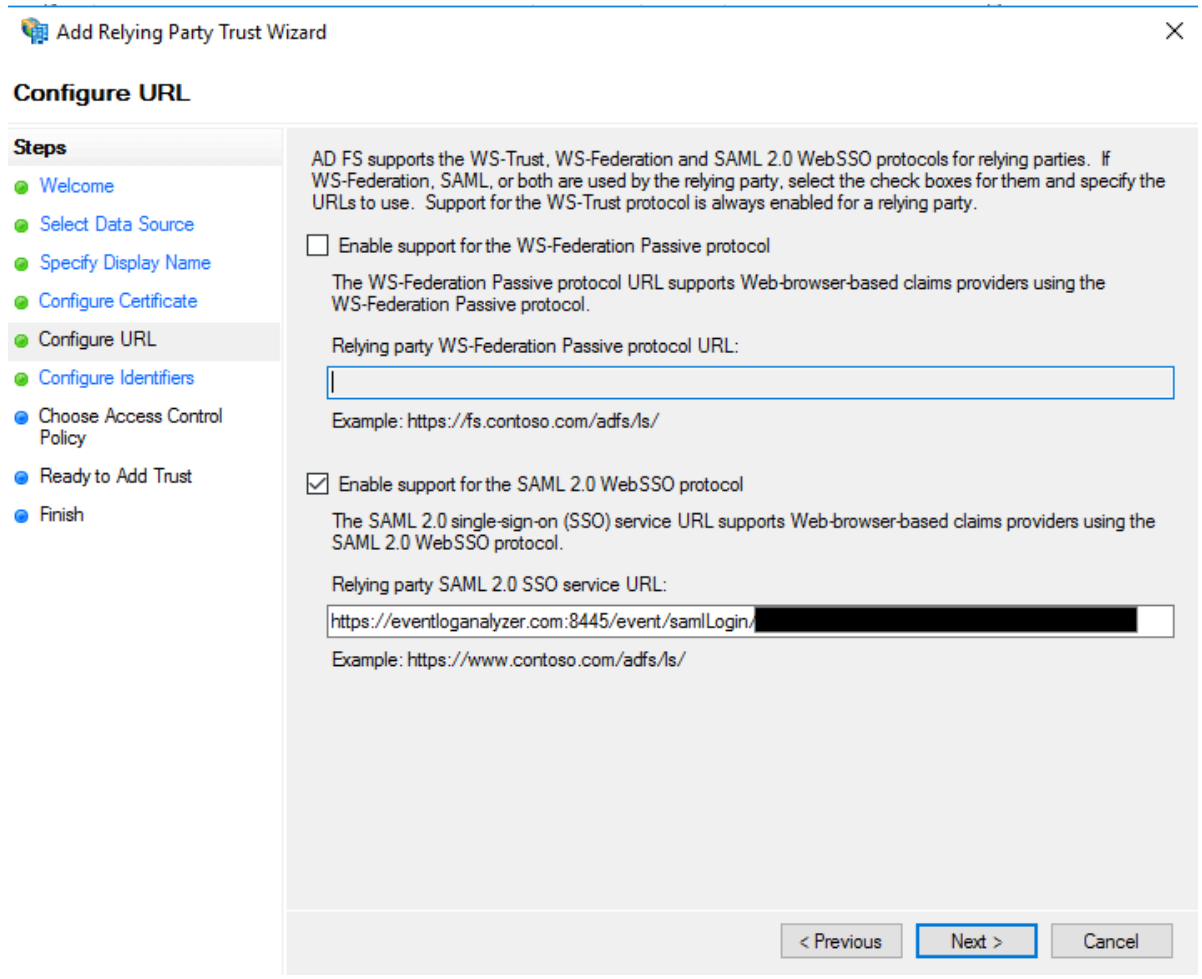
Relying Party Trust and Claim Rules

During configuration, you will need to add a Relying Party Trust and create claim rules. A claim is an attribute that is used for identifying an entity to establish access. For example, the Active Directory UserPrincipalName.A Relying Party Trust is created to establish the connection between two applications for authentication purposes by verifying claims. In this case, AD FS will trust the relying party (EventLog Analyzer) and authenticate users based on the claims generated. Claims are generated from claim rules by applying certain conditions on them.

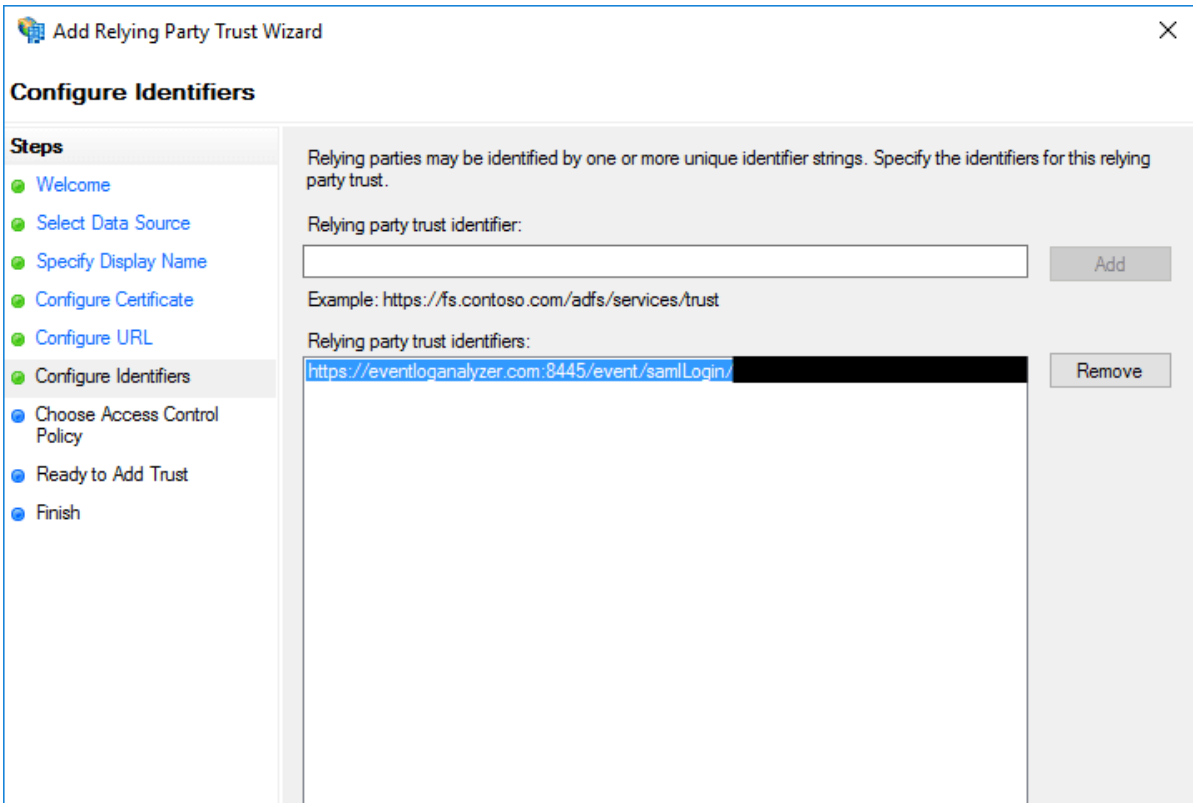
Step 1: Adding a Relying Party Trust

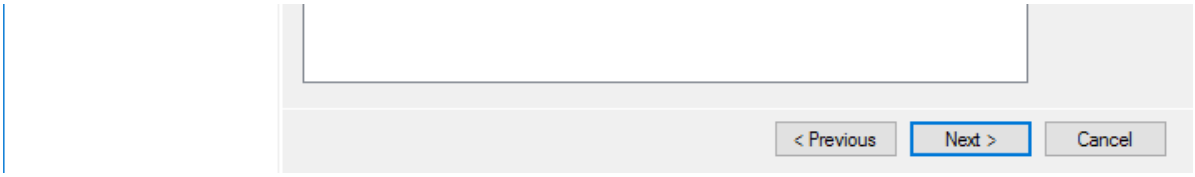
1. The connection between AD FS and EventLog Analyzer is created using a Relying Party Trust (RPT). Select the Relying Party Trusts folder from AD FS.
2. From the Actions sidebar, select Add Relying Party Trust. The Add Relying Party Trust Wizard opens.
3. Click Start.
4. In the Select Data Source page, click on the Enter Data About the Party Manually option and click Next.
5. In the Specify Display Name page, enter a display name of your choice and also add additional notes if required. Click Next.
6. On the Configure Certificate screen, If you want to encrypt SAML Assertion, Upload the Encryption Certificate, CA-signed or Self-Signed (Downloaded from Settings → Admin Settings → General → Logon Settings → Single Sign-On → SAML Authentication → Advanced Settings → Encryption Configuration → Download Self-Signed Certificate).
7. On the Configure URL screen, check the box labeled Enable Support for the SAML 2.0 WebSSO protocol. The Relying party SAML 2.0 SSO service URL will be the ACS URL of your EventLog Analyzer server. Note that there is no trailing slash at the end of the URL. For example: https://eventloganalyzer.com/samlLogin/XXXXXXXXXXXXXXXXXXXXXXXX

> Note
>
> - ACS URL/Recipient URL: Log into EventLog Analyzer web console with admin credentials.
> - Navigate to Settings → Admin Settings → General → Logon Settings → Single Sign-On → SAML authentication → ACS URL/Recipient URL. Copy the ACS URL/Recipient URL.



8. In the next page, for the Relying party trust identifiers option, add the Issuer URL/Entity ID.



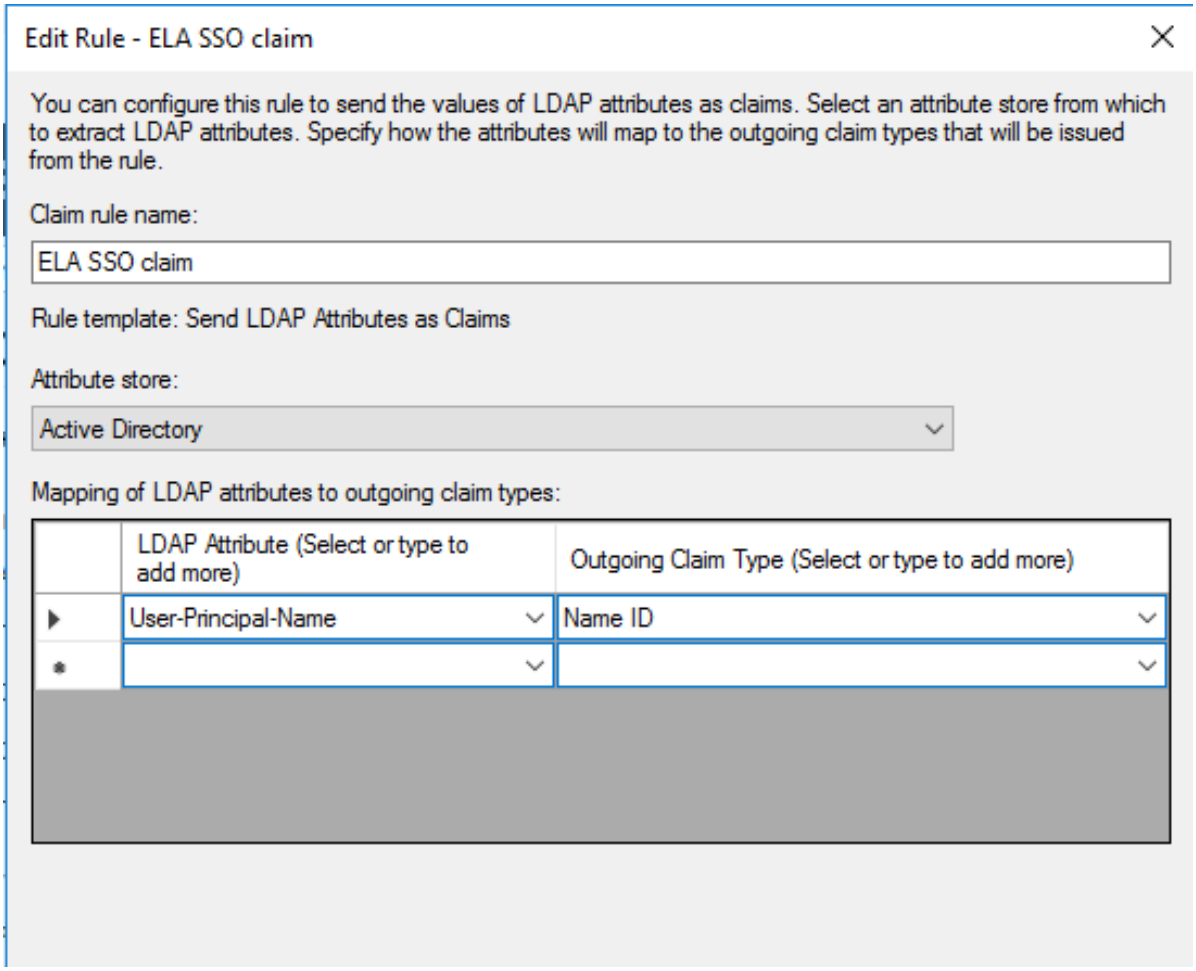


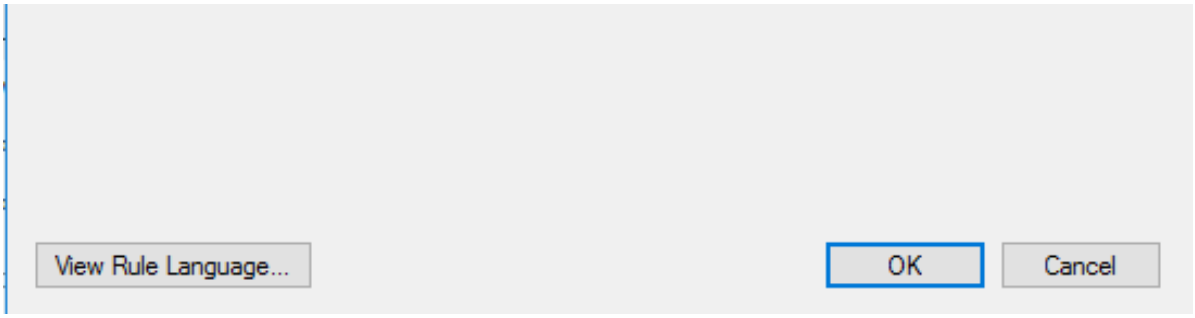
9. In the Choose Issuance Authorization Rules page, you can choose to either Permit all users to access this relying party or Deny users to access this relying party. Click Next.
10. The next two pages will display an overview of the settings you have configured. In the Finish page, click Close to exit the wizard. If you choose the option Configure claims issuance policy for this application when the wizard closes, the Claim Rules Editor will open automatically.

Step 2: Creating a Claim Rule

Once you have configured the Relying Party Trust, you can create the claim rules using the Claim Rules Editor, which opens by default when you finish creating the trust.

1. To create a new rule, click on Add Rule.
2. From the list of claim rule templates available, select Send LDAP Attributes as Claims. Click Next.
3. In the next page, provide a Claim rule name and select Active Directory as the attribute store.
4. From the LDAP Attribute column, select the Attribute that matches with User Principle Name or SamAccountName or Username of Active Directory User.
5. Select Name ID in Outgoing Claim Type.

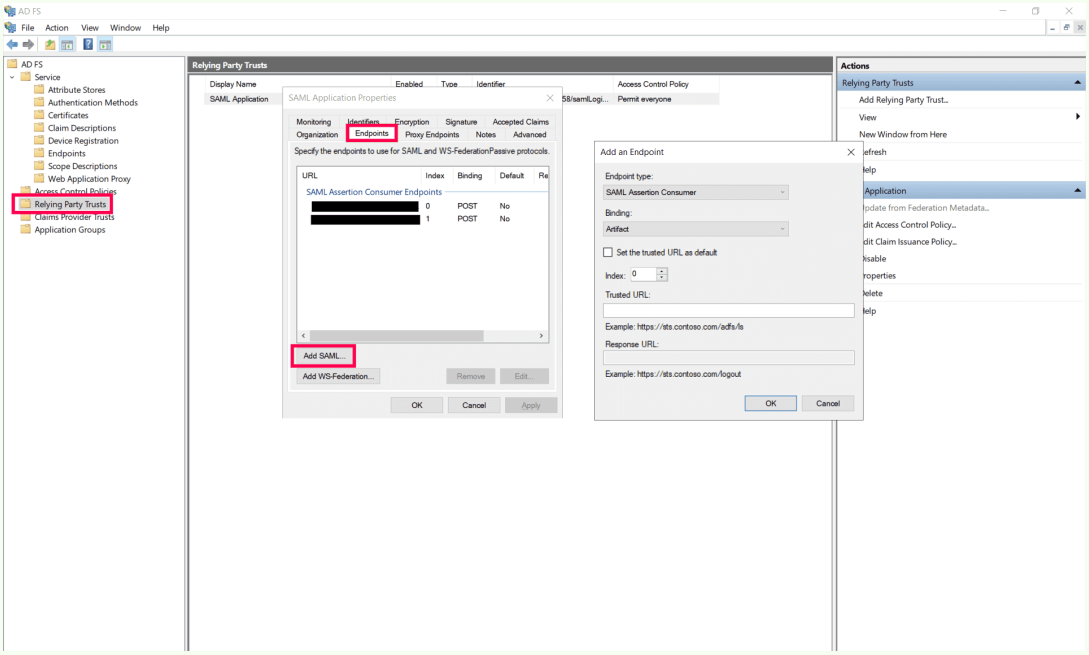




6. After completing the AD FS configuration, download the metadata file by clicking on the Identity Provider metadata link. For example: https://adfsserver.domain.com/FederationMetadata/2007-06/FederationMetadata.xml. You will need this file while configuring SAML authentication in EventLog Analyzer. So, save this file and keep it safe.

Note

If you want to configure multiple ACS url, navigate to the Relying Party Trusts and find the rule you've created. Right-click on the rule and click Properties.
In the window which opens, find the Endpoints tab and click the Add SAML button.
Select Binding as POST.
In the Trusted URL box, paste the Access url
For example, if you have another access url: eventloganalyzer-server-1:8445
Navigate to Settings → Admin Settings → General → Logon Settings → Single Sign-On → SAML Authentication.
ACS url shown in configuration page: https://eventloganalyzer.com:8445/samlLogin/XXXXXXXXXXXXXXXXXXXXXXXX
You need to enter as https://eventloganalyzer-server-1:8445/samlLogin/XXXXXXXXXXXXXXXXXXXXXXXX



For Windows Server 2016:

1. Open PowerShell with administrative properties in your ADFS server.
2. Run the following command to enable IdP-initiated SSO:
   Set-ADFSProperties -EnableIdPInitiatedSignonPage $true
3. Run the following code to enable RelayState:
   Set-ADFSProperties -EnableRelayStateForIDPInitiatedSignon $true
4. Restart the ADFS server.

Step 3: Configuring AD FS in the product

1. Log in to EventLog Analyzer as an Administrator.
2. Navigate to Settings→ Admin Settings → General → Logon Settings → Single Sign-On.
3. Mark the checkbox against Enable Single Sign-On.
4. Select the SAML Authentication radio button.
5. Select AD FS from the Identity Provider (IdP) drop-down.
6. Click Browse and upload the metadata file you downloaded from Step 6 (2).
7. In Advanced Settings, Select SAML response as Unsigned and SAML Assertion as Signed.
8. Select Signature Algorithm as SHA256.
9. In Encryption Configuration, Configure Assertion Encryption if Assertion is encrypted.
10. Click Save.

Accessing the product through AD FS

1. To access EventLog Analyzer, use the URL provided below:
   https://adfsserver.domain.com/idpinitiatedsignon.aspx
2. ADFSserver is the server in which the ADFS is deployed.
3. Select EventLog Analyzer app name from the list of applications.

Configuring single sign-on using custom identity provider

You can configure any custom identity provider of your choice to enable single sign-on to access EventLog Analyzer. Follow the steps outlined in the previous sections for supported identity providers to set up EventLog Analyzer within your chosen identity provider.

Configure custom identity provider in the product

1. Log in to EventLog Analyzer as an Administrator.
2. Navigate to Admin ->Administration -> Logon Settings -> Single Sign-On.
3. Mark the checkbox against Enable Single Sign-On.
4. Select the SAML Authentication radio button.

5. Select Custom Identity Provider from the drop down list.
6. Upload the metadata file of the custom identity provider.
7. Click Save to complete the configuration.

NTML Authentication

To enable NTLM-based single sign-on, follow the steps listed below:

To enable single sign-on for multiple components and domains, follow the steps listed below:

1. Navigate to Settings → Admin Settings → General → Logon Settings → SSO Settings.
2. Mark the check-box Enable Single-Sign On with Active Directory.

> **Note**
>
> To enable NTLMv2 SSO for ManageEngine EventlogAnalyzer, you will have to download the Jespa JAR file and add it to the product's lib folder. For more information, click here. If you have already enabled NTLMv2 SSO, you can continue using the feature and no further actions are needed.

3. Select the components that you wish to enable single sign-on from the Select Components drop-down box.

> **Note**
>
> The component will only be displayed if the component supports single sign-on.

4. Select the domains that you wish to enable single-sign on from the Select Domains drop-down box.
5. Click Save Settings.

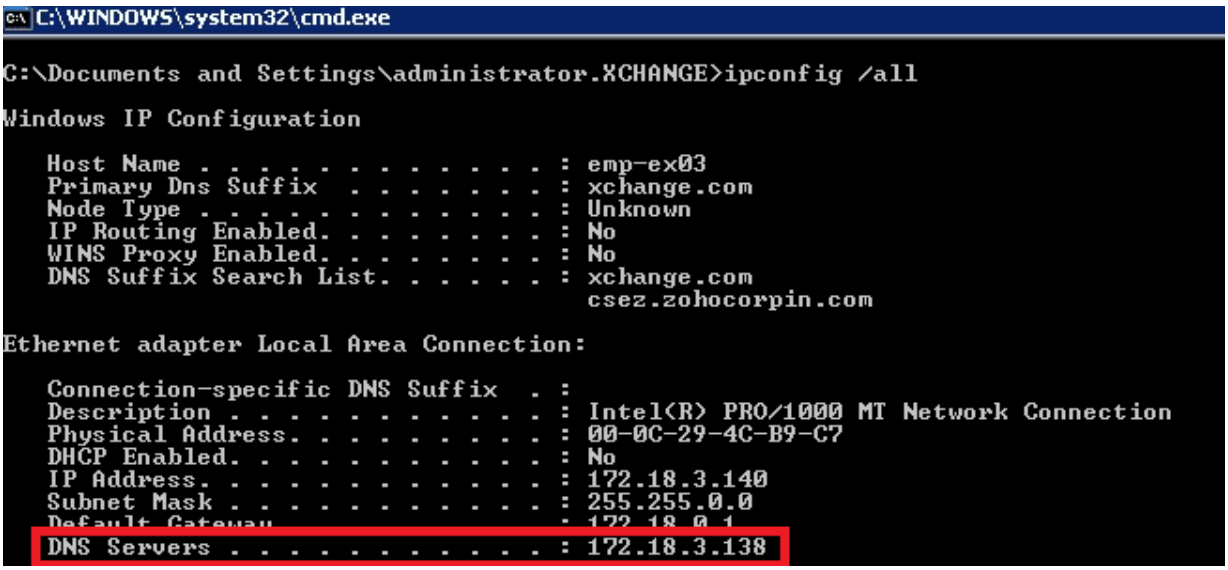
> **Note**
>
> If the product is installed as a service, configure the service account with administrator privileges by following the steps listed below.
>
> - Click Start → run → services.msc.
> - Locate the service name Manageengine EventLogAnalyzer.
> - Right click the service and select Properties → Log On.
> - Select This account and provide the credentials.

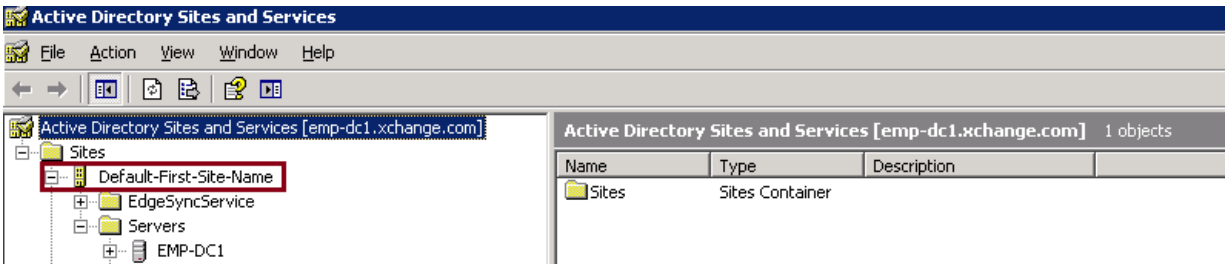
To modify existing single sign-on settings,

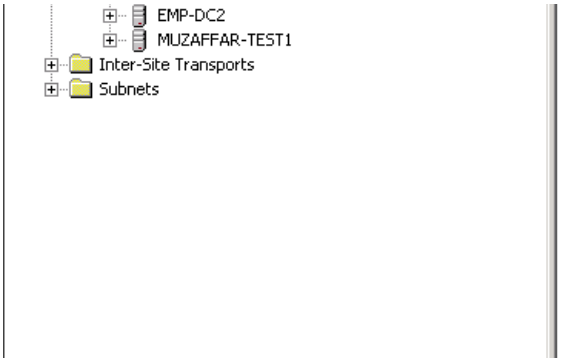
1. Navigate to Settings → Admin Settings → General → Logon Settings → SSO Settings.

2. Click the icon in the status column against the domain that you wish to modify the settings for.
3. Enter the Computer Name and Password in the respective fields. Click on the Create this computer account in the domain check-box to create a computer with the entered credentials if it is not already present in the domain.
4. Click Advanced. If the DNS Servers and DNS Site are not filled automatically after entering the computer name and password, enter them manually.
5. Click Save.

> **Note**
>
> To identify the DNS Server IP address:
> Open Command Prompt from a machine belonging to the domain that you have selected
> Type ipconfig /all and press enter
> Use the first IP address displayed under DNS Server
> To identify the DNS Site:
> Open Active Directory Sites and Services
> Expand the Sites and identify the Site in which the Domain Controller configured under the selected domain appears
> Use the Site name for DNS Site
> See the images below for reference.







Troubleshooting steps for SSO - NTLM Authentication:

Please ensure that you have performed the following actions before troubleshooting.

1. Added the site to a trusted site.
2. Added the technician's details in EventLog Analyzer's "Technicians and Roles" for whom SSO is enabled.
3. Not accessing EventLog Analyzer Web Client in Workgroup Machine.
4. Accessing EventLog Analyzer Web Client on the machine that belongs to the domain in which you've configured SSO.
5. Not accessing EventLog Analyzer Web Client in Private or Incognito Window.

I. Change browser settings to allow Single Sign-On

Trusted sites are the sites with which NTLM authentication can occur seamlessly. If SSO has failed, then the most probable cause is that the EventLog Analyzer URL isn't a part of your browser's trusted sites. Kindly add the EventLog Analyzer URL in the trusted sites list. Follow the steps given below:

- Microsoft Edge (link to the steps below)
- Chrome (link to the steps below)
- Firefox (link to the steps below)

> Note
>
> It is recommended that you close all browser sessions after adding the URL to the trusted sites list for the changes to take effect.

> Note
>
> Google Chrome and Microsoft Edge use the same internet settings. Changing the settings either in Microsoft Edge or in Chrome will enable NTLM SSO in both browsers. It is again recommended to close both the browser sessions for the changes to be enabled.

Microsoft Edge

- Open Control Panel → click the Internet Options button.
- In the Internet Options dialog box that opens, click the Security tab, and then click a security zone (Local intranet, Trusted sites, or Restricted sites).
- Click Sites.
- Click on the advanced button and add the EventLog Analyzer site to the list of intranet site.
- Click Close, and then click OK.
- Close all browser sessions and reopen your browser.

Chrome

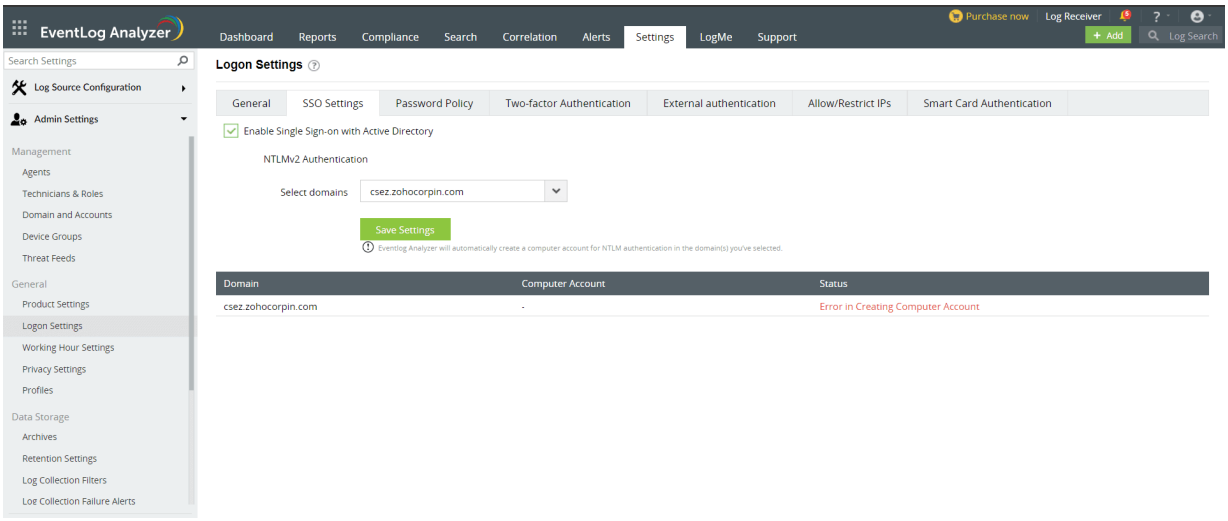
- Open Control Panel → click the Internet Options button.
- In the Internet Options dialog box that opens, click the Security tab, and then click a security zone (Local intranet, Trusted sites, or Restricted sites).
- Click Sites.
- Click on the advanced button and add the EventLog Analyzer site to the list of intranet sites.
- Click Close, and then click OK.
- Close all browser sessions and reopen your browser.

Firefox

- Open Firefox web browser and type about:config in the address bar.
- Click I'll be careful, I promise in the warning window.
- In the Search field, type: network.automatic-ntlm-auth.trusted-uris.
- Double-click the "network.automatic-ntlm-auth.trusted-uris" preference and type the URL of EventLog Analyzer in the prompt box. If there are sites already listed, type a comma and then the URL of EventLog Analyzer. Click OK to save the changes.
- Close all browser sessions and reopen your browser.

II. Check the computer account configuration

Status: Error in Creating Computer Account



This error can be due to any of the reasons listed below:

Invalid domain credentials in EventLog Analyzer

This could happen when the credentials of the user account specified in the domain settings section of EventLog Analyzer are expired. To update the credentials and synchronize it with EventLog Analyzer, follow these steps:

1. Log into EventLog Analyzer web-console with admin credentials.
2. Click on Settings → Admin Settings → Management → Domain and Accounts and update the domain credentials (i.e., username and password).
3. Synchronize the updated domain credentials with EventLog Analyzer by navigating to EventLog Analyzer → Admin tab and clicking on the Sync now button.

Domain controllers are not accessible from EventLog Analyzer

When EventLog Analyzer cannot reach the specified domain controllers (DCs), you must add another DC that it can access. To do this:

1. Log into EventLog Analyzer web-console with admin credentials.
2. Click Settings → Admin Settings → Management → Domain and Accounts and specify the name of the relevant DC, and also the credentials of the account that EventLog Analyzer should use.
3. Synchronize the updated domain controller with EventLog Analyzer by navigating to Settings → Admin Settings → Management → Domain and Accounts tab and clicking on the Sync now button.

Non-conformance to password policy

This error occurs when the password of the automatically created computer accounts for NTLM authentication does not meet the domain password policy settings. To resolve this issue, you need to create a computer account manually with a password in accordance with the domain policy settings. To accomplish this, follow the steps given below:

- Click the error message: 'Error in creating a new computer account', in the status column against the domain in which you wish to create a computer account.
- Create a computer account manually by entering Computer Name and Password.

9.3.4. Smartcard authentication

Last updated on: September 12, 2025

In this page

Overview

Smartcard Authentication

Add a new smartcard

Edit a configured smartcard

Enable/Disable a smartcard

Delete a configured smartcard

Overview

Smart card authentication adds an extra layer of login security by requiring both the card and its PIN. Certificates are mapped to LDAP attributes for seamless user verification across domains. This section covers prerequisites, configuration, and management actions.

Smartcard Authentication

If you have a smart card authentication system enabled in your environment, you can configure the product to authenticate users through it, bypassing other first factor authentication methods.
What is smartcard authentication?

- This feature provides an additional authentication option by enabling the use of smart cards/PKI/certificates to grant access to the tool.
- It strengthens the security further because getting access to the product shall then require the user to possess the smart card and know the personal identification number (PIN) as well.

How does this authentication work?

- When a user attempts to access the product's web-interface, they would be allowed to proceed further only after completing smart card authentication in the machine, i.e., by presenting the smart card and subsequently entering the PIN.
- The web-interface supplements smart card technology with SSL communication. So, the user is prompted to specify the X.509 certificate for getting access.
- Users can choose to provide the certificate from the smart card or the local certificate store, in which case the product performs the steps to authenticate the user with the certificate.
- The users can also choose to decline providing the certificate, and the tool takes them to the usual login page for authentication.

Steps to configure smartcard authentication settings:
In the product, navigate to the Smart Card Authentication sub-tab as shown in the below image.

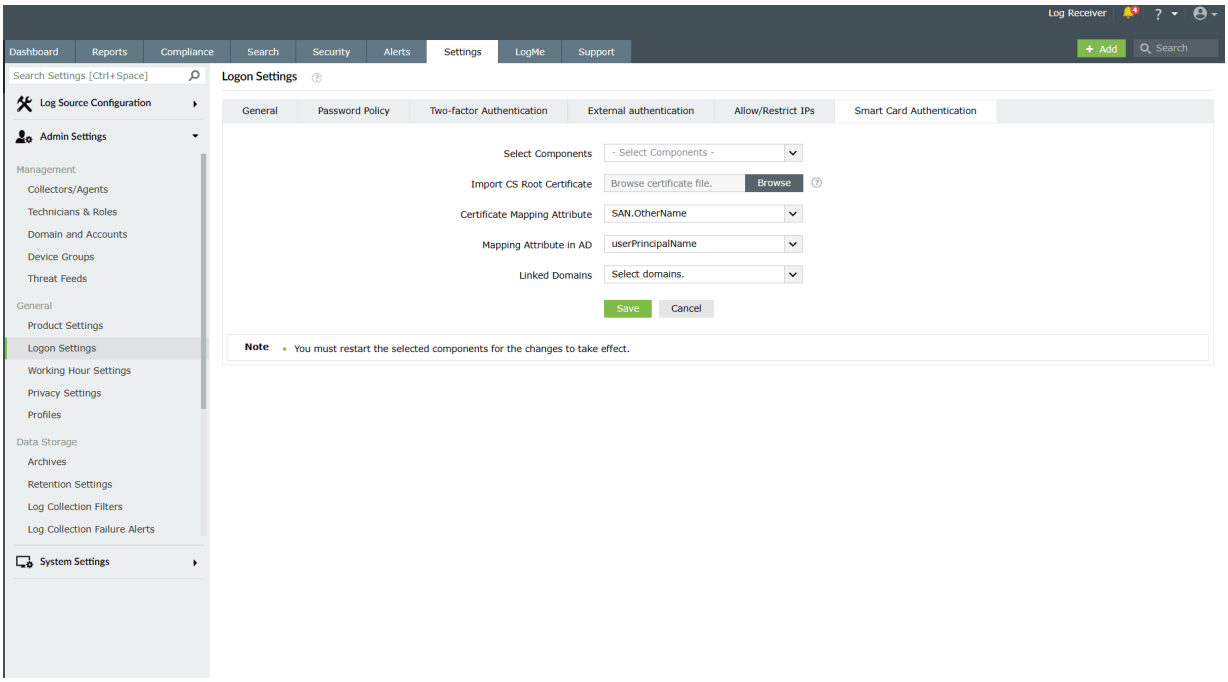


Image 1: Smart card authentication in logon settings

Configuring smartcard authentication

Phase 1: Enable SSL Port

SSL (Secure Sockets Layer) port must be enabled for configuring smart card authentication settings. To configure the SSL connection settings read Connection Settings.

Phase 2: Access smartcard authentication settings

- Navigate to the Smart Card Authentication module in the product console.
- Click on the + Add a New Smartcard button located at the top-right corner of the screen.

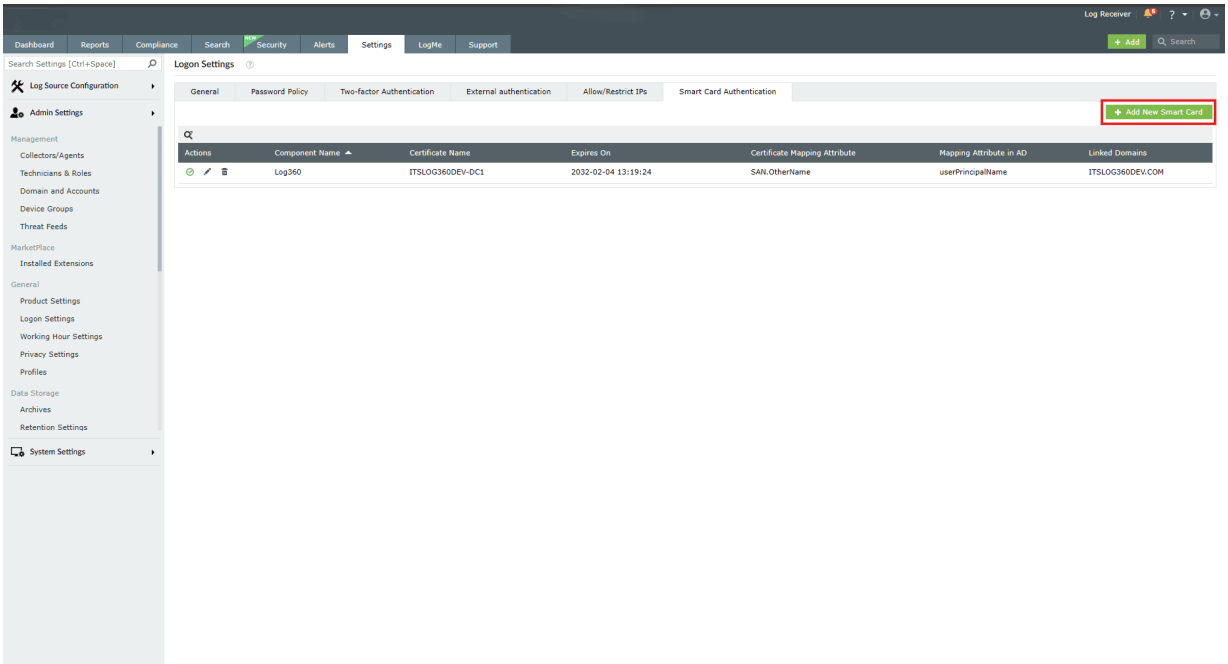


Image 2: Adding new smart card authentication in logon settings

> NOTE
>
> The option to add/manage Smartcard(s) will be available only when it is successfully configured first.

Phase 3: Import the CA Root Certificate

- To verify smart card certificates, the product must trust the issuing Certificate Authority (CA).
- In the Import CA Root Certification field, click on Browse and select the CA root certificate file from your computer.
- You can download the CA root certificate from your CA server from:http://CertificateAuthorityServerName/certsrv/

Phase 4: Configure mapping attributes

Mapping attribute in certificate

- In the Certificate Mapping Attribute field, specify the certificate attribute for mapping.
- The user details need to be mapped between the smart card certificate and the product's database. This denotes that the attribute in the smart card certificate that uniquely identifies the user should match with the corresponding value in the product's user database.
- This mapping involves specifying which attribute in the certificate should be taken up for comparison with which attribute in the product's user store. There is a provision for the flexibility to specify any attribute of the smart card certificate that you feel uniquely identifies the user in your environment.
- You may choose any attribute among SAN.OtherName, SAN.RFC822Name, SAN.DirName, SAN.DNSName, SAN.URI, email, distinguishedName and CommonName.
- In case any other attribute is used to identify the user in your environment uniquely, contact support to add that attribute.

Mapping attribute in AD

- In the Mapping Attribute in AD field, specify the LDAP (Lightweight Directory Access Protocol) attribute that should be matched with the specified certificate attribute. Here you need to specify the particular LDAP attribute that uniquely identifies the user in the product's user store, example: sAMAccountName.
- The available attributes are cn, displayName, distinguishedName, employeeID, employeeNumber, givenName, mail, mobile, name, objectGUID, objectSID, sAMAccountName and userPrincipalName.
- During authentication, the product reads the value corresponding to the certificate attribute that you specified in Certificate Mapping Attribute and compares it with the specified LDAP attribute in Mapping Attribute in AD.

Phase 5: Link domains

- In the Linked Domains field, select the appropriate domains from the drop-down menu.

Phase 6: Save settings

- After all configurations are made, click on Save.
- Once saved, smart card authentication will be enabled for the selected domains and user mappings.
- After you have added a smartcard for authentication, you can perform any of the following functions:
  - Add a new smartcard
  - Edit a configured smartcard
  - Enable/Disable a smartcard
  - Delete a configured smartcard

Add a new smartcard

1. In the product console, navigate to the Settings tab and click on Logon Settings listed under Admin Settings.

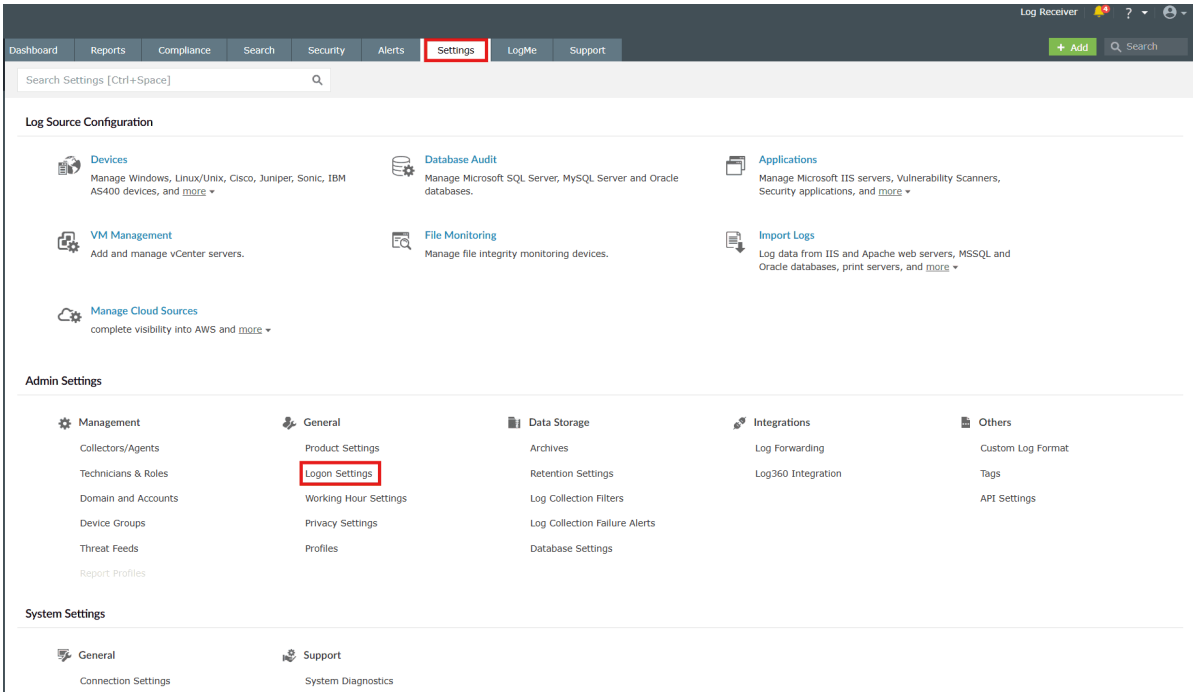
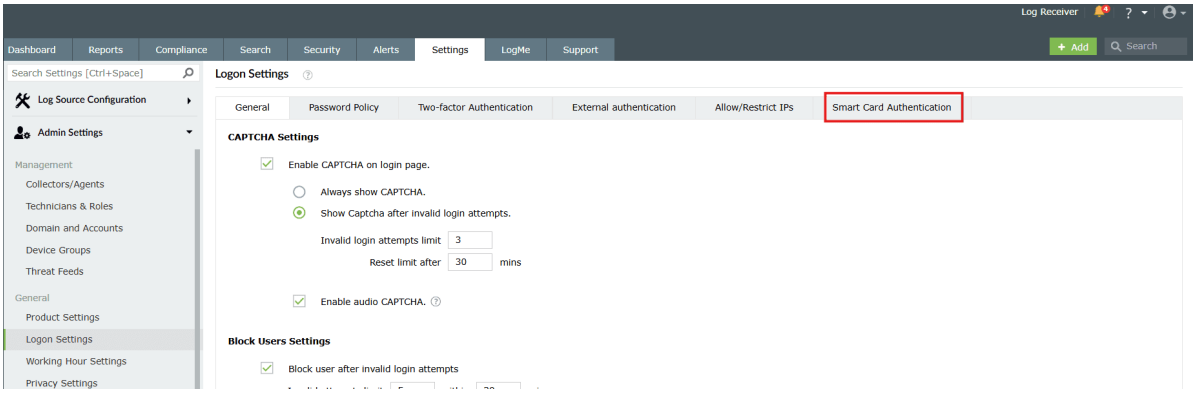


Image 3: Logon settings via settings tab

2. Select the Smart Card Authentication sub-tab.



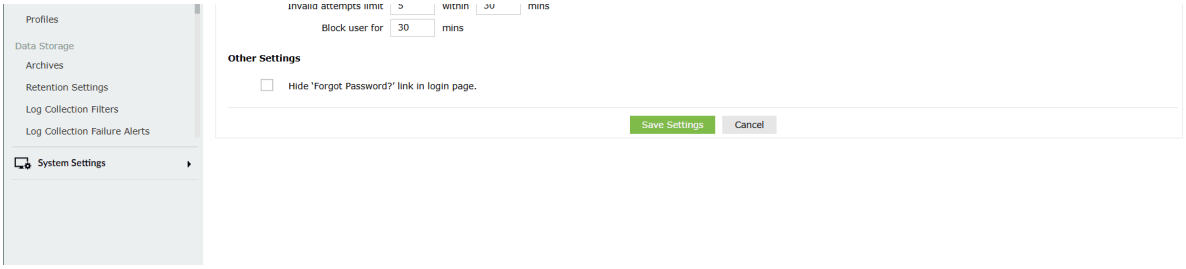


Image 4: Smart card authentication logon settings

3. Click on the Add a New Smart Card button at the top-right corner of the page.

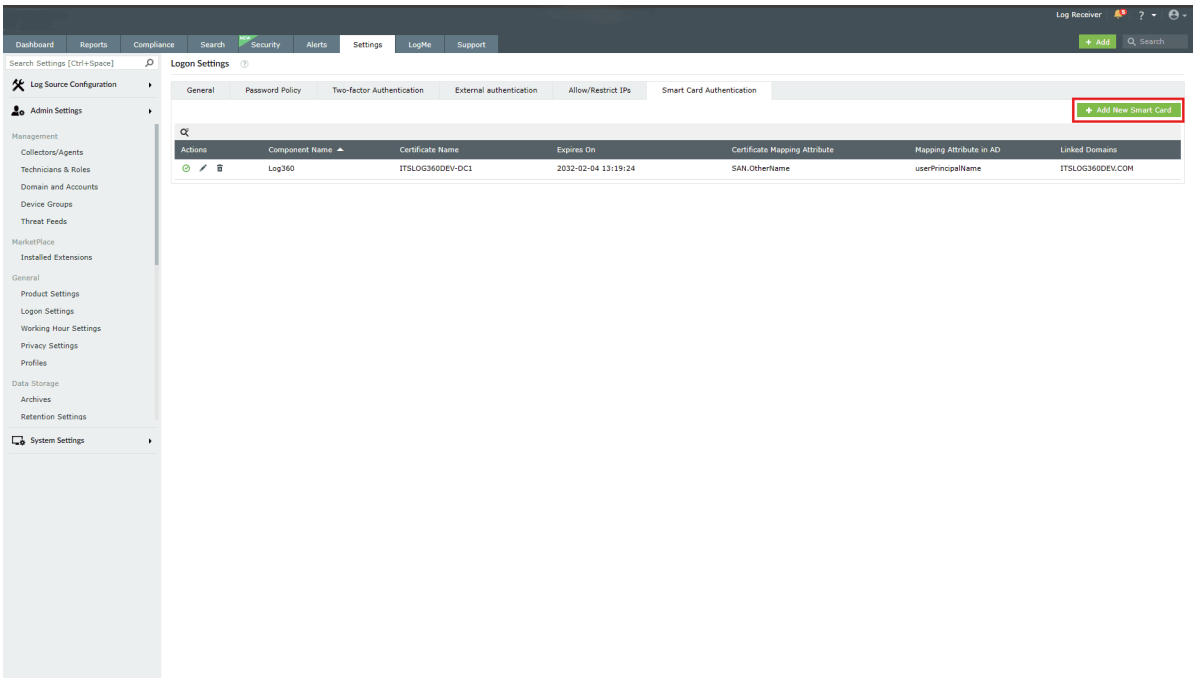


Image 5: Adding new smart card in logon settings

4. Enter the required details and click Save.

Edit a configured smartcard

1. In the Smart Card Authentication sub-tab, locate the smart card you want to edit.
2. Click the edit icon in the corresponding row.

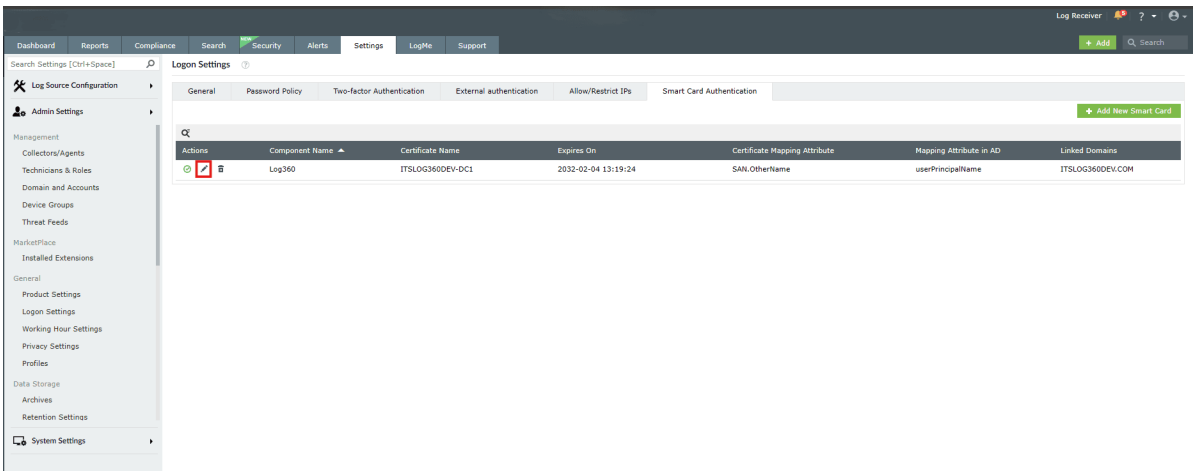


Image 6: Editing smart card in logon settings

3. Modify the required settings.
4. Click Save.

Enable/Disable a smartcard

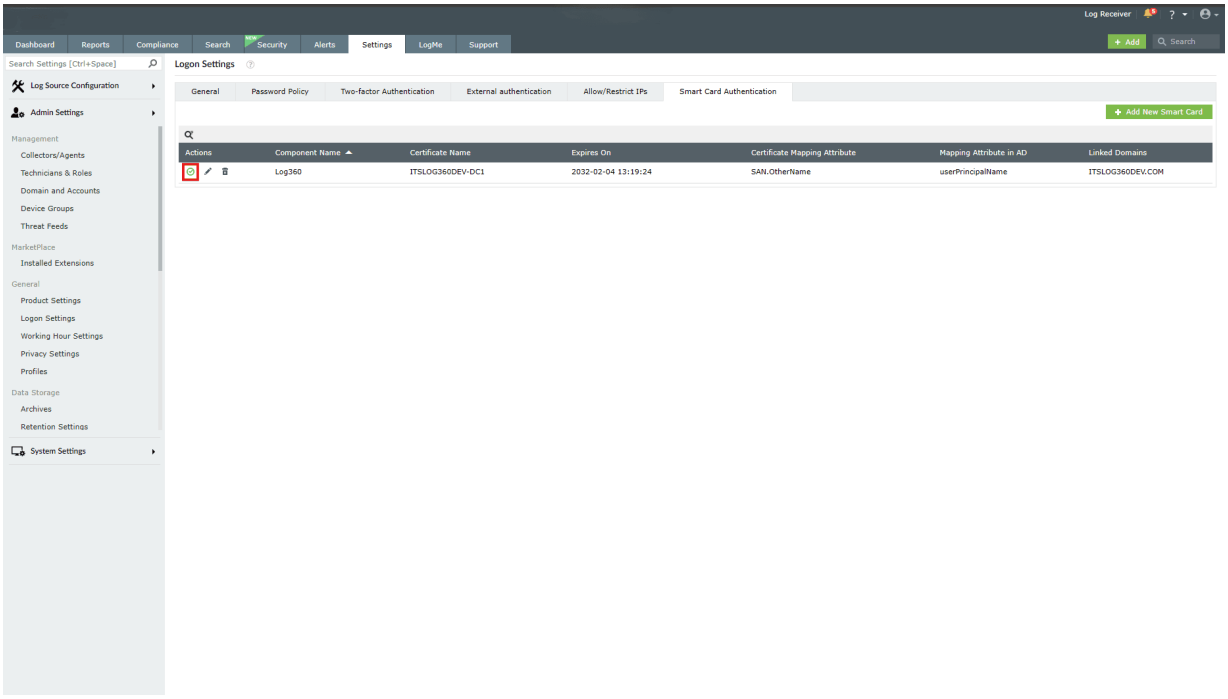


Image 7: Enable/disable smart card in logon settings

Disabling a smartcard

1. Click on the currently enabled icon under the Actions column to disable the smartcard.
2. As soon as you perform this action, the icon indicates that the smartcard is now disabled, and the below pop-up message appears briefly.

Enabling a smartcard

1. Click on the currently disabled icon under the Actions column to enable the smartcard.
2. As soon as you perform this action, the icon indicates that the smartcard is now enabled, and the below pop-up message appears briefly.

Delete a configured smartcard



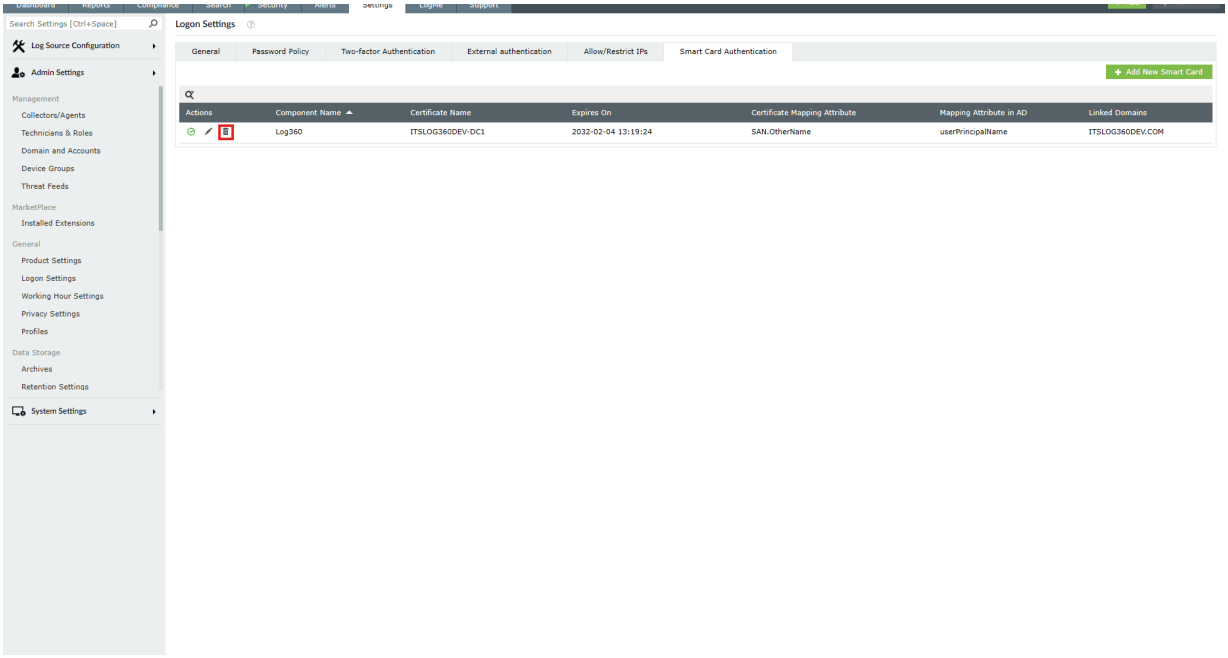


Image 8: Delete smart card in logon settings

1. In the Smart Card Authentication sub-tab, locate the smartcard you want to delete.
2. Click the delete icon in the corresponding row.
3. Click Yes to confirm the deletion.

Read also

This document explained how to configure and manage smartcard authentication, including adding, editing, enabling, disabling, and deleting smartcards. For more information on related authentication and access control settings, refer to the following help documents:

- General logon settings
- Two-factor authentication
- Allow/restrict IP addresses

9.3.5. Allow/restrict IPs and external authentication

Last updated on: September 12, 2025

In this page

Overview

External authentication

Allow/Restrict IPs

Smart Card Authentication

Overview

This page outlines advanced authentication and access control options to secure user logins. You can enable external authentication via Active Directory or RADIUS, and control inbound traffic with Allow/Restrict IPs. These settings ensure only trusted users and devices can access the product.

External authentication

External authentication lets you integrate Active Directory (AD) or RADIUS servers with the product.

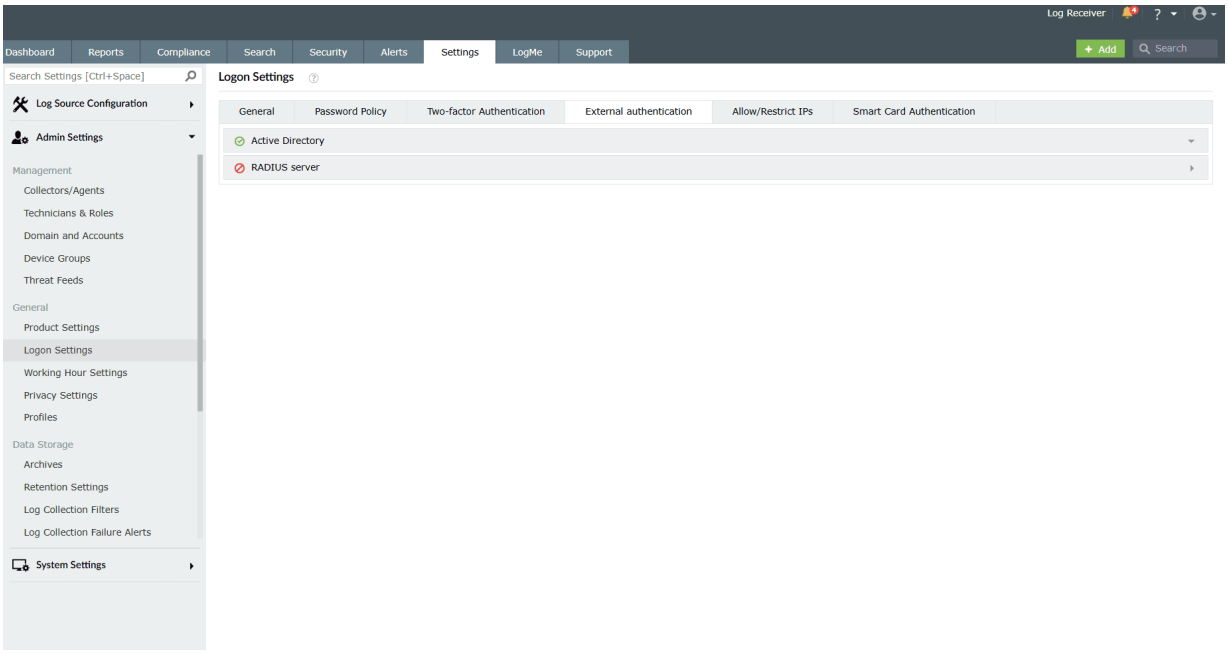


Image 1: External authentication logon settings

Active Directory

Active Directory authentication allows AD technicians to log in to the product using their AD credentials. If this feature is disabled, AD technicians will no longer be able to access the product.

By default, this setting is enabled. Click on the Disable Active Directory Authentication button if you wish to

By default, this setting is enabled. Click on the Disable Active Directory Authentication button if you wish to disable this setting.

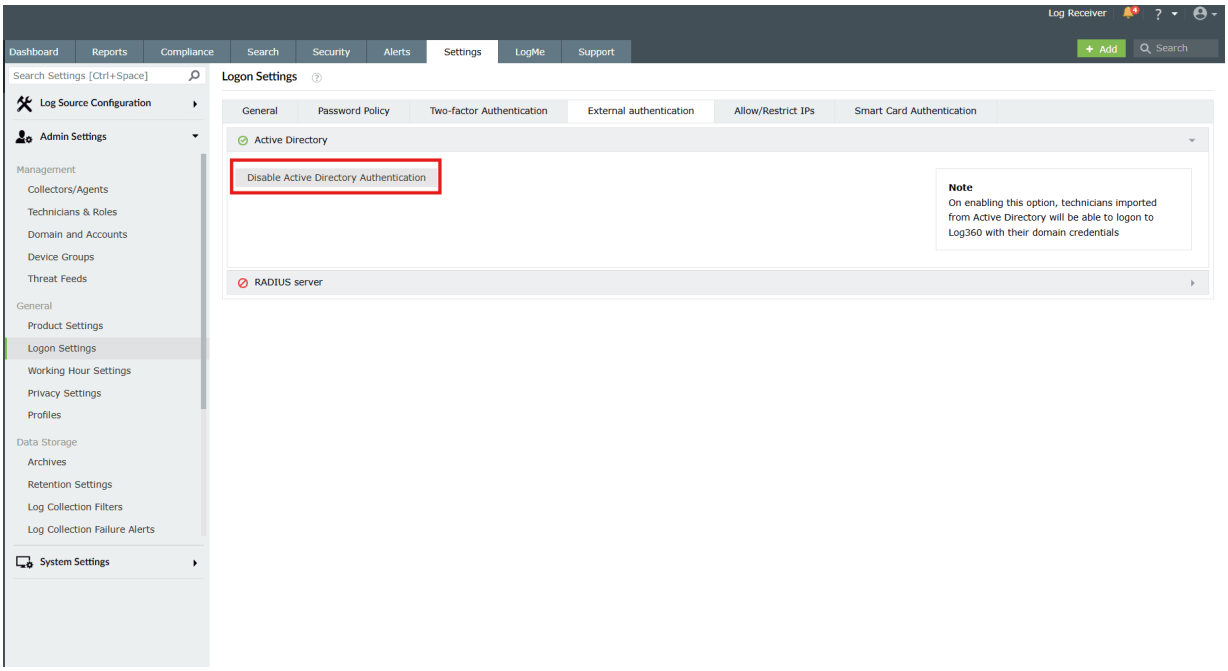


Image 2: Active Directory authentication in external authentication logon settings

RADIUS Server

Remote Authentication Dial-In User Service (RADIUS) is an industry standard client/server authentication protocol that enhances security by protecting networks from unauthorized access.

Phase 1: Integrate RADIUS with Log360

1. Log in to the RADIUS server.
2. Navigate to clients.conf file.(/etc/raddb/clients.conf).
3. Add the following snippet in the clients.conf file.
4. client Log360ServerName
   {
   ipaddr = xxx.xx.x.xxx
   secret = <secretCode>
   nastype = other
   }
5. Restart RADIUS server.

Phase 2: Configure the product console for RADIUS

1. Navigate to the RADIUS Server authentication in the product console.
2. This setting is disabled by default. Enable it by clicking on the empty checkbox in order to access the related configurations.



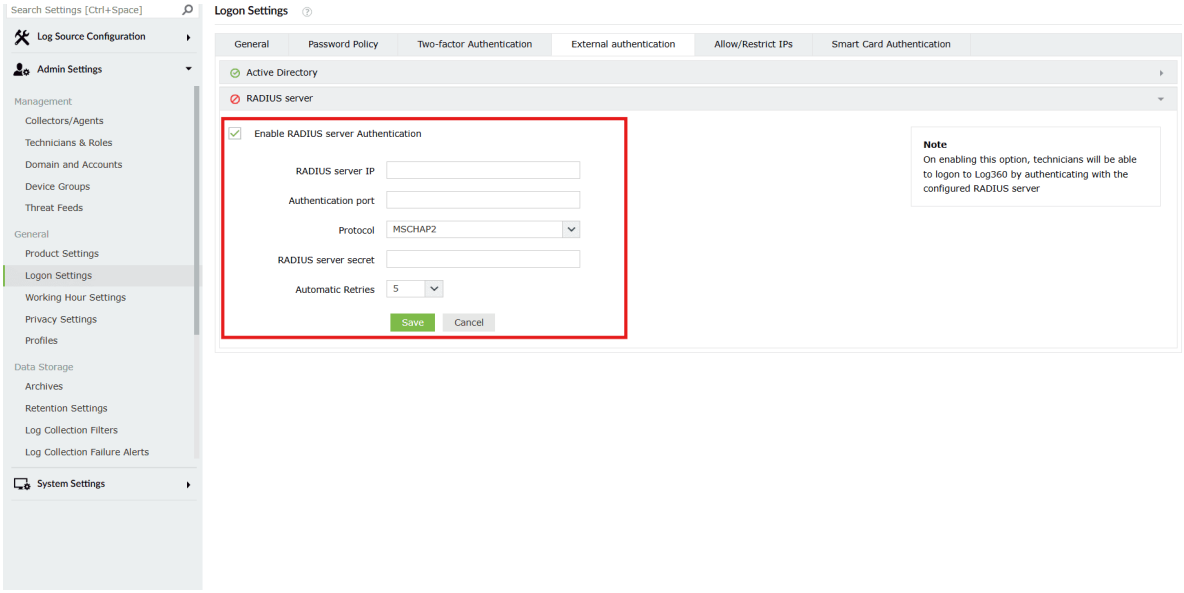


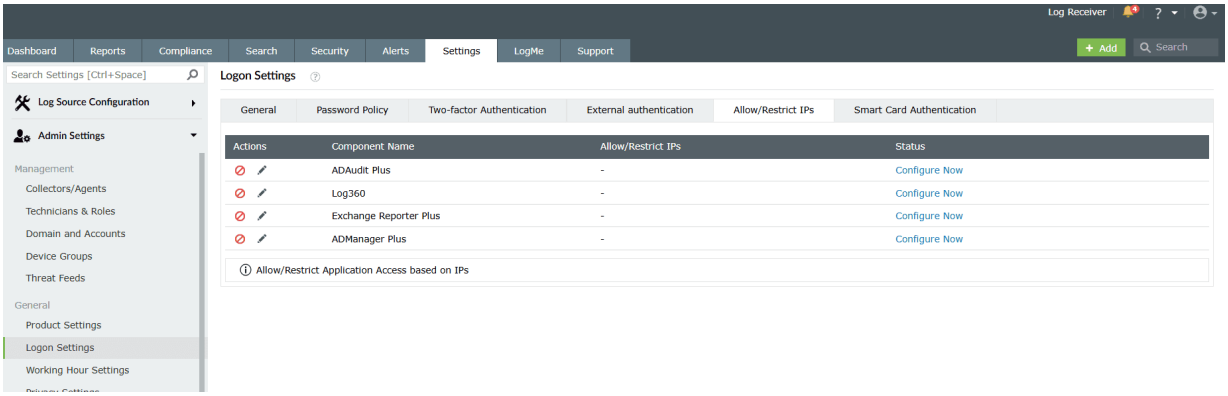
Image 3: RADIUS authentication in external authentication logon settings

3. Fill in the required fields:
    - RADIUS server IP: Enter the IP address of the RADIUS server.
    - Authentication port: Enter the port number for RADIUS authentication.
    - Protocol: Select the protocol used for RADIUS authentication from the drop-down list. The available protocols are PAP, CHAP, MSCHAP and MSCHAP2.
    - RADIUS server secret: Provide the security key that was added to the clients.conf file in RADIUS server.
    - Automatic Retries: Define the number of times the system will retry RADIUS authentication if the initial attempt fails.
4. After making the necessary configurations, click on Save.

Allow/Restrict IPs

One way to add another layer of security is by allowing or restricting inbound connections to specific IPs or IP ranges. This adds an additional layer of security by allowing connection from only trusted sources and blocking unwanted and malicious traffic.

The IP restriction can be applied for the entire product, specific URLs within the product, or APIs. By default, all of them are in a restricted state. You must manually enable them in order to allow IPs from those components.



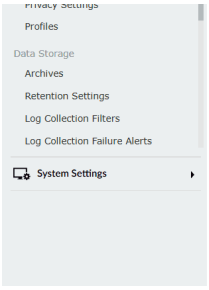


Image 4: Allow/restrict IPs in logon settings

Allow IPs from a specific component(s):

1. Click on the currently restricted icon under the Actions column to allow IPs from the respective component(s).
2. As soon as you perform this action, the icon changes to and the configuration box slides open for that component.

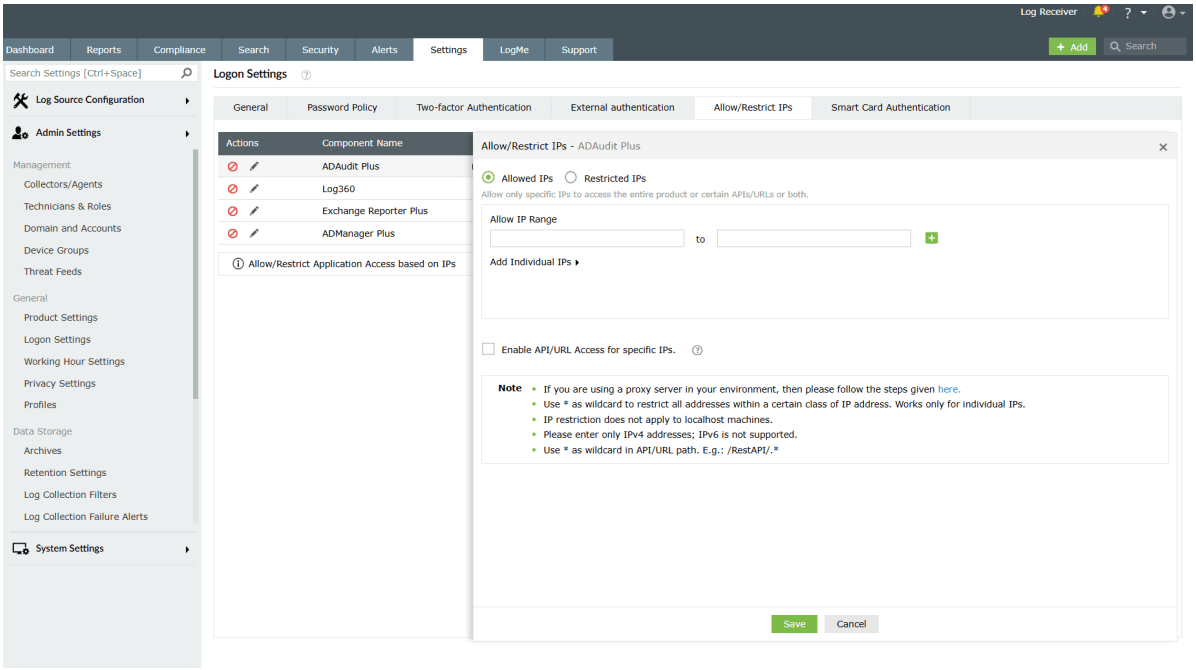


Image 5: Allow/restrict IPs in logon settings

3. Select the Allowed IPs or the Restricted IPs option.
   - Allowed IPs option will allow you to specify a range of IPs that alone should be allowed.
   - Restricted IPs option will allow you to specify a range of IPs that alone should be restricted.
4. Based on your requirements, enter the desired IP addresses.
   - Adding multiple IP ranges: Click [+] icon if you want to allow or restrict access to multiple IP address ranges.
   - Allow/restrict individual IPs: Click Add Individual IPs if you want to allow or restrict access to individual IP addresses. You can add multiple individual IP addresses by separating the values using comma.

Appendix for reference:

Appendix for reference:

- Use * as a wildcard character: Individual IP addresses can include wildcard characters, so that all addresses within a certain class of address will be restricted. For example, denying access to address 192.168.2.* would restrict access to all addresses within that subnet.
- You can also enter hostname instead of IP addresses.
- You can allow or restrict only IPv4 addresses. IPv6 is not supported.
- The Remote Integrated Child Components (RICC) server IP address cannot be restricted in Log360
- The implementation of IP restriction for forward proxy is not supported.
- After initially configuring IP Restriction or Reverse Proxy in Log360, a manual restart of the child products is necessary.
- When the child products are installed remotely and the Reverse Proxy is set up in Log360, manually add the parent product server's IP as an internal proxy in the child product. Following this, manually restart the child products.

If you have changed the 3rd party reverse proxy settings of the product or any of its integrated components for which you are enabling IP-based restriction, then:

- Add the following line to the server.xml file (default location: <InstallationDirectory>/conf/server.xml): <ValveinternalProxies="192\.168\.0\.10|192\.168\.0\.11"trustedProxies="172\.168\.0\.10|176\.168\.0\.11" />
- Edit the values of internalProxies and trustedProxies as per your environment.
- Enter IP address while specifying the values for internalProxies and trustedProxies, and use the vertical bar (|) character to enter multiple values.
- Restart for the changes to take effect.
- Repeat these steps for the integrated components as well.

In case you wish to allow specific IPs or URLs from specific products:

Click on the checkbox "Enable API/URL Access for specific IPs " to access the configuration:

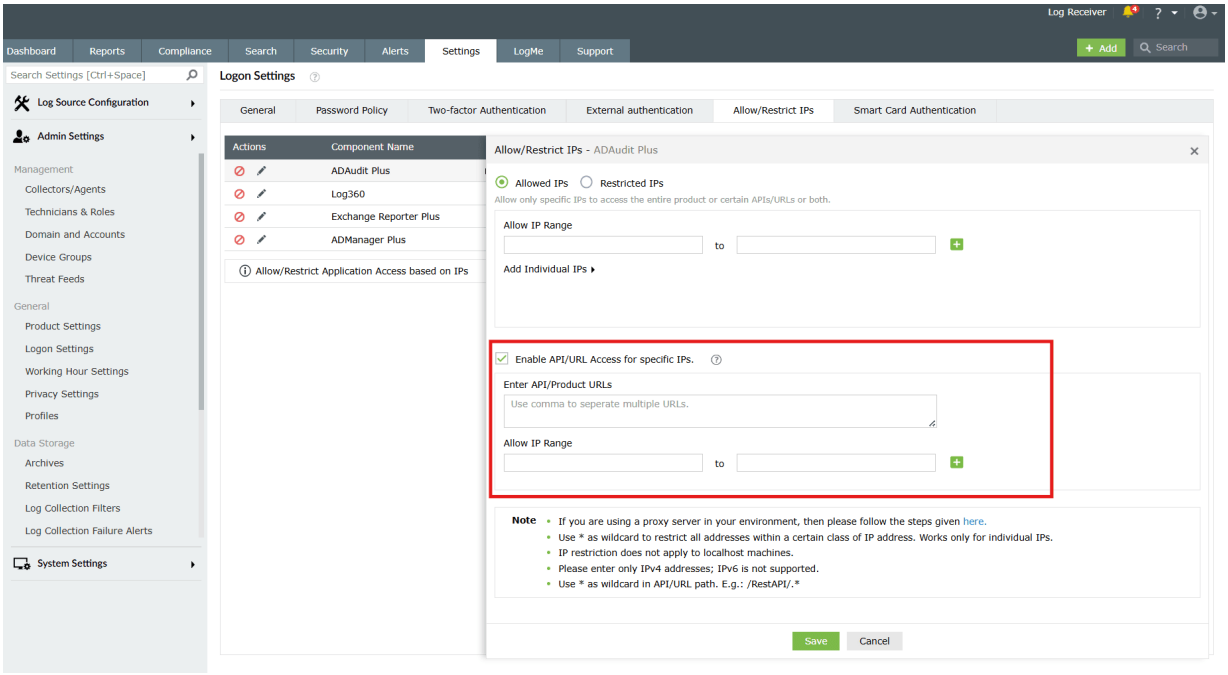


Image 6: Allow/restrict IPs for URLs in logon settings

1. Enter the API/Product URLs in the box provided.
   Sample URL paths: /Admin.do, /Configuration.do, /Dashboard.do
   Sample API paths: /RestAPI/WC/Integration, /RestAPI/WC/LogonSettings

   NOTE

   - Use * as a wildcard character to restrict access to a broader range of APIs or URLs. For example, use /RestAPI/WC/.* to restrict all API calls that start with /RestAPI/WC/.
   - The API/URL path should start with /. For example, /Admin.do and /RestAPI/WC/.
   - Enter only the path of the API or URL. For example, if the entire product URL is https:testserver:8095/Admin.do, then enter only /Admin.do.
   - Only alphanumeric characters (A-Z, a-z, 0-9) and the following special characters are allowed: period (.), forward slash (/), and asterisk (*).

2. Enter the IP addresses as per your requirement. Click [+] icon if you want to allow access to multiple IP address ranges.
3. Finally, click Save to save the settings. Upon successful completion of the action, the below pop-up appears.

   Settings saved successfully.

   If any changes are made to the 3rd party reverse proxy for the product, or any of its integrated components, then:

   - Add the following line to the server.xml file (default location: <InstallationDirectory>/conf/server.xml): <ValveinternalProxies="192\.168\.0\.10|192\.168\.0\.11"trustedProxies="172\.168\.0\.10|176\.168\.0\.11" />
   - Edit the values of internalProxies and trustedProxies as per your environment.
   - Enter IP address while specifying the values for internalProxies and trustedProxies, and use the vertical bar (|) character to enter multiple values.
   - Restart Log360 for the changes to take effect.
   - Repeat these steps for the integrated components as well.

   NOTE

   - The purpose of configuring InternalProxies and TrustedProxies is to determine which IP addresses are regarded as internal or trusted. By configuring these settings, organizations can improve their network security by controlling the access and use of IP addresses within their network.
   - InternalProxies are IP addresses that are trusted and from within the organization network. These IP addresses are typically used by internal services, such as printers and servers.

- TrustedProxies are IP addresses that are external to the network but still maintain a high level of trust and reliability. These IP addresses are typically associated with external services like websites and databases.

Managing IP restriction

You can also make the following changes to this setting:

- Enable/disable IP-based restriction: Use the icon under the Actions column to enable or disable IP-based restriction. Icon means IP-based restriction is enabled for a component and icon means IP-based restriction is disabled.
- Edit IP-based restriction settings: Click icon to edit. The same configuration box slides in, and you can add, delete, or edit the IP ranges and individual IP addresses. You can also perform this
- Summary details: Click the link under the Allow/Restrict IPs column to view the IPs that are allowed or restricted from accessing a component.

Read also

This document explained the general and password policy logon settings. You can also explore other logon settings such as two-factor authentication, external authentication, and allow/restrict IPs for enhanced login security. For more understanding, refer to the below help documents:

- General logon settings
- Two-factor authentication
- Smartcard authentication

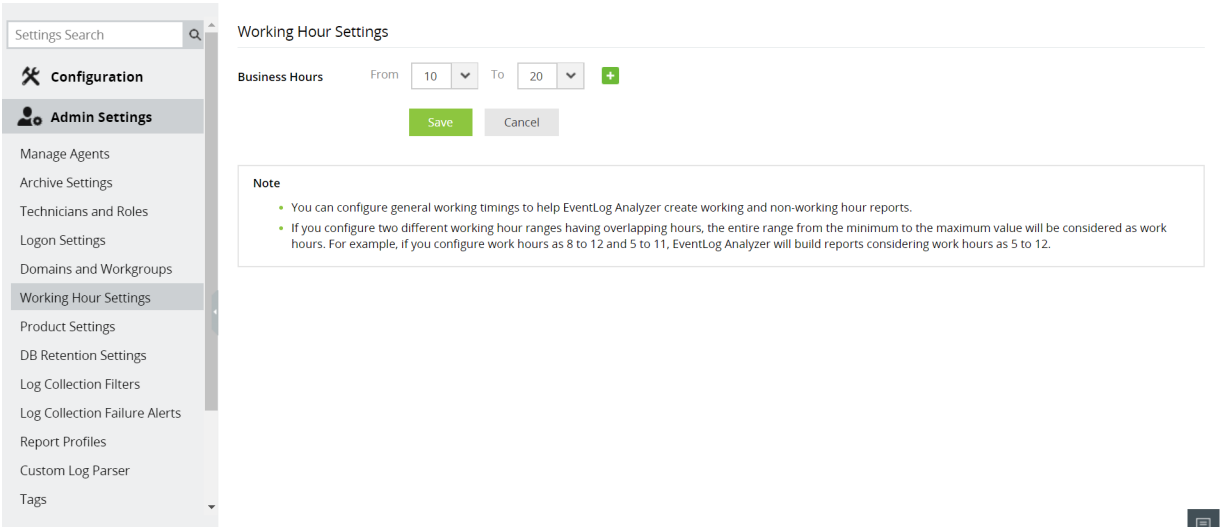
9.3.6. Working Hour Settings

Last updated on: September 12, 2025

EventLog Analyzer generates trend reports to analyze network patterns. This depends on the working hours and non-working hours of each organization. You can configure the working hours in EventLog Analyzer, so that it recognises and generates trend reports for the configured time period. You also have the option of configuring multiple working hour ranges.

To configure working hours,

- In the Settings tab, go to Admin Settings >Working Hour Settings.



- Configure your organization's working hours by selecting appropriate From and To values.
- To configure multiple time ranges, click the + icon and select the next working hour range.
- Once the necessary working hours have been selected, click Save.

> **Note**
>
> If two working hour ranges with overlapping hours are configured, EventLog Analyzer will set the working hours to be the entire range, from the least to the highest value. For example, if the configured time ranges are 8 to 12 and 5 to 11, EventLog Analyzer's working hours will be set as 5 to 12.

9.3.7. Reset Account Settings

Last updated on: September 12, 2025

In this page

Overview

Reset admin password

Unblock admin account

Reset TFA enrollment

Overview

This page explains how to reset account settings for the default admin in Log360. It covers steps to reset the admin password, unblock the admin account, and reset Two-Factor Authentication (TFA) enrollment.

Reset admin password

Follow the steps below to reset the admin password of your account.

For Windows:

1. Navigate to the <Log360>/troubleshooting folder.
2. Execute the resetPwd.bat file.
3. The admin password will be reset to the default password: admin.
4. Please contact your administrator to change the password for other local admins.

For Linux:

1. Open a terminal.
2. Navigate to the <Log360>/troubleshooting folder.
3. Execute the resetPwd.sh file.
4. You can access the account using admin as the password.
5. Please contact your administrator to change the password for other local admins.

Unblock admin account

Multiple unsuccessful login attempts may block the default admin account for security reasons. The account will be automatically restored after a short period. To unblock it immediately, follow these steps:

For Windows:

1. Navigate to the <Log360>/bin/adsf folder.
2. Run the unblockAccount.bat file.

For Linux:

1. Open a terminal.
2. Navigate to the <Log360>/bin/adsf folder.
3. Execute the unblockAccount.sh file.

Reset TFA enrollment

To reset the two-factor authentication (TFA) settings for the default admin account, follow the steps below:

For Windows:

1. Go to the <Log360>/bin/adsf folder.
2. Execute the resetAdminTFAEnrollment.bat file.
3. Log in to Log360 and re-register for TFA as per your preference.

For Linux:

1. Open a terminal.
2. Navigate to the <Log360>/bin/adsf folder.
3. Execute the resetAdminTFAEnrollment.sh file.
4. Log in to Log360 as the default admin and complete TFA re-enrollment.

Read also
This page explained about resetting account settings for the default admin.

9.3.8. Domain and Accounts

Last updated on: September 12, 2025

In this page

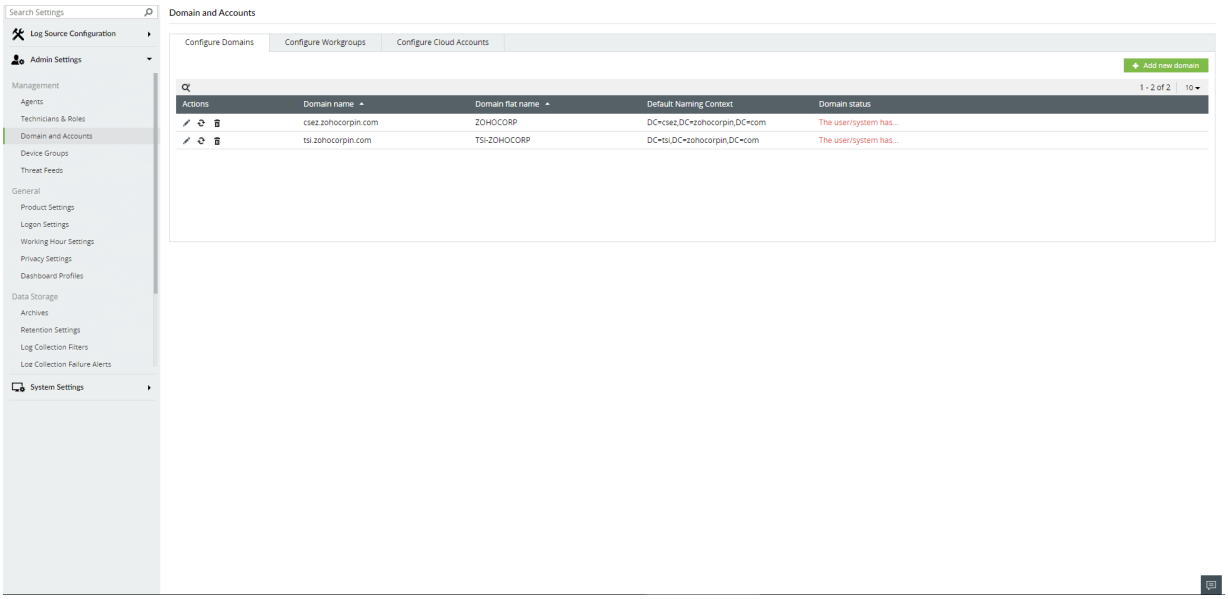
Adding a Domain

Update a Domain

Update a Workgroup

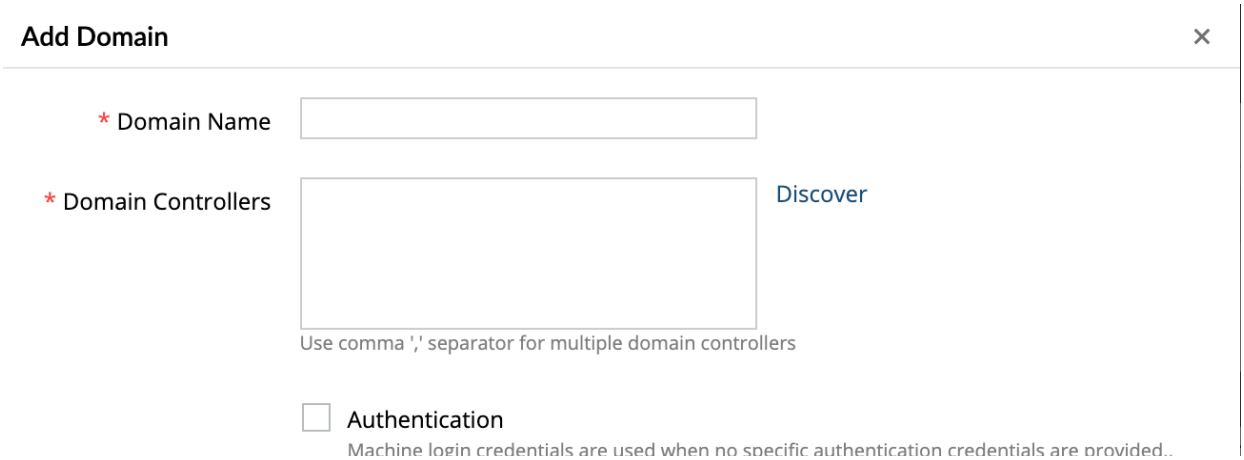
Cloud accounts

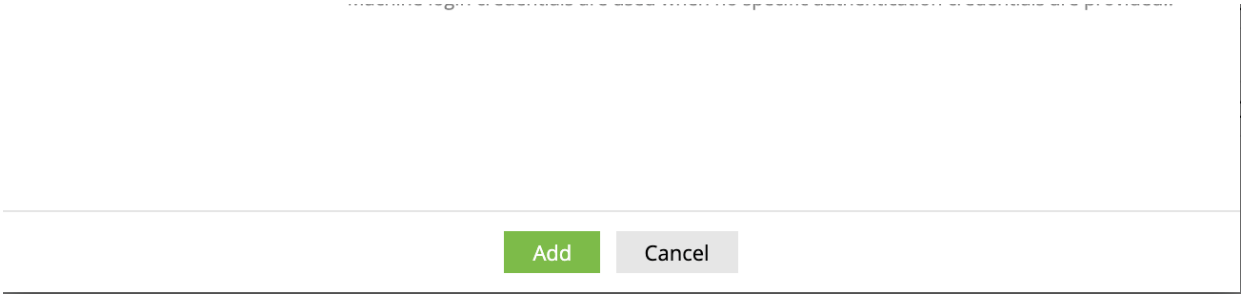
The Domain and Accounts page lists all the Active Directory domains and workgroups discovered by EventLog Analyzer. It also lists all the Cloud Accounts that are added to Eventlog Analyzer. This page allows you to update, reload, or delete a domain, workgroup, or cloud account by clicking the respective icons.
Settings > Admin Settings > Domain and Accounts



Adding a Domain

To add a new domain, click the Add new domain button. This will open the Add Domain window.





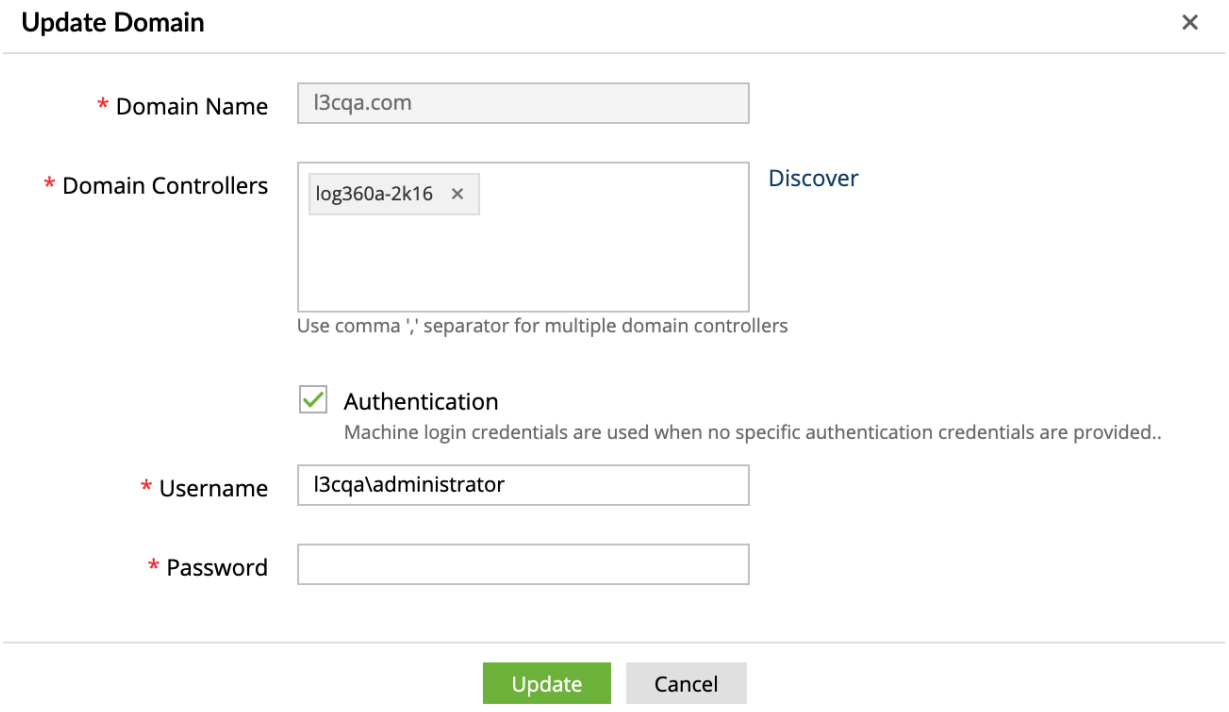
1. Enter the domain name.
2. Click the Discover link to discover the domain controllers. Alternatively, you may also key in the domain controllers' names in the Domain Controllers field, separated by commas.
3. Enter the admin credentials (Username and Password)

> **Note**
>
> When the credentials are not provided, the local machine's login credentials are used.

4. Click the Add button.

Update authentication credentials

To update a domain's authentication credentials, click the Update icon in the Actions column.



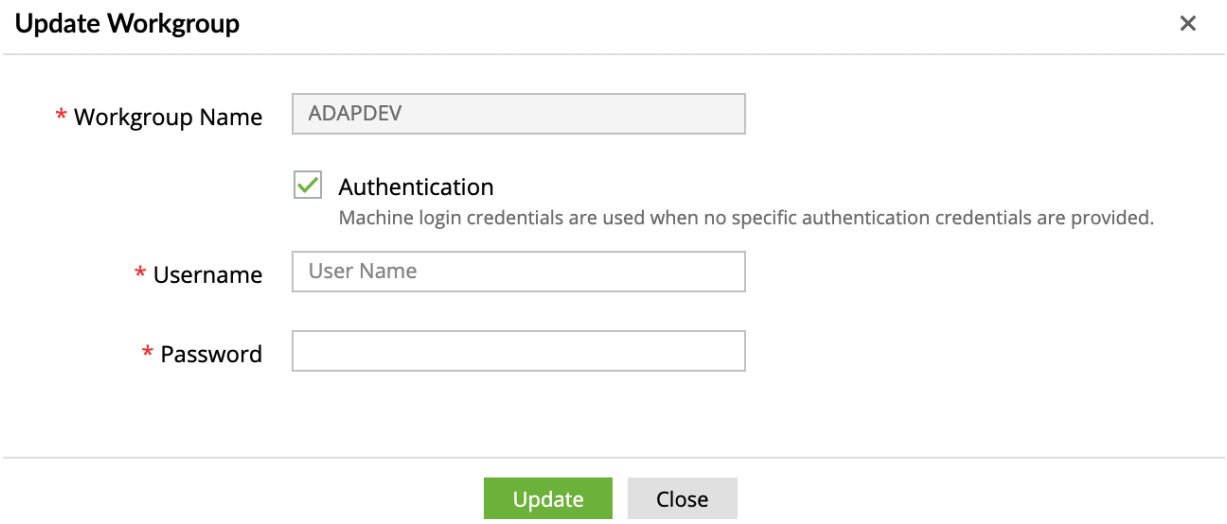
1. Click the Discover link to automatically discover the domain controllers. Alternatively, you may also key in the domain controllers' names in the Domain Controllers field, separated by commas.
2. Modify the authentication credentials. Note that the machine login credentials are used when no

authentication credentials are provided.

3. Click the Update button.

Update a workgroup's credentials

To update a workgroup, click the Update icon in the Actions column.



1. Modify the authentication credentials. Note that the machine login credentials are used when no authentication credentials are provided.
2. Click the Update button.

Cloud accounts

1. Add a cloud account
2. Update a cloud account
3. Delete a cloud account

What logs does EventLog Analyzer collect?

EventLog Analyzer collects CloudTrail logs, S3 server access logs, and ELB access logs from AWS.

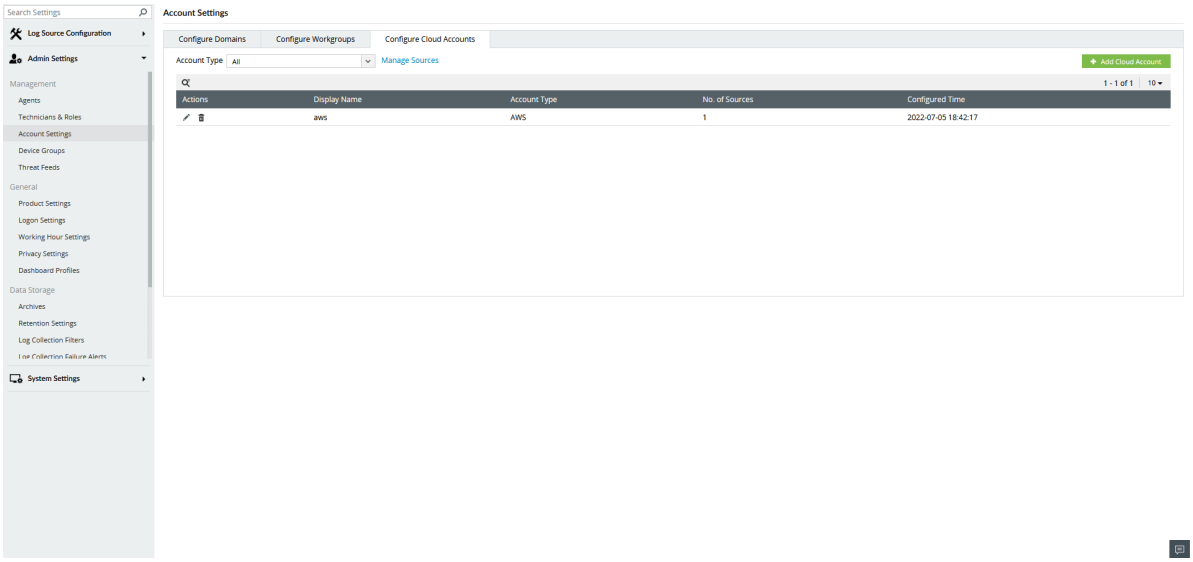
What does EventLog Analyzer offer you?

- Central management of public cloud: Supports the major public cloud platforms like Amazon Web Services (AWS).
- Detailed reports for the AWS cloud environment: A number of predefined reports provide detailed information on events that occur in Amazon S3, EC2, Route 53, Elastic IP, Elastic Network Interfaces, WAF, RDS, STS, VPC, ELB, S3 Bucket traffic logs, and Auto Scaling.

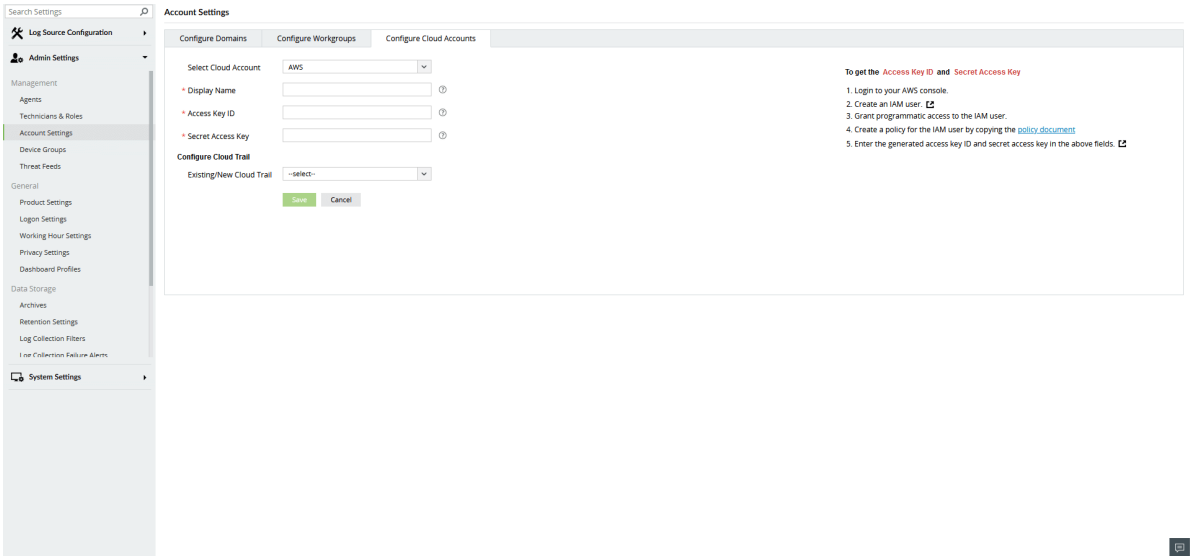
Adding a cloud account

To add a new cloud account, follow the steps given below.

- Open EventLog Analyzer and select the Settings tab. Then, navigate to Domain and Accounts under Admin Settings.



- Choose the Configure Cloud Accounts tab and click the + Add Cloud Account button. This will open the Add Cloud Account window.

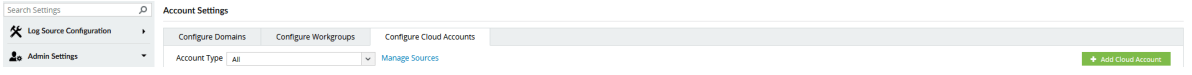


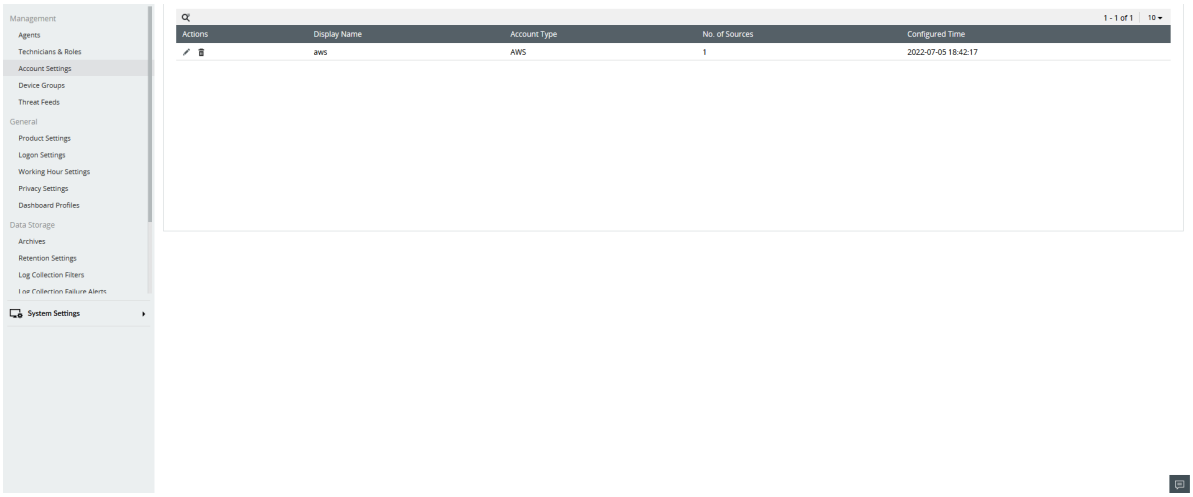
- Select a Cloud Account Type from the drop-down menu.
- Enter the Display name and Access Key ID.
- Enter the Secret Access Key value.
- Follow cloud trail configuration instructions
- Click Save.

Updating a cloud account

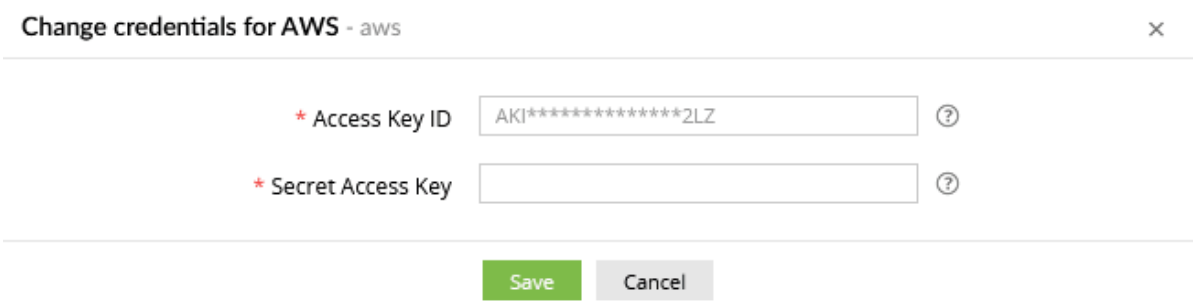
To edit a cloud account, follow the steps given below.

- Open EventLog Analyzer and select the Settings tab. Then, navigate to Domain and accounts under Admin Settings.





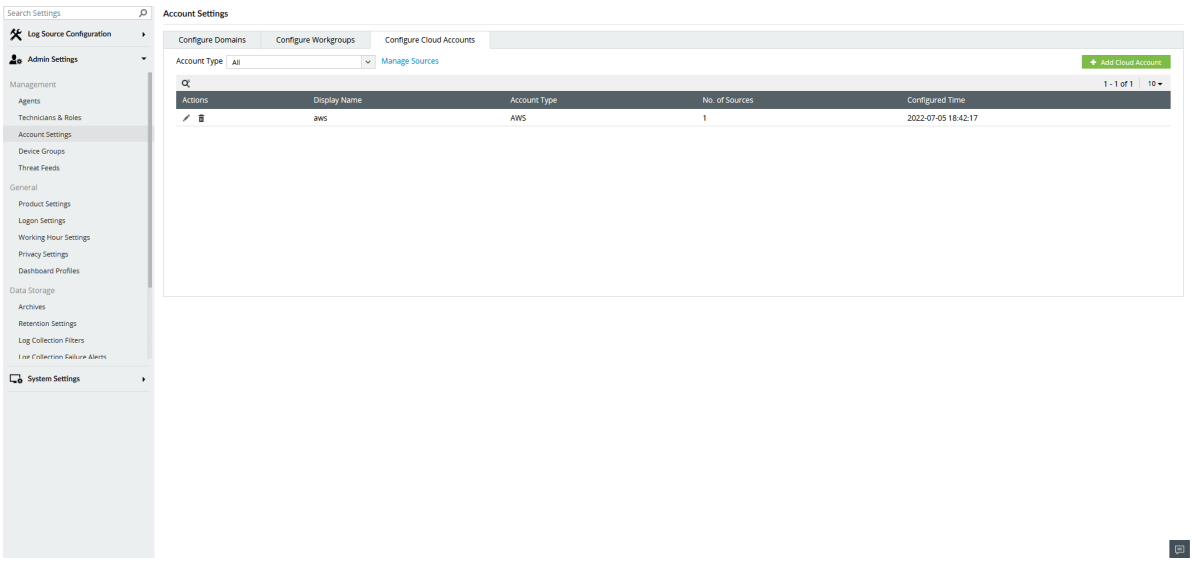
- Choose the Configure Cloud Accounts tab and click the icon corresponding to the desired cloud account.



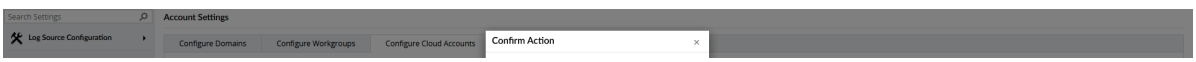
- Enter the new credentials for the cloud account such as the Access Key ID and Secret Access Key and click Save.

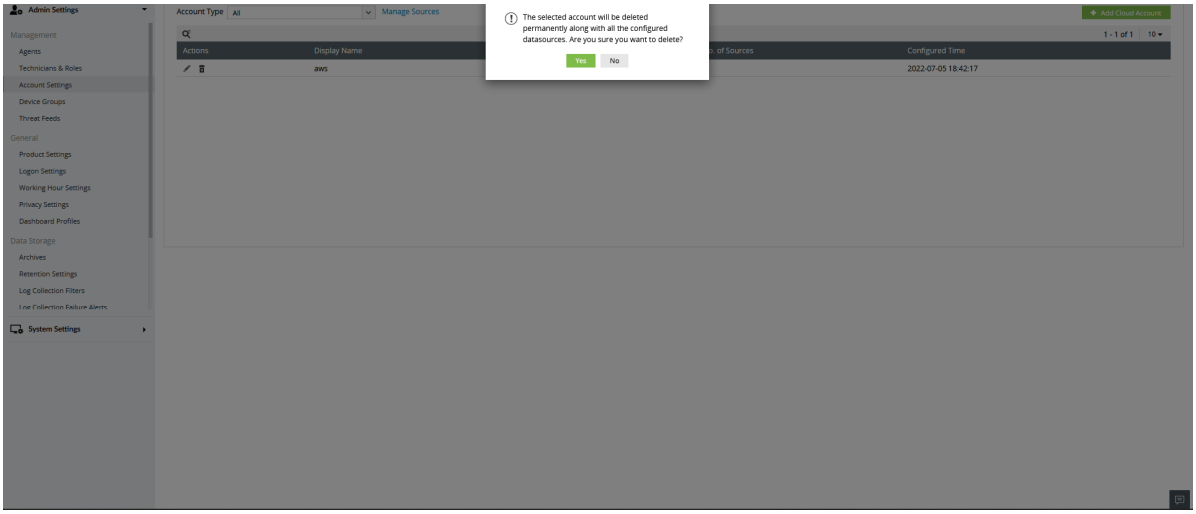
Deleting a cloud account

- Open EventLog Analyzer and select the Settings tab. Then, navigate to Domain and accounts under Admin Settings.



- Choose the Configure Cloud Accounts tab and click the delete icon corresponding to the desired cloud account.



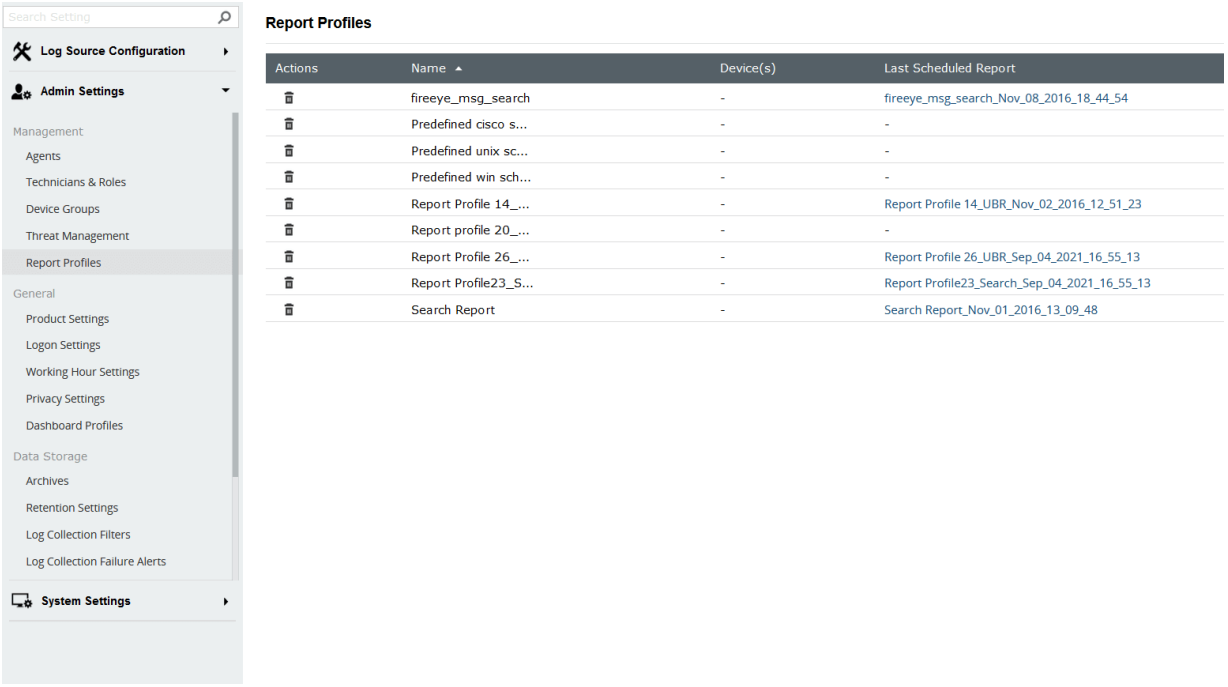


- Select Yes in the dialogue box that prompts you to confirm the action.

9.3.9. Report Profiles

Last updated on: September 12, 2025

To generate a report in EventLog Analyzer, create a report profile, using the following menu option:
Settings tab > Admin Settings > Management > Report Profiles
To create a report profile refer to the procedure given in the ‘How to create custom reports’ section.



How to delete report profile?

1. Delete the profile(s) by clicking on the delete icon.

9.3.10. NTLMv2 SSO configuration

Last updated on: September 12, 2025

EventLog Analyzer uses Jespa to provide NTLMv2 SSO. To enable NTLMv2 SSO in EventLog Analyzer, follow the steps listed below.

NOTE

- To authenticate EventLog Analyzer using Windows built-in SSO, a Computer account must be created in Active Directory Domanin Services (AD DS). Only a Computer account can validate NTLM credentials with the NETLOGON service on AD DS domain controllers. The NETLOGON service will reject a regular User account
- The default package has a Jespa (third-party) limitation which supports unlimited users for 60 days and only 25 users after. If you want to continue using Jespa for NTLM authentication for unlimited users beyond 60 days, you will need to purchase it from IOPLEX.

- Download the latest Jespa JAR file.
- Add the downloaded file to the <EventLog Analyzer home>/lib folder. <EventLog Analyzer home> is the location where EventLog Analyzer is installed.
- Restart EventLog Analyzer for the changes to take effect.

Please contact if you require any assistance in configuring NTLMv2 SSO for your users.

9.4.1. Eventlog Analyzer REST APIs

Last updated on: September 12, 2025

In this page

Steps to generate AuthToken

EventLog Analyzer provides REST Application Programming Interfaces (API) to enable seamless integration of its log management features with other applications. The API enables you to access EventLog Analyzer from other applications and perform necessary log monitoring and analysis with ease. Here are the APIs available and the steps to use them:

> Note
>
> Tokens have admin access and can access all device data without any limitations.

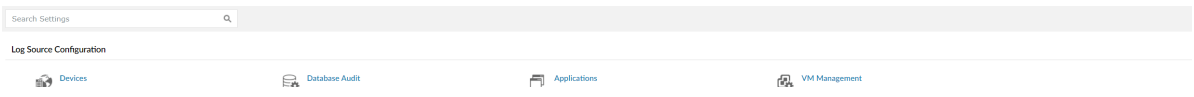
API	Function
Get log sources	To get the list of log sources available in EventLog Analyzer.
Get log fields	To get the list of parsed log fields from the processed logs.
Get log types	To get the list of all log types available in EventLog Analyzer.
Synchronous search	To perform search in Eventlog Analyzer. All search results are obtained by the server before they are returned to the user.
Asynchronous search	The Search is performed in the background and the user is provided with a request ID. The status of the request can be monitored using the Jobs endpoint.
Jobs endpoint	To fetch or delete the status of all the running, failed or completed Asynchronous search, alert tasks.
Jobs Result endpoint	To fetch the search, alert results of the completed Asynchronous search tasks.
Get alert profiles	To get the list of all alert profiles available in EventLog Analyzer.

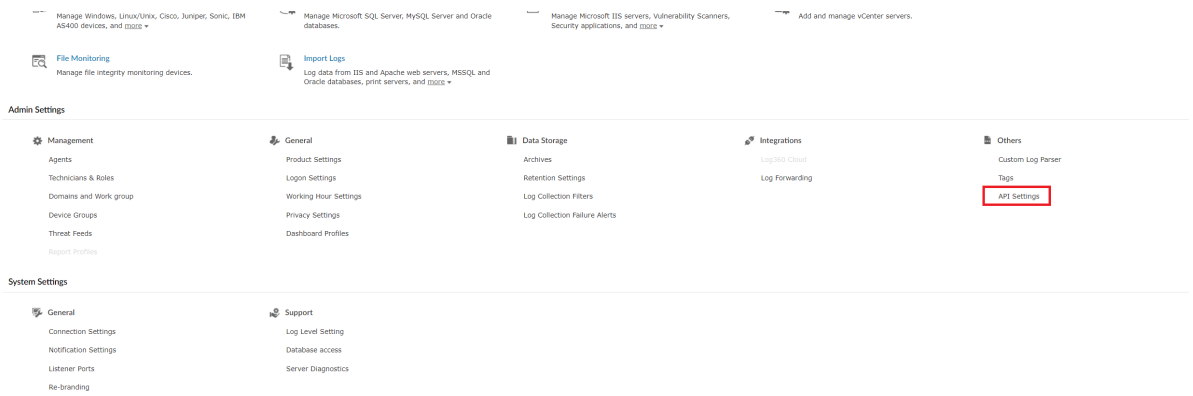
API	Function
Synchronous alerts	To get alerts data in Eventlog Analyzer. All alert results are obtained by the server before they are returned to the user.
Asynchronous alerts	The alert data retrieval is performed in the background and the user is provided with a request ID. The status of the request can be monitored using the Jobs endpoint.
Get Product Details	To get EventLog Analyzer product details.
Disable Device	To disable a log source in EventLog Analyzer.
Sync Incident Status/Severity using Ticket	To update an incident's status/severity based on the created ticket.
Export Incident using Ticket	To export an incident from a created ticket.
Disable Ticket Notification	To disable alert profile notification for ticketing tool connections.
Execute Workflow	To execute a predefined workflow in EventLog Analyzer.

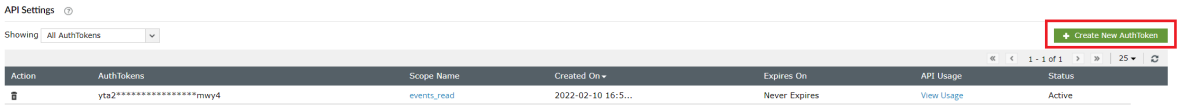
Steps to generate AuthToken

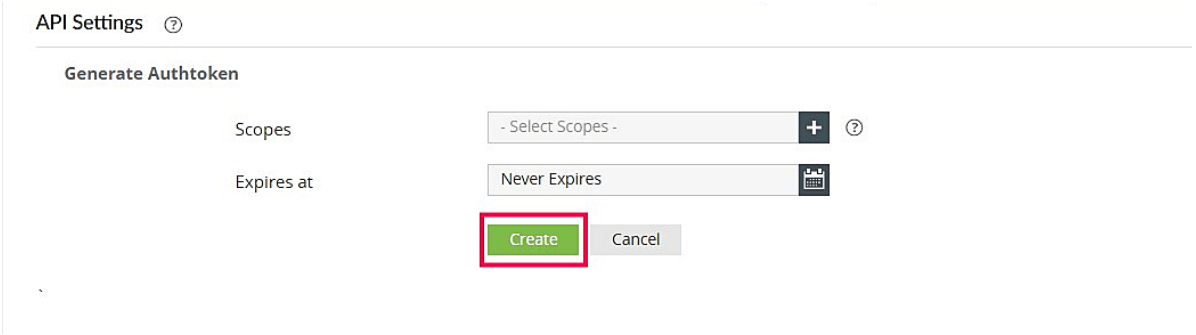
To access EventLog Analyzer from your applications or services, you need an authorization token from EventLog Analyzer. You can generate the same by following the steps below.

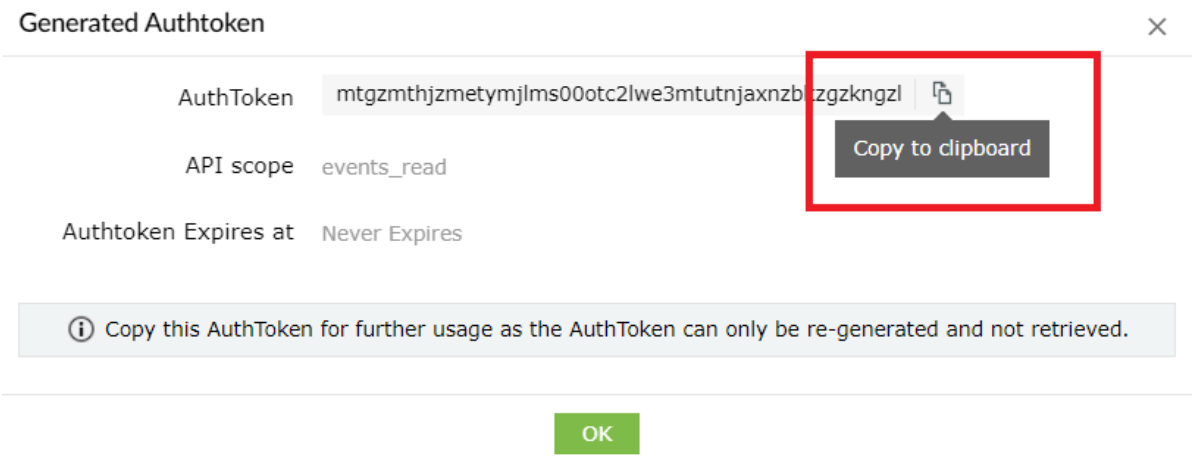
1. Login to the EventLog Analyzer web console as an administrator.
2. Go to Settings > Admin Settings > API Settings > click Create New AuthToken.
3. In Generate AuthToken tab, select the API Scopes, and set an appropriate expiry time for the AuthToken.
4. Scopes define the APIs that can be accessed using the generated AuthToken. You can choose one or more APIs to be part of a scope.
5. Click Create to generate the token.
6. Your AuthToken will be generated. Please ensure that you copy the token displayed for integrating it with external applications since they cannot be retrieved again, only regenerated.




Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more
Manage Microsoft SQL Server, MySQL Server and Oracle databases.
Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more
Add and manage vCenter servers.
File Monitoring
Manage file integrity monitoring devices.
Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more
Admin Settings
Management
Agents
Technicians & Roles
Domains and Work group
Device Groups
Threat Feeds
Report Profiles
General
Product Settings
Logon Settings
Working Hour Settings
Privacy Settings
Dashboard Profiles
Data Storage
Archives
Retention Settings
Log Collection Filters
Log Collection Failure Alerts
Integrations
Log360 Cloud
Log Forwarding
Others
Custom Log Parser
Tags
API Settings
System Settings
General
Connection Settings
Notification Settings
Listener Ports
Re-branding
Support
Log Level Setting
Database access
Server Diagnostics


API Settings
Showing All AuthTokens
Create New AuthToken
1 - 1 of 1
25
Action
AuthTokens
Scope Name
Created On
Expires On
API Usage
Status
yta2**********mwy4
events_read
2022-02-10 16:5...
Never Expires
View Usage
Active


API Settings
Generate Authtoken
Scopes
- Select Scopes -
Expires at
Never Expires
Create
Cancel


Generated Authtoken
AuthToken
mtgzmthjzmetymjlms00otc2lwe3mtutnjaxnzb
zgzkngzl
Copy to clipboard
API scope
events_read
Authtoken Expires at
Never Expires
Copy this AuthToken for further usage as the AuthToken can only be re-generated and not retrieved.
OK

9.4.2. Get log sources API

Last updated on: September 12, 2025

The API returns the list of log sources available in EventLog Analyzer.

Request URL

```
GET http://hostname:8095/RestAPI/v1/meta/log_sources?from=1&to=10
```

Request Header

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	Authtoken generated from API Settings page. e.g: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx

Request Parameter

Parameter name	Default value	Mandatory	Description
From	1	No	Start value of the list
To	10	No	End value of the list

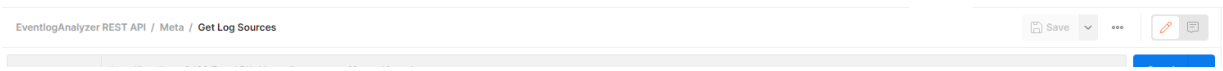
Response

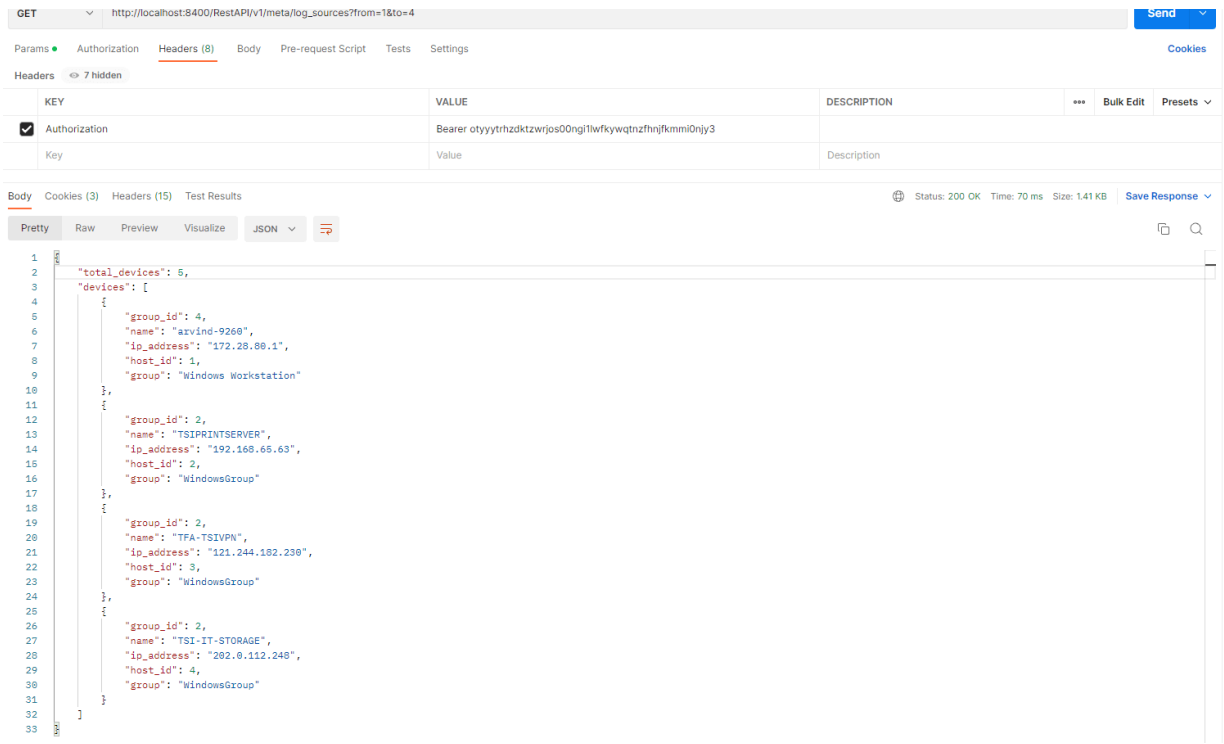
The response will be a JSON object which will contain the list of devices.

Parameter name	Description
devices	JSON Array of devices

Example usage using cURL

Example usage using Postman (Third party tool)






```
{
    "total_devices": 5,
    "devices": [
        {
            "group_id": 4,
            "name": "arvind-9260",
            "ip_address": "172.28.80.1",
            "host_id": 1,
            "group": "Windows Workstation"
        },
        {
            "group_id": 2,
            "name": "TSIPRINTSERVER",
            "ip_address": "192.168.65.63",
            "host_id": 2,
            "group": "WindowsGroup"
        },
        {
            "group_id": 2,
            "name": "TFA-TSIVPN",
            "ip_address": "121.244.182.230",
            "host_id": 3,
            "group": "WindowsGroup"
        },
        {
            "group_id": 2,
            "name": "TSI-IT-STORAGE",
            "ip_address": "202.0.112.248",
            "host_id": 4,
            "group": "WindowsGroup"
        }
    ]
}
```

9.4.3. Get log fields API

Last updated on: September 12, 2025

The API returns the list of parsed log field from processed logs available in EventLog Analyzer. Log Fields can be used to create search queries.

Request URL

```
GET http://hostname:8095/RestAPI/v1/meta/log_fields
```

Request Header

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	Authtoken generated from API Settings page. e.g: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx

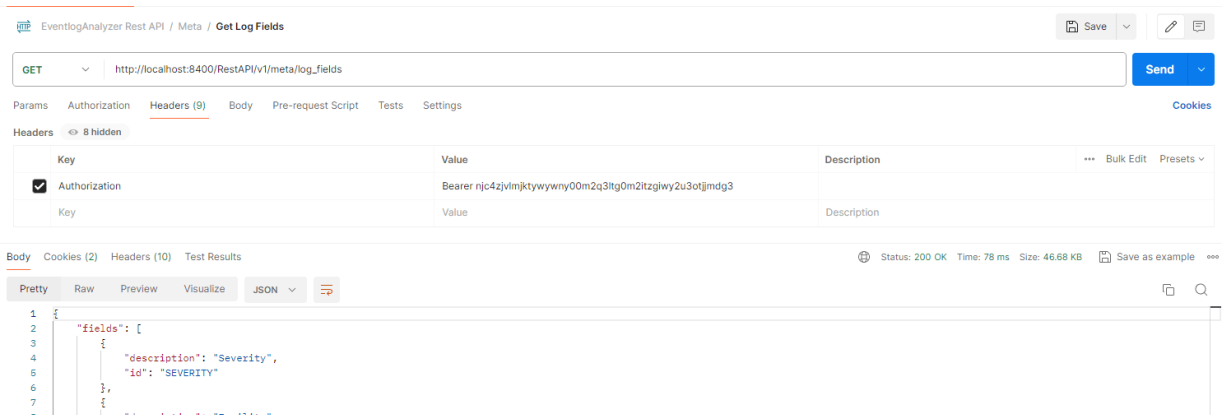
Response

The response will be a JSON object which will contain the list of fields.

Parameter name	Description
fields	JSON Array of fields

Example usage using cURL

Example usage using Postman (Third party tool)



```
        "description": "Facility",
        "id": "FACILITY"
    },
    {
        "description": "Source",
        "id": "SOURCE"
    },
    {
        "description": "Process Id",
        "id": "PROCESSID"
    },
    {
        "description": "Process Id",
        "id": "processid"
    },
    {
        "description": "Event Name",
        "id": "IENAME"
    },
    {
        "description": "Username",
        "id": "USERNAME"
    },
    {
```

9.4.4. Get log types API

Last updated on: September 12, 2025

The API returns the list of log types along with their ids available in EventLog Analyzer. Log types can be used to create search queries to filter search by log types.

Request URL

```
GET http://hostname:8095/RestAPI/v1/meta/log_types
```

Request Header

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	Authtoken generated from API Settings page. e.g: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx

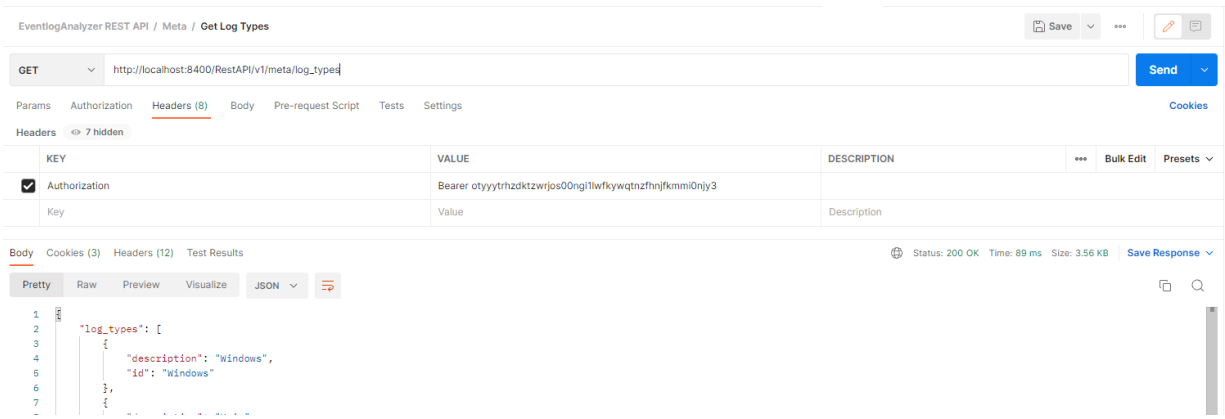
Response

The response will be a JSON object which will contain the list of fields.

Parameter name	Description
log_types	JSON Array of log types

Example usage using cURL

Example eusag using Postman (Third party tool)



```
        "description": "Unix",
        "id": "Unix"
    },
    {
        "description": "Hypervisor/ESXi",
        "id": "Hypervisor"
    },
    {
        "description": "Cisco Device",
        "id": "Cisco Device"
    },
    {
        "description": "FIM",
        "id": "FIM"
    },
    {
        "description": "SonicWall Device",
        "id": "SonicWall Device"
    },
    {
        "description": "Juniper Device",
        "id": "Juniper Device"
    },
    {
        "description": "Palo Alto Device",
        "id": "PaloAlto Device"
    },
    {
        "description": "Fortinet Device",
        "id": "Fortinet Device"
```

9.4.5. Asynchronous Search API

Last updated on: September 12, 2025

The API allows you to run search requests in the background, wherein you can monitor the progress of the request and view the results as and when they become available.
Here are the steps involved in executing a synchronous search query:

- You can make a search request with a set of required metadata and asynchronous parameters.
- The server will respond with a request ID and execute the search in background thread.
- You can check the status of the request through the Jobs endpoint.
- Once the job is done, you can fetch the results using the jobs/results endpoint.
- The search results will be available in EventLog Analyzer for 24 hours after which they are deleted by the cleanup thread.

Request URL

```
POST http://hostname:8095/RestAPI/v1/search/async
```

Request Header

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	AuthToken generated from API Settings page. e.g: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx

Request Parameters

The request needs to be sent in the body of the request using JSON format. And should contain following key/value parameters

Parameter name	Default value	Mandatory	Type	Description
query	*	No	String	Start value of the list
hosts	all	No	JSONArray	List of hosts to search
groups	all	No	JSONArray	List of device groups to search

Parameter name	Default value	Mandatory	Type	Description
from	current time - 24 hours	No	Long	Start time for search in Unix milliseconds
to	current time	No	Long	End time for search in Unix milliseconds

Note

1. When the cursor is passed, the other parameters are not required.
2. Quotes i.e (" ") in query string should to be escaped. If query in EventLog Analyzer's search page is REMOTE_INTERFACE = "switch 1", then for Rest Api the query parameter should be written as "REMOTE_INTERFACE = \"switch 1\""

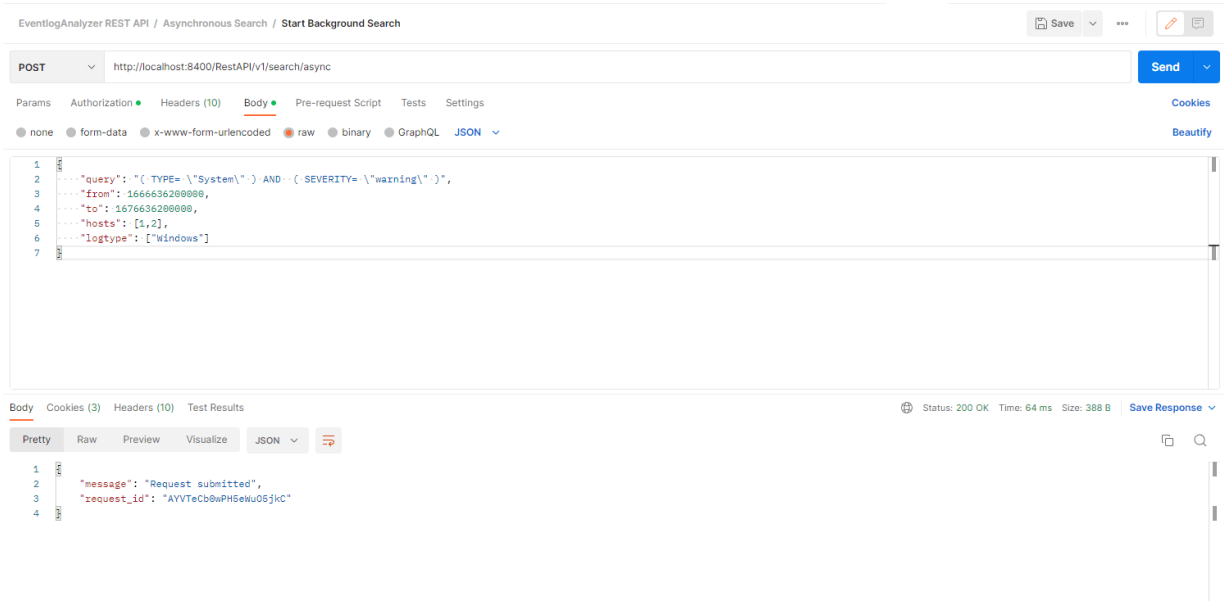
Response

The response will be a JSON object which will contain the following key/value pairs

Parameter name	Description
request_id	Request ID of the background search , type = string

Example usage using cURL

Example usage using Postman (Third party tool)



9.4.6. Jobs API

Last updated on: September 12, 2025

The API allows you fetch/delete the status of all the running and completed background search/alerts task running in EventLog Analyzer.

A) Get jobs status:

Request URL

```
GET http://localhost:8095/RestAPI/v1/jobs
```

Request Header

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	

Request Parameters

Parameter name	Mandatory	Type	Description
request_id	No	String	If provided only this request_id's status will be fetched

Response

The response will be a JSON object which will contain the following key/value pairs

Parameter name	Description
total	cursor for the next set of results
requests	JSON array contains information about each job as a JSONObject. Each JSONObject contains following fields • running_time_in_millis = Human-readable running time, type = long • hits_done = Total hits done • status = Status of job, values = SUCCESS or FAILED or RUNNING • submitted_at = Epoch time in unix milliseconds at which the job was submitted • started_at = Epoch time in unix milliseconds at which the job started

Parameter name	Description
	• running_time = Job running time • last_synced_time = Last synced time in unix milliseconds when the status was flushed to database • total_pages = Total number of pages in this search result • request_id = Request ID of the job

B) Delete jobs:

This allows you to delete the job and its hits

```
DELETE http://localhost:8095/RestAPI/v1/jobs
```

Request Header

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	

Request Parameters

Parameter name	Mandatory	Type	Description
request_id	No	String	If provided only this request_id's status will be fetched

Response

The response will be a JSON object which will contain a message field

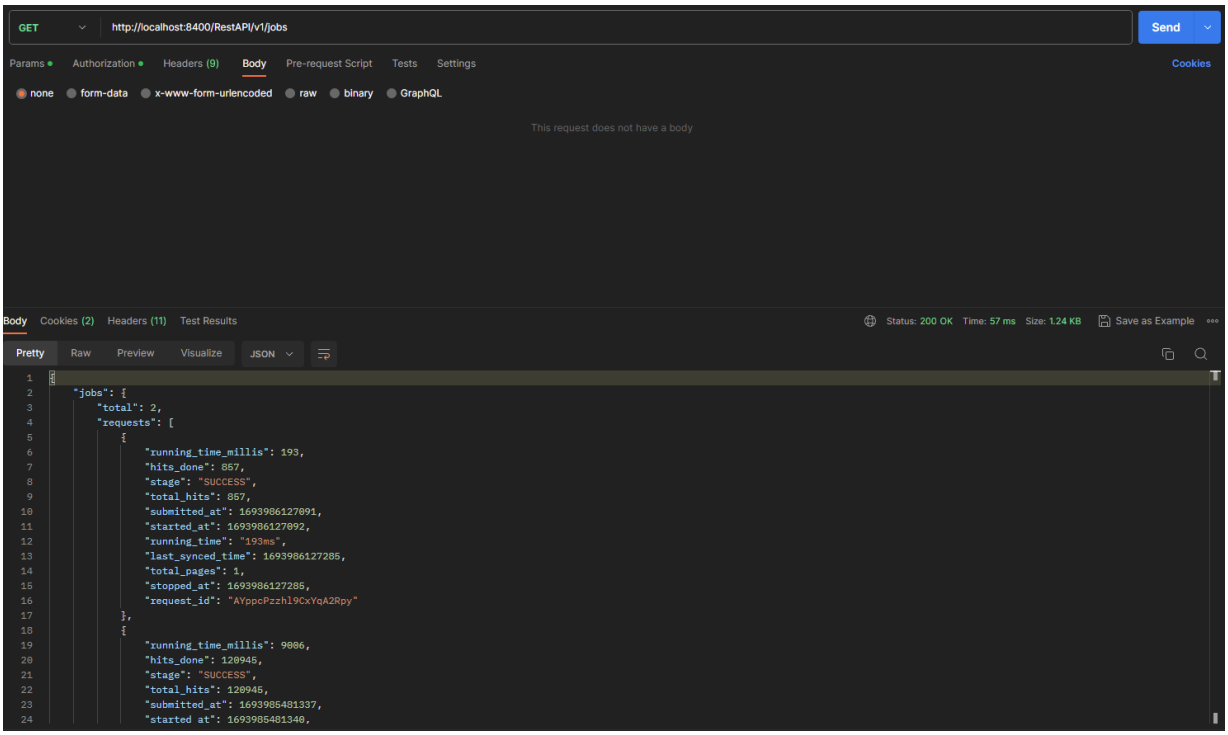
Parameter name	Description
message	result of the delete request

Example usage using cURL

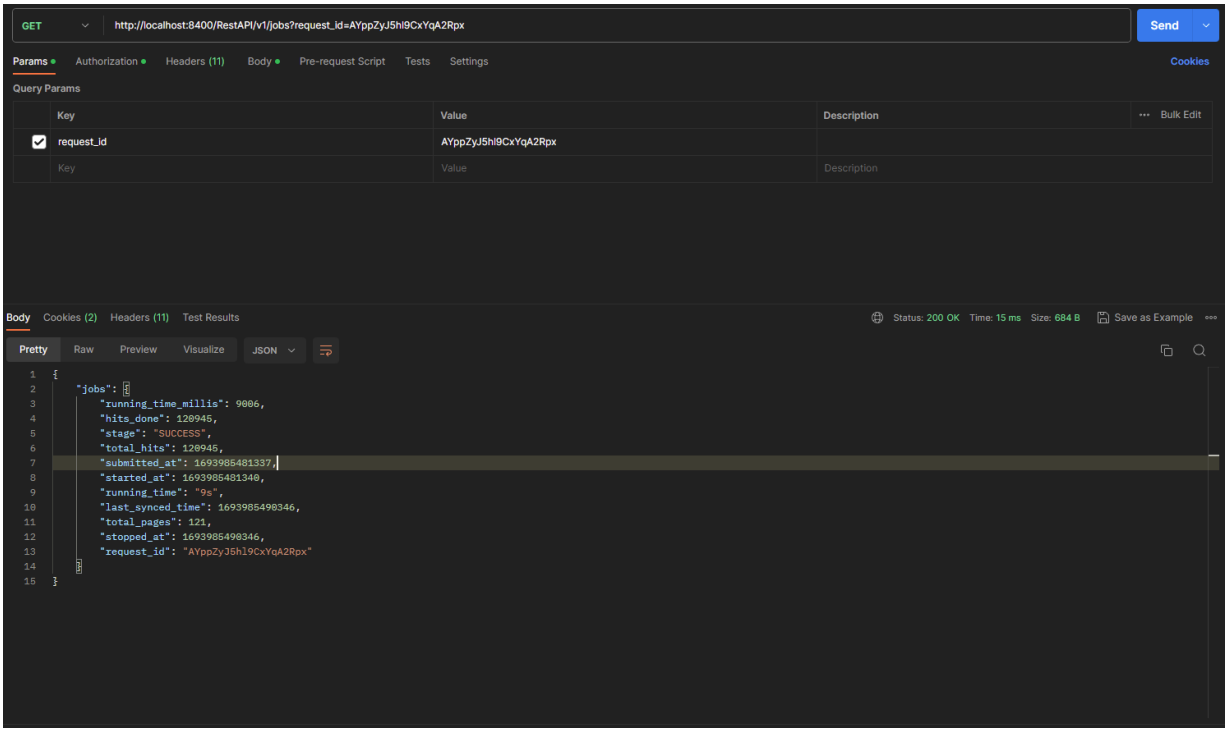
i) Delete status info & hits for particular request_id

Example usage using Postman (Third party tool)

i). Get status for all jobs

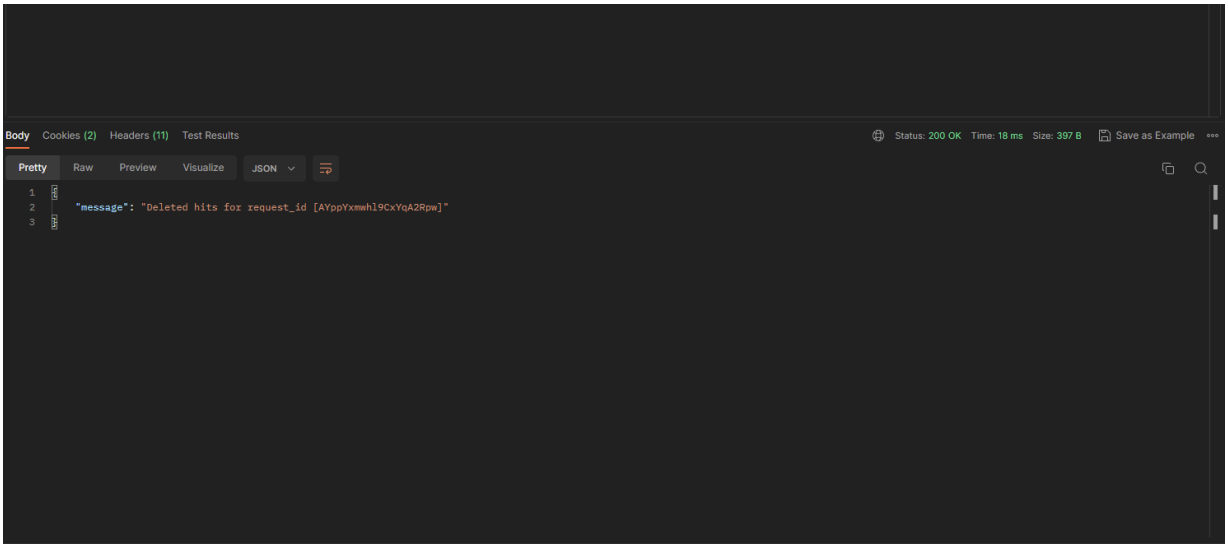


ii) Get status for particular request_id



iii) Delete hits for particular request_id




Body
Cookies (2)
Headers (11)
Test Results
Status: 200 OK
Time: 18 ms
Size: 397 B
Save as Example
Pretty
Raw
Preview
Visualize
JSON
1
2
3
"message": "Deleted hits for request_id [AYppYxmwhl9CxYqA2Rpw]"

9.4.7. Results API

Last updated on: September 12, 2025

The API allows you fetch the results for the async search/alerts task.

Request URL

```
GET http://localhost:8095/RestAPI/v1/jobs/results
```

Request Header

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	

Request Parameters

Parameter name	Mandatory	Type	Description
request_id	Yes	String	request_id of the async search task returned by async endpoint
page_no	No	Int	if provided fetched particular page number of the result-set

Response

The response will be a JSON object which will contain the following key/value pairs

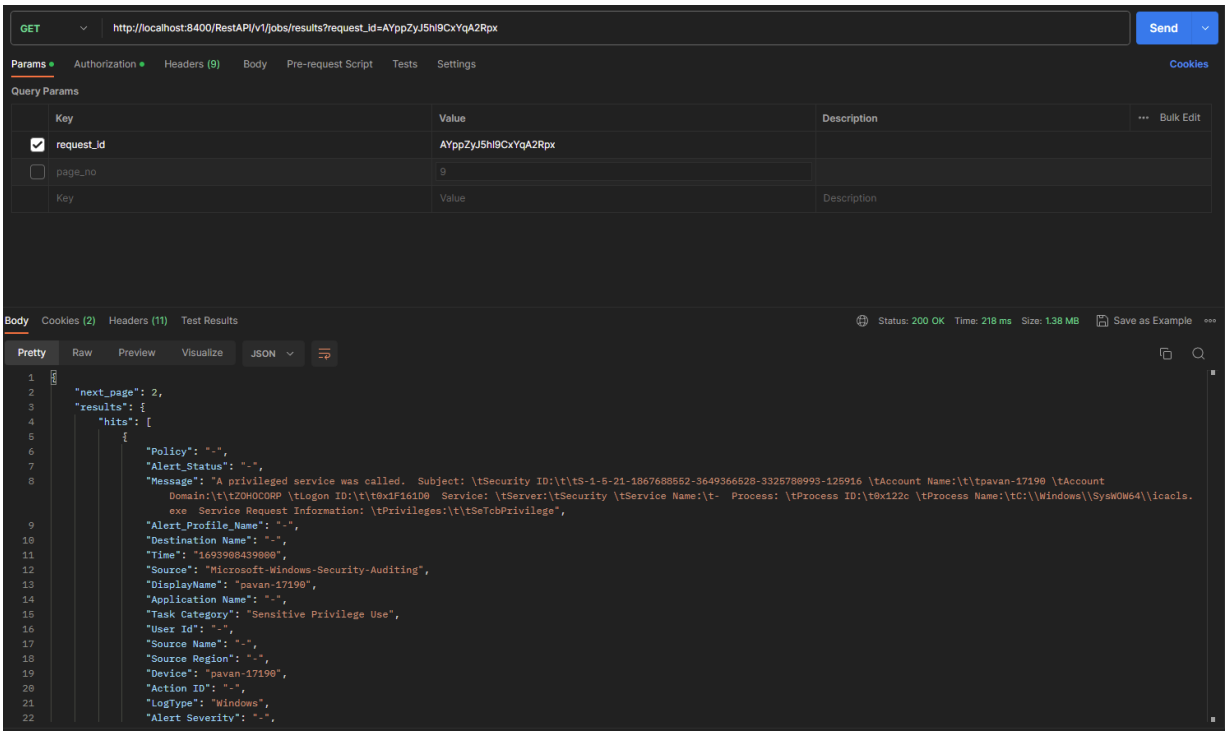
Parameter name	Description
next_page	Next page number of the result set
results	JSON object which contain search hits for the request Contains following fields • hits: List of search hits • hits_count_in_current_page: Hits count in current search response

Example usage using cURL

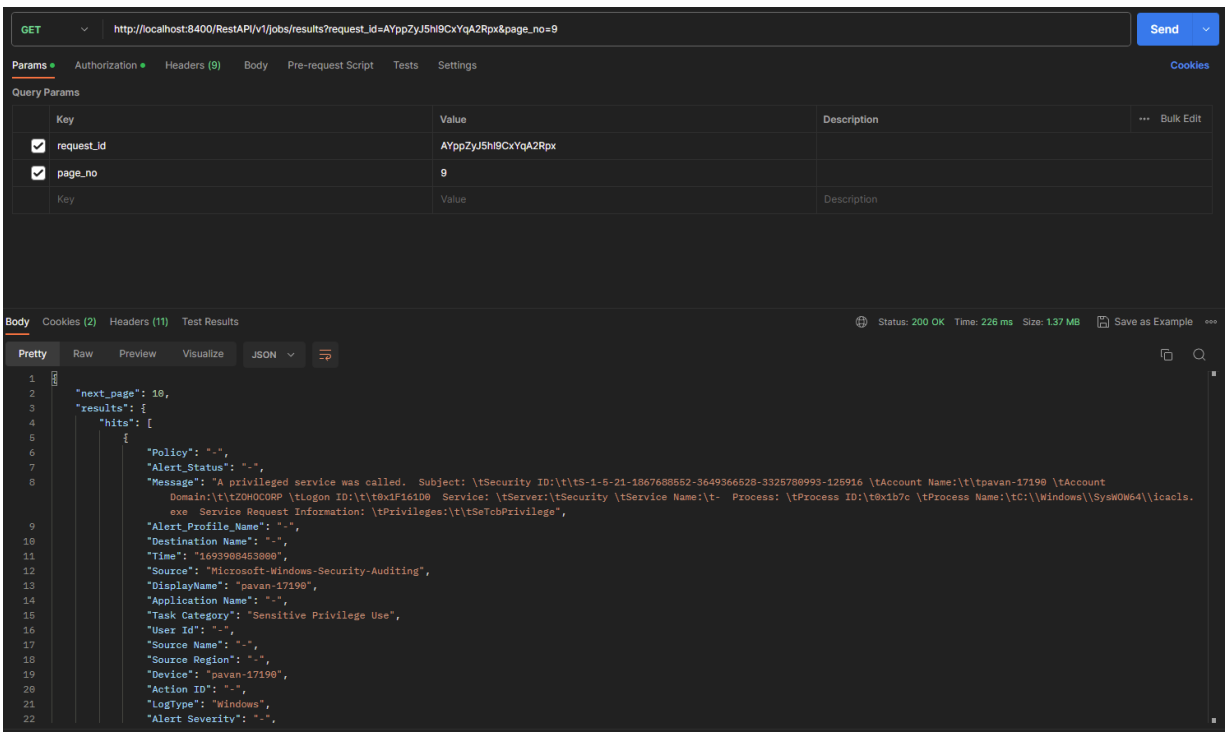
i) Delete status info & hits for particular request_id

Example usage using Postman (Third party tool)

i) Get results of async search



ii) Get particular page of results of async search



9.4.8. Get alert profiles API

Last updated on: September 12, 2025

The API returns the alert profile data that are available in EventLog Analyzer. The Alert Profile metadata can be used to filter alert search request.

Request URL

```
POST http://hostname:8095/RestAPI/v1/meta/alert_profiles
```

Request Header

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	Authtoken generated from API Settings page. e.g: Bearer mdrkodg0odmtmznlocg0ndziltg0mgftmwzkztsjmjvdzwmx

Request Parameters

The request needs to be sent in the body of the request using JSON format. And should contain following key/value parameters

Parameter name	Default value	Mandatory	Type	Description
type	all	No	JSONArray	List of alert profile types
severity	all	No	JSONArray	List of severity
status	all	No	JSONArray	List of status

Response

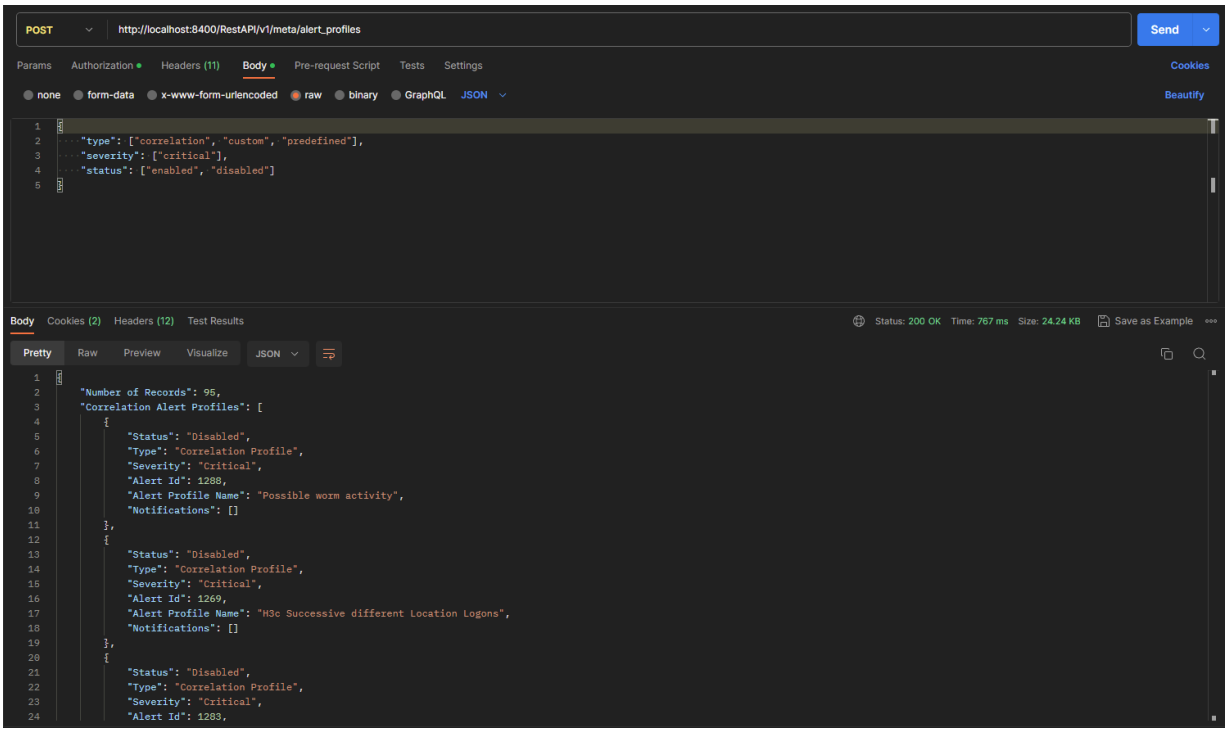
The response will be a JSON object which will contain the list of fields.

Parameter name	Description
Number of Records	The count of records in the fetched response data

Parameter name	Description
Profile Based Alerts	JSON Array of profile based alerts
Correlation Alert Profiles	JSON Array of correlation alert profiles

Example usage using cURL

Example usage using Postman (Third party tool)



9.4.9. Synchronous Alerts API

Last updated on: September 12, 2025

The API allows you to retrieval of alert data via EventLog Analyzer.
When you perform an api call with the synchronous alert method, your query will be sent to the EventLog Analyzer server, which will obtain all the results before returning it to you. The total time taken for the process depends on the number of search results obtained.
Here are the steps involved to execute a synchronous alert query:

- Create an alert request with a set of relevant metadata.
- The server executes the request on the request thread and responds with the result.
- The server responds with cursor when there are additional results to be displayed other than the predefined number of results that are displayed.
- You can keep requesting with the next cursor to get the next set of results. This needs to be done until all alert hits are consumed and the server doesn't send a cursor back.
- EventLog Analyzer's cursor stays live for five minutes, if not used.

Request URL

```
POST http://hostname:8095/RestAPI/v1/alerts
```

Request Header

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	AuthToken generated from API Settings page. e.g: Bearer nzxcvda0odmtmznloc00ndziltg0mgutmwzkhtljmjvmzbyt

Request Parameters

The request needs to be sent in the body of the request using JSON format. And should contain following key/value parameters

Parameter name	Default value	Mandatory	Type	Description
query	*	No	String	Start value of the list
alert_profiles	all	No	JSONArray	List of alert profiles

Parameter name	Default value	Mandatory	Type	Description
severity	all	No	JSONArray	List of severity
status	all	No	JSONArray	List of status
from	current time - 24 hours	No	Long	Start time for search in Unix milliseconds
to	current time	No	Long	End time for search in Unix milliseconds
cursor	-	No	String	Cursor from next query

Note

1. When the cursor is passed, the other parameters are not required.
2. Quotes i.e (" ") in query string should to be escaped. If query in EventLog Analyzer's search page is REMOTE_INTERFACE = "switch 1", then for Rest Api the query parameter should be written as "REMOTE_INTERFACE = \"switch 1\""

Response

The response will be a JSON object which will contain the following key/value pairs

Parameter name	Description
hits	JSON object which contain alert hits for the request Contains following fields hits: List of alert hits hits_count_in_current_page: Hits count in current alert hit response

Example usage using cURL

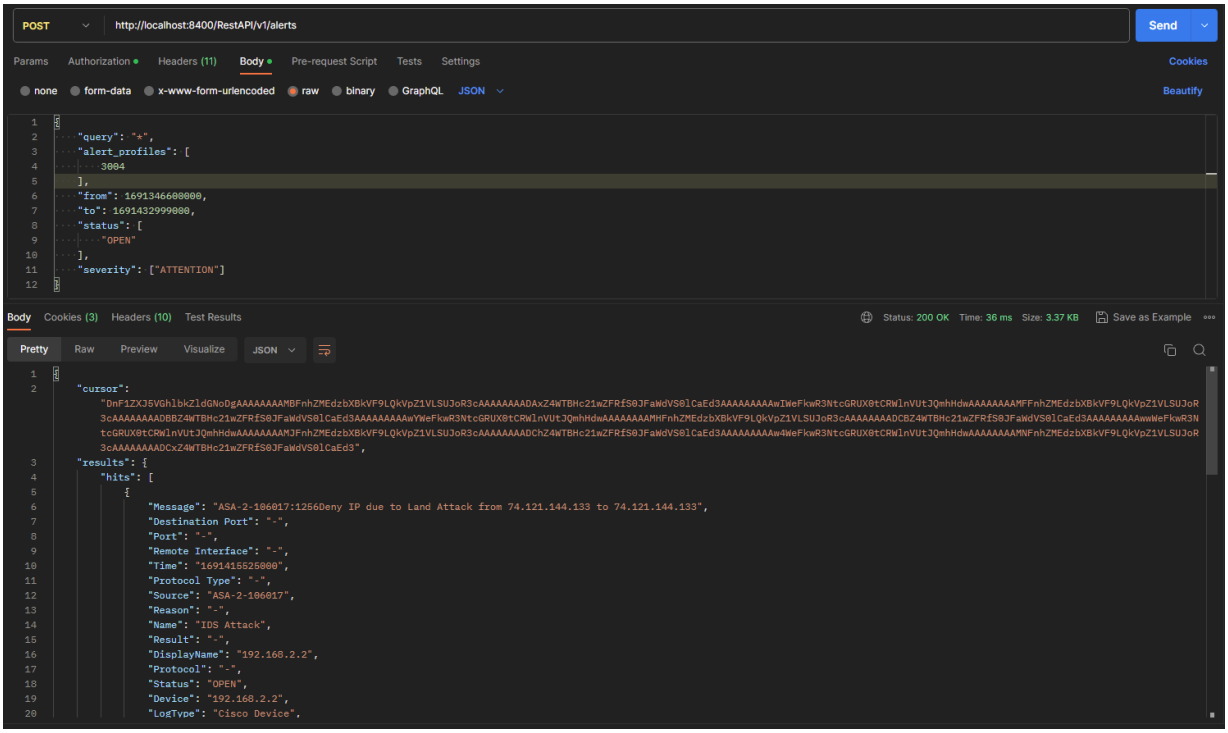
i) Search request with query

ii) Search request with cursor

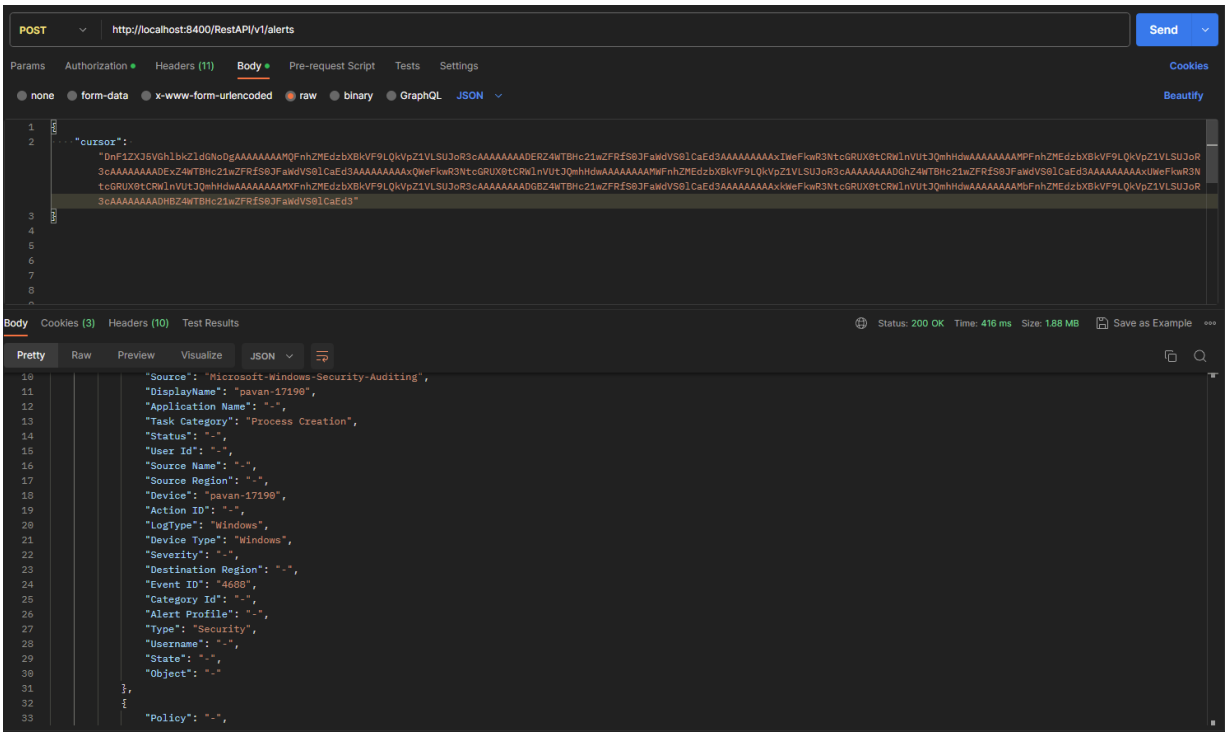
iii) Invalid Search query

Example usage using Postman (Third party tool)

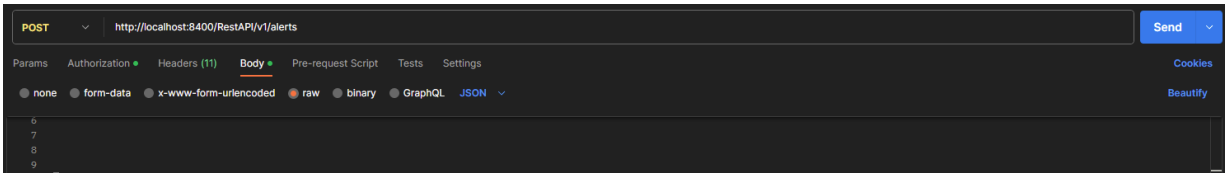
i) Search request with query

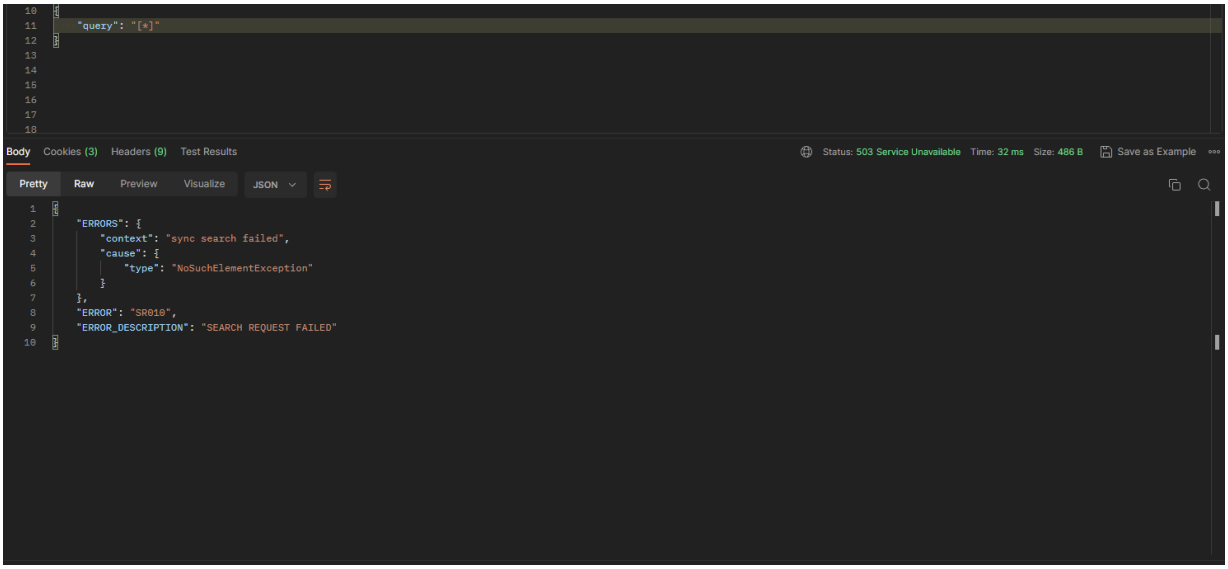


ii) Search request with cursor



iii) Invalid query




"query": "[*]"
Body
Cookies (3)
Headers (9)
Test Results
Status: 503 Service Unavailable
Time: 32 ms
Size: 486 B
Save as Example
Pretty
Raw
Preview
Visualize
JSON
"ERRORS": [
"context": "sync search failed",
"cause": {
"type": "NoSuchElementException"
},
"ERROR": "SR010",
"ERROR_DESCRIPTION": "SEARCH REQUEST FAILED"

9.4.10. Asynchronous Alerts API

Last updated on: September 12, 2025

The API allows you to run alert search requests in the background. With help of this you can monitor the progress of the request and view the results as and when they become available.
Here are the steps involved in executing an asynchronous alerts query:

- You can make a request with a set of required metadata and asynchronous parameters.
- The server will respond with a request ID and the search is performed in background thread.
- You can check the status of the request through the Jobs endpoint.
- Once the job is done, you can fetch the results using the jobs/results endpoint.
- The search results will be available in EventLog Analyzer for 24 hours after which they are deleted by the cleanup thread.

Synchronous Alerts	Asynchronous Alerts
It retrieves data within the retention period. The response time taken is based on data fetched.	It retrieves large amount of data based on the given criteria. The response will be a request ID and the search is performed in background thread
In order to acquire the next set of results, keep requesting with the next cursor.	Once the job is done, in order to acquire the next result page, search with the next page_no using the job results endpoint.
Response is valid only for 5 minutes.	Response will be valid upto 24 hours.

Request URL

```
POST http://hostname:8095/RestAPI/v1/alerts/async
```

Request Header

Header name	Value	Mandatory	Description

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	AuthToken generated from API Settings page. e.g: Bearer nzxcvda0odmtmznloc00ndziltg0mgutmwzkhtljmjvmzbyt

Request Parameters

The request needs to be sent in the body of the request using JSON format. And should contain following key/value parameters

Parameter name	Default value	Mandatory	Type	Description
query	*	No	String	Start value of the list
alert_profiles	all	No	JSONArray	List of alert profiles
severity	all	No	JSONArray	List of severity
status	all	No	JSONArray	List of status
from	current time - 24 hours	No	Long	Start time for search in Unix milliseconds
to	current time	No	Long	End time for search in Unix milliseconds

Note:

1. Quotes i.e (" ") in query string should to be escaped. If query in EventLog Analyzer's search page is REMOTE_INTERFACE = "switch 1", then for Rest Api the query parameter should be written as "REMOTE_INTERFACE = \"switch 1\""

Response

The response will be a JSON object which will contain the following key/value pairs

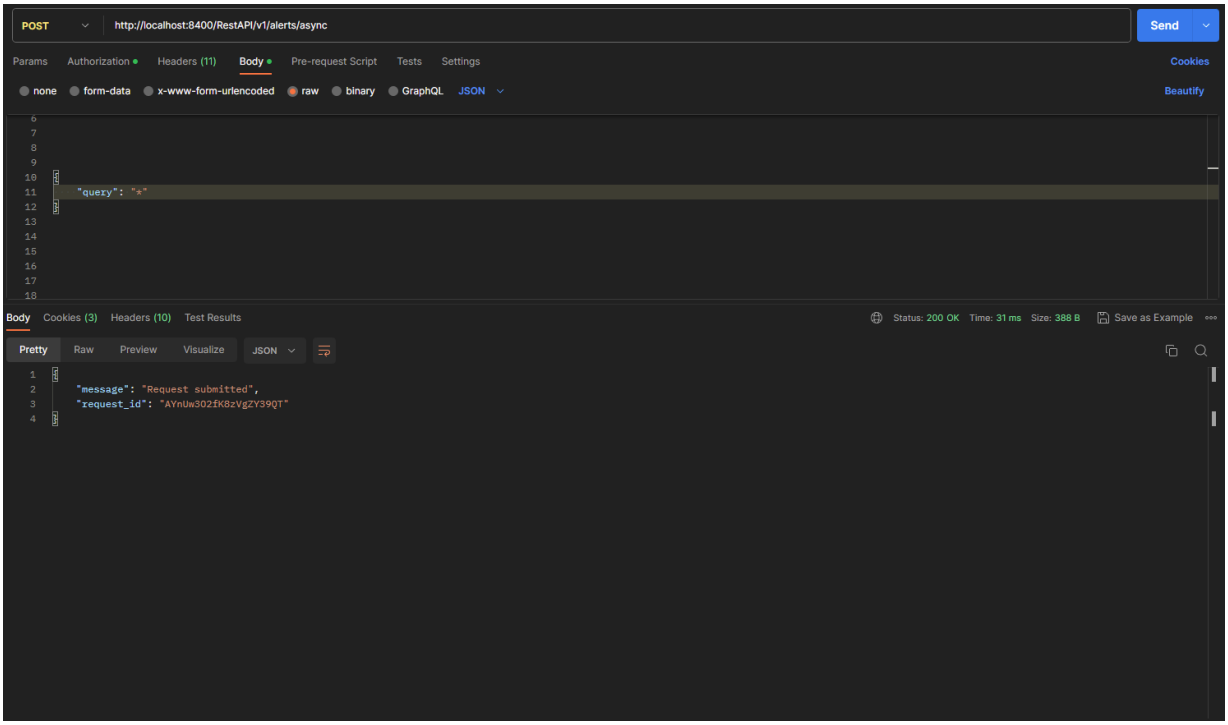
Parameter name	Description
hits	JSON object which contain search hits for the request Contains following fields hits: List of alert hits

Parameter name	hits_count_in_current_page: Hits count in current alert hit response Description

Example usage using cURL

i) Search request with query

Example usage using Postman (Third party tool)



9.4.11. Synchronous Search API

Last updated on: September 12, 2025

The API allows you to perform search against EventLog Analyzer.
When you perform a search with the synchronous search method, your query is sent to the EventLog Analyzer server, which will obtain all the results before returning it to you. The time taken for the process depends on the number of search results obtained.
Here are the steps involved in executing a synchronous search query:

- Create a search request with a set of relevant metadata.
- The server executes the request on the request thread and responds with the result.
- The server responds with cursor when more results are present.
- You can keep requesting with the next cursor to get the next result set. This needs to be done until all search hits are consumed and the server doesn't send a cursor back.
- EventLog Analyzer's cursor stays live for five minutes, if not used.

Request URL

```
POST http://hostname:8095/RestAPI/v1/search
```

Request Header

Header name	Value	Mandatory	Description
Authorization	Bearer {{AuthToken}}	Yes	AuthToken generated from API Settings page. e.g: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx

Request Parameters

The request needs to be sent in the body of the request using JSON format. And should contain following key/value parameters

Parameter name	Default value	Mandatory	Type	Description
query	*	No	String	Start value of the list
hosts	all	No	JSONArray	List of hosts to search
				List of device groups to

groups Parameter name	all Default value	No Mandatory	JSONArray Type	search Description
from	current time - 24 hours	No	Long	Start time for search in Unix milliseconds
to	current time	No	Long	End time for search in Unix milliseconds
cursor	-	No	String	Cursor from next query

Note

1. When the cursor is passed, the other parameters are not required.
2. Quotes i.e (" ") in query string should to be escaped. If query in EventLog Analyzer's search page is REMOTE_INTERFACE = "switch 1", then for Rest Api the query parameter should be written as "REMOTE_INTERFACE = \"switch 1\""

Response

The response will be a JSON object which will contain the following key/value pairs

Parameter name	Description
hits	JSON object which contain search hits for the request Contains following fields hits: List of search hits hits_count_in_current_page: Hits count in current search response

Example usage using cURL

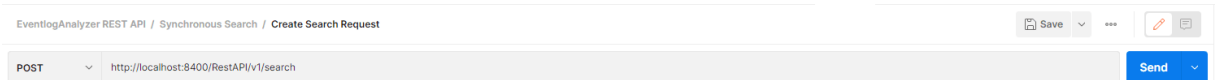
i) Search request with query

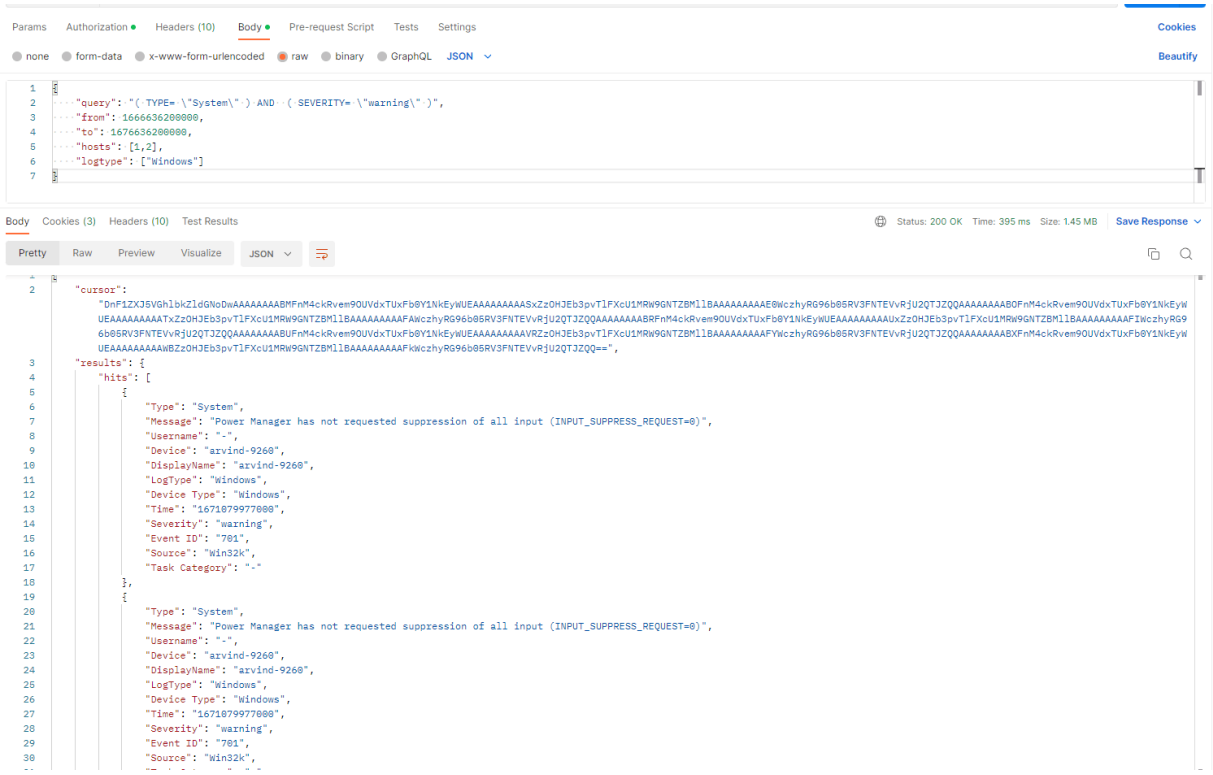
ii) Search request with cursor

iii) Invalid Search query

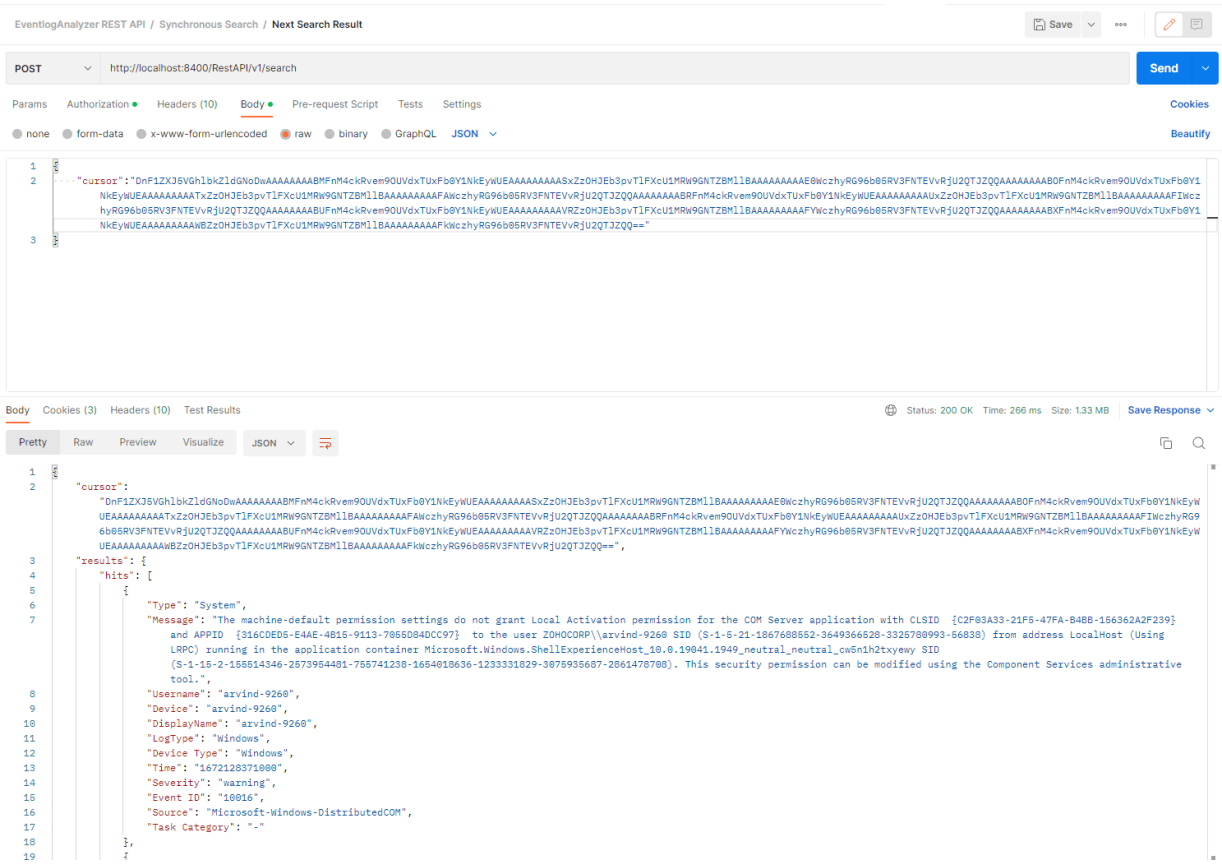
Example usage using Postman (Third party tool)

i) Search request with query

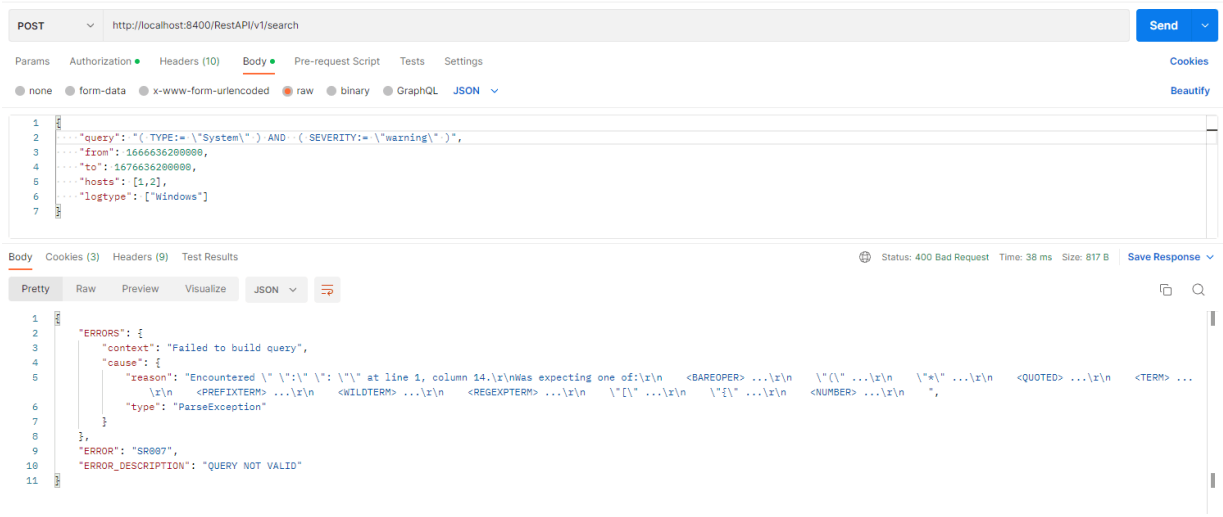




ii) Search request with cursor



iii) Invalid query


POST
http://localhost:8400/RestAPI/v1/search
Send
Params
Authorization
Headers (10)
Body
Pre-request Script
Tests
Settings
Cookies
none
form-data
x-www-form-urlencoded
raw
binary
GraphQL
JSON
Beautify
{
"query": "(TYPE:= \"System\") AND (SEVERITY:= \"warning\")",
"from": 1666636200000,
"to": 1676636200000,
"hosts": [1,2],
"logtype": ["Windows"]
}
Body
Cookies (3)
Headers (9)
Test Results
Status: 400 Bad Request
Time: 38 ms
Size: 817 B
Save Response
Pretty
Raw
Preview
Visualize
JSON
{
"ERRORS": {
"context": "Failed to build query",
"cause": {
"reason": "Encountered \" \":\" \": \"\" at line 1, column 14.\r\nWas expecting one of:\r\n <BAREOPER> ...\r\n \"(\" ...\r\n \"*\" ...\r\n <QUOTED> ...\r\n <TERM> ...\r\n <PREFIXTERM> ...\r\n <WILDTERM> ...\r\n <REGEXPTERM> ...\r\n \"[\" ...\r\n \"{\" ...\r\n <NUMBER> ...\r\n ",
"type": "ParseException"
}
},
"ERROR": "SR007",
"ERROR_DESCRIPTION": "QUERY NOT VALID"
}

9.5.1. System Settings

Last updated on: September 12, 2025

Carry out the necessary configurations required for setting up EventLog Analyzer.

The following are the system settings:

- Notification Settings
- Manage Account TFA
- Install EventLog Analyzer as a service
- Connection Settings
- Rebranding
- System Diagnostics
- Database Access
- Log Level Settings
- Port Management

9.5.2. Connection settings

Last updated on: September 12, 2025

In this page

Overview

What is SSL?

Certificates and Certifying Authority (CA)

SSL Certificate

Certifying Authority

Keystore

CSR

The Usual SSL Issuance Process

Configuring the SSL settings

General settings

Connection Type

General Settings

SSL Certification Tool

Case 1: Apply Certificate

Case 2: Generate Certificate

Proxy Settings

Extracting EventLog Analyzer SSL Certificate

SSL Troubleshooting Tips

These settings are used for general configuration related to product connections, such as access permissions, certificates, and proxy settings. These configurations enable secure access to the product server.

Overview

The SSL Settings page lets you configure secure communication between the product and client systems. By enabling SSL and managing certificates, you can ensure encrypted data transfer, prevent unauthorized access, and comply with security standards. The configuration options include selecting the connection type (HTTP/HTTPS), managing certificates through the built-in SSL Certification Tool, setting up a proxy server, and extracting EventLog Analyzer certificates when required.

What is SSL?

Acronym for Secure Socket Layer, SSL is an encryption technology to secure the data exchange between a website and its visitor's web browser. Normally, when a user communicates with a website, say submits his credit card information, the data travels to the server as plain text, which is susceptible to data theft!
On the other hand, if this data is encrypted, then no eavesdropper can read it! Thus, it's really very important to secure a website with SSL!

Certificates and Certifying Authority (CA)

SSL Certificate:

This is a digital identity of a company, which ensures that a visitor is talking only to its intended website, and whatever data he submitted to the site is encoded and reaches only the intended site. This system is analogous to banks recognizing their customers by their signatures. In this case, the browsers (thereby the end-users) are programmed to trust these CA presented certificates.

Certifying Authority:

- Regulatory organizations, who, with the help of standard policies, issue certificates to a domain, declaring them trustworthy. Every certificate they generate is unique to the company they are certifying, which makes identification easy.
- CAs secure all necessary information about a company before issuing a certificate for it and also keep updating it in their records, which adds to the trustworthiness.
- Some of the popular CAs are Verisign, Comodo & GoDaddy etc.

Keystore

Keystore is specifically designed to store various kinds of encryption information.

CSR

- In order for a CA to generate an SSL certificate for a company, it first collects the information about the company and other identifiers such as public key (digital signature), and then binds them all with its certificate (which could be a piece of encrypted token or something similar). In doing so, it generates a unique identifier for the company.
- Thus every certificate issuance process begins with a "certificate request" from the company. CAs refer to this process as "Certificate Signing Request" (CSR). The CAs accept the company information and digital signatures in a special form of file - the ".csr" file.

The usual SSL issuance process

It involves 3 steps:

- First you generate a CSR and submit it to CA.
- CA binds this CSR with its digital signatures and returns it.
- Now, you bind all this with your company domain.

Configuring the SSL settings

1. In the product console, navigate to the Settings tab and click on Connection Settings listed under System Settings as shown in the below image.

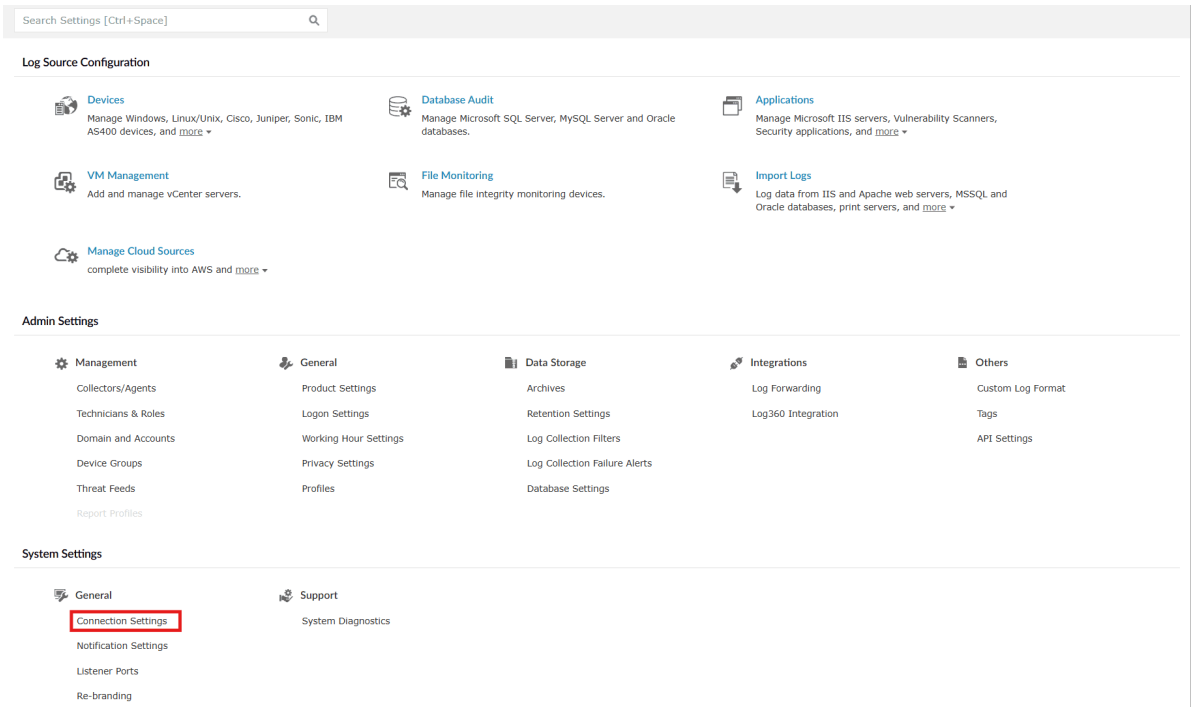


Image 1: Configuring connection settings via the settings tab

> **NOTE**
>
> You can also access these settings via the Enforce HTTPS configuration in the Security Hardening module. Refer to the Product Settings help document to learn more.

2. The Connection Settings module will be displayed on the screen consisting of three sub-tabs:
   - General settings
   - SSL Certification Tool
   - Proxy settings

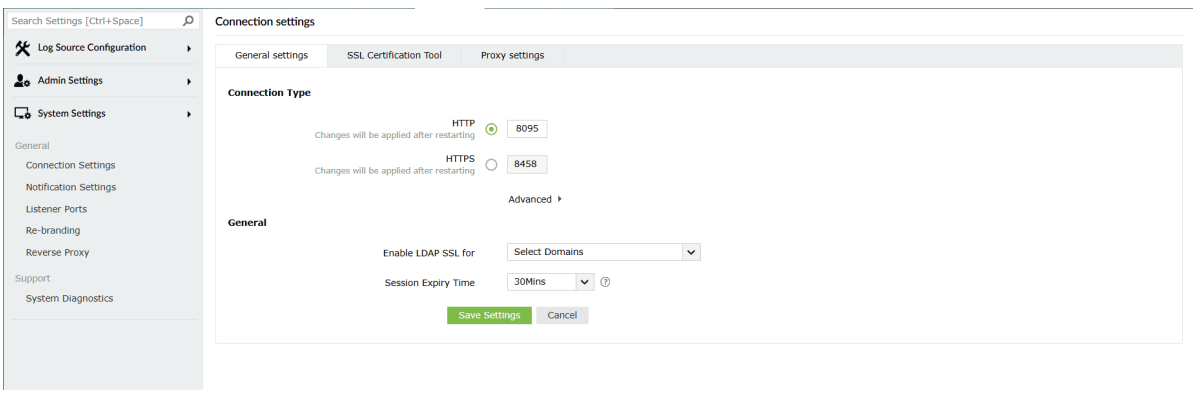


Image 2: Connection settings configurations

Read further to know how to configure these settings.

General settings

This tab covers the general product settings, including options to configure the web server port, supported protocols, TLS, and session expiry time.

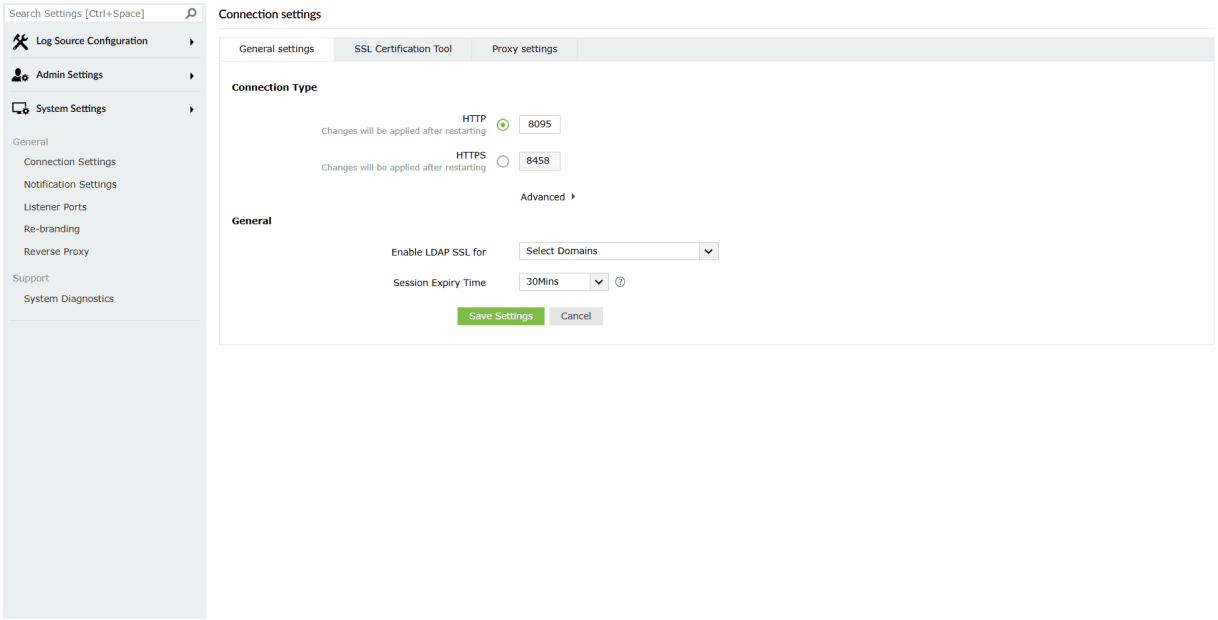


Image 3: General settings under connection settings

Connection Type

1. Choose your connection type. You can choose to use either HTTP or HTTPS.
2. Specify the port number of your choice after choosing the type of connection.

> NOTE
>
> The HTTP and HTTPS port numbers should be different from each other.

   The default ports are- HTTP: 8095, HTTPS: 8458.
3. Click on Advanced for advanced settings.

   Case 1: HTTP

Case 1: HTTP

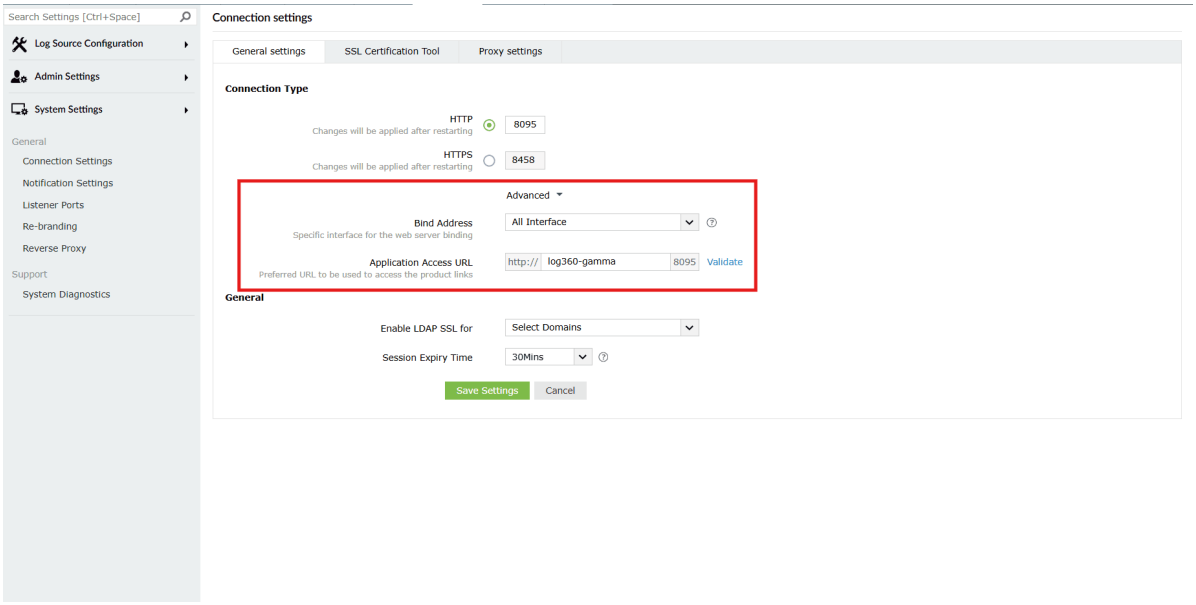


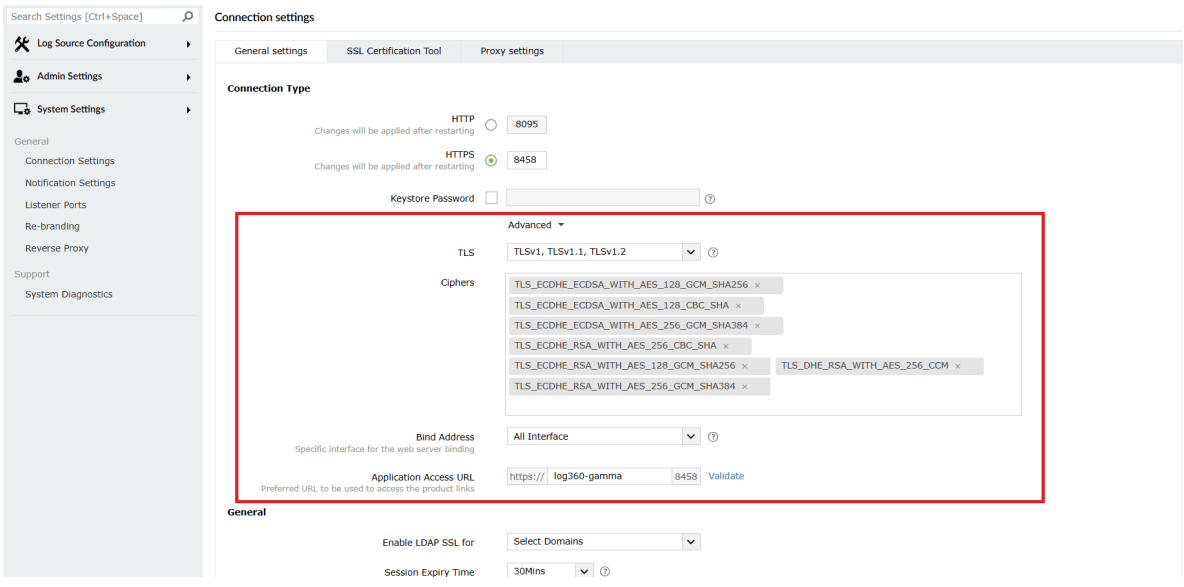
Image 4: Configuring connection type in general settings tab

Configure the advanced options for HTTP:

- Bind Address : Select the IP address to which the product's web port and its underlying listeners should be bound with. You can choose 10.71.24.153. You can choose from the bind addresses that are provided in the drop-down.
- Application Access URL : Specify the DNS (Domain Name System) host name using which network communication would take place between agents. Click on Validate. After a successful validation, the result will be visible as Success.

Case 2: HTTPS

In the case of HTTPS, there is an additional field called Keystore Password. If you require the keystore password to be encrypted, enable this option and provide the required password. The keystore password will be encrypted and stored. The field becomes available for editing once you click on its corresponding checkbox.



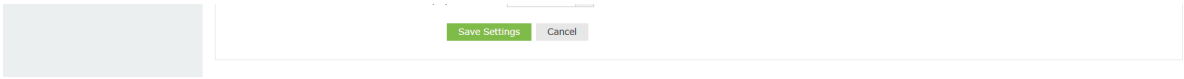
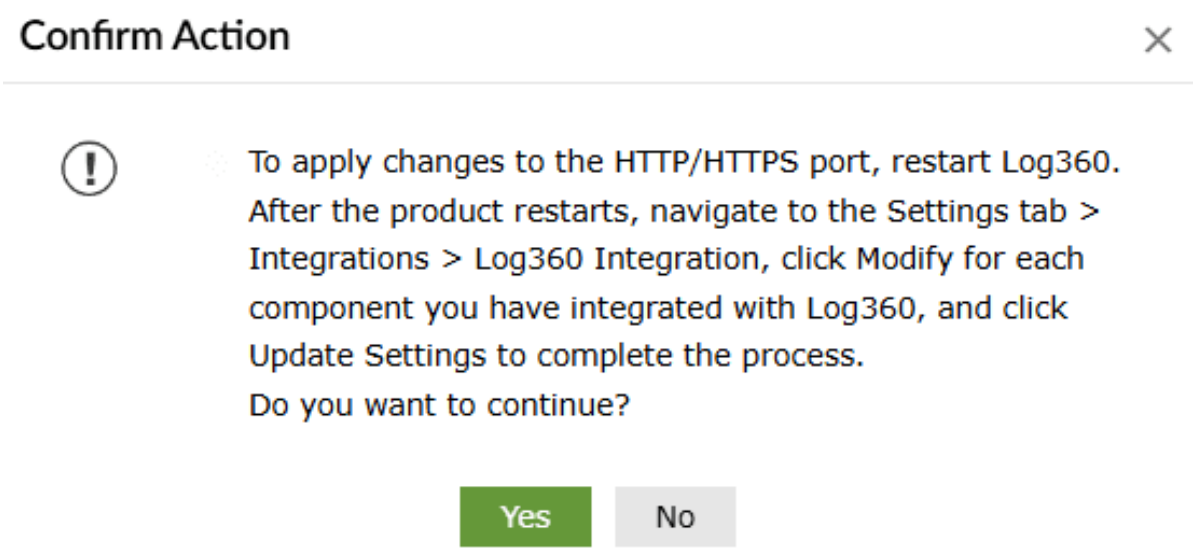


Image 5: Configuring connection type in general settings tab

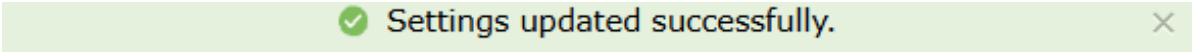
Configure the advanced options for HTTPS:

- TLS: From the drop-down available choose any/multiple TLS (Transport Layer Security) protocols to bound with the product's server.
- Ciphers: Select the respective cipher suites compatible with the Above selected TLS version. The list of default ciphers supported in Log360 and EventLog Analyzer are:
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CCM
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- Bind Address : Select the IP address to which the product's web port and its underlying listeners should be bound with. You can choose from the bind addresses that are provided in the drop-down.
- Application Access URL : Specify the DNS host name using which network communication would take place between agents. Click on Validate. After a successful validation, the result will be visible as Success.

4. Click on Save Settings. For the updated configurations to come into effect, the product must be restarted. A Confirm Action pop-up appears for the same. Click on Yes.

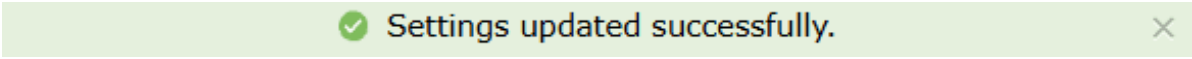


5. Upon successful completion of action, the below pop-up appears.



General

1. Enable LDAP SSL for: To configure LDAP SSL (Lightweight Directory Access Protocol over Secure Sockets Layer), click on the drop-down to view the list of domains to enable this setting for by ticking the checkbox.
2. Session Expiry Time: Select the, maximum duration for which a user session can stay idle, following which it expires. The available time intervals are 15Mins, 30Mins, 45Mins, 1Hrs, 2Hrs, 3Hrs and Never. For the updated configurations to come into effect, the product must be restarted.
3. Click on Save Settings to store the configured settings.
4. Upon successful completion of action, the below pop-up appears.



5. For the updated configurations to come into effect, the product must be restarted.

SSL Certification Tool

This tab allows you to apply SSL certificates, either by generating a self-signed certificate or by importing your own certificate.

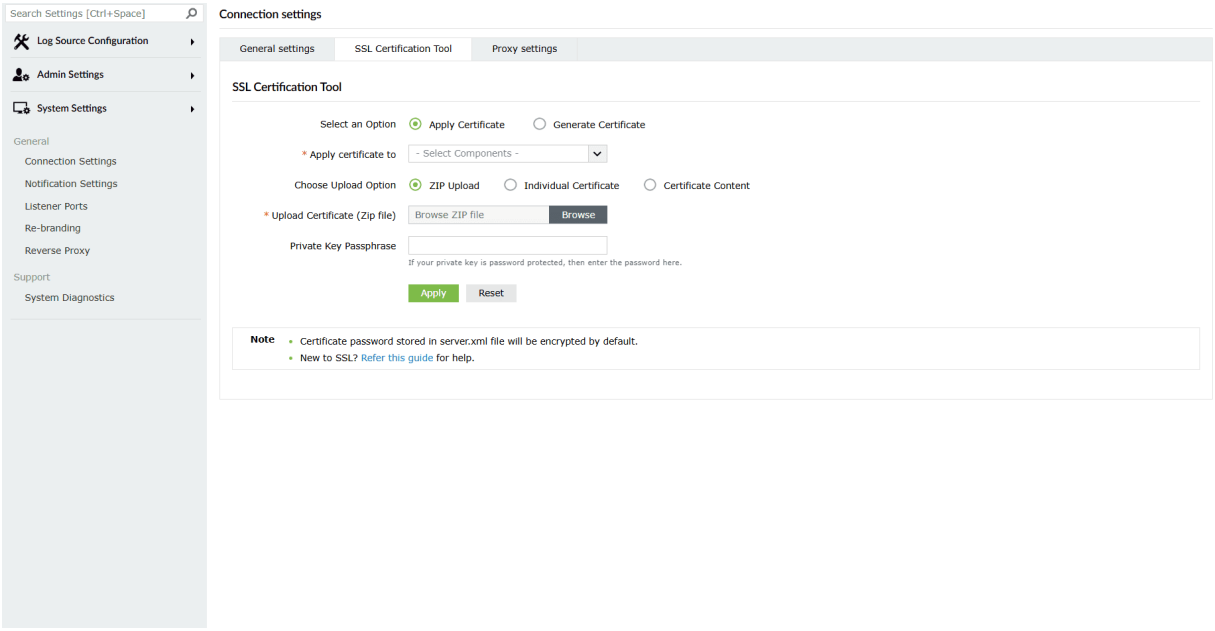


Image 6: Apply SSL certificates via connection settings

The Select an Option field contains options based on two cases:

- Apply Certificate: Click on this option in the case where you already have an SSL certificate.
- Generate Certificate: In the case where you do not have an existing certificate, click on this option to generate an SSL certificate upon completion of which, you can follow the steps from the Apply Certificate option.

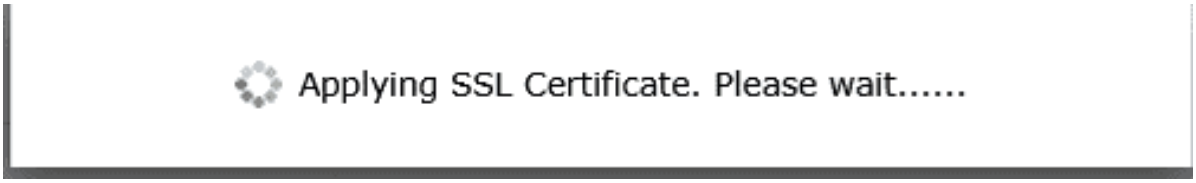
Case 1: Apply Certificate

If you already have a SSL certificate, follow the steps listed below to apply it.

- Apply certificate to: In the drop-down, select the component for which you want to apply the SSL certificate.
- Choose Upload Option: Choose an upload option based on the certificate file type.
  - ZIP upload:
    - If your CA has sent you a ZIP file, then select ZIP Upload, and upload the file.
    - If your CA has sent you individual certificate files—user, intermediary, and root certificates, then you can put all these certificate files in a ZIP file and upload them.
  - Individual Certificate:
    - If your CA has sent you just one certificate file (PFX or PEM format), then select Individual Certificates, and upload the file.
    - If your CA has sent the certificate content, then paste the content in a text editor and save it as a CER, CRT, or PEM format, and upload the file.
  - Certificate Content:
    - If your CA has sent just the certificate content, then choose this option and paste the entire content in the Paste Certificate Content field.
- Upload Certificate/Paste Certificate Content: Based on the upload option, upload your certificate in this field.
- Private Key Passphrase: If the certificate contains a password-protected private key, enter the password in this field.

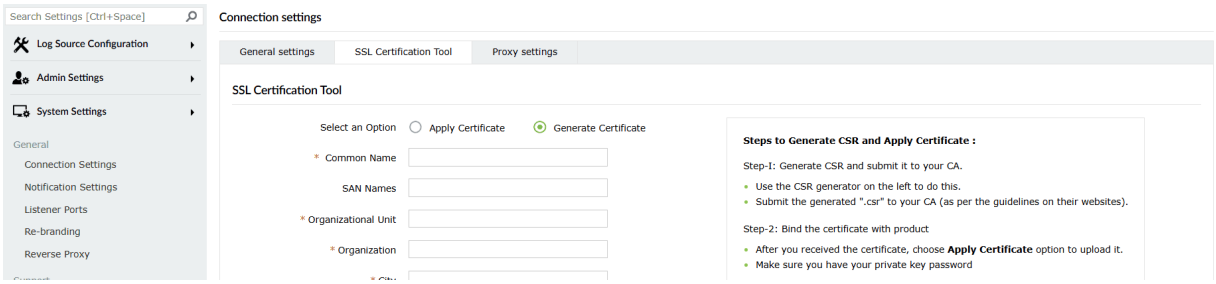
> NOTE
>
> : Only Triple DES encrypted private keys are currently supported.

- Click on Apply. The below pop-up appears briefly.



- Finally, restart the product.

Case 2: Generate Certificate



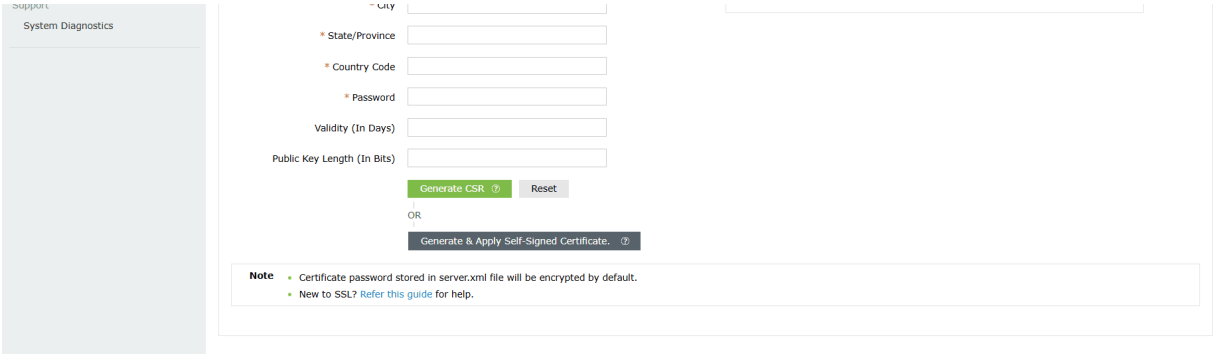


Image 7: Generate SSL certificate via connection settings

If you don't have an SSL certificate, select the Generate Certificate option and fill the required fields as listed below:

- Common Name: Enter the name of the server. Example: For the URL https://servername:9251, the common name is servername.
- SAN Names: Subject Alternative Name (SAN) allows you to specify additional host names for a single SSL certificate. Use a comma to separate multiple values.
- Organizational Unit: Enter the department's name which you want to be displayed in the certificate.
- Organization: Enter the legal name of your organization.
- City: Enter the name of the city as provided in your organization's registered address.
- State/Province: Enter the name of the state or province as provided in your organization's registered address.
- Country Code: Enter the two letter code of the country where your organization is located.
- Password: Enter a password to secure the keystore. It should be at least 6 characters. You will be asked to enter this password while installing the signed certificates. For self-signed certificates, by default, the password is encrypted.
- Validity (In Days): Specify the number of days for which the SSL certificate will be considered valid.

  NOTE

  When no value is entered, by default, the certificate will be considered to be valid for 90 days.

- Public Key Length (In Bits): Specify the size of the public key. Larger the size, the stronger the key. Default size is 2048 bits, which can only be incremented in multiples of 64.

  NOTE

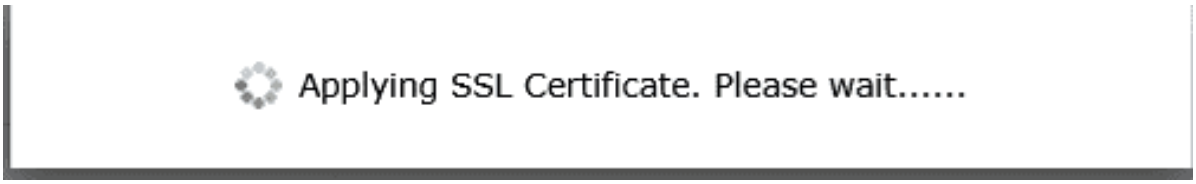
  The default value is 2048 bits and its value can only be incremented in multiples of 64.

- After all values have been entered, you can select either of these two options:
  - Generate CSR: This method allows you to generate the CSR file and submit it to your CA (Certificate

Authority). Using this file, your CA will generate a custom certificate for your server.

- Click Download CSR or manually get it by going to the <Install_dir>\Certificates folder.
- Once you have received the certificate files from your CA, follow the steps listed under Apply Certificate to apply the SSL certificate.

- Generate & Apply Self-signed Certificate: This option allows you to create a self-signed certificate and apply it instantly to the product. However, self-signed SSL certificates come with a drawback. Anyone accessing the product secured with a self-signed SSL certificate will be shown a warning telling them that the website is not trusted, which may cause concern.



- After completion of this process, you can follow the steps under Apply Certificate.

Proxy settings

This setting allows you to configure a proxy server for accessing the product server.

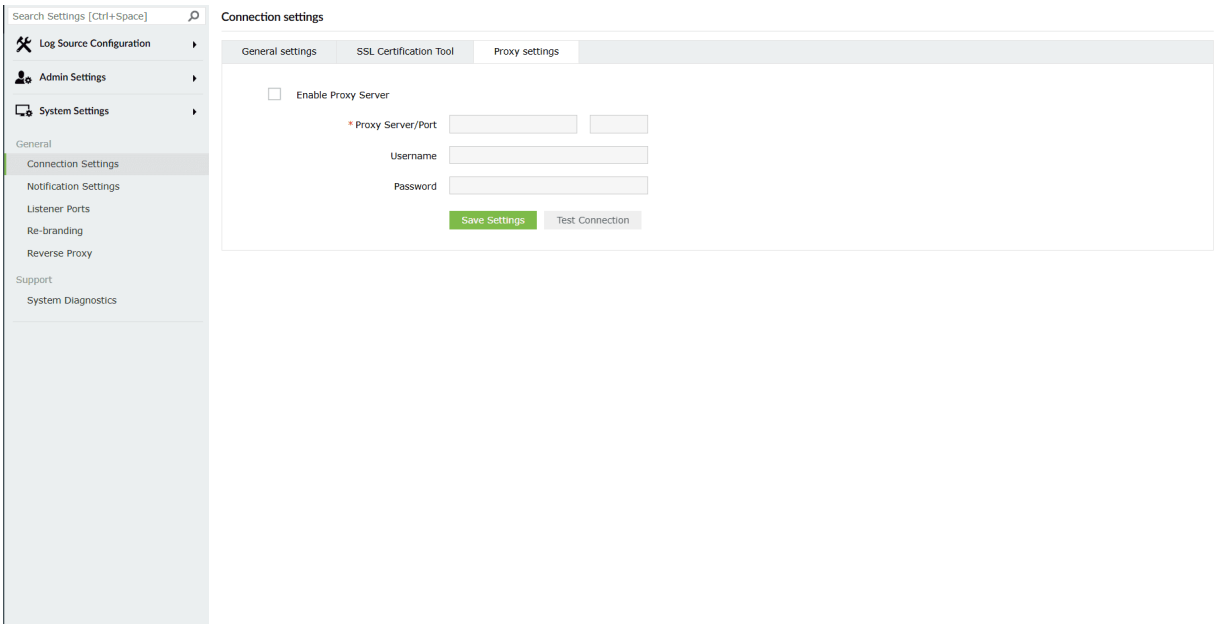


Image 8: Configuring proxy settings via connection settings

- Select the Enable Proxy Server check box. The required fields will then be marked as available to edit/configure.
- Configure the server by entering Proxy Server Name/Port, Username, and Password in the provided fields.
- Click on Save Settings to save the configured proxy server.
- Click on the Test Connection button for a verification if the proxy server is able to connect from the product server

Extracting EventLog Analyzer SSL certificate

This guide provided in this section is specific for only EventLog Analyzer console
If you are currently using the Log360 component EventLog Analyzer and if it utilizes a self-signed certificate, proceed as follows to extract the certificate in the desired format.
If a self-signed certificate hasn't been generated through EventLog Analyzer's certification tool, begin by generating the certificate through the tool, then continue with the subsequent steps.

```
PRODUCT_LOCATION/jre/bin/keytool -exportcert -keystore
PRODUCT_LOCATION/conf/server.p12 -storetype PKCS12 -storepass STOREPASS -alias
ALIAS -file CERTIFICATE.crt
```

Replace the placeholders accordingly:

- STOREPASS: Password used during self-signed certificate generation.
- ALIAS: Common name used during self-signed certificate generation.
- CERTIFICATE: Desired name for the certificate file.

Import SSL Certificate into EventLog Analyzer trust store:

Use the following command to import the certificate into the trust store of the desired product.

```
PRODUCT_LOCATION/jre/bin/keytool -import -noprompt -trustcacerts -alias ALIAS -file
CERTIFICATE.crt -keystore PRODUCT_LOCATION/jre/lib/security/cacerts -storepass changeit
```

Replace the placeholders accordingly:

- ALIAS: Suitable alias for the certificate.
- CERTIFICATE: Certificate to be imported.

SSL Troubleshooting Tips

This section helps you troubleshoot SSL server certificate–related issues that you might encounter in the product console.

1. Blocked Content

Description:
This problem arises when the product console is configured to use HTTPS under connection settings while an integrated component is still configured to use HTTP. As a result, the component cannot be accessed from the

apps pane.
Resolution:
If the product console uses HTTPS, all integrated components must also be configured to use HTTPS (SSL) for successful access.

2. Certificate Name Mismatch

Description:
This error occurs when the common name of the SSL certificate does not exactly match the hostname of the server hosting the product console.
Resolution:
Obtain a new SSL certificate for the current hostname of the server.

3. Hostname Mismatch

Description:
This error occurs when the SSL certificate of a component is issued for a hostname that differs from the hostname of the product console. For example, the console could be installed on a parent domain while a component runs on a child domain.
Resolution:
Configure a valid SSL wildcard certificate and apply it to both the product console and the component.

4. Invalid Certificate

Description:
This error occurs when the SSL certificate configured with the product console is invalid (for example, expired or improperly issued).
Resolution:
Reconfigure the product console to use a valid SSL certificate.

5. Problem Trusting the Security Certificate

Description:
This error occurs when a component integrated with the product console is running on an older build.
Resolution:
Upgrade all integrated components to the latest build.

6. Certificate Not Trusted by JVM (Advanced Scenario)

Description:
This exception occurs when you configure an SMTP mail server or web server with SSL in the product console and the server uses a self-signed certificate. The Java Runtime Environment (JRE) bundled with the console does not trust self-signed certificates unless explicitly imported.
Resolution:
You need to import the self-signed certificates used by the server in the JRE package used by the product console. Follow the steps given below:
Step 1: Download the certificate
For SMTP servers:

Note

To download the certificate used by SMTP server, you must have OpenSSL installed. You can download it from here.
Open the command prompt and change to the bin folder in the OpenSSL installed location.
Now run the following command,
openssl.exe s_client -connect SMTPServer: Portno -starttls smtp > certificatename.cer

- For example, openssl.exe s_client -connect smtp.gmail.com:587 -starttls smtp > gmailcert.cer

For Web Servers:

- Open the web URL in a browser.
- Click the padlock icon on the address bar.
- Click More Information. This opens the Certificate Viewer window showing the certificate used by that web server.
- Click View Certificate.
- When the Certificate window showing Certificate Information Authority opens, click the Details tab.
- Click Copy to File.
- In the Certificate Export Wizard that opens, click Next.
- Select the format as DRE encoded binary X.509 (.CER) and click Next.
- Enter the path where you wish to save the file and click Finish.

Step 2: Import the certificates in JRE package of the product console.

- Open a command prompt and change to the \jre\bin folder. For example: C:\ManageEngine\product console name\jre\bin.
- Run the following command,

```
Keytool -importcert -alias myprivateroot -keystore ..\lib\security\cacerts -file
```

- For example: Keytool -importcert -alias myprivateroot -keystore ..\lib\security\cacerts -file C:\smtpcert.cer
- Enter changeit when prompted for a password.
- Enter y when prompted Yes or No.
- Close the command prompt and restart the product.

For certificates signed by Public Certificate Authority

If the certificate is signed by Public Certificate Authority, follow the steps below:

- Open browser settings
- Open Privacy / Privacy and Security Tab
- Under Security Tab, click on Manage Certificates.

- Please make sure the CA certificate is not under Untrusted Publishers.
- If the certificate is not under Untrusted Publishers, open the Trusted Root Certification Authorities tab to check if the Public Certification Authority you signed is available.
- If it is not available, please import the Certification Authority certificate and restart the browser.

For certificates signed by a Local Certificate Authority or it is self signed

If the web client is accessed under Domain machine, Please follow the below steps.

- Start the Group Policy Management snap-in.
- Right-click the respective GPO, and then click Edit.
- Open Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies, right-click Trusted Root Certification Authorities, and then click Import.
- On the Welcome to the Certificate Import Wizard page, click Next.
- On the File to Import page, choose the certificates, and then click Next.
- On the Certificate Store page, click Place all certificates in the following store, and then click Next.
- On the Completing the Certificate Import Wizard page, verify that the information you provided is accurate, and then click Finish.

If the web client is accessed under a Non-domain machine, Please follow the below steps.

- Open Browser settings
- Open Privacy / Privacy and Security Tab
- Under Security Tab, click on Manage Certificates.
- In the Certificates popup, open Trusted Root Certification Authorities.
- Please import the Certification Authority certificate and restart the browser.

For certificates signed by Public Certificate Authority

If the certificate is signed by Public Certificate Authority, follow the steps below:

- Open browser settings
- Open Privacy / Privacy and Security Tab
- Under Security Tab, click on Manage Certificates.
- Please make sure the CA certificate is not under Untrusted Publishers.
- If the certificate is not under Untrusted Publishers, open the Trusted Root Certification Authorities tab to check if the Public Certification Authority you signed is available.
- If it is not available, please import the Certification Authority certificate and restart the browser.

For certificates signed by a Local Certificate Authority or it is self signed

If the web client is accessed under Domain machine, Please follow the below steps.

- Start the Group Policy Management snap-in.
- Right-click the respective GPO, and then click Edit.

- Open Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies, right-click Trusted Root Certification Authorities, and then click Import.
- On the Welcome to the Certificate Import Wizard page, click Next.
- On the File to Import page, choose the certificates, and then click Next.
- On the Certificate Store page, click Place all certificates in the following store, and then click Next.
- On the Completing the Certificate Import Wizard page, verify that the information you provided is accurate, and then click Finish.

If the web client is accessed under a Non-domain machine, Please follow the below steps.

- Open Browser settings
- Open Privacy / Privacy and Security Tab
- Under Security Tab, click on Manage Certificates.
- In the Certificates popup, open Trusted Root Certification Authorities.
- Please import the Certification Authority certificate and restart the browser.

Read also

This document explained how to configure SSL settings in Log360 and EventLog Analyzer, including connection types, certificate management, proxy configuration, and extracting certificates. For more information, refer to the following pages:

- How to update the web server port
- Database settings

9.5.3. Notification Settings

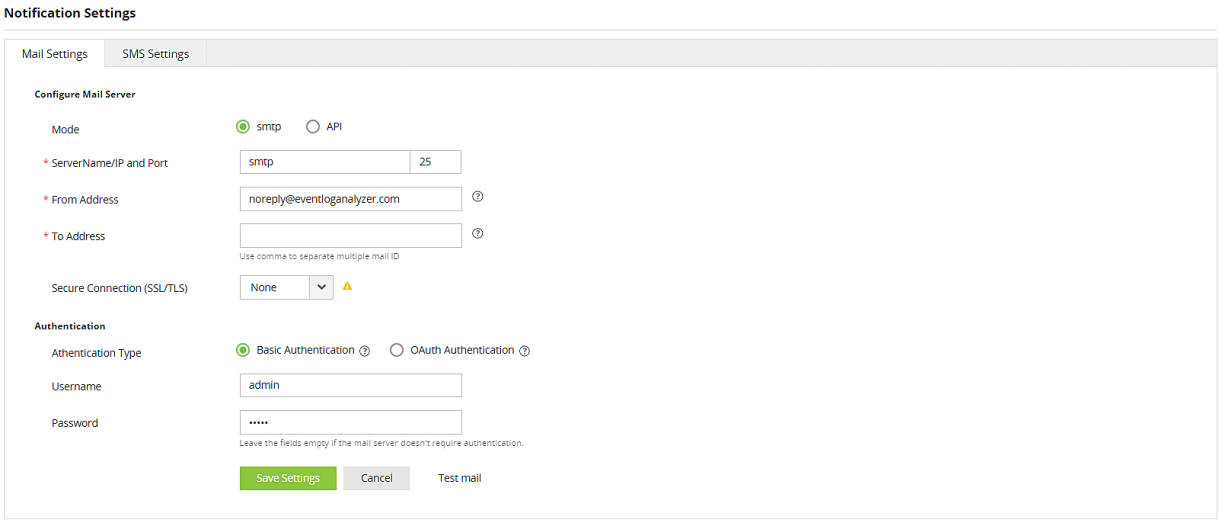
Last updated on: September 12, 2025

EventLog Analyzer distributes the scheduled and automatically-generated reports to users via email. It notifies users with alerts via both email and SMS.
The email and SMS settings can be configured according to your environment's requirements.

Email Settings

To configure or change email settings,

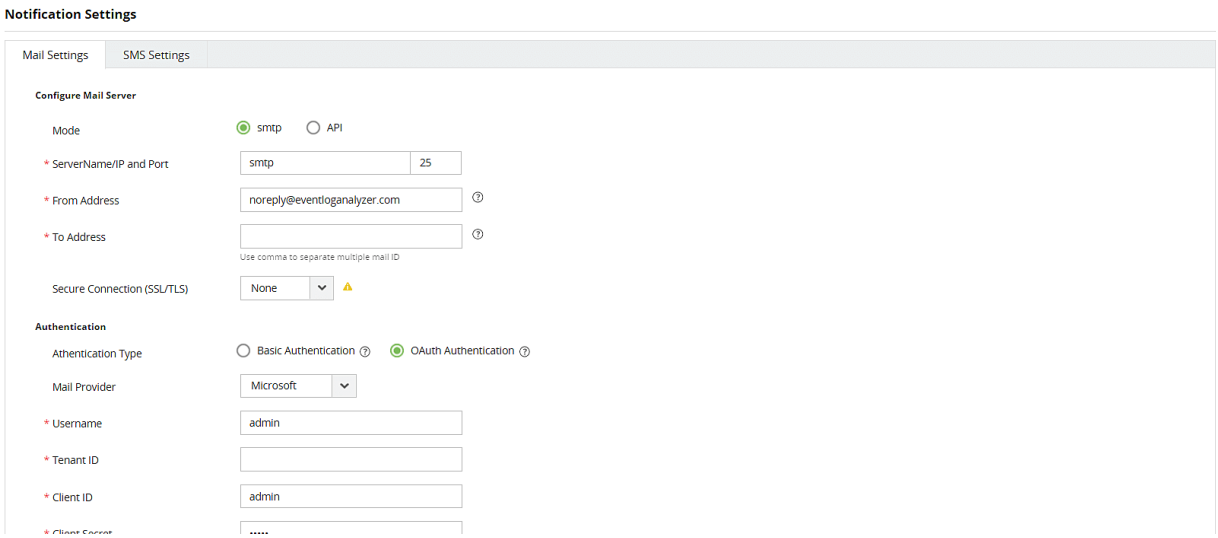
- Navigate to Settings > System Settings > Notification Settings > Mail Settings.

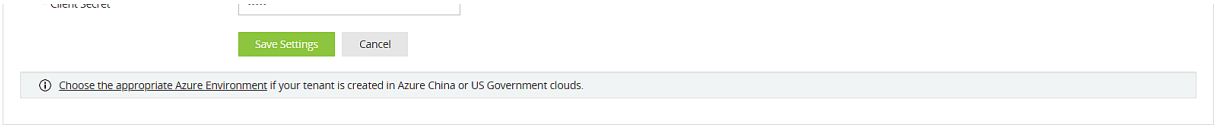


EventLog Analyzer provides two modes of mail server configuration:

- SMTP
- API

SMTP





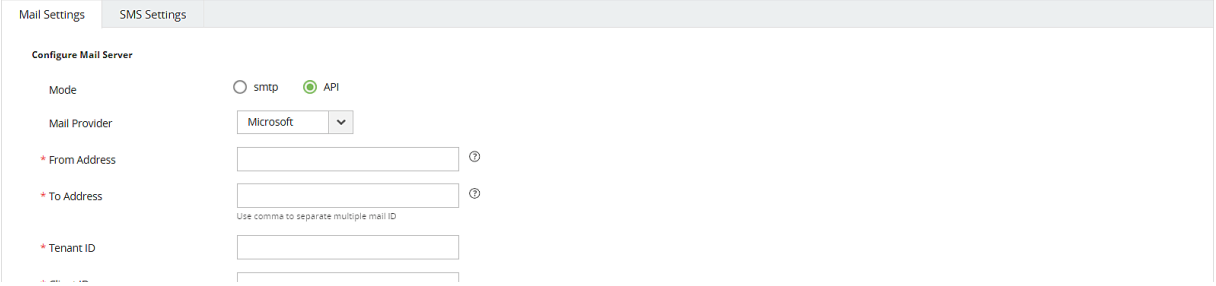
This method allows you to create and authenticate a mail server via Basic or OAuth authentication.

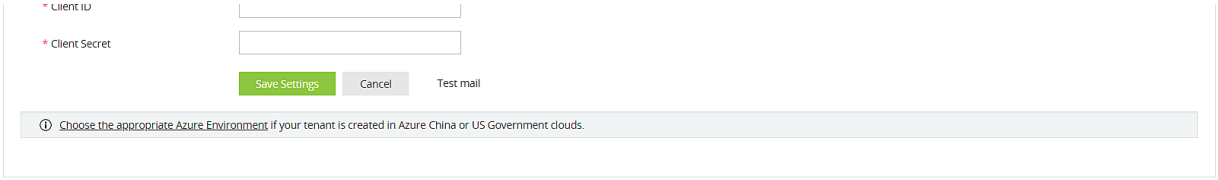
To configure an SMTP mail server,

1. In the field, select SMTP.
2. Enter your mail server's Server Name or IP, and Port Number in the respective fields.
3. In the From Address field, enter the email address that will be used to send out notifications, alerts, etc., from eventLog Analyzer.
4. In the To Address field, enter your email address if you wish to receive notifications for the emails sent from eventLog Analyzer.
5. Select the connection security type from the available options: SSL, TLS, or None.
6. Select the authentication type from the options provided:
   - Basic authentication
   - OAuth authentication
7. Basic authentication
   - Enter the Username and Password to access the mail server.
   - If your mail server does not require authentication, leave the fields empty.
8. OAuth authentication
   - Select your mail provider from the available options: Microsoft or Google.
   - If your mail provider is Microsoft, provide the Username, Tenant ID, Client ID, and Client Secret in the respective fields. In eventLog Analyzer, the Azure Cloud is considered the default Azure environment. You can modify the Azure environment setting by clicking the Choose the appropriate Azure environment link.

     > **Note**
     >
     > To learn how to find your Azure Tenant ID, Client ID, and Client Secret, click here.

9. If you have selected Basic Authentication in step 6, you can have Log360 send a test email by clicking the Test Mail button.
10. Click Save Settings to save your mail server configuration.





API

This method allows you to create and authenticate a mail server via your mail provider's API.

- In the Mode field, select API.
- Select your mail provider from the available options: Microsoft or Google.
- In the From Address field, enter the email address that will be used to send out notifications, alerts, etc., from eventLog Analyzer.
- In the To Address field, enter your email address if you wish to receive notifications for the emails sent from eventLog Analyzer.
- If your mail provider is Microsoft, provide the Tenant ID, Client ID, and Client Secret in the respective fields. In EventLog Analyzer, the Azure Cloud is considered the default Azure environment. You can modify the Azure environment setting by clicking the Choose the appropriate Azure environment link.

> **Note**
>
> To learn how to find your Google Tenant ID, Client ID, and Client Secret, click here.

- If your mail provider is Google, upload the JSON private key file.

> **Note**
>
> To learn how to get your JSON private key file, click here.

- Click Save settings.

Steps to find your Azure Tenant ID, Client ID, and Client Secret for SMTP mail server configuration

- Log in to portal.azure.com.
- Under Azure services, click App registrations → New registration.
- Provide a Name of your choice and select the Supported account types. (Leave it as default).
- In the Redirect URI field, select web & paste the following OAuth link: https://identitymanager.manageengine.com/api/public/v1/oauth/redirect (or) You can also add the localhost redirect API in the following syntax. protocol://localhost:port_number/context_if_any/RestAPI/WC/OAuthSetting For example, http://localhost:8095/event/RestAPI/WC/OAuthSetting. If you have only added localhost as the redirect URI, you must access the product using localhost to configure mail server

you must access the product using localhost to configure mail server.

- On the next page, you will find the application details. Copy the Client ID & Tenant ID.
- From the left pane, click Certificates & secrets → New client secret.
- Provide a Description for the client secret, and in the Expires field, choose the validity of the client secret and click Add.
- The client secret will be generated. Copy the string displayed under Value.
- Click Save setting and complete the authorization prompt.

Steps to find your Google Workspace Client ID, and Client Secret for SMTP mail server configuration

- Log in to console.developers.google.com.
- In the dashboard, click Create to create a new project if there is no existing project or select any existing project and click New Project.
- Enter the Project Name. In the Location field, click Browse and select the parent organization. Click Create.
- In the left pane of the displayed project details page, click APIs & Services → Library.
- From the available list of APIs, select Gmail API and click Enable. You can use the search option to find the API quickly.
- In the left pane, click OAuth consent screen and choose the User Type. If you don't have a Google workspace account, choose External User.
- Provide the Application Name, Application Logo, and the support email of your help desk, developer information, and click Save & continue.
- Click Add or Remove Scopes, choose Gmail API (https://mail.google.com/), and click Update. Then, click Save & Continue.
- Add a test user and click Save & continue.
- In the left pane, click Credentials → Create Credentials → OAuth Client ID.
- Select the application type as Web Application. Provide a name of your choice.
- In the Authorized Redirect URIs, paste the following OAuth link: https://identitymanager.manageengine.com/api/public/v1/oauth/redirect (or) You can also add localhost redirect API in the following pattern. protocol://localhost:port_number/context_if_any/RestAPI/WC/OAuthSetting For example, http://localhost:8095/event/RestAPI/WC/OAuthSetting. If you have only added localhost as the redirect URI, you must access the product using localhost to configure the mail server.
- Click Save.
- Click DOWNLOAD JSON to download the file containing the authorization server details. Copy the Client ID and Client Secret displayed on the screen.

Steps to find your Azure Tenant ID, Client ID, and Client Secret for API mail server configuration

- Log in to portal.azure.com.
- Under Azure services, click App registrations → New registration.

- Under Azure services, click App registrations → New registration.
- Enter a Name of your choice and choose the Supported account types. (If you're unsure about the supported account types, select Accounts in the organizational directory only).
- In the left pane, click API Permission → Add a permission.
- Click Microsoft Graph → Application permission.
- Search Mail and select the permission Mail.Send. Click Add Permission.
- Click Grant admin consent.
- Copy the Client ID & Tenant ID displayed.
- In the left pane, click Certificates & secrets → New client secret.
- Provide a Description for the client secret. In the Expires field, choose the validity of the client secret and click Add.
- The client secret will be generated. Copy the string displayed under Value.

Steps to download JSON private key for API mail server configuration

- Log in to console.developers.google.com.
- Open the Service accounts page.
- Click Create Project. Enter the project name, organization and location. Click Create.
- Click + Create service account button from the top row.
- Under Service account details, type a name, ID, and description for the service account, then click Create and continue.
- If required, you can also select the IAM roles to be granted to the service account using the Grant this service account access to project option.
- Click Continue
- If required, you can add the users or groups that are allowed to use and manage the service account.
- Click Done.
- Click the email address for the service account you created.
- Click the Keys tab.
- In the Add key dropdown list, select Create new key.
- Select key type as JSON.
- Click Create.

Your new public/private key pair will be generated and downloaded to your machine. Please keep the private key safe as this will be the only copy, and you cannot generate the same private key again.
Once you have downloaded the JSON private key, you'll have to enable Gmail API service and provide domain-wide authority to the service account.

Enable Gmail API service

- Login to console.developers.google.com.

- Select the project from the dropdown menu.
- Click + Enable APIS and Services.
- Select Gmail API and click Enable.

Delegating domain-wide authority to the service account

- Log in to the Google Workspace domain's Admin console as a super administrator.
- Navigate to Main menu → Security → Access and data control → API Controls.
- In the Domain wide delegation pane, select Manage Domain Wide Delegation.
- Click Add new.
- In the Client ID field, enter the service account's Client ID. You can find your service account's client ID on the Service accounts page.
- In the OAuth scopes (comma-delimited) field, enter the list of scopes that your application should be granted access to. For example, if your application needs domain-wide full access to the Google Mail API, enter: https://mail.google.com.
- Click Authorize.

Your application now has the authority to make API calls as users in your domain (to "impersonate" users). When you prepare to make authorized API calls, specify the user to impersonate as.

SMS Settings

To configure or change SMS settings,

- Navigate to Settings > System Settings > Notification Settings > SMS Settings.
- For sending SMS alerts, you can configure EventLog Analyzer to use a GSM modem or a custom SMS gateway of your own.

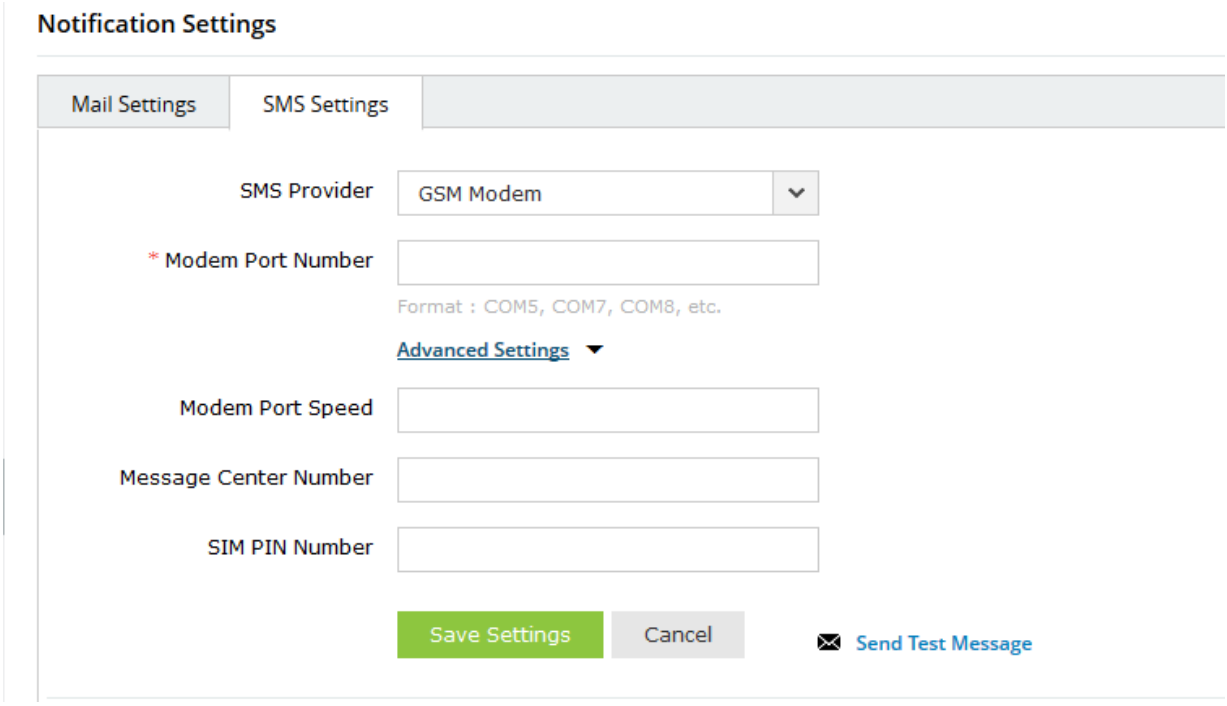
GSM Modem Configuration

Custom SMS Gateway Configuration

GSM Modem Configuration

To configure a GSM modem,

1. Go to Settings > System Settings > Notification Settings > SMS Settings.
2. In the SMS Provider drop-down field, select GSM Modem.
3. In Modem Port Number, enter the hardware port of the EventLog Analyzer server machine to which the SMS hardware component provided by the telecom service provider is connected.
4. Click Save Settings to complete configuration.
5. If the SMS settings are not configured here, EventLog Analyzer prompts you to configure SMS settings at the Alert Profile Creation screen.



Steps involved in configuring the modem port and modem speed:

- Connect your GSM Modem to the serial communication port.
- Only a serial cable must be used for connectivity.
- The port number for Windows devices will be comX. For example, COM7 or COM8.
- Enter the port number to which the modem is connected. For example, COM1.

Requirements for establishing SMS server connection:

- The modem/mobile must have GSM functionality with a provision to insert a SIM card.
- It should support 7-bit (GSM default alphabet), 8-bit, and Unicode (UCS2) encoding.
- Ensure that the GSM modem configured with EventLog Analyzer is not used by any other application.
- If you experience any issue in sending SMS notifications through the GSM modem, please restart EventLog Analyzer and try again.
- Matching these criteria will allow EventLog Analyzer to support your modem/mobile phone.

Custom SMS Gateway Configuration

You can configure you own custom SMS gateway, provided the gateway which is based on HTTP, SMTP or SMPP.

HTTP-based SMS Provider:

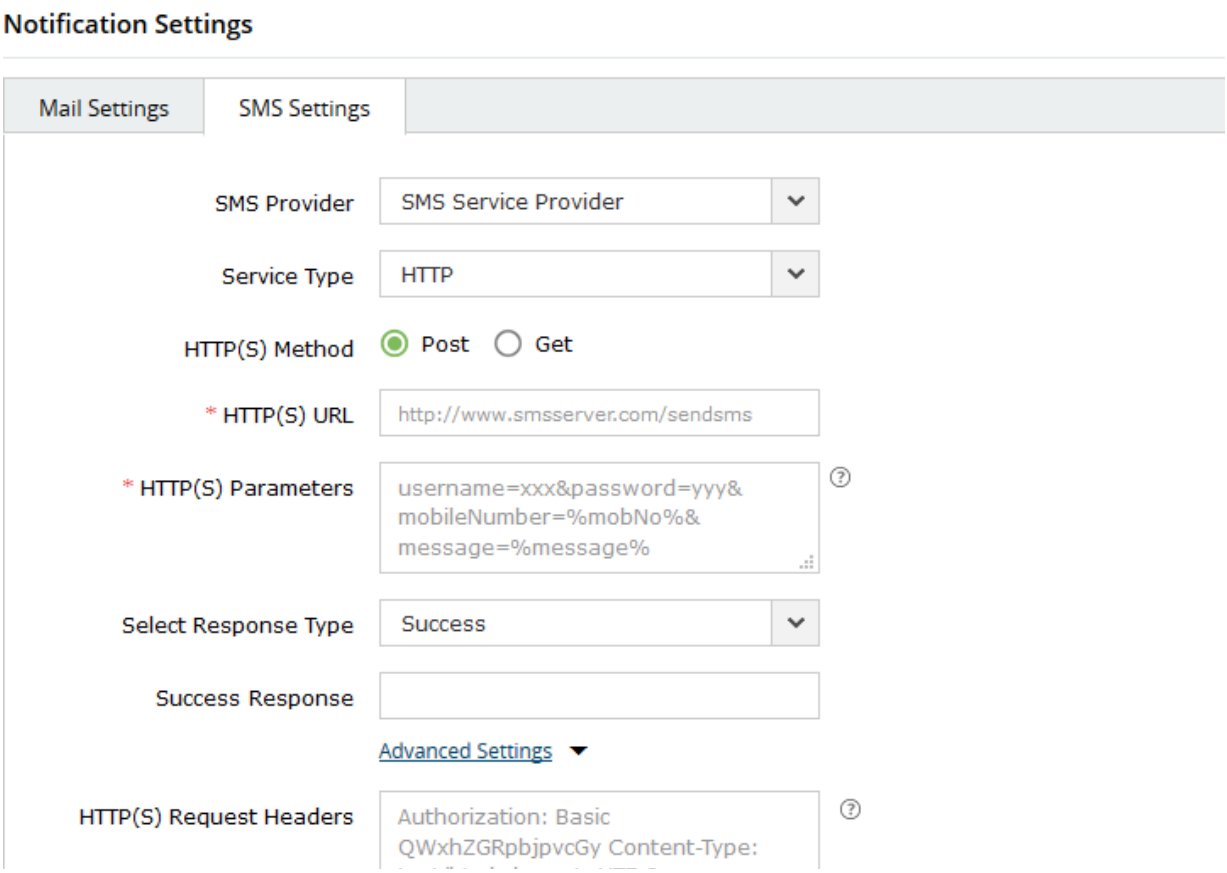
- Navigate to Settings > System Settings > Notification Settings > SMS Settings.
- In the SMS Provider drop-down field, select SMS Service Provider.
- In the Service Type drop-down field, select HTTP.
- In the HTTP(S) Method field, select whether you want to use the Post or Get method for sending SMS

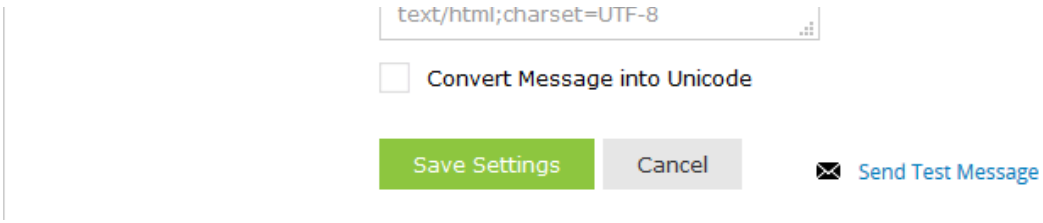
- In the HTTP(S) Method field, select whether you want to use the Post or Get method for sending SMS.
- In the HTTP(S) URL field, enter the URL of your SMS gateway provider.
- In the HTTP(S) Parameters field, enter the HTTP parameters specific to your SMS provider.

> Note Separate the HTTP parameters with ampersand (&) symbols.

Example format userName=xxx&password=yyy&mobileNumber=%mobNo&message=%message%
where,
userName = the parameter which is used to denote the API authentication username
xxx = API authentication username
password = the parameter which is used to denote the API authentication password
yyy = API authentication password
mobileNumber = recipient parameter
%mobNo% = this macro denotes the user's mobile number
message = message parameter
%message% = this macro denotes the SMS message content
More HTTP Parameters - If you SMS provider requires more parameters like unicode and apiID, include them as well using the '&' sign

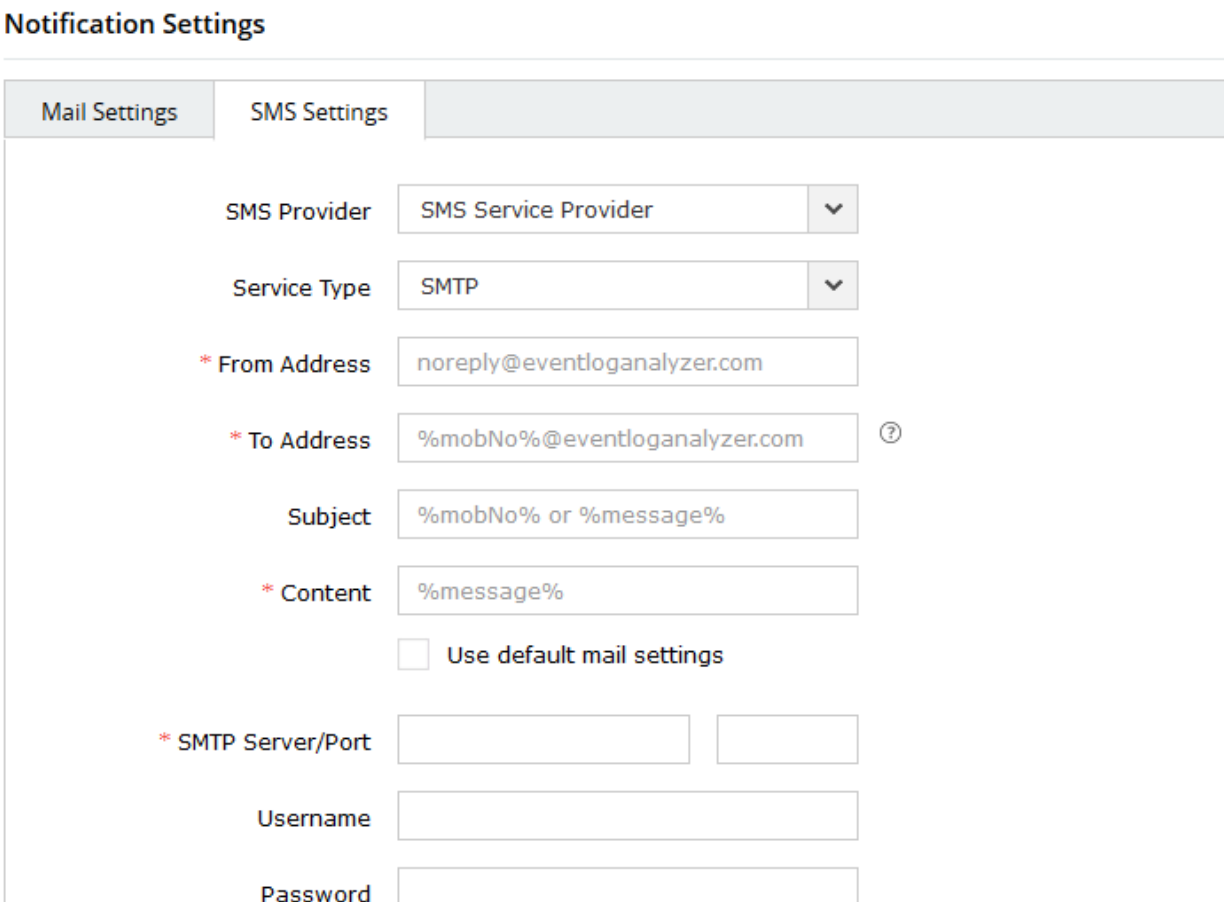
- Specify the response you get from your provider to determine the success of sending the SMS.
- Click Advanced Settings and enter the HTTP request headers specific to your SMS provider.
- Select the check box Convert Message into Unicode to send SMS in Unicode format.
- Click Save Settings to complete configuration.

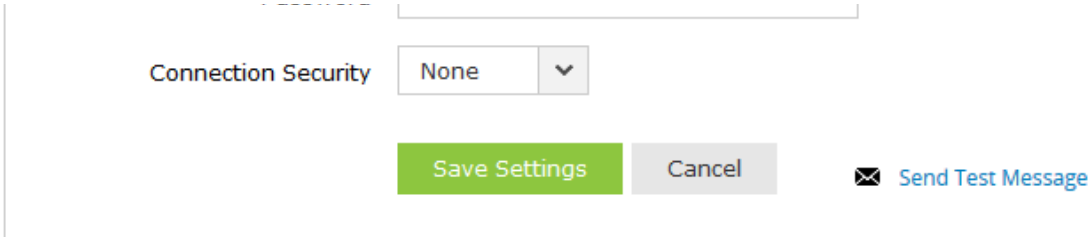




SMTP-based SMS Provider:

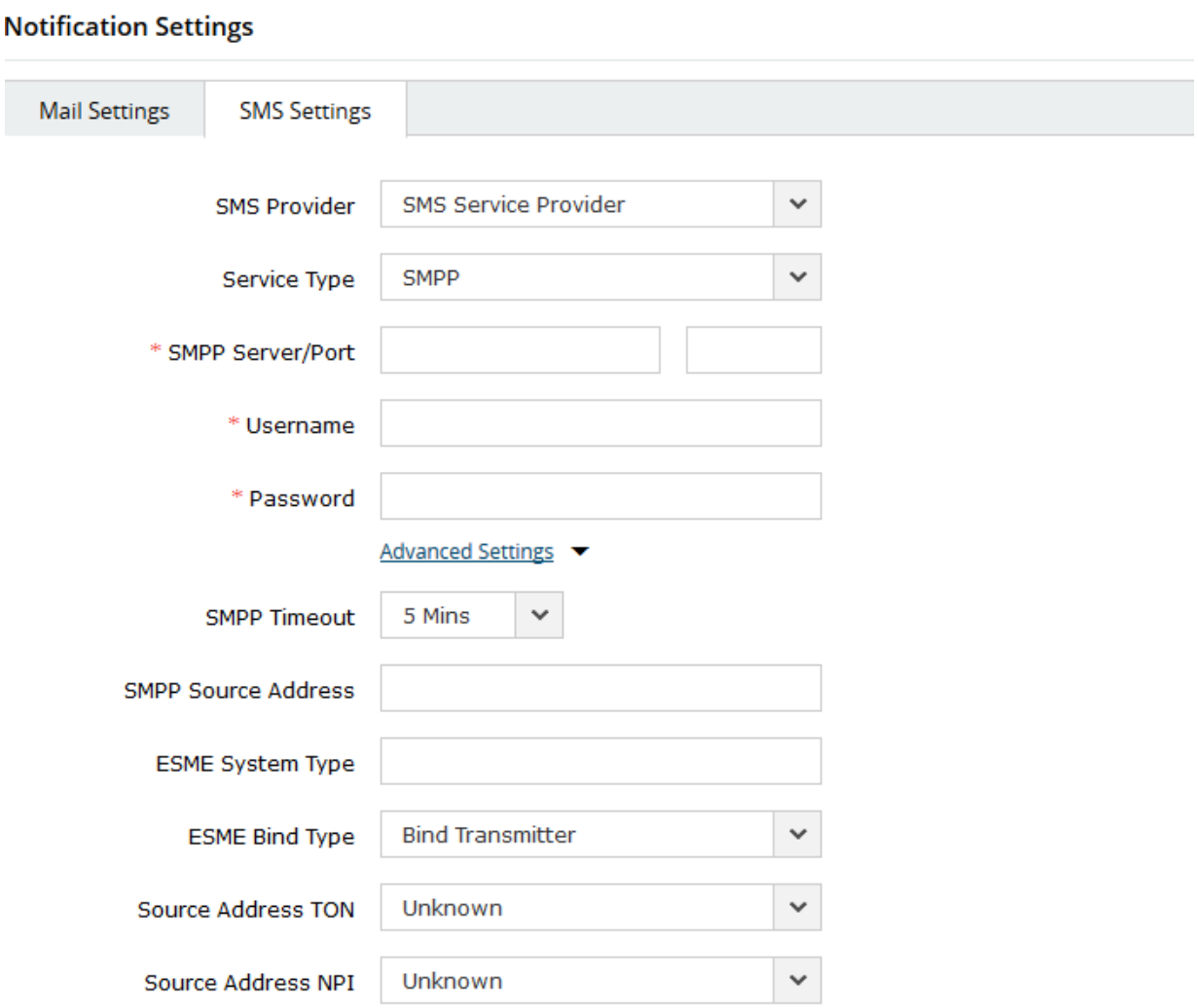
- Navigate to Settings > System Settings > Notification Settings > SMS Settings.
- In the SMS Provider drop-down field, select SMS Service Provider.
- In the Service Type drop-down field, select SMTP.
- In the From Address field, enter an email address from which you want to send the SMS. For example, noreply@eventloganalyzer.com
- In the To Address field, enter the %mobNo% macro followed by the email of your provider. For example: %mobNo%@clickatell.com. Refer to your SMS provider to know the exact values.
- In the Subject field, enter either the mobile number or message, which is based on your SMS provider.
- In the Content field, enter appropriate data, which varies based on the SMS provider.
- In the SMTP Server/Port field, enter the name or IP address of the SMTP Server and its port number.
- Enter appropriate credentials for the SMTP server in the Username and Password fields.
- Click Save Settings to complete configuration.

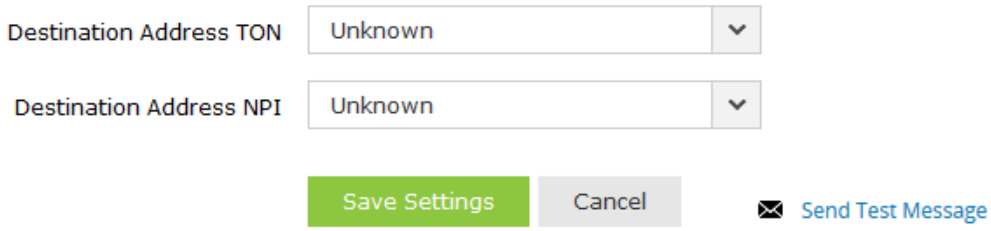




SMPP-based SMS Provider:

- Navigate to Settings > System Settings > Notification Settings > SMS Settings.
- In the SMS Provider drop-down field, select SMS Service Provider.
- In the Service Type drop-down field, select SMTP.
- In the SMPP Server/Port field, enter the name or IP address of the SMPP Server and its port number.
- Enter appropriate credentials for the SMPP server in the Username and Password fields.
- Click Advanced Settings and in the SMPP Source Address field, enter the appropriate IP address.
- Select the type of number (TON) and numeric plan indicator (NPI) of the source address.
- Select the type of number (TON) and numeric plan indicator (NPI) of the destination address.
- Click Save Settings to complete configuration.




Destination Address TON
Unknown
Destination Address NPI
Unknown
Save Settings
Cancel
Send Test Message

9.5.4.1. Listener ports overview

Last updated on: September 12, 2025

In this page

Overview

Prerequisites

Need for listener port configuration

Key functionalities

Configuring Syslog listener ports

Accessing Syslog listener ports

Manage Syslog listener ports

Adding a Syslog listener port

Manage default Syslog listener port

Deleting a Syslog listener port

Enable/disable a Syslog listener port

Enable/disable a Syslog listener port for selective collectors/agents

Edit a syslog listener port

Collector/agent selection

Overview

The Listener Port console provides an interface for configuring and managing ports used to receive incoming logs and messages. Log360 supports both Syslog listener ports (UDP/TCP/TLS) and SNMP Traps listener ports (UDP) for receiving logs. With these ports, external devices and applications send logs and traps to the collector/agent.

Prerequisites

- Port availability: Ensure that the configured ports are not used by any other applications or services on the Log360 server.
- Firewall and antivirus rules:
  - Allow all incoming traffic on the specified ports on the agent/machine running the Log360 server's firewall.
  - Some antivirus software may block unknown or custom ports by default. Ensure that your antivirus tool is also configured to permit traffic on the configured listener ports.
- Network devices configuration: Configure the external devices to send Syslog messages/SNMP Traps to the server's IP address and the designated port.

server's IP address and the designated port.

Need for listener port configuration

Without properly configured listener ports, the server cannot receive, process, or analyze the incoming log data.

Key functionalities

- Seamless log collection: Logs from the network devices can be received only when the appropriate ports are open and listening.
- Protocol flexibility: You can configure multiple ports for different protocols (UDP, TCP, TLS) based on your network's security and reliability requirements.
- Security and access control: By selectively enabling or disabling ports per collector/agent, you can restrict log intake to trusted sources and minimize your attack surface.

Configuring Syslog listener ports

The Listener Ports module lets you manage the ports used to receive incoming logs from external devices. You can assign protocols (UDP, TCP, TLS), configure default Syslog ports, and control which collectors or agents listen on specific ports. This section explains how to access the configuration interface for the Syslog listener ports and perform actions like adding new Syslog listener ports, editing existing ones, and managing port-to-collector/agent mappings to streamline log intake.

Accessing Syslog listener ports settings

1. In the product console, navigate to the Settings tab and click on Listener ports listed under System Settings as shown in the below image.

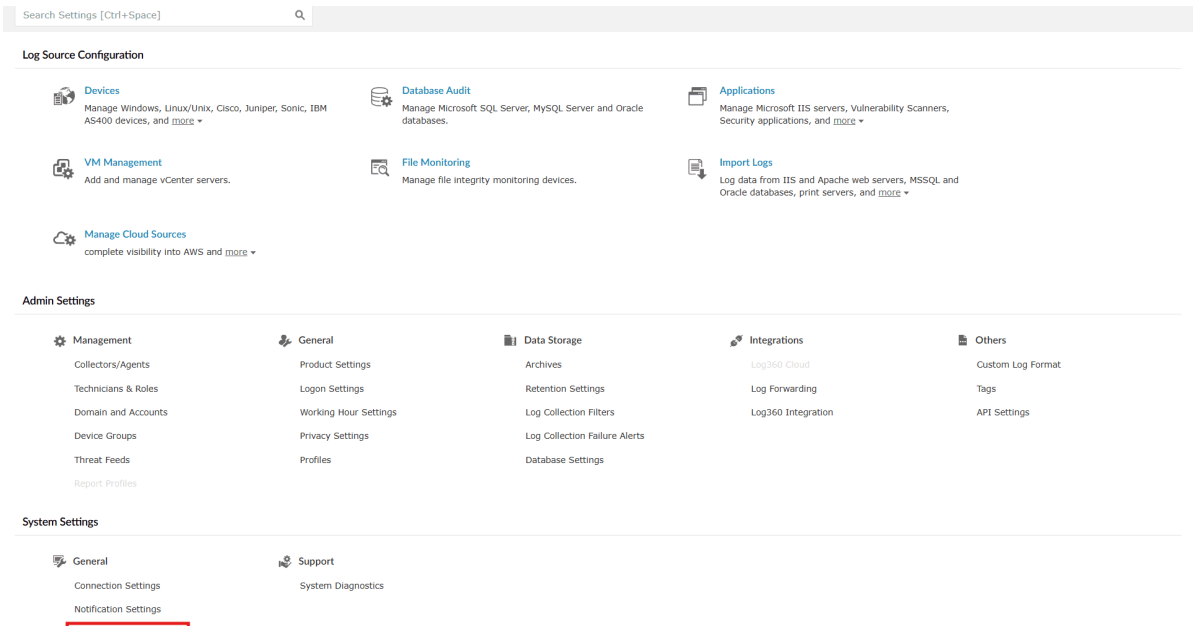




Image 1: Accessing listener ports settings

2. The Listener Ports module for Syslog ports configuration provides you with:
   - Port: Displays the port number
   - Action: Option to enable/disable, edit, delete or make default the listener port(s).
   - Protocol: Displays the operating protocol for that particular port.
   - Associated Collectors/Agents: Displays all the collectors/agents associated with the corresponding port number.

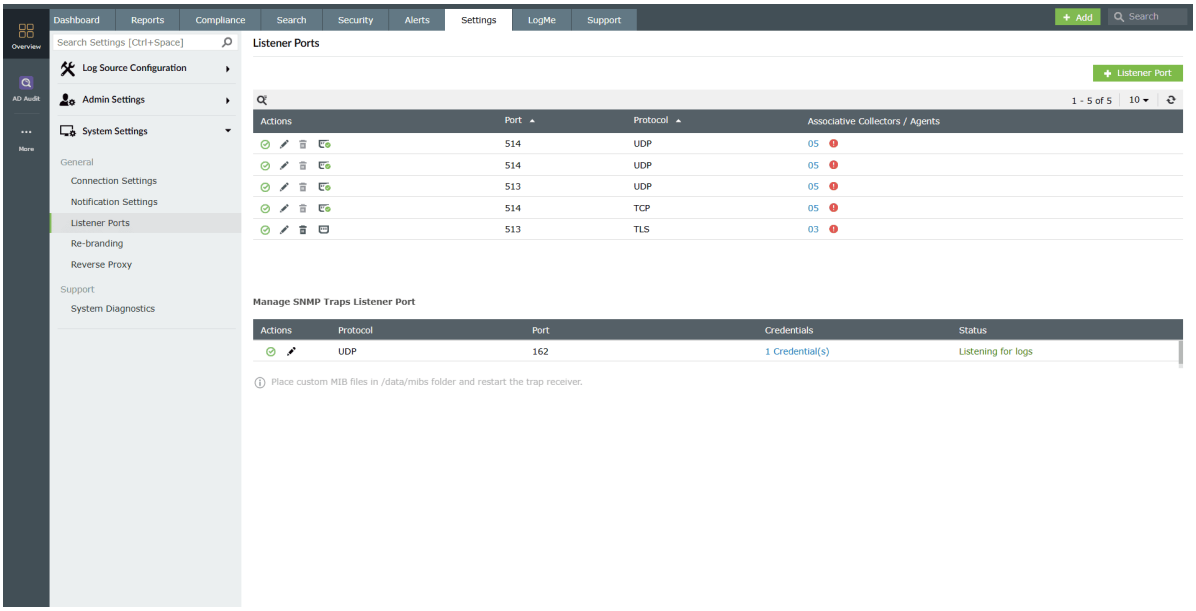


Image 2: Listener ports configuration via the Settings tab

Manage Syslog listener ports

The following are the available actions for the syslog ports under listener port configuration:

- Add a Syslog port
- Manage default Syslog port
- Delete a Syslog port
- Enable/disable a Syslog port
- Enable/disable a Syslog port for selective collectors/agents
- Edit an existing Syslog port

Adding a Syslog port

1. Navigate to the Listener Ports module in the product console and click on the +Listener Port button as highlighted below.

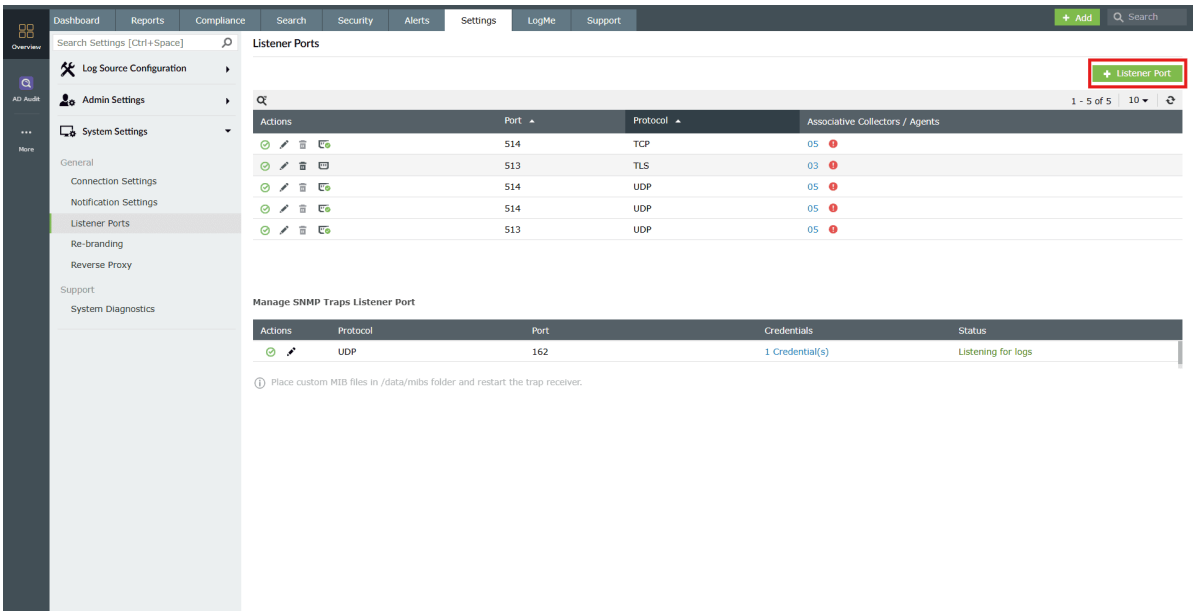
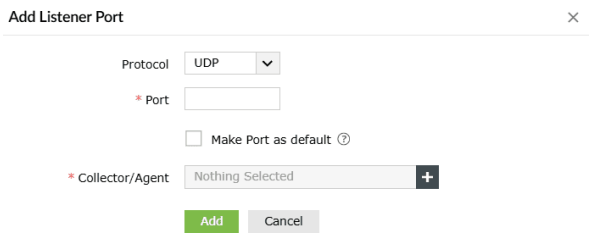


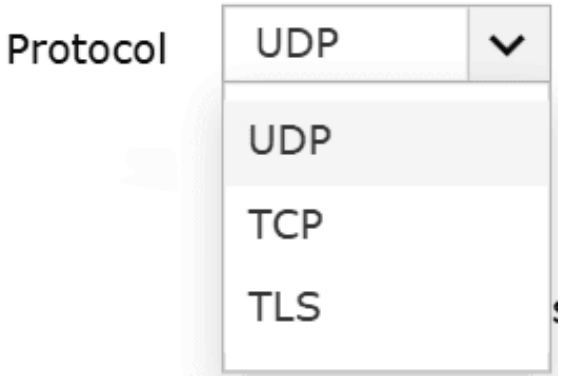
Image 3: Adding a listener port via the Settings tab

2. The Add Listener Port pop-up slides in.



3. Fill in the required fields:

- Protocol: Select the protocol from the drop-down.



- Port: Specify the port number for log collection.
  - Fill in the check-box provided if you wish to make that specific port the default port number that will be automatically associated to newly added collector/agents in future configurations. Ensure the pre-requisites are met before filling in the port number.

- Add Collector/Agent: Select the Collector/Agent(s) on which this port can be enabled.

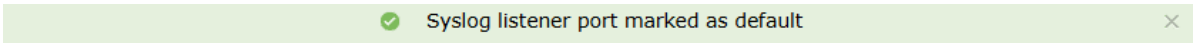
> NOTE
>
> - The Select Collector/Agent option will be visible only if a remote collector/agent has been added in the server.
> - For each protocol, you can add only 6 ports.

4. Click on Add.
5. Upon successful completion of the action, the below pop-up appears.



Manage default Syslog listener port

1. To make a port as a default port for syslog collection, click the  icon under the Actions tab.
2. Upon successful completion of the action, the below pop-up appears.



3. Similarly, to remove a port from being default, click on the remove as default port icon  .
4. Upon successful completion of the action, the below pop-up appears.

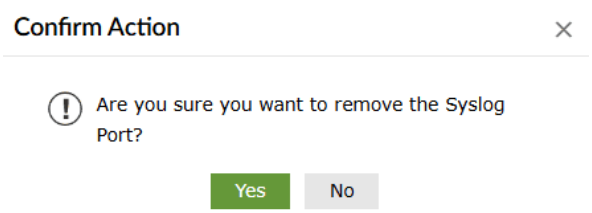


Once you make the port default, all collector/agent(s) will listen through that specific port.

Deleting a Syslog port

> Note
>
> Default ports cannot be deleted. You must remove a port as default port first to delete it.

1. Click on the Delete icon under the Actions column to delete a listener port.
2. A Confirm Action pop-up appears. Click on Yes.



3. Upon successful completion of the action, the below pop-up appears.



Enable/disable a Syslog listener port

Enabling a Syslog listener port

1. Click on the currently disabled icon under the Actions column to enable the port.
2. As soon as you perform this action, the icon indicates that the port is now enabled and the below pop-up message appears briefly.



Disabling a Syslog listener port

1. Click on the currently enabled icon under the Actions column to disable the port.
2. As soon as you perform this action, the icon indicates that the port is now disabled and the below pop-up message appears briefly.



Enable/disable a Syslog listener port for selective collectors/agents

1. Click on the corresponding number in the Associated Collectors/Agents column for the port you wish to view the associated collectors/agents for.

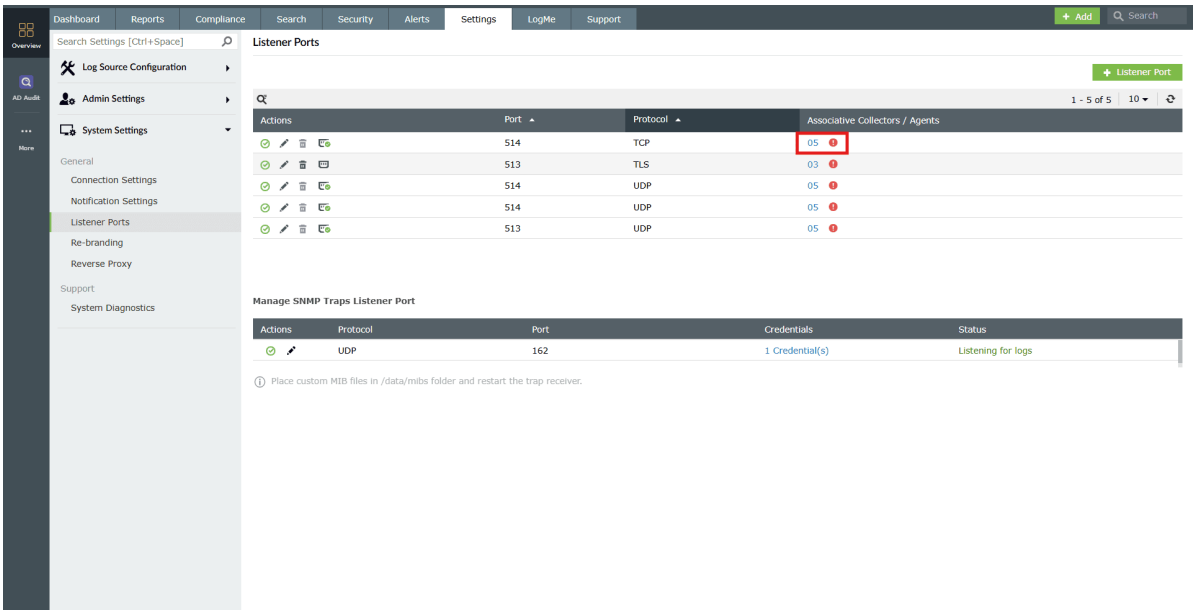
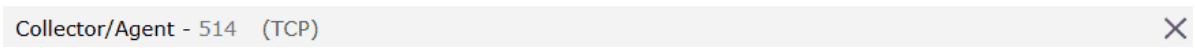


Image 4: Associated collectors/agents for the syslog listener ports

2. This will open the list of Collectors/Agents and their status along with a troubleshooting link , in the case of an error.



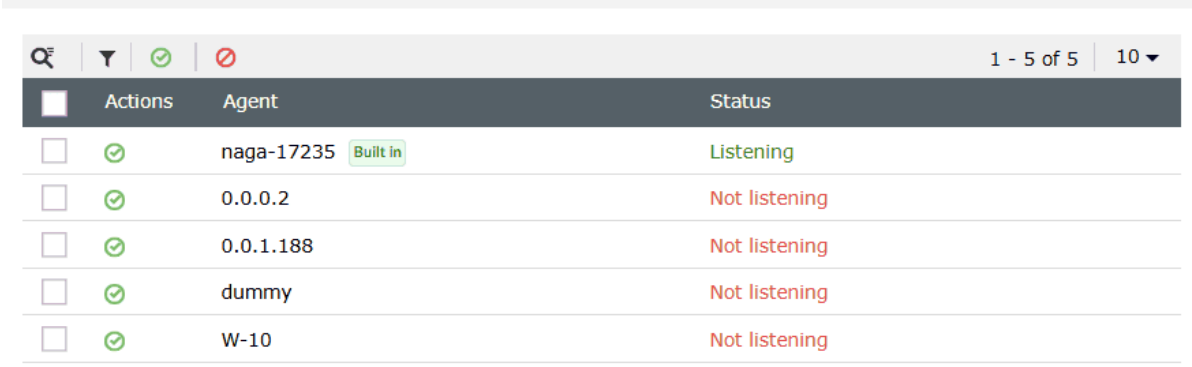


Image 4: Associated collectors/agents for the syslog listener ports

> Note
>
> By default, all Collectors/Agents are in an enabled state.

To enable:

1. Click on the currently disabled icon under the Actions column to enable the port for that specific collector/agent.
2. As soon as you perform this action, the icon indicates that the port is now enabled for that particular collector/agent, and the below pop-up message appears briefly.

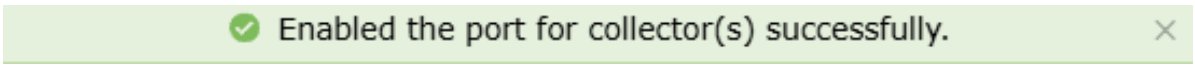
To disable:

1. Click on the currently enabled icon under the Actions column to disable the port for that specific collector/agent.
2. As soon as you perform this action, the icon indicates that the port is now disabled for that particular

collector/agent, and the below pop-up message appears briefly.

To enable/disable a port for multiple collectors at once:

1. Select the desired collectors by clicking on the checkboxes provided and click on the enable/disable icon at the top.
2. Upon successfully enabling, the below pop-up appears.

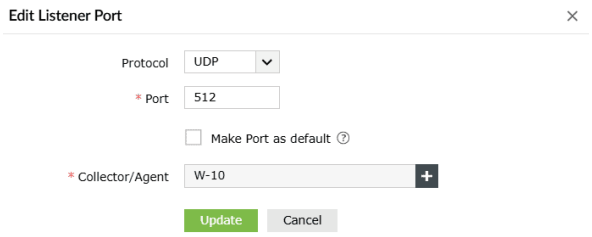


3. Upon successfully disabling, the below pop-up appears.

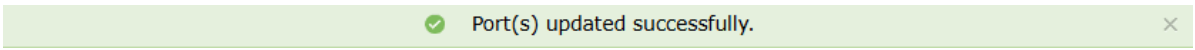


Edit a Syslog listener port

1. Click on the Edit icon under the Actions column to edit the respective port.
2. The Edit Listener Port box will be displayed. Make the necessary edits and click on Save.



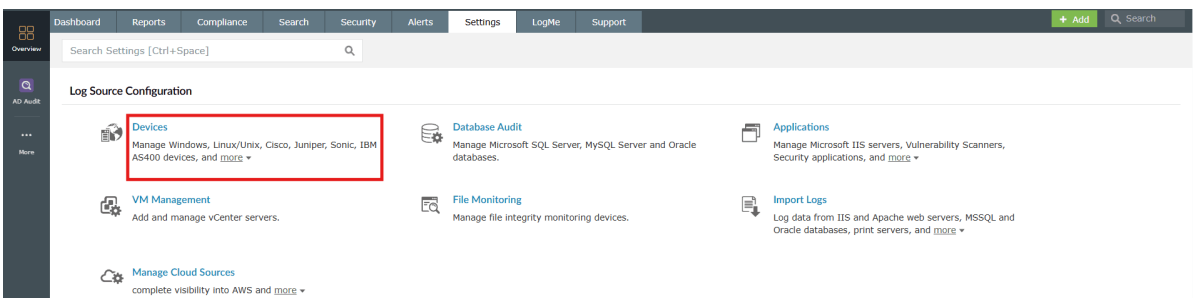
3. The changes are updated instantly. Upon successful completion of the action, the below pop-up appears.



Associating a collector/agent for a device

Use this interface to select a collector or agent while configuring the device/application or the listener port(s).

1. In the product console, navigate to the Settings tab and click on Devices.



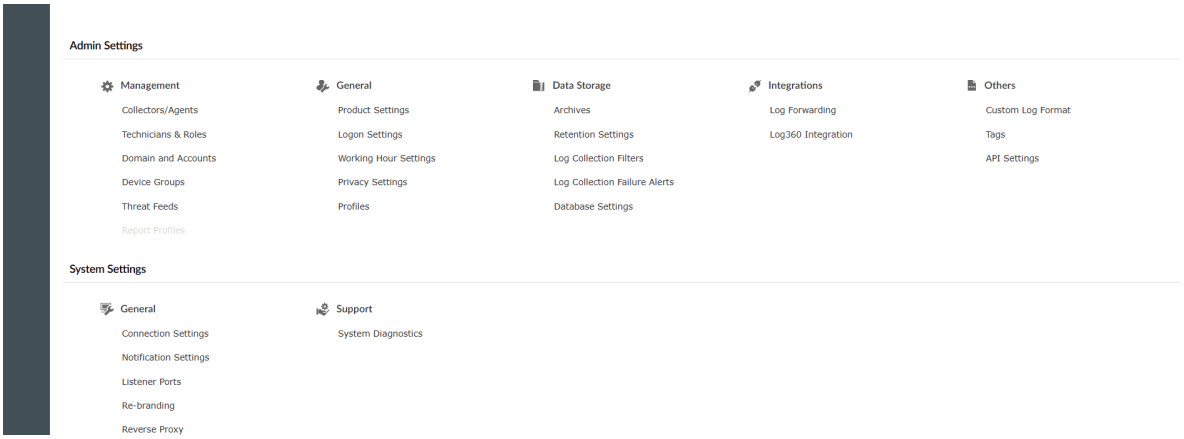


Image 5: Add devices via the Settings tab

2. Click on the +Add Device(s) button as highlighted below.

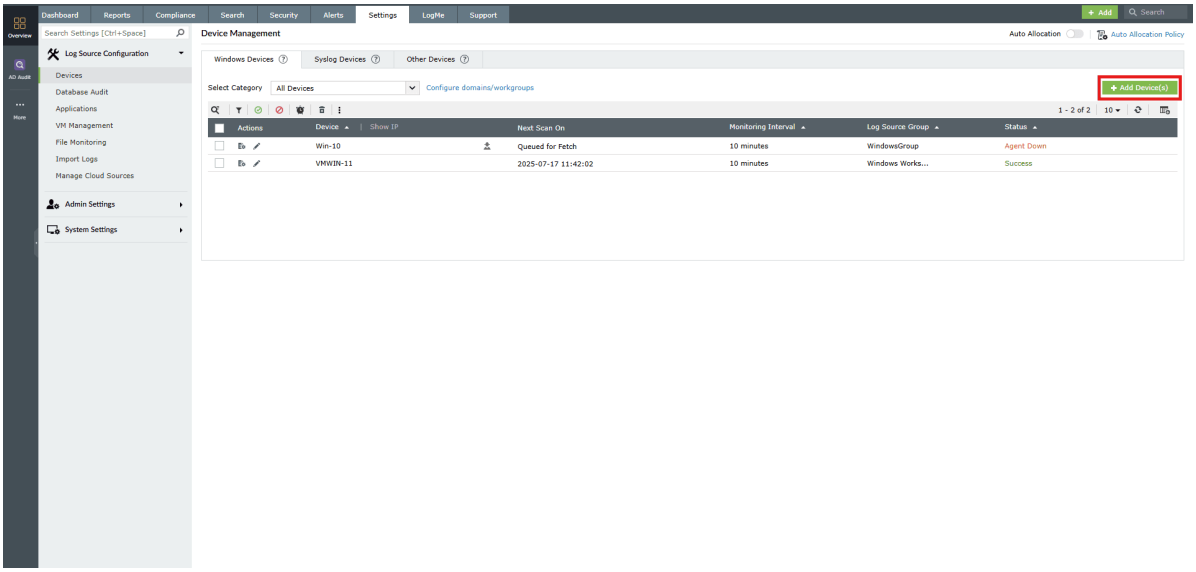
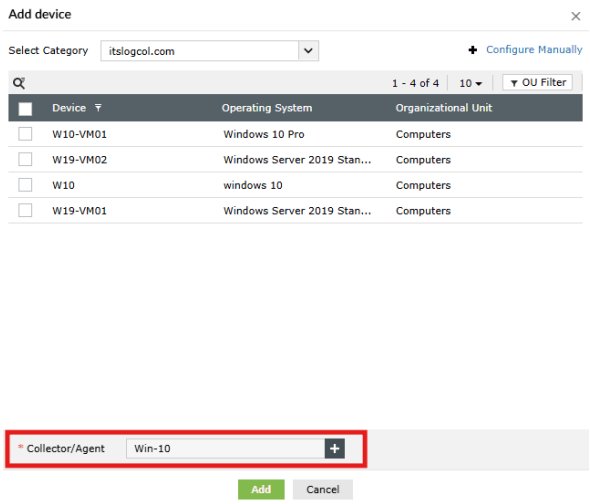


Image 6: Adding a device to a listener port configuration

3. The Add device pop-up box appears. In the Collector/Agent field as highlighted below, click the plus + icon to display the list of available collectors/agents.



4. Select the appropriate collector/agent from the list that appears on the screen.

4. Select the appropriate collector/agent from the list that appears on the screen.



5. Click on Add to confirm your choice and proceed.

Read also

This document explained how to configure and manage listener ports (Syslog listener ports) in the product console, covering prerequisites, key features, and selective control options. For more on enhancing log collection and device integration, refer to the related pages below:

- SNMP Traps port management

9.5.4.2. SNMP Traps port management

Last updated on: September 12, 2025

In this page

Overview

Configuring a device to send SNMP traps

Manage SNMP Trap listener ports

Enable/disable SNMP Trap listener port

Edit SNMP Trap listener port

Update credentials for SNMP Trap

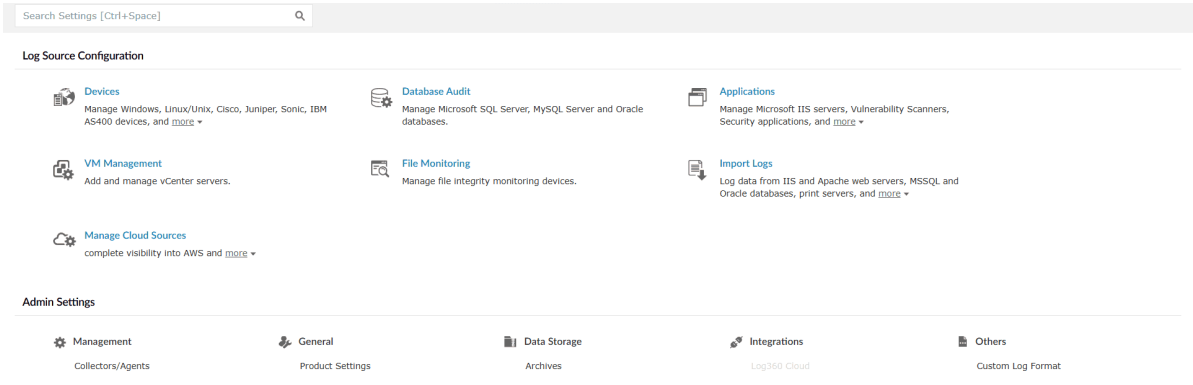
Overview

The SNMP Trap listener port management capability allows you to configure and control how SNMP traps are received from devices that are added for monitoring. This includes setting up trap destination ports, enabling or disabling the SNMP Trap listener ports, editing port values, and managing SNMP credentials for various protocol levels (V1, V2c, V3). This helps maintain secure and accurate log ingestion from SNMP-supported devices.

Configuring a device to send SNMP traps

> NOTE
>
> To configure a network device to send SNMP traps, ensure that SNMP is enabled in the product, and then enable traps in your network device.

1. In the product console, navigate to the Settings tab and click on Listener ports listed under System Settings as shown in the below image.



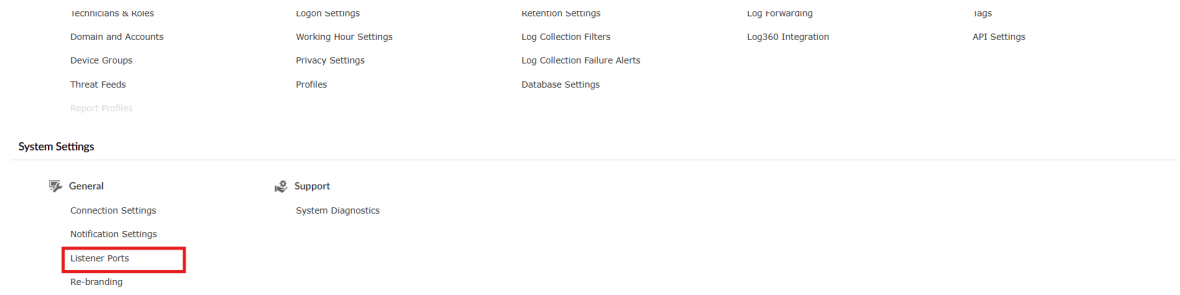


Image 1: SNMP Traps listener ports configuration via the Settings tab

2. You will be taken to the Listener Ports segment. You can find the fields listed under Manage SNMP Traps Listener Port, as highlighted below.

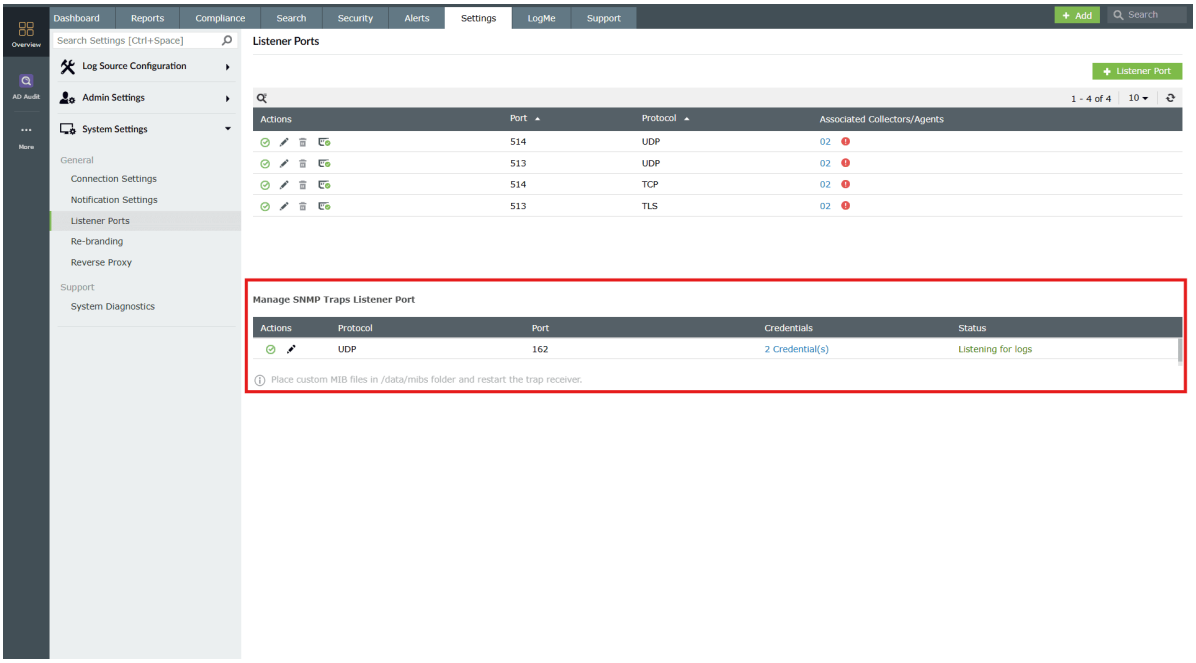


Image 2: Managing SNMP Traps ports under the listener ports configuration

3. In your device settings configuration, set the trap destination host address to the IP address or the hostname of the corresponding product's server.
4. Set the trap destination port to 162 or to the SNMP port configured in the product—Log360, EventLog Analyzer, and Log360 Cloud.
5. Specify the SNMP credentials that are already configured.
6. Save the configuration.

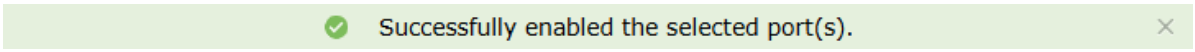
> **NOTE**
>
> By default, the product's server listens to port 162 (UDP) for SNMP traps.

Manage SNMP Trap listener ports

Enable/disable SNMP Trap listener port

Enabling an SNMP Trap listener port

1. Click on the currently disabled icon under the Actions column to enable the port.
2. As soon as you perform this action, the icon indicates that the port is now enabled and the below pop-up message appears briefly.



Disabling an SNMP Trap listener port

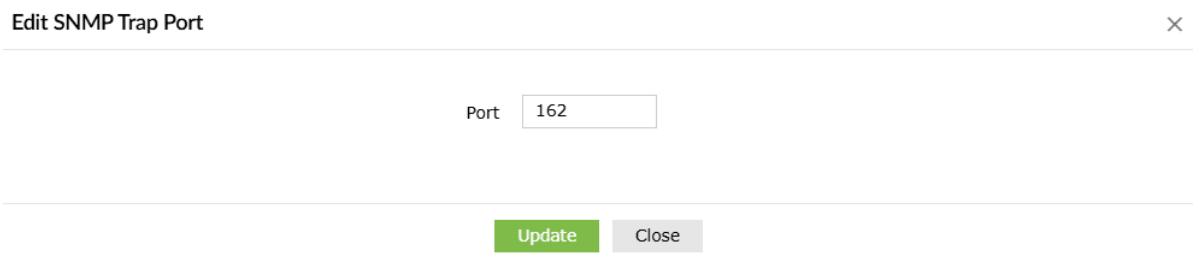
1. Click on the currently enabled icon under the Actions column to disable the port.
2. As soon as you perform this action, the icon indicates that the port is now disabled and the below pop-up message appears briefly.



Edit SNMP Trap listener port

To edit the port using which Log360 listens to SNMP traps:

1. Click on the Edit icon under the Actions column to edit the respective SNMP Trap port. The Edit SNMP Trap listener Port pop-up appears as shown below.

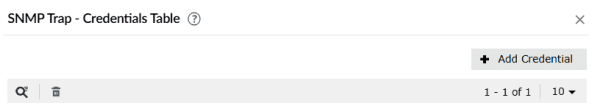


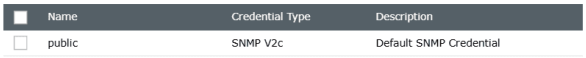
2. Enter the desired port number and click on Update.
3. Upon successfully enabling, the below pop-up appears. The edits are instantly made, and you can see the updated configuration in the console.



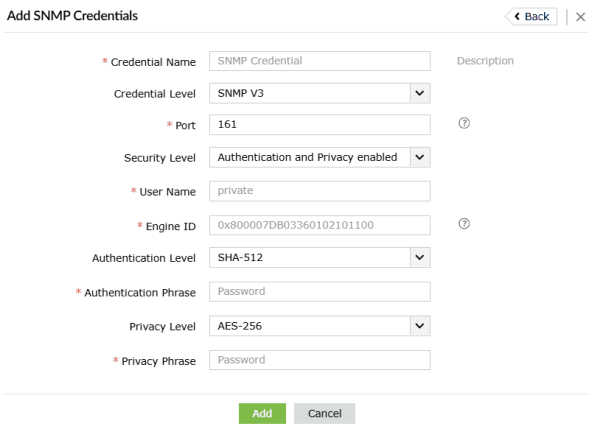
Updating credentials for SNMP Trap

1. Click on the Credentials button under the Credentials field. The SNMP Trap - Credentials Table pop-up appears.



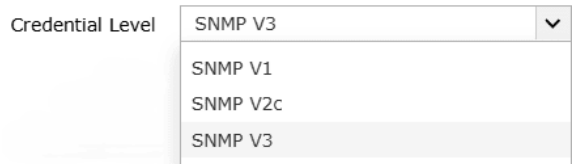


2. Click on the Add Credential button to add a new SNMP credential. The Add SNMP Credentials pop-up appears as below.

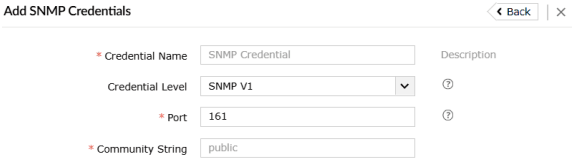


3. Fill in the required fields

- Enter the Credential Name for SNMP Credential.
- Select the required Credential Level.
- Enter the desired Port number. This port will only be used by the workflow and syslog device discovery modules.
  There are two different cases based on the Credential Level you have chosen.



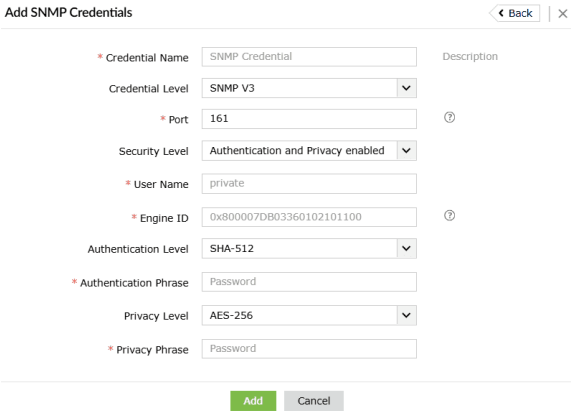
Case 1: If the required Credential Level is chosen as either V1 or V2c



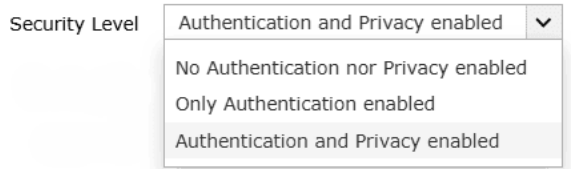


The SNMP V1/V2C will also require you to provide the Community String for SNMP Trap and discovery.

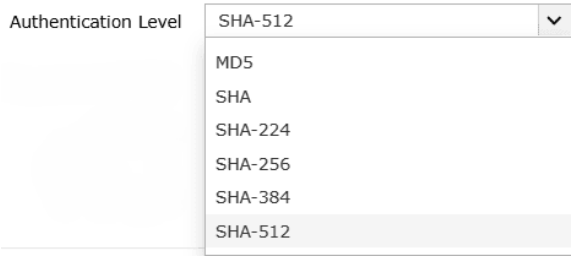
Case 2: If the required Credential Level is chosen as V3



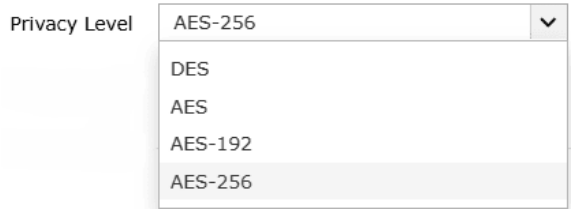
- Choose a Security Level from the drop-down.



- Enter the User Name.
- Enter the Engine ID. This will be used for trap collection and sending traps in workflows.
- Select the SNMPV3 credential's Authentication Level.



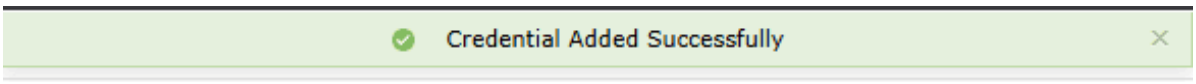
- Enter the Authentication Phrase for SNMPv3 credential.
- Select the SNMPV3 credential's Privacy Level.



- Enter Privacy Phrase for SNMPv3 credential.

4. After filling all the required fields, click on Add.

5. Upon successful completion of the action, the below pop-up appears.



> **NOTE**
>
> When a device not added to the product's server starts sending SNMP traps to the product, it will automatically be listed under Other Devices in Settings > Configuration > Manage Devices. Additionally, it will be listed under General Applications as SNMP Trap Application.
> The credentials added here can be used when discovering devices via Settings > Configuration > Manage Devices > Syslog Devices and credentials added while discovering devices can be used for SNMP trap collection.

Read also

This document covered how to configure SNMP Trap listener ports, enable or disable port access, and update SNMP credentials in Log360. For more on network device integration and log ingestion methods, refer to the following page:

- Configure listener ports

9.5.5. Re-branding in Log360

Last updated on: September 12, 2025

In this page

Overview

Steps to rebrand the Log360 client

Overview

Log360 allows you to customize the product interface by replacing default logos, images, and links with your own branding. This feature is particularly useful for Managed Security Service Providers (MSSPs) who want to deliver a personalized experience for their clients.
You can modify the logos and images used in the product interface and reports, as well as the strings and links displayed on login pages and other sections of the product.
This page explains how you can rebrand the Log360 client to reflect your organization's branding.

Steps to rebrand the Log360 client

1. In your account, navigate to the Settings tab.
2. Under System Settings, click Rebranding.

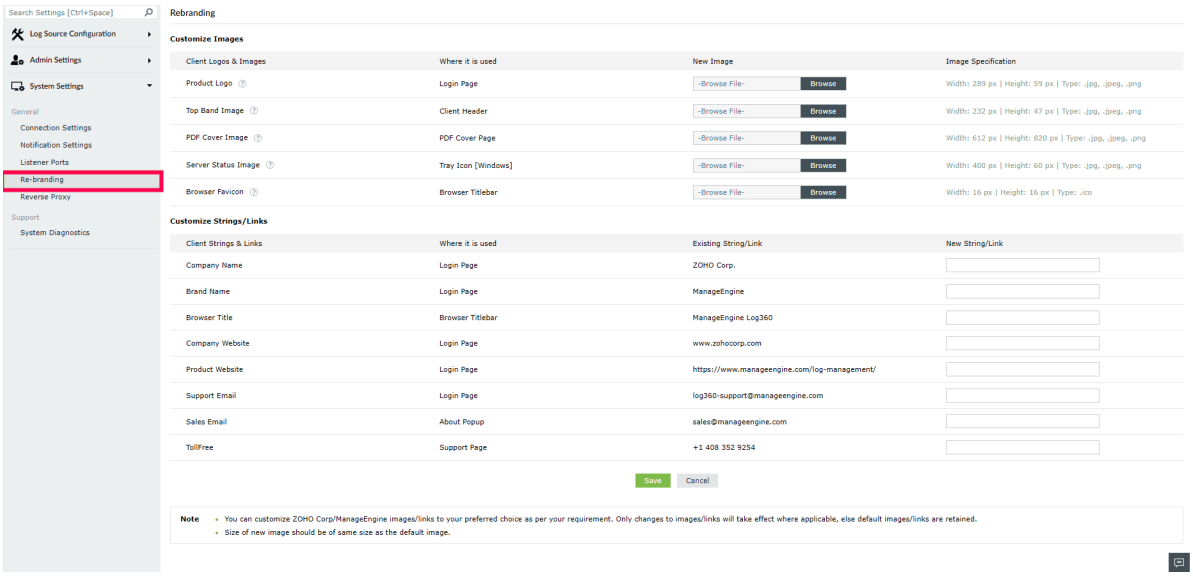


Figure 1: Navigating to Re-branding

3. Under the Customize Images section, you can replace default product images with your organization's branding.
4. To update an image, click Browse next to the image you want to replace.
5. Select the new image from your system.

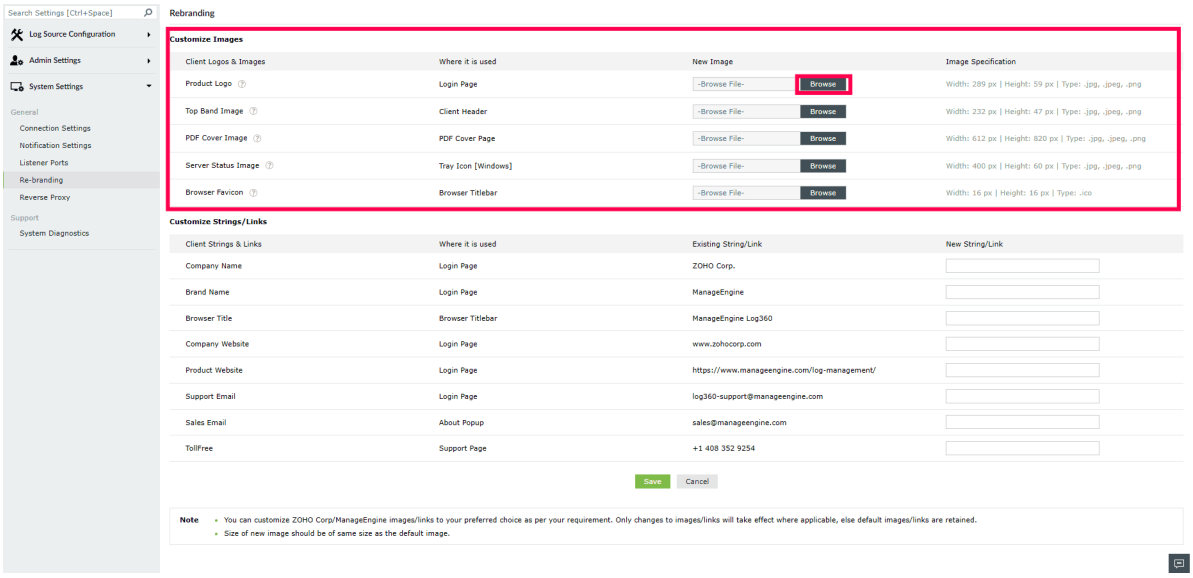


Figure 2: Customizing images

6. Ensure the image meets the specified dimensions and file type requirements displayed in the Image Specification column.
7. Under the Customize Strings/Links section, you can replace the default text and links with your organization's details.

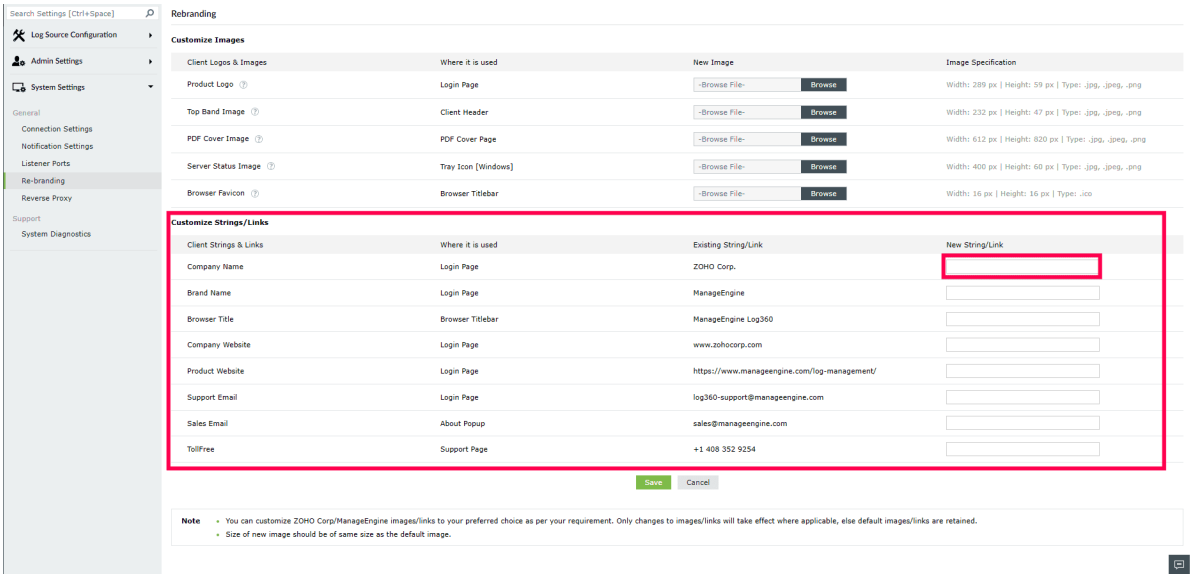


Figure 3: Customizing strings/ links

8. To update, locate the string or link you want to customize.
9. Enter the new string or link in the corresponding field.
10. Click Update to update the customized images/logos and strings/texts.

> **NOTE**
>
> You can customize all ZohoCorp/ManageEngine images and links as per your requirement
>
> - Customization takes effect only for the updated images or links. Unchanged fields will retain their

default values.

- The size of the new image should match the size of the default image.
- Only the following image file formats are supported: .jpg, .jpeg, .png,

Read also

This page explained about rebranding the Log360 client.

9.5.6. System Diagnostics

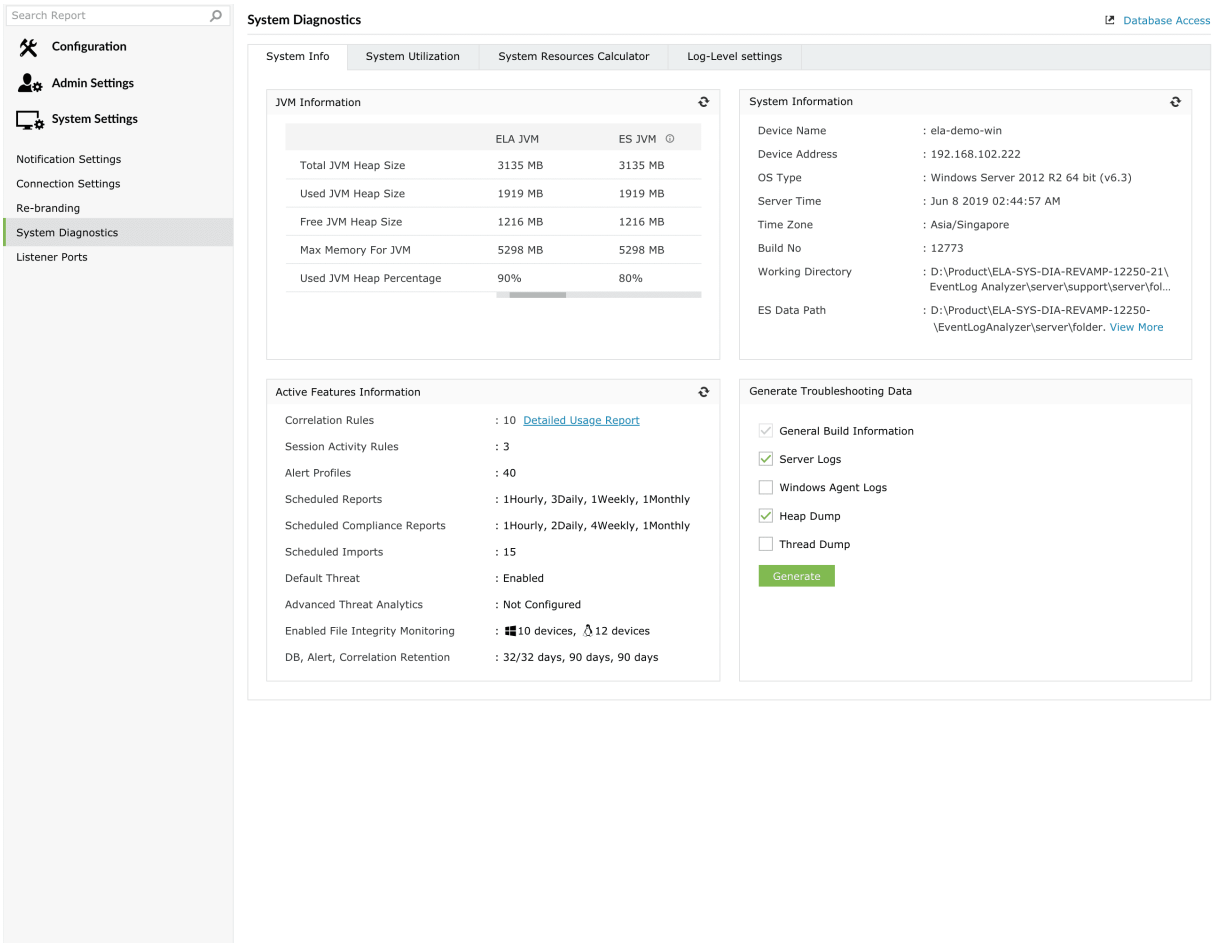
Last updated on: September 12, 2025

- System Info
- System Utilization
- Database Access
- System Resource Calculator
- Log Level Settings

9.5.7. System Info

Last updated on: September 12, 2025

The System Info page provides essential product configurations such as JVM details, active features, system specifics, and a troubleshooting widget for quick issue resolution.



JVM Information - The information about the ELA JVM and ES JVM are listed.
System Information - Crucial system details like device name, OS type, and timezone are listed. It also includes the product build number, EventLog Analyzer's working directory, and ES Data Path for comprehensive system insight.
Active Features Information: This section lists active/enabled product configurations, including the number of alert profiles, correlation rules, scheduled reports/imports, and retention details, providing a concise overview of operational settings.

Generate Troubleshooting Information:

This allows users to select, compress, and upload logs for analysis by the support team.
The logs include:

- General Build Information: A text file containing all details available on this page.
- Server Logs: Including ELA and ES logs.
- Windows Agent Logs: Agents logs can be collected, requiring credentials for installed agents. For manually installed agents, logs should be collected manually.

installed agents, logs should be collected manually.

- Heap Dump
- Thread Dump

How to collect agent logs manually?

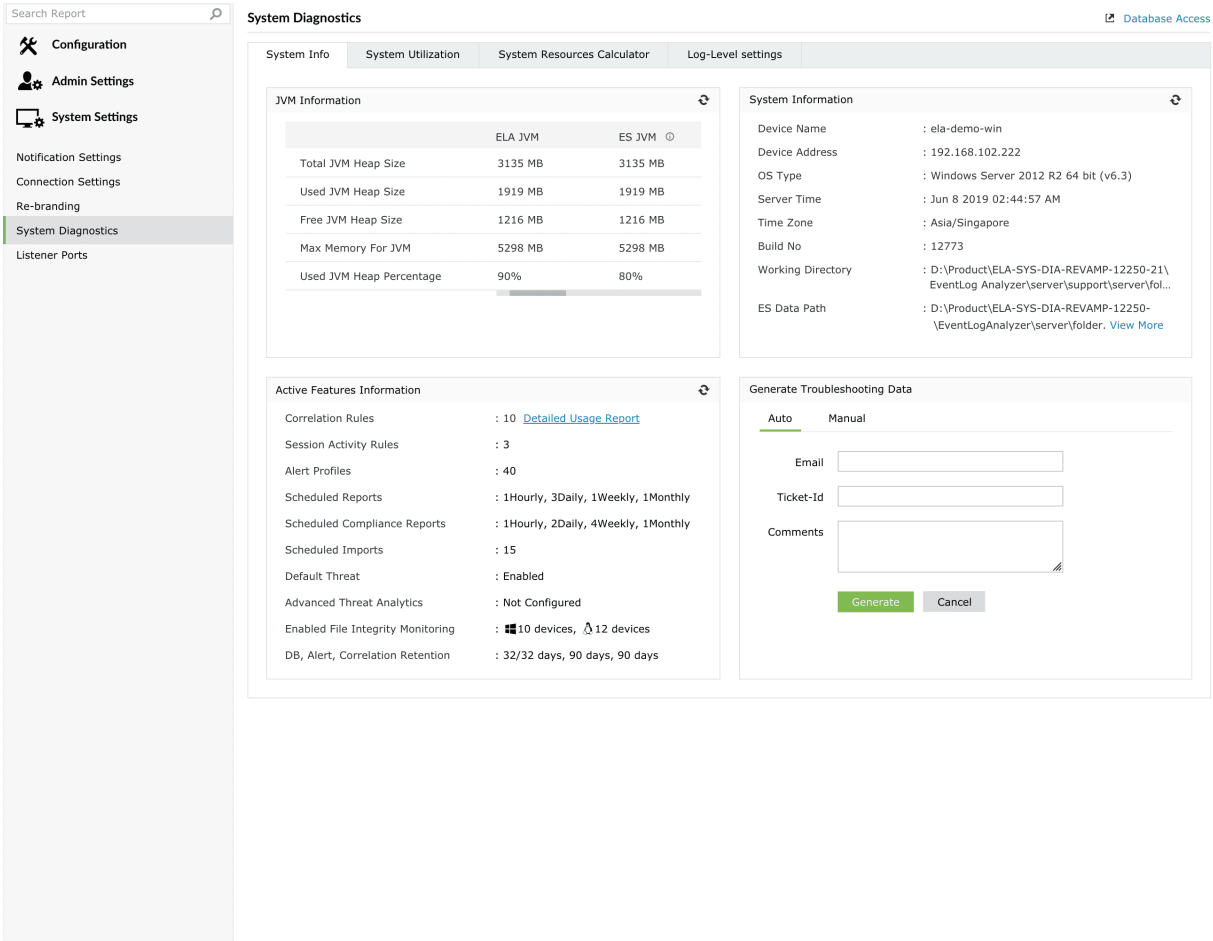
1. Log into the agent-installed machine.
2. Navigate to the installation folder of the agent (e.g., C:\Program Files (x86)\EventLogAnalyzer_Agent).
3. Locate the logs folder.
4. Collect the logs.
5. Upload the logs to https://bonitas.zohocorp.com/.

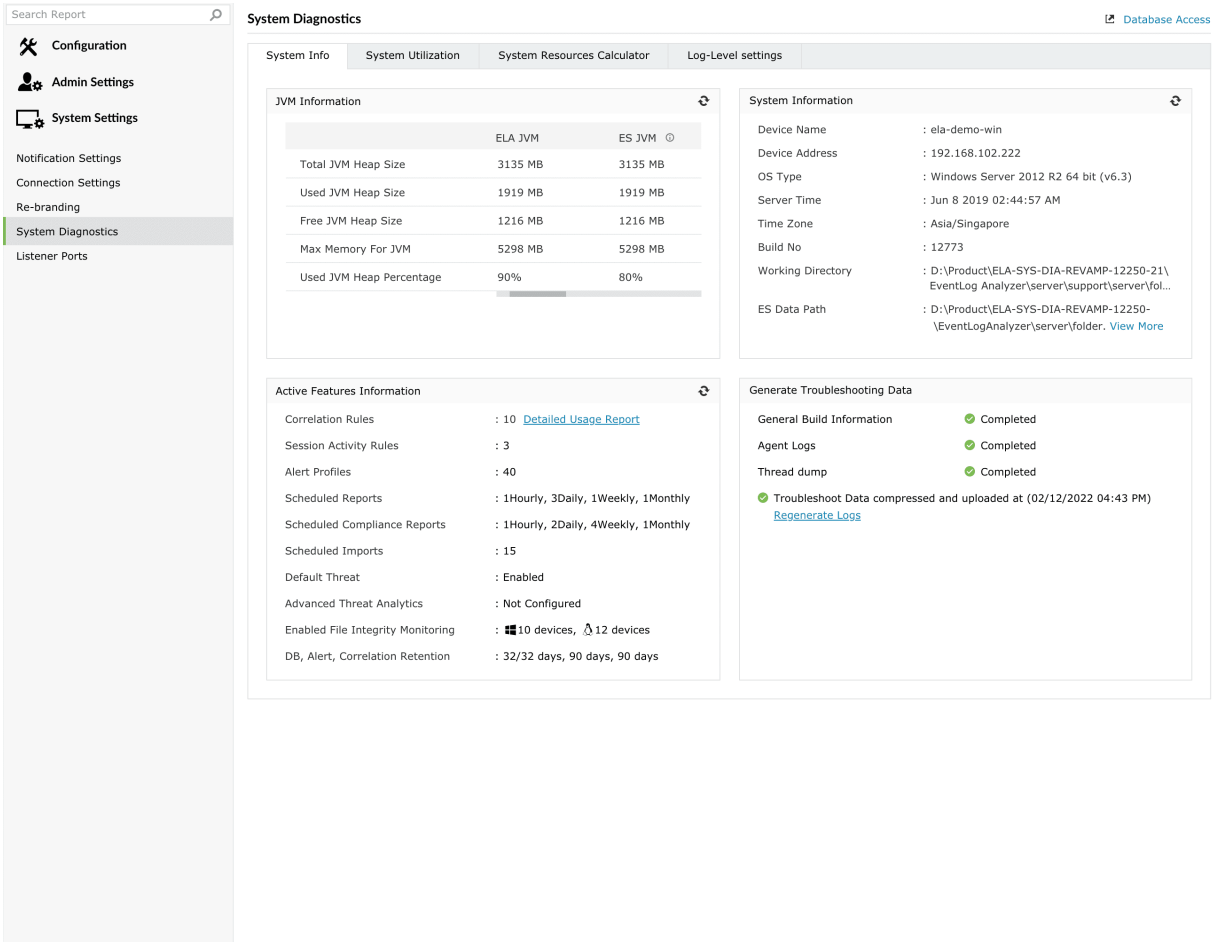
Automated upload process:

- Utilize the Auto option to compress and upload logs directly to the support server.
- Provide the necessary details, such as mail-id and ticket-id.
- Upon uploading, an acknowledgment mail will be sent.

Manual upload process:

- Alternatively, compress the logs manually.
- Choose the manual option for upload.
- Proceed with the manual upload to the server.



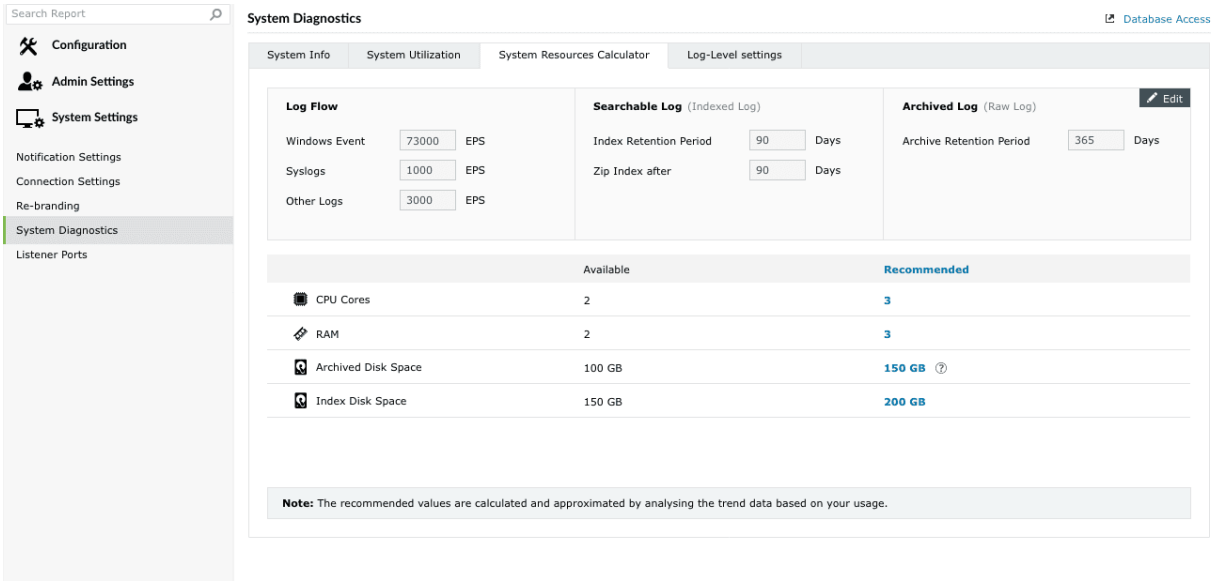

Search Report
Configuration
Admin Settings
System Settings
Notification Settings
Connection Settings
Re-branding
System Diagnostics
Listener Ports
System Diagnostics
Database Access
System Info
System Utilization
System Resources Calculator
Log-Level settings
JVM Information
ELA JVM
ES JVM
Total JVM Heap Size 3135 MB 3135 MB
Used JVM Heap Size 1919 MB 1919 MB
Free JVM Heap Size 1216 MB 1216 MB
Max Memory For JVM 5298 MB 5298 MB
Used JVM Heap Percentage 90% 80%
System Information
Device Name : ela-demo-win
Device Address : 192.168.102.222
OS Type : Windows Server 2012 R2 64 bit (v6.3)
Server Time : Jun 8 2019 02:44:57 AM
Time Zone : Asia/Singapore
Build No : 12773
Working Directory : D:\Product\ELA-SYS-DIA-REVAMP-12250-21\EventLog Analyzer\server\support\server\fol...
ES Data Path : D:\Product\ELA-SYS-DIA-REVAMP-12250-\EventLogAnalyzer\server\folder. View More
Active Features Information
Correlation Rules : 10 Detailed Usage Report
Session Activity Rules : 3
Alert Profiles : 40
Scheduled Reports : 1Hourly, 3Daily, 1Weekly, 1Monthly
Scheduled Compliance Reports : 1Hourly, 2Daily, 4Weekly, 1Monthly
Scheduled Imports : 15
Default Threat : Enabled
Advanced Threat Analytics : Not Configured
Enabled File Integrity Monitoring : 10 devices, 12 devices
DB, Alert, Correlation Retention : 32/32 days, 90 days, 90 days
Generate Troubleshooting Data
General Build Information Completed
Agent Logs Completed
Thread dump Completed
Troubleshoot Data compressed and uploaded at (02/12/2022 04:43 PM)
Regenerate Logs

9.5.8. System Resource Calculator

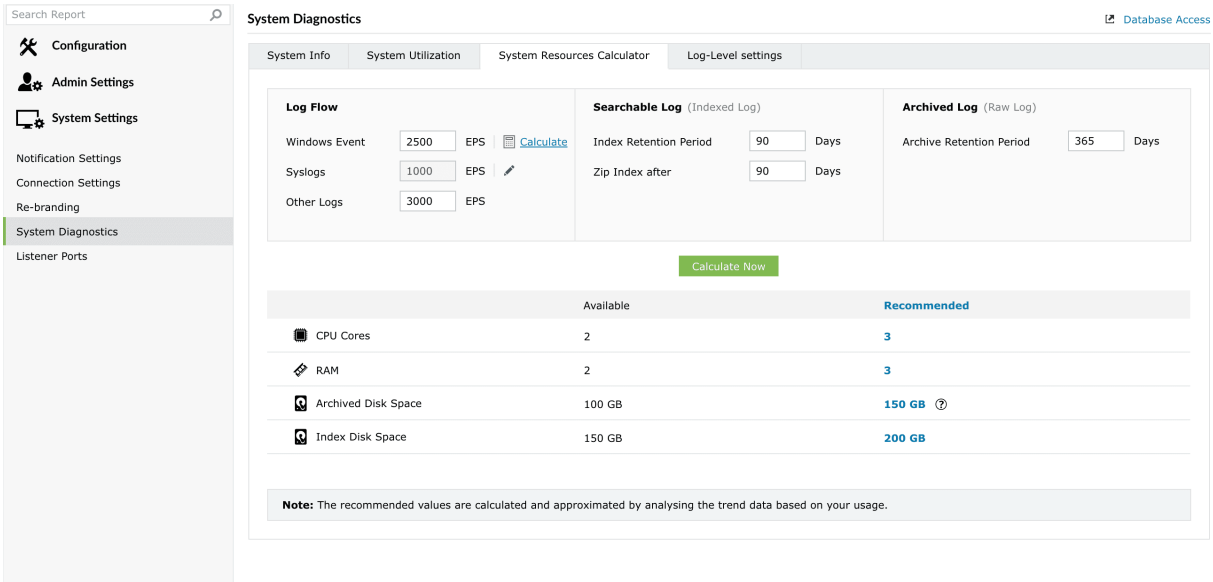
Last updated on: September 12, 2025

Recommended system resources are determined by analyzing the trend of your log flow rate and the resources it consumes. This information is extrapolated to align with your retention days.

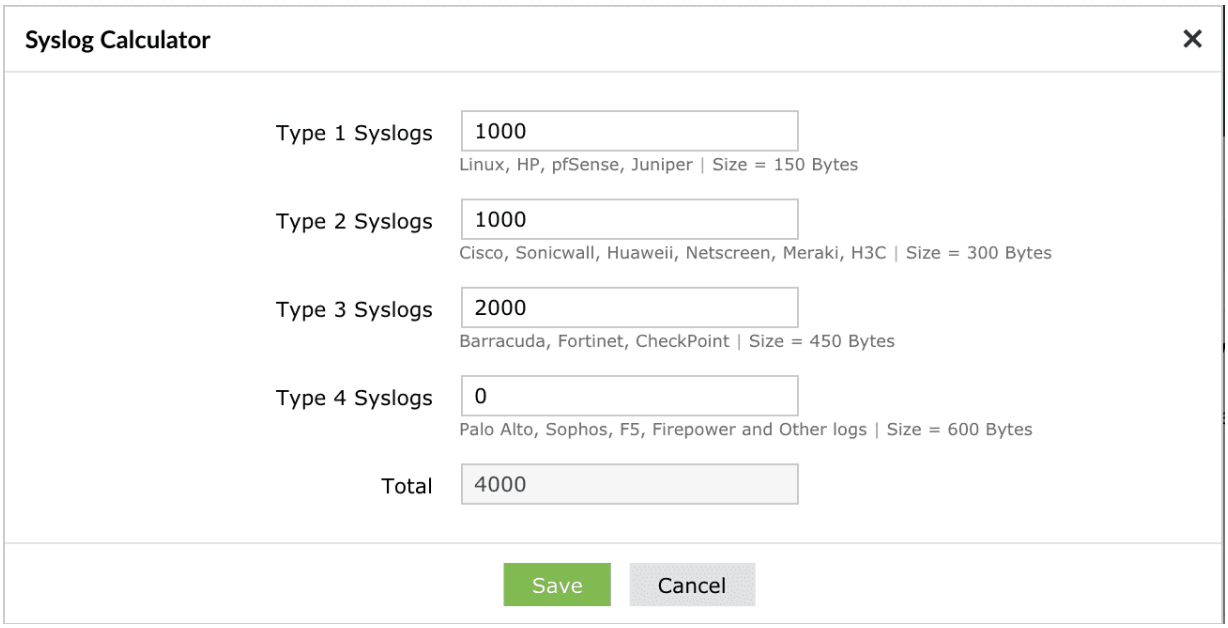
> **Note**
>
> The recommendation is based on trend data; it's advisable to run the product for at least 7 days to obtain more accurate recommendations.



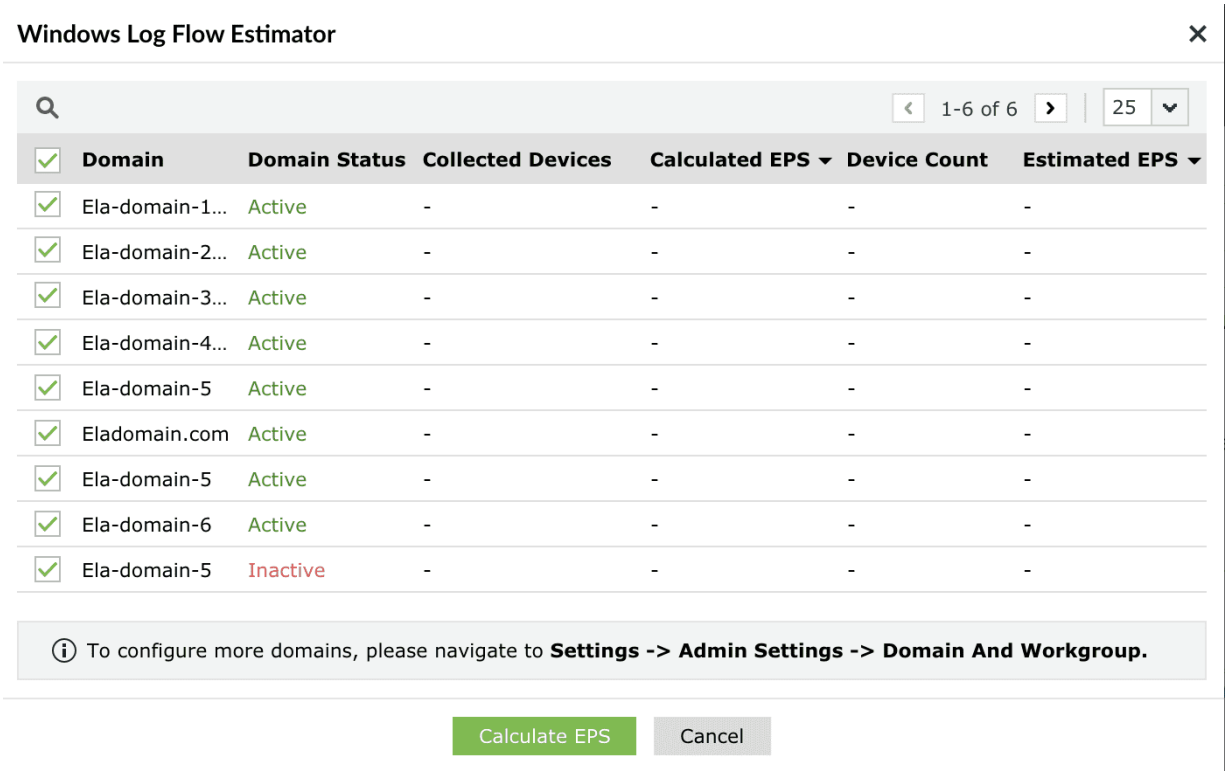
Modify log flow and retention values by clicking on "edit" to tailor your configurations according to your needs.

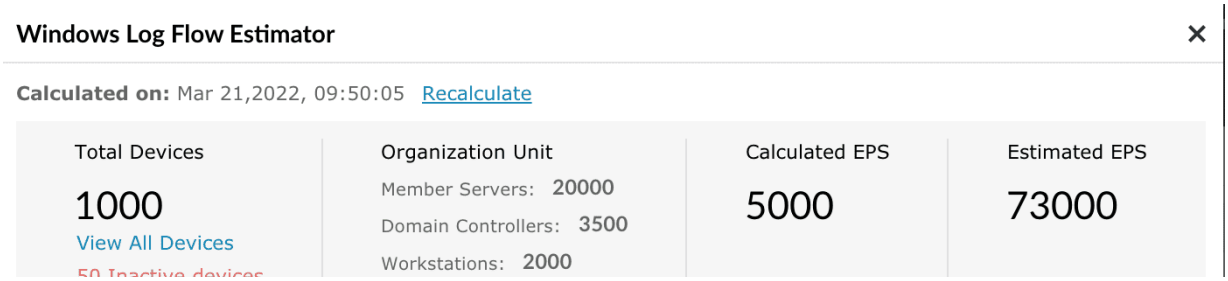


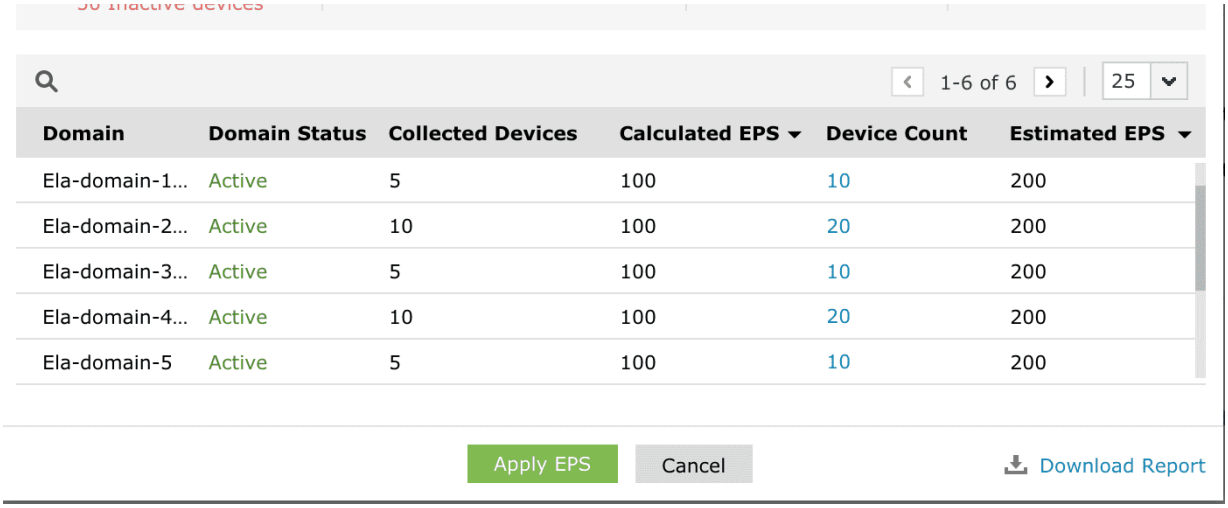
Clicking the edit icon triggers a popup where you can specify the types of syslogs you want to add, allowing you to tailor your configurations.



You can calculate the Windows Log flow rate for the configured domains.

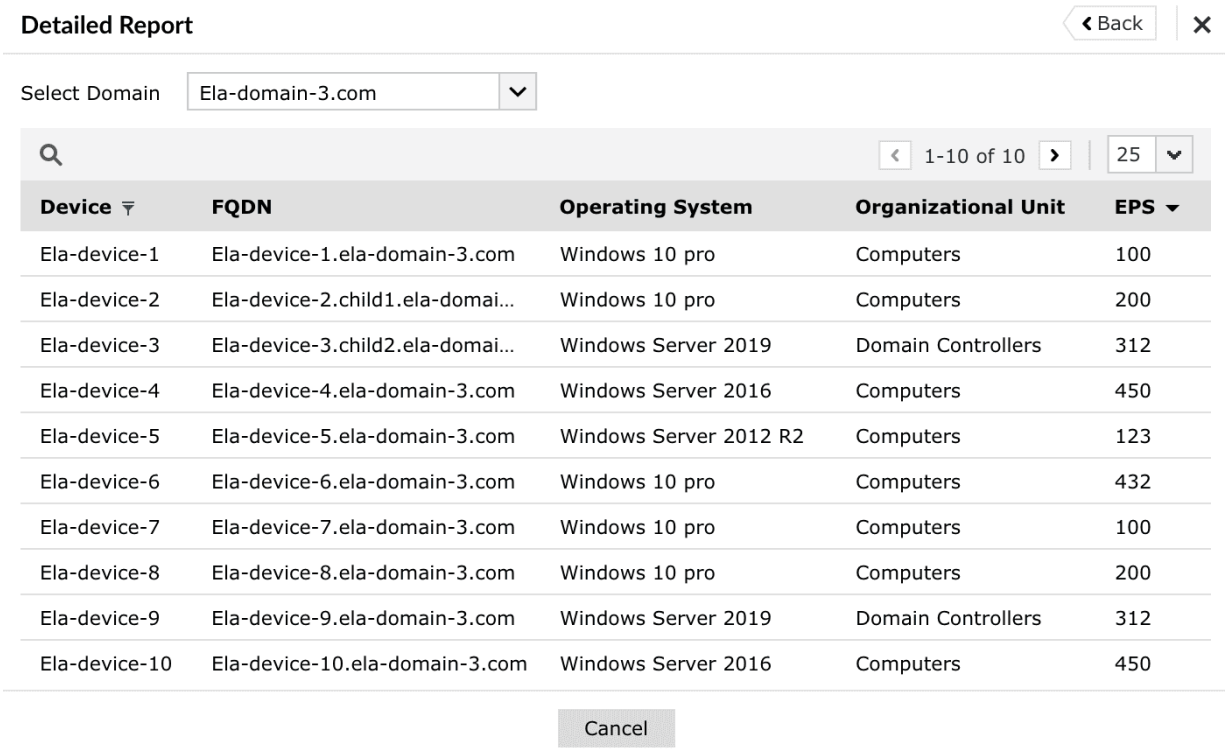




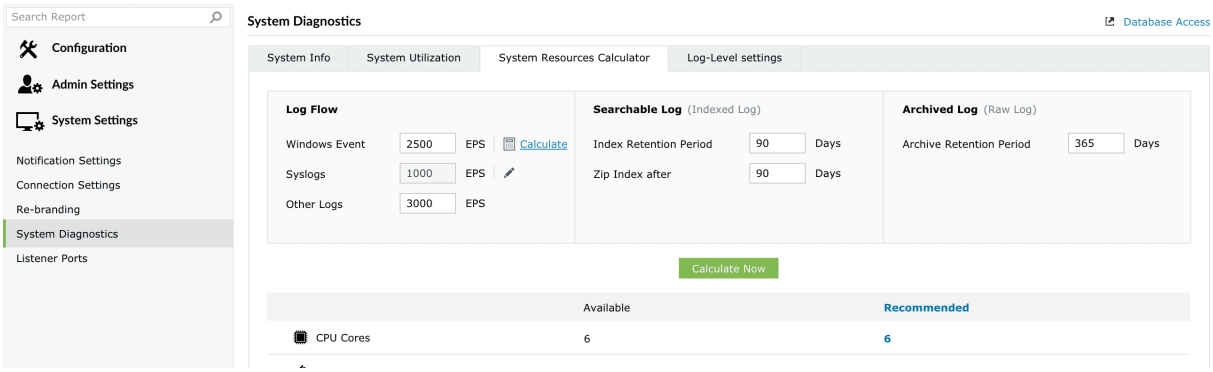


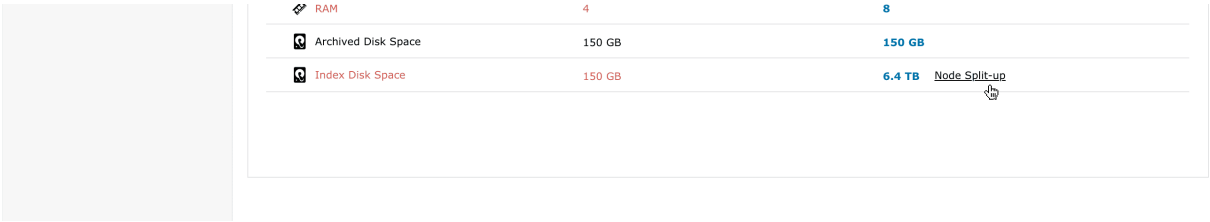
You can then apply the calculated EPS, to view your recommendations.

Clicking the Device count of each domain enables viewing the EPS of individual devices within the domain.



If the recommended value for Index Disk Space exceeds 1.5TB, the ES - Node Recommendation will be displayed.





Additional ES Node Recommendations

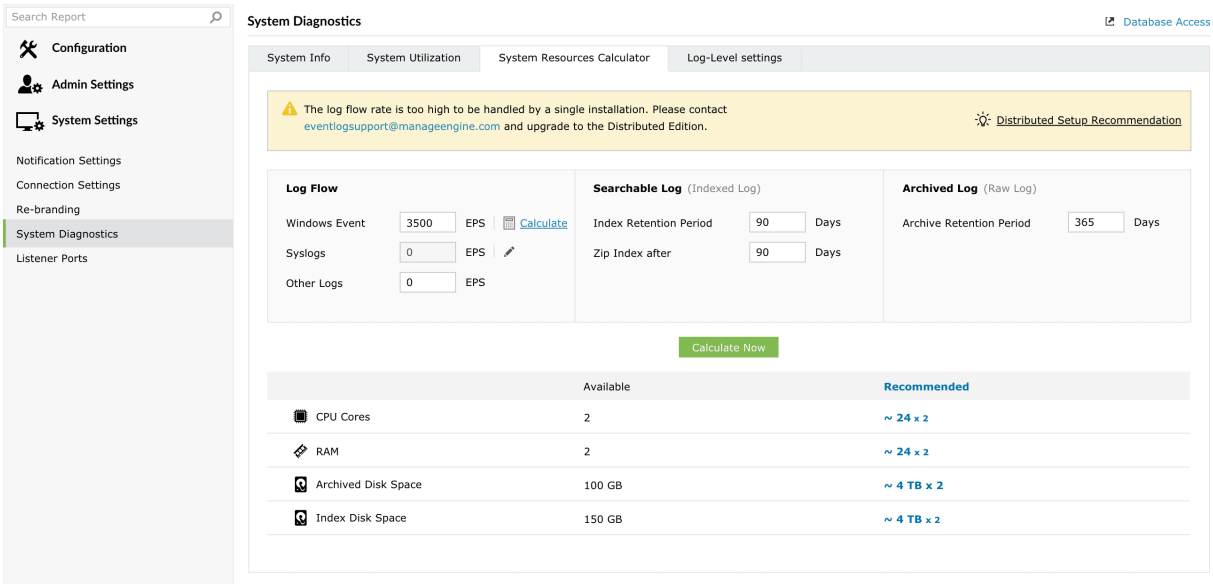
Required Disk Space : **6.4 TB**

It is recommended to split the load with 5 ES Nodes, with each node handling 800GB - 1TB of data with system requirements as below,

Hardware	Minumum	Recommended
Base Speed	2.4 GHZ	**3 GHz**
Core	12	**16**
RAM	64	**64**
Disk Space	1.2 TB	**1.5 TB**
IOPS	1500*	**1500***

OK

When the Log flow exceeds the high flow threshold, i.e., 3000 Windows EPS, the distributed setup recommendation will be shown.



Distributed Setup Split-Up

It is recommended to configure 3 Managed Server with the below system requirements,

Low Flow - 1 | Normal Flow - 0 | High Flow - 2

Hardware	Low Flow	Normal Flow	High Flow
Processor cores	6	12	24
RAM	16 GB	32 GB	64 GB
IOPS	150	750	1500
Disk Space	1.2 TB	3 TB	4 TB
Network card capacity	1 GB/s	1 GB/s	10 GB/s
CPU Architecture	64-bit	64-bit	64-bit

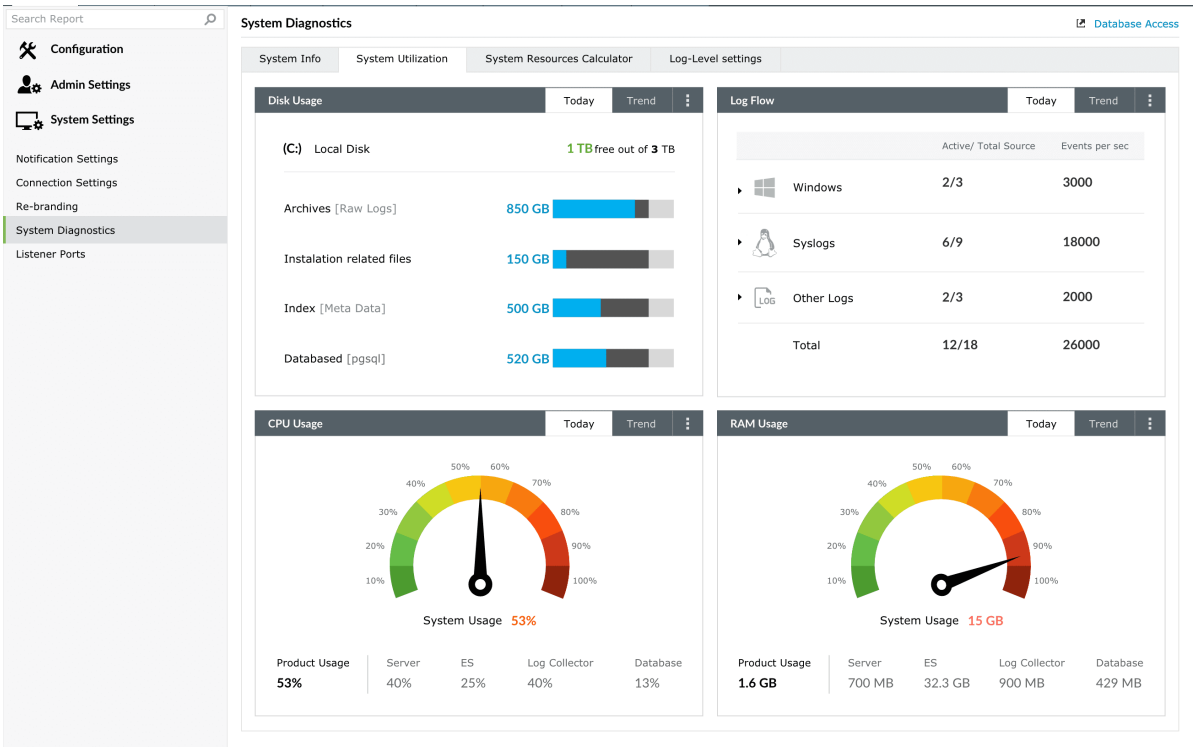
OK

9.5.9. System Utilization

Last updated on: September 12, 2025

To check the performance of the EventLog Analyzer server, you can use the System Diagnostics menu.

- In the Settings tab, navigate to System Settings > System Diagnostics.



- The details of Disk Usage, Log Flow, CPU Usage, and RAM Usage of ManageEngine EventLog Analyzer will be displayed here.

Disk Usage

For calculating the disk usage, we take four different modules into account, namely Archive, Index, Database, and Product disk space.

Recommendations

Here are some actions you can take if any module's disk space is low:

Archive disk usage

- Increase the disk space for the archive location.
- Reduce the archive zip creation interval so that the archive files will be zipped quicker and the disk usage will be reduced.
- Reduce the incoming log flow from the devices by collecting only the required logs. This helps avoid filling up disk space, and is accomplished using log collection filters.
- Decrease the archive retention period from the default of 90 days. If the archive retention period is set to

- Decrease the archive retention period from the default of 90 days. If the archive retention period is set to "forever", it can cause an increase in disk usage.

Index disk usage

- Increase the disk space at the indexing location.
- Change the indexing location from the default directory to another directory. Refer to this documentation to learn how to change the index location.
- Reduce the retention period. The index retention period is similar to the database retention period. It can be changed in Settings > Admin Settings > DB Retention Settings > Current Storage size.
- Reduce the incoming log flow, using log collection filters to avoid filling up the disk space.

Database disk usage

- Increase the disk space at the database location.
- If the disk utilization for the database is abnormal, contact EventLog Analyzer support and provide the following details:
  - Database retention period
  - Log inflow rate

Product disk usage

- Increase the disk space in the disk where EventLog Analyzer is installed.
- If the EventLog Analyzer instance is installed in the same directory as Windows, please migrate the instance to some other directory.
- Contact EventLog Analyzer support with these details about the folder that occupies the majority of the disk space:
  - (ELA-HOME)/ES/CachedRecord -> Number of entries
  - (ELA-HOME)/data/AlertDump -> Number of entries

Log Flow

Devices in a network generate huge quantities of logs, and this can slow down your system. Ensure that you collect only those logs that you require. Reducing the log flow can help optimize the usage of resources such as CPUs and servers, as it would require dealing with a lesser number of logs. A reduced log flow rate also reduces the load on databases and archives.

- Log Flow shows three different categories, namely Windows, Syslogs and Other logs.
- It displays the incoming log flow of all the devices based on log type.

This dashboard allows you to monitor the log flow rate for the different types of logs and manage your resources accordingly. You can also check the Trends tab to get a better idea of the log flow rates in the recent past.

Resource Usage

CPU and RAM usage displays the resources being used by the product's executables and the total usage by the server hosting EventLog Analyzer. Product executables include the server, Elasticsearch, the log collector, and the database.

Recommendations

Here are some actions that you can take to optimize the usage of resources:

CPU Usage

- Increase the number of CPU cores available.
- Check if there are any Cached Records being processed from (ELA-HOME)/ES/CachedRecord.
- Check if there is an Alert Dump in (ELA-HOME)/data/AlertDump.
- If the CPU usage is still high, contact Eventlog Analyzer support with the above details.

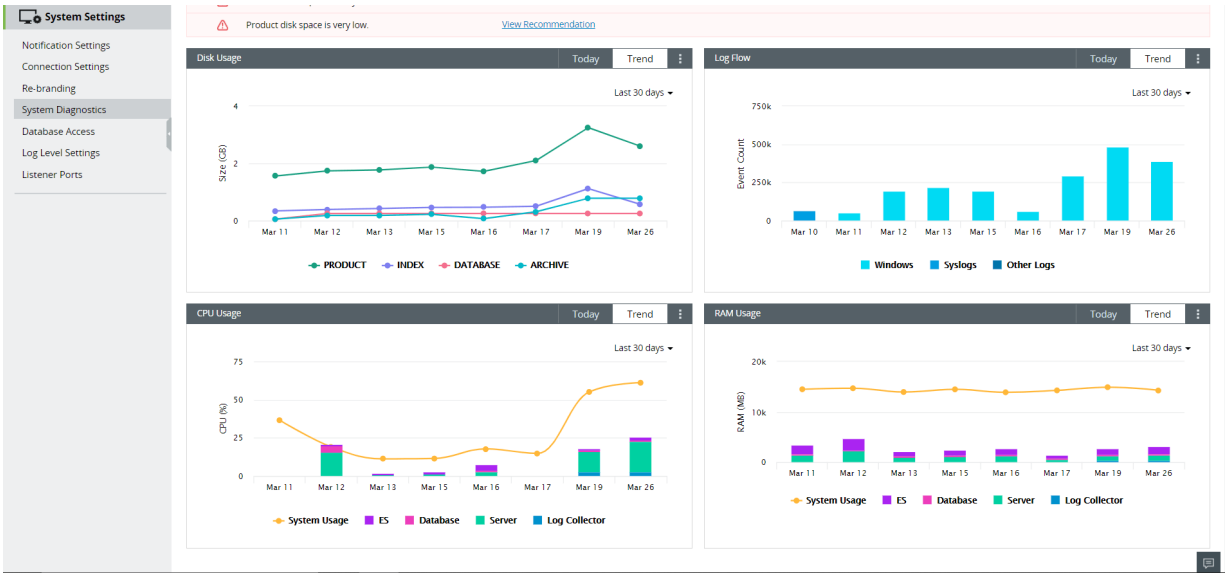
RAM Usage

- Increase the amount of RAM available.
- If the RAM usage is still high, contact EventLog Analyzer support.

Trends

EventLog Analyzer allows you to view the trends of the resources being utilized over a period of time. The Trends tab contains the data for each day the product is up and running, and can be viewed in three different formats:

- Last 7 days
- Last 14 days
- Last 30 days



9.5.10.1. SSL configuration for Log360

Last updated on: September 12, 2025

Log360 supports SSL connection to ensure security of data transferred between the browser and the Log360 server.

Steps to apply SSL certificate and enable HTTPS

Let's see how to generate and apply a SSL certificate for LOg360 and its integrated components.

- Navigate to Admin → General Settings → SSL Certification Tool.
- If you don't have a SSL certificate, select the Generate Certificate option and follow the steps here.
- If you already have a SSL certificate, select the Apply Certificate option and follow the steps here.

> **Note**
>
> SHA256 with RSA algorithm is currently supported for the SSL certificates.

Apply Certificate

If you already have a SSL certificate, follow the steps listed below to apply it.

- In the Apply Certificate to drop-down, select the component for which you want to apply the SSL certificate.
- Choose an Upload Option based on the certificate file type.
  - ZIP upload:
    - If your CA has sent you a ZIP file, then select ZIP Upload, and upload the file.
    - If your CA has sent you individual certificate files—user, intermediary, and root certificates, then you can put all these certificate files in a ZIP file and upload it.
  - Individual Certificates:
    - If your CA has sent you just one certificate file (PFX or PEM format), then select Individual Certificates, and upload the file.
    - If your CA has sent the certificate content, then paste the content in a text editor and save it as a CER, CRT, or PEM format, and upload the file.
  - Certificate Content:
    - If your CA has sent just the certificate content, then choose Certificate Content option, and paste the entire content.
- If the certificate file requires a password, then enter it in the Certificate Password field. Or, if the certificate contains a password-protected private key, enter the password in the Private Key Passphrase field.

> **Note**
>
> Only Triple DES encrypted private keys are currently supported.

- Click Apply.
- Finally, restart Log360.

Generate Certificate

- In the Common Name field, enter the name of the server.

  Example: For the URL https://servername:9251, the common name is servername.
- In the SAN Names field, specify the additional hostnames (e.g., sites, IP addresses, common names) that must be protected by the certificate.
- In the Organizational Unit field, enter the department's name which you want to be displayed in the certificate.
- In the Organization field, enter the legal name of your organization.
- In the City field, enter the name of the city as provided in your organization's registered address.
- In the State/Province field, enter the name of the state or province as provided in your organization's registered address.
- In the Country Code field, enter the two letter code of the country where your organization is located.
- In the Password field, enter a password that consists of at least 6 characters to secure the keystore.
- In the Validity (In Days) field, specify the number of days for which the SSL certificate will be considered valid.

  > **Note**
  >
  > When no value is entered, the certificate will be considered to be valid for 90 days.

- In the Public Key Length (In Bits) field, specify the size of the public key.

  > **Note**
  >
  > The default value is 2048 bits and its value can only be incremented in multiples of 64.

- After all values have been entered, you can select either of these two options:
  - Generate CSR

    This method allows you to generate the CSR file and submit it to your CA. Using this file, your CA will generate a custom certificate for your server.
    - Click Download CSR or manually get it by going to the <Install_dir>\Certificates folder.
    - Once you have received the certificate files from your CA, follow the steps listed under Apply Certificate to apply the SSL certificate.
  - Apply Self-signed Certificate

This option allows you to create a self-signed certificate and apply it instantly in the product. However, self-signed SSL certificates come with a drawback. Anyone accessing the product secured with a self-signed SSL certificate will be shown a warning telling them that the website is not trusted, which may cause concern.

9.5.10.2. What is SSL?

Last updated on: September 12, 2025

Acronym for Secure Socket Layer, SSL is an encryption technology to secure the data exchange between a website and its visitor's web browser. Normally, when a user communicates with a website, say submits his credit card information, the data travels to the server as plain text, which is susceptible to data theft!
On the other hand if this data is encrypted, then no eavesdropper can read it! Thus, it's really very important to secure a website with SSL!

Certificates and Certifying Authority (CA)

SSL Certificate:

This is a digital identity of a company, which ensures that a visitor is talking only to its intended website and whatever data he submitted to the site is encoded and reach only the intended site. This system is analogous to banks recognizing their customers by their signatures. In this case, the browsers (thereby the end-users) are programmed to trust these CA presented certificates.

Certifying Authority:

Regulatory organizations, who, with the help of standard policies, issue certificates to a domain, declaring them trustworthy. Every certificate they generate is unique to the company they are certifying, which makes identification easy.
CAs secure all necessary information about a company before issuing a certificate for it and also keep updating it in their records, which adds to the trustworthiness.
Some of the popular CAs are Verisign, Comodo & GoDaddy etc.

Keystore

Keystore is specifically designed to store various kinds of encryption information.

CSR

In order for a CA to generate an SSL certificate for a company, it first collects the information about the company and other identifiers such as public key (digital signature), and then binds them all with its certificate (which could be a piece of encrypted token or something similar). In doing so, it generates a unique identifier for the company. Thus every certificate issuance process begins with a "certificate request" from the company. CAs refer to this process as "Certificate Signing Request". The CAs accept the company information and digital signatures in a special form of file - the ".csr" file.

The Usual SSL Issuance Process

It involves 3 steps:

- First you generate a CSR and submit it to CA.
- CA binds this CSR with its digital signatures and returns it.
- Now, you bind all this with your company domain.

To enable SSL for Log360

For detailed instructions on how to enable SSL for Log360.

9.5.10.3. Server Settings

Last updated on: September 12, 2025

Under server settings, you can configure the mail server for sending notifications, alerts, etc., from the product and proxy settings in case you are using a proxy server. The following settings can be found here:

Mail Settings

Log360 provides two modes of mail server configuration:

1. SMTP
2. API

SMTP

This method allows you to create and authenticate a mail server via Basic or OAuth authentication.
To configure an SMTP mail server,

1. In the field, select SMTP.
2. Enter your mail server's Server Name or IP, and Port Number in the respective fields.
3. In the From Address field, enter the email address that will be used to send out notifications, alerts, etc., from Log360.
4. In the Admin Mail Address field, enter your email address if you wish to receive notifications for the emails sent from Log360.
5. Select the connection security type from the available options: SSL, TLS, or None.
6. Select the authentication type from the options provided:
   - Basic authentication
   - OAuth authentication
7. Basic authentication
   - Enter the Username and Password to access the mail server.
   - If your mail server does not require authentication, leave the fields empty.
8. OAuth authentication
   - Select your mail provider from the available options: Microsoft or Google.
   - If your mail provider is Microsoft, provide the Username, Tenant ID, Client ID, and Client Secret in the respective fields. In Log360, the Azure Cloud is considered the default Azure environment. You can modify the Azure environment setting by clicking the Choose the appropriate Azure environment link.

> Note:

To learn how to find your Azure Tenant ID, Client ID, and Client Secret, click here.

9. If you have selected Basic Authentication in step 6, you can have Log360 send a test email by clicking the Test Mail button.
10. Click Save Settings to save your mail server configuration.

API

This method allows you to create and authenticate a mail server via your mail provider's API.

- In the Mode field, select API.
- Select your mail provider from the available options: Microsoft or Google.
- In the From Address field, enter the email address that will be used to send out notifications, alerts, etc., from Log360.
- In the Admin Mail Address field, enter your email address if you wish to receive notifications for the emails sent from Log360.
- If your mail provider is Microsoft, provide the Tenant ID, Client ID, and Client Secret in the respective fields. In Log360, the Azure Cloud is considered the default Azure environment. You can modify the Azure environment setting by clicking the Choose the appropriate Azure environment link.

  Note:

  To learn how to find your Google Tenant ID, Client ID, and Client Secret, click here.

- If your mail provider is Google, upload the JSON private key file.

  Note:

  To learn how to get your JSON private key file, click here.

- Click Save settings.

Steps to find your Azure Tenant ID, Client ID, and Client Secret for SMTP mail server configurtion

- Log in to portal.azure.com.
- Under Azure services, click App registrations → New registration.
- Provide a Name of your choice and select the Supported account types. (Leave it as default).
- In the Redirect URI field, select web & paste the following OAuth link: https://identitymanager.manageengine.com/api/public/v1/oauth/redirect (or) You can also add the localhost redirect API in the following syntax.
  protocol://localhost:port_number/context_if_any/RestAPI/WC/OAuthSetting
  For example, http://localhost:8095/RestAPI/WC/OAuthSetting. If you have only added localhost as the redirect URI, you must access the product using localhost to configure mail server.

- In the next page, you will find the application details. Copy the Client ID & Tenant ID.
- From the left pane, click Certificates & secrets → New client secret.
- Provide a Description for the client secret, and in the Expires field, choose the validity of the client secret and click Add.
- The client secret will be generated. Copy the string displayed under Value.
- Click Save setting and complete the authorization prompt.

Steps to find your Google Workspace Client ID, and Client Secret for SMTP mail server configurtion

- Log in to console.developers.google.com.
- In the dashboard, click Create to create a new project if there is no existing project or select any existing project and click New Project
- Enter the Project Name. In the Location field, click Browse and select the parent organization. Click Create.
- In the left pane of the displayed project details page, click APIs & Services → Library.
- From the available list of APIs, select Gmail API and click Enable. You can make use of the search option to find the API quickly.
- In the left pane, click OAuth consent screen and choose the User Type. If you don't have a Google workspace account, choose External User.
- Provide the Application Name, Application Logo, and the support email of your help desk, developer information, and click Save & continue.
- Click Add or Remove Scopes, choose Gmail API (https://mail.google.com/), and click Update. Then, click Save & Continue.
- Add a test user and click Save & continue.
- In the left pane, click Credentials → Create Credentials → OAuth Client ID.
- Select the application type as Web Application. Provide a name of your choice.
- In the Authorized Redirect URIs, paste the following OAuth link: https://identitymanager.manageengine.com/api/public/v1/oauth/redirect (or) You can also add localhost redirect API in the following pattern.
  protocol://localhost:port_number/context_if_any/RestAPI/WC/OAuthSetting
  For example, http://localhost:8095/RestAPI/WC/OAuthSetting. If you have only added localhost as the redirect URI, you must access the product using localhost to configure the mail server.
- Click Save.
- Click DOWNLOAD JSON to download the file containing the authorization server details. Copy the Client ID and Client Secret displayed on the screen.

Steps to find your Azure Tenant ID, Client ID, and Client Secret for API mail server configurtion

- Log in to portal.azure.com.
- Under Azure services, click App registrations → New registration.
- Enter a Name of your choice and choose the Supported account types. (If you're unsure about the supported account types, select Accounts in the organizational directory only).

- In the left pane, click API Permission → Add a permission.
- Click Microsoft Graph → Application permission.
- Search Mail and select the permission Mail.Send. Click Add Permission.
- Click Grant admin consent.
- Copy the Client ID & Tenant ID displayed.
- In the left pane, click Certificates & secrets → New client secret.
- Provide a Description for the client secret. In the Expires field, choose the validity of the client secret and click Add.
- The client secret will be generated. Copy the string displayed under Value.

Steps to download JSON private key for API mail server configurtion

- Log in to console.developers.google.com.
- Open the Service accounts page.
- Click Create Project. Enter the project name, organization and location. Click Create.
- Click + Create service account button from the top row.
- Under Service account details, type a name, ID, and description for the service account, then click Create and continue.
- If required, you can also select the IAM roles to be granted to the service account using the Grant this service account access to project option.
- Click Continue
- If required, you can add the users or groups that are allowed to use and manage the service account.
- Click Done.
- Click the email address for the service account you created.
- Click the Keys tab.
- In the Add key dropdown list, select Create new key.
- Select key type as JSON.
- Click Create.

Your new public/private key pair will be generated and downloaded to your machine. Please keep the private key safe as this will be the only copy, and you cannot generate the same private key again.
Once you have downloaded the JSON private key, you'll have to enable Gmail API service and provide domain-wide authority to the service account.
Enable Gmail API service

- Login to console.developers.google.com.
- Select the project from the dropdown menu.
- Click + Enable APIS and Services.
- Select Gmail API and click Enable.

Delegating domain-wide authority to the service account

Delegating domain-wide authority to the service account

- Log in to the Google Workspace domain's Admin console as a super administrator.
- Navigate to Main menu → Security → Access and data control → API Controls.
- In the Domain wide delegation pane, select Manage Domain Wide Delegation.
- Click Add new.
- In the Client ID field, enter the service account's Client ID. You can find your service account's client ID on the Service accounts page.
- In the OAuth scopes (comma-delimited) field, enter the list of scopes that your application should be granted access to. For example, if your application needs domain-wide full access to the Google Mail API, enter: https://mail.google.com.
- Click Authorize.

Your application now has the authority to make API calls as users in your domain (to "impersonate" users). When you prepare to make authorized API calls, specify the user to impersonate as.

SMS Settings

You can configure Log360 to use your own GSM modem or your custom SMS gateway.

- GSM modem configuration
- Custom SMS Provider configuration

1. Configuring GSM Modem

- Navigate to Admin → General Settings → Server Settings.
- Click SMS Settings tab.
- Select GSMModem from the SMS Provider drop down box.
- Specify the Modem Port Number.
- Click Save Settings.

Steps involved in configuring the modem port & modem speed:

- Connect your GSM Modem to the Serial Communication Port.
- Only a serial cable must be used for connectivity.
- The port number for Window Devices will be comX. Eg. com7 or com8.
- Enter the Port Number to which the modem is connected :eg.(COM 1).

Requirements for Establishing SMS Server Connection:

- Modem/mobile must have GSM functionality with a provision to insert the SIM card.
- Should support 7-bit (GSM default alphabet), 8-bit and Unicode (UCS2) encoding.
- Make sure the GSM modem configured with Log360 is not used by any other application.
- If you experience any issue in sending SMS notifications through GSM modem, please restart Log360 and try again.

- Matching these criteria allows Log360 to support your modem/ mobile phone.

2. Configuring Custom SMS Provider

You can configure you own custom SMS gateway provided that the gateway is HTTP or SMTP based. Please follow the steps given below:

- HTTP-based SMS Provider
- SMTP-based SMS Provider
- SMPP-based SMS Provider

HTTP-based SMS provider:

- Navigate to Admin → General Settings → Server Settings.
- Click SMS Settings tab.
- Select Custom from the SMS Provider drop down box.
- Select HTTP from the Send SMS via drop down box.
- Select whether you want to use Post or Get HTTP method for sending SMS.
- Enter the HTTTP URL of your SMS gateway provider.
- Enter the HTTP Parameters specific to your SMS provider.

Note:

- Separate the HTTP parameters by an ampersand (&) sign.
- Example format: userName=xxx&password=yyy&mobileNumber=%mobNo&message=%message%.
- You can use the following parameters:
  - userName = the parameter which is used to denote the API authentication username.
  - xxx = API authentication username.
  - password = the parameter which is used to denote the API authentication password.
  - yyy = API authentication password.
  - mobileNumber = recipient parameter.
  - %mobNo% = this macro denotes the user's mobile number.
  - message = message parameter.
  - %message% = this macro denotes the SMS message content.
  - More HTTP Parameters - If you SMS provider requires more parameters like unicode and apiID, include them as well using the '&' sign.
- Specify the response you get from your provider to determine whether the SMS has been sent successfully.
- Click Advanced Settings. Enter the HTTP Request Headers specific to your SMS provider.

- Select the option Convert Message into Unicode to send SMS in Unicode format.
- Click Save.

SMTP-based SMS provider:

- Navigate to Admin → General Settings → Server Settings.
- Click SMS Settings tab.
- Select Custom from the SMS Provider drop down box.
- Select SMTP from the Send SMS via drop down box.
- In the From Address field enter an email address from which you want to send the SMS. Eg: noreply@adselfserviceplus.com
- In the To Address field enter the %mobNo% macro followed by the email of your provider. For example: %mobNo%@clickatell.com. Refer your SMS provider to know the exact values.
- Enter the details required in the Subject field. Generally, it would be either mobile number or message depending upon your SMS provider.
- Enter the details required in the Content field. This also depends on your SMS provider. Please refer them to know the exact values.
- Click SMTP Server Settings.
- Enter the name or IP address of the “SMTP Server” and its Port number.
- Enter the username and password of the SMTP server.
- Click Save.

Note: If you don't configure the SMTP server settings, then the mail server configured under the Mail Settings tab will be used.

SMPP-based SMS provider:

- Navigate to Admin → General Settings → Server Settings.
- Click SMS Settings tab.
- Select Custom from the SMS Provider drop down box.
- Select SMPP from the Send SMS via drop down box.
- Enter the SMPP Server Name and its SMPP Server Port.
- Enter the Username and Password of the SMPP server.
- Click Advanced Settings.
- Enter the SMPP Source Address.

- Select the Source Address's TON (type of number).
- Select the Source Address's NPI (Numeric Plan Indicator).
- Select the Destination Address's TON.
- Select the Destination Address's NPI.
- Click Save Settings.

Proxy Settings

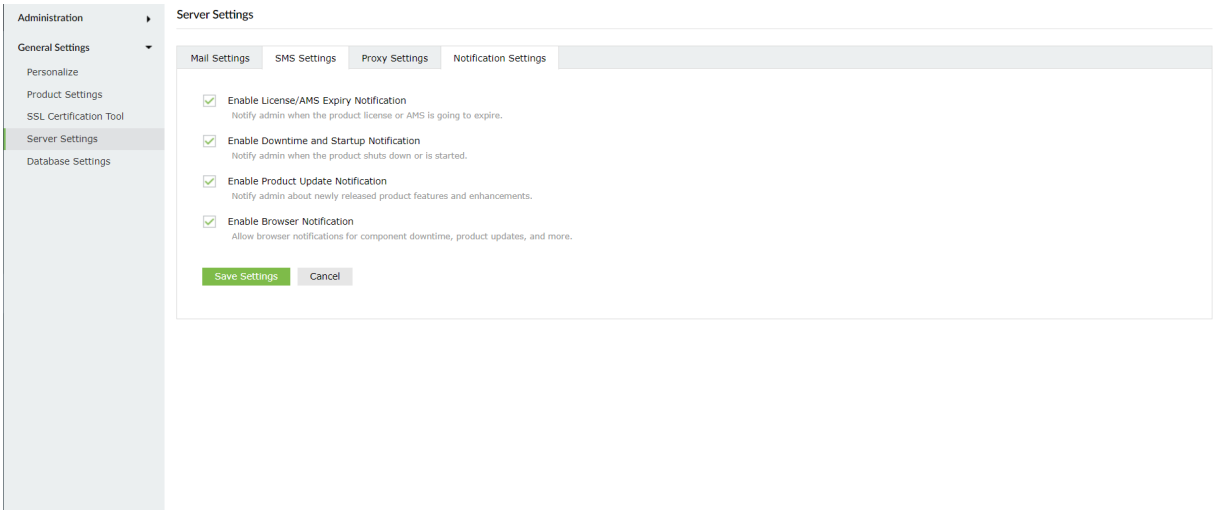
- Navigate to Admin → General Settings → Server Settings.
- Click on the Proxy Settings tab.
- Select the Enable Proxy Server option.
- Enter the proxy server's name or IP address and the port number in their respective fields.
- Enter the username and password credentials for accessing the proxy server.
- Click Save Settings.

Alternatively, you can also change the Proxy settings by following the steps listed below:

- Navigate to Support tab.
- Click on Check for updates box at the top right corner of the page.
- Click Settings link in the pop-up that appears, then click on Proxy Settings tab.
- Select Enable Proxy Server option.
- Enter the proxy server's name or IP address and the port number in their respective fields.
- Enter the username and password credentials for accessing the proxy server.
- Click Save Settings.

Notification Settings

These settings help you select the notifications you receive from Log360.



- Navigate to Admin → General Settings → Server Settings → Notification settings.
- To notify the admin when the license is about to expire, check the box next to Enable License/AMS Expiry Notification.
- To notify the admin when the application shuts down unexpectedly, check the box next to Enable Downtime Notification.
- To notify the admin about newly released product features and enhancements, check the box next to Enable Product Update Notification.
- To receive notifications from Log360 as push notifications straight to your web browser, check the box next to Enable Browser Notification.
- Click Save Settings.

9.5.11. Agent Administration

Last updated on: September 12, 2025

In EventLog Analyzer, an agent might be required in one of the following two scenarios:

- If you want to monitor the files in Windows file servers.
- If there are any RPC connectivity issues between the log source and the EventLog Analyzer server.
- Installation of Windows agent application is mandatory to collect Windows eventlogs for EventLog Analyzer deployed on Linux operating systems.

Supported operating systems:

EventLog Analyzer agent can be installed and run on the following operating systems
Windows Client OS: Windows XP and Above
Windows Server OS: Windows Server 2003 and Above

Linux:

- Linux RedHat RHEL
- Linux SuSE
- Linux Fedora
- Linux CentOS
- Linux Ubuntu
- Linux Debian

Installing the EventLog Analyzer agent

> Note: For additional information on what is needed in order for Windows agent to operate properly, click here.

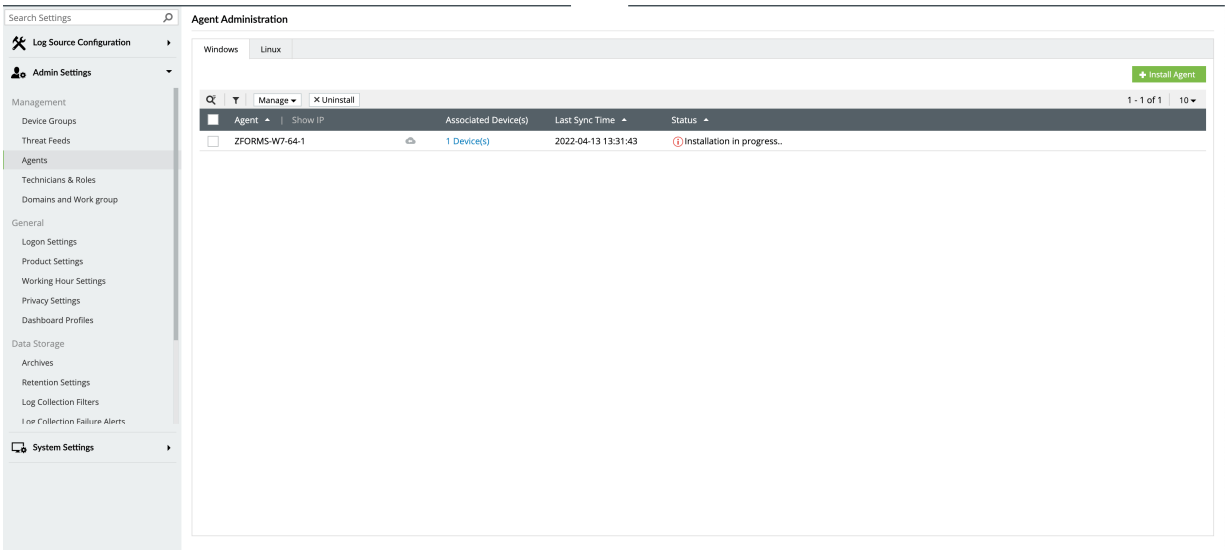
The following are the different ways in which you can deploy the EventLog Analyzer agent in devices:

- Using the EventLog Analyzer console
- Using GPOs
- Using Microsoft System Center Configuration Manager (SCCM) or some similar software deployment tool
- Manual installation

Using EventLog Analyzer console:

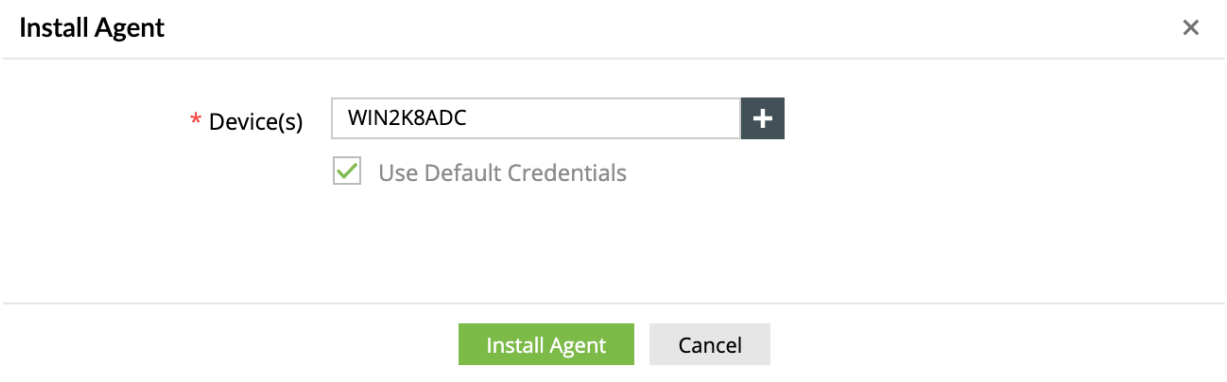
To install the EventLog Analyzer agent using the product console,

- In the Settings tab, navigate to Admin Settings → Manage Agents.
- Click + Install Agent and then the + icon corresponding to Device(s).

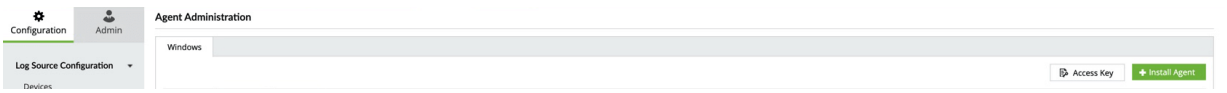


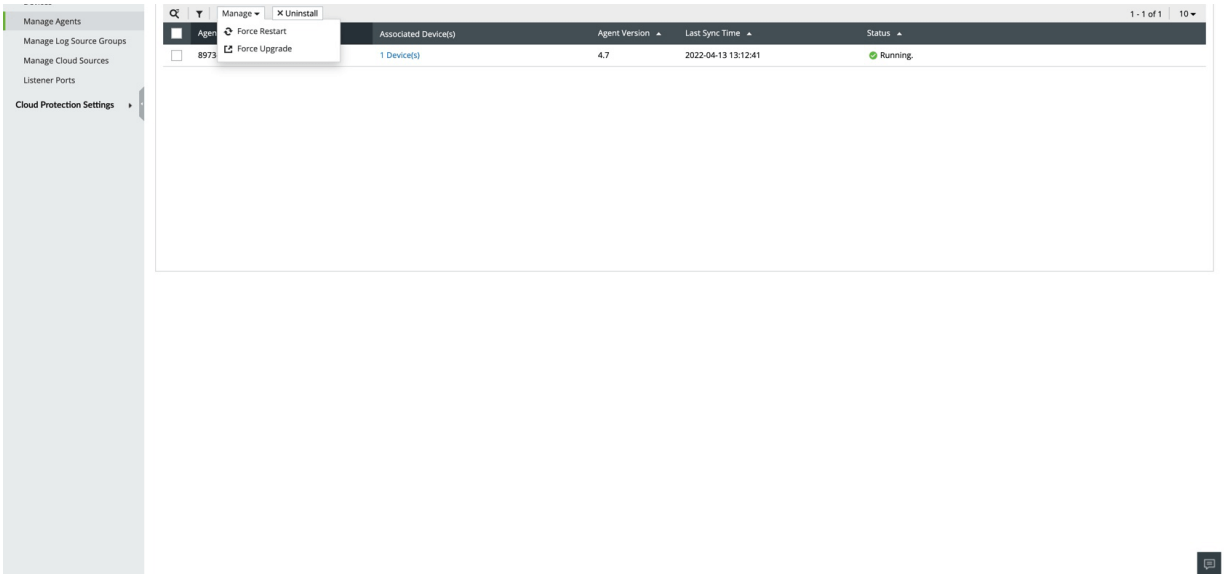
- Select the devices on which you want to install the agent.
- Enter the login name and password to access the device(s). This account should have admin privileges to install the agent successfully. Or you can also choose the Use Default Credentials option.

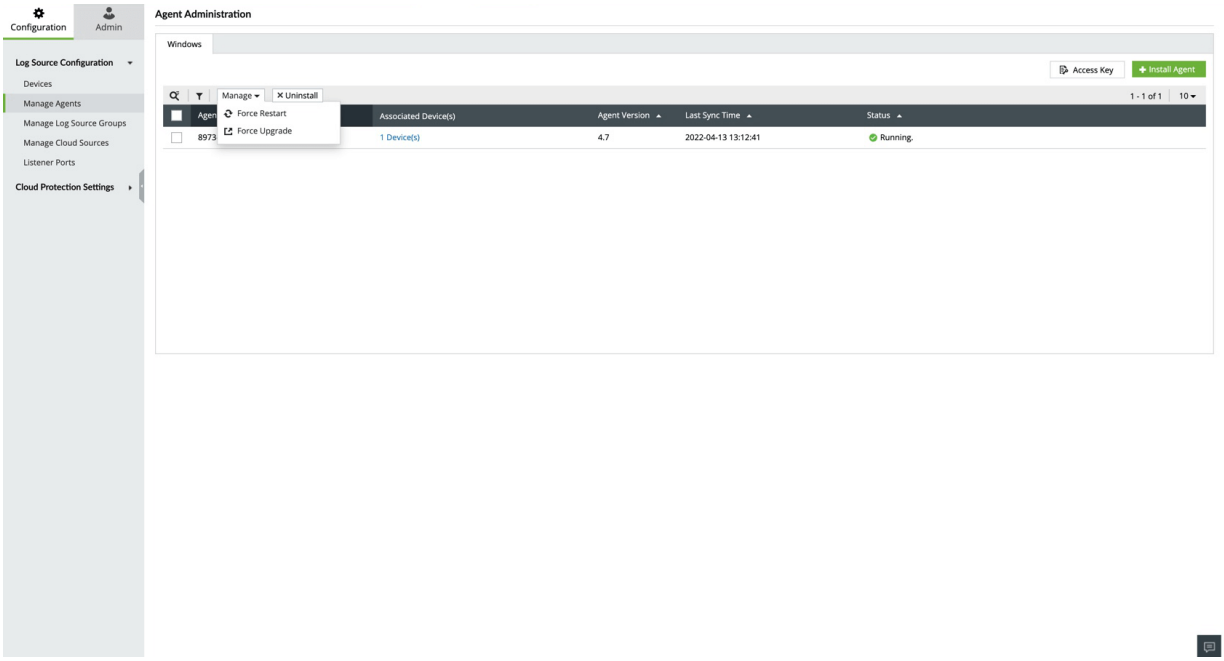
> **Note**
>
> If multiple devices are selected, ensure that the credentials are valid for all the devices.



- Use the Verify Credential link to validate the credentials entered.
- Finally, click Install Agent to initiate agent installation.







Using GPOs:

Before beginning to install the EventLog Analyzer agent using GPOs, place the following files in a network-shared folder of the server:

- InstallEventLogAgent.vbs (Path: <Installation Directory>\ManageEngine\EventLog Analyzer\tools\scripts)
- EventLogAgent.msi (Path: <Installation directory>:\EventLog Analyzer\lib\native)

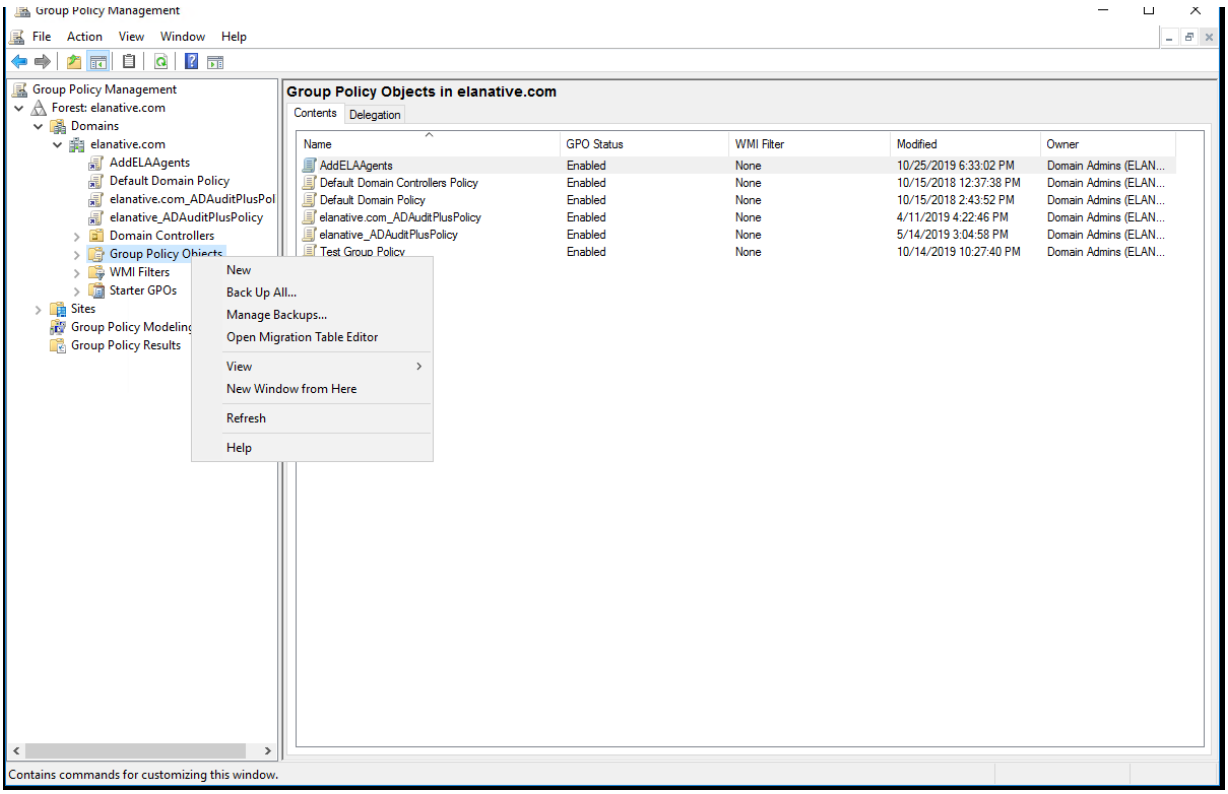
To install the agent via GPOs:

Step 1: Creating a GPO

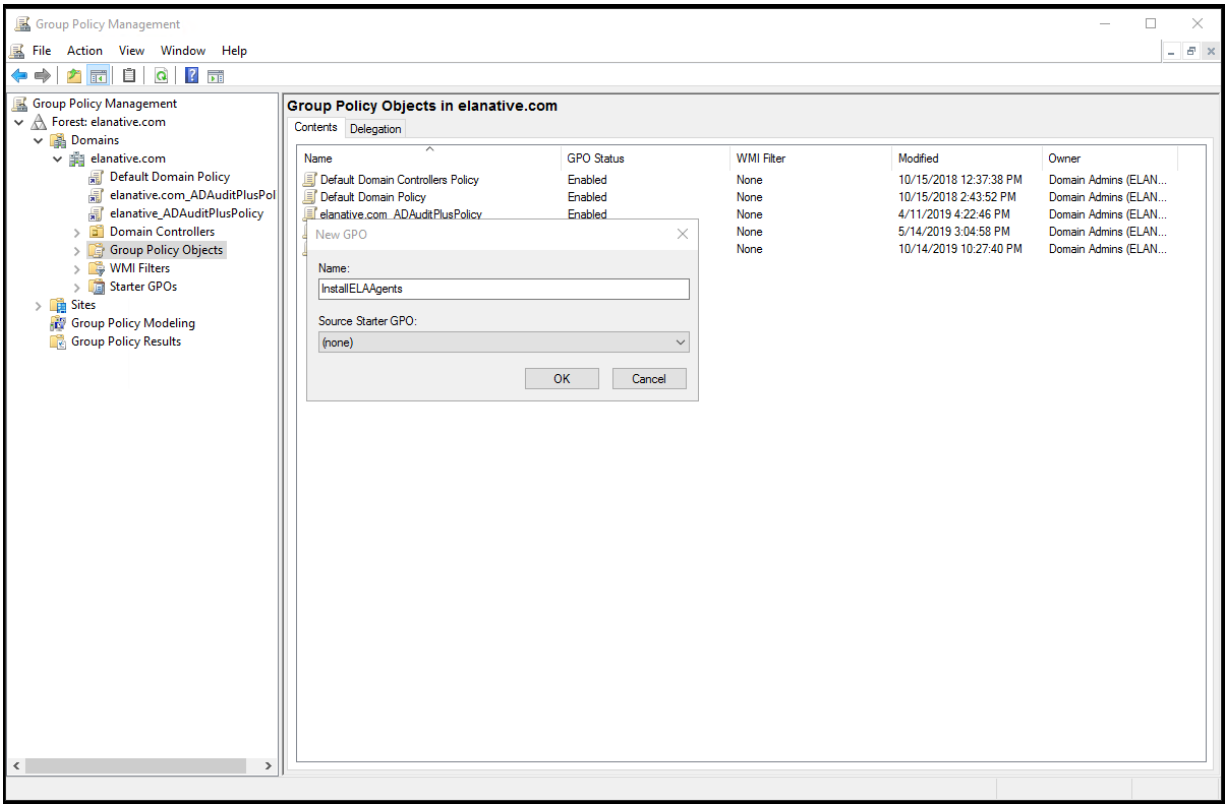
Create a new GPO as follows (based on the Windows Server version):

1. Open Group Policy Management.
2. In the left pane, right-click the Group Policy Objects container and select New.





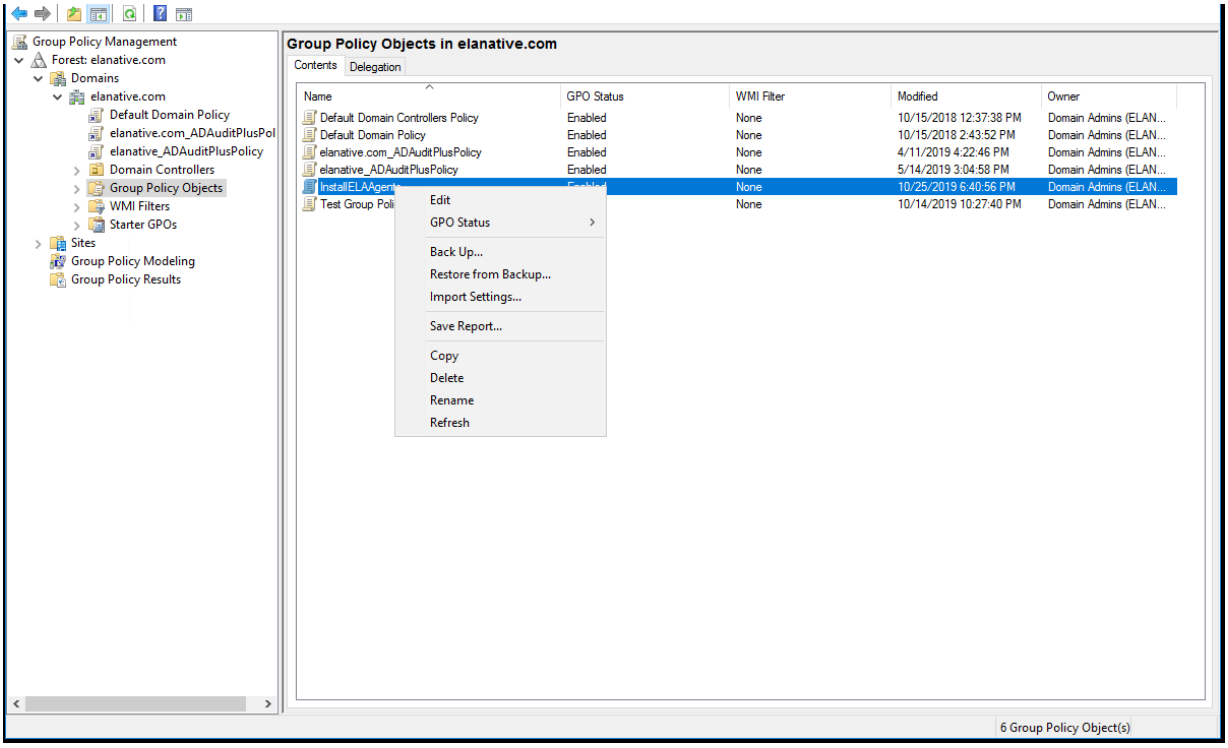
1. Give the GPO a suitable name and click OK.



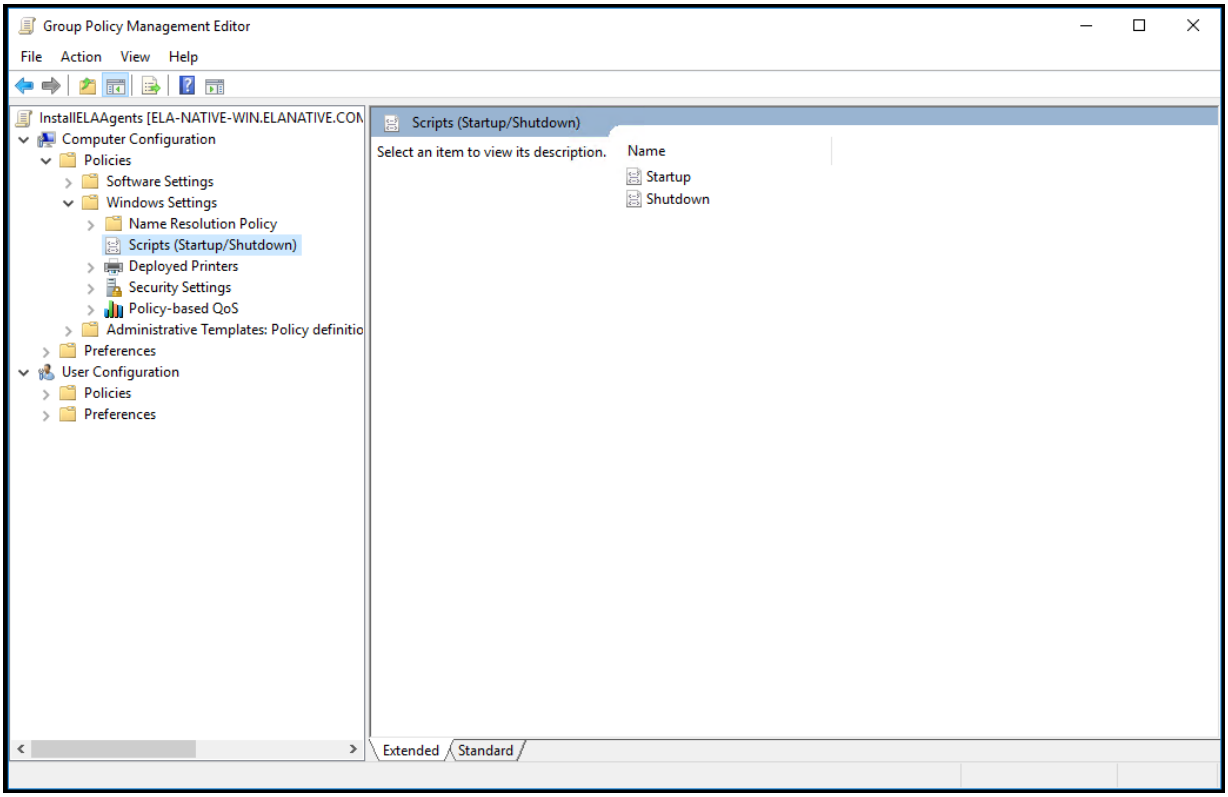
Step 2: Configuring script settings

1. Right-click the newly created GPO and click Edit.



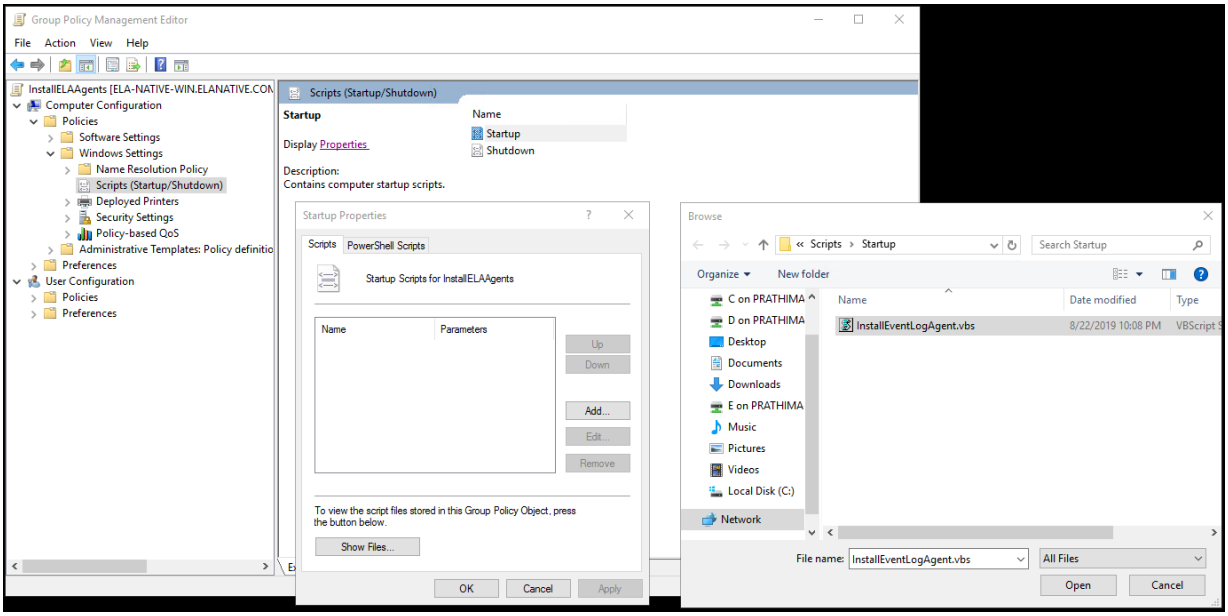


1. For Windows Server 2003, in the right pane of the GPO editor, double click Computer Configuration and navigate to Windows Settings → Scripts (Startup/Shutdown) → Startup.
2. For Windows Server 2008 and later, navigate to Computer Configuration → Policies → Windows Settings → Scripts (Startup/Shutdown) → Startup.



1. Right-click Startup and in the dialog box that appears, click Add.
2. In the Add Script dialog box, click Browse and select InstallEventLogAgent.vbs from the shared location

2. In the Add Script dialog box, click Browse and select InstallEventLogAgent.vbs from the shared location.

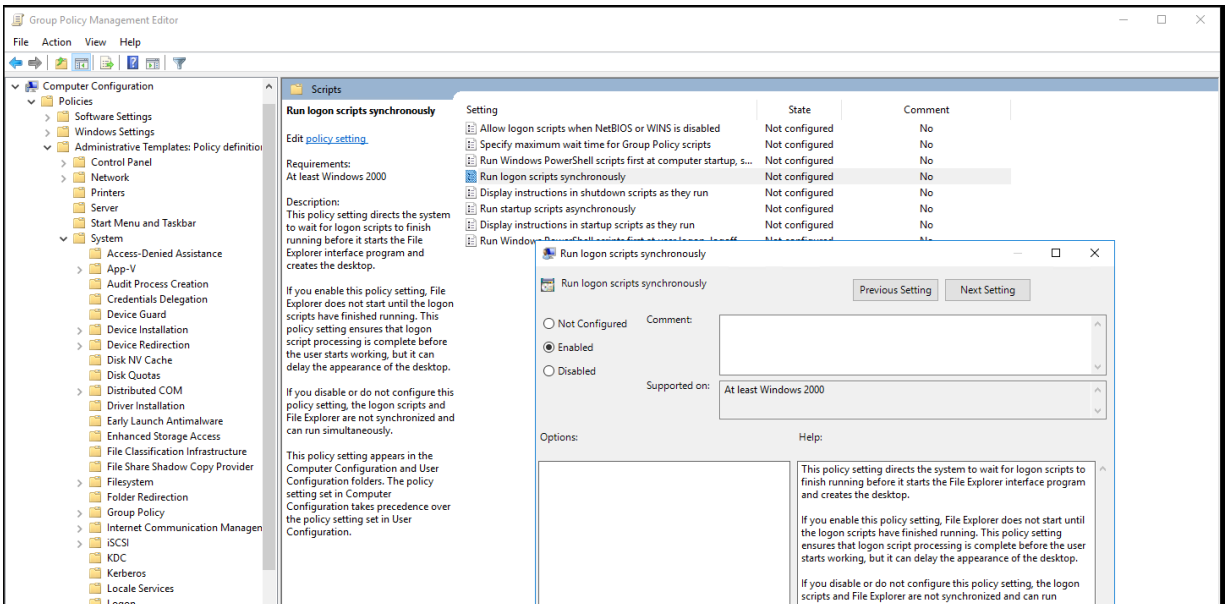


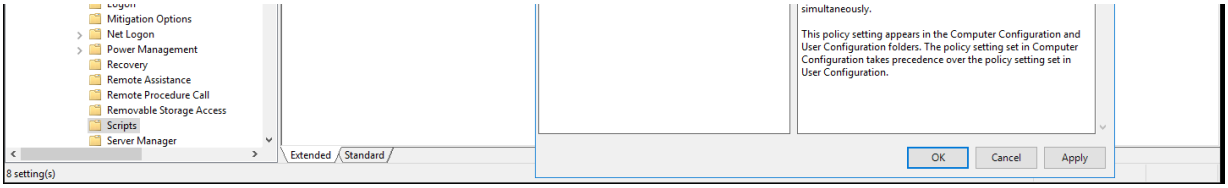
1. In the Script Parameters field, enter the following parameters:

   Example:
   /MSIPATH:"\\192.168.1.5\elaagent\EventLogAgent.msi" /SERVERNAME:"DC01"
   /SERVERIPADDRESS:"192.168.1.5" /SERVERPORT:"8095" /SERVERPROTOCOL:"http"
2. Click OK to return to the Startup Properties dialog box.
3. Click Apply and then OK.

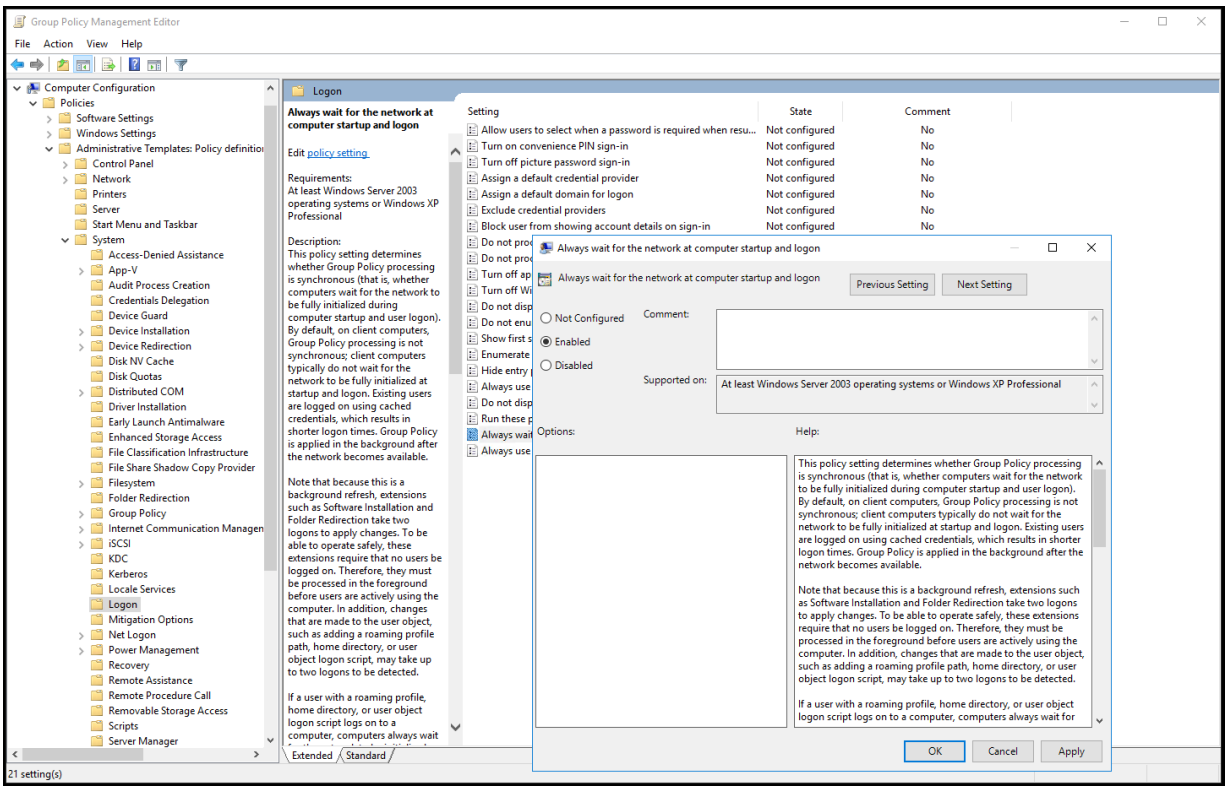
Step 3: Configuring Administrative Template Settings

1. In the left pane of the Group Policy Management Editor, navigate to Computer Configuration → Administrator Templates → System.
2. Under System, select Scripts.
3. In the right pane of the GPO Editor, double-click Run logon scripts synchronously and enable it.
4. Click Apply and then OK.

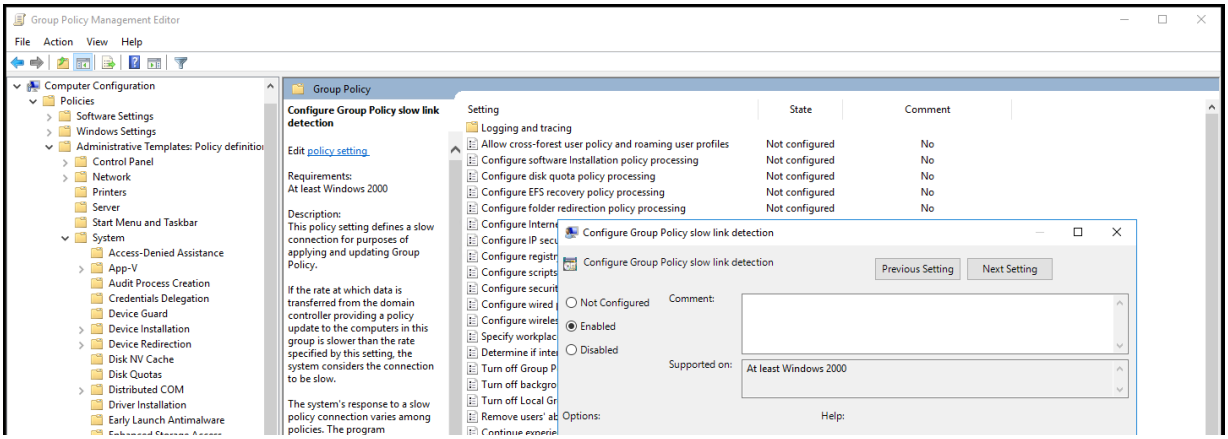


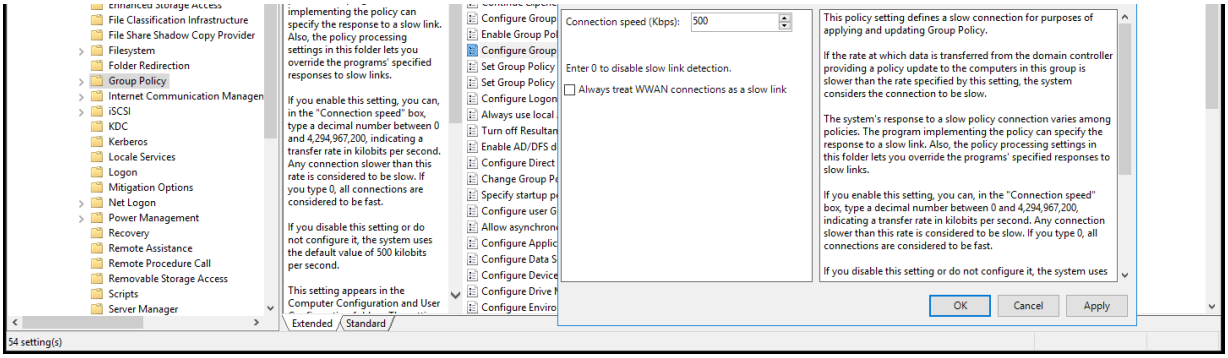


1. Similarly, enable Maximum wait time for Group Policy scripts.
2. Then, navigate to Logon under System.
3. In the right pane, double-click Always wait for the network at startup and logon and enable it.
4. Click Apply and then OK.



1. Then, navigate to Group Policy under System.
2. In the right pane, double-click Group Policy slow link detection and enable it.
3. Click Apply and then OK.

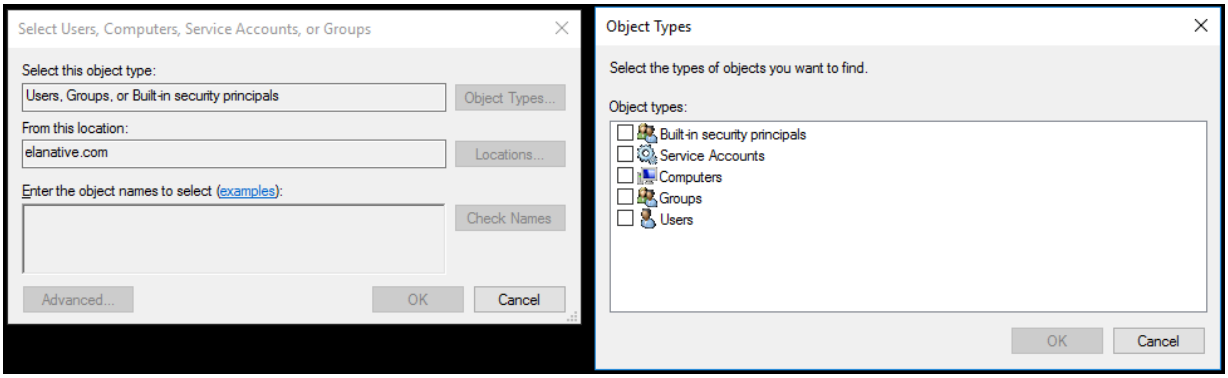




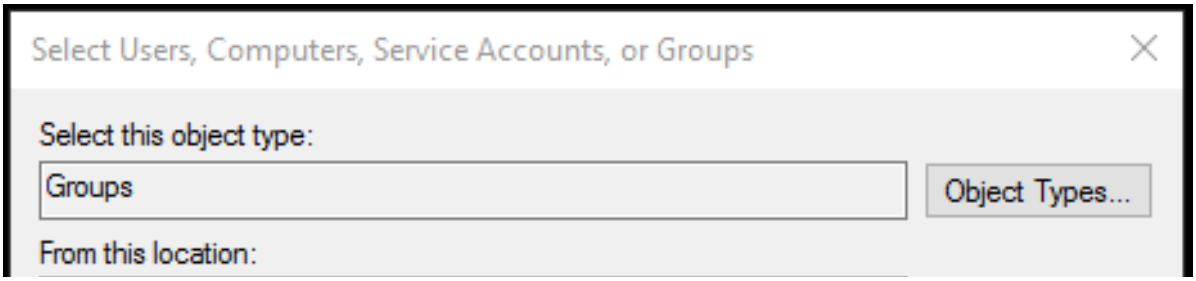
Step 4: Applying the GPO

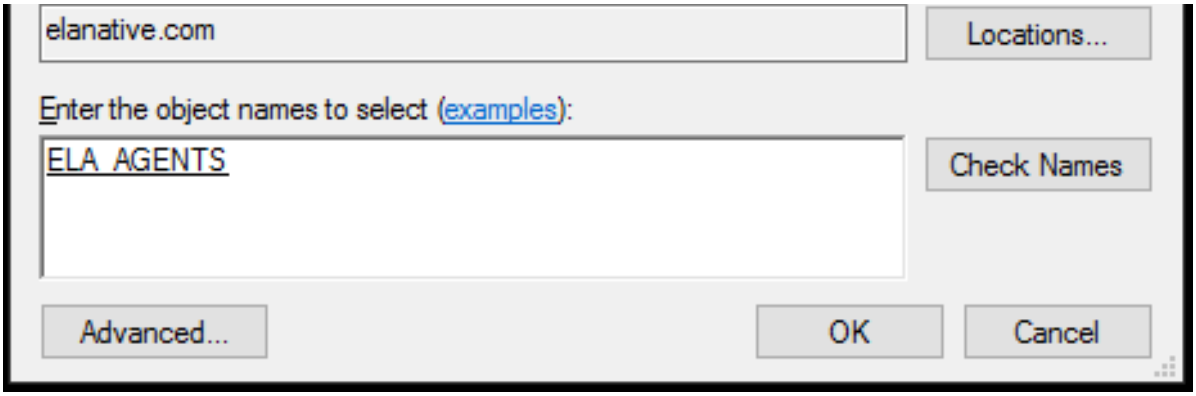
> Tip: For installing the agent on multiple computers at one go, create an AD group and add all the computers on which the agent needs to be installed to the group. Then, apply the GPO to that group.

1. On the left pane of the Group Policy Management Editor, right-click the GPO you are working on and select Properties.
2. Navigate to the Security tab and unselect the Apply Group Policy permissions for Authenticated Users.
3. Click Add and in the dialog box that appears, click Object Types.



1. If you want to apply the GPO to computers directly, ensure Computers is selected and then click OK. For applying it to a group, ensure Groups is selected and then click OK.
2. Enter the name of the desired computer(s) and/or group(s) and click Check Names.
3. Select the desired computer(s) and/or group(s) and click OK to return to the properties dialog box.

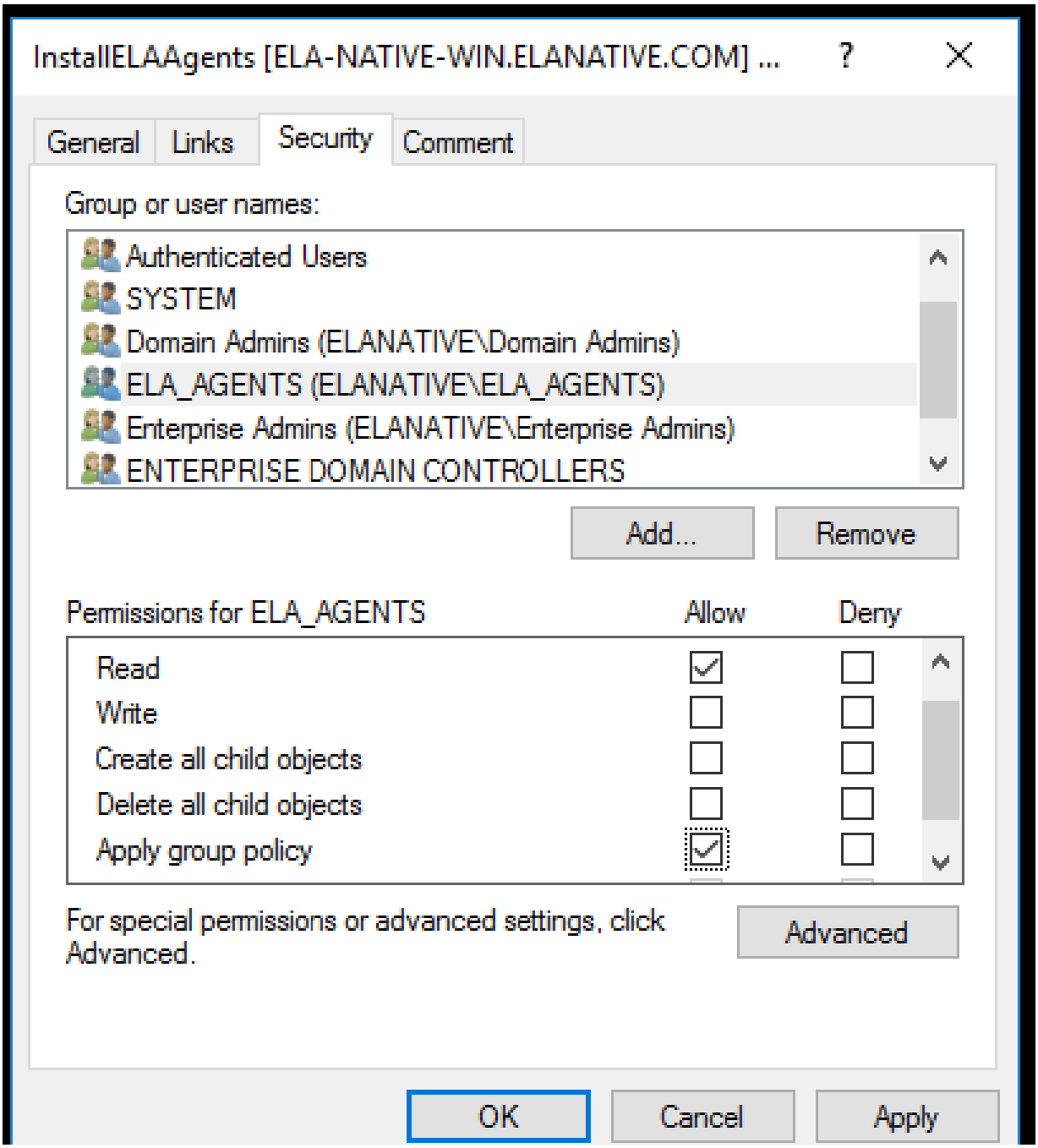




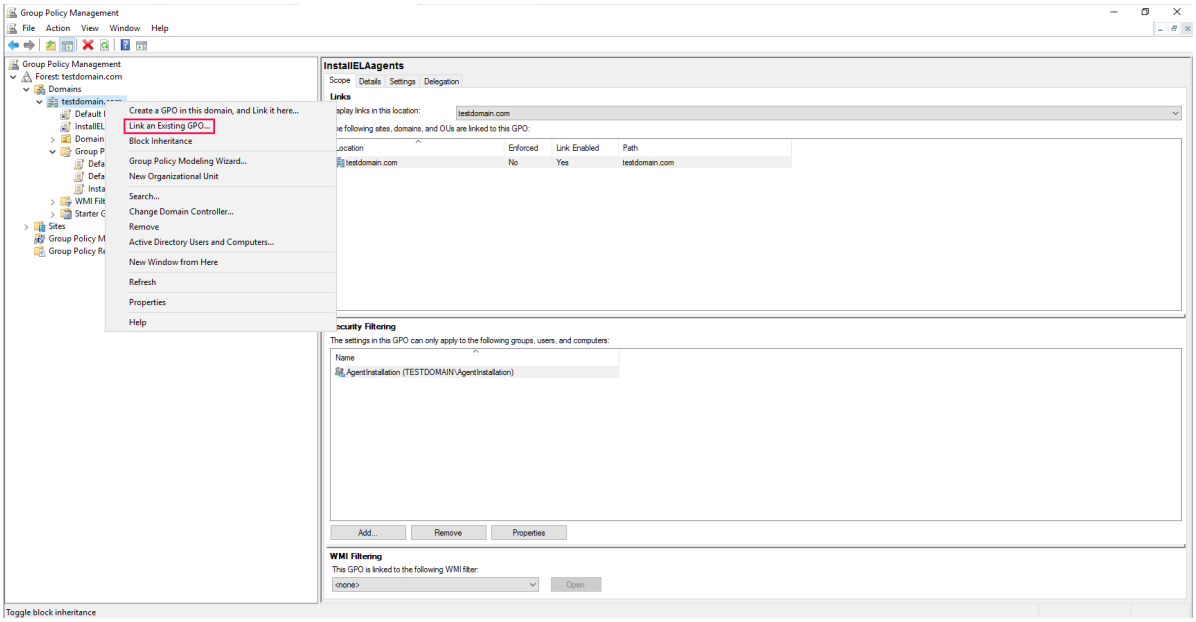
4. In the Security tab, apply the following permissions to the selected group(s) and/or computer(s):

   (i) Read > Allow

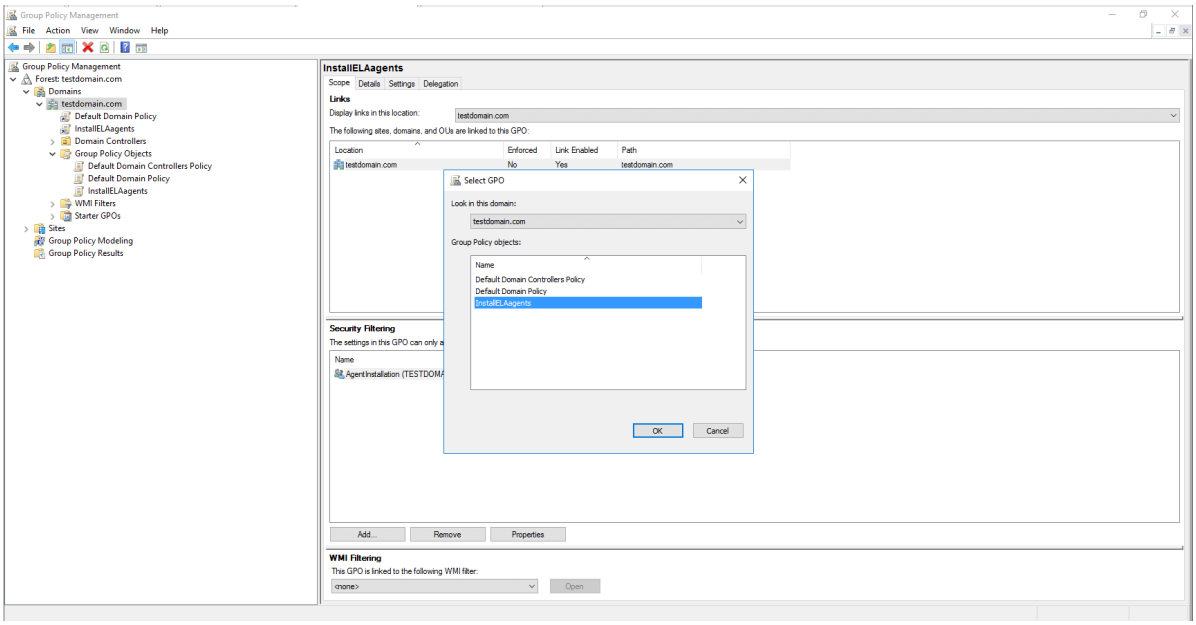
   (ii) Apply Group Policy > Allow



1. Click Apply and then OK.
2. Right-click on the Domain and click on "Link an Existing GPO..." option



3. Now select the GPO you are working on and Click OK.



4. Restart the computers to complete applying the GPO and wait for the reset password / unlock account link to appear on the Windows logon screen.

Note: After installing the EventLog Analyzer agent using GPO, make sure to disable or delete the GPO, or the scripts will continue to run at every startup.

Using Microsoft System Center Configuration Manager (SCCM) or some similar software deployment tool:

Place the appropriate installer file (EventLogAgent_<Arch>.bin for Linux or Eventlogagent.msi for Windows) in a network-shared folder. Then, on the devices where the agent needs to be installed, execute the following command:

For Windows:

Example: msiexec.exe /i "EventLogAgent.msi" /qn /norestart /L*v "Agent_Install.log" SERVERNAME="me-eventlog" SERVERIPADDRESS="10.51.241.163" SERVERPORT="8095" SERVERPROTOCOL="http" ENABLESILENT=yes ALLUSERS=1

For Linux:

Example: ./EventLogAgent_64.bin --silent SERVERNAME="me-eventlog" SERVERIPADDRESS="10.51.241.163" SERVERPORT="8095" SERVERPROTOCOL="http" > ./ELAAgent_InstallationLog.log 2>&1

Agent installation via Endpoint Central (formerly called Desktop Central)

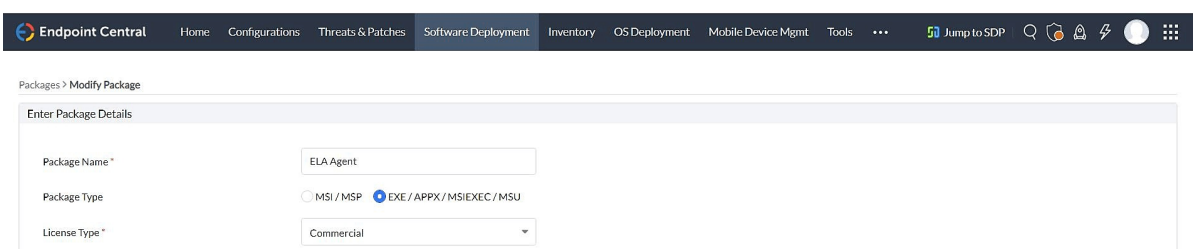
Create an MSI package:
MSI is an installer package file format used by Windows.

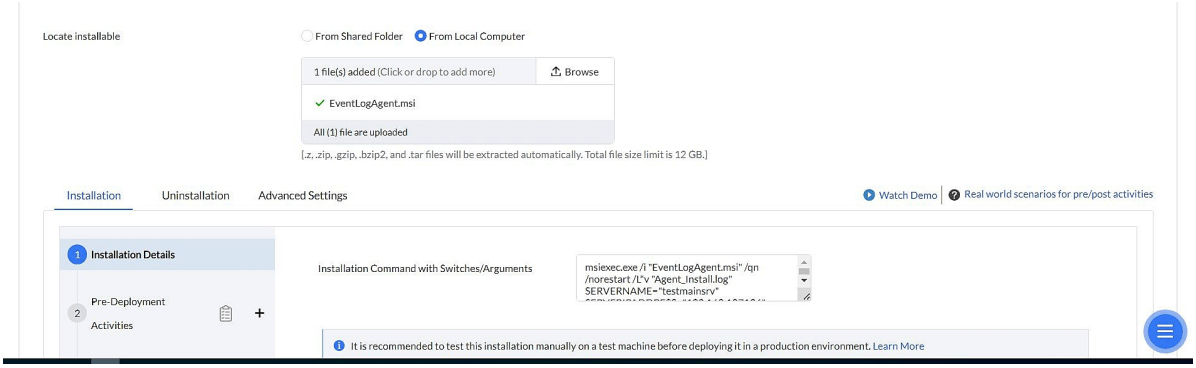
- Log in to the Endpoint Central console as an administrator.
- Navigate to Software Deployment > Packages > Add Package and select Windows from the drop-down menu.

Fill out the details in the fields available as follows:

- Package Name: Choose a name, such as ELA Agent.
- Package Type: Select EXE / APPX / MSIEXEC / MSU
- License Type: Select Commercial from the drop-down menu.
- Locate installable: Choose Shared Folder or Local Computer depending on the location of your EventLog Agent installation file.

> Note: EventLog Analyzer provides .msi files for Windows and .bin files for Linux systems.





The above image is for the installation on Windows.

- In the Installation tab, browse and select the desired MSI file for the EXE/APPX/MSIEXEC/MSU File Name field.
- Update and enter the following text in the EXE/APPX/MSIEXEC/MSU Properties for Installation field.
  Example:
  msiexec.exe /i "EventLogAgent.msi" /qn /norestart /L*v "Agent_Install.log" SERVERNAME="me-eventlog" SERVERIPADDRESS="10.51.241.163" SERVERPORT="8095" SERVERPROTOCOL="http" ENABLESILENT=yes ALLUSERS=1
- Click on Add Package to save.

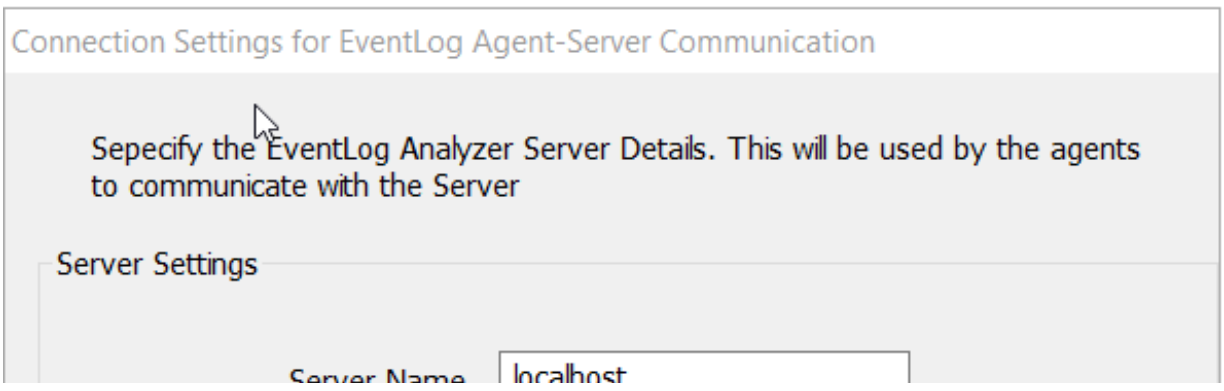
Manual installation:

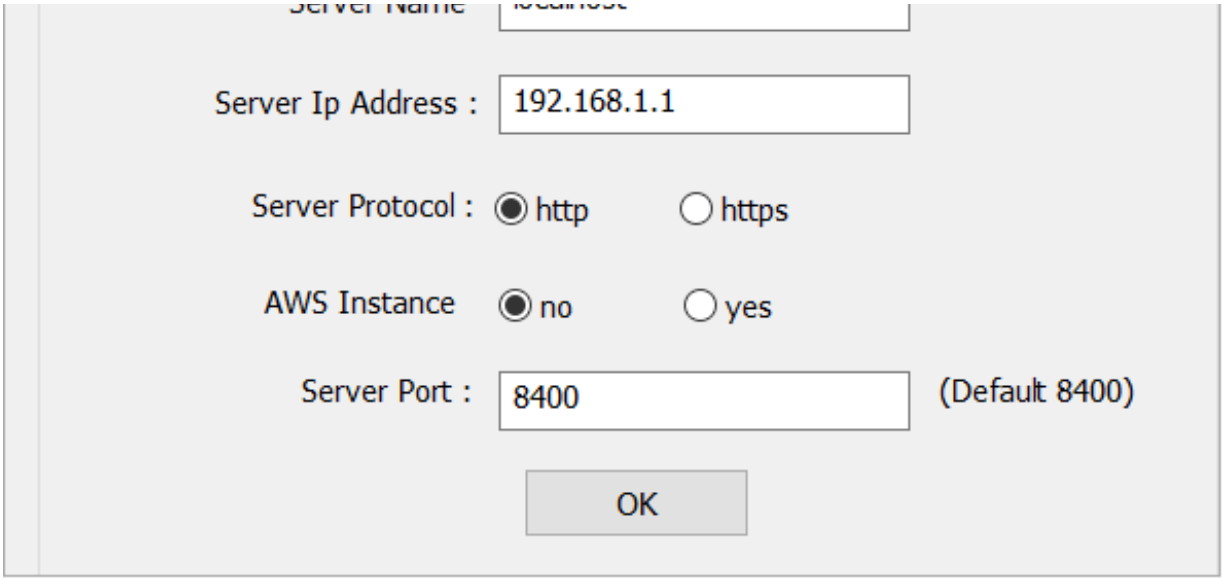
For Windows devices:

- On the machine where the agent is installed, open a browser and paste the following command into the browser's URL

  Here:
- <eventlog_server> = Name of the server on which EventLog Analyzer is installed
- <eventlog_server_port> = Web server port used by EventLog Analyzer (By default Eventlog Analyzer uses web server port 8095 for HTTP)

  For example: localhost:8095/event/downloadMsi.nms?platform=windows
- EventLogAgent.msi will be downloaded automatically. Double-click EventLogAgent.msi to start installation.
- After clicking Next in the welcome screen and the Confirm Installation dialog box, the following dialog box will be displayed. Enter the details and click OK.





- Installation will be completed.

For Linux devices,
The agent has to be configured in Manage File Integrity Monitoring page of EventLog Analyzer. Refer Configuring File Integrity Monitoring to configure the agent in Linux devices. If installation fails due to permission denial, you can manually install it by executing the following command.

Installation Command:

HTTP Command:
HTTPS Command:

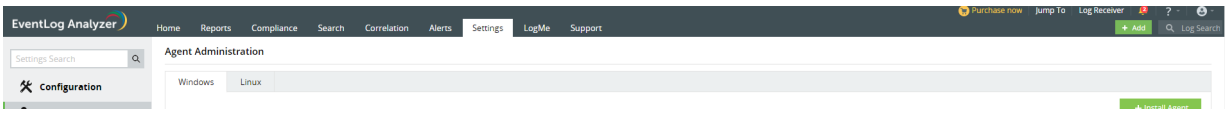
Example:

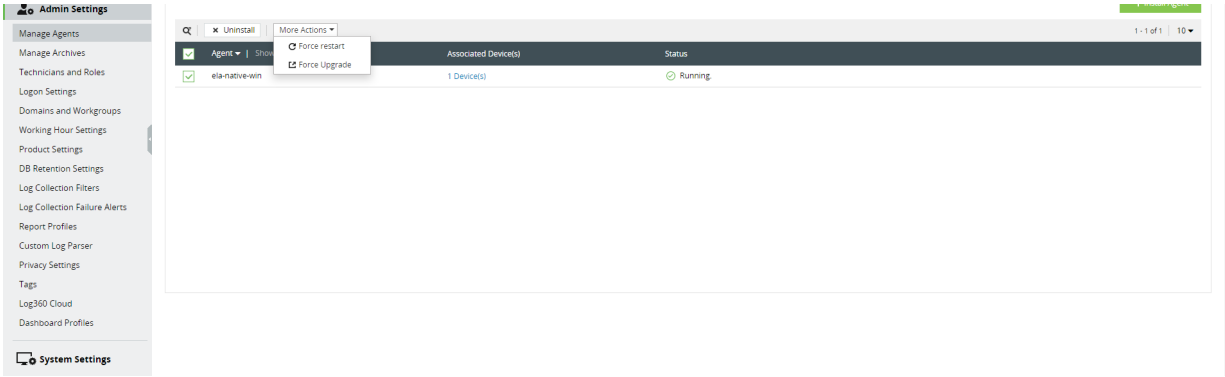
Sudo User:
Non-Sudo User:
For Sudo User:
Make sure to include the prefix "sudo -s" before running the installation command.

> Note: For non-sudo user, ensure that you are logged in as the auditing user. This is important because the agent will automatically consider the current user as the auditing user. If you are not logged in as the auditing user, please refer to the troubleshooting tips for setting privileges for agent folder.

Managing EventLog Analyzer agents

Using EventLog Analyzer's console, you can uninstall, upgrade, and force the agent to restart.





Uninstalling the EventLog Analyzer agent

To uninstall the EventLog Analyzer from device(s),

- In the Settings tab, navigate to Admin Settings > Manage Agents.
- Select the device(s) from which you want to remove the agent.
- Click Uninstall and select Yes in the pop-up box that appears.

Another method to uninstall the EventLog Analyzer from device(s) is by using add or remove programs,

- Navigate to Windows start menu > Add or remove programs in your desktop.
- Select the "ManageEngine EventLog Analyzer Agent".
- Click Uninstall.

Forcing restart of the EventLog Analyzer agent

To force the EventLog Analyzer to restart,

- In the Settings tab, navigate to Admin Settings > Manage Agents.
- Select the device(s) on which you want to restart the agent.
- Select More Actions and click Force restart in the drop-down box that appears.
- In the pop-up box that appears, select Yes.

Forcing upgrade of the EventLog Analyzer agent

Upgrading the EventLog Analyzer agent through Force Upgrade,

- In the Settings tab, navigate to Admin Settings > Manage Agents.
- Select the device(s) on which you want to upgrade the agent.
- Select More Actions and click Force upgrade in the drop-down box that appears.
- In the pop-up box that appears, select Yes.

9.5.12. Install EventLog Analyzer as a service

Last updated on: September 12, 2025

In this page

Windows

Linux

The steps to install EventLog Analyzer as a service for Windows and Linux machines are given below.

Windows:

1. Establish a remote connection with the server where EventLog Analyzer is installed.
2. Open the command prompt with Admin privileges.
3. Navigate to <Eventlog Analyzer>\bin
4. Execute the following commands sequentially to ensure that the instance is not running:
   - shutdown.bat
   - stopDB.bat
   - stopSEC.bat
5. Execute the following command to install EventLog Analyzer as a service.
   - service.bat -i
6. Go to services.msc and start the ManageEngine EventLog Analyzer service.

> **Note**
>
> Commands related to ManageEngine EventLog Analyzer service:
> - Install the service: service.bat -i
> - Start the service: service.bat -t
> - Stop the service: service.bat -p
> - Remove the service: service.bat -r

Linux:

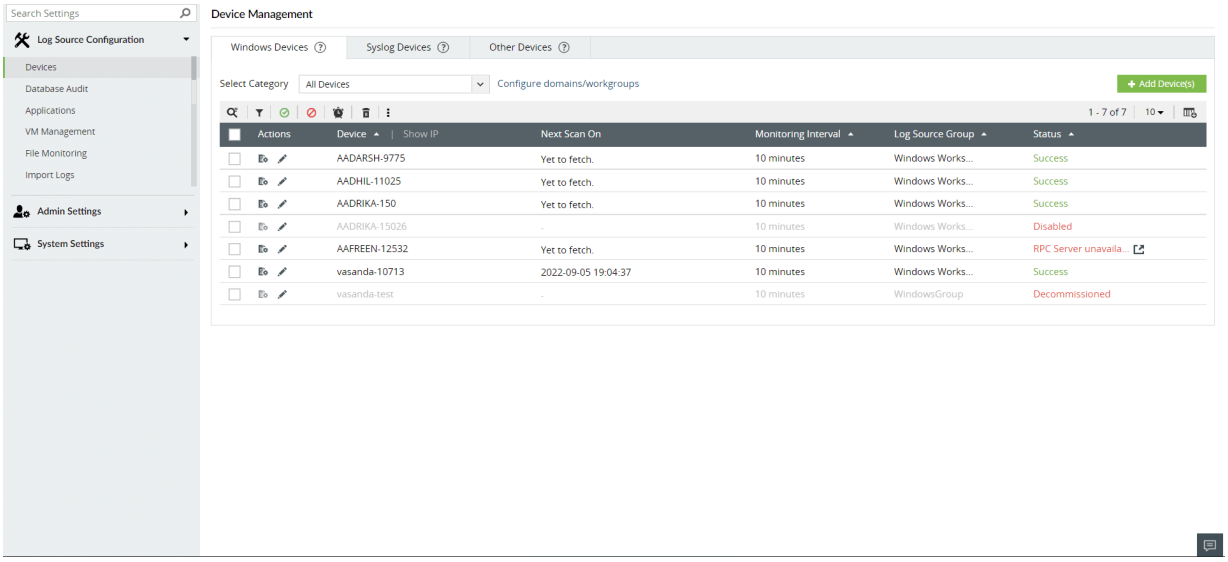
1. Establish a remote connection with the server where EventLog Analyzer is installed.
2. Navigate to <Eventlog>\bin

3. Execute the following commands sequentially with Admin privileges to ensure that the instance is not running:
    - sudo sh shutdown.sh
    - sudo sh stopDB.sh
    - sudo sh stopSEC.sh
4. Execute the command "sudo sh ConfigureAsService.sh -i"
5. Execute the command "service eventloganalyzer status" to verify the service installation.

9.6.1. Device Management

Last updated on: September 12, 2025

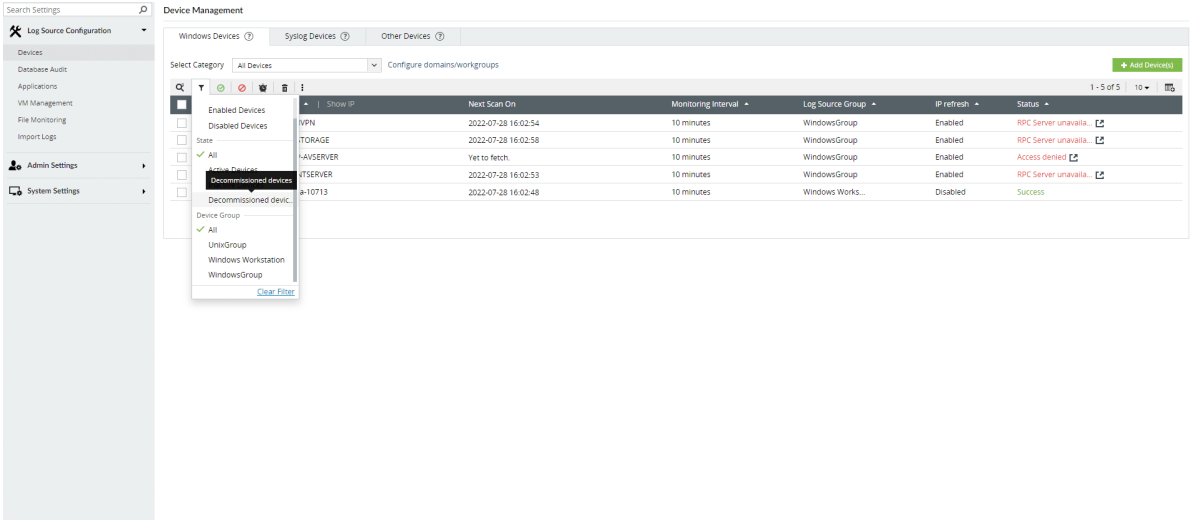
All the devices added to EventLog Analyzer for monitoring can be viewed under Settings > Configuration > Manage Devices.



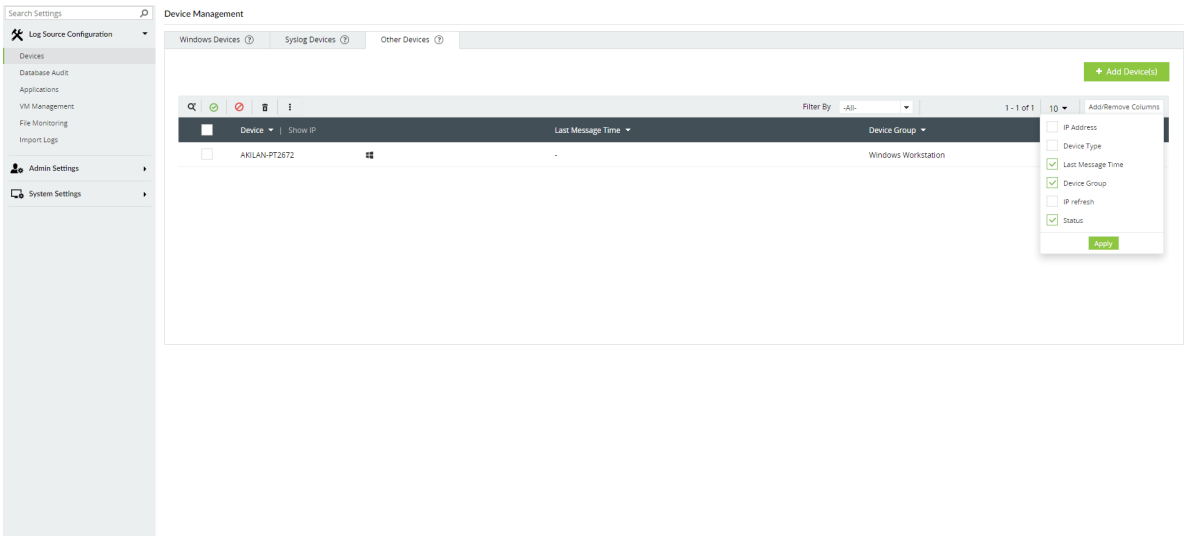
> **Note**
>
> When you rename an AD device in domain, the device name automatically gets renamed in device management too.

In this page, you can find three tabs: Windows Devices, Syslog Devices and Other Devices. Under Windows Devices, you can use the Select Category drop-down menu to select a domain or workgroup.

1. Devices are displayed with the following icons: Search, Enable, Disable, Filter Change Monitor time interval, and Delete. The Filter option lets you choose the devices for reports by their status (enabled/disabled), state (active/inactive/decommissioned) and device group.



2. The table displays the following columns:



1. Checkbox against all devices
2. Actions: Configure event source file and Update icons.
3. Device Name
4. Device IP address
5. Last Message Time
6. Device Group
7. Next Scan On: Shows when the next scan is scheduled. The Scan Now link against each device will scan the device instantly.
8. Monitoring Interval: The period for collection of logs.
9. IP refresh: Status of automatic IP refresh
10. Status: Status of log collection.

Quick Links

- Configuring Auto Log Forward for Unix machines
- Configure domains and workgroups
- Manage Device Groups

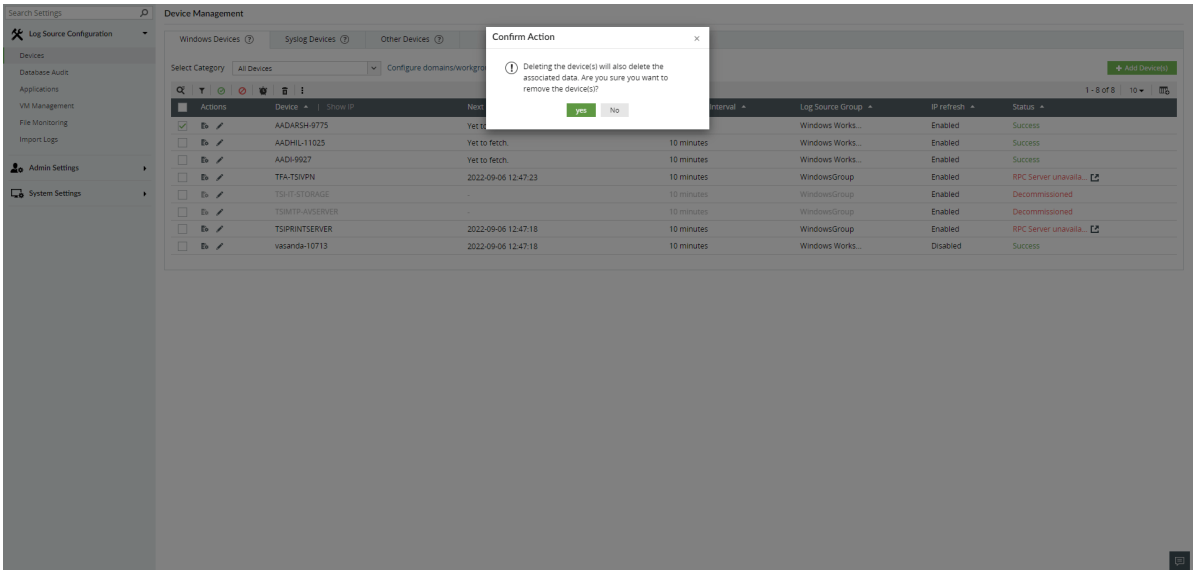
Manage Devices

How to add a device?

Refer to Add Device.

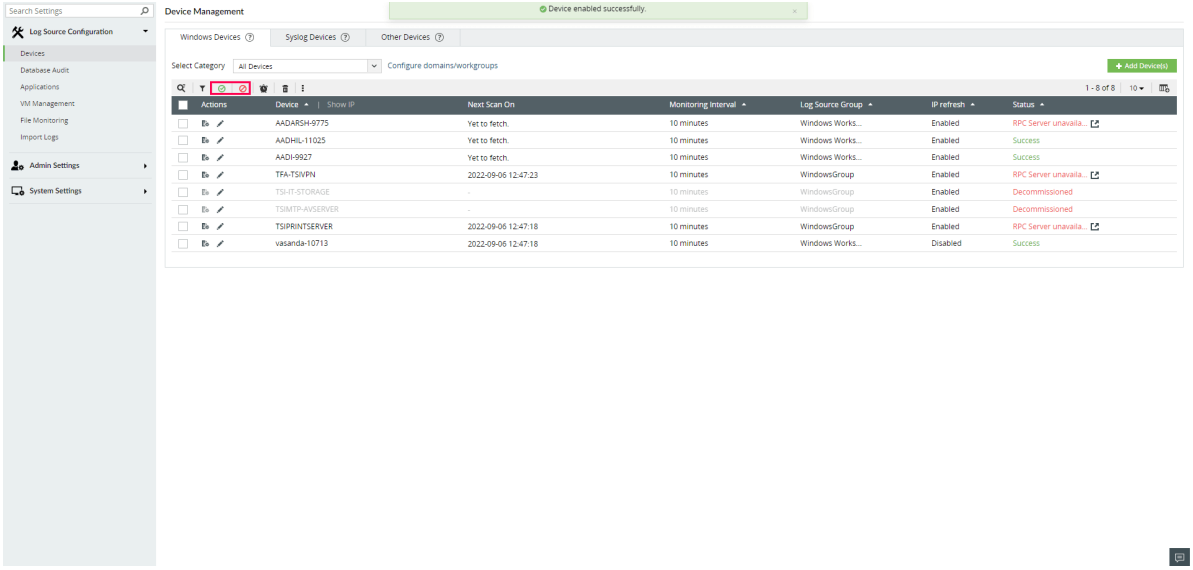
How to delete a device?

1. Go to Settings > Configuration > Manage Devices.
2. Select the appropriate tab from Windows Devices, Syslog Devices, Other Devices.
3. Select the checkbox(es) against the respective device(s).
4. Click the delete icon in the action menu.
5. Click Yes in the delete confirmation pop-up.



How to disable/enable a device?

1. Navigate to Settings > Configuration > Manage Devices.
2. Select the appropriate tab from Windows Devices, Syslog Devices, Other Devices.
3. Select the device(s) by selecting the respective check box(es).
4. Click the disable or enable icons in the action menu.



How to change the monitoring interval?

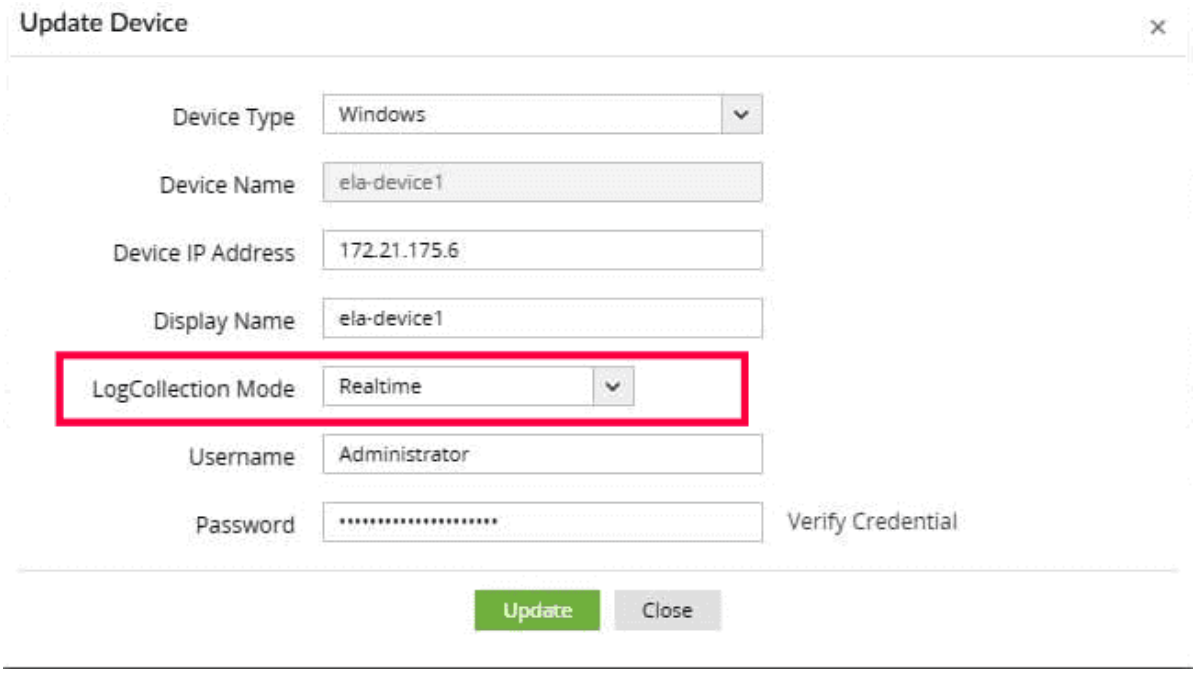
To change the monitoring interval for multiple devices in bulk, follow the given steps.

1. Navigate to Settings > Configuration > Manage Devices > Windows Devices
2. Select the device(s) by selecting the respective check box(es).
3. Click the Change monitor interval icon in the action menu.
4. In the box that opens, select the time interval in minutes as needed.
5. Click Update.



To change the monitoring interval for individual devices, follow the given steps.

1. Navigate to Settings > Log Source Configuration > Manage Devices.
2. In the Windows Devices tab, click the Edit icon beside the corresponding device.
3. Select the required Log Collection Mode — either Realtime or Scheduled with the desired time interval.
4. Enter the required credentials.
5. Click Update to save the changes.



Note

When EventLog Analyzer is installed on a Linux server, the log collection interval cannot be modified in bulk, and the Change Monitor Interval icon will not appear on the Device Management page. However, you can change the log collection mode for individual devices using the above

steps.

Note

You can select multiple devices and configure them for either

- Real-time log collection or Scheduled collection with a specific monitoring interval.
- Log360 Cloud\EventLog Analyzer lets you collect logs from up to 25 devices in real-time per agent.

How to update a device's configuration?

1. Go to Settings > Configuration > Manage Devices > Windows Devices.
2. Click the edit icon for the device. For Syslog Devices and Other Devices, hover over the device for edit icon to appear.
3. This opens the Update Device box where you can edit Device Type, Display Name, and Log Collection Mode.
4. You should be able to refresh the IP from the console without specifying the new IP manually
5. You can manually change the IP too in case there are any issues with the auto updation. You can go back to auto IP updation easily from the console

Note

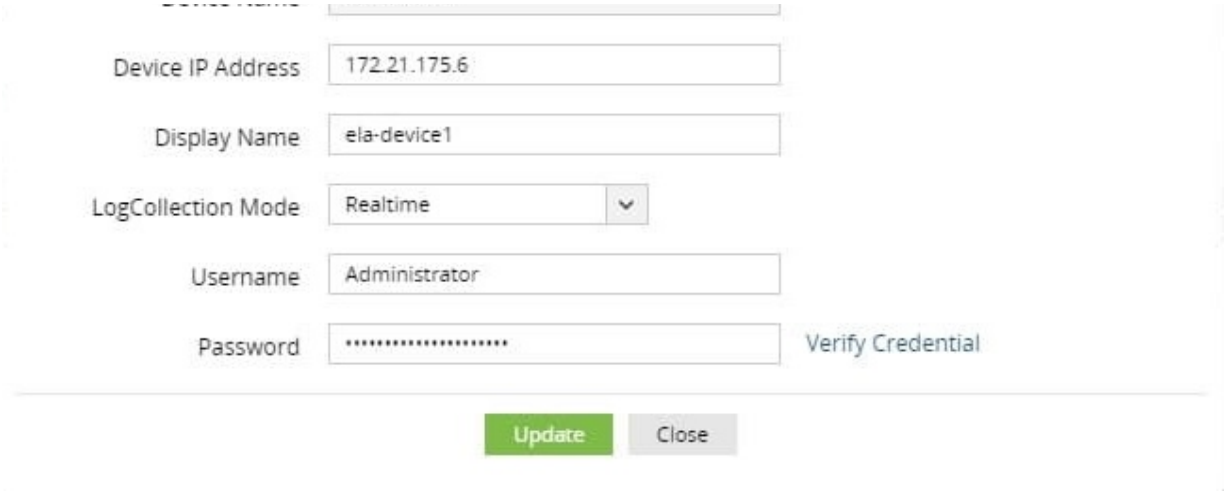
The Log Collection Mode can be configured either for real-time log collection or for scheduled collection with monitoring interval.

6. Click AD details to view object GUID - The unique identifier for a Domain object.
7. Click Advanced to edit Encoding Type and Time zone.
8. Click Update.

Note

Auto IP updation schedule will be disabled for devices which have manual IP selected.

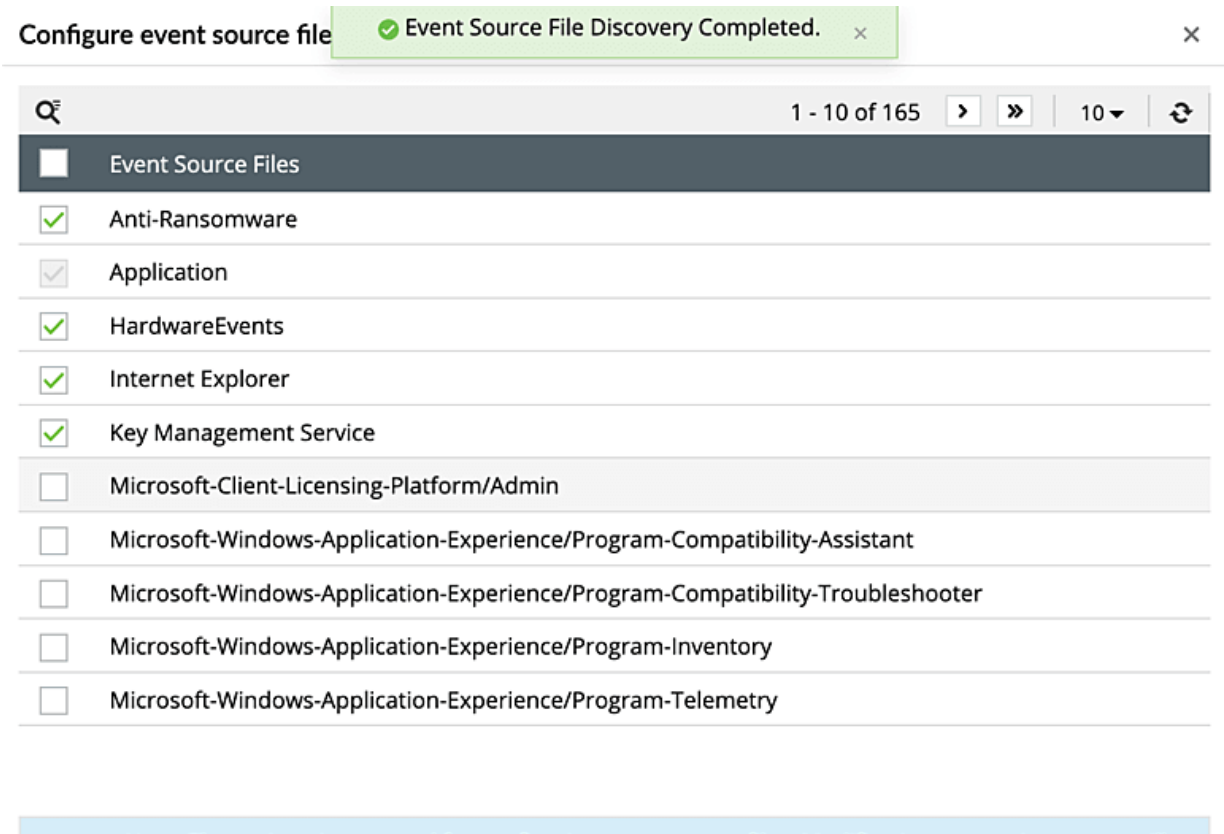


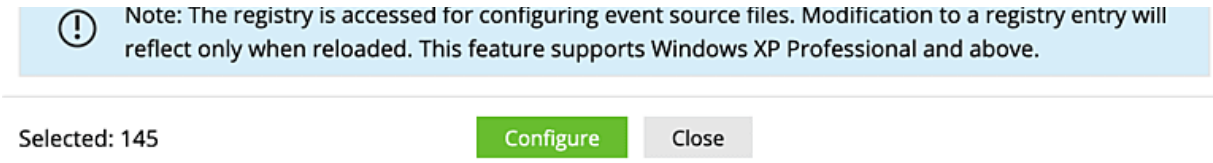


How to configure event source files in a device?

1. Go to Settings > Configuration > Manage Devices > Windows.
2. Click the Configure Event Source Files icon for the device.
3. In the Event source files dialog box, select the type(s) of event source files.
4. Click Configure.

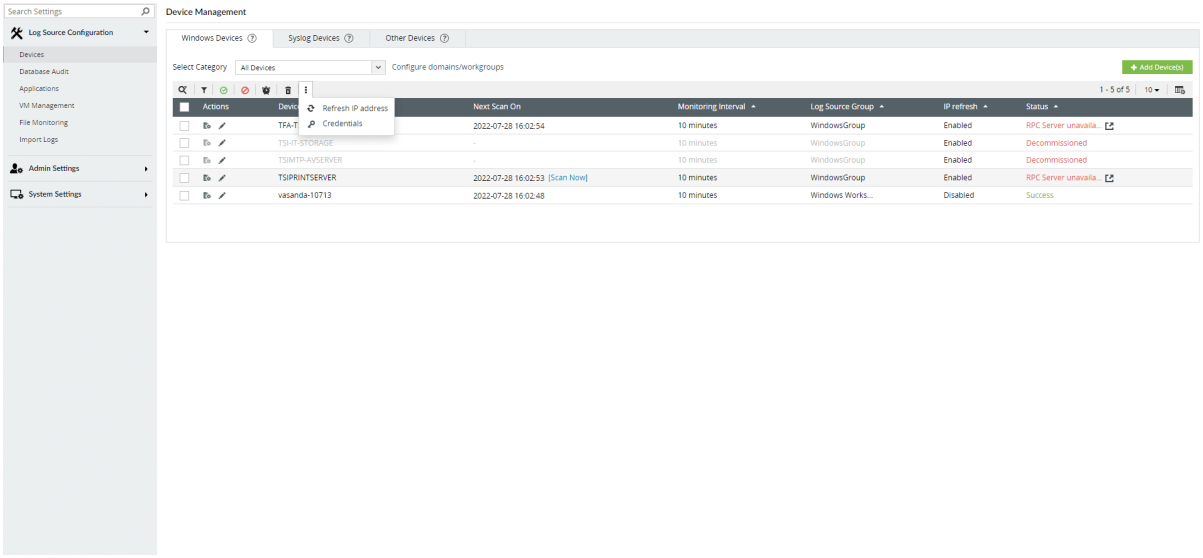
> Note: The registry is accessed for configuring event source files. Modifications to a registry entry will reflect only when reloaded. This feature supports Windows XP Pro and above.



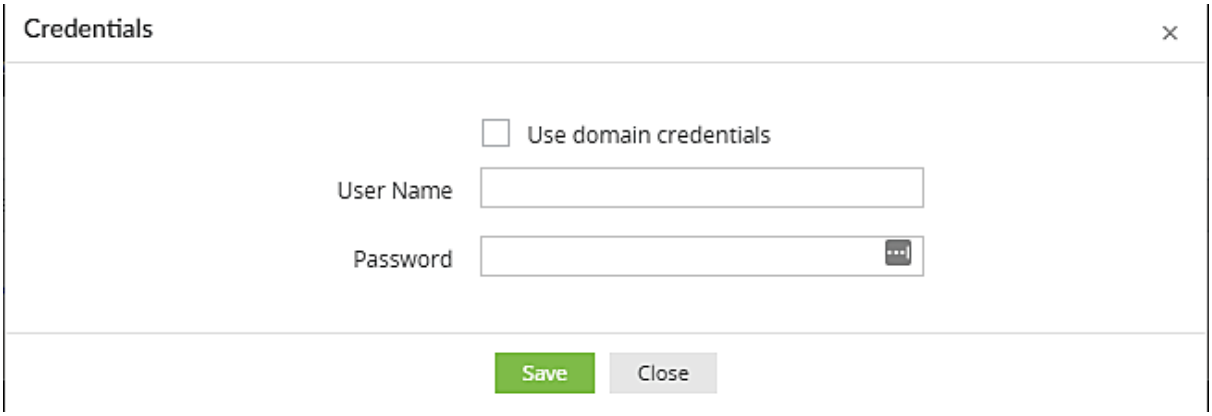


How to Bulk update credentials

1. Go to Settings > Devices > Windows devices > click on the ⋮ icon > Select credentials

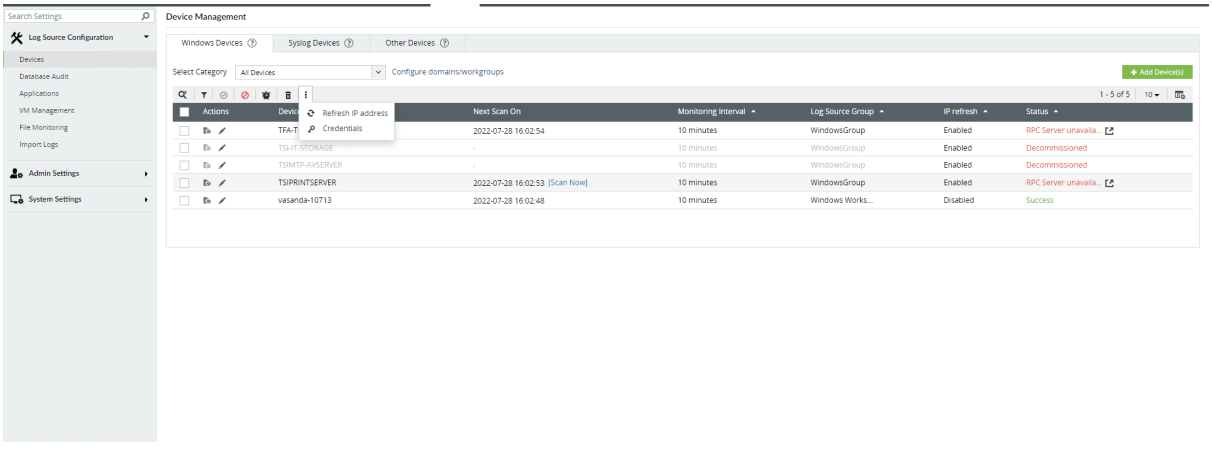


2. Update your user name and password. Click on Save

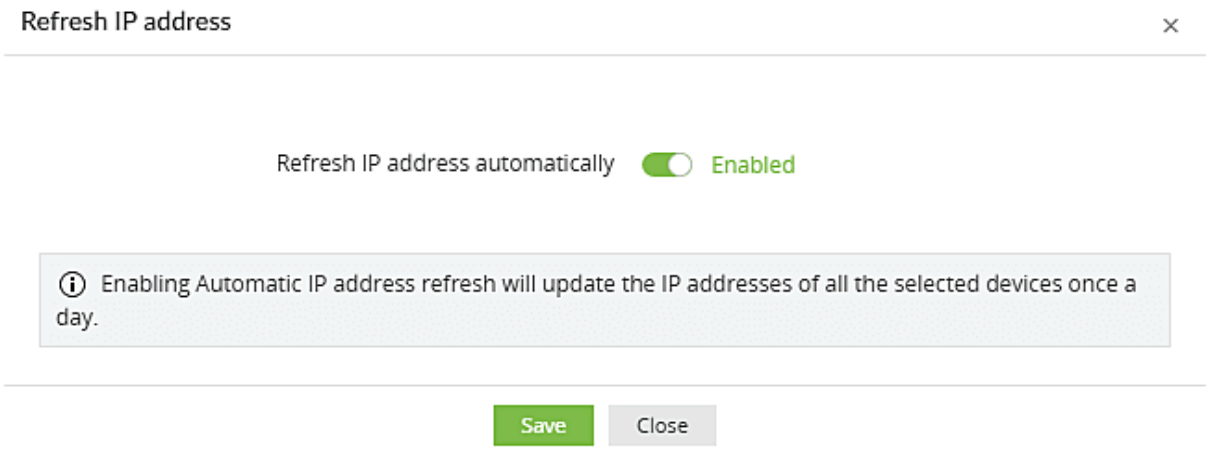


How to bulk refresh IP

1. Go to Settings > Devices > Windows devices > click on the ⋮ icon > select Refresh IP

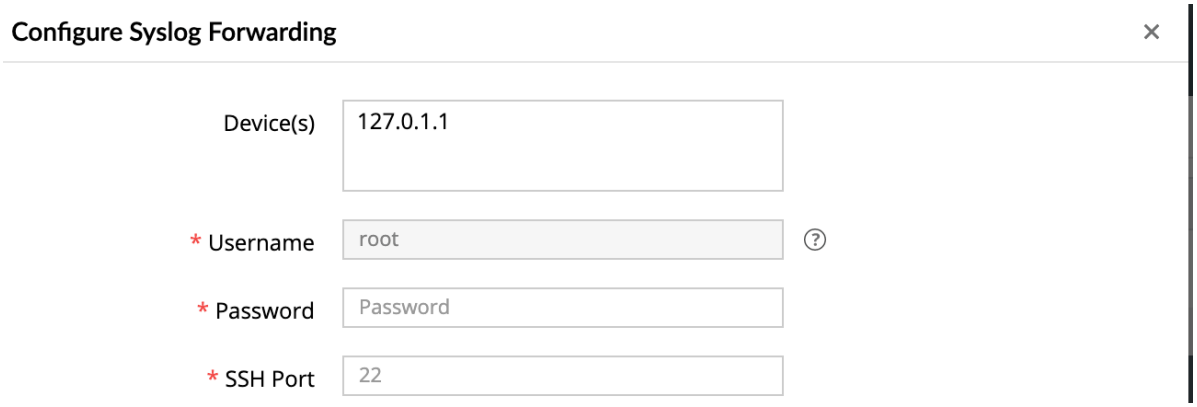


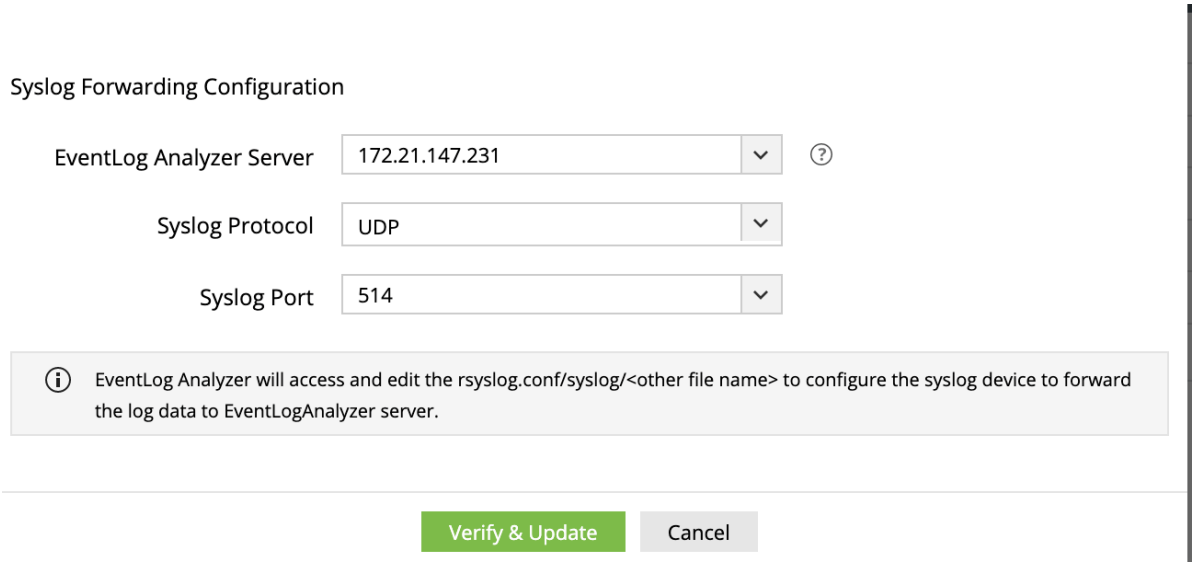
2. Enable/Disable button: When 'Enable IP address automatically' is checked, automatic IP refresh will be enabled for the devices. If it is unchecked, automatic IP refresh will be disabled.
3. Enable/Disable button will not show the status of automatic IP refresh of selected device.
4. By switching to Enable option and clicking on the save button, IP refresh will be performed on selected devices.



Configure Auto Log Forward for Unix devices

1. Go to Settings > Configuration > Manage Devices > Syslog Devices.
2. Select the Unix device by ticking the checkbox.
3. Click Configure Auto Log Forward in the Actions menu.
4. Enter the root login credentials for the Unix device and SSH port number.
5. For configuring syslog forwarding , enter the IP address of the EventLog Analyzer server.
6. Select the protocol — TCP/UDP.
7. Specify the Syslog Port number. Note that the default port numbers are 513 and 514 for UDP and 514 for TCP.
8. Click Verify & Update.




Syslog Forwarding Configuration
EventLog Analyzer Server
172.21.147.231
Syslog Protocol
UDP
Syslog Port
514
EventLog Analyzer will access and edit the rsyslog.conf/syslog/<other file name> to configure the syslog device to forward the log data to EventLogAnalyzer server.
Verify & Update
Cancel

9.6.2. Steps to configure external applications

Last updated on: September 12, 2025

Configuring ManageEngine Password Manager Pro

Here are the steps to configure Password Manager Pro.

1. Login to Password Manager Pro.
2. Navigate to Audit -> Resource Audit -> Audit Actions -> Configure Resource Audit. Enable the Generate Syslog option for all operations and click Save.
3. Navigate to Audit -> User Audit -> Audit Actions -> Configure User Audit. Enable the Generate Syslog option for all operations and click Save.
4. Navigate to Admin -> Integration -> SNMP Traps / Syslog Settings and click Syslog Collector.
   - Enter the EventLog Server name and a port that the EventLog Analyzer instance is listening to.
   - Select the protocol (UDP/TCP) and a facility name. Click Save.

Configuring ManageEngine OpManager

The following are the steps to configure ManageEngine OpManager.

1. Login to OpManager.
2. Navigate to Settings -> Notifications.
3. Click Add.
   Profile Type
   Select Syslog Profile and enter the following details.
   - Destination Host - EventLog Analyzer server name or IP address.
   - Destination Port - Any port that the EventLog Analyzer instance is listening to.
   - Severity and Facility must be the default values i.e. $severity and kernel.

   For EventLog Analyzer to parse logs from OpManager, the message variables in the syslog profile of OpManager should be entered in the following format:
   Mandatory message variables
   - ALARM_MESSAGE:$message
   - ALARM_ID:$alarmid
   - ALARM_CODE:$alarmid

   Other important message variables
   - ALARM_SOURCE:$displayName
   - ALARM_CATEGORY:$category
   - ALARM_SEVERITY:$stringseverity

- ALARM_TRIGGER_TIME:$strModTime
- ALARM_EVENT_TYPE:$eventType
- Entity: $entity
- Last Polled Value: $lastPolledValue

4. Click Next.

Criteria

- Click on the Criteria check-box.
- Enable the notification for all severities and click Next.

Device Selection

- Select the By Device option and select all the devices listed under Remaining Devices and click Next.

Schedule

- You don't have to configure anything in this section. Click Next.

Preview

- Enter a profile name and click Save.

> **Note**
>
> If the same machine is running two or more ManageEngine products, ensure the following:

- The ports used by the products are unique.
- The EventLog Analyzer port receiving logs from OpManager and Password Manager Pro is not used by other ManageEngine products.



9.6.3.1. Device Auto Allocation in Log360 | Overview

Last updated on: September 12, 2025

In this page

What is Device Auto Allocation?

Key functionalities

Pre-requisites

Allocation flow

Use cases

What is device auto allocation?

Device auto allocation is the process of automatically assigning the discovered Windows devices from workgroups and domains, to collectors. In case of an agent-based collection, the allocation happens through agents where policies with defined rules and collector load will define device mapping to the appropriate agent. And in the case of agent-less log collection method, direct allocation of device(s) to the native or local collector takes place. - Device allocation in Log360 is governed by user-defined policies called Auto Allocation Policies that specify the criteria like domain names, OU (Organizational Unit) filters, workgroups, and device limits. This auto allocation capability will help you streamline the onboarding of devices into a centralized monitoring system, reducing manual work and ensuring that every device in your organization's large network is monitored.

Key functionalities

- Device onboarding automation: Replaces manual device allocation by auto-assigning devices or scheduling runs, based on pre-defined policies. The allocation is performed either on the domain basis or workgroup.
- Granular control:
  - With the help of multiple policies, define allocation rules based on workgroups, OUs, set device count limits, include OU filter for domains and more, per agent or collector.
  - You can include or exclude OUs under specific domains depending upon your requirements.
  - Each policy maps to an agent/local native collector.
- Load balancing: To ensure even distribution and prevent congestion, devices will be automatically assigned to collectors with the least load.
- Failsafe conditions: Clear status is notified in case the policies are not applicable or if a collector's device limits are reached.

NOTE

If Auto Allocation is

If Auto Allocation is-
Disabled during execution: The device allocation stops immediately.
Enabled: The device allocation will start instantly and will be scheduled to run daily at 12 PM, thereafter.

1. Auto allocation
Process where the solution automatically assigns discovered Windows devices to collectors or agents based on predefined rules and configured criterion, eliminating the need for manual assignment.
2. Auto allocation policies
User-defined rules that decide how and where devices should be assigned based on criteria like domain, OU, or workgroup.
3. Collector or local native collector
A server or component that receives and processes logs from devices. In agent-less setups, the local native collector on the same machine handles the respective device's logs.
4. Agent
A specific software installed on a device with the purpose of collection and sending of log data to Log360. Used in agent-based auto allocation for more granular control.

Pre-requisites

Role-based access control

Only admins of the console can define, access, and modify the auto allocation policies.

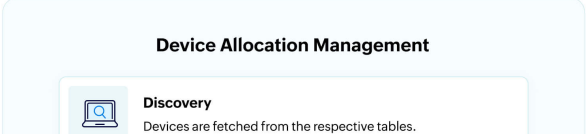
Supported devices

Windows devices

Domain or workgroup pre-requisites

- Ensure that the devices must be discovered in the device discovery process before the allocation.
- The devices to be auto-allocated must belong to a recognized domain or workgroup.
- The said domain must also be configured in the product console with the available OUs for policy mapping.
- For domain-based policies, it must be ensured that the OU structure or hierarchy is synchronized properly.

Allocation flow





NOTE

- In the case of an agent-less device collection, the "Agent selection" step is omitted in the workflow of device auto allocation and the "OU validation" step is carried out after which the device(s) will be automatically allocated to the native/local collector.
- Only one agent/collector can be mapped per policy.
- In case an agent is deleted, the agent is also dynamically removed from all the existing internal mappings during task execution.

Use cases

1. Dynamic scaling of SIEM infrastructure across business units

Use case

Regional divisions of a global company are operated with distributed agents handling logs from the different locations/business units.

With Device Auto Allocation

Devices can be routed automatically in each location or business unit to their respective local collector or agent with collector load-balancing and OU-based filters. This will also help divisional teams ensure that every endpoint is allocated promptly, efficient fault isolation, and region-specific threat visibility.

2. Zero touch onboarding for compliance-ready log collection

Use case

In large enterprises with thousands of endpoints across their AD domains and workgroups, there is a higher scope for human error when each and every device from all those endpoints is to be accounted for in the SIEM (Security Information and Event Management) solution for audit and compliance purposes like HIPAA, PCI-DSS, GDPR and more.

With Device Auto Allocation

The Auto Allocation feature ensures that as soon as a device is discovered, it is assigned to an agent/collector and that no device goes unmonitored. With this, human error is eliminated and onboarding is sped up, while ensuring complete audit trails right from Day 1.

> MITRE ATT&CK framework
>
> Device Auto Allocation can help you eliminate onboarding blind spots that are commonly exploited by attackers during their initial entry phase. Can mitigate T1133 (External Remote Services) Exploitation

Read also

This document elaborated the configuration, prerequisites, and functionality of the Device Auto Allocation feature in Log360. For related features and extended device management capabilities, refer to the articles below:

- Auto Allocation Configuration
- Auto Allocation Policy Configuration
- Check Unallocated Device(s) status
- Sync Settings

9.6.3.2. Configuring auto allocation

Last updated on: September 12, 2025

In this page

Overview

Configuring auto allocation (enable/disable)

Enabling auto allocation

Disabling auto allocation

Overview

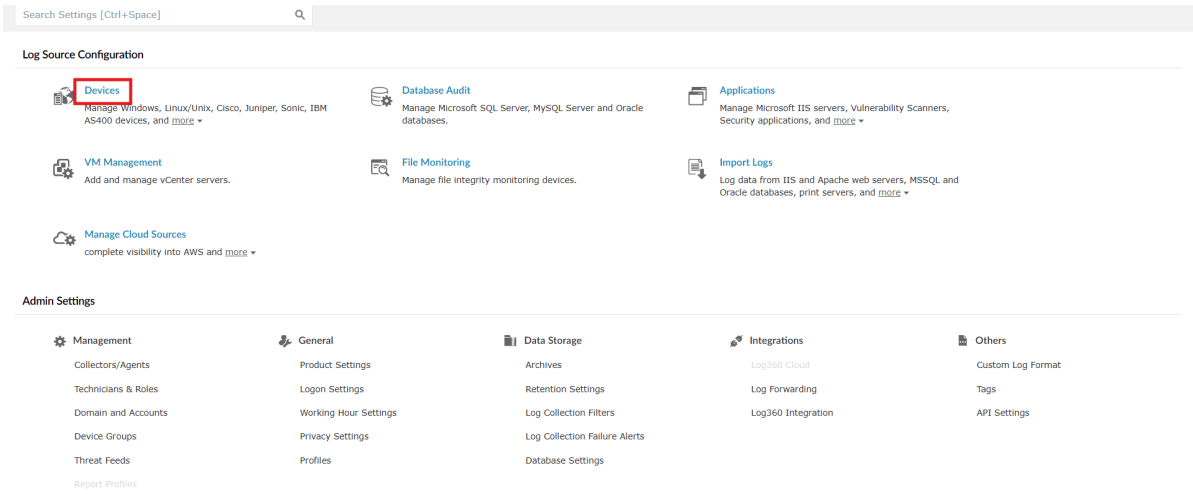
The auto allocation capability must be manually enabled to begin assigning discovered Windows devices to the appropriate collectors. Once enabled, the system automatically evaluates devices against configured policies and performs scheduled allocations. This section guides you through enabling or disabling the feature and explains what happens when it's turned on or off.

Configuring auto allocation (enable/disable)

Enabling auto allocation

> NOTE
>
> By default, the auto allocation feature is in a disabled state. It must be manually enabled in order to make use of its functionality.

1. In the product console, navigate to the Settings tab and click on Devices.



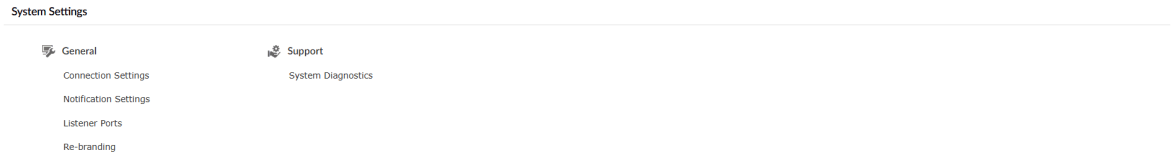


Image 1: Device settings

2. You will be taken to the Device Management module. On the right-hand side, you can find the toggle to enable/disable Auto Allocation. Click on the toggle to enable this function.

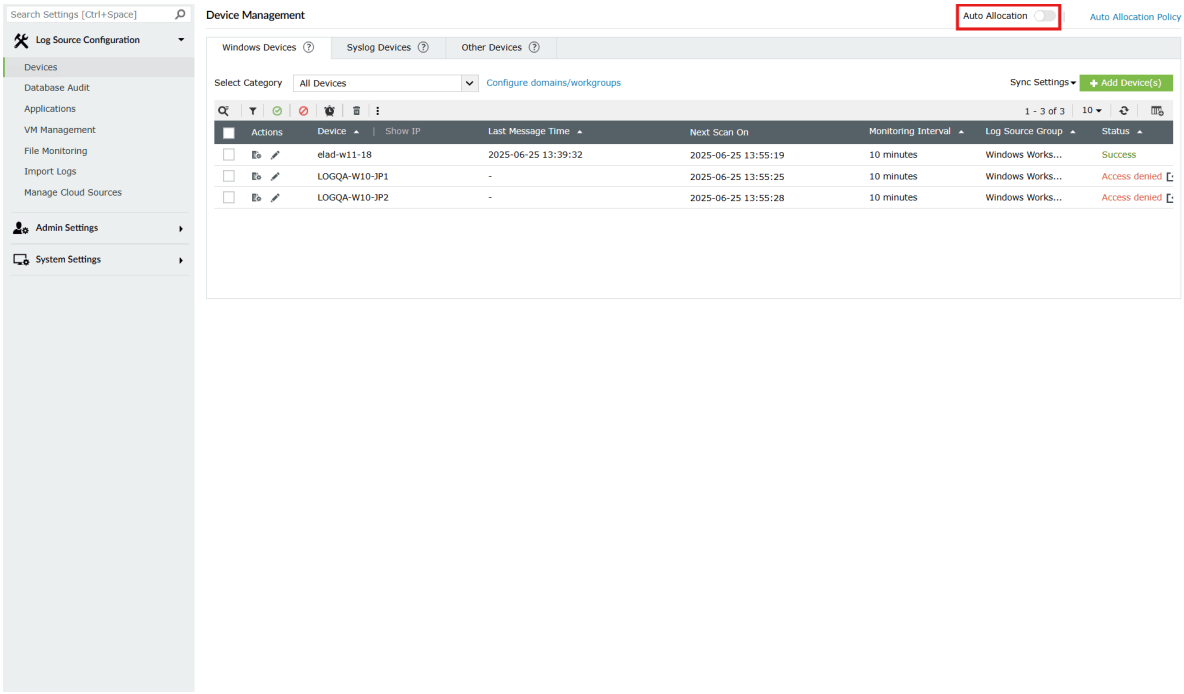
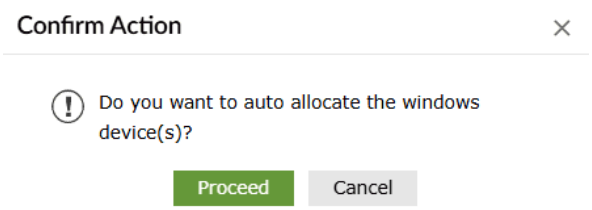
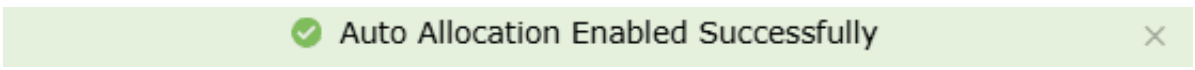


Image 2: Auto allocation in the product console

3. After you click on the toggle to enable auto allocation, a Confirm Action pop-up is displayed to enable auto allocation in Windows. Click on Proceed.



4. As soon as you select proceed, the toggle turns from Auto Allocation to Auto Allocation  and the below pop-up appears briefly as a confirmation of the successful changes made.



5. Now, auto allocation is enabled, and the product starts allocating devices immediately and will perform a daily allocation check at the scheduled time.

What happens after enabling auto allocation?

- Discovered devices from Workgroups and Domains will be evaluated against all the currently active Auto Allocation Policies.
- The system:
  - Matches devices based on policy rules (OU, domain, workgroup)
  - Selects the agent/collector with the lowest load at that moment, within the defined limits.
  - Allocates the device(s) and logs its status in the Device Management > Add Devices popup under the Reason column.

Disabling auto allocation

1. Follow the same steps- Step 1 and Step 2 as Enabling auto allocation to locate the toggle. Click on the (currently enabled) toggle.
2. As soon as you perform the above action, the toggle turns from Auto Allocation  to and the below pop-up appears.



Read also

This document explained how to enable or disable the device auto allocation feature and what happens after activation. For further information on managing device assignments and policies, refer to the articles below:

- Configuring auto allocation policies
- Check unallocated device(s) status
- Sync settings

9.6.3.3. Configuring auto allocation policies

Last updated on: September 12, 2025

In this page

Overview

Configuring auto allocation policies

Enabling/disabling a policy

Enabling a policy

Disabling a policy

Edit a policy

Trigger auto allocation manually

Overview

Auto Allocation Policies define how discovered devices are assigned to collectors in the product, based on criteria like domains, workgroups, and Organizational Units (OUs). This section explains how to manage these policies—enabling or disabling them, editing policy rules, and instantly triggering allocation—so that devices are automatically and efficiently onboarded into the monitoring system.

Configuring auto allocation policies

1. Navigate to the Settings tab and click on Devices.

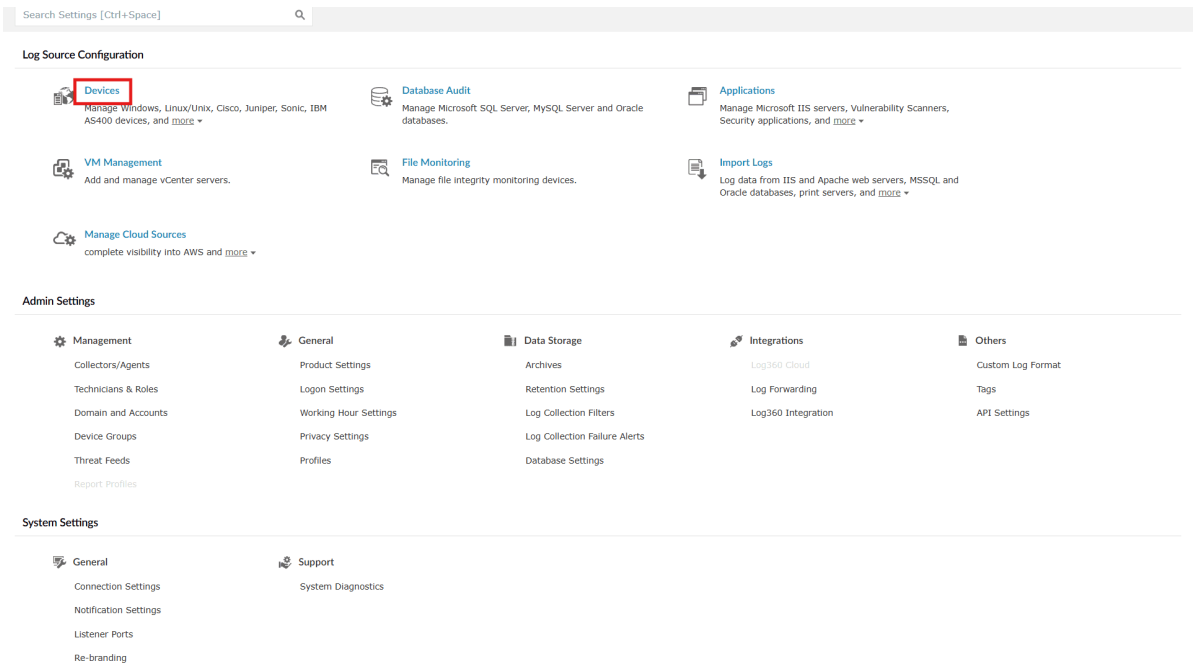


Image 1: Device settings in the product console

Image 1: Device settings in the product console

2. You will be taken to the Device Management module. On the right-hand side, you will find Auto Allocation Policy as shown below. Click on it.

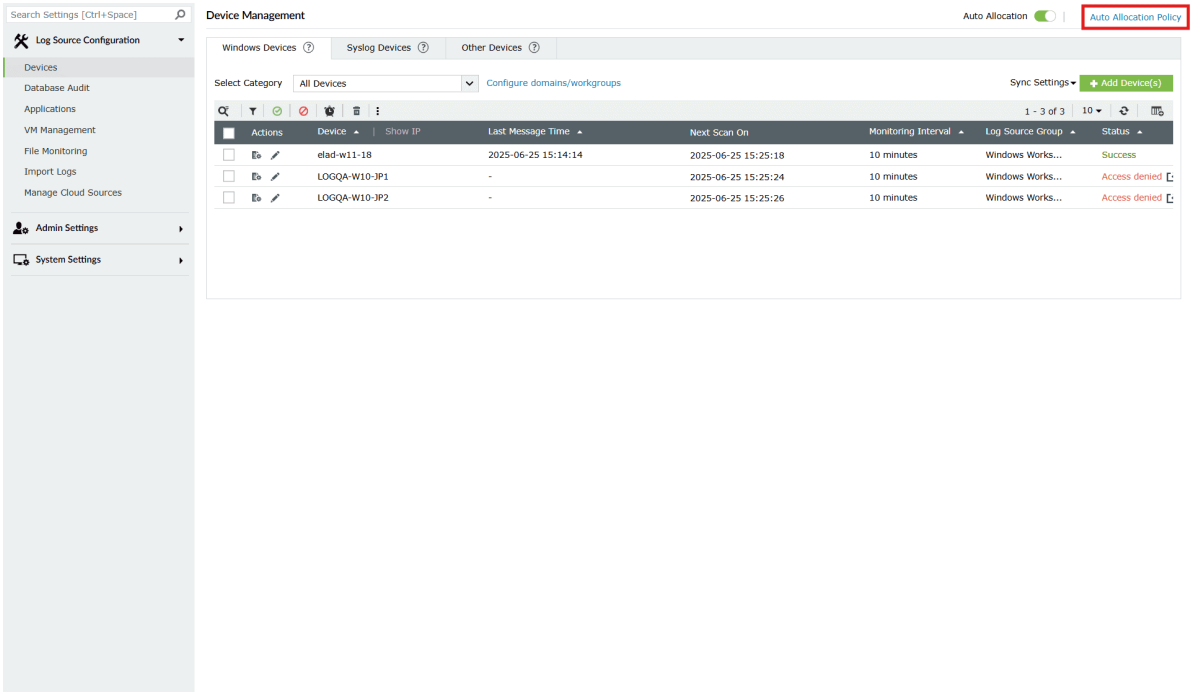


Image 2: Auto allocation policy in the product console

3. You will be taken to the list of all policies. Here, you can:
   - Check the status of the policies and/or enable/disable the policies.
   - Edit a policy.
   - You can trigger auto allocation for all policies at any time. (Only when the auto allocation feature is in an enabled state.)

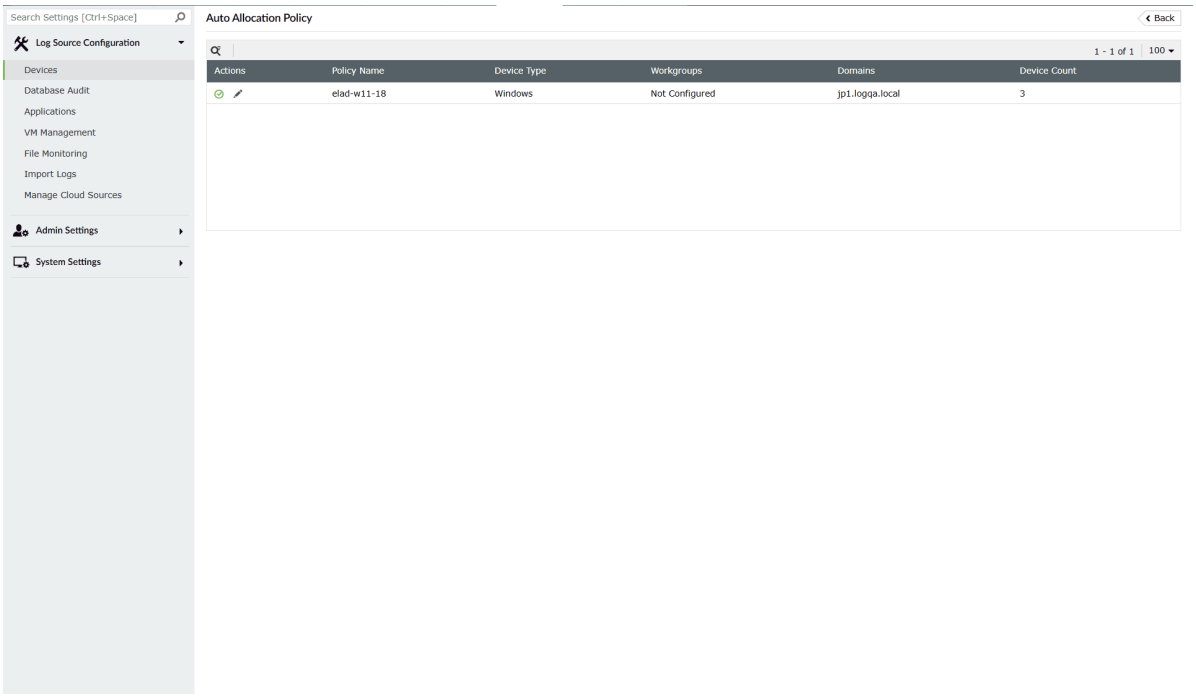


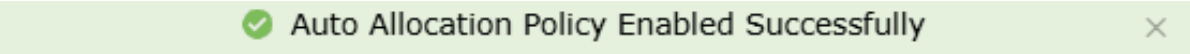
Image 3: Device auto allocation policy in the product console

> NOTE
>
> By default, the auto allocation policy is configured for the localhost server.

Enabling/disabling a policy

Enabling a policy

1. Click on the disabled icon under the Actions column to enable the policy.
2. As soon as you perform this action, the icon indicates that the policy is now enabled and the below pop-up message appears briefly.



Disabling a policy

1. Click on the enabled icon under the Actions column to disable the policy.
2. As soon as you perform this action, the icon indicates that the policy is now disabled and the below pop-up message appears briefly.



Enable/Disable multiple policies at once

1. Click on the empty checkbox(es) in the first column in order to select the respective policies.
2. Click on the Enable/Disable icons in the ribbon above the rules list.

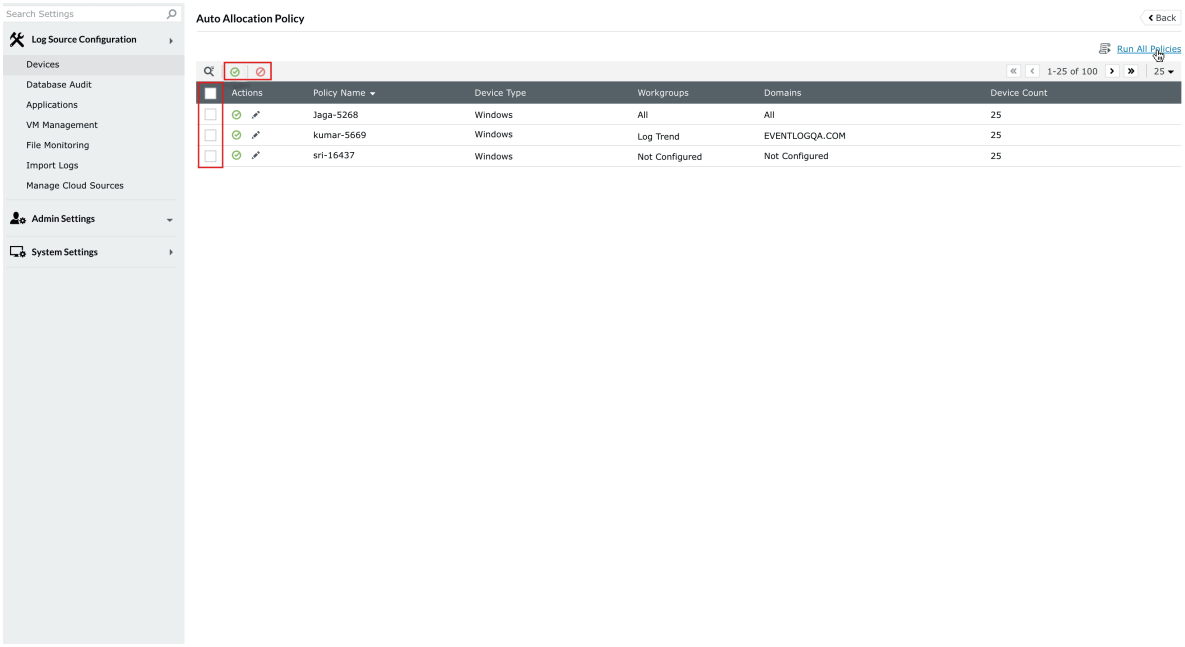
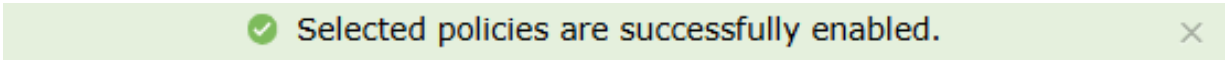


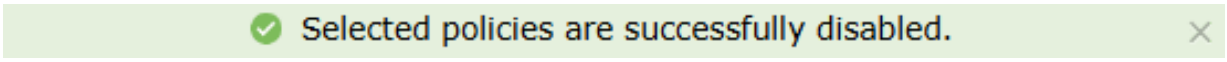
Image 4: Enable/Disable multiple policies at once

3. Upon successful completion of the action, the below pop-up appears.

When enabled successfully:



When disabled successfully:



Edit a policy

1. To edit a policy, click on the Edit icon under the Actions column. A slider appears that includes the fields for editing the policy.

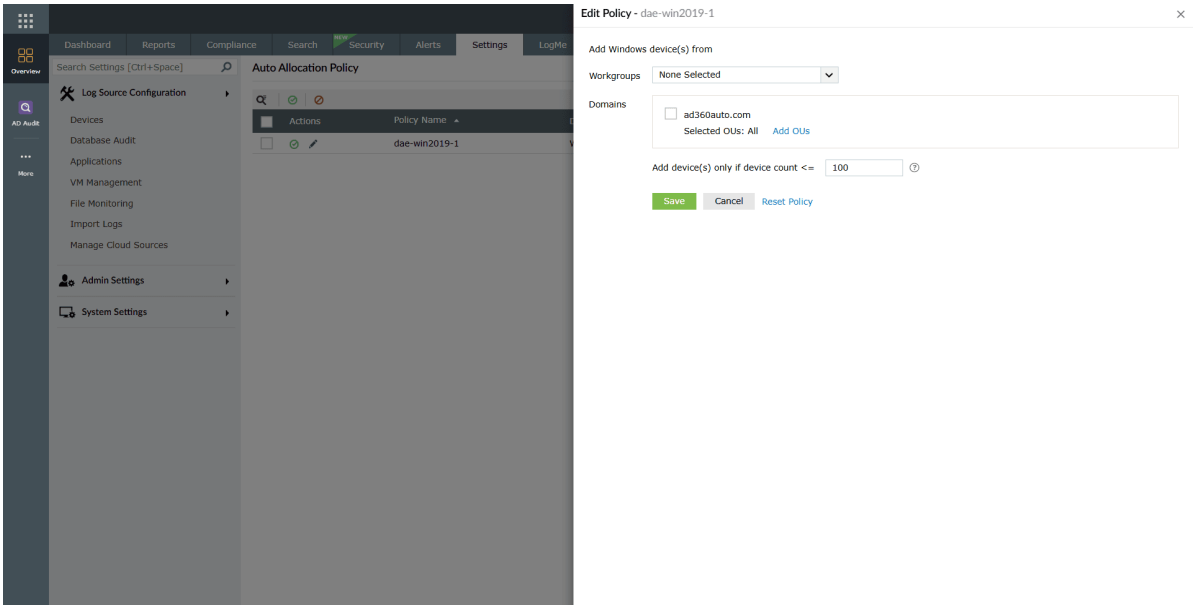
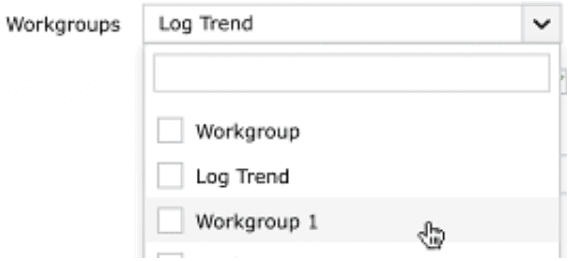
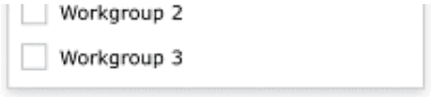


Image 5: Editing an auto allocation policy

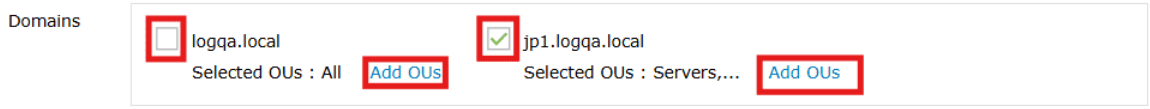
2. Fill out the fields according to your requirements.

- Workgroups: You can select the workgroup to add devices from those workgroups only.

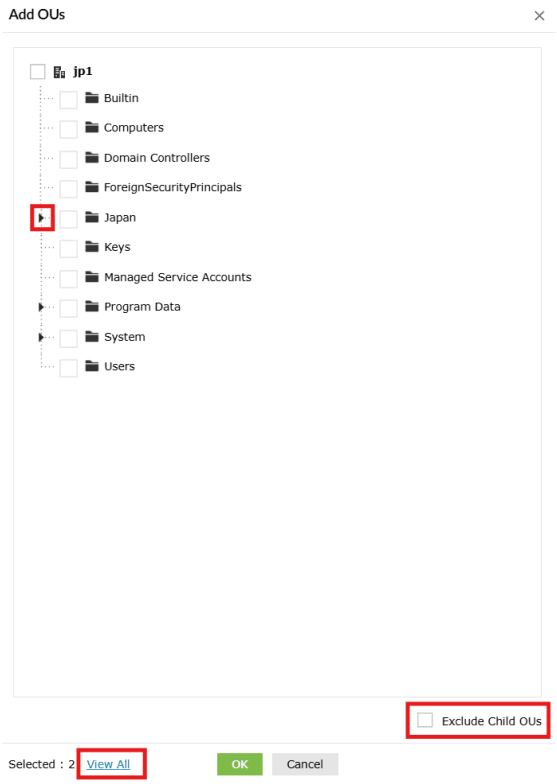




- Domains: Add devices only from selected OUs (Organizational Units) in the selected domains. Use the checkbox to select or deselect the domains to add devices.



  - Click Add OUs to add devices by filter the selected OUs.



  - Click on the □button to expand the OUs that include sub-folder(s).
  - Use Exclude Child OUs option to select parent OUs only.
  - Use View All button to see the selected OUs in Summary View



  - Click OK button to finalize the selected OUs.
- Add Device(s) only if device count <= :
  - Device count must be between 1 & 100

- Device count also includes Non-Windows Devices

> NOTE
>
> The specified device count limit applies to only the associated devices with a speciifc collector.

3. Click on the Save button after you have made all the necessary changes.
4. Upon successful completion of the action, the below pop-up appears.



Trigger auto allocation manually

This function allows you to run the device allocation process instantly. This is useful when any changes have been made to the allocation policies and you don't want to wait for the next scheduled run. This, in turn, ensures that the policy updates take immediate effect.

Steps to trigger auto allocation manually

1. In the Auto Allocation Policy module itself, click on the Run All Policies button to allocate devices as per all policies immediately.

> NOTE
>
> This option will not be available unless auto allocation is enabled.

2. As soon as you click on it, the below pop-up appears, indicating the instant start of a new auto allocation run with the updated policy.



Read also

This document covered how to configure and manage auto allocation policies in the product. For more related functionalities, refer to the following articles:

- Check unallocated device(s) status
- Sync settings

9.6.3.4. Check unallocated device(s) status

Last updated on: September 12, 2025

In this page

Overview

Check unallocated device status

Overview

This section guides you through accessing the unallocated device(s) list, understanding the reasons for unallocation, and taking corrective action to ensure full monitoring coverage.

Check unallocated device status

To view devices that couldn't be assigned through auto allocation, you can check the status of unallocated devices and gain insights as to why certain devices remain unallocated and take corrective action, if needed.

Steps to check status of unallocated device(s)

1. Navigate to the Settings tab and click on Devices.

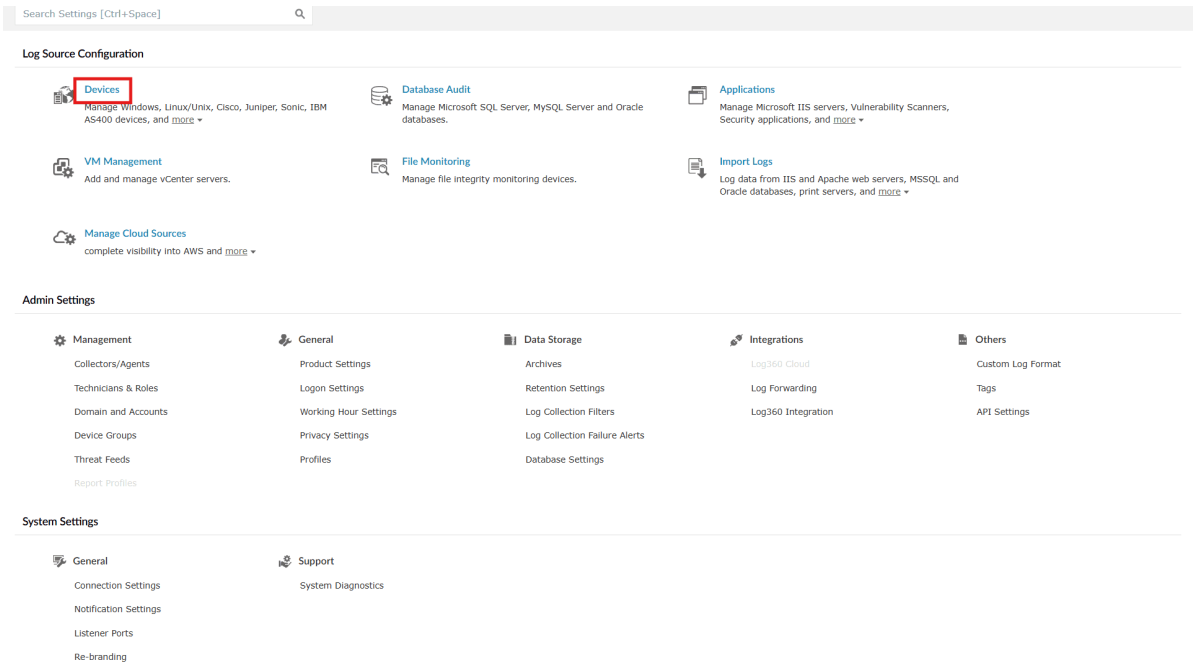


Image 1: Device settings in the product console

2. You will be taken to the Device Management module. Click on the Add Device(s) button to check the status of unallocated devices.

> **NOTE**
>
> Status will be shown only when the auto allocation feature is in an enabled state.

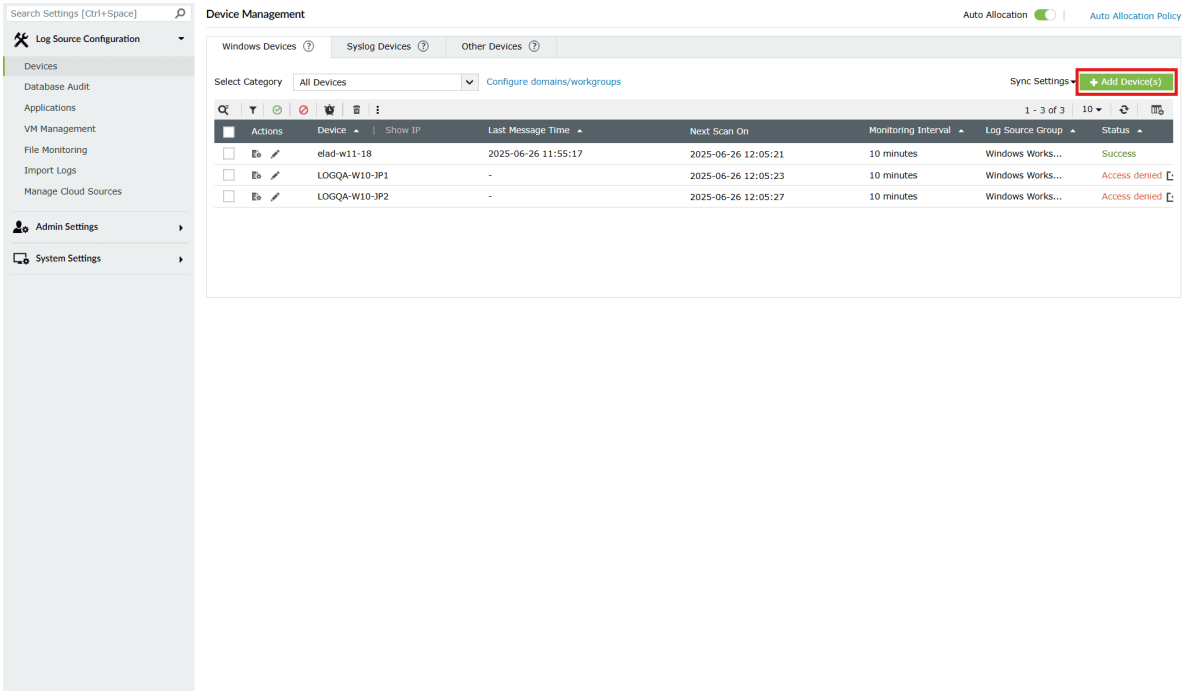


Image 2: Device allocation settings in the product console

3. A pop-up box appears along with a list of the Unallocated Device(s), their Operating System, the Organizational Unit they belong to, and the Reason for being unallocated.

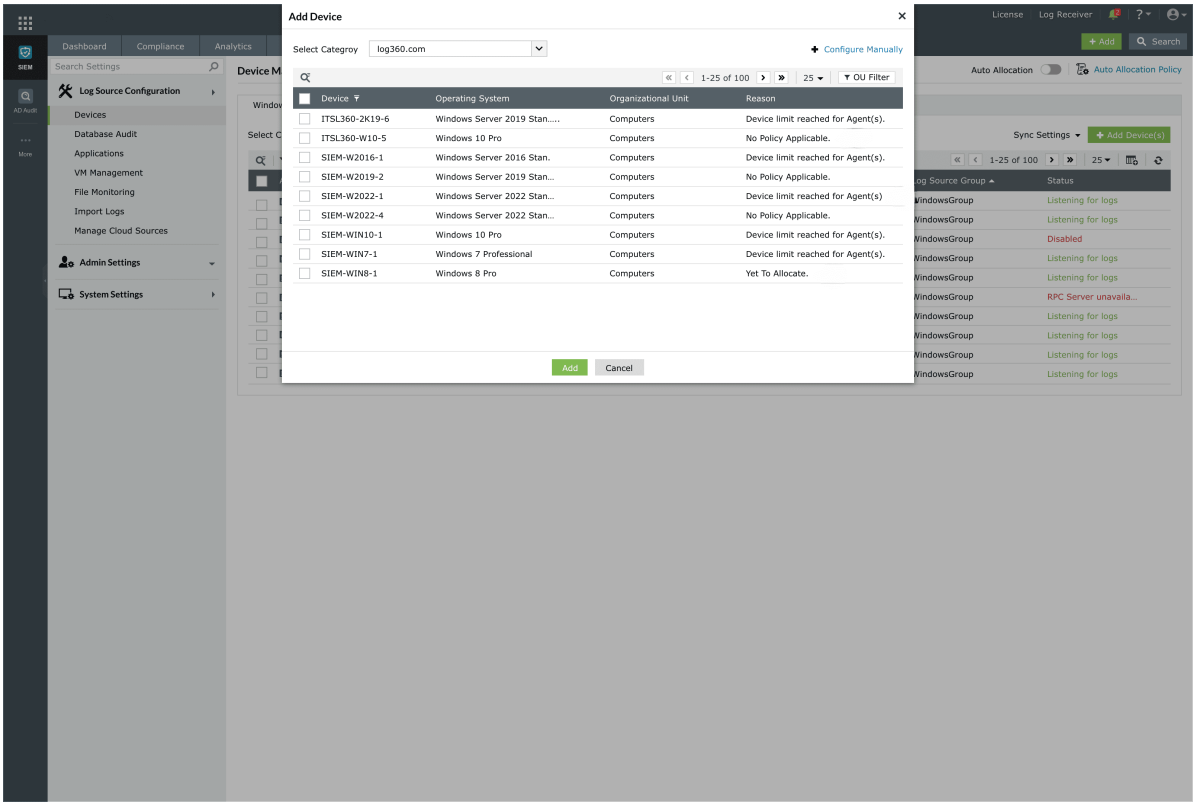


Image 3: Device auto allocation in the product console

Hover the mouse pointer over the reason you would like to read completely, and a tool-tip highlighting the full version of the reason appears. There are three different types of status that could be listed under the possible reason(s) for the unallocation as listed below:

- No Policy Applicable: The device does not match the criteria of the policy with respect to the selected domain, OU (Organizational Unit) container or the workgroup in the policy.
- Device limit reached for Agent(s): The Auto Allocation Policy's device count limit has been reached.
- Yet to Allocate: Device is yet to be allocated in the upcoming schedule.

Read also

This document explained how to check the status of devices that were not allocated through auto allocation. For more details on related features, see the articles below:

- Sync settings

9.6.3.5. Sync settings

Last updated on: September 12, 2025

In this page

Overview

Device Addition sync settings

Overview

Log360 allows two-way synchronization of device data with its identity threat detection and response component, ADAudit Plus. This section explains how to enable or disable the addition sync settings, helping you control whether devices are synced from ADAudit Plus to Log360 and vice versa, based on your configuration needs.

> NOTE
>
> Device Auto Allocation is supported only for Windows instances and not for Linux environments.

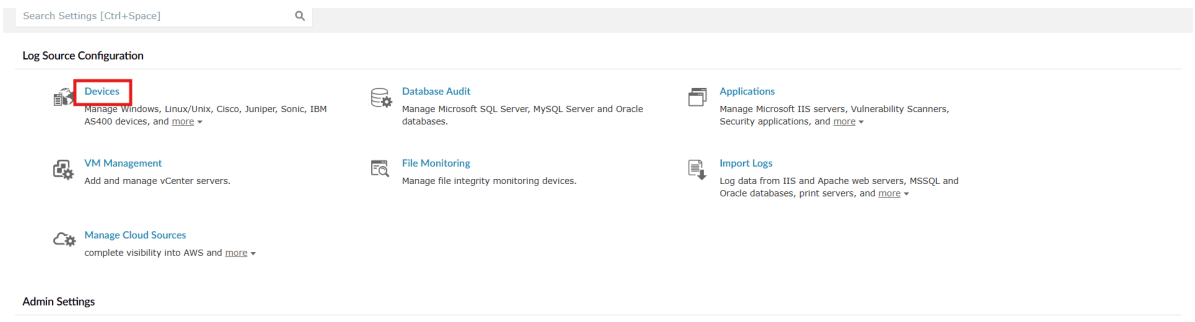
Enable/disable sync settings

> NOTE:
>
> This function is available only to the users who have integrated their ADAudit Plus to their Log360 console.

This settings will help you control the regular synchronization of device(s) data between ADAudit Plus and Log360.

Steps to enable device addition sync settings

1. In Log360 console, navigate to the Settings tab and click on Devices.



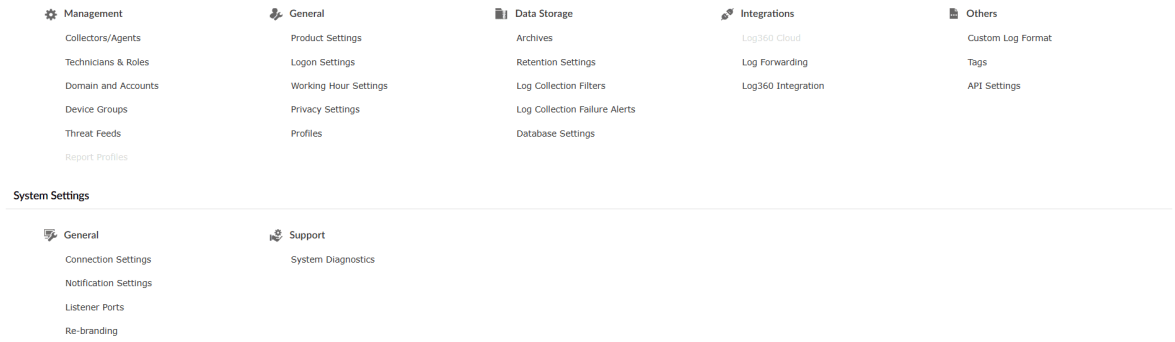


Image 1: Device auto allocation

2. You will be taken to the Device Management module. Click on the Sync Settings button.

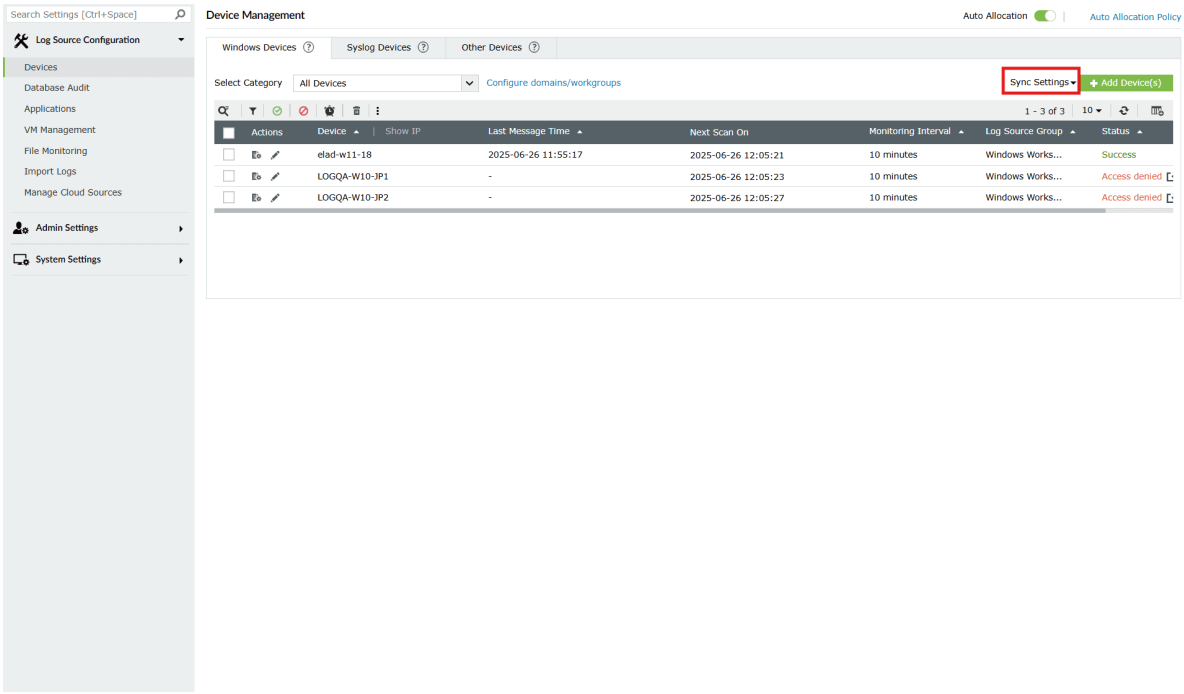


Image 2: Sync settings in device allocation in the product console

3. The Sync Settings popup will appear like the below.

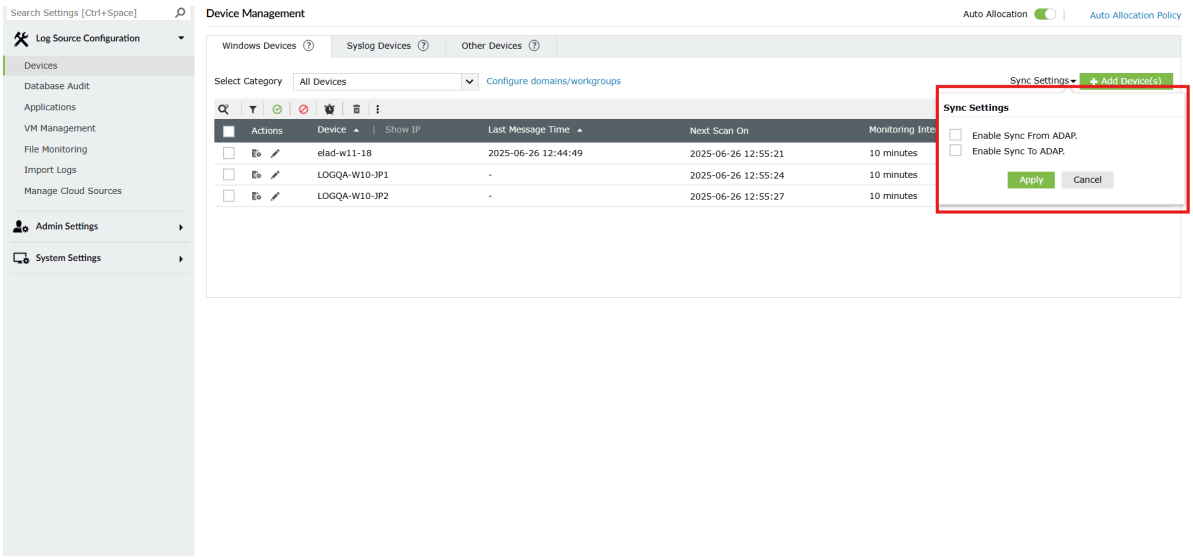
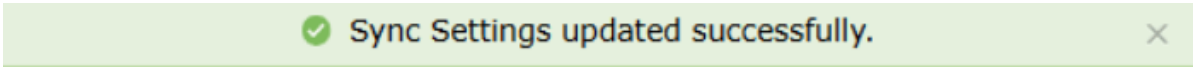


Image 3: ADAudit Plus Sync settings in device allocation in the product console

4. Click on:
   - Enable Sync From ADAudit Plus checkbox: To sync the devices from ADAudit Plus to Log360. If it's not selected, then the device will not sync to Log360 which is integrated with ADAudit Plus.
   - Enable Sync To ADAudit Plus checkbox: To sync the devices from Log360 to ADAudit Plus. If it's not selected, then the device will not sync to ADAudit Plus which is integrated with Log360.

   In case you wish to enable the sync, ensure that the checkbox is ticked. In case you wish the sync to be disabled, ensure that the checkbox is empty.
5. Once you have made the necessary settings, click on the Apply button to save your configuration.
6. Upon successful completion of the action, the below pop-up appears.



NOTE

Only Device addition will sync inbetween products. enable and disable actions will not sync. On Deletion, it will ask in deletion popup weather to sync the delete to other product or not. For more information about deletion sync refer this.

Read also

This document explained how to configure sync settings between the product console and ADAudit Plus. For related configuration and device management topics, refer to:

- What is Device auto allocation?
- Configuring auto allocation

9.6.4. Manage Security Applications

Last updated on: September 12, 2025

> **Note**
>
> Previously known as 'Threat sources'

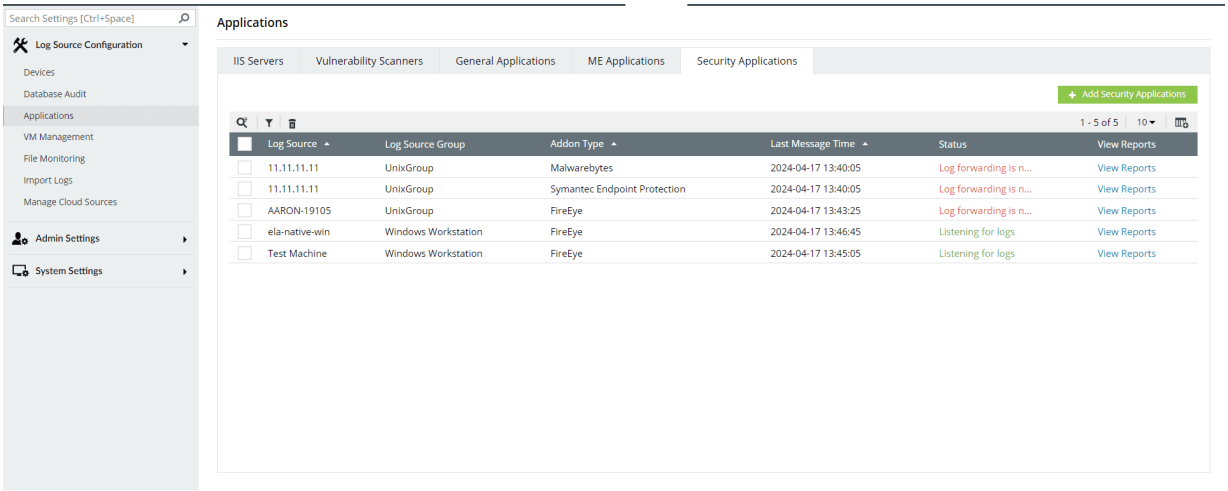
This dashboard lets you manage all security applications monitored by EventLog Analyzer.
Settings > Log Source Configuration > Applications > Security Applications

How to add a security application?

How to add a security application? Add Security application.

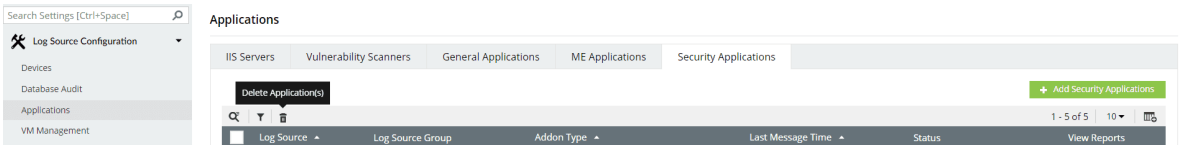
How to view a security applications report?

1. Go to Settings > Log Source Configuration > Applications > Security Applications
2. Click on the View Report icon on the right corresponding to the security application.



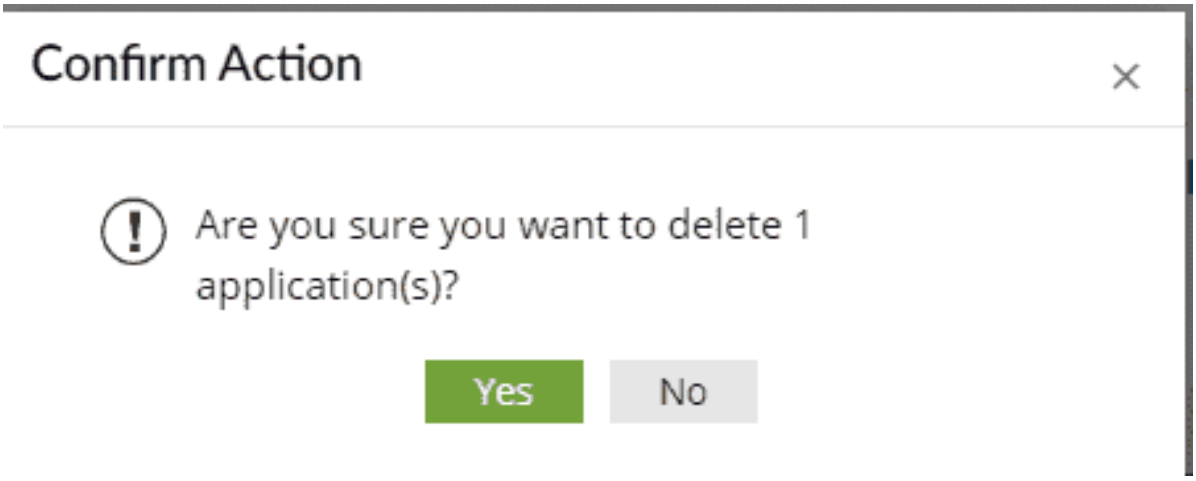
How to delete a security application?

1. Go to Settings > Log Source Configuration > Applications > Security Applications
2. Select the security application you want to delete and click on the delete icon.





3. Click Yes in the delete confirmation pop-up.



9.6.5. Applications

Last updated on: September 12, 2025

This module lets you manage the applications being monitored by EventLog Analyzer. Applications such as IIS Servers, Vulnerability Scanners, and Security Applications can be added, deleted, and viewed.

Extensions

Applications that are integrated as extensions can be found under the Other Applications tab. Currently, the following application extensions are available for EventLog Analyzer:

- Veeam
- Dropbox

9.6.6. Threat Management

Last updated on: September 12, 2025

This page elaborates the steps to manage the threat sources of EventLog Analyzer.

Enabling or disabling the default threat server

Adding TAXII server

Editing TAXII server configuration

Deleting TAXII server

Managing TAXII feeds

Advanced threat analytics

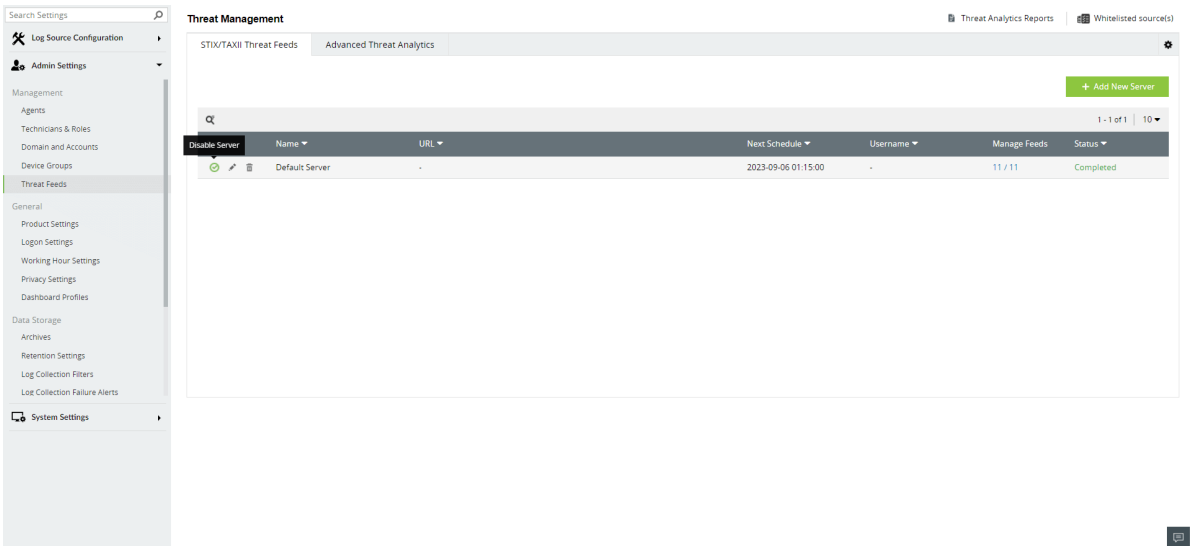
Enabling or disabling the default threat server

What is the default threat server?

EventLog Analyzer collects threat information from various STIX/TAXII based threat feeds such as Firehol, PhishTank, ThreatFox, AlienVault OTX and Cyware on a daily basis. The threat information (malicious IPs, URLs, and domain names) is processed and stored on the ManageEngine cloud server. EventLog Analyzer securely connects to the cloud service and downloads the threat feed everyday. Using this information, it detects and raises an alert immediately when malicious sources interact with your enterprise network.

How to enable or disable the default threat server?

1. Go to Settings > Threat Management > STIX/TAXII Threat Feeds.
2. Click the enable/disable icon under Actions to enable/disable the default server.



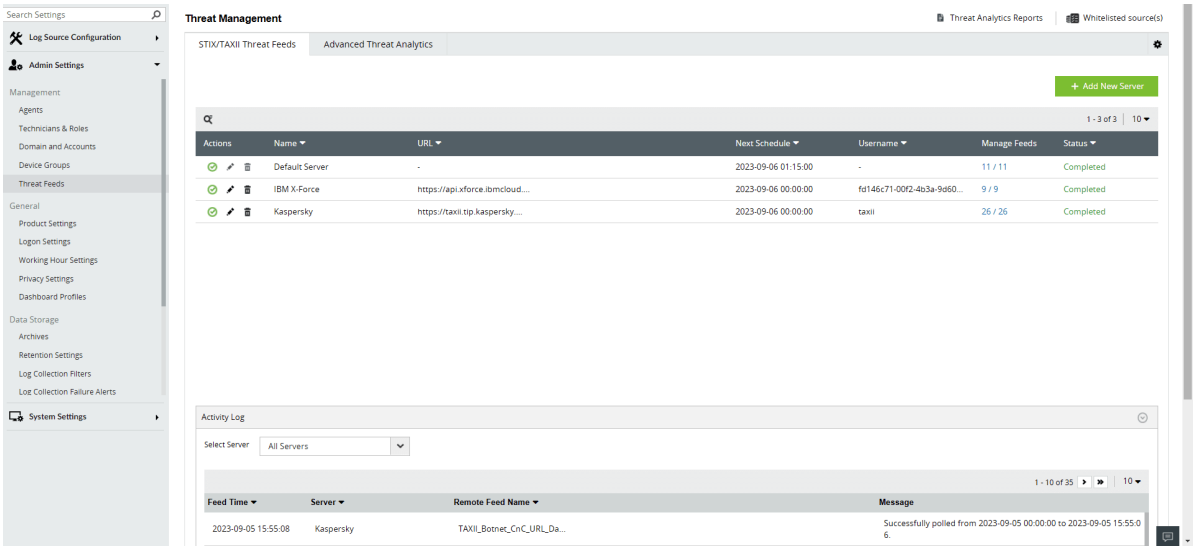
Note

You cannot edit or delete the default server.

By default, the default threat server is disabled when Advanced Threat Analytics (ATA) is enabled as ATA has a much larger and more accurate threat data set. If required, you can override this by enabling the default threat server again. When default threat server is enabled, if a particular threat source is not flagged by ATA, EventLog Analyzer will check in default threat server's threat database and flag the threat source accordingly.

How to add a new STIX/TAXII server?

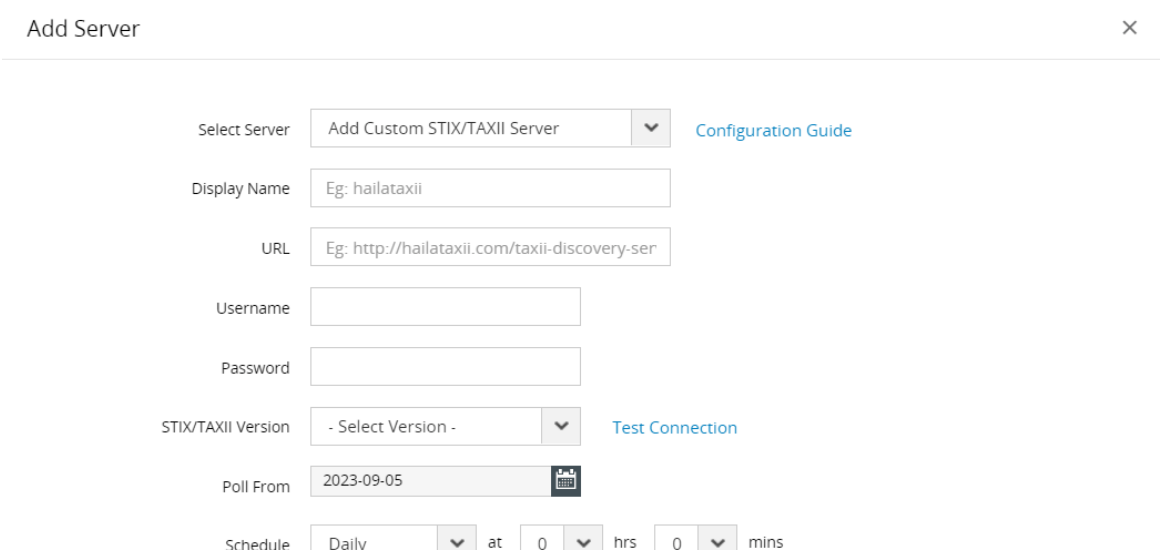
1. Go to Settings > Threat Management > STIX/TAXII Threat Feeds.
2. Click Add New Server.

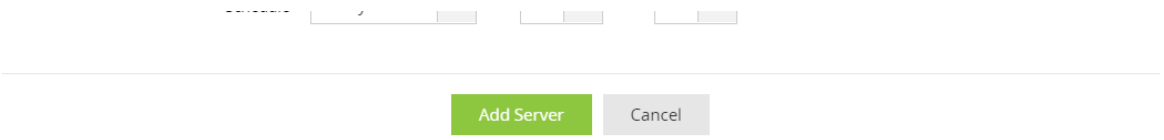


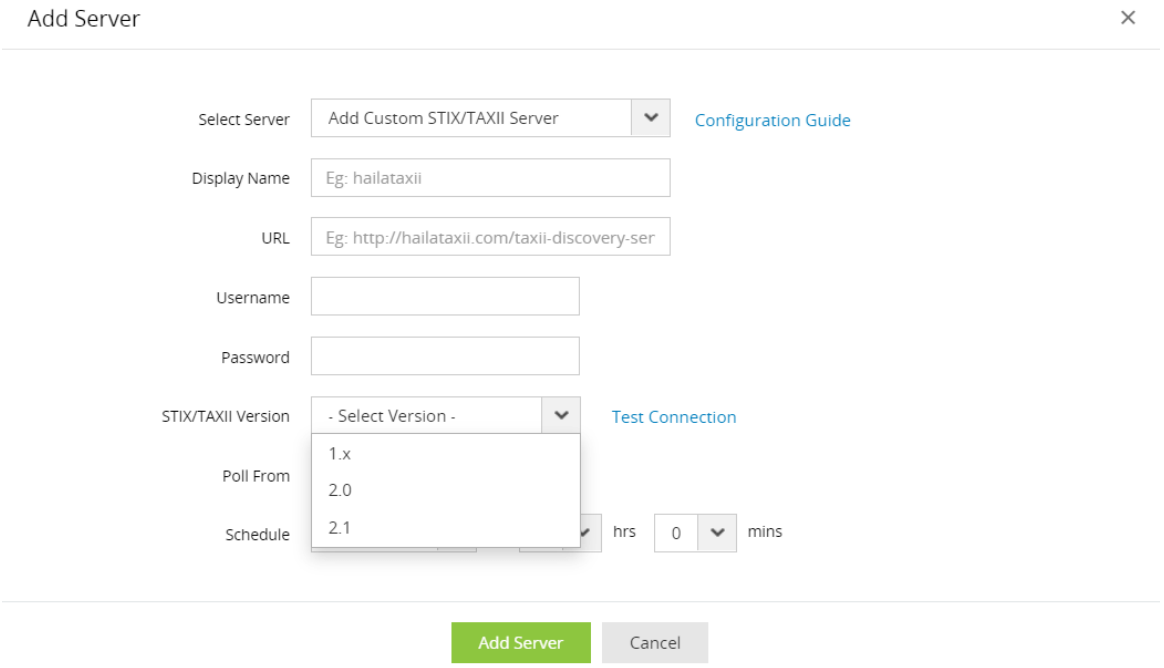
Find the "Add New Server" button located on the top right corner.

3. In the Add Server box,

- For a Custom STIX/TAXII Server, enter the Display Name, URL, Username, Password and choose the STIX/TAXII Version of the server.

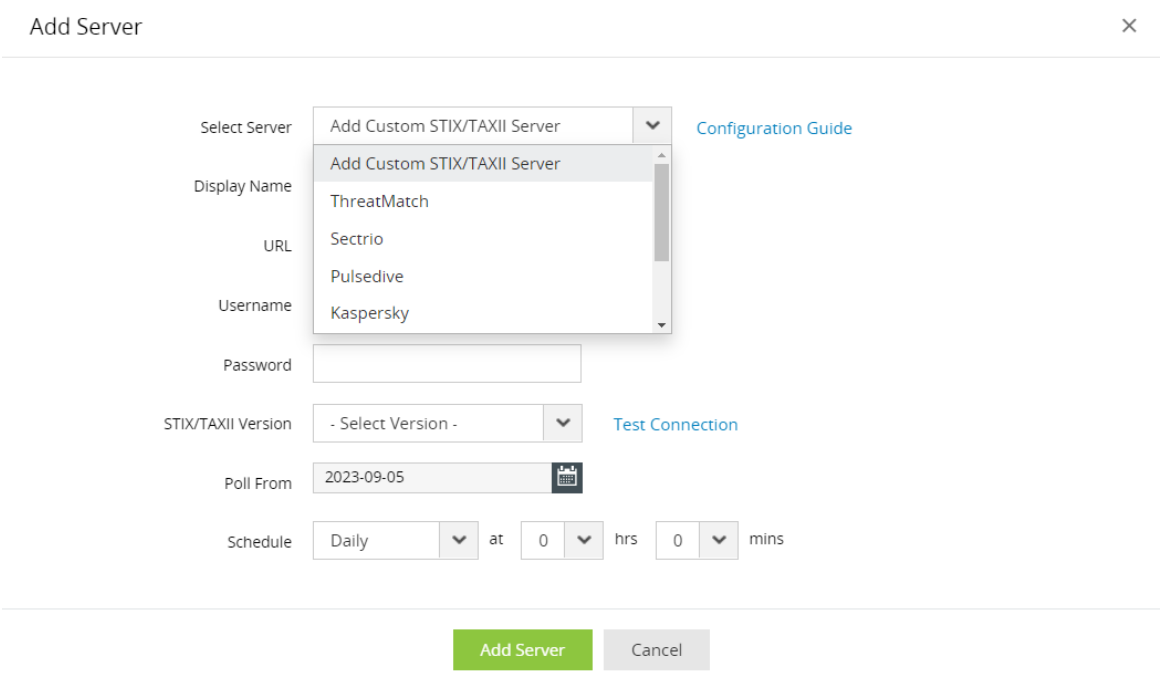






Choose the STIX/TAXII version of the custom server that is to be configured

- For Quick-Deploy Servers, choose a STIX/TAXII server from drop-down, enter the Credentials (Username or API key or Client ID, Password or Secret key) as required for the corresponding server. URL and Display name are both automatically assigned by EventLog Analyzer for Quick- Deploy Servers.



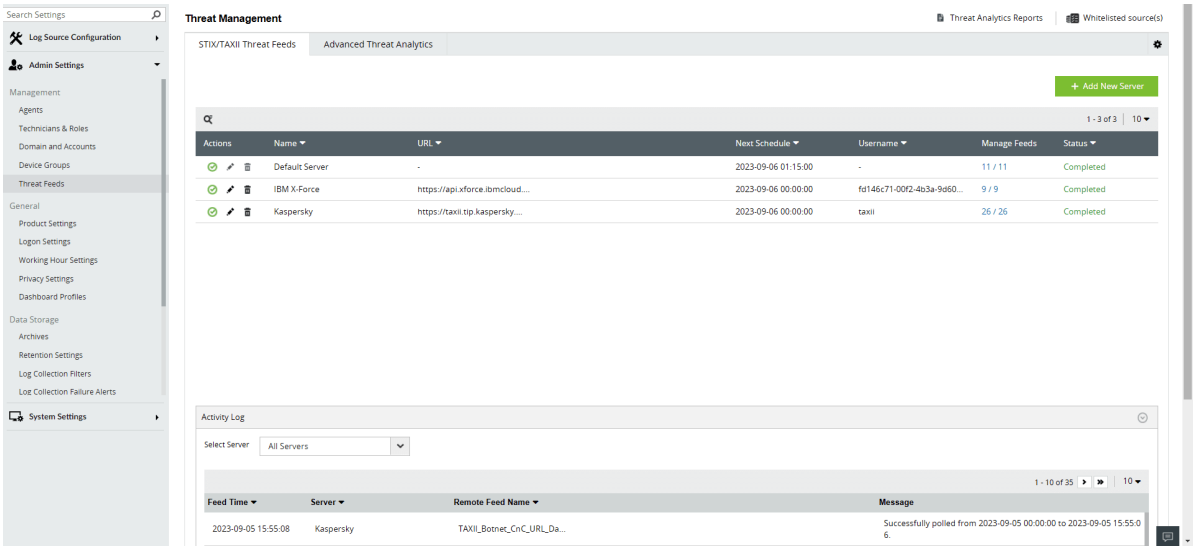
Choose a Quick Deploy Server from the options presented in the drop down box.

4. In the Poll From section, specify the start date from when the feeds should be collected.

5. In the Schedule drop down list, select the schedule frequency and the time for syncing data from the TAXII server.
6. To save the server configuration, click Add Server.

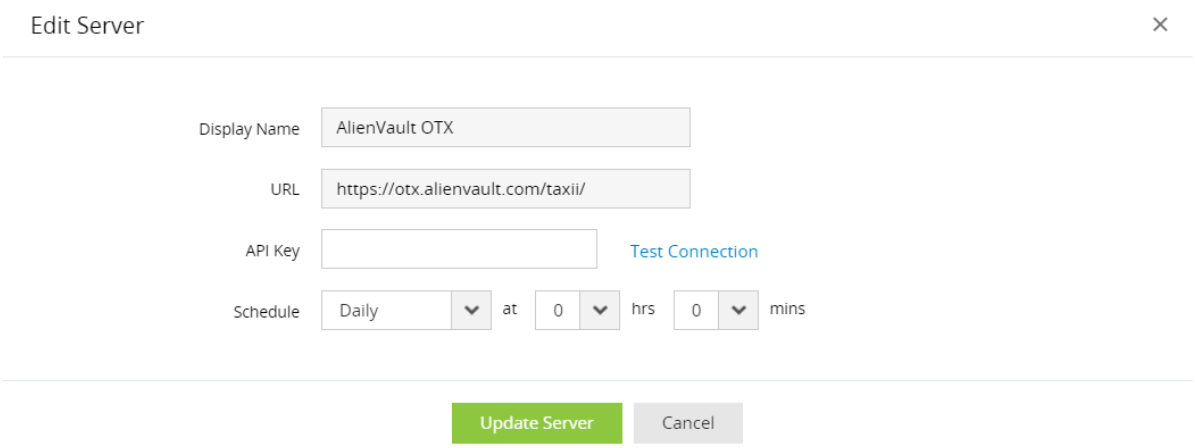
How to edit TAXII server configuration?

1. Go to Settings > Threat Management.
2. Click the edit icon against the server.



The edit option is present under the Actions column for each server.

3. You can make the required changes such as the schedule to sync data from the TAXII server.

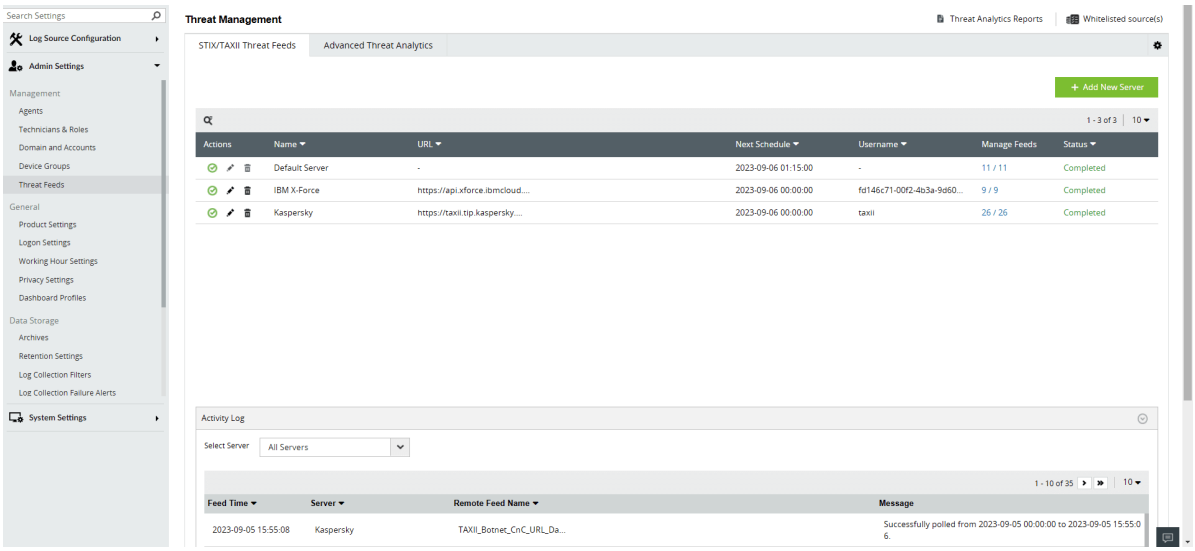


4. To save the changes made, click the Update Server button.

How to delete TAXII server?

To delete an existing TAXII server,

1. Go to Settings > Threat Management.
2. Click the delete icon corresponding to the server to be deleted.

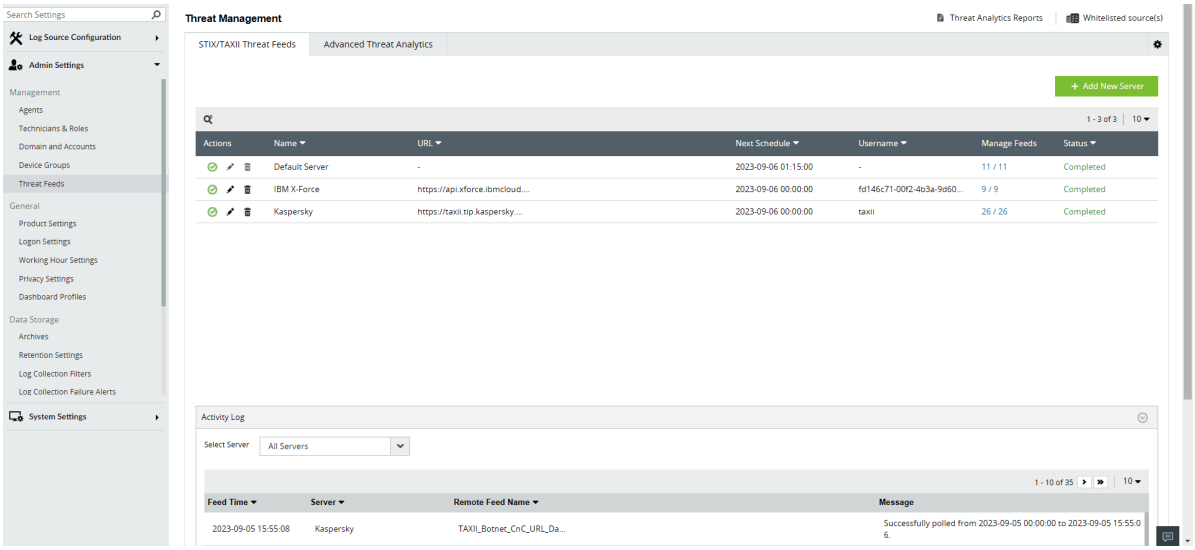


The delete option is present under the Actions column for each server.

3. Click Yes in the delete confirmation pop up box.

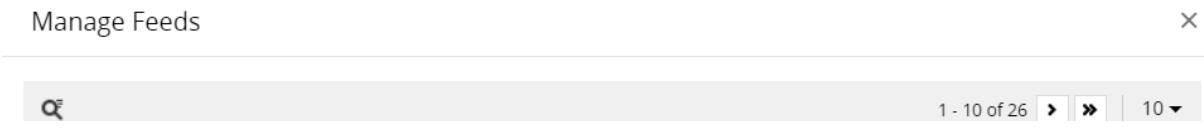
How to manage TAXII server feed?

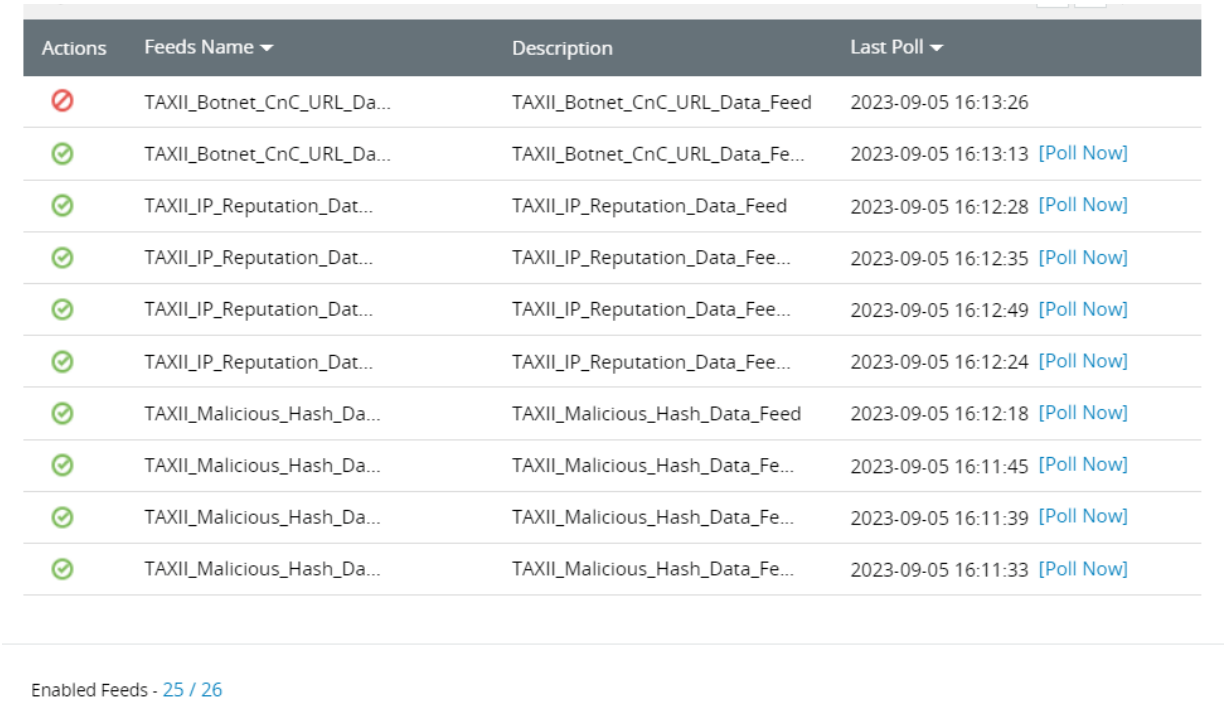
1. Go to Settings > Threat Management > STIX/TAXII feeds.
2. Click Manage Feeds corresponding to the server to be managed.



The Manage Feeds option can be found within the dedicated column for each server.

3. Click the enable/disable icon under Actions to enable/disable polling for the corresponding feed. Click Yes in the pop-up to confirm.
4. Click Poll now poll the feed immediately.





Actions	Feeds Name	Description	Last Poll
	TAXII_Botnet_CnC_URL_Da...	TAXII_Botnet_CnC_URL_Data_Feed	2023-09-05 16:13:26
	TAXII_Botnet_CnC_URL_Da...	TAXII_Botnet_CnC_URL_Data_Fe...	2023-09-05 16:13:13 [Poll Now]
	TAXII_IP_Reputation_Dat...	TAXII_IP_Reputation_Data_Feed	2023-09-05 16:12:28 [Poll Now]
	TAXII_IP_Reputation_Dat...	TAXII_IP_Reputation_Data_Fee...	2023-09-05 16:12:35 [Poll Now]
	TAXII_IP_Reputation_Dat...	TAXII_IP_Reputation_Data_Fee...	2023-09-05 16:12:49 [Poll Now]
	TAXII_IP_Reputation_Dat...	TAXII_IP_Reputation_Data_Fee...	2023-09-05 16:12:24 [Poll Now]
	TAXII_Malicious_Hash_Da...	TAXII_Malicious_Hash_Data_Feed	2023-09-05 16:12:18 [Poll Now]
	TAXII_Malicious_Hash_Da...	TAXII_Malicious_Hash_Data_Fe...	2023-09-05 16:11:45 [Poll Now]
	TAXII_Malicious_Hash_Da...	TAXII_Malicious_Hash_Data_Fe...	2023-09-05 16:11:39 [Poll Now]
	TAXII_Malicious_Hash_Da...	TAXII_Malicious_Hash_Data_Fe...	2023-09-05 16:11:33 [Poll Now]

Enabled Feeds - 25 / 26

Quick-Deploy STIX/TAXII Servers

Follow the instructions above to integrate Quick-Deploy STIX/TAXII threat intelligence feeds with EventLog Analyzer. You may need to contact your vendor directly to obtain the credentials for configuration.

AlienVault OTX

Learn more about Alienvault OTX API. Sign up to receive API key.

Cyware Threat Intelligence

Learn more about CywareThreatIntelFeeds. To receive credentials, signup here.

IBM X-Force

Learn more about IBM X-Force Integration. To purchase, please click here.

Kaspersky Threat Intelligence

Learn more about Kaspersky Threat Feeds. To purchase, please click here.

PulseDive Threat Intelligence

Learn more about PulseDive. To purchase, please click here.

Sectrio Threat Intelligence

Learn more about Sectrio. To purchase, please click here.

SecAlliance- ThreatMatch Intelligence

Learn more about ThreatMatch. To purchase, please click here.

STIX/TAXII versions of the Quick-Deploy Servers supported in EventLog Analyzer:

S.no	SERVER NAME	STIX/TAXII VERSION
1	AlienVault OTX	1.x
2	Cyware Threat Intelligence	2.1
3	IBM X-Force	2.0
4	Kaspersky Threat Intelligence	2.1
5	Pulsedive Threat Intelligence	2.1
6	Sectrio Threat Intelligence	2.1
7	SecAlliance-ThreatMatch Intelligence	2.1

10.1.1.1. Security dashboard

Last updated on: September 12, 2025

In this page

Overview

Security tab in the dashboard

Security Analytics- A breakdown of the dashboard

Data in precise numbers

Overview

The Security Analytics Dashboard offers a unified view of your organization's threat landscape, turning detection data into actionable insights. Key elements of this dashboard:

- Visual representation of high-level metrics
- MITRE ATT&CK mapping
- Historical trends

With compact widgets for quick decision-making and expanded views for deep investigations, the dashboard helps monitor evolving threats, uncover patterns, and streamline incident response with precision.

Security tab in the dashboard

1. In the product console, click on the Security tab in the dashboard as highlighted below.

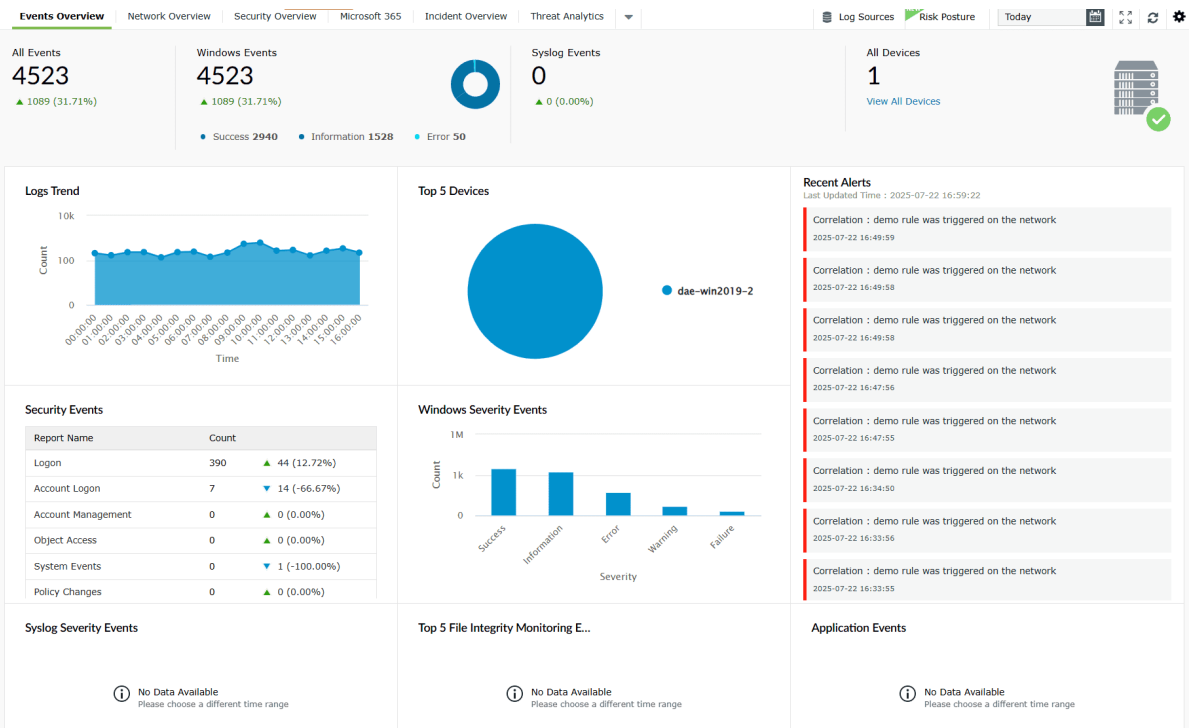


Image 1: Security tab in the dashboard

2. You will be taken to the Security Analytics dashboard.

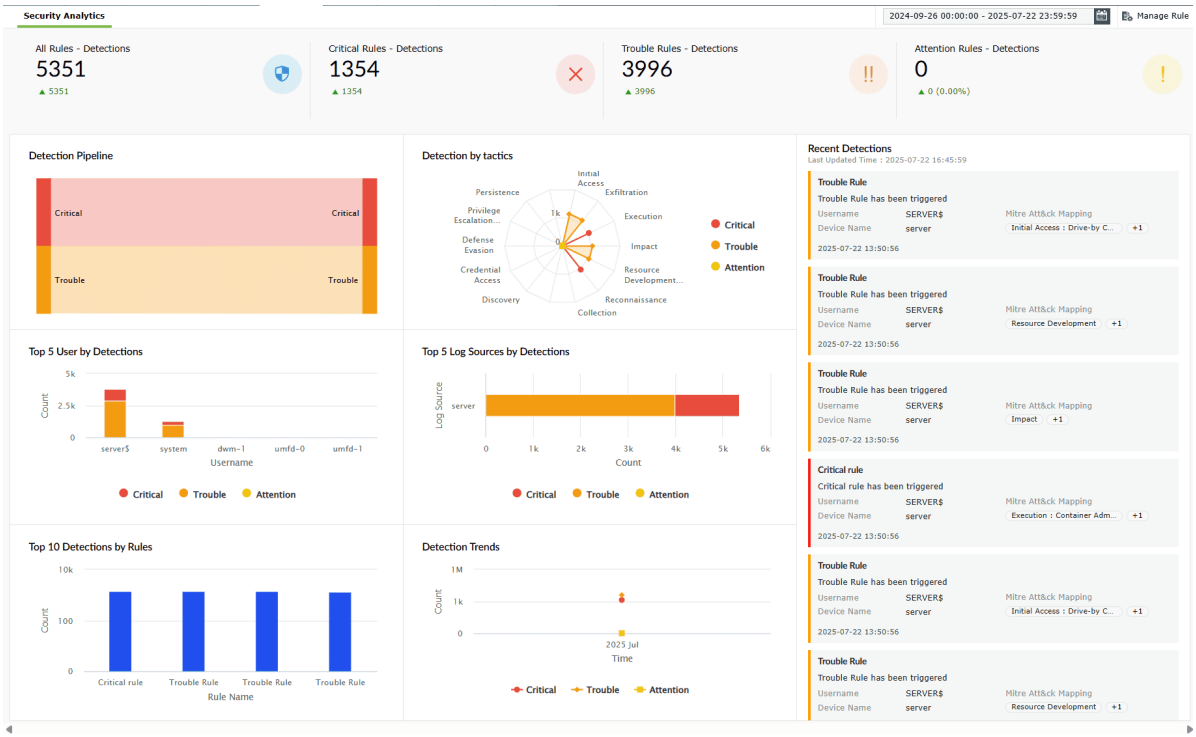


Image 2: Security analytics dashboard

Read further to understand the role of each widget in this tab and how it contributes to your network's security analytics.

> NOTE
>
> To make the best use of this dashboard make sure that the rules for the detection are active and properly configured since this dashboard provides data and insights based on the currently active rules and their unique configurations.

Security Analytics- A breakdown of the dashboard

Data in precise numbers

The four compact elements in the top-most ribbon of the Security Analytics dashboard offer a high-level snapshot of detection activities across all three severity levels with accurate numbers, providing quick visibility into the total number of detections classified based on their distribution in severity levels of the rules as follows:

- All Rules - Detections
- Critical Rules - Detections
- Trouble Rules - Detections

- Attention Rules - Detections

These shall assist the security teams instantly gauge the overall threat landscape, prioritize the incident response efforts, and also monitor trends in the detection volumes over time.

A. Compact views

1. All Rules - Detections

This component provides the total count of all the detections made across every configured rule, offering a quick overview of your organization's threat landscape.



Details displayed

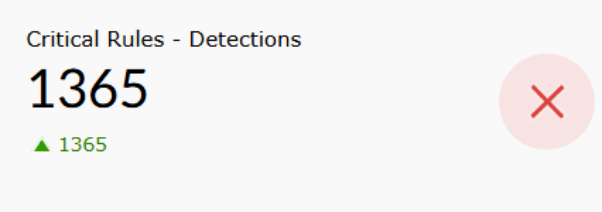
- Detection count: Total number of triggered detections across all rules.
- Growth/decline indicator: A green arrow highlights the decrease in detection counts, whereas a red one indicates an increase.

Role in Security Analytics

- Acts as the primary metric for overall threat volume.
- Helps track total security events within a given time frame.
- Serves as a baseline for comparing the distribution of critical and trouble detections.

2. Critical Rules - Detections

This component focuses on detections triggered by high-severity (critical) rules that require immediate attention.



Details displayed

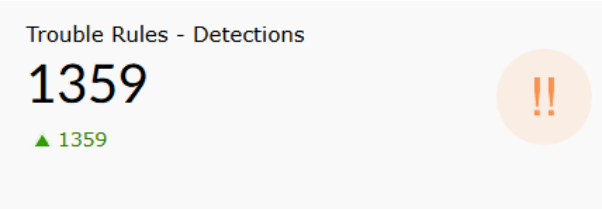
- Detection count: Total number of critical detections.
- Visual indicator: A red icon emphasizes the high-priority nature of these events.
- Growth/decline trend: Green arrow indicates a decrease in detection volume, whereas a red one indicates an increase.

Role in Security Analytics

- Highlights security events with the highest risk and urgency.
- Helps prioritize immediate incident response actions.
- Serves as a key metric for assessing serious vulnerabilities or ongoing attacks.

3. Trouble Rules - Detections

This component displays the count of detections flagged by medium-severity (trouble) rules, representing potential risks or suspicious activities.



Details displayed

- Detection count: Total number of trouble-level detections.
- Visual indicator: Orange icon signals events that need closer monitoring.
- Growth/decline trend: Green arrow indicates changes in detection volume, whereas a red one indicates a decline.

Role in Security Analytics

- Helps monitor and investigate potential threats before they escalate.
- Provides visibility into less urgent but still relevant anomalies.
- Assists in tuning detection rules for medium-risk scenarios.

4. Attention Rules - Detections

This component tracks detections triggered by low-severity (attention) rules, indicating minor anomalies or early warning signs.

Details displayed

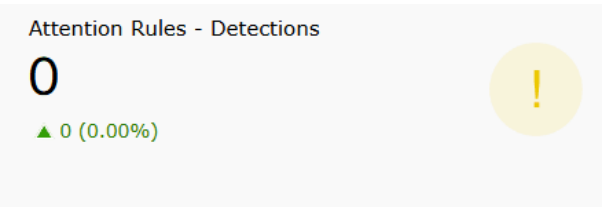
- Detection count: Total number of attention-level detections.
- Visual indicator: Yellow icon signifies a lower risk level.
- Growth/decline trend: Green arrow indicates changes in detection volume, whereas a red one indicates a decline.

Role in Security Analytics

- Offers context for early detection of unusual behavior.
- Helps identify non-critical patterns that could develop into threats.
- Complements higher-severity detections by providing a broader security overview.

B. Expanded view of all four components

While the compact displays offer quick yet effective insights, clicking on the displayed count of any of these four components provides an expanded view of the same, which includes added details and context surrounding these detections.



Upon clicking on the total count displayed in the compact view of any of the components, the expanded view appears with data arranged in an array of columns as shown above.

Available actions

- Clicking on the Export as button allows you to choose a format to export the said data either in a PDF format or a CSV file.
- Clicking on the Report export history icon allows you to view the complete history of the past data exports that have taken place for that particular report.

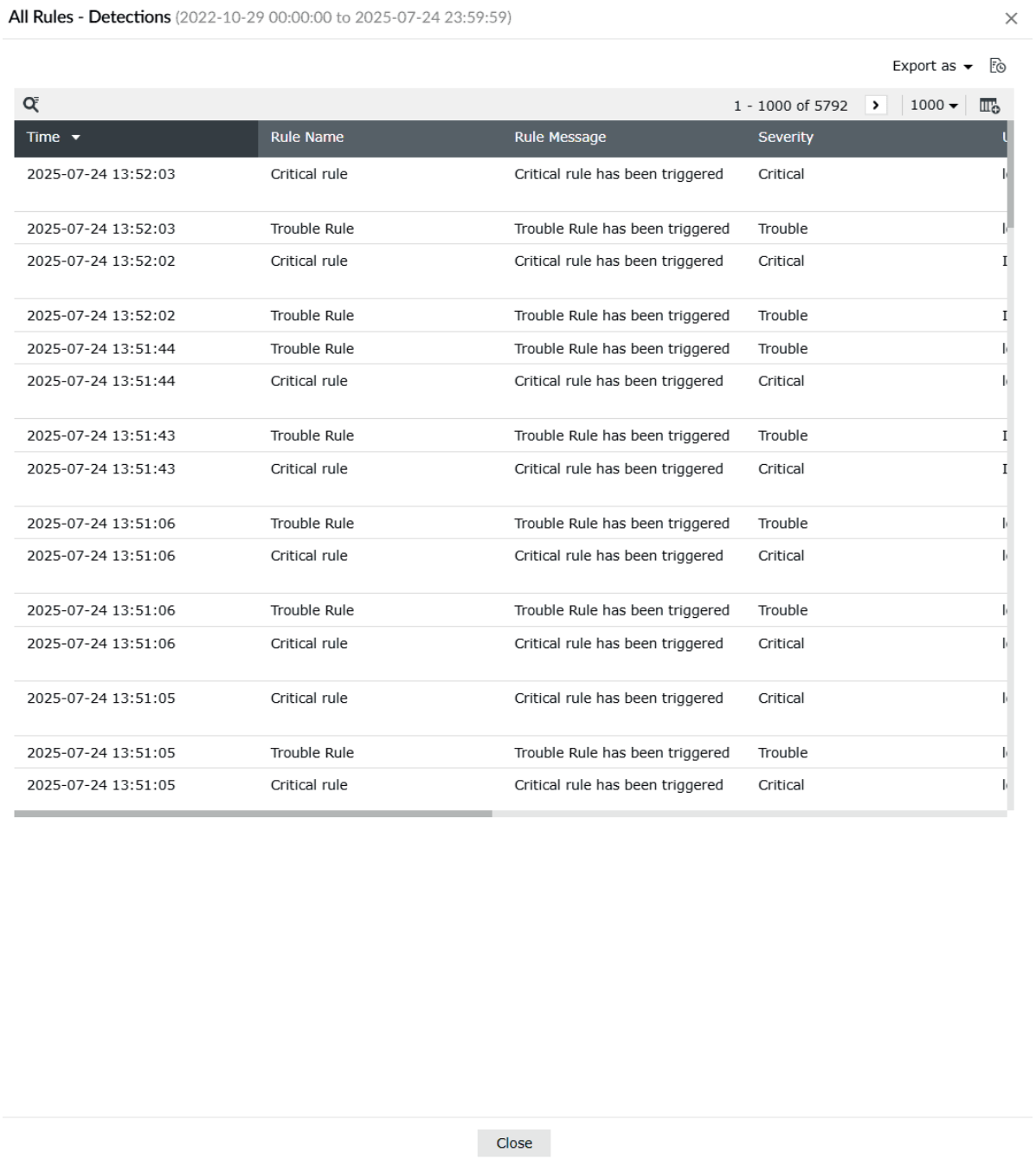


Image 3: All rules detections in security analytics dashboard

- Clicking on the icon on the top-right corner of the data table allows you to select/deselect and Apply what data you wish to view separated by columns.

Details displayed (list of available columns)

- Time: Timestamp for when the rule was triggered.
- Rule Name: Detected rules categorized by their severity level- Critical, Trouble, or Attention.
- Rule Message: A brief descriptive message about the triggered detection.
- Severity: Indicates the severity of the rule detected.
- Username: The account responsible for the activity.
- Log Source: Source system or device associated with the detected activity.
- MITRE ATT&CK Mapping: Tactic and technique classification aligned with the MITRE ATT&CK framework.
- Tags: Additional contextual tags, such as industry verticals.

Role in Security Analytics

- Enables deep investigation of every triggered rule by showing when and where it occurred.
- Assists in prioritizing response based on severity, helping SOC teams act swiftly on critical alerts.
- Maps suspicious activities to known threat tactics (via MITRE ATT&CK) for quicker threat attribution and analysis.
- Enhances visibility into user behavior, log source reliability, and attack patterns.
- Supports fine-tuning of rules by providing granular, real-time feedback on their effectiveness and noise levels.

Read also

This page explained the security dashboard's purpose, how to access it, and the role of its widgets. You also learned how compact and expanded views help track detections by severity, uncover patterns, and prioritize response.

- Security dashboard widgets

10.1.1.2. Security dashboard widgets

Last updated on: September 12, 2025

In this page

Overview

Dashboard widgets

Detection Pipeline

Detection by Tactics

Recent Detections

Top 5 Users by Detections

Top 5 Log Sources by Detections

Overview

The Security Dashboard provides a centralized view of detections across your environment. It helps security teams monitor threats, analyze patterns, and prioritize incidents using real-time visuals and context-driven insights.

Dashboard widgets

Widgets provide real-time snapshots of the detections, trends, and key security metrics made by the detection engine, helping you quickly assess and respond to threats proactively. In the widgets containing graphs, clicking on a severity type removes data corresponding to it from the said graph(s).
There are a total of 7 widgets available in the Security Analytics dashboard:

1. Detection Pipeline
2. Detection by Tactics
3. Recent Detections
4. Top 5 Users by Detections
5. Top 5 Log Sources by Detections
6. Top 10 Rules by Detections
7. Detection Trend

Every widget in this dashboard includes two icons in its top-right corner:
Expand : This option provides an expanded view of that widget, offering more, and deeper insights related to it.
Refresh : Clicking on the Refresh icon instantly re-assesses the real-time log data and updates the widget with the same, ensuring you never miss even a second worth of key findings from your network's security analysis.
Severity colors

Security events (excluding the Top 10 rules by detections widget) are categorized by severity levels as set during the rules configuration, represented through distinct colors for quick identification as listed below:

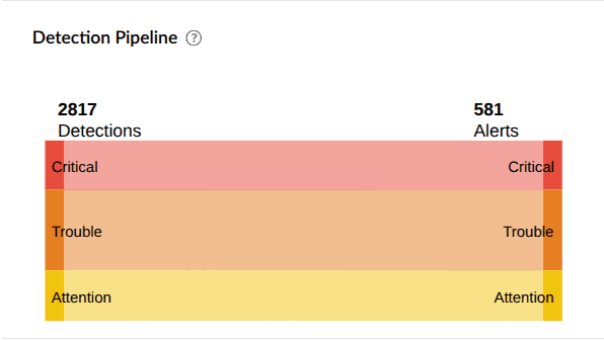
- Red- Critical: Represent severe, high-priority security detections that require immediate attention and possible mitigation steps.
- Orange- Trouble: Indicate medium-level events/incidents hinting at potential risks, suspicious activities, or policy violations that demand prompt investigation.
- Yellow- Attention: Denote low-level detections that require monitoring but pose no immediate risk.

Below is a complete breakdown of all the widgets that the Security Analytics dashboard is comprised of:

1. Detection Pipeline

The Detection Pipeline visualizes the flow of the detections and alerts across the three severity levels. It provides a quick overview of how many events were detected, categorized, and then escalated into actionable alerts.

A. Concise widget view



Details displayed

- Detections: The total count of events flagged by the system.
- Alerts: Number of detections that have been flagged as alerts.
- Severity distribution: Each of the three severity levels is displayed with its corresponding event(s) count.

Role in Security Analytics

The Detection Pipeline widget acts as the starting point for threat monitoring by helping analysts:

- Quickly identify the severity distribution of all the current threats.
- Detect spikes or anomalies in alert generation.
- Streamline the investigation process by focusing on high-priority alerts.

B. Expanded widget view

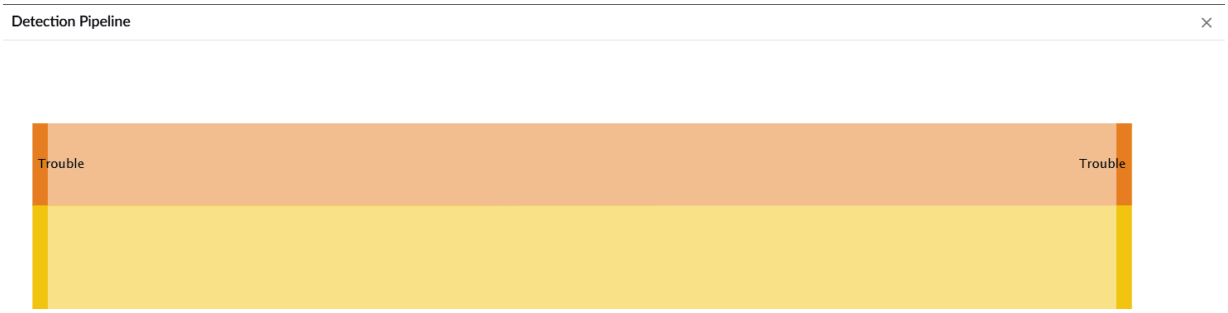




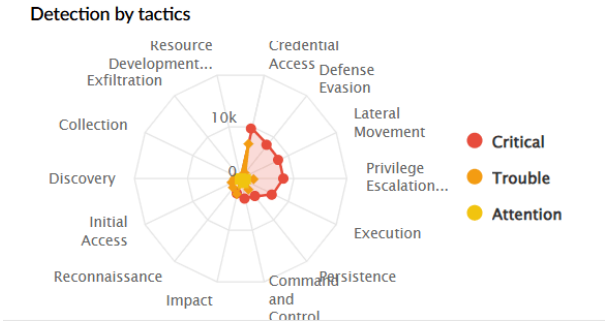
Image 1: Detection pipeline widget in security analytics dashboard

The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.

2. Detection by Tactics

The Detection by Tactics chart maps all the flagged events to the MITRE ATT&CK framework. It shows which stages of the cyberattack lifecycle, such as Initial Access, Execution, Privilege Escalation, are being set in motion via simultaneous events/activities.

A. Concise widget view



Details displayed

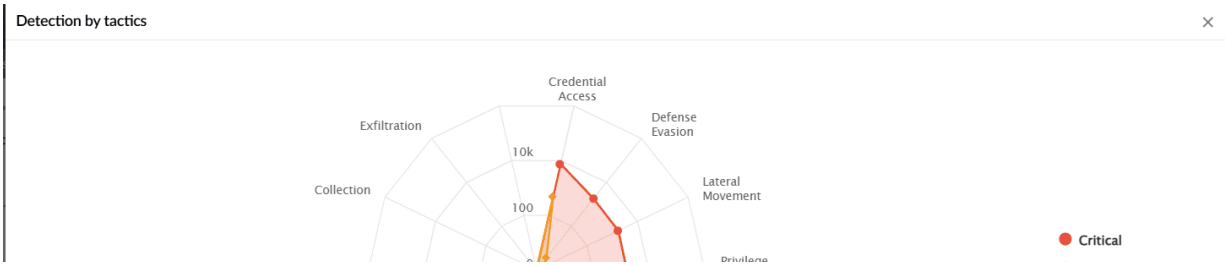
- Tactic categories: Includes the possible common attack stages like Initial Access, Discovery, Exfiltration, and Lateral Movement.
- Severity overlay: Each tactic is color-coded by the three severity levels.

Role in Security Analytics

This widget provides a tactical view of potential adversary behavior, helping teams:

- Analyze and understand attack patterns and prevalent tactics in their environment.
- Prioritize security controls for the most frequently targeted attack phases.
- Align detection rules with industry-recognized attack models for enhanced defense.

B. Expanded widget view



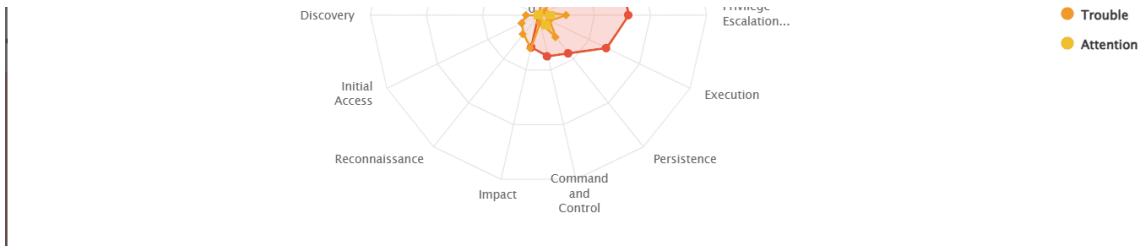


Image 2: Detection by tactics widget in security analytics dashboard

- The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.
- Clicking on any data point representing a detection count slides open the data table for that particular rule severity level, similar to the expanded view of the four components.

3. Recent Detections

The Recent Detections widget provides a chronological list of the events triggered most recently, enabling real-time incident visibility.

A. Concise widget view

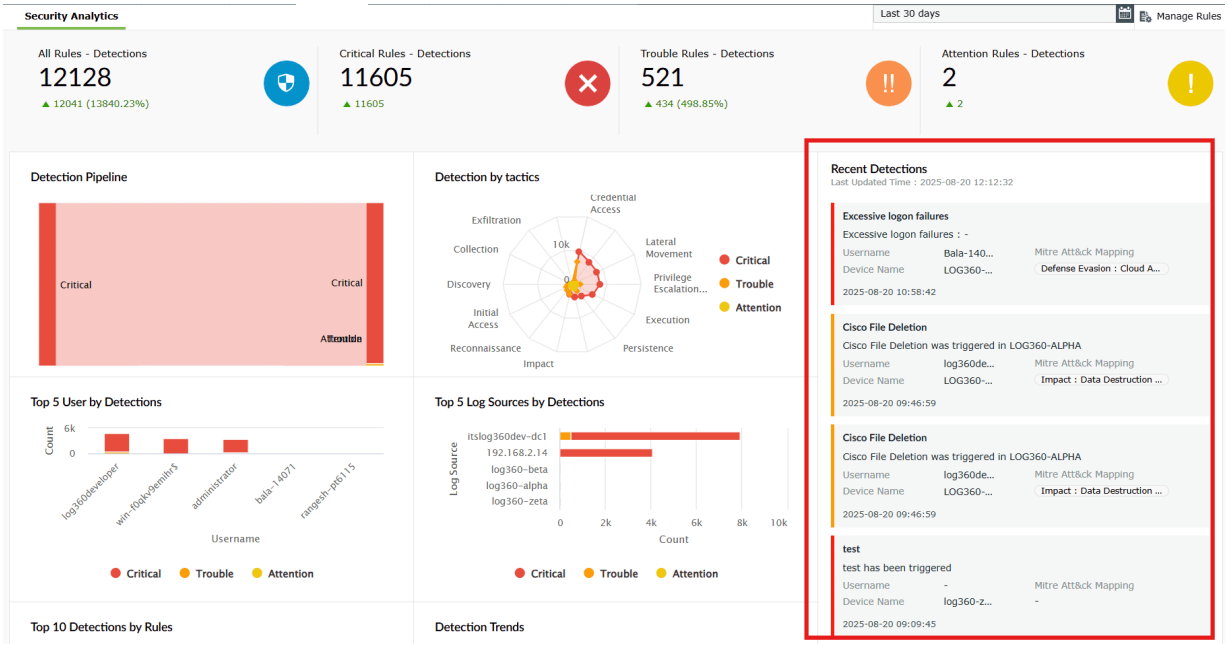


Image 3: Recent detections widget in security analytics dashboard

Details displayed

- Rule name: The name of the rule that is associated with the detection triggered.
- Description: Brief summary of the detection. For example, "Interactive Logon – A process deleted a system backup".
- Username: Identifies the username of the account associated with the event/activity.
- Log Source: Specifies the origin device or system.

- MITRE ATT&CK Mapping: Associates the detection with a specific technique(s) or tactic(s) from the MITRE ATT&CK framework.
- Timestamp: Captures the exact date and time of the event occurrence.

Role in Security Analytics

This widget serves as a real-time threat feed, helping security analysts:

- Quickly detect and respond to emerging threats.
- Correlate events with specific users and devices.
- Perform rapid triage using MITRE mappings to understand the nature of attacks.

B. Expanded widget view

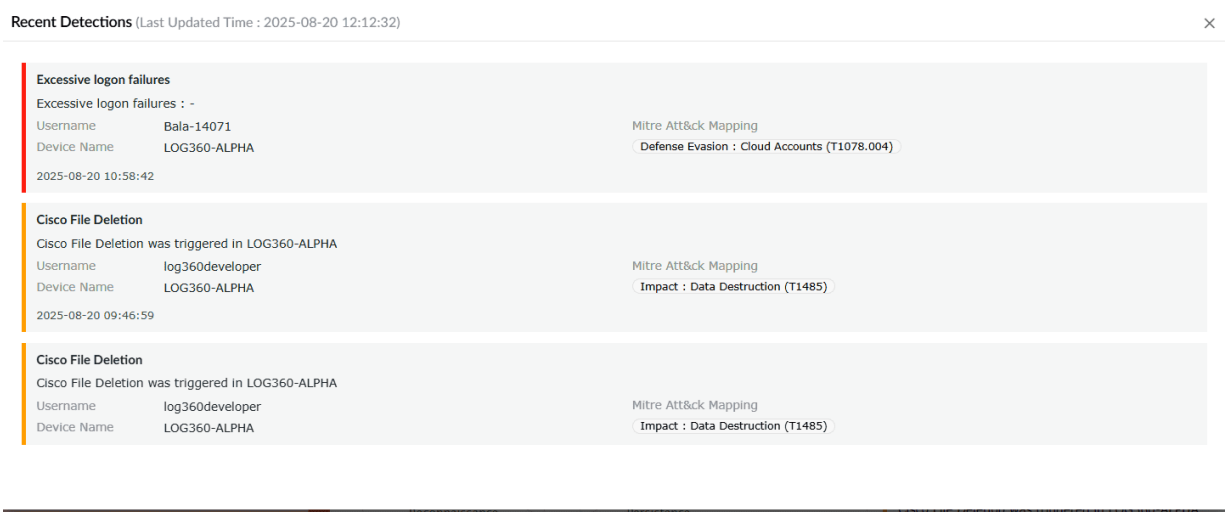
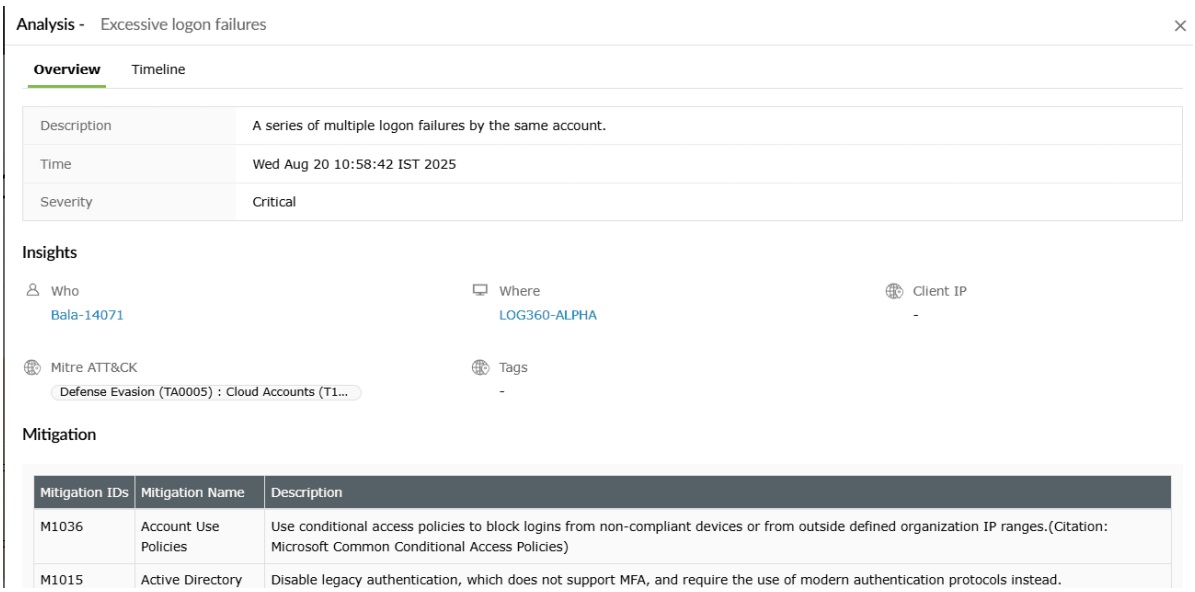


Image 4: Recent detections widget in security analytics dashboard

- The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the details of the most recent detections.
- Upon clicking on any rule from this view (or compact view), a complete analysis of that rule slides open as shown below.



	Configuration	
M1032	Multi-factor Authentication	Use multi-factor authentication for cloud accounts, especially privileged accounts. This can be implemented in a variety of forms (e.g. hardware, virtual, SMS), and can also be audited using administrative reporting features.(Citation: AWS - IAM Console Best Practices)
M1027	Password Policies	Ensure that cloud accounts, particularly privileged accounts, have complex, unique passwords across all systems on the network. Passwords and access keys should be rotated regularly. This limits the amount of time credentials can be used to access resources if a credential is compromised without your knowledge. Cloud service providers may track access key age to help audit and identify keys that may need to be rotated.(Citation: AWS - IAM Console Best Practices)
M1026	Privileged Account Management	Review privileged cloud account permission levels routinely to look for those that could allow an adversary to gain wide access, such as Global Administrator and Privileged Role Administrator in Azure AD.(Citation: TechNet Credential Theft)(Citation: TechNet Least Privilege) (Citation: Microsoft Azure security baseline for Azure Active Directory) These reviews should also check if new privileged cloud accounts have been created that were not authorized. For example, in Azure AD environments configure alerts to notify when accounts have gone many days without using privileged roles, as these roles may be able to be removed.(Citation: Microsoft Security Alerts for Azure AD Roles) Consider using temporary, just-in-time (JIT) privileged access to Azure AD resources rather than permanently assigning privileged roles. (Citation: Microsoft Azure security baseline for Azure Active Directory)
M1018	User Account Management	Periodically review user accounts and remove those that are inactive or unnecessary. Limit the ability for user accounts to create additional accounts.
M1017	User Training	Applications may send push notifications to verify a login as a form of multi-factor authentication (MFA). Train users to only accept valid push notifications and to report suspicious push notifications.

Image 5: Recent detections analysis in security analytics dashboard

- This analysis contains the following-
  - Overview tab:
    - Description- Text field summarizing what the rule is about (empty in this case).
    - Time- Exact timestamp of when the rule was triggered.
    - Severity- Indicates the impact level of the rule triggered - here, it is Critical.
    - Insights section-
      - Who: Username involved in the triggered rule.
      - Where: Device or host where the event occurred.
      - Client IP: IP address of the client involved in the incident.
      - MITRE ATT&CK: Mapping to known adversarial tactics/techniques.
      - Tags: Labels giving contextual information
    - Mitigation section-
      - Mitigation: Recommended or recorded response actions.
  - Timeline tab: Inserts the detection in a chain of consecutive events providing a larger picture of all the occurring activities in a context that fits.

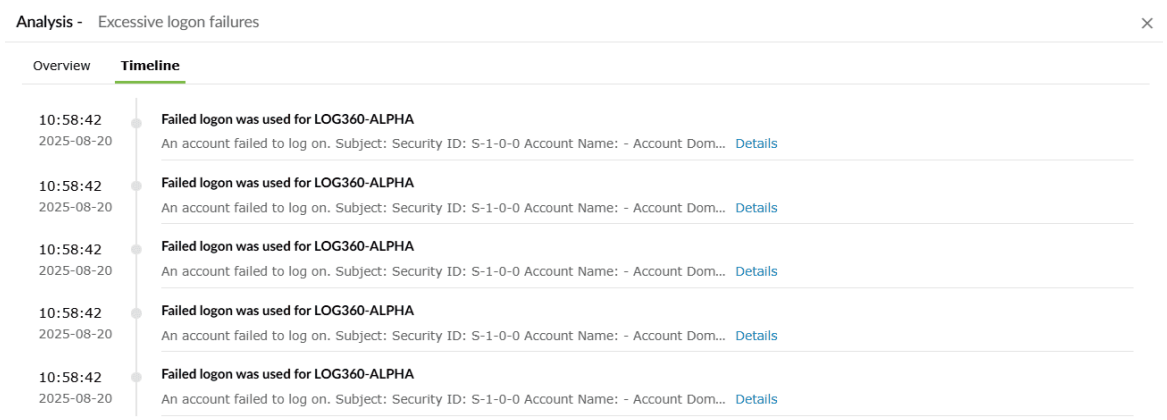


Image 6: Recent detections analysis in security analytics dashboard

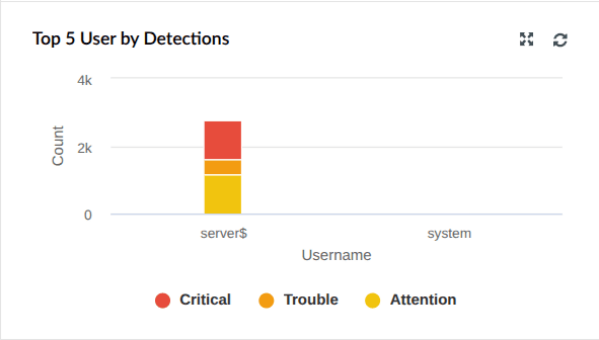
- Clicking on the Details button prompts open a pane containing ALL details of that particular event associated with that rule detection. Below is the list of details provided:
  - Risk Level
  - Message
  - Source
  - Remote DeviceIp
  - Logon Type
  - Process Id
  - OS Category
  - Host Type
  - LogonId
  - Task Category
  - Member Group SID
  - Authentication Package Name
  - Event Name
  - Device
  - GUID
  - Logon Process
  - Severity
  - Key Length
  - Event ID
  - ACTION_TAG
  - Type
  - Caller LogonID
  - Username

- Username
- Security Id
- Source Port Number
- Domain

4. Top 5 Users by Detections

This chart highlights in a statistical view the top five user accounts with the highest detection counts, broken down by severity.

A. Concise widget view



Details displayed

- Username: Displays the usernames of the accounts of the top 5 users on the x-axis.
- Count: Total number of detections per user on the y-axis.
- Severity breakdown: Stacked bars visualize the proportion of the three severity levels of the alerts per user.

Role in Security Analytics

- Identifies compromised accounts or potential insider threats.
- Helps prioritize account audits for high-risk users.
- Provides a behavioral snapshot of every suspicious user's activity patterns.

B. Expanded widget view

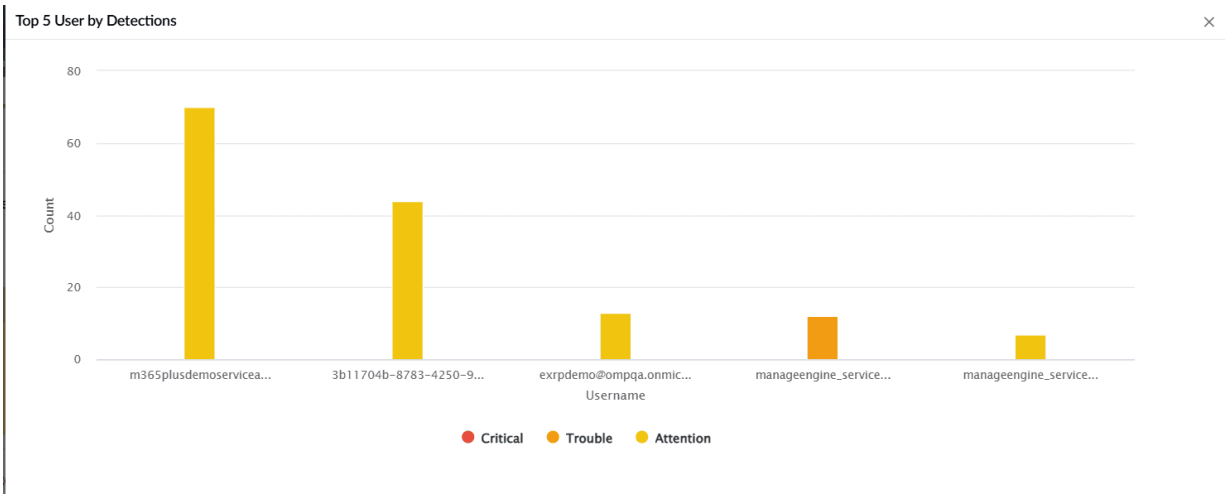


Image 7: Top 5 users by detections widget in security analytics dashboard

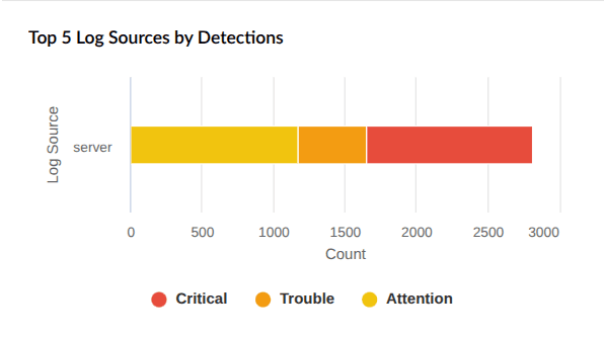
Image 7: Top 5 users by detections widget in security analytics dashboard

The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.

5. Top 5 Log Sources by Detections

This chart shows the devices or systems contributing the highest in order to the total detection counts.

A. Concise widget view



Details displayed

- Log Source: Specifies the origin device or system on the y-axis.
- Count: Number of detections per log source on the x-axis.
- Severity split: Bars of the graph, color coded with the three severity levels indicate which devices are generating alerts of varied severity.

Role in Security Analytics:

- Highlights the most vulnerable or frequently attacked devices.
- Helps you focus on device hardening efforts on potential high-risk systems.
- Provides insights into log source health and configurations.

B. Expanded widget view

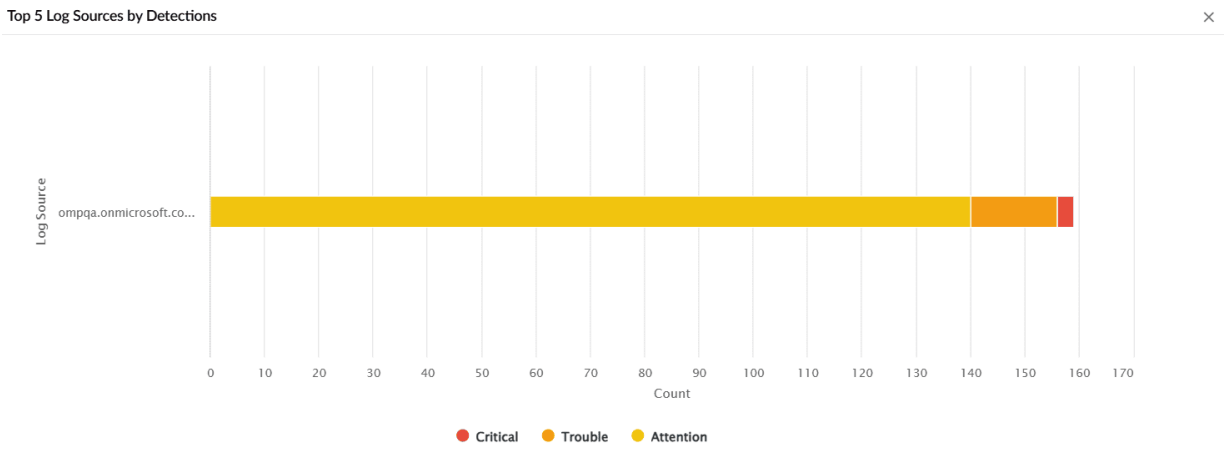


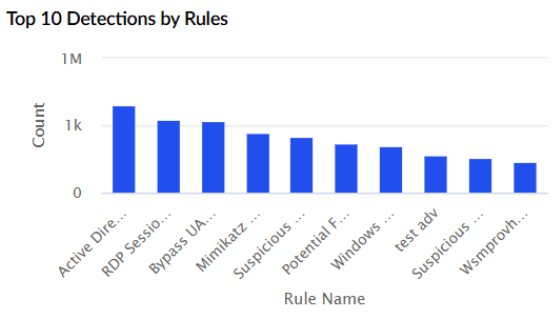
Image 8: Top 5 log sources by detections widget in security analytics dashboard

The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.

6. Top 10 Detections by Rules

This bar chart displayed here ranks the top 10 detection rules based on the frequency of detected triggers.

A. Concise widget view



Details displayed

- Rule Name: Includes rules such as Excessive file access, Repeated operations, or Brute force on the x-axis
- Count: Displays how many times each rule was triggered on the y-axis.

Role in Security Analytics

- Identifies recurring threats or common triggers.
- Assists in fine-tuning detection rules to reduce false positives.
- Provides data to optimize threat hunting and response strategies.

B. Expanded widget view

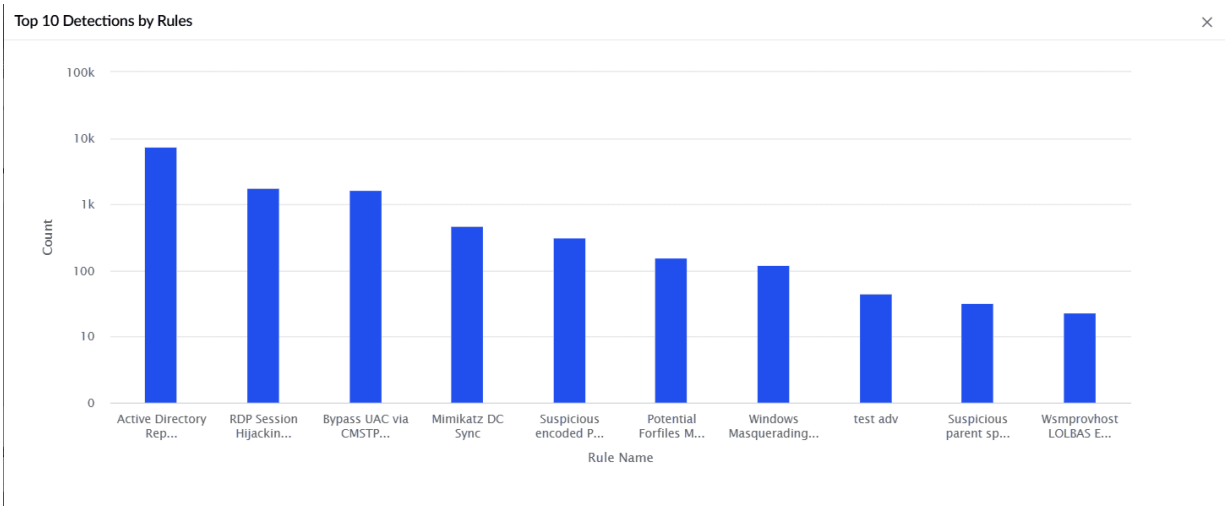


Image 9: Top 10 detections by rules widget in security analytics dashboard

- The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of

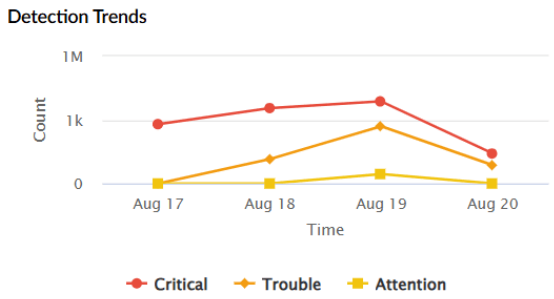
the rules spread across the severity levels.

- Clicking on any data bar representing detection count slides open the data table for that particular rule severity level, similar to the expanded view of the four components.

7. Detection Trends

The Detection Trends chart tracks detection activity over time, segmented by severity.

A. Concise widget view



Details displayed

- Time: Displays yearly or monthly detection counts spread across the x-axis.
- Count: Displays the total count of detections across time periods on the y-axis.
- Severity trend lines: Separate lines of the graph track the detections assorted based on the three severity levels.

Role in Security Analytics

- Helps spot anomalies or sudden spikes in activity.
- Provides historical context for incident analysis.
- Aids in capacity and resource planning for security operations.

B. Expanded widget view

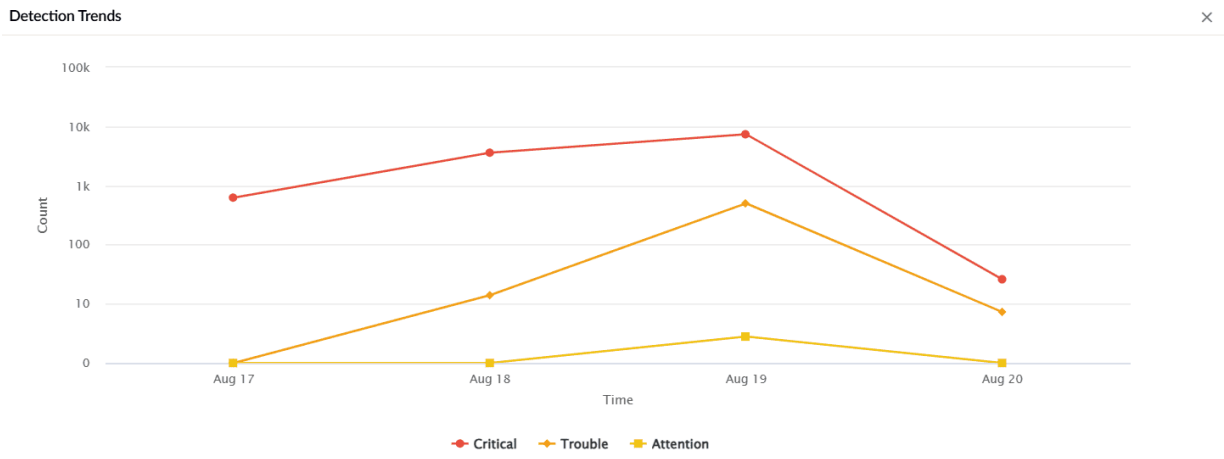


Image 10: Detections trends widget in security analytics dashboard

The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.

Actions available in the Security Analytics dashboard

There are two mainly available actions in this tab:

1. Custom time range: For data analysis in the form of widgets.
2. Manage Rules: To view the rule management module. It acts as the backbone of the security analytics capability of Log360 by creating a highly effective framework that is followed by the analysis-identification-detection cycle by the SIEM (Security Information and Event Management) solution that assists you in safeguarding your enterprise network and enforcement of active threat detection and proactive threat response mechanisms.

Custom time range

1. Navigate to the Security Analytics dashboard via the Security tab and click anywhere in the highlighted area as shown below.

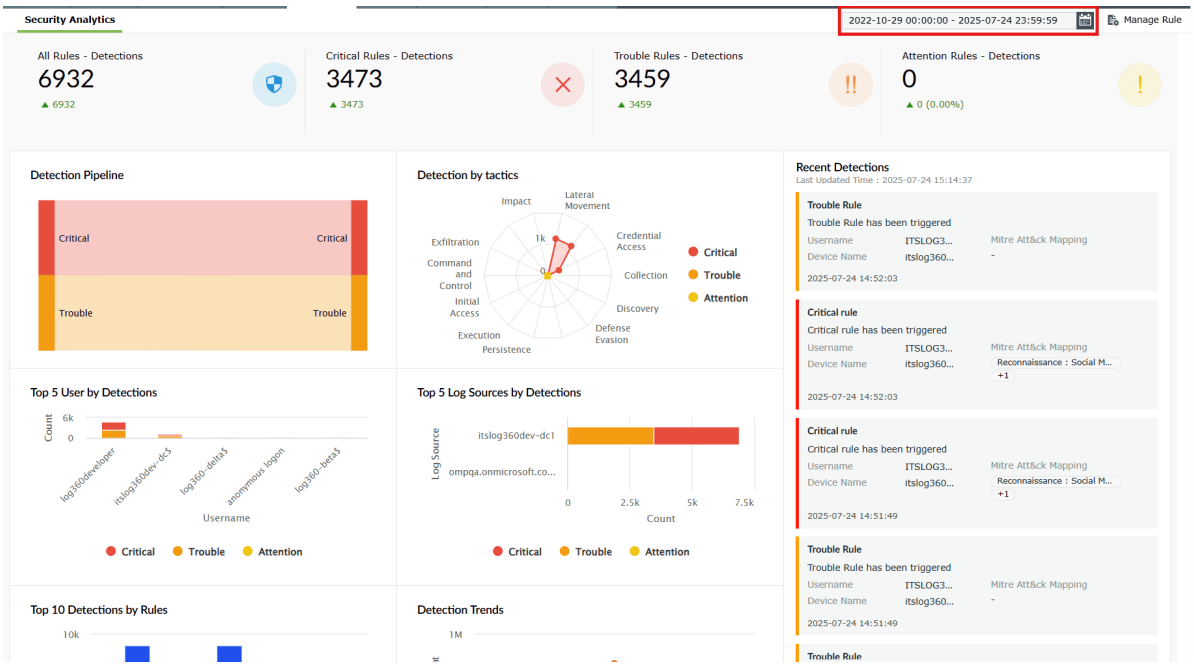
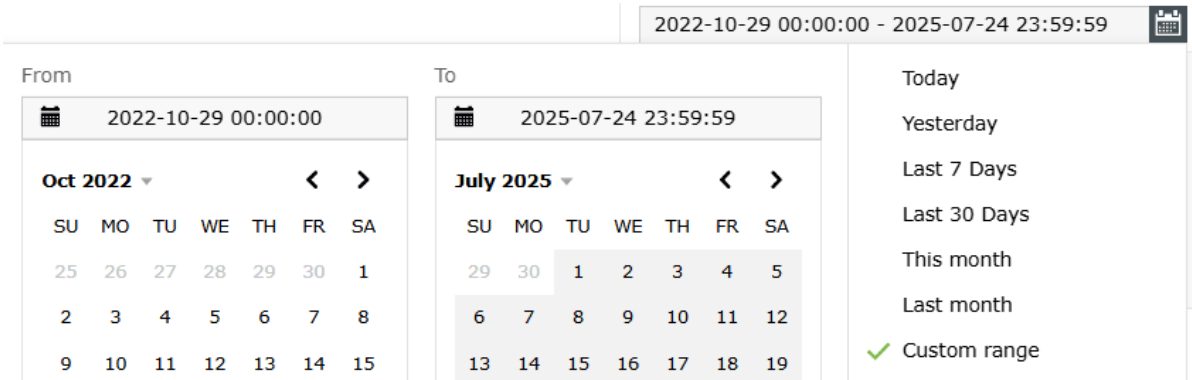
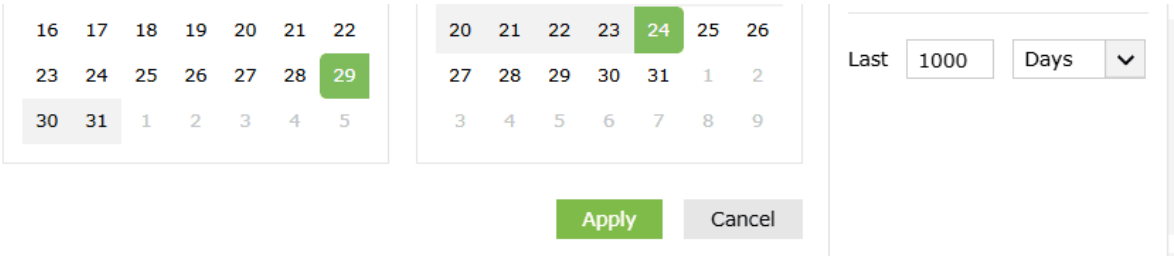


Image 11: Configuring detections time period in security analytics dashboard

2. The action prompts open the calendar view along with predefined time ranges for you to choose from.





3. You can:
   - Select the start date and end date for your desired time range.
   - Click on any of the predefined time ranges available that suits your requirements.
   - Click on Custom range and then proceed to enter a number in the box provided below that will represent the past number of days worth of data you wish to view.
4. Click on Apply.
5. Upon completion of action, you will see that the Security Analytics dashboard is instantly updated according to the time range you have selected.

Manage Rules

1. Navigate to the Security Analytics dashboard via the Security tab and click on the Manage Rule option as highlighted in the below image.

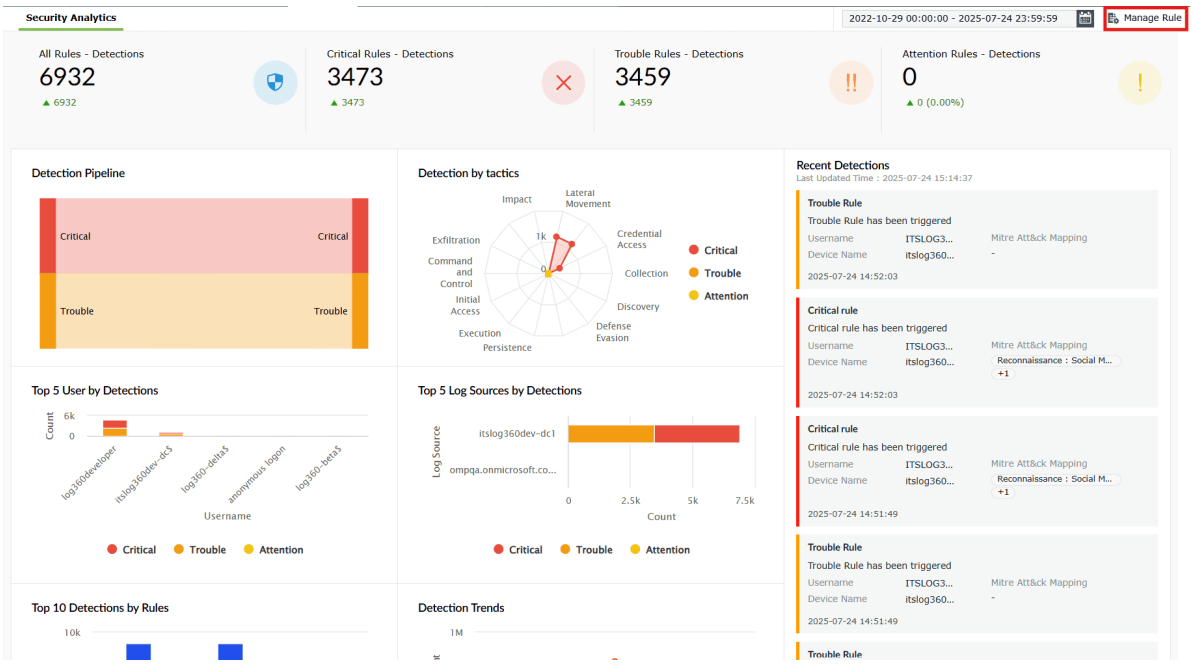
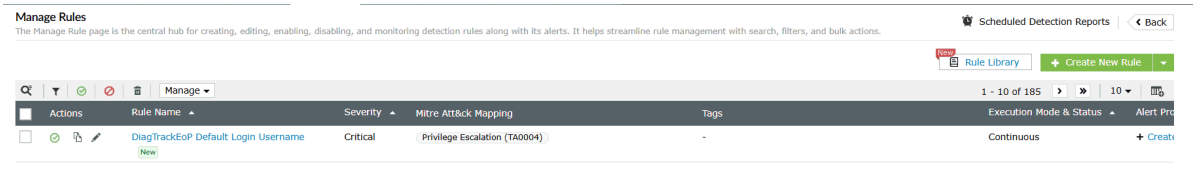


Image 12: Manage rules button in the security tab

2. You will be taken to the Manage Rules module, which is the central hub for managing rules, allowing you to configure rules efficiently.



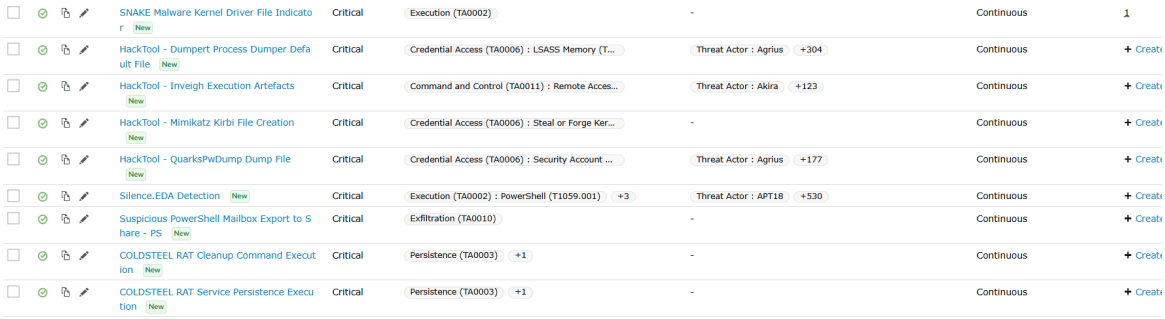


Image 13: Manage rules module via the security tab

Click here to learn more about rule management and how to configure rules.

Dashboard customization

The Security Analytics tab in itself cannot be customized via the Security tab. Instead, the same sub-tab is provided in the product as the Detection Overview sub-tab in the Dashboard tab.

The Detection Overview dashboard includes everything that is provided in the Security Analytics tab while also allowing you to customize the dashboard and the widgets in it.

To learn how to customize your Detection Overview dashboard in the main Dashboard tab, refer to the Dashboard View help document.

Read also

This page detailed all seven security dashboard widgets, their compact and expanded views, and how they help you monitor threats, analyze adversary tactics, and identify high-risk users, rules, and devices.

- Security dashboard overview

10.1.2.1. Rule management overview

Last updated on: September 12, 2025

In this page

Overview

Rule Management

Why is Rule Management important for threat detection?

Predefined Rules

Types of Rules

How does rule management logic guide anomaly detection?

How to access rules?

Use Cases

Overview

This page covers why and how rule management plays a crucial role in anomaly detection within your network. By managing rules you effectively optimize Log360's UEBA engine to monitor specific behaviors you want to watch for. This helps in narrowing down the scope and saving time and resources by focusing on relevant events and thus receiving alerts as per the conditions defined. When the defined conditions are met, the ML model detects and flags the behavior as anomalous.

Rule Management

- Functionality: The Rule Management capability is a centralized platform designed to streamline the management of all rule types, including ATA (Advanced Threat Analytics), MITRE, Correlation, and UEBA (User and Entity Behavior Analytics). This unified interface eliminates the need for navigating disparate tools, providing a seamless and efficient experience for users managing security rules.
- Rule management allows you to define the conditions under which a specific user or entity will be flagged as anomalous. The Machine Learning model first establishes a baseline behavior of all the users and entities in your network during the training phase in order to be able to differentiate the deviation from the usual behavior. Rule configuration provides the foundation for the ML model to spot these deviations, thus providing a framework for the anomaly detection logic.

Why is Rule Management important for threat detection?

Probing into every event log out of the hundreds that are collected each day is a tedious and near-impossible task. Rules help narrow down the scope for threat detection by targeting specific or widely known risky and unusual behaviors in your environment for threats like insider attacks, brute-force attacks, data exfiltration, etc.

Rule configuration will add an advantage of being able to scan such threats from every angle, like monitoring the usual login times, performing an unusually high number of actions in a time range, or specific files being modified or accessed, and so on.
In short, rules will allow your security admins to specify what to watch for in logs to automatically raise an alert when those specific events occur.

Predefined Rules

The product offers a set of built-in rules that will help you get started with threat detection and security analysis of your enterprise network. These pre-defined rules are tailored to meet all the criteria of some of the most common threat patterns like privilege escalations, malware indicators, etc.
From a user's point of view, these rules not only save your time but also serve as templates for you to clone and customize as per your organization's growing needs via custom rule creation. Fine-tune the anomaly detection scope by optimizing event filter criteria, severity, specific actions to be targeted, etc.
Pre-defined rules are installed in an enabled state by default. For On-Premise (OP) deployments, there are no restrictions. However, for On-Demand (OD) deployments, if the license count is exceeded, the rules will be installed in a disabled state.Rule enablement on installation:

- High-severity rules are enabled by default after installation, provided a valid license is available.
- Rules that require high computational resources will also be enabled automatically.
- Standard rules are enabled by default.

Types of Rules

There are three categories of rules provided:

- Standard Rules
  Standard rules are simple rules which serve the purpose of filtering and identifying specific events based on the action chosen in the configuration.
- Anomaly Rules
  These rules are single-event/action based rules that leverage the anomaly model. They trigger when the specified event or action exceeds the configured limit or violates the conditions defined in the anomaly model.
- Advanced Rules
  These are rules whose scope of anomaly detection is broader as they are configured with a set of sequential events/actions that serve as the criteria. These rules are designed to detect complex, multi-step attack patterns.

How does rule management logic guide anomaly detection?

The UEBA engine uses rule management logic to scan for anomalies in two ways:

- Real-time, as soon as event logs are collected. For this, Real-time anomaly detection (RT) must be enabled.
- Scheduled logs, by default, are scheduled for intervals of one hour each. Therefore, all the logs in the span of the past hour will be forwarded for anomaly detection.

- Intelligent mode: When an anomaly action is selected, the rule's default execution mode is set to Intelligent.

1. Event ingestion: Event logs are collected by the log collector in real-time (or in scheduled batches.)
2. Event queuing: The incoming events are parsed and then queued for analysis.
3. Rule evaluation: Each queued event is analyzed by the ML model against the currently active set of rules. Anomaly rules test the events the anomaly models configured in the rules, while Advanced rules are inclusive of multiple actions or criteria or; sequences linked to multiple actions.
4. Anomaly detection and risk scoring: The ML model uses the behavioral baselines it gathered during its training phase in order to detect anomalies, if any. Any match of events with the active rules contributes to the risk score attribution to the users and entities associated with those events.

In this way, rule management ensures that relevant anomalies are triggered as soon as such events are logged and the configured behavioral patterns and thresholds are matched

How to configure rules?

To configure the rules, follow the below steps:

1. In the product console, navigate to the Security tab. You will be taken to the Security Analytics Overview sub-tab.

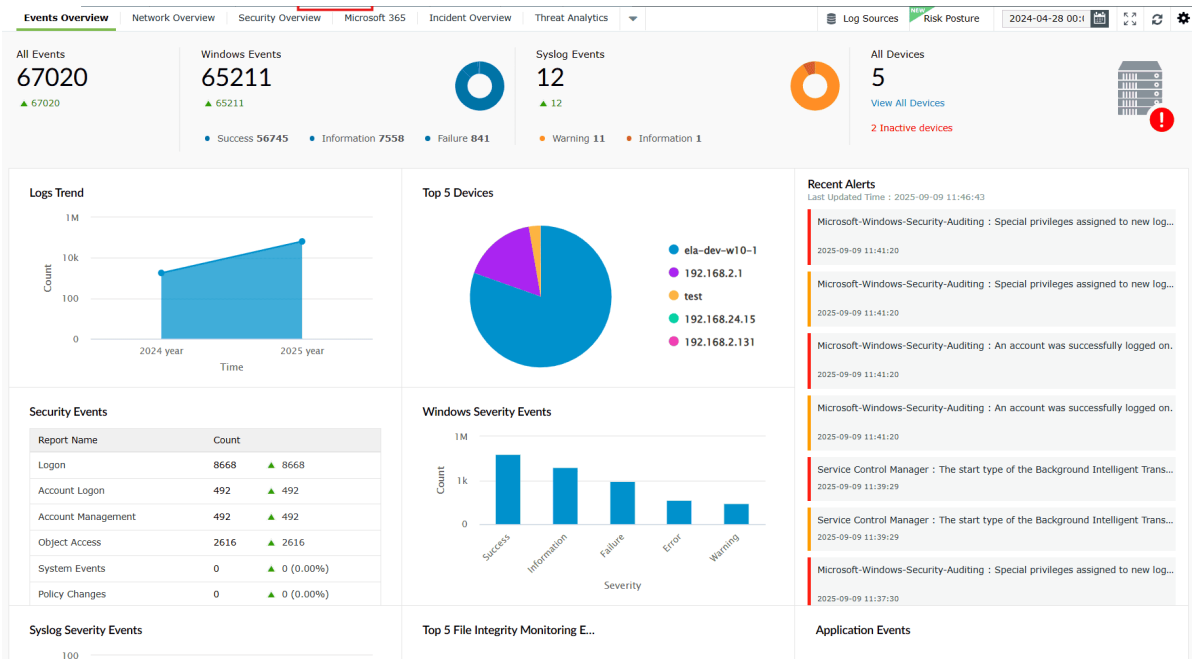
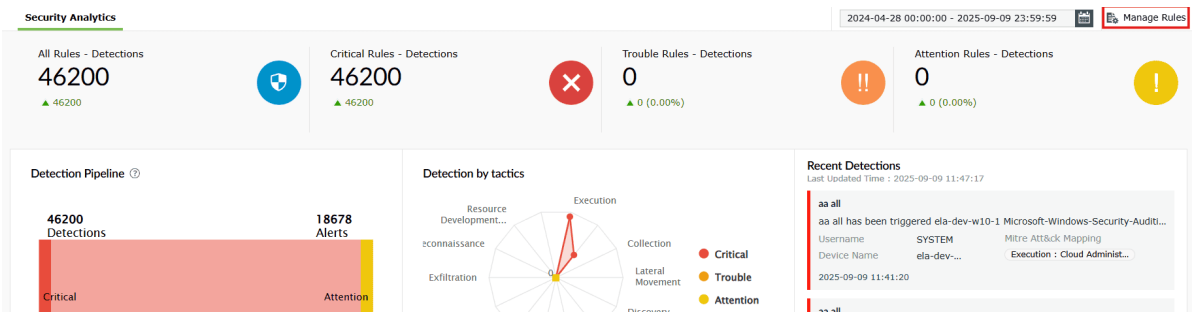


Image 1: Security tab in dashboard

2. Click on the Manage Rule button on the extreme right of the sub-tabs ribbon.



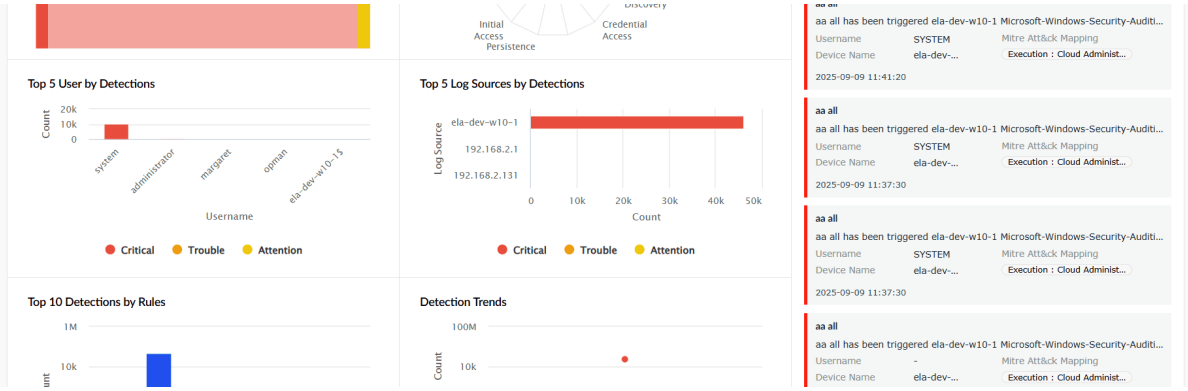


Image 2: Manage rules in security dashboard

3. You will then be taken to the Manage Rules module. This is the centralized hub for managing rules, rule creation, editing, etc.

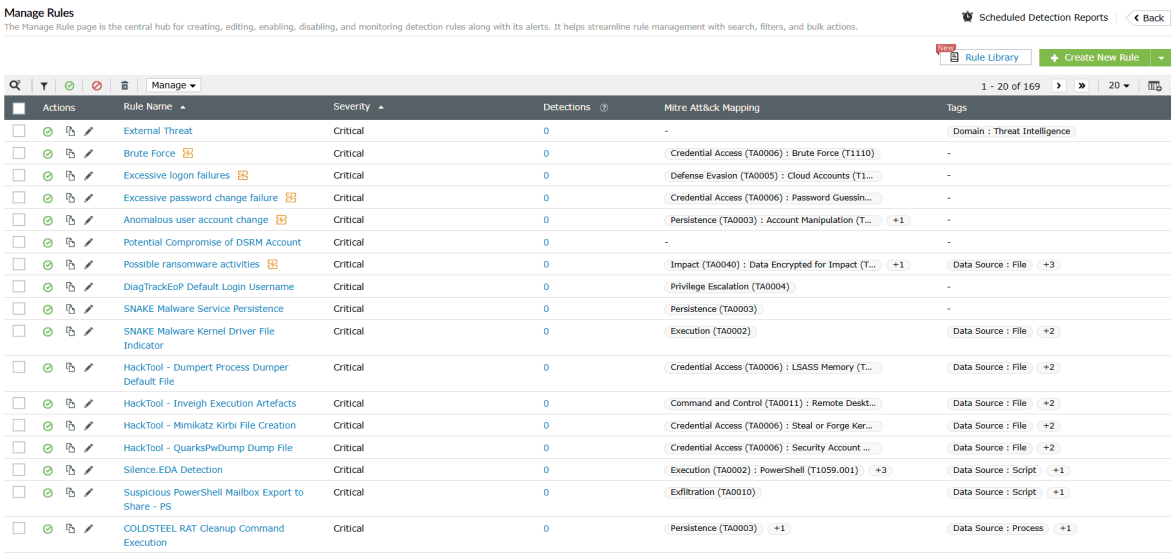


Image 3: Manage rules module via the security dashboard

Use Cases

Template-based onboarding of rule coverage for new teams

Use case

A new business unit with similar operational workflows is onboarded into the organization's cloud environment.

With effective rule management

Administrators can clone pre-defined rules like "Unusual login location" or "Failed logons", customize them for the new users and entities, and activate those rules. Once active, the rules start monitoring activity based on the configured logic, helping speed up deployment while maintaining consistent monitoring standards across the organization.

Detecting account takeover attempts - Privilege Escalation

Use case

Use case

A user with read-only access is now suddenly involved in admin-level activities like modifying user permissions or security settings.

With effective rule management

Pre-defined rule associated with privilege escalation can be activated and tailored (if needed) with filters like device type, or role-based user group to monitor such spikes in privilege use which could be potential Insider Threat. The ML model flags such activities against the user's usual behavioral baselines, enabling a speedy remediation.

Focused Anomaly detection for critical roles or systems

Use case

The finance department is the integral aspect of an organization, demanding attention and scrutiny.

For example: Access to payroll files during non-business hours.

Scenario A- Anomaly rules: A sales user attempts to access the payroll files.

Scenario B- Advanced rules: A sales user attempts to access the payroll files, that too during non-business hours.

With effective rule management

Security admins can configure rules to be role-specific and monitor abnormal activity specifically focusing on the finance department.

The ML engine formulates and uses the baseline behavior per role to involve contextual accuracy in anomaly detection.

Read also

This document explained how rule management helps optimize anomaly detection, from using predefined rules to configuring advanced rules for complex attack patterns.

- Understanding rules
- Creating custom rules
- Query grammar
- Managing rules
- Scheduled detection reports

10.1.2.2. Understanding rules

Last updated on: September 12, 2025

In this page

Overview

Standard Rules

Anomaly Rules

Advanced Rules

Actions - Log Types supported

Other fields

Execution mode: Differences in operator modes

Rule specific use cases

Overview

This page explains the three types of rules used in security analytics: standard rules for basic event filtering, anomaly rules for detecting unusual single-event behavior, and advanced rules for identifying complex attack sequences. Each rule type comes with configuration fields, filters, thresholds, and anomaly models to provide flexible monitoring and precise threat detection.

Standard Rules

Standard rules are basic rules that will merely identify and filter specific events from the collected logs depending on the selected action. In this simple configuration, the desired action is chosen with the optional filters or thresholds. Standard rules do not involve anomaly models or behavioral baselining. They are simply just to view and monitor log data that matched the exact conditions, so that you can focus on other events of interest.

Understanding the rule configuration fields

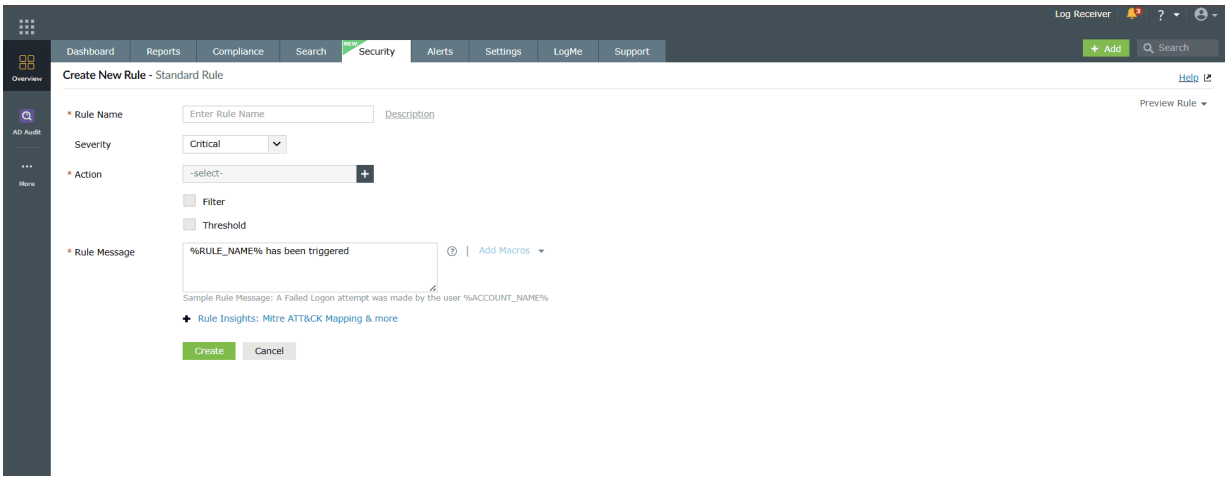
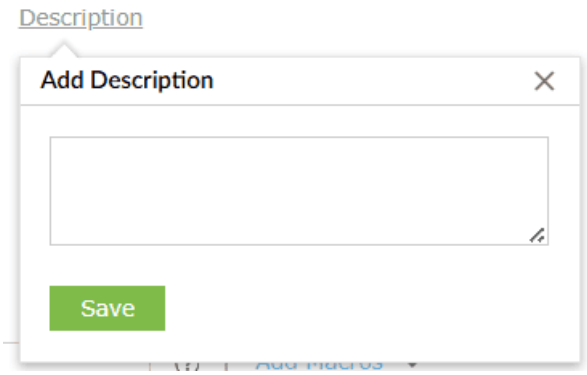
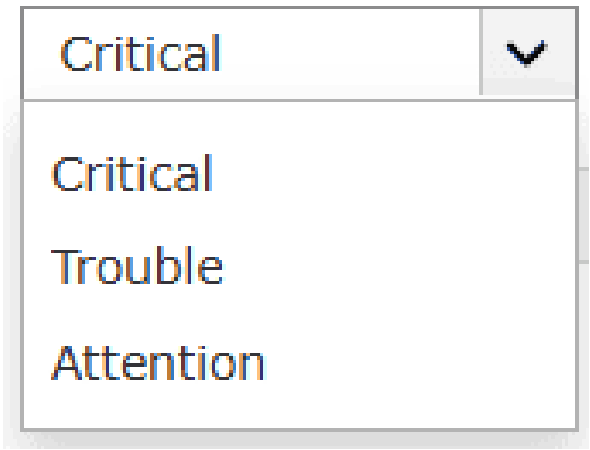


Image 1: Creating standard rule

- Rule Name: Give a unique name for the rule for identification.
- Description (optional): A brief explanation about the rule and its purpose.



- Severity: Choose a severity level you wish to associate this rule with. For instance, trouble level criteria indicate a moderate level of severity. The three levels of severity are:
  - Critical
  - Trouble
  - Attention



- Action: Select the log event type you want the rule to monitor. Read further for a detailed list of Log Types supported by all the three rule types associated with 600+ actions available.
  If you wish to Create Custom Action, refer to the Creating Custom rules help document.
- Filter (optional): Add one or more criteria for the log events to be filtered based upon. This will narrow down log events for rule application.

NOTE:

A maximum of only 5 filters can be set for any rule.

- Threshold (optional):
  - Define a distinct or count based event occurrence limit for repetition over a period of time. Upon exceeding the limit, the rule is triggered.
  - You can also configure Sum and Average (Avg) thresholds in addition to count-based thresholds.
  - Threshold conditions can be applied based on a group-by of specific fields, allowing more granular detection and control.
- Rule Message: Include the text you wish for the alert message to display when the rule is triggered.



Anomaly Rules

Anomaly rules in the rules category of security analytics are configurations specific to anomaly detection relevant to only a single action from the rule criteria. Each anomaly rule applies to one selected event type- the action. For example, "Failed File Accesses", "Account Deleted", "Group Deleted".

Understanding the rule configuration fields

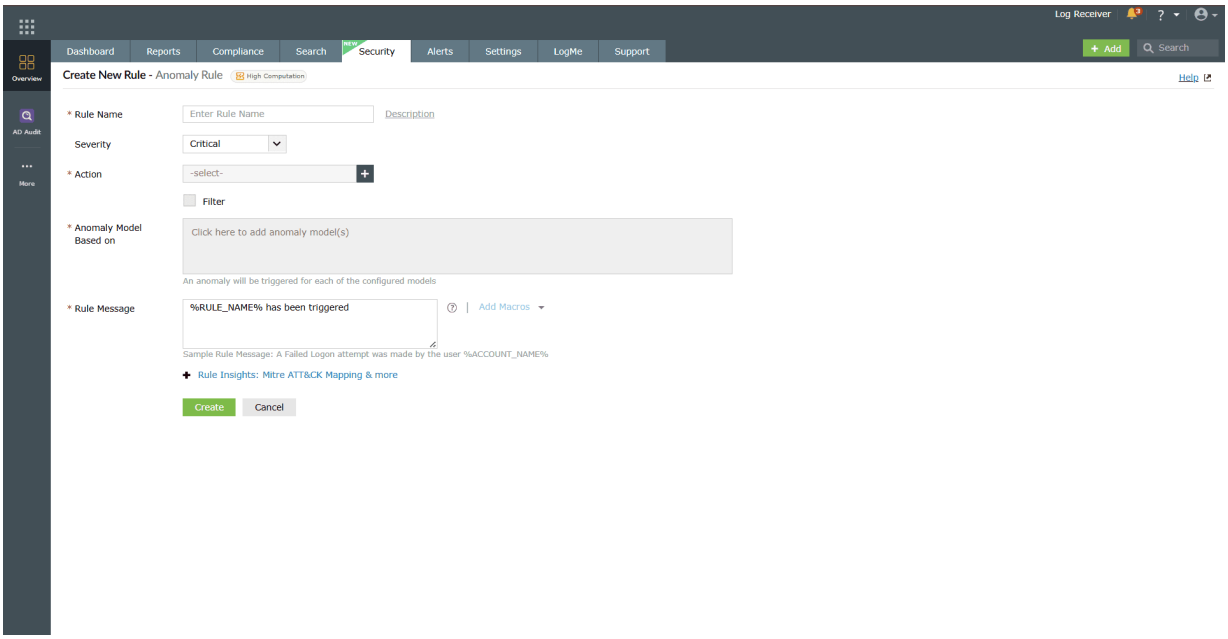
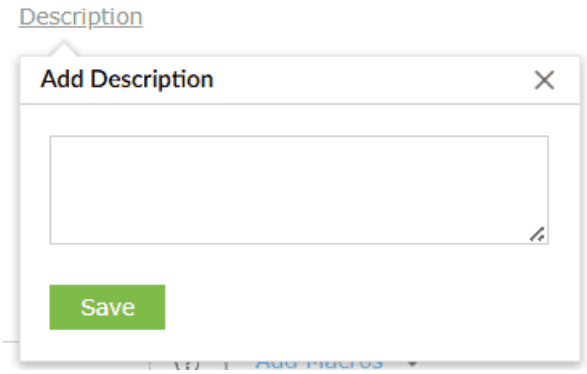
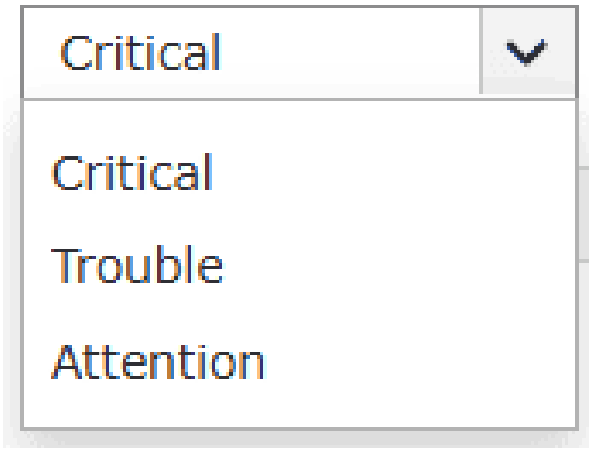


Image 2: Creating anomaly rule

- Rule Name: Give a unique name for the rule for identification.
- Description (optional): A brief explanation about the rule and its purpose.



- Severity: Choose a severity level you wish to associate this rule with. For instance, trouble level criteria indicate a moderate level of severity. The three levels of severity are:
  - Critical
  - Trouble
  - Attention

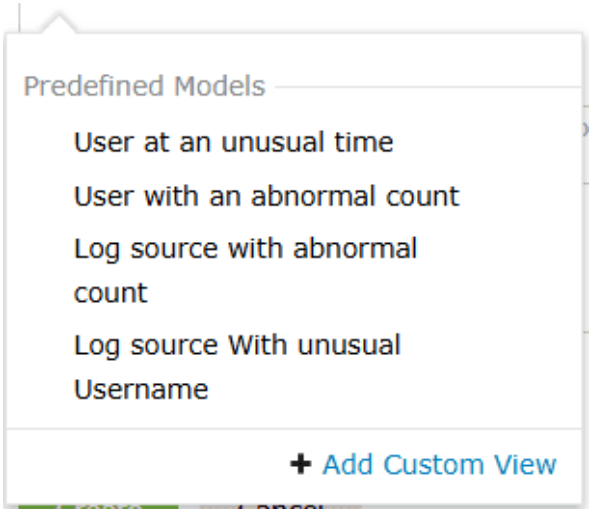


- Action: Select the log event type you want the rule to monitor. Read further for a detailed list of Log Types supported by all the three rule types associated with 600+ actions available in Log360.
  If you wish to Create Custom Action refer to the Creating custom rules help document.

> NOTE:
>
> Only 1 action may be selected per anomaly rule.

- Filter (optional): Add one or more criteria for the log events to be filtered based upon. This will narrow down log events for rule application.

- Anomaly Model Based on: Choose the anomaly model(s) to define how deviations from normal behavior will be detected. An anomaly will be triggered for each of the configured models and two behavioral constructors - On Host, By User. There are five primary anomaly models:
  - User at an unusual time: To detect user activity that occurs outside of the user's typical login/access hours.
  - User with an abnormal count: To detect users that perform an action more or less frequently than their usual behavior.
  - Log source at an unusual time: To detect log sources that generate events outside of their usual operating hours or expected activity windows.
  - Log source with abnormal count: To detect the log sources that generate an unusually high or low volume of events.
  - Log source with unusual username: To detect the log sources associated by a certain username, which is not the one the log source is typically associated with.



NOTE:

A maximum of only 5 anomaly models can be set for a rule.

- Rule Message: Include the text you wish for the alert message to display when the rule is triggered.



Advanced Rules

Advanced Rules

Unlike Anomaly rules that primarily focus only on a single action for anomaly detection, Advanced rules help in detection of complex, multi-step incidents by correlating sequences of events corresponding to multiple actions. Additionally, by linking actions in sequence, you can spot attack patterns that span over several event types, for instance, several logon failures followed by a successful login.
The action sequences are defined in order, and the rule will be triggered when the full pattern of actions occurs. Each action can further be fine-tuned by configuring field-based filters to narrow down the events to those meeting all specified conditions.

Understanding the rule configuration fields

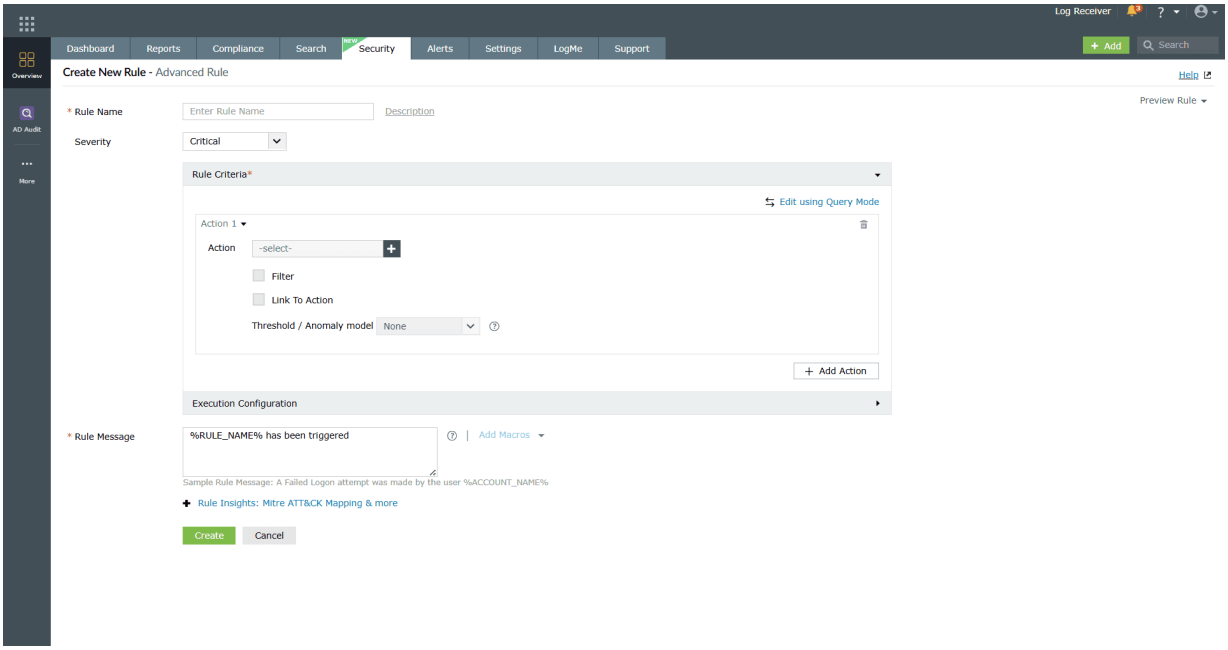
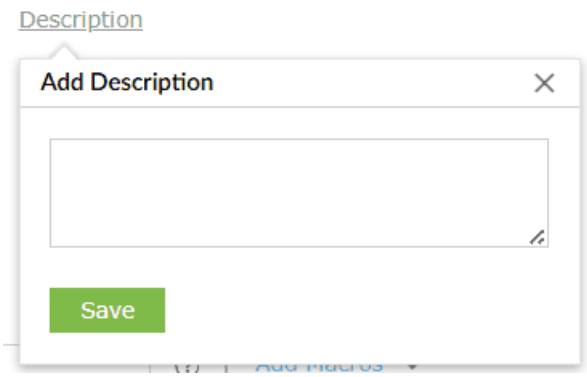


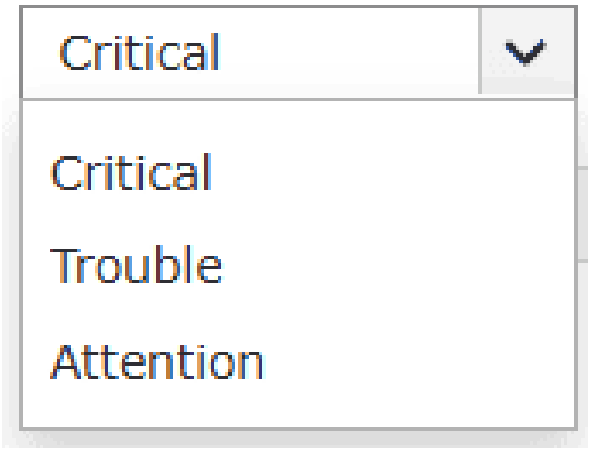
Image 3: Creating advanced rule

- Rule Name: Give a unique name for the rule for identification.
- Description (optional): A brief explanation about the rule and its purpose.



- Severity: Choose a severity level you wish to associate this rule with. For instance, trouble level criteria indicates a moderate level of severity. The three levels of severity are:
  - Critical
  - Trouble

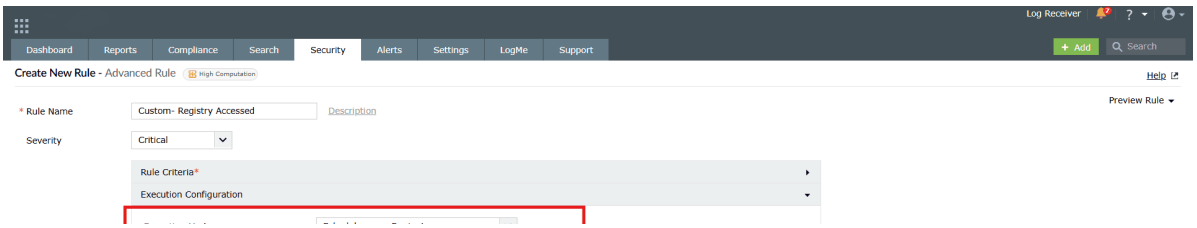
- Trouble
- Attention



- Rule Criteria
- Action: Select the log event type you want the rule to monitor. For Advanced rules, multiple actions can be selected. Read further for a detailed list of Log Types supported by all the three rule types associated with 600+ actions available in Log360.
  If you wish to Create Custom Action refer to the Creating custom rules help document
- Filter (optional): Add one or more criteria for the log events to be filtered based upon. This will narrow down log events for rule application.
- Link To Action: In the case where you have chosen multiple actions, you can link those actions to one another so that events involving those actions can be correlated and monitored for suspicious activity.
- Threshold/Anomaly model:
  - Threshold (optional): Define a distinct or count based event occurrence limit for repetition over a period of time. Upon exceeding the limit, the rule is triggered.
  - Anomaly Model: Choose the anomaly model(s) to define how deviations from normal behavior will be detected. An anomaly will be triggered for each of the configured models.

> NOTE:
>
> Either Threshold or Anomaly Model configuration can only be selected, but not both, as they cannot function together. This limitation applies to the entire rule, with only one option allowed across all actions.

- Execution configuration: The Execution configuration option can be used in order to schedule a rule as per the requirement. This option is available only for the advanced rules.



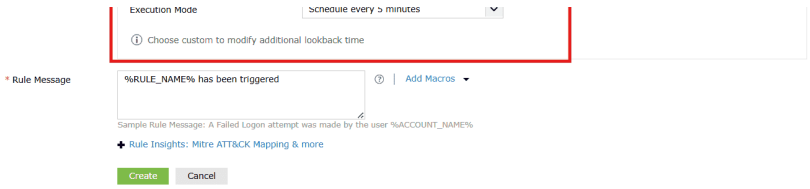
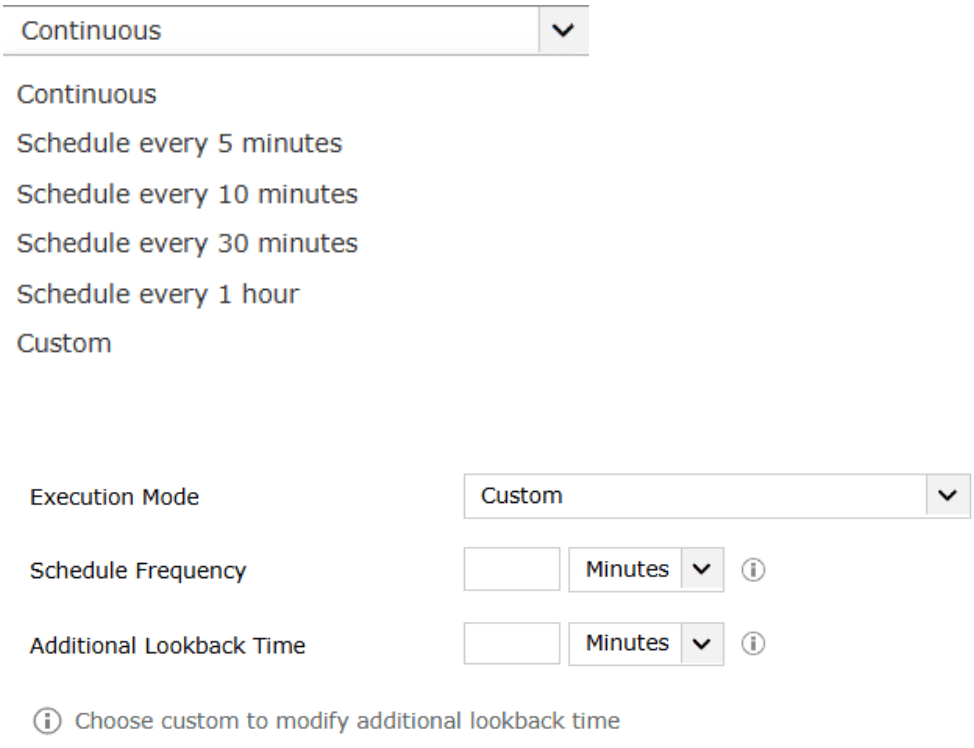


Image 4: Configuring the execution mode

This setting includes Continuous and predefined scheduled time ranges like 5 minutes, 10 minutes, 30 minutes, 1 hour along with an additional custom option, where Schedule Frequency and Additional Lookback Time will have to be configured.

> NOTE:
>
> In case an anomaly action is selected for the rule, the execution configuration operates in the intelligent mode, wherein the execution mode will be automatically assigned based on the rule and its criteria. You cannot manually configure the execution configuration.



- Rule Message: Include the text you wish for the alert message to display when the rule is triggered.



Actions - Log Types supported

Below is the list of all Log Types supported by all three rule types associated with 600+ actions available in Log360.

Stormshield Device	HP Device
Topsec Device	FirePower Device
Sangfor Device	ForcePoint Device
Dell Device	H3C Device
CEF Format	pfSense Device
Malwarebytes	SNMP Trap
McAfee	IBM AS/400
Apache Access Logs	Cisco Device
DHCP linux logs	F5 Device
DHCP windows logs	Unix

MySQL Logs	FIM
MSSQL Server Logs	Threat Analytics
Terminal	Darkweb
Printer	vCenter
SAP ERP audit Logs	Hypervisor/ESXi
Oracle	FireEye
Syslog Archive File	Symantec Endpoint Protection
Syslog	Symantec DLP
Windows Archive File	Nessus
DB2 Logs	Qualys
PostgreSQL Logs	OpenVAS
Password Manager Pro	Nmap
ITOM Solution	Nexpose
ADAudit Plus	Trend Micro
ADManager Plus	IIS W3C FTP Logs
ADSelf Service Plus	IIS W3C Web Server Logs
Endpoint Central	IBM Maximo Logs

Service Desk Plus	Syslog Application
Windows	SQL Server
SonicWall Device	Sysmon
Juniper Device	AWS CloudTrail
PaloAlto Device	AWS S3
Fortinet Device	AWS ELB
CheckPoint Device	AWS ALB
Arista Device	AWS NLB
Barracuda Device	Salesforce Event Log
WatchGuard Device	Salesforce Setup Audit Trail
Sophos Device	Microsoft Entra ID
Huawei Device	Exchange Online
Meraki Device	M365 General
NetScreen Device	Sharepoint Online

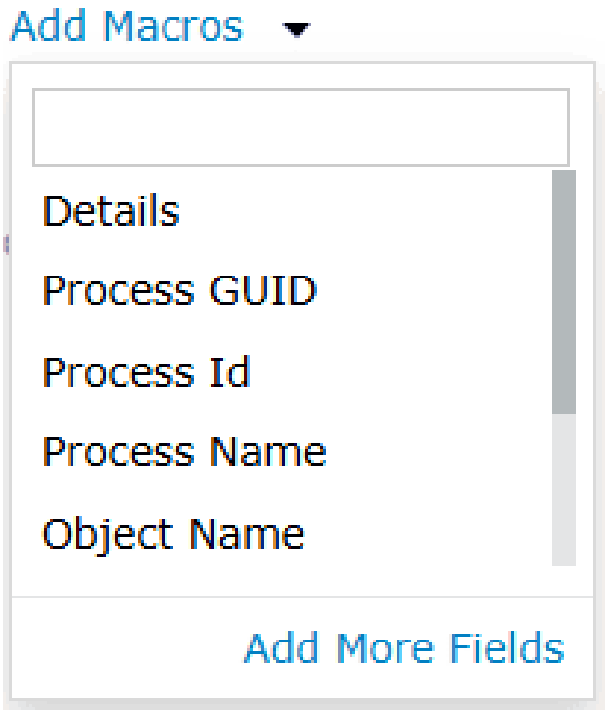
If you wish to choose all the Log Types at once, click on the Select All checkbox.

Other fields

1. Add Macros

The Macros field in all the three rule types contains the list of field names. Upon selecting one for a rule, that particular field name is used for generating the rule message when that rule is triggered. The complete field

options in Macro varies from action to action that has been selected in the rule creation.



2. Rule Insights: MITRE ATT&CK Mapping & more

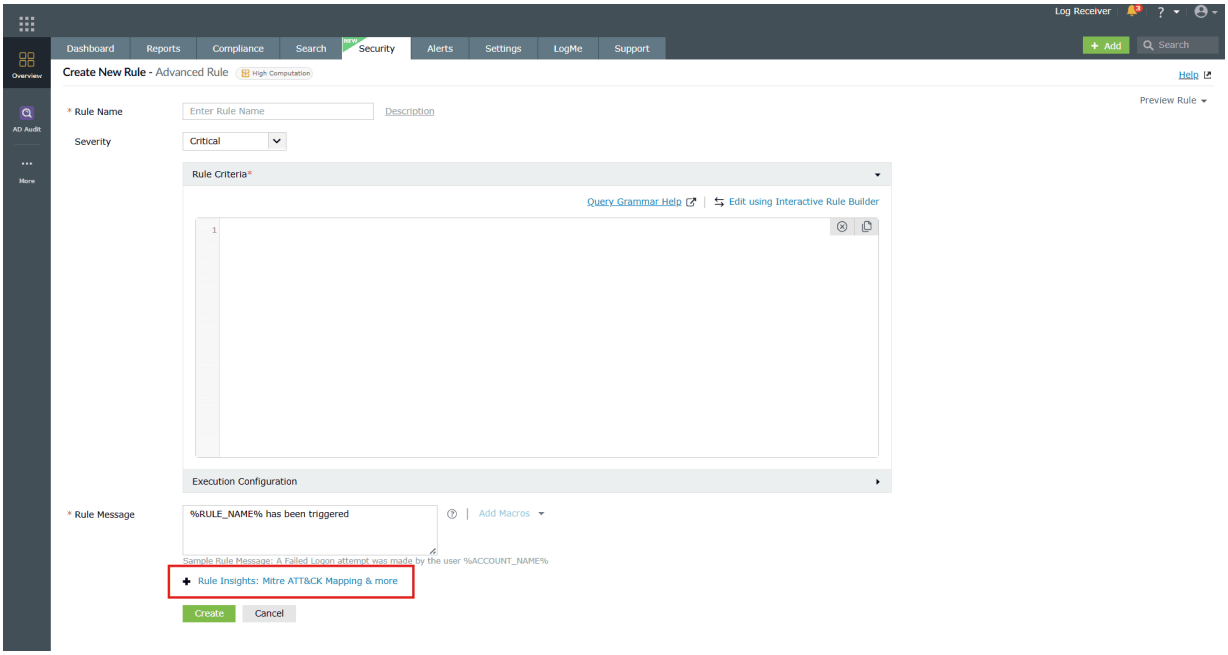
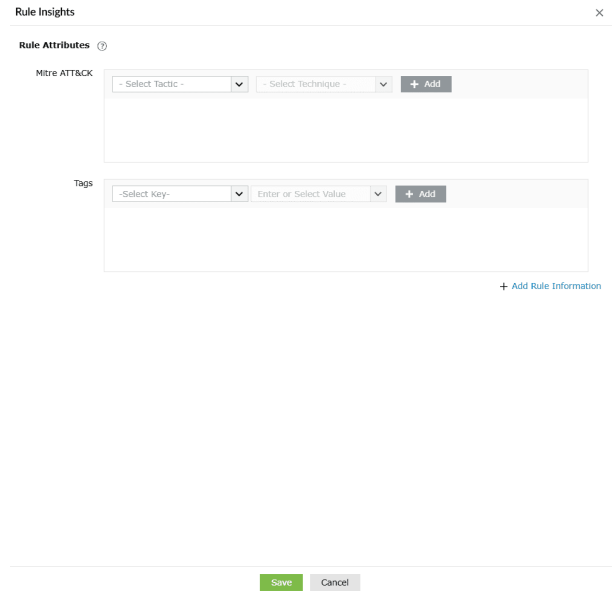


Image 5: Configuring the rule information

This option will help you by providing context for the selected rule by mapping it to any relevant MITRE ATT&CK techniques and tactics. You can then understand the threat behavior this rule is aligning with, in turn, aiding in threat investigation and response effectively. By providing tagging, MITRE mappings, and enriched contextual details for all rule types, the system ensures that you can create robust, organized, and actionable rules tailored to your security needs.

Clicking on it will slide open the fields box for Rule Insights.

Clicking on it will slide open the fields box for Rule Insights.



Rule Attributes

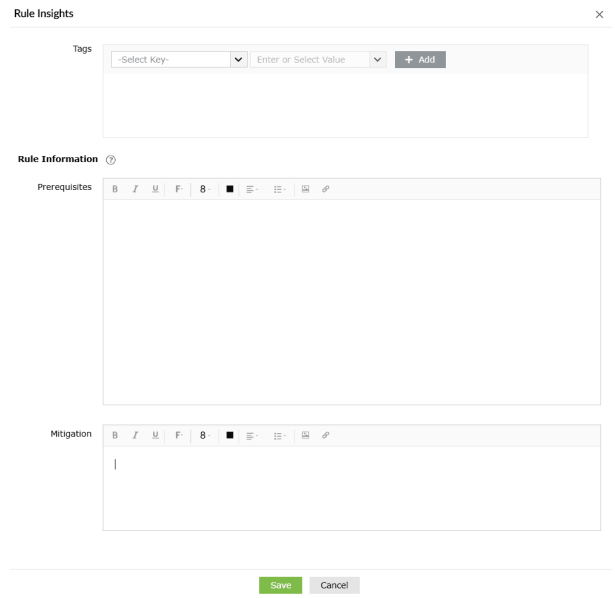
Rule Attributes enable mapping and tagging rules with specific attributes for better organization and actionable insights. They are used to help efficiently manage rules and help with data enrichment.

MITRE ATT&CK

- List of tactics will be given as a dropdown with a search option as well.
- When a tactic is selected, its associated technique will be listed in the technique dropdown.
- If a technique has a sub-technique, it will be listed under that technique.
- If both tactic and technique are selected, an Add option will be given and it will add to the list.
- Cancel icon will delete a row from the added list.

For more information, refer MITRE ATT&CK TTP(S) Framework Integration.

When you click on Add Rule Information, the below appears on the screen.



Rule information

Rule information provides additional contextual information about rule execution and mitigation strategies. It helps technicians make configuration changes and take preventive actions to enhance detections and keep the environment secure.

- Prerequisites
  - Prerequisites define the conditions or requirements that must be in place for a security rule to work effectively. They ensure that the rule can function as intended and produce accurate detections.
  - This will be shown in the Security Rule's reports page when there is no data found for this particular report, and also in the Rule summary drilldown.
- Mitigation
  - Mitigation outlines the steps to respond to or neutralize threats detected by the security rule. It provides actionable guidance to minimize the impact of a security event.

2. Preview Rule

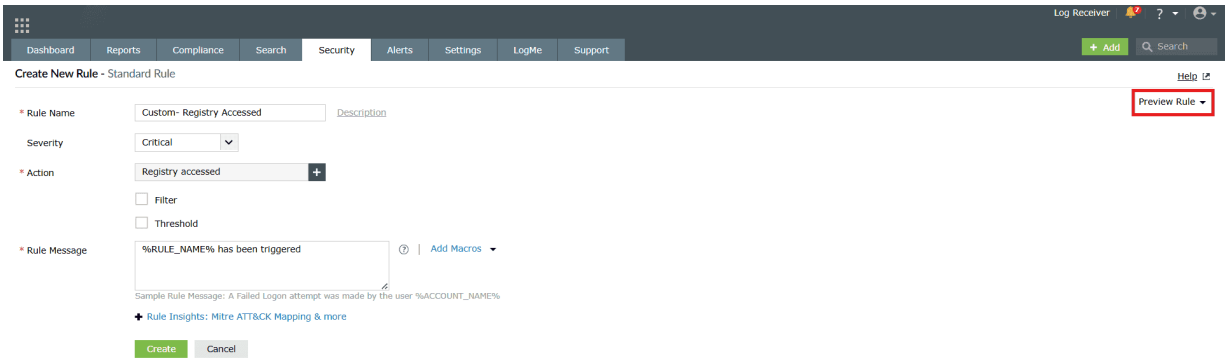


Image 6: Rule preview option of a rule

- The Preview Rule option is visible only after an action is selected in the rule configurations.
- You can also have an option to select a date range via the calendar.
- If additional criteria is added or removed, the preview can be reloaded using the reload preview option.
- Detection reports will only be applicable for the data triggered after the rule is created, but the preview rule will be based on the already collected logs as well.

- In Advanced Rule creation, the overall rule preview will be displayed first, and you can then switch to corresponding action previews, if needed.

Execution mode: Differences in operator modes (Continuous vs. Scheduled)

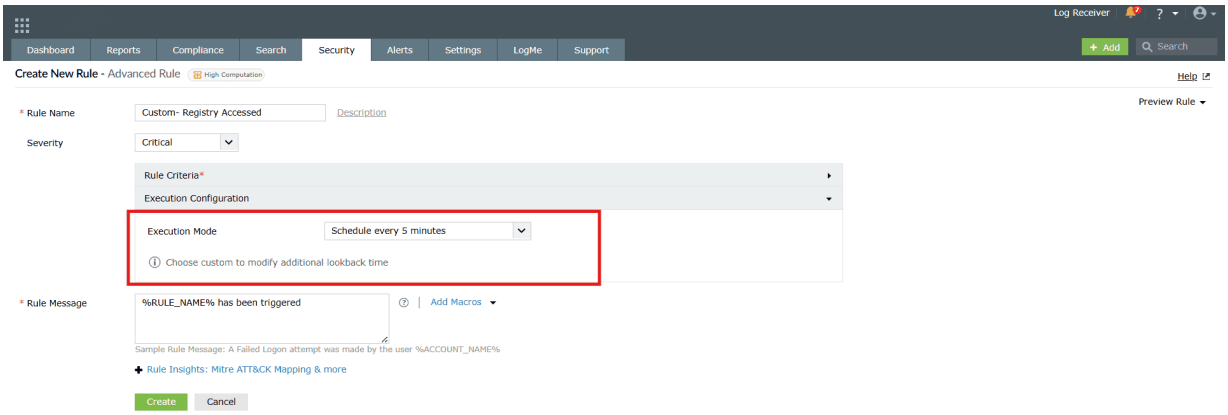


Image 7: Configuring the execution mode

Loopback time

Definition:

Loopback time is an additional period configured to extend the log search window for scheduled rules. For example, if the schedule interval is set to 5 minutes and the loopback time is also configured as 5 minutes, the system analyzes a total of 10 minutes of logs (the current 5 minutes plus the previous 5 minutes).

Purpose:

This ensures that events occurring just before the scheduled interval are also considered during rule evaluation, minimizing the risk of missing detections that span across schedule boundaries.

Disadvantage:

Enabling loopback can lead to data overlap across consecutive schedules. Since the same set of logs may be re-evaluated in multiple intervals, this may result in duplicate detections.

Standard rule (Single action rule)

Condition	Continuous Mode	Scheduled Mode

Condition	Continuous Mode	Scheduled Mode
	• Every log is analyzed.	• If the schedule runs at 11:05, the search query is initiated from 11:00 to 11:05 with that action filter.
Threshold: 10 events within 10 min (Schedule 5 min, LoopBack 0)	• If the log matches the action, data is maintained until the threshold is reached. • Maximum time to maintain un-triggered data is 24 hours. • If 100 events are received within that time, 10 detection reports are triggered.	• Threshold time is 10 min, but in this case, only 5 min logs are retrieved as per schedule execution time. • If the result has 10 or more events, the detection is triggered. • If 100 events are received, all are triggered in a single detection report. • If partial logs are received in-between schedules within the threshold time, those events will not trigger because previous schedule data is not maintained in memory.
Threshold: 10 events within 10 min (Schedule 5 min, LoopBack 5 min)	No change in the above flow.	• If the schedule runs at 11:05, the query is initiated from 10:55 to 11:05 with the action filter. • Logs from 10:55 to 11:00 are already analyzed in the previous schedule, so duplicates may occur.
Threshold: 10 events within 10 min (Schedule 30 min, LoopBack 0 min)	No change in the above flow.	• If the schedule runs at 11:30, queries are split based on schedule time divided by threshold time: • Q1=11:00–11:10, • Q2=11:10–11:20, • Q3=11:20–11:30. • If the action and threshold are matched within a query, a detection report is triggered. • If partial logs are received in-between queries within threshold time, those events will not trigger because previous query data is not maintained in memory.
Threshold: 10 events within 10 min (Schedule 25 min, LoopBack 0 min)	No change in the above flow.	Same as the above case but queries are split as: • Q1=11:00–11:10, • Q2=11:10–11:20, • Q3=11:20–11:25.
		Same as the above case but queries are split as:

Threshold: Condition 10 events within 10 min (Schedule 30 min, LoopBack 20 min)	Continuous Mode No change in the above flow.	• Q1=10:40–10:50, Scheduled Mode • Q2=10:50–11:00, • Q3=11:00–11:10, • Q4=11:10–11:20, • Q5=11:20–11:30.

Advanced rule (More-than one action rule)

Condition	Continuous Mode	Scheduled Mode
Action 1: 10 events within 10 min, Followed By 5 minAction 2: 9 events within 10 min, Followed By 12 minAction 3: 5 events within 5 min (Schedule 10 min, LoopBack 0 min)	• Same as the continuous execution standard rule flow for Action 1. • Followed by working given below: • Action 2 first event (E1) must trigger within “A1.E10 time + FB1”. • Remaining events must meet Action 2 condition, then success is achieved. • Action 3 first event (E1) must trigger within “A2.E9 time + FB2”. • Remaining events must meet Action 3 threshold condition, then success is achieved. • Example :- • A1 event is triggered between time period 10:50–10:54 (E1=10:51, E10=10:54). • If A1 succeeds, A2.E1 must trigger between	• Same as the scheduled execution standard rule for Action 1. • At threshold time ≤ schedule + loopback time, a single query is generated. • Followed by working given below: • A2 threshold must be met within “A1.E1 + FB1”. • If FB1 / threshold time < 1, the followed by time is taken as max; threshold is not considered. • A3 threshold must be met within “A2.E1 + FB2”. • If FB2 / threshold time > 1 (e.g., 2.4), queries are split as below: • A3.Q1=first 5 min, • A3.Q2=second 5 min, • A3.Q3=remaining min. • If logs fall between 2 queries, events will not trigger. • If schedule time exits, events will not trigger. • Schedule working: • Queries are framed only between schedule + loopback. • Example:A1.Q1=10:50–11:00. A1.E1=10:51, remaining A1.E2–E10=10:52–10:59. • If A1 succeeds, A2 events must trigger within 10:51–10:56 (A1.E1+FB1). • If A2 succeeds, A3 events must trigger within

Condition	Continuous Mode	Scheduled Mode
	must trigger between 10:54–10:59. (Example: A2.E5=10:58, A2.E9=10:58). • If A2 succeeds, A3.E1 must trigger between 10:58–11:10. (Example: A3.E1=11:09, A3.E2=11:14).	A3.Q1=10:53–10:58 or A3.Q2=10:58–11:00. • If A3 matches one query, 1 detection is triggered. • If both queries match, 2 detections are triggered. • Reports generated: • Report 1 – A1, A2, A3Q1 events. • Report 2 – A1, A2, A3Q2 events.
Action 1: 10 events within 10 min, Followed By 25 minAction 2: 9 events within 10 min, Followed By 12 minAction 3: 5 events within 5 min (Schedule 30 min, LoopBack 20 min)	No change in the above flow.	• Schedule starts at 11:00. • A1 – Number of queries = (schedule + loopback) / A1 threshold = (30+20)/10=5.A1.Q1=10:10–10:20, then: A1.Q2=10:20–10:30, A1.Q3=10:30–10:40, A1.Q4=10:40–10:50, A1.Q5=10:50–11:00. • If events match in multiple queries, each query is considered a separate detection. • Example: A1.Q2, A1.Q3, A1. • Q5 has success data (A1.Q2.E1=10:26, A1.Q3.E1=10:34, A1.Q5.E1=10:56). • A2 – If FB1 > A2 threshold, queries are split 25/10=2.5: • A2.Q1A=10:26–10:36, • A2.Q1B=10:36–10:46, • A2.Q1C=10:46–10:51. • A2.Q2A=10:34–10:44, • A2.Q2B=10:44–10:54, • A2.Q2C=10:54–10:59. • A2.Q3A=10:56–11:00 (remaining schedule only). • If multiple queries match, each is considered a separate detection. • Example: A2.Q1B, A2.Q2B, A2.Q2C have success (a separate detection. • Example: Q2B & A1.Q3, S3: A2.Q2C & A1.Q3). • A3 – Queries split like FB1 > A2 threshold, 12/5=2.4:

Condition	Continuous Mode	Scheduled Mode
		• A3.Q1A=10:41–10:46, • A3.Q1B=10:46–10:51, • A3.Q1C=10:51–10:53. • A3.Q2A=10:53–10:58, • A3.Q2B=10:58–11:00. • A3.Q3A=10:57–11:00. • If logs fall between schedules, they will not trigger. • If all queries match, 6 detections are shown with A1 and A2 duplicate logs.

Rule specific use cases

Anomaly rules

1. Brute-Force login attempt

Use case

A service account logs 20 failed login events in a very short window of time. This is a strong indicator of an ongoing attempt for a Brute-Force or credential-stuffing attack.

With Anomaly rules

An active Anomaly rule of "Logon Failure" action paired with a count-based anomaly model aids in a rapid threat detection of account compromise attempts. As a threat response, the window for attacker(s) to pivot into the network may be blocked.

> NOTE:
>
> In addition to the said anomaly rule, an advanced rule can take threat detection to another level by correlating the failed logins with a subsequent successful login from the same account.

2. Suspicious third-party account activity

Use case

A managed-service vendor account starts configuring changes after the usual business hours.

With Anomaly rules

"Configuration change" action could be paired with a time-based anomaly model for a focused monitoring of activities taking place during non-business hours. For instance, 9 AM to 6 PM are the usual working hours for

this user, who is now performing actions at 3 AM. Additionally, location-based anomaly model can help flag changes made from unexpected geo locations.
These deviations from the established baselines trigger an anomaly, helping the security team to investigate promptly and prevent possible credential compromise or session hijacking.

Advanced rules

1. Data Exfiltration via bulk modifications

Use case

An unauthorized user deleted or renamed large batches of files on a critical file server.
With Advanced rules
An advanced rule correlating "file deletion" actions with "bulk file rename" events along with a threshold on total file access count within a 10-minute window and filters will narrow down the scope to the unauthorized critical server access.

2. Unauthorized application deployment in QA environment

Use case

A non-DevOps user deploys/runs an unauthorized executable in a staging environment.
With Advanced rules
An advanced rule correlating "executable creation" with "scheduled task creation" on QA-tagged machines and filters on user roles with a threshold on event sequence within 10 minutes flags such unauthorized deployment activity early on.
Read also
This document explained how standard, anomaly, and advanced rules work, their configuration options, and practical use cases such as brute-force attempts, suspicious account activity, and data exfiltration.

- Rule management overview
- Creating custom rules
- Query grammar
- Managing rules
- Scheduled detection reports

10.1.2.3. Creating custom rules

Last updated on: September 12, 2025

In this page

Overview

Rule creation

How to create a new rule?

Standard Rule

Anomaly Rule

Advanced Rule

Overview

This page explains the process of building custom rules to detect security events. You can create standard rules for basic filtering, anomaly rules for unusual single-event behavior, or advanced rules for complex multi-step patterns. Each rule type supports fields like severity, filters, thresholds, anomaly models, and MITRE ATT&CK mappings to add context and make detections more actionable.

Rule creation

Functionality:

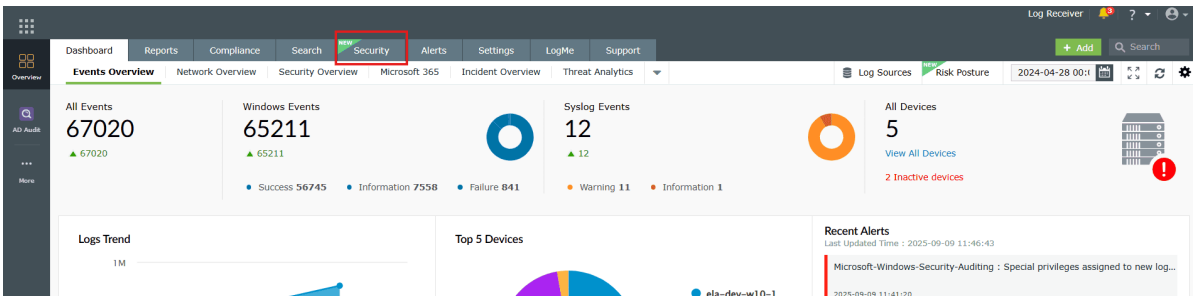
A simple and robust way of building security rules that are required for their environment.

Use case:

To create security rules of any type (standard, anomaly-based, or advanced) with detailed tagging, MITRE ATT&CK mappings, and additional context like prerequisites and mitigations for better organization and actionable insights.

How to create a new rule?

1. In the product console, click on the Security tab.



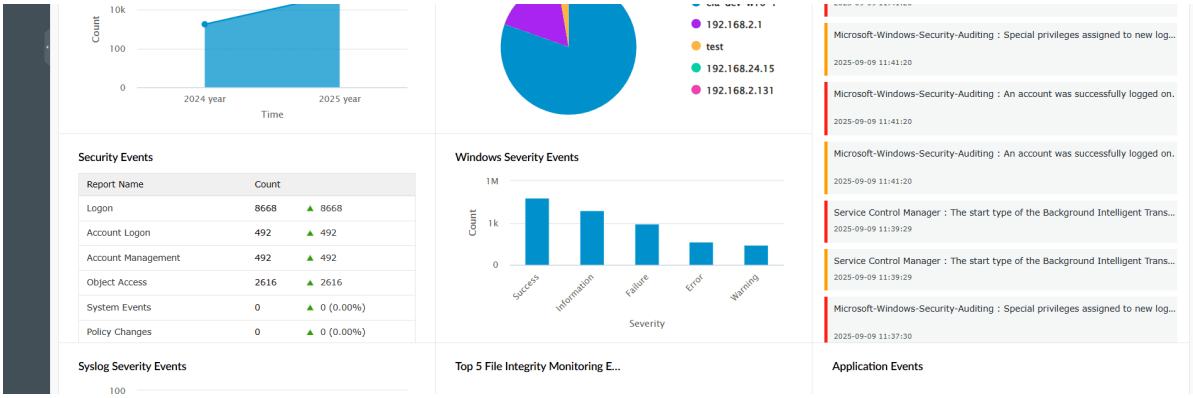


Image 1: Security tab in dashboard

2. Click on the Manage Rule option in the right end.

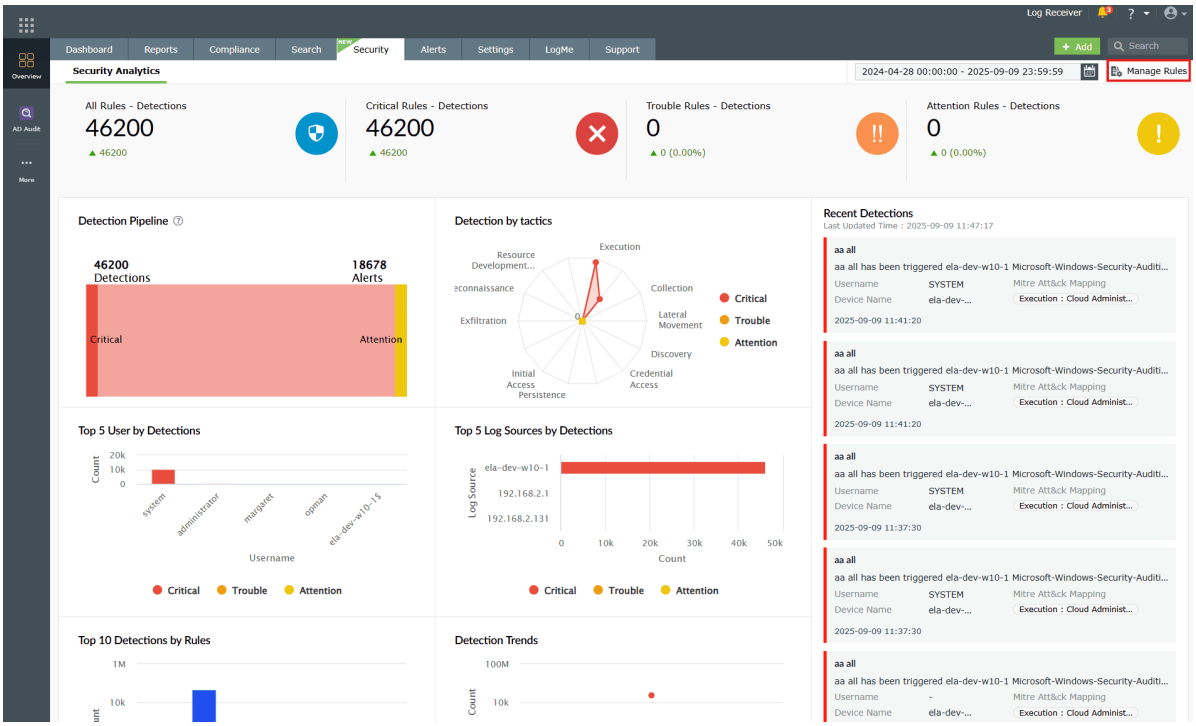
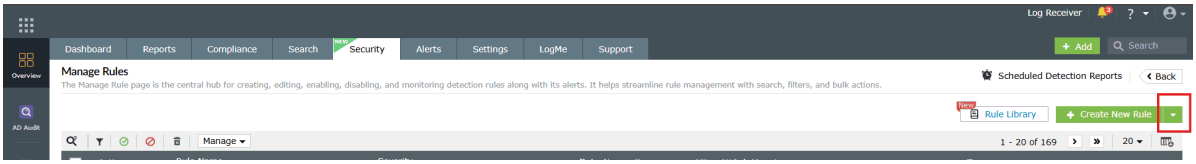


Image 2: Manage rules in security dashboard

3. You will be taken to the page with the complete list of rules. In the right side, you will find "Create New Rule". Click on the drop-down button available for this option.

> NOTE:
>
> If you click directly on Create New Rule, you will be directly taken to the Standard Rule creation page.



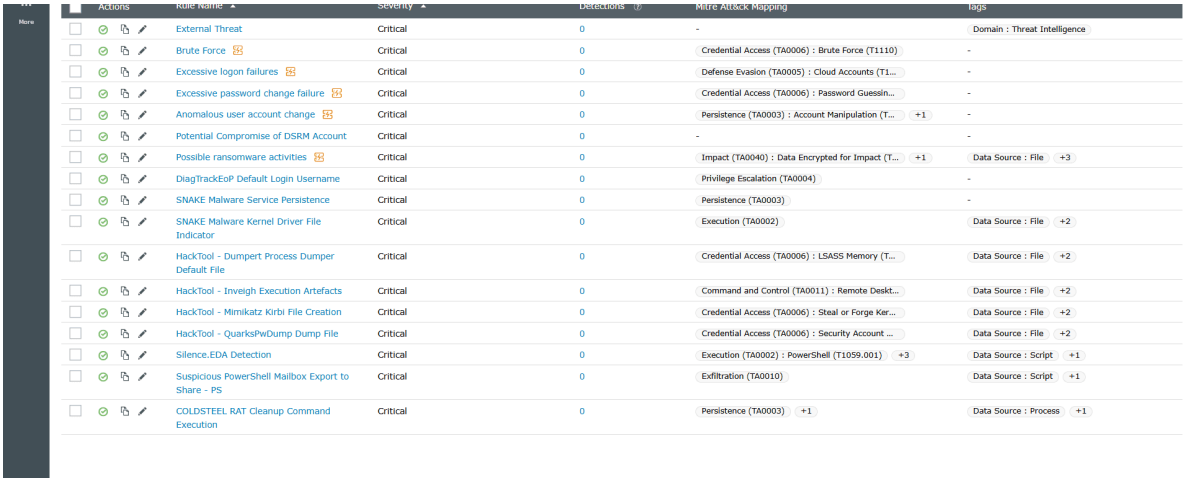
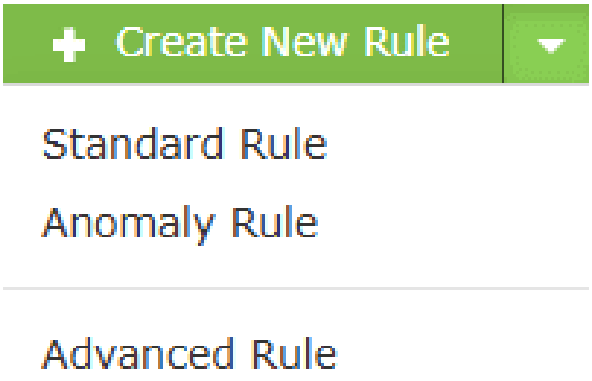


Image 3: Manage rules module via the security dashboard

4. The drop-down expands into the Standard Rule, Anomaly Rule, and Advanced Rule options of rule creations. Click on your preferred rule type based on your requirements.



Read further on how to create a rule in each of the three rule types.

Standard Rule

Steps to create a Standard rule

1. Navigate to the Standard Rule type. You will be taken to the page consisting of fields that define the rule criteria, like in the below image. To understand more about the fields refer to the Understanding rules help document.

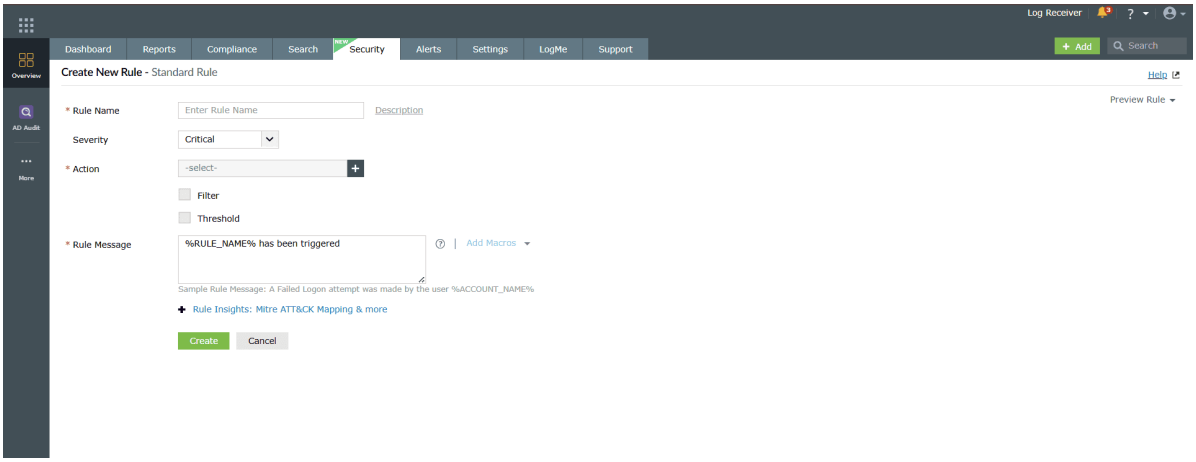
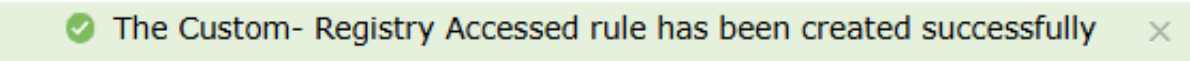


Image 4: Create a standard rule

2. Rule Name should be given, and a description for a rule is optional. Click on Description, and a popup will open for the same in case you want to add description.
3. Choose a Severity level from Critical, Trouble, and Attention. This field will be Critical by default.
4. Choose the Action based on which you wish to create the rule. Read further to know how to Create Custom Action.
    - Filter can be applied but only if a rule needs to run for just a specific case.
    - List of fields will be displayed with respect to the selected action and its log format.
    - If the list of fields exceeds 5, a search option will be shown to find and navigate to that field.
    - Threshold can be applied if a rule needs to run after a certain threshold value.
5. Rule Message can also be given to provide a formatted message across the detection reports for the triggered rule.
    - Fields in the message will be defined from Macros.
6. Rule Insights: MITRE ATT&CK Mapping & more is optional and can also be configured for a rule.
7. After entering the required fields, click on Create.
8. Upon successful completion of the action, the below pop-up appears.



Anomaly Rule

Steps to create an Anomaly rule

1. Navigate to the Anomaly Rule type. You will be taken to the page consisting of fields that define the rule criteria, like in the below image. To understand more about the fields refer to the Understanding rules help document.

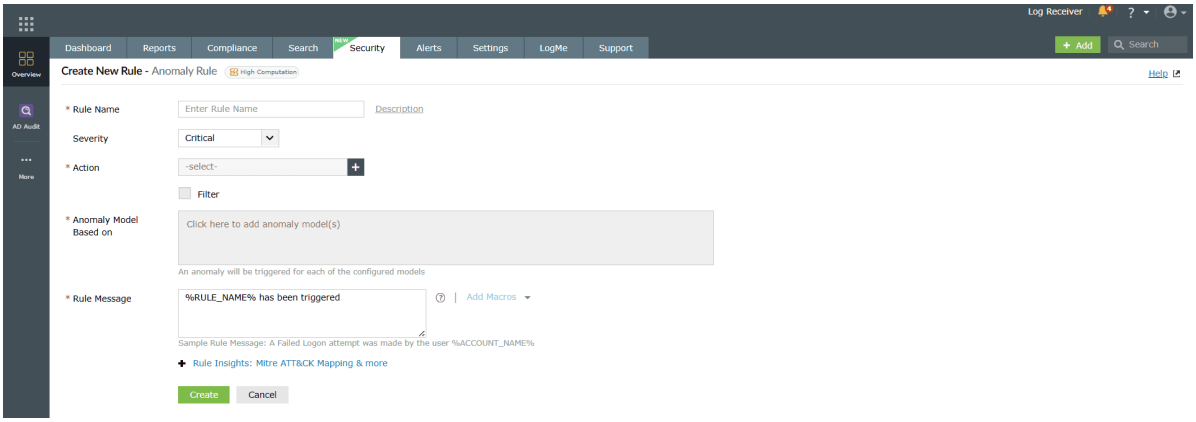
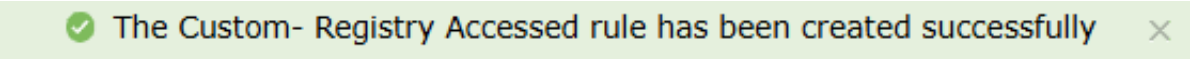


Image 5: Create an anomaly rule

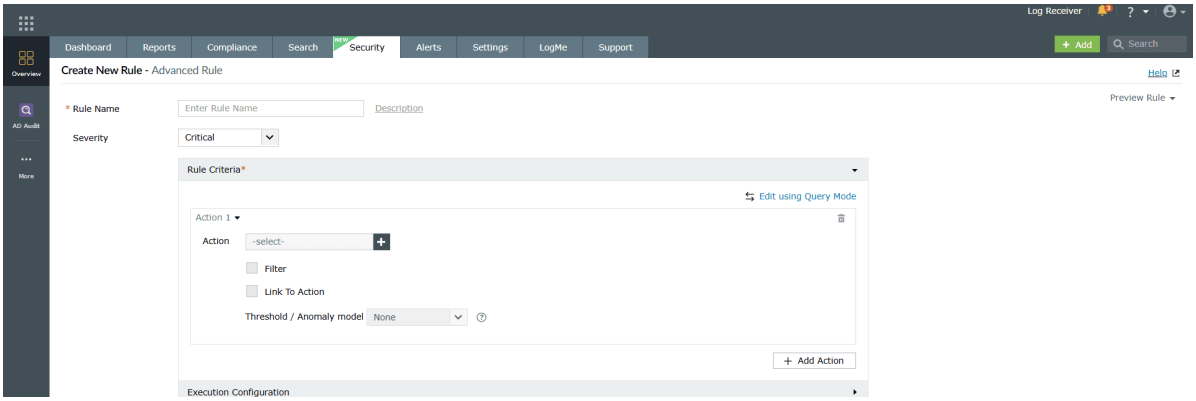
2. Rule Name should be given, and Description for a rule is optional. Click on description, and a popup will open for the same in case you want to add description.
3. Choose a Severity level from Critical, Trouble, and Attention. This field will be Critical by default.
4. Choose the Action based on which you wish to create the rule. Read further to know how to Create Custom Action.
    - Filter can be applied but only if a rule needs to run for just a specific case.
    - List of fields will be displayed with respect to the selected action and its log format.
    - If the list of fields exceeds 5, a search option will be shown to find and navigate to that field.
    - Threshold can be applied if a rule needs to run after a certain threshold value.
5. Choose the Anomaly Model Based on to define how deviations from normal behavior will be detected. A maximum of 5 models can be selected.
6. Rule Message can also be given to provide a formatted message across the detection reports for the triggered rule. Fields in the message will be defined from Macros.
7. Rule Insights: MITRE ATT&CK Mapping & more is optional and can also be configured for a rule.
8. After entering the required fields, click on Create.
9. Upon successful completion of the action, the below pop-up appears.



Advanced Rule

Steps to create an Advanced rule

1. Navigate to the Advanced Rule type. You will be taken to the page consisting of fields that define the rule criteria, like in the below image. To understand more about the fields refer Understanding rules page.



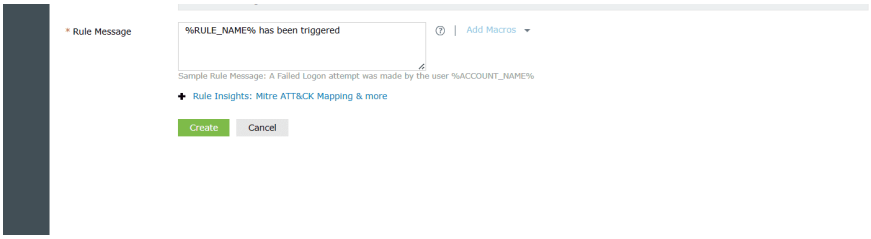
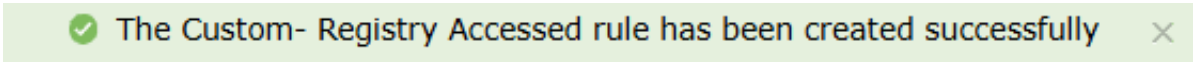


Image 6: Create an advanced rule

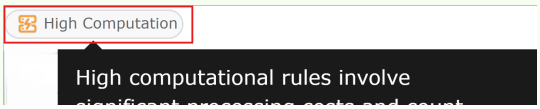
2. Rule Name should be given, and Description for a rule is optional. Click on description, and a popup will open for the same in case you want to add description.
3. Choose a Severity level from Critical, Trouble, and Attention. This field will be Critical by default.
4. Rule Criteria
   Edit using Interactive Rule Builder
   - Action selection will be the same as Standard Rule creation, but multiple actions can be selected as per existing correlation rules. Read further to know how to Create Custom Action.
   - Filter and Threshold will also be the same as Standard Rule creation.
   - Link To Action: In the case where you have chosen multiple actions, you can link those actions to one another so that events involving those actions can be correlated and monitored for suspicious activity.

   Edit using Query Mode
   - Exclusive to advanced rule building, in this mode, you can configure the criteria and parameters by querying with the help of Query Syntax and Query Grammar for the same. Refer to Query Grammar to know more.
5. Define the Execution Configuration if you wish to schedule the rule.
6. Rule Message can also be given to provide a formatted message across the detection reports for the triggered rule.
   - Fields in the message will be defined from Macros.
7. Rule Insights: MITRE ATT&CK Mapping & more is optional and can also be configured for a rule.
8. After entering the required fields, click on Create.
9. Upon successful completion of the action, the below pop-up appears.



What is a High Computation Rule?

If a threshold is applied to any rule, it will be calculated for licensing since it is highly intensive, and it will be marked as a High Computation Rule. The indicator will be visible in the rules list and also during the creation of the said rule.



significant processing costs and count towards your subscription. Know more

How to create Custom Action in advanced rules?

1. While choosing an Action during rule configuration, you can find an option to create a custom action as per your requirements. Click on Create Custom Action as highlighted in the below image.

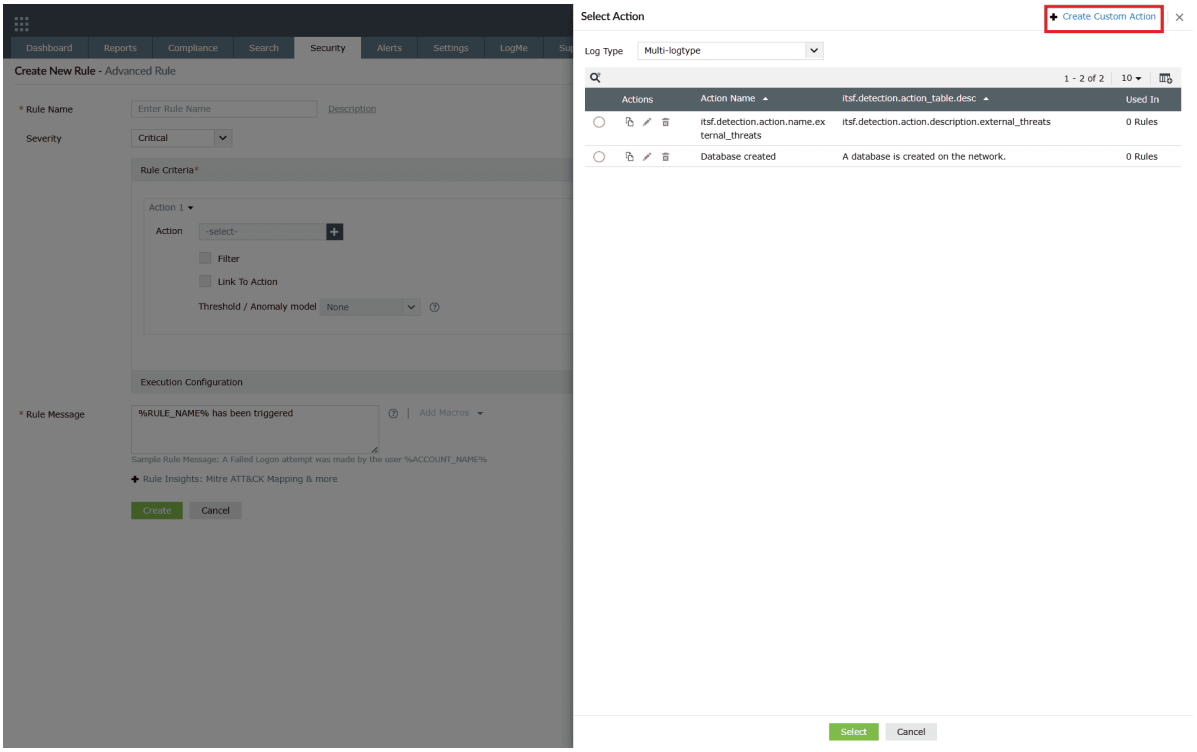
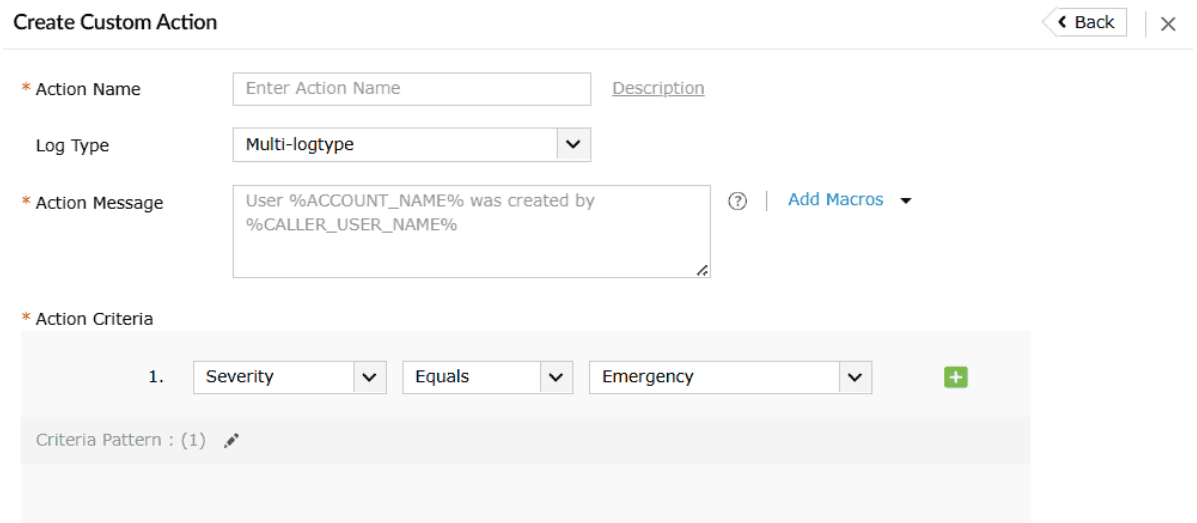


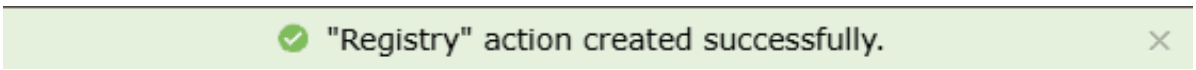
Image 7: Create custom action

2. The necessary fields to be defined will be shown as below.





3. Configure by setting the field values:
    - Action Name and Log Type are mandatory fields.
    - Description is an optional field. Click on it to view the description box.
    - Action Message is used for displaying a formatted message for the action used.
    - Macros can be added to the Action Message format.
    - Action Criteria will define the conditions which must be met for that specific action to be triggered.
    - Fields like Macros will be displayed with slight variations in the drop-down options depending upon the selected Log Type.
4. Once you have entered the required field values, click on Create.
5. Upon successful completion of the action, the below pop-up appears.



Read also

This document explained how to create new rules, configure standard, anomaly, and advanced rules, and set up custom actions for more flexible monitoring.

- Rule management overview
- Understanding rules
- Query grammar
- Managing rules
- Scheduled detection reports

10.1.2.4. Manage rules

Last updated on: September 12, 2025

In this page

- Overview
- Accessing the Manage Rules page
- Fields in the manage rules table
- Actions column
- Enable/Disable rules
- Clone a rule
- Edit a rule
- Delete rule(s)
- Filter rule(s)
- Other configurations to manage rules
- Rule Name column
- Rule Details
- Prerequisites
- Mitigation
- Execution Details
- Rule tuning
- Severity
- MITRE Att&ck Mapping
- Tags
- Execution Mode & Status
- Alert Profiles
- Created By
- Rule Type
- Installed Time
- Last Modified Time
- Detections

Overview

This page explains how to use the Manage Rules module to oversee all detection rules in a centralized view. It covers actions such as enabling, disabling, cloning, editing, deleting, filtering, and importing/exporting rules. Each rule entry provides detailed information, including severity, MITRE ATT&CK mapping, tags, execution mode, alert profiles, and detection history. Additional features such as rule tuning, prerequisites, and mitigation steps help administrators refine detections, improve performance, and align rules with security frameworks.

Accessing the Manage Rules page

1. Navigate to the Security tab via the dashboard and click on Manage Rule as highlighted below.

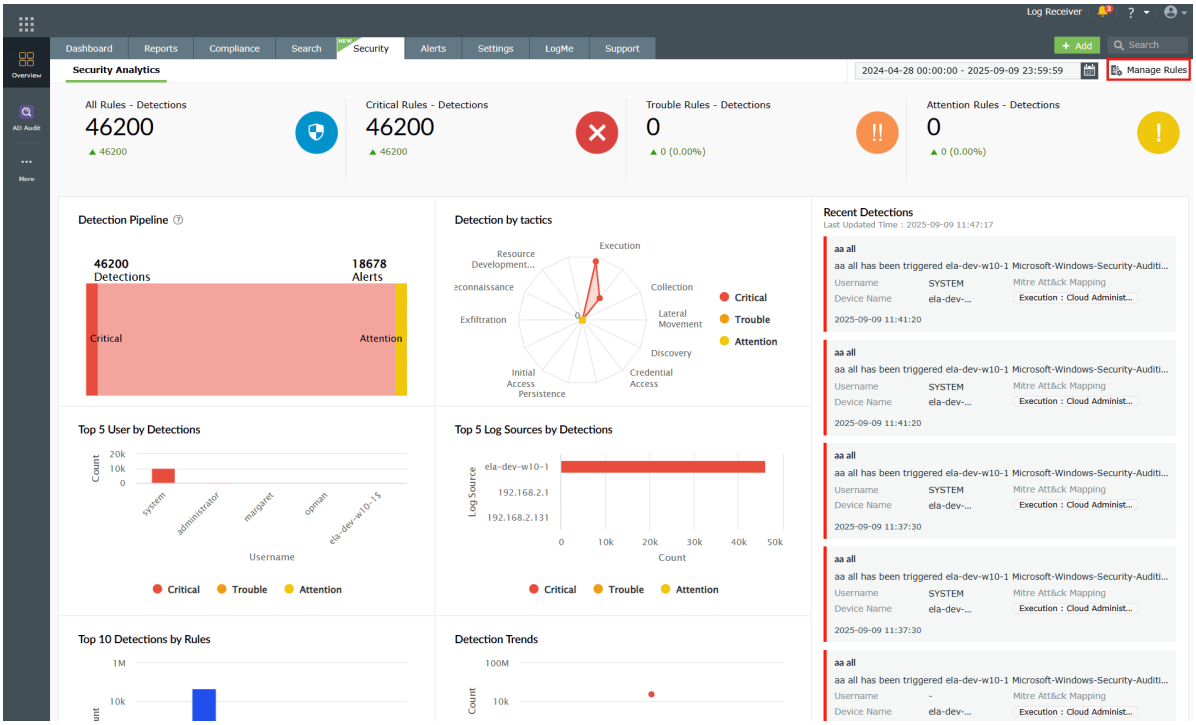
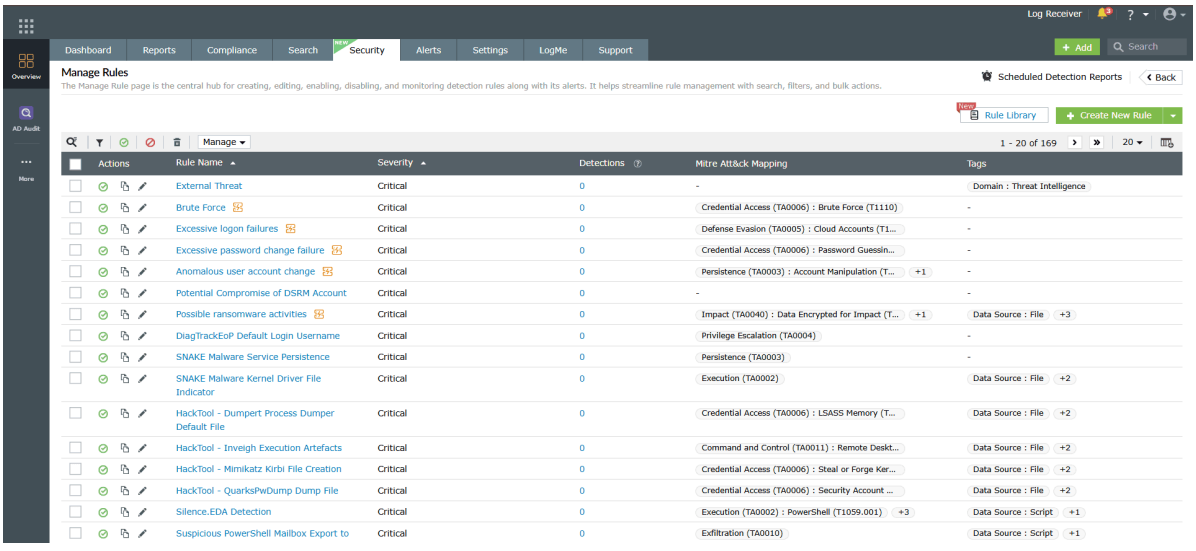


Image 1: Manage rules in security dashboard

2. You will be taken to the Manage Rules page with the complete list of rules as shown in the below image. It is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.



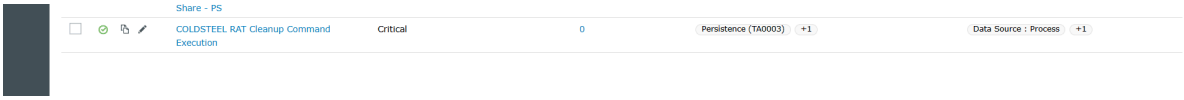


Image 2: Manage rules module via the security dashboard

Fields in the manage rules table

A. Actions column

The actions column acts as a medium for you to take required actions on the rule(s) as per your needs. Below are the available rule actions in the Manage Rules module.

- Enable/disable rules
- Clone rule
- Edit rule
- Delete rule(s)

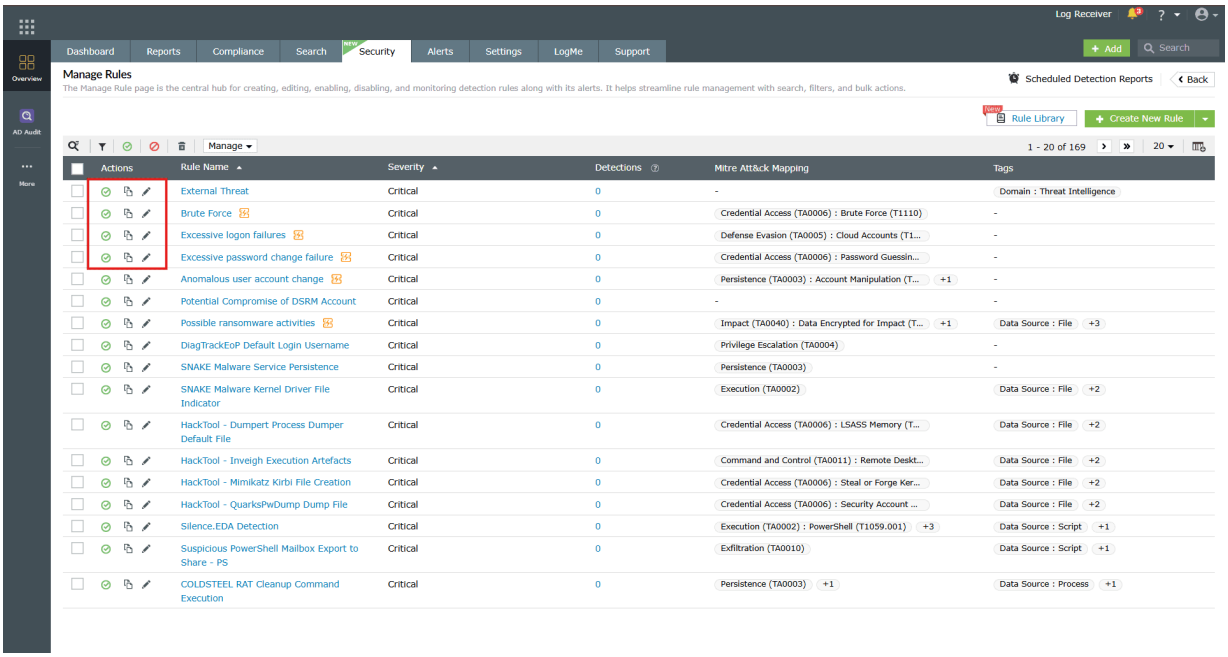
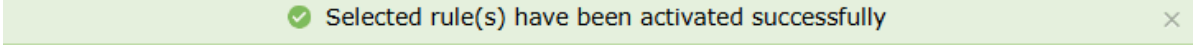


Image 3: Available actions in the manage rules module

Enable/Disable rules

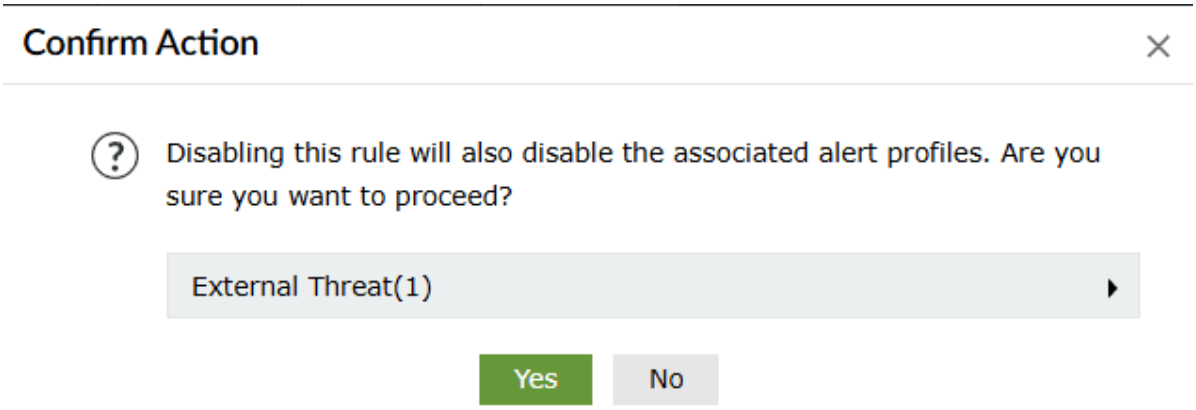
Enabling a rule

1. Click on the disabled icon under the Actions column to enable the rule.
2. As soon as you perform this action, the icon indicates that the rule is now enabled and the below pop-up message appears briefly.



Disabling a rule

1. Click on the enabled icon under the Actions column to disable the rule.
2. A confirm action pop-up will appear if an alert profile is associated with the said rule. Click on Yes to proceed.



3. As soon as you perform this action, the icon indicates that the rule is now disabled and the below pop-up message appears briefly.



Enable/Disable multiple rules at once

1. Click on the empty checkbox(es) in the first column in order to select the respective rules.
2. Click on the Enable/Disable icons in the ribbon above the rules list.

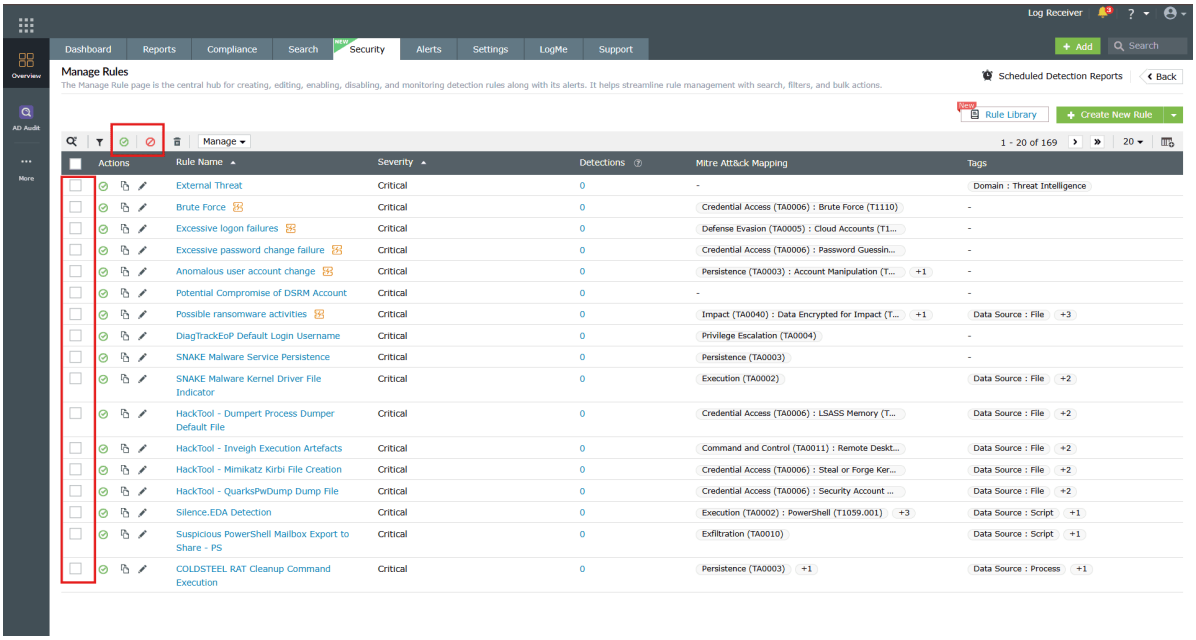


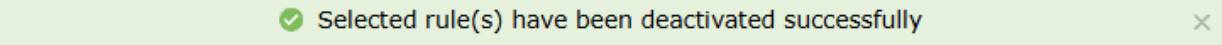
Image 4: Bulk actions in the manage rules module

3. Upon successful completion of the action, the below pop-up appears.

When enabled:

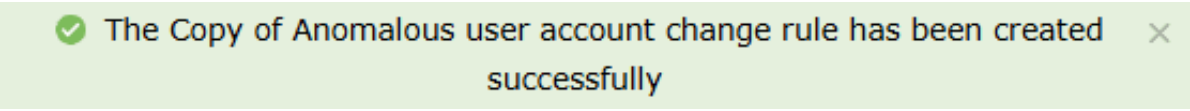


When disabled:



Clone a rule

1. Click on the Clone icon under the Actions column to clone the respective rule.
2. Depending upon the rule type—Standard, Anomaly, or Advanced—you will be taken to the specific configuration page of that particular rule.
3. Make the necessary changes in the field values in order to customize the cloned rule and click on Create.
4. Upon successful completion of the action, the below pop-up appears.

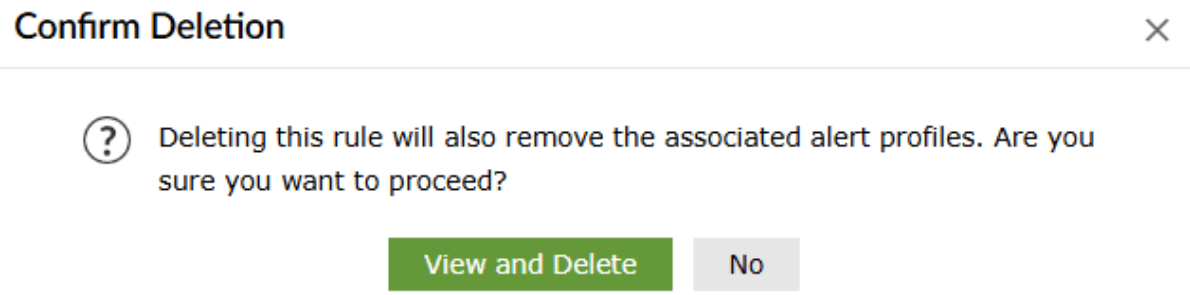


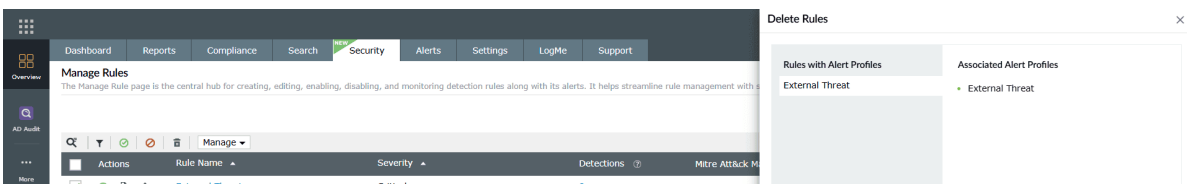
Edit a rule

1. Click on the Edit icon under the Actions column to edit the respective rule.
2. Depending upon the rule type—Standard, Anomaly, or Advanced—you will be taken to the specific configuration page of that particular rule.
3. Make the necessary edits in the field values and click on Update.
4. The rule will be updated instantly in the rules list.

Delete rule(s)

1. Click on the empty checkbox(es) in the first column in order to select the respective rules.
2. Then click on the Delete icon in the ribbon above the rules list.
3. A Confirm Action pop-up appears. Click on Delete.





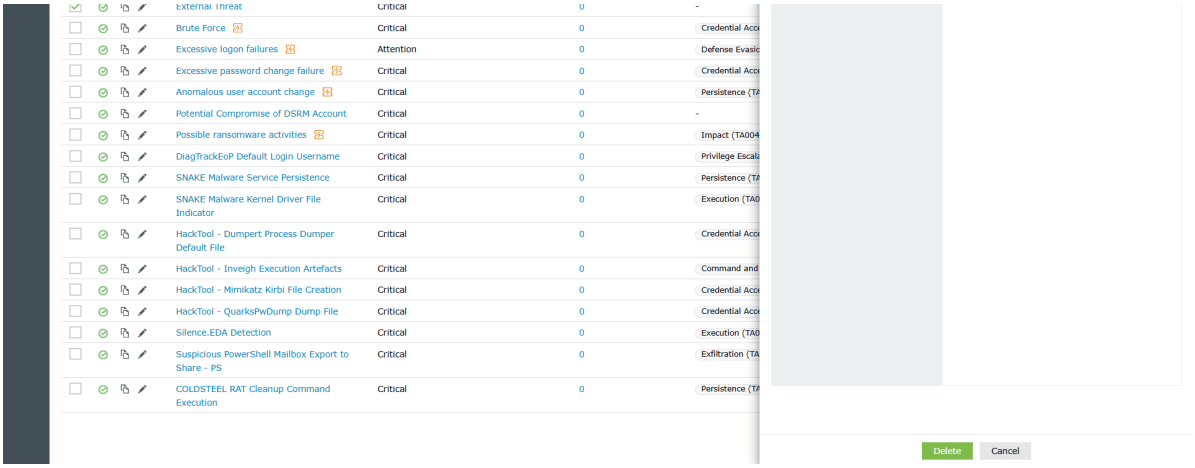
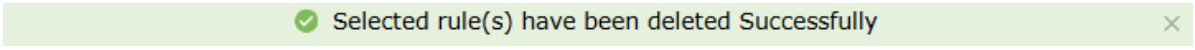


Image 5: Deleting rule in the manage rules module

4. Upon successful completion of the action, the below pop-up appears.



Filter rule(s)

1. Click on the Filter icon in the ribbon above the rules list.

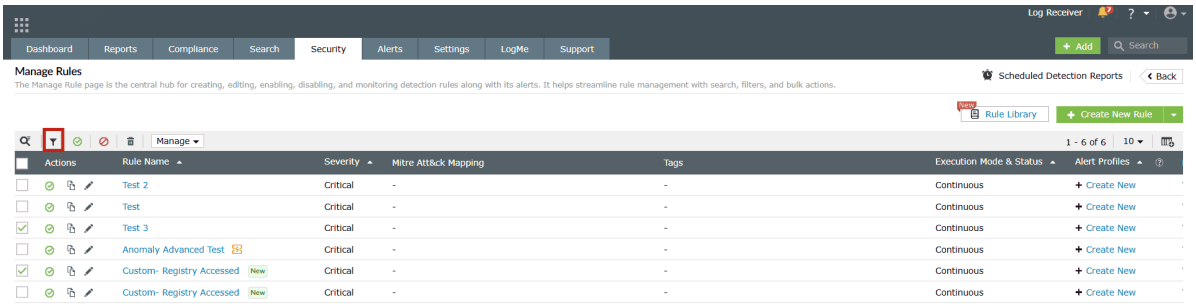
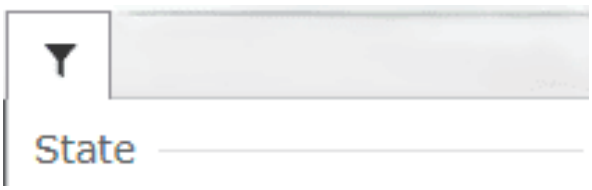
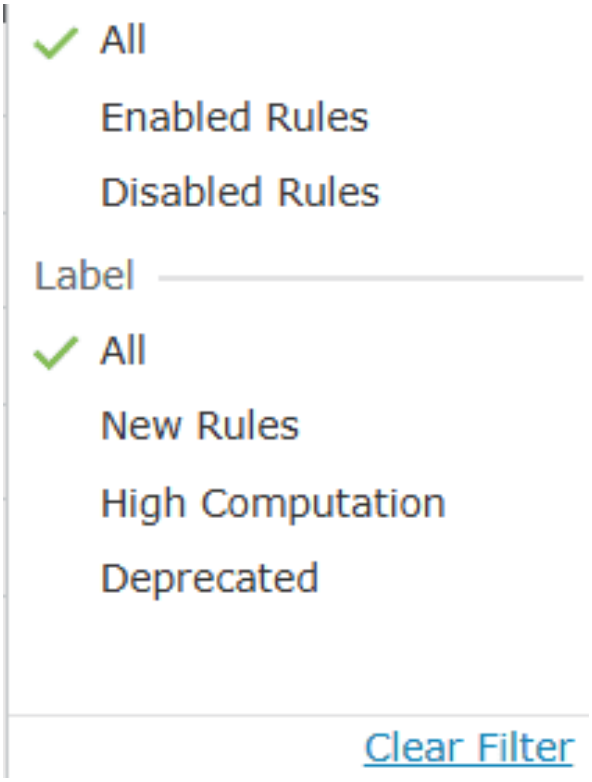


Image 6: Filtering rules in the manage rules module

2. The following filter options appear.





3. You can choose multiple filters at once. Click on a filter to select it. Click on it again if you want to deselect it. The rules get filtered instantly as you click on any filter option.
4. Click on the Clear Filter option to undo all/any filtering that has been done to the rules.

Other configurations to manage rules

1. Click on the empty checkbox(es) in the first column in order to select the respective rules you wish to configure.
2. In the ribbon above the list of rules, an option to further Manage rules is available.

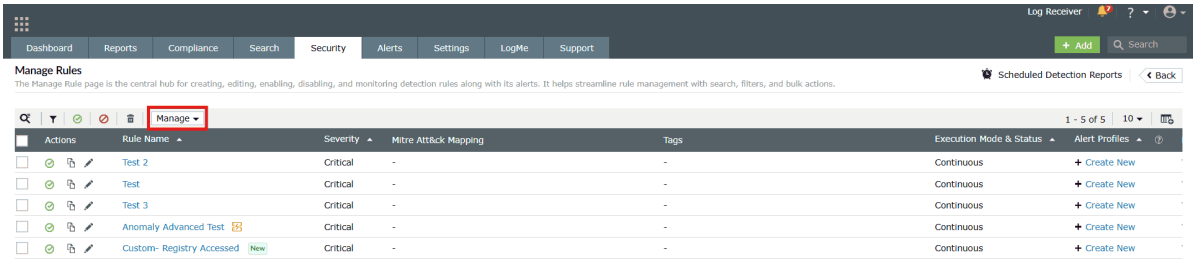
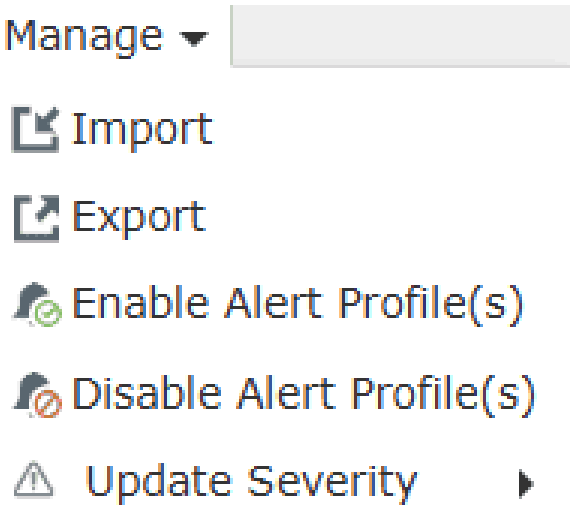


Image 7: Managing rules in the manage rules module

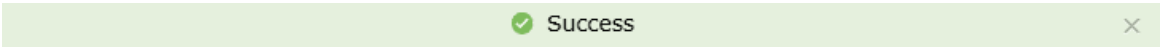
Image 7: Managing rules in the manage rules module

3. Click on it for the Manage tab to expand the configurations.

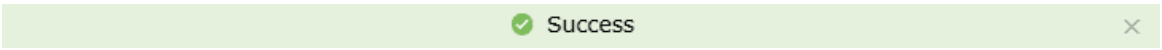


4. Configurations:

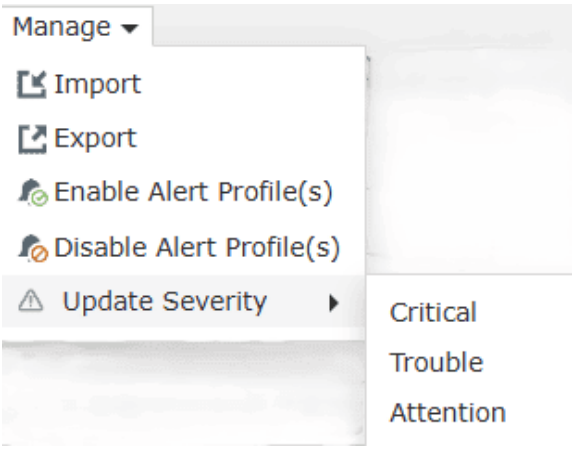
- Import: Import the desired rules by uploading a file containing the rules.
- Export: Instantly download the selected rules along with the configuration details. This option is applicable only for custom created rules.
- Enable Alert Profile(s): Click on it to Enable Alert Profile(s) for the selected rule(s) and the configuration is instantly updated displaying the below pop-up.



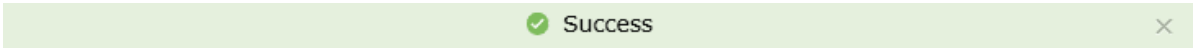
- Disable Alert Profile(s): Click on it to Disable Alert Profile(s) for the selected rule(s) and the configuration is instantly updated displaying the below pop-up.



- Update Severity: Click/Hover on it to view the three severity levels and choose the one you wish to apply.



The configuration is instantly updated displaying the below pop-up.



B. Rule Name column

The Rule Name column lists the names of all the configured rules till date.

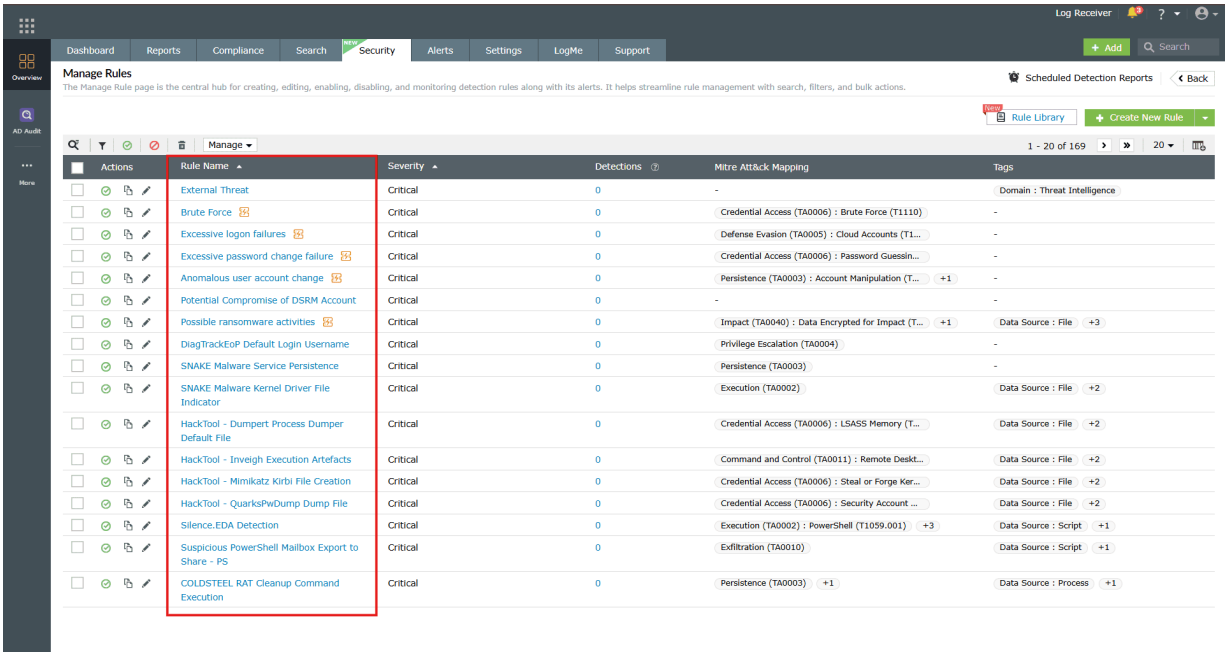


Image 8: Rule names in the manage rules module

Clicking on any rule name prompts the Rule Summary box to slide open. It includes 4 sub-tabs:

- Rule Details
- Prerequisites
- Mitigation
- Execution Details

Rule Details

Provides a summary of the rule along with the respective details and options to add exceptions for that particular rule.

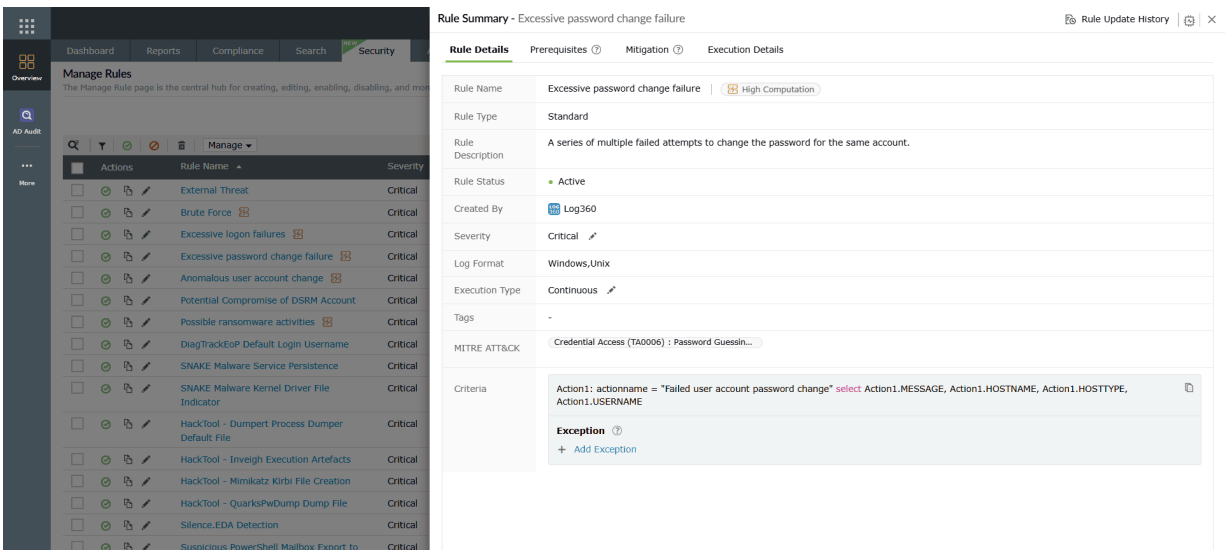
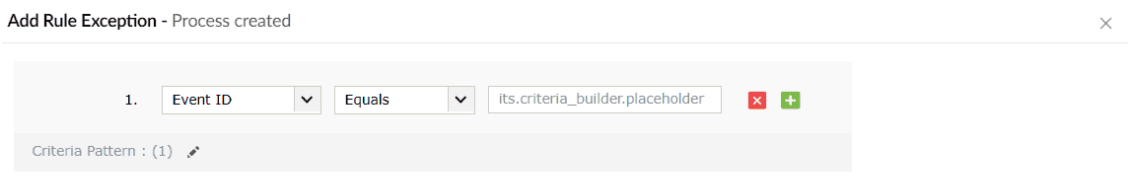




Image 9: Rule details in the manage rules module

1. Rule Name: Displays the unique rule name assigned by you for this rule.
2. Rule Type: Displays which category of rules this rule comes under - Standard, Anomaly, or Advanced.
3. Rule Description: Displays whatever description you have added for this rule, if any.
4. Rule Status: Displays whether the rule is currently in an Active state or Inactive.
5. Created By: Displays the user (identified by their role in this network) who has created this rule.
6. Severity: Displays the Severity level set during the rule configuration - Critical, Trouble, or Attention.
7. Log Format: Shows the log type associated with the rule.
8. Execution Type: Displays the Execution Configuration mode set for this rule - Continuous; Schedule every 5 minutes, 10 minutes, 30 minutes, 1 hour; and Custom.
9. Tags: Categorizes the rule based on industry or type.
10. MITRE ATT&CK: Maps the rule to relevant MITRE tactics and techniques.
11. Criteria: Displays the rule conditions in query format.
    - Exception: The Exception defines the criteria for the detection engine to rule out cases from the detections and reports. A detection will not be created if the set conditions from the rule exception match.
        - When you click on the Add Exception button, the Add Rule Exception box slides open.





- You can configure the exceptions you wish to rule out from detections and reports.
- Click on the Save button to save the rule exception.
- Upon successful completion of the action, the below pop-up appears.



- If you wish to reset and reconfigure that exception you can click on Clear Exception, and the configurations are reset.
- Click on Cancel if you wish to abort the process.

Prerequisites

This sub-tab provides an interface for you to check and ensure that the required dependencies of the rule are met for proper detection.

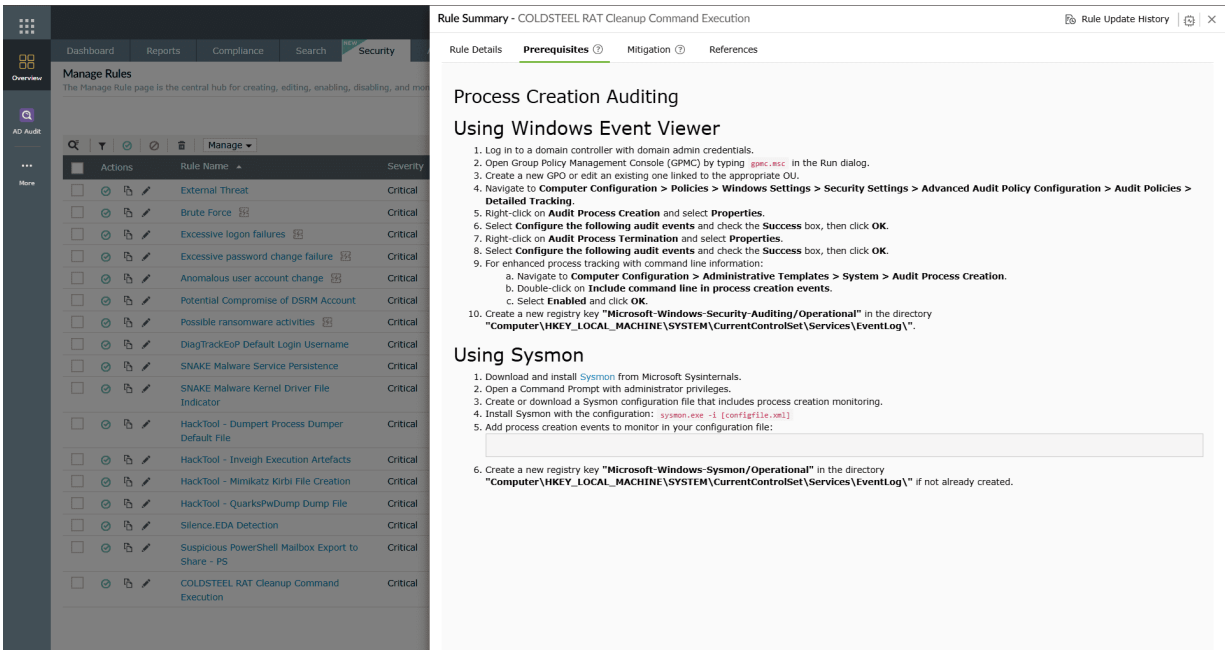


Image 10: Rule prerequisites in the manage rules module

Mitigation

This sub-tab provides an interface for you to take recommended actions to minimize risks and prevent future threats. Mitigations are pre-added for predefined rules, whereas for custom rules they must be manually added by the user.

Case 1: Mitigation steps existing in the rule configuration.

- Mitigation IDs: Lists the MITRE ATT&CK mitigation techniques associated with the detected rule or threat.
- Description: Provides actionable guidance on how to mitigate or reduce the impact of the threat, such as

- Description: Provides actionable guidance on how to mitigate or reduce the impact of the threat, such as configuration changes, security policies, or best practices.
- False positives: Indicates the likelihood of false positives for the specific detection.

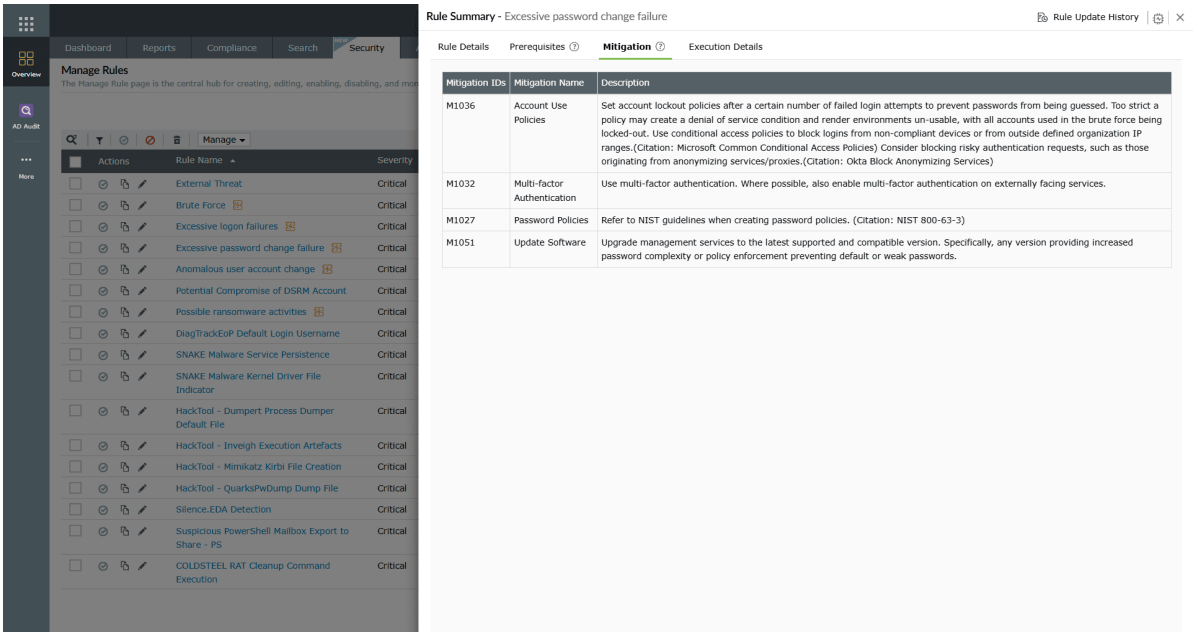


Image 11: Rule mitigation in the manage rules module

Case 2: No existing mitigation steps.
In such cases, it is implied that no mitigation is necessary for that particular rule.

Execution Details

Used to identify high-computation continuous rules in terms of memory usage. It also shows which of the currently collected logs fall under this rule's actions.

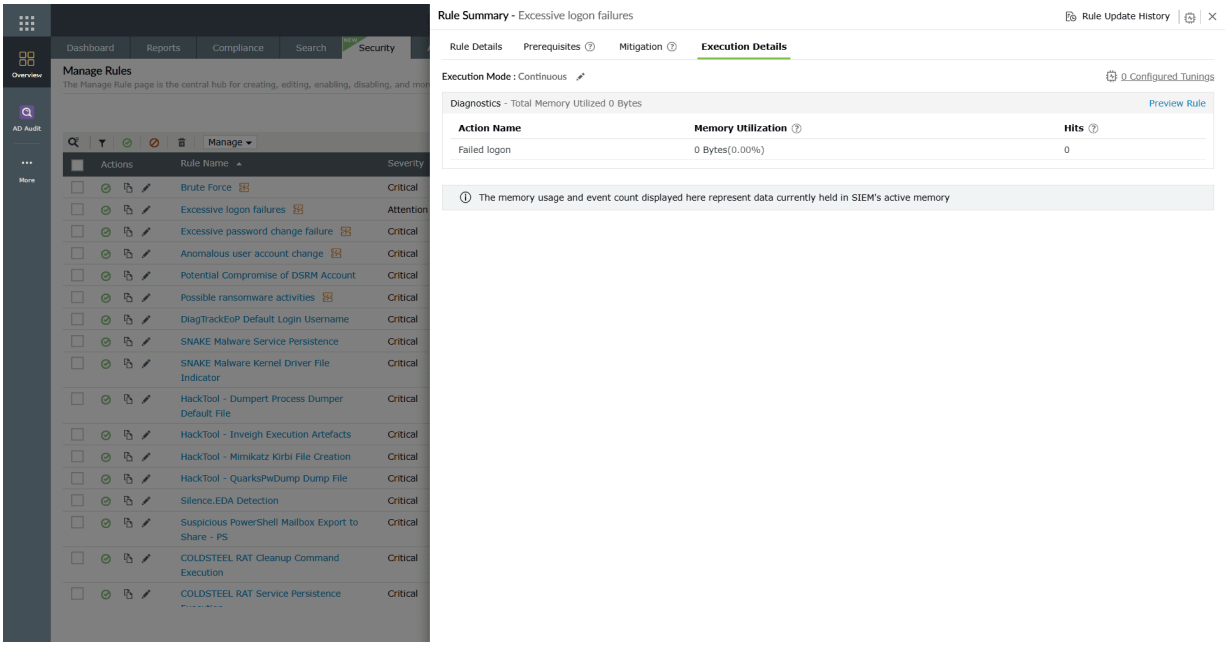


Image 12: Rule execution details in the manage rules module

Execution Mode:

1. Execution Mode: Displays the Execution Configuration mode set for this rule—Continuous; Schedule every 5 minutes, 10 minutes, 30 minutes, 1 hour; and Custom.
2. Diagnostics: Provides insights into the resource usage and activity generated by the rule. This helps you verify how the rule performs during execution.
    - Action Name: Displays the event/action associated with this particular detection. For example, Successful logon.
    - Memory Utilization: Track total memory used during action execution in near real time.
    - Hits: Track the total number of hits for the action in near real time.
3. Execution History: Displays a timeline of the rule's past executions, including event counts and memory consumption recorded during each run. This helps you review the rule's performance over time and troubleshoot any anomalies.
4. Refer to the understanding rules page to learn more about the differences in the execution mode for continuous and scheduled modes.

Rule tuning

The Rule Tuning option in helps administrators refine detection rules by optimizing query execution. It analyzes the way rules are processed and provides actionable insights to improve performance. By applying these recommendations, you can reduce execution load, improve query speed, and eliminate unnecessary noise. Below are the enhancements rule tuning can help administrators with:

- Enhances rule performance by reducing unnecessary execution overhead.
- Prevents timeouts and delays during query runs.
- Minimizes false positives by excluding known or repetitive patterns.
- Helps scale detection efficiency as log volume grows.

> NOTE
>
> Tuning insights are generated from query response analysis. Applying them may affect result consistency. Review before applying.

1. Click the icon in the top-right corner of the Rule Summary box to view the rule tuning configurations box.
2. The Rule Tuning panel opens, displaying:
    - Rule conditions and actions.
    - Tuning insights and recommendations.
    - A preview of rule execution with graphical output.

Available actions:

1. Tuning insights
    - Provides action-based suggestions, such as:

- Adding grouping fields to reduce the number of query executions.
- Using the Limit operator to control cardinality.
- Excluding specific usernames, devices, or fields to minimize load.

- You can:
  - Apply individual tunings.
  - Use Apply All Tunings for bulk optimization.

2. Rule preview
   - Generates a sample output graph showing query execution trends.
   - Displays execution time and data results (e.g., usernames, devices).
   - Helps validate whether tuning improves efficiency without losing accuracy.
3. Handling query timeouts
   - If a scheduled task fails due to query timeout, you can:
     - Adjust the query timeout value.
     - Apply recommended tunings.
     - Configure exceptions manually to filter out known patterns.

Example use case: Brute Force detection

Consider the Brute Force rule, which detects failed and successful Windows logins within a specific timeframe.

- Without tuning, this rule may return large datasets causing execution delays.
- With tuning, you can:
  - Add grouping by username/device.
  - Limit the number of results analyzed.
  - Exclude repeated usernames or devices to reduce execution load.

Result: Faster query response, reduced noise, and more efficient detection of brute-force attempts.

Rule tuning best practices

- Always preview the rule before applying tunings.
- Avoid over-filtering, as it may suppress genuine alerts.
- Use manual exceptions for repetitive patterns instead of disabling rules.
- Periodically revisit tuning recommendations as log volume and attack patterns evolve.

C. Severity

Displays the severity level set for the rules- Critical, Trouble or Attention.

D. Mitre Att&ck Mapping

Tactic and technique classification aligned with the MITRE ATT&CK framework that are associated with the rules.

E. Tags

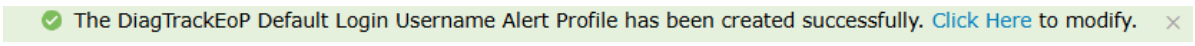
Additional contextual tags, such as threat actor, software, industry verticals that are associated with the rules.

F. Execution Mode & Status

Displays the Execution Configuration mode set for each rule.

G. Alert Profiles

- Provides the option to create an alert profile for all the rules listed here.
- When you click on the Create Alert Profile option, an alert profile for the corresponding rule is created instantly and the below pop-up appears.



- When you click on the Click Here option provided in the pop-up as shown above, you will be taken to the Edit Alert Profile module. Read the Alert Profile help page to learn more about editing and assigning alert profiles.

H. Created By

Displays the user (identified by their role in this network) who has created this rule.

I. Rule Type

Displays the rule category- Standard, Anomaly, or Advanced.

J. Installed Time

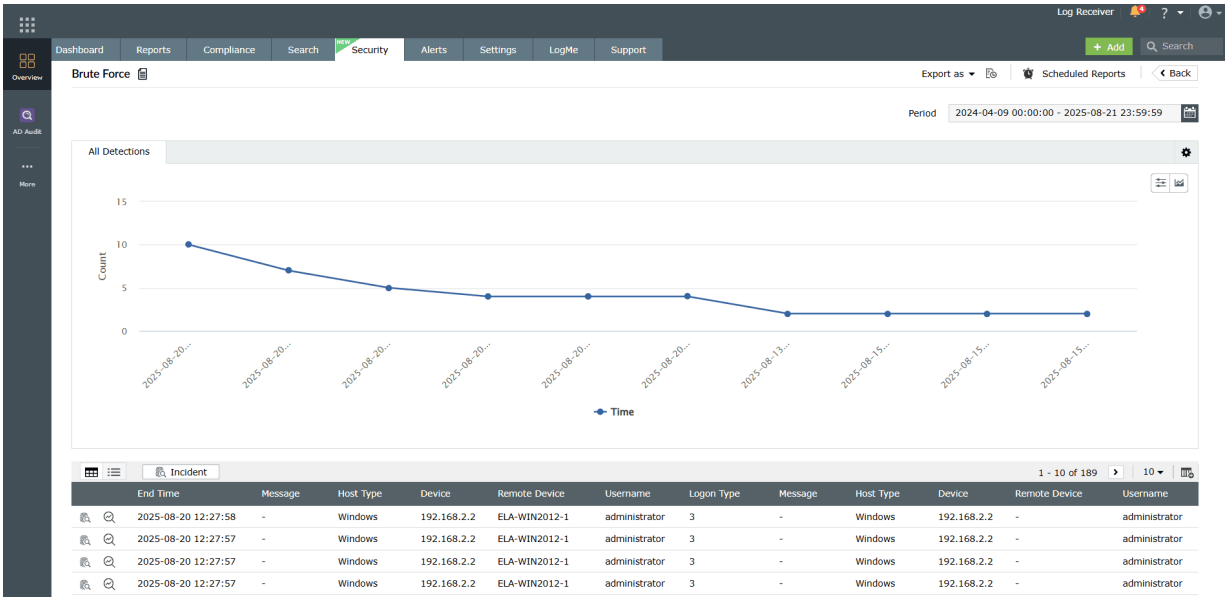
Displays the time of rule installation from the Rule Library.

K. Last Modified Time

Displays the time of the most recent modification done to the rule.

L. Detections

Click on the View Detections link to view all the detections that were triggered by that particular rule. A periodic graph of the detections will be shown to you for that particular rule as given below.



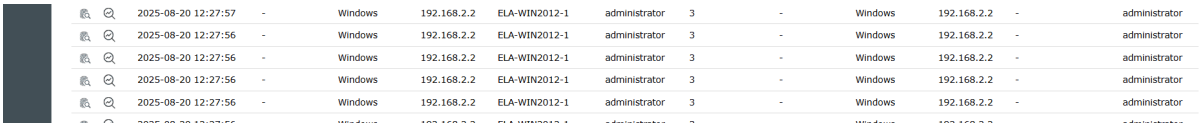


Image 13: Rule detection details in the manage rules module

The details displayed in the detection are as follows:

- Detection graph:
  - A visual depiction showing the event count over time that triggered the respective rule for quick anomaly spotting. Upon clicking the drop-down arrow available beside the graph, you will be shown the different types of graphs to choose from.
- Event Log Table: Displays details of each detected event that triggered the rule such as End Time, Event IDs, Log Source, Time, User Name, Domain, Message, etc. Clicking on the icon on the top-right corner of the data table allows you to select/deselect and Add what fields you wish to view separated by columns. You can choose fields from the many options provided.

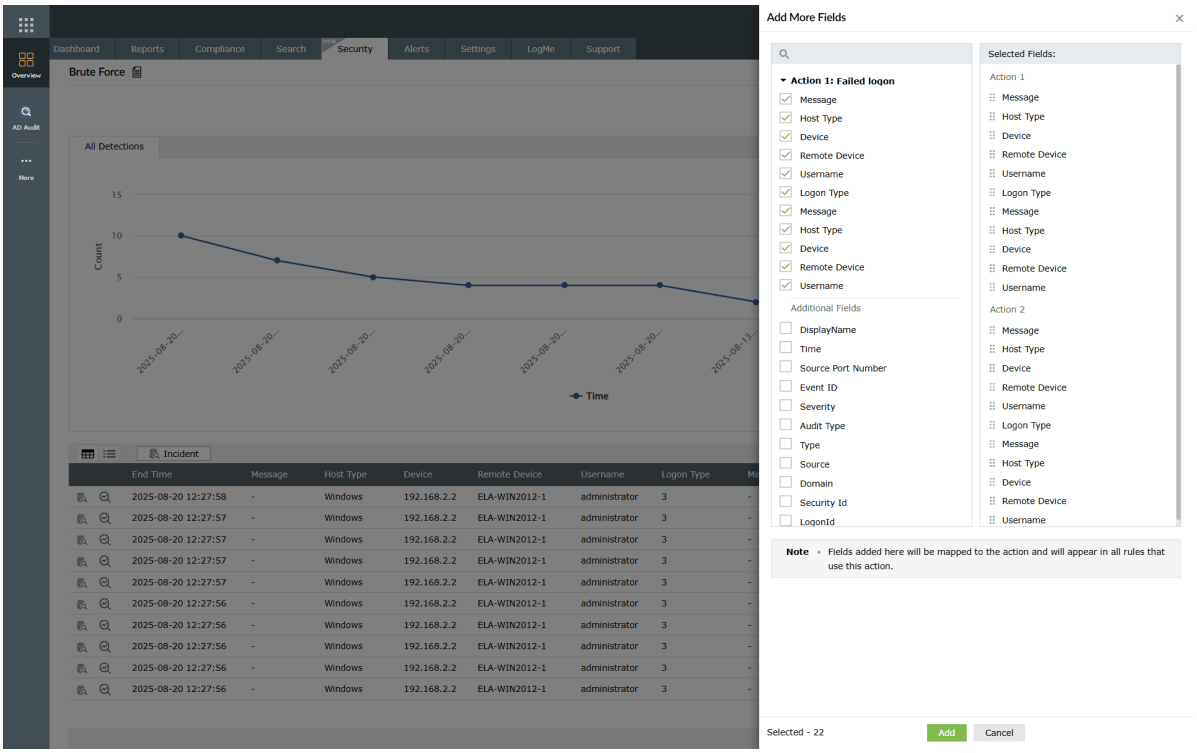
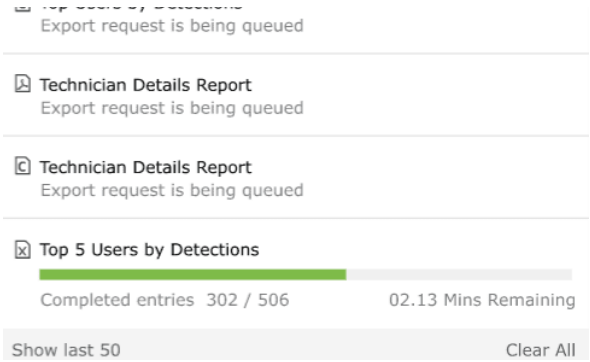


Image 14: Rule detection details columns in the manage rules module

Available actions in the detections module:

- Clicking on the button allows you to choose a format to export the said data either in a PDF format or a CSV file.
- Clicking on the Report export history icon allows you to view the complete history of the past data exports that have taken place for that particular report.





- You can also customize the time range for the detection by clicking on



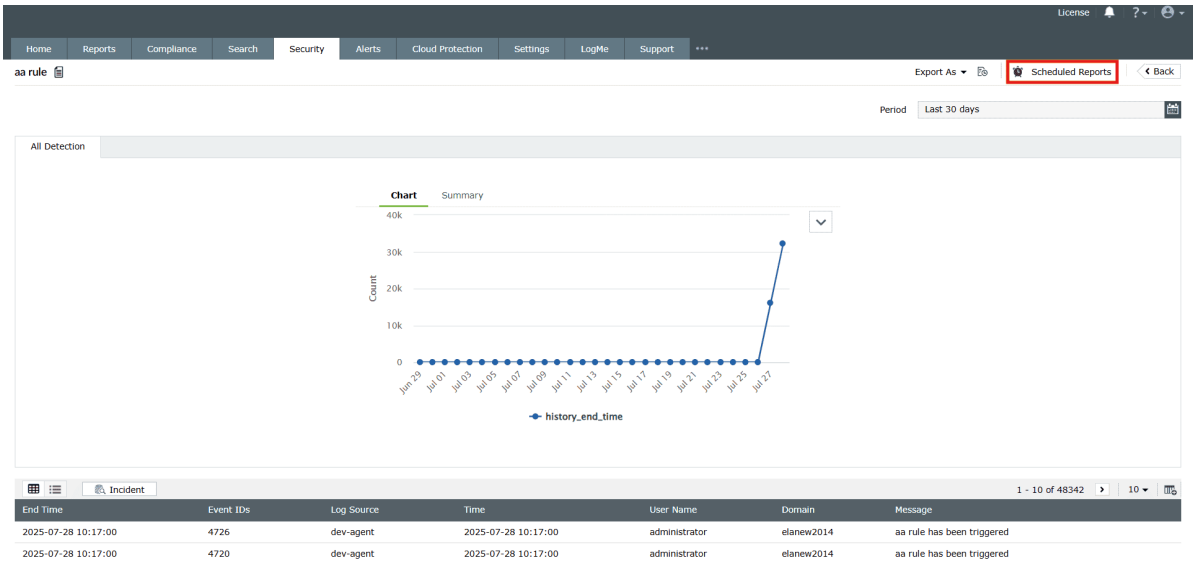
You can:

- Select the start date and end date for your desired time range.
- Click on any of the predefined time ranges available that suits your requirements.
- Click on Custom range and then proceed to enter a number in the box provided below that will represent the past number of days worth of data you wish to view.
- Click on Apply.

Scheduled Reports

> NOTE
>
> You can access the detection reports from the Manage Rules module directly. Read Scheduled Detection Reports to learn more.

1. Click on the Scheduled Reports option as highlighted below.



2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered

Image 15: Rule scheduled reports in the manage rules module

2. The available schedules for those rule reports (if any) will be shown on the screen.
3. You can create a schedule for a particular rule by following the steps below:

- Click on Create Schedule as highlighted below.

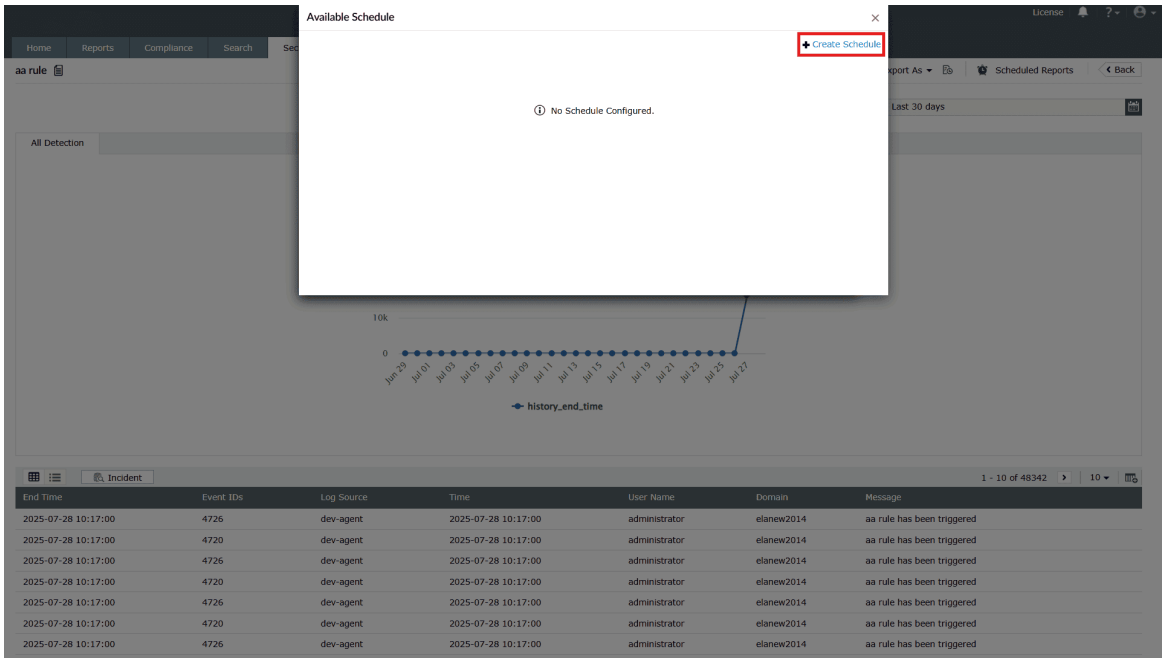
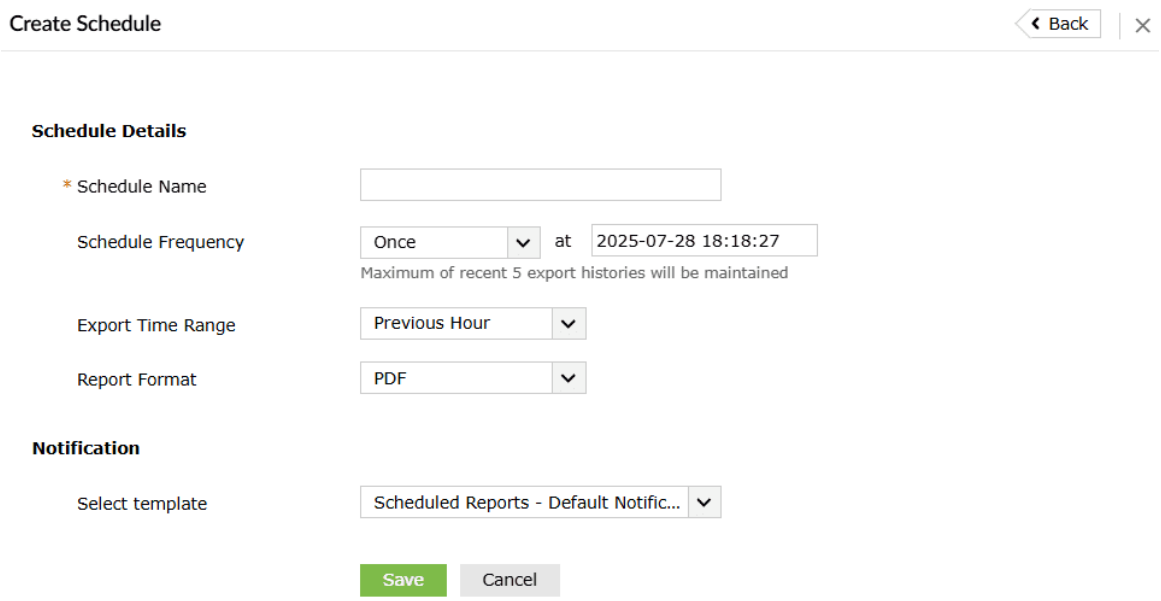
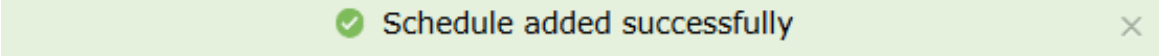


Image 16: Create scheduled reports in the manage rules module

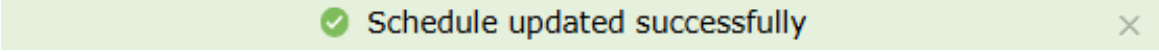
- Upon clicking, the pop-up will display the fields to Create Schedule.



- Fill the necessary fields:
  - Schedule Details
    - Schedule Name: Assign a unique name to the schedule.
    - Schedule Frequency: Define how often the schedule should run (hourly, daily, weekly, or monthly).
    - Export Time Range: Specify the time range of data to include (e.g., last 24 hours, last 7 days, or custom).
    - Report Format: Choose the preferred format for the exported report (PDF, CSV, XLS).
  - Notification
    - Select Template: Pick a predefined report template or customize one.
- After configuring the schedule, click on Save. Upon successful completion, the schedule is updated in the pop-up box, along with a confirmation message.



- You can also edit the schedule by clicking on the edit icon in the pop-up box. The same fields appear for editing.
- Edit and click on Update. Upon successful completion, the schedule is updated in the pop-up box, along with a confirmation message.



Read also

This document explained how to navigate the Manage Rules page, perform key actions on rules, view detailed rule summaries, tune performance, and generate detection reports for deeper analysis.

- Rule management overview
- Understanding rules
- Creating custom rules
- Query grammar
- Scheduled detection reports

10.1.2.5. Query grammar

Last updated on: September 12, 2025

In this page

- Overview
- Basic Criteria
- Datatypes
- Numerical relational operators
- String relational operators
- Logical Operators
- Example
- Query Syntax
- Advanced operator
- isMalicious function
- isVulnerable function
- misConfiguredFor function
- Query components
- Aggregation Function
- Sort Operator
- Timewindow Operator
- Groupby Operator
- Distinct Operator
- Having Operator
- First/Last Operator
- With Operator
- Order of Statements
- Lookup criteria
- Correlation criteria
- Arithmetic operator
- Correlation multi-action
- Link statement
- Sequence statement
- Def and Filter statement

Select statement

Use case specific examples

Detection rule limitation

Overview

Query Grammar is the language you can use while building the Query Syntax that the ML (Machine Learning) model understands and helps you build rule criteria and rule parameters during advanced rule creation.
This page contains the complete query grammar reference, including basic criteria, supported datatypes, relational and logical operators, advanced functions, aggregation constructs, correlation statements, and practical detection examples.

Basic Criteria

1. Datatypes
2. Numerical relational operators
3. String relational operators
4. Logical Operators
5. Example

1. Data types

Type name	Description	Examples
String	A string value	"surname" "198.51.100.255" "Number of bytes"
Int	An integer value	23 -32 4000000244553
Float	A floating-point number.	3.14 -1.2e5
Timespan	A time interval represented by one or two digits followed by 's' for seconds, m'for minute. 'h' for hour, 'd' for days, 'w' for week, 'M'for month, 'q'for quarter, 'y'for year.	2s, 45m, 4h, 2d, 3w, 2M, 4q, 1y
Memory	A data size represented in 'B' for bytes, "KB' for kilobytes, 'MB' for megabytes, 'GB' for gigabytes 'TB' for terabytes, 'PB' for	2B, 3KB, 3 MB,

Type name	Description	34GB, 9TB, 9PB Examples
Date-time	A date-time format represented by "YYYY-MM-DD", "YYYY-MM-DD HH-MM-SS"	"2000-08-30" "2000-08-30 15:45:06"
IP	An IP value	"10.13.29.70" "127.0.0.1/16"

2. Numerical relational operators

Operators	Description	Supported data types	Examples
>	Greater than	Int, Float, Memory, IP	source_IP > 10.53.12.0
>=	Greater than or Equal to	Int, Float, Memory, IP	source_ip < 10.53.12.0
<	Less than	Int, Float, Memory, IP	source_IP < 10.53.12.0
<=	Less than or Equal to	Int, Float, Memory, IP	source_IP <= 10.53.12.0
=	Equal to	String, Int, Float, Memory, IP	EventID=4624
!=	Not Equal to	String, Int, Float, Memory, IP	EventID!=4624
in/IN	Equals to one of the elements	String, Int, Float, IP	EventID in (4624,4625)
notin/NOTIN	Not equals to any of the elements	String, Int, Float, IP	EventID notin (4624,4625)
isExist	Field isn't an empty string, and it isn't null.	For all fields	For all fields

Operators	Description	Supported data types	Examples
isNotExist	Field is an empty string, and it is null.	For all fields	isNotExist(source_ip)

3. String relational operators

Operators	Description	Examples
=	Equal to	username = "name"
!=	Not Equal to	username != "name"
contains/CONTAINS	Returns true if the field has a set of data	eventname contains "success"
notcontains/NOTCONTAINS	Returns true if the field hasn't set of data	eventname notcontains "success"
startswith/STARTSWITH	Returns true if the field value starts with data	username startswith "Ja"
endswith/ENDSWITH	Returns true if the field value ends with data	username endswith "kumar"
notstartswith/NOTSTARTSWITH	Returns true if the field value does not start with data	username notstartswith "Ja"
notendswith/NOTENDSWITH	Returns true if the field value does not end with data	username notendswith "kumar"
matches/MATCHES	Returns true if the field value matches the regex	username matches "pree*"
notmatches/NOTMATCHES	Returns true if the field value does not match the regex	username notmatches "pree*"
=	Equal to	username = "name"

4. Logical Operators

Operators Operators	Description Description	Examples Examples
AND/and	Returns true only if both condition are true	username = "preethi" and eventid=4624
OR/or	Returns true if either of the condition is true, regardless of the other condition.	eventid = "4688" or eventid = "592"

Example

- Basic Criteria for Repeated failed SUDO commands:logtype="unix" and iename = "sudo command execution failed"
- Basic Criteria for Excessive password change failure:common_report_name = "user account password changes" and severity = "failure" or iename = "password update failure"
- Basic Criteria for Ryuk Wake on LAN Command:logtype in ("Windows", "Fortinet", "Sonic wall") and (eventid = "4688" or eventid = "592") and (commandline contains "8 lan" or commandline contains "9 rep")
- Basic criteria for window failed logon:logtype = "Windows" and actionname = "Failed logon"
- Basic criteria for success logon:actionname = "Success logon"

NOTE:

- logtype will contain values such as *(include all logtype), Windows, Unix, Cisco, etc.
- Using actionname operator, we can use predefined actions in the query.

Query Syntax

The query language supports different operators and clauses. Below is the complete syntax reference.

1. Base syntax:

action_name:
logtype = (* | windows | syslog | ...) [logical_operator basic_criteria ...] with [aggregate_func(fieldname), ...]
Example: eventid = 4624

2. Sorting:

| sort fieldname (asc | desc)

3. Histogram:

| histo fieldname range(initial, initial to end) sort [aggregateField | count] (asc | desc)

4. Time window:

| timewindow value unit sort [aggregateField | count] (asc | desc) limit value having count operator value

5. Grouping:

| groupby fieldname with [aggregate_func(fieldname), ...] sort [aggregateExpr | count] (asc | desc) limit nums having [aggregateExpr | count] comparison_operator nums

> NOTE:
>
> - Operators inside the brackets (groupby, histo, etc.) may appear in any order.
> - The timeslice operator can occur only once.
> - The groupby and histo operators can occur up to three times in any order.

6. Distinct:

| distinct fieldname sort (asc | desc) limit [1-200] having count operator value

7. Post-processing:

| having aggregateExpr operator value [logical_operator (aggregateExpr operator value)]
| isanomalous(field, model, field)

8. First and last:

| first [1-10] fieldname [, fieldname ...]
| last [1-10] fieldname [, fieldname ...]

9. Lookup:

| lookup <event-field> in <lookup-table.lookup-field> set <event-destfield> AS <lookup-table.lookup-destfield>

10. Definitions:

def: variable_name = <expression>
Supported types: int, string, float, time, boolean

11. Filtering:

filter: <condition>
This removes results that do not match the condition.

12. Event sequence:

follow: actionname1 followedby | notfollowedby actionname2 within [1-60] (millisecond | second | minute | hour | day)
Example: correlation-based detection of one event followed by another within 10 minutes.

13. Selection:

select action_name.field, action_name.fields, def_name

Advanced operator

1. isMalicious function
2. isVulnerable function
3. misConfiguredFor function

1. Is Malicious

- The 'isMalicious' condition is available only for IP address fields. It checks if the detected IP address is present in the predefined list of malicious IP addresses stored in the internal database.
- This function returns true or false.

Syntax: isMalicious(fieldname)
Example: External Remote Services
Failed Logon From Public IP:
logtype = "*" and eventid = 4625 and isExists(remoteip) and isMalicious(remoteip)

2. Is Vulnerable

- Available only after integration with Endpoint Central and can be used with device fields. Checks if a device is tagged as vulnerable in Endpoint Central and identifies devices vulnerable to specific attacks (e.g., CVE-2023-38831).
- This function returns true or false.

> NOTE:
>
> This operator is available only for EventLog Analyzer's continuous execution mode.

Syntax:
isVulnerable(fieldname)
isVulnerable(fieldname , matchvalue)
Examples:
A. Microsoft Outlook Vulnerability Exploitation
Outlook connecting to webDAV or SMB Share:
logtype = "windows" and eventid = 4656 and objectname contains "\REGISTRY\MACHINE\SYSTEM" or objectname contains "Services" or objectname contains "WebClient\NetworkProvider,LanmanWorkstation\NetworkProvider" and accesslist contains "ReadData (or ListDirectory)" and isVulnerable(Device Name, "CVE-2023-23397")
| groupby processname
Suspicious webDAV client execution via Rundll.exe:
logtype = "sysmon" and iename = "Sysmon Process Creation" and parentprocessname contains "svchost.exe" and parentprocesscommandline contains "-s WebClient" and processname contains "rundll.exe" and processname = Outlook connecting to webDAV or SMB Share.processname

B. AWS Failed logon
Error events:
logtype = "aws cloudtrail" and isVulnerable(errorcode)

3. MisconfiguredFor

Available only after integration with Endpoint Central and can be used with device fields. Detects devices with misconfigurations identified by Endpoint Central (e.g., Windows Credential Guard disabled).

> NOTE:
>
> This operator is available only for EventLog Analyzer's continuous execution mode.

Syntax:
misConfiguredFor(fieldname , match_value)
Examples:
A. Built-in guest account privilege escalation
Successful Network Guest Logon:
logtype = "windows" and eventid = 4624 and username contains "Guest" and logontype = 3 and MisconfiguredFor(Devicename, "Built-in guest account is not disabled or properly restricted")
| groupby logonid
B. Privileged Operation Attempt:
logtype = "windows" and eventid = 4672 and logonid = Successful Network Guest Logon.logonid and MisconfiguredFor(Devicename, "Built-in guest account is not disabled or properly restricted")
C. User Account Local Group Membership change Attempt:
logtype = "windows" and eventid = 4732 and groupname contains "Administrators" and logonid = Successful Network Guest Logon.logonid and MisconfiguredFor(Devicename, "Built-in guest account is not disabled or properly restricted")

Query components

- Aggregation Function
- Sort Operator
- Timewindow Operator
- Groupby Operator
- Distinct Operator
- Having Operator
- First/Last Operator
- With Operator
- Order of Statements

1. Aggregation Function

Function	Description	Syntax	Example	Output
SUM	• Returns the sum of the selected values in the field. • Returns a single numerical value.	sum(field) or SUM(field)	sum(bytes_in)	3.27mb (3,432,605)
AVG	• Returns the average of the values in the field. • Returns a single numerical value.	avg(field) or AVG(field)	avg(_zl_timestamp)	1.36kb (1,393.156)
MAX	• Returns the maximum value in the field. • Returns a single numerical value.	max(field) or MAX(field)	max(received_bytes_i)	107.61kb (110,196)
MIN	• Returns the minimum value in the field. • Returns a single numerical value.	min(field) or MIN(field)	min(received_bytes_i)	107.61kb (110,196)
STDEV	• Returns the standard deviation of the given field. • Returns a single numerical value.	stdev(field) or STDEV(field)	stdev(_zl_timestamp)	2.46kb (2,521.297)
	• Returns the number of log messages that match the query. • With "with"			

Function	Description	Syntax	Example	Output
COUNT	• With "with" operator → returns a number. • With "having" operator → returns a boolean (true/false).	count	having count > 100	true/false
DCOUNT	Returns the count of distinct values. With "with" operator → returns a number. With "having" operator → returns a boolean (true/false).	dcount(field) or DCOUNT(field)	having dcount(_zl_host) > 2	true/false

2. Sort Operator

- Sorts all results by specified fields.
- By default results are sorted by count descending.
- After "sort", only non-aggregate fields are allowed.
- Syntax: sort fieldname1 (asc/desc) [, fieldname2 (asc/desc) ...]
- Example:
  - logtype="windows" and eventid = 4625 | sort username asc, hosttype desc

3. Timewindow Operator

- Groups logs into specified slices of time.
- After "sort", only aggregate fields are allowed.
- Max limit value for group by keyword is 1000.
- Possible timewindow units: y (year), M (month), w (week), d (day), h (hour), m (minute), s (second).
- Syntax: timewindow value unit sort [aggregateField, count] (asc/desc) limit value having count operator value
- Examples:
  - logtype="windows" | timewindow 5m
  - logtype="windows" | timewindow 5m sort count desc
  - logtype="windows" | timewindow 1h sort sum(bytes_in) as totalBytes asc
  - logtype="windows" | timewindow 1h sort timewindow desc
  - logtype="windows" | timewindow 5m limit 5
  - logtype="unix" and eventid = 4625 | timewindow 10m limit 10 having count > 100
  - logtype="windows" | timewindow 10m | group by username

- logtype="windows" | timewindow 10m | groupby username

4. Groupby Operator

- Used to get unique values of a field.
- When multiple groupby fields are given, the first is primary and second is secondary.
- After "sort", only aggregate fields are allowed.
- Maximum limit for groupby is 1000.
- Syntax: groupby fieldname1 with aggregateField sort [aggregateField, count] [asc/desc] limit [1-1000] having aggregateExpr operator value
- Examples:
  - logtype="unix" | groupby username sort sum(sent_bytes_i) as total desc
  - logtype="unix" | groupby username sort sum(sent_bytes_i) as total desc limit 10 | groupby hostname
  - logtype="unix" | groupby username sort sum(sent_bytes_i) as total desc limit 10 | groupby hostname with sum(sent_bytes_i) as total
  - logtype="windows" and eventid = 4625 | groupby username having count > 100
  - logtype="windows" and eventid = 4625 | groupby username having avg(sent_bytes) as average > 10 MB
  - logtype="windows" | groupby username limit 20 | groupby hosttype having avg(sent_bytes_i) as average > 10MB | groupby hostname having sum(received_bytes_i) as total < 500 MB

5. Distinct Operator

- Fetches a table with only distinct values.
- Only one distinct field is allowed.
- Distinct field can only be sorted by count.
- Max limit for distinct = 200.
- Syntax: distinct fieldname sort (asc | desc) limit [1-200] having count operator value
- Examples:
  - logtype="windows" | distinct zuid
  - logtype="windows" | distinct zuid sort asc
  - logtype="windows" | distinct zuid limit 150
  - logtype="windows" | distinct location having count > 5

6. Having Operator

- Post-result operator. Used for outer aggregation conditions.
- Syntax: having aggregateExpr operator value [logical operator (aggregateExpr operator value)]
- Examples:
  - logtype="unix" and eventname contains "logon" | having count > 120

- logtype="windows" and eventid = 4625 | having avg(sent_bytes) as average > 10 MB

7. First/Last Operator

- First operator returns the earliest logs, last operator returns the most recent logs.
- Either first or last can be used.
- Limit can be used with first/last.
- Maximum limit = 10.
- Syntax: first/last [1-10] fieldname1 (, fieldname2, ...)
- Examples:
  - logtype="windows" | groupby status | first 2 request_uri,remote_ip
  - logtype="windows" | groupby status | last 2 request_uri,remote_ip

8. With Operator

- Aggregate expression can be used in basic criteria and group operators.
- Syntax: with aggregateExpr (, aggregateExpr ...)
- Examples:
  - logtype="windows" and with sum(sent_bytes) as bytesSum, avg(received_bytes) as average | groupby srcip
  - logtype="windows" and | groupby srcip with sum(sent_bytes) as bytesSum, avg(received_bytes) as average

9. Order of Statements

| basic_criteria with field.aggregate_func [, field.aggregate_func, ...]
| sort field (asc/desc)
[| histo fieldname range(initial, initial to end) sort [aggregateField, count] [asc/desc]
| timewindow value limit value
| groupby field sort aggregate(field) (asc/desc) limit number]
| distinct field
| first/last [1-10] fieldname
| having (groupby_field.field / timewindow.count operator /
groupby_field.distinct_field.aggregate/aggregate_func.field) operator value
NOTE:

- Operators inside brackets may occur in any order.
- Timewindow can occur only once.
- Groupby and histo can occur up to three times in any order.

Lookup criteria

Lookup query

The lookup operator lets you fetch extra information from a lookup table.
It matches event field names and values with lookup table field names.

- If "set" is not used → it works like lookupcontains (checks if a key exists). It returns True/False.
- If "set" is used → it fetches values from the lookup table and stores them in fields you choose.

Syntax:

lookup event-field in lookup-table.lookup-field [and/or more conditions] (set lookup-table.lookup-destfield as newfield)

Examples:

- logtype = windows and eventid = 4625 → lookup username in user_details.user
- logtype = windows and eventid = 4625 → lookup username in user_details.user set user_details.ip_address as ip, user_details.port as port
- logtype = windows and eventid = 4625 → lookup username in user_details.user and device in user_details.hostname set user_details.ip_address as ip, user_details.port as port

Correlation criteria

1. Arithmetic operator
2. Correlation multi-action
3. Link statement
4. Sequence statement
5. Def and Filter statement
6. Select statement

1. Arithmetic operator

Operator	Description	Example
+	Add	timestamp + 3600000ms > 4800000
-	Subtract	timestamp - 3600000ms > 2400000
*	Multiply	ratio = (failure_event.count / access.count)
/	Divide	ratio = (failure_event.count / access.count) * 100

2. Correlation (Multi-Action)

- You can define multiple actions (e1, e2, etc.) with conditions.
- Each action must have basic criteria. Aggregate functions and lookups are optional.

- Syntax: actionname : basic_criteria | aggregate criteria | lookup_criteria | correlation_criteria
- Examples:
  - e1: logtype = cisco and common_report_name in (unix user added, firewall user added, user account created, computer account created)
  - e2: logtype = cisco and common_report_name in (computer account deleted, user account deleted, unix user deleted, firewall user deleted) and hosttype = e1.hosttype and targetuser = e1.targetuser and _zl_timestamp between e1._zl_timestamp and (e1._zl_timestamp + 3600000ms)

3. Link statement

- The link statement compares whether one action's field matches or does not match another action's field.
- You can combine it with other conditions using AND / OR / NOT.
- Syntax: fieldname (operator) actionname.fieldname [and/or more comparisons]
- Examples:
  - Brute force login
    - e1: logtype = windows and event_name = failed windows login | groupby username | groupby devicename
    - e2: logtype = windows and event_name = successful windows login and username = e1.username and devicename = e1.devicename
    - Sequence: e1 followedby e2 within 10m
    - Select e1.username, e2.devicename
  - Anomalous user account change
    - e1: logtype = windows and common_report_name in (unix user added, firewall user added, user account created, computer account created)
    - e2: logtype = windows and common_report_name in (computer account deleted, user account deleted, unix user deleted, firewall user deleted) and hosttype = e1.hosttype and targetuser = e1.targetuser and time >= e1.time
    - Select e1.hosttype, e1.targetuser

4. Sequence statement

- Defines whether one action follows or does not follow another within a specific time.
- You must always specify the time frame.
- Syntax: sequence : action1 (followedby / notfollowedby) action2 within time [and action2 followedby/notfollowedby action3 ...]
- Examples:
  - File Access Without Authorization
    - e1: logtype = windows and eventid = 4663 (object access attempt)
    - e2: logtype = windows and eventid = 4656 (handle requested)
    - Sequence: e1 notfollowedby e2 within 5m

- Select e1.username, e1.devicename
- Brute Force Login
  - e1: logtype = windows and event_name = failed windows login | groupby username | groupby devicename
  - e2: logtype = windows and event_name = successful windows login and username = e1.username and devicename = e1.devicename
  - Sequence: e1 followedby e2 within 10m
  - Select e1.username, e2.devicename
- Ragnar Locker ransomware detection
  - e1: logtype = windows and processid = 4688 and processname = msiexec.exe
  - e2: logtype = windows and eventid = 4654 and objectname contains Program Files(X86) and endswith VirtualAppliances\va.exe and devicename = e1.devicename
  - e3: logtype = windows and processid = 4688 and processname = e2.objectname and devicename = e1.devicename
  - Sequence: e1 followedby e2 within 30m followedby e3 within 2m
- Suspicious SQL Backup Activity
  - e1: logtype = windows and eventid = 4625 | distinct devicename
  - e2: logtype = windows and eventid = 4624 and devicename = e1.devicename and username = e1.username
  - e3: logtype = mssql and actionid = lgis
  - e4: logtype = * and action = ba
  - Sequence: e1 followedby e2 within 10m and e3 followedby e4 within 5m

5. Def and Filter statement

Def statement

- The def statement calculates an expression and puts the resulting value into a search results field.
- It is used to create a new field in your search results, and the values in that new field are the result of an expression.
- In a def statement, you can only get the overall count, average, or sum, such as action count or action-based field aggregation like 'e1.count' or 'e1.sent_bytes.sum'.
- Syntax: def: variable_name = actionname. (count / field.aggregate_function) operator actionname. (count | field.aggregate_function / value)

Filter statement

- The filter operator keeps only the records that match the filter criteria.
- The def statement field constraints will apply to the filter statement.
- Syntax: filter: (def_variable_name / actionname. (count / field.aggregate_function)) operator value

Example: Ratio of two events:

- access: logtype="windows" and
- failure_event: logtype="windows" and and
- def: ratio = count(failure_event) / count(access)
- def: percent = ratio * 100
- filter: percent > 50
- Select ratio, count(failure_event), count(access)

6. Select statement

- Select is used to display fields or aggregates you want to see in results.
- Syntax: select fields, aggregates
- Examples:
  - Excessive logon failures
    - e1: logtype = windows and common_report_name in (router logon failed, unix logon failed, firewall logon failed, logon failed, vpn logout, firewall logoff, failed cloud logon) | groupby username
    - Select e1._zl_timestamp, e1.hostname
  - Anomalous user account change
    - e1: logtype = windows and common_report_name in (unix user added, firewall user added, user account created, computer account created)
    - e2: logtype = * and common_report_name in (computer account deleted, user account deleted, unix user deleted, firewall user deleted) and hosttype = e1.hosttype and targetuser = e1.targetuser and _zl_timestamp between e1._zl_timestamp and (e1._zl_timestamp + 3600000ms)
    - Select e1._zl_timestamp, e1.log_uuid, e2._zl_timestamp, e2.log_uuid
  - Excessive VPN logon failure
    - failed_logon: logtype = * and eventtype = vpn_logon_failure | distinct username having count > 5
    - Select failed_logon.username, count(failed_logon)
  - Suspicious file access
    - file_access: logtype = windows and eventid = 4663 | groupby username | groupby objectname having count > 3
    - file_modified: logtype = windows and eventid = 4663 and type = modify and username = file_access.username and objectname = file_access.objectname
    - Sequence: file_access followedby file_modified within 5m
    - Select file_access.username, file_modified.objectname, count(file_access.objectname)

Use case specific examples

Below are practical examples of how query grammar can be applied to detect common security scenarios. Each

example shows the query logic, supported operators, and output fields.

1. Successful Logon

Description: Detects successful logon events in Windows.
Query:

```
logtype = "Windows"
and eventid = 4624
and message contains "successful logon"
```

2. Excessive Failed Login attempts

Description: Flags usernames or devices with excessive failed login attempts.
Query:

```
logtype in ("windows", "unix")
and eventid = 4625
| groupby username
| groupby devicename having count > 10
```

3. Brute Force Login detection

Description: Detects brute-force attempts where multiple failed logins are followed by a successful login for the same user on the same device within a short time window.
Query:
Step 1 – Failed Logins (e1):

```
e1:
logtype = "windows"
and event_name = "Failed Windows Login"
| groupby username
| groupby devicename
```

Step 2 – Successful Login (e2):

```
e2:
logtype = "windows"
and event_name = "Successful Windows Login"
and username = e1.username
and devicename = e1.devicename
```

Sequence Logic:

```
e1 followedby e2 within 10m
```

Final output:

```
select e1.username, e2.devicename
```

4. Port Scanning attack

Description: Identifies devices or IPs scanning multiple ports within a short period.
Query:

```
e1:
logtype in ("unix", "windows", "sysmon")
and event_name = "allowed connection"
| groupby remoteip
```

| groupby host
| groupby port having count > 100
select e1.host, count(e1.host)

5. Data Exfiltration detection

Description: Detects unusually high outbound data transfer volumes.
Query:
netlog:
logtype = "unix"
and event_name = "allowed connection"
| groupby srcip
| groupby destip having sum(sentbytes) > 100MB
select netlog.srcip, netlog.destip, sum(netlog.sentbytes)

6. Ratio of Failed vs. Successful events

Description: Calculates the percentage of failed access events compared to total access events.
Query:
Step 1 – Total Access events:
access:
logtype = "*"
and type = "access"
Step 2 – Failed Access events:
failure_event:
logtype = "*"
and type = "access"
and status = "failure"
Define ratio:
def: ratio = (failure_event.count / access.count) * 100
Filter high failure rate:
filter: ratio > 50
Final output:
select ratio, access.count, failure_event.count

Detection rule limitation

Detection rule limitations specify the functional constraints and operator support across ELA and L3C correlation modes.
The below table details differences in supported operators, thresholds, aggregations, and query constructs between scheduled and continuous detection rules.

Feature	Description	EventLog Analyzer scheduled correlation	EventLog Analyzer continuous correlation	Log360 Cloud scheduled correlation	Log360 Cloud continuous correlation

Feature	Description	EventLog Analyzer IP range not supported correlation	EventLog Analyzer All operators continuous supported correlation	Log360 Cloud IP range not supported correlation	Log360 Cloud All operators supported correlation
Numerical relational operator	Basic comparisons (>, <, =, !=, >=, <=, in, not in, exists, not exists, between, not between)				
String relational operator	Text-based comparisons (contains, not contains, starts with, ends with, matches, not matches)	Matches and Not matches not supported	All operators supported	Matches and Not matches not supported	All operators supported
Logical operator	Logical conditions (and, or)	All supported	All supported	All supported	All supported
Advanced operator	Security checks (isMalicious, isVulnerable, misconfiguredFor)	Only isMalicious supported	All supported	None supported	Only isMalicious supported
Link to statement	Links actions in the criteria builder	Multiple + nested criteria supported	Multiple supported; nested not supported	Multiple + nested criteria supported	Up to 3 criteria supported; nested not supported
Threshold limits	Threshold count limit	No limit	Max limit 999	No limit	Default limit 10 (can be increased)
IN operator value limit	Max number of terms inside IN	25	25	25	25
Aggregation functions	Aggregates (sum, avg, max, min, stdev, percentile, count, distinct)	All supported	Only count and distinct supported	All supported	Only count and distinct supported
WITH operator	Use of aggregate functions in basic criteria	Up to 10 terms	Not supported	Up to 10 terms	Not supported
Sort operator	Sort results by fields	Supported (max 5	Not supported	Supported (max 5	Not supported

Feature	Description	EventLog Analyzer scheduled correlation	EventLog Analyzer continuous correlation	Log360 Cloud scheduled correlation	Log360 Cloud continuous correlation
Time window operator	Sets time-based threshold	Up to 7 days; max 200	No limit (time window not supported)	Up to 1 day; max 200	Default 1 hour (extendable); time window not supported
Histo operator	Histogram functionality	Not supported	Not supported	Not supported	Not supported
GroupBy operator	Group fields in criteria	Max 3 fields	No limit	Max 3 fields (with restrictions)	Max 3 fields
Distinct operator	Distinct count in threshold/query	Only 1 distinct field (no sort/limit)	Only 1 distinct field (no sort/limit)	Only 1 distinct field (no sort/limit)	Only 1 distinct field (no sort/limit)
Max GroupBy + Distinct	Limit on combined use	Max 3 groupby + 1 distinct	Multiple groupby + 1 distinct	Either (max 2 groupby + 1 distinct) or (max 3 groupby + 0 distinct)	Max 3 groupby + 1 distinct
First/Last operator fields	Returns first or last record	Max 10 fields	Not supported	Max 10 fields	Not supported
isAnomalous operator	UEBA anomaly detection	–	–	–	–
Arithmetic operator	Arithmetic in queries	Supported	Not supported	Supported	Not supported
Maximum action limit	Number of actions allowed	Up to 10	Up to 10	Up to 3	Up to 3

Sequence statement Feature	Ordered event checks (followed by / not followed by) Description	Up to 7 days EventLog Analyzer scheduled correlation	Up to 30 days EventLog Analyzer continuous correlation	Up to 1 day Log360 Cloud scheduled correlation	Up to 1 hour Log360 Cloud continuous correlation
Def statement	Create new calculated fields	Max 10	Not supported	Max 10	Not supported
Filter statement	Keep records matching condition	Max 10	Not supported	Max 10	Not supported
Select statement	Choose fields (alias in scheduled rules only)	Max 20	Max 20	Max 20	Max 20
Query length	Maximum characters per query	10000	10000	10000	10000
Anomaly action in advanced rule	Cannot combine anomaly with threshold/groupby/distinct/link criteria	–	–	–	–

Read also

This document explained how query grammar supports advanced rule creation, from defining criteria with operators and functions to applying correlation logic and building practical detection use cases.

- Rule management overview
- Understanding rules
- Creating custom rules
- Managing rules
- Scheduled detection reports

10.1.2.6. Scheduled detection reports

Last updated on: September 12, 2025

In this page

Overview

Scheduled detection reports

Overview

The Scheduled Detection Reports feature in the Manage Rules module provides a way to generate and export periodic reports for rule-based detections. Administrators can create new schedules, define frequency, select rules, configure export formats, and set notifications. These reports provide detailed visibility into detections over a specified time range, helping with trend analysis, compliance requirements, and continuous monitoring.

Scheduled detection reports (via the Manage Rules module)

Provides logs detected for a particular rule over a specified period of time.

1. You can access these reports by clicking on the Scheduled Detection Reports option in the Manage Rules module as highlighted below.

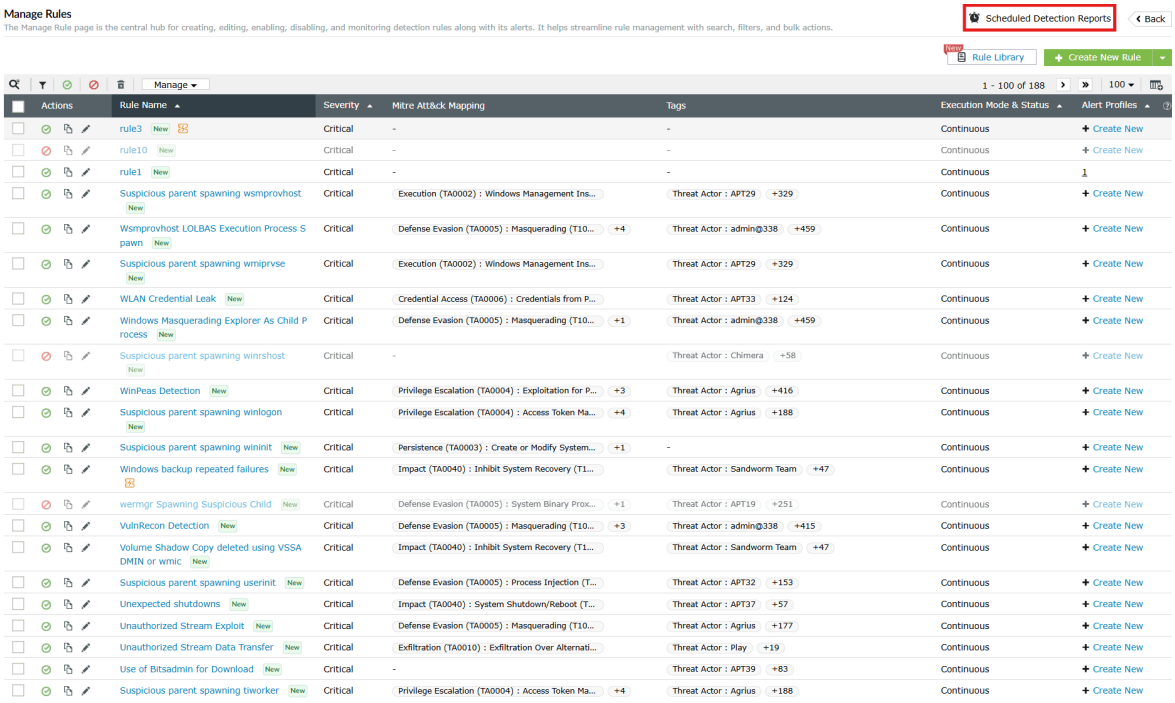


Image 1: Scheduled reports in the manage rules module

2. You will be taken to the Scheduled Reports module.

To create a new schedule for the report(s)

1. Click on the Create New Schedule button as highlighted below.

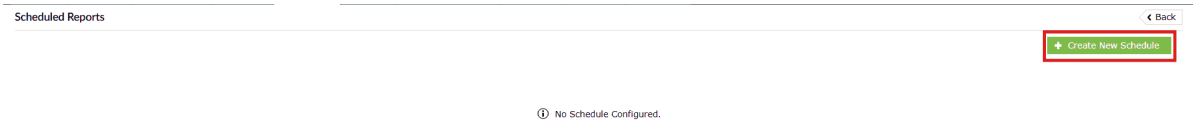


Image 2: Create scheduled reports in the manage rules module

2. You will be taken to the Create Schedule module.

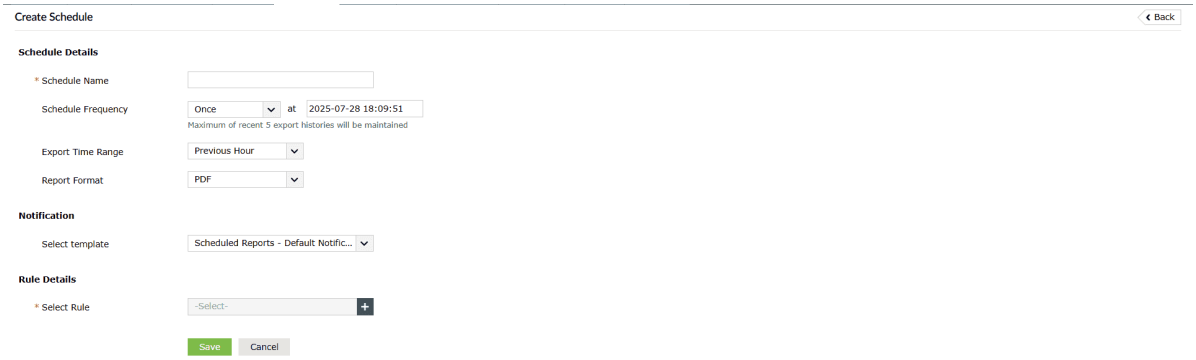


Image 3: Create scheduled reports in the manage rules module

- Schedule Details
  - Schedule Name: Assign a unique name to the schedule.
  - Schedule Frequency: Define how often the schedule should run (hourly, daily, weekly, or monthly).
  - Export Time Range: Specify the time range of data to include (e.g., last 24 hours, last 7 days, or custom).
  - Report Format: Choose the preferred format for the exported report (PDF, CSV, XLS).

- Notification
  - Select Template: Pick a predefined report template or customize one.
- Rule Details
  - Select Rule: Choose the anomaly rule(s) you want to associate with the schedule. Reports and alerts generated will be based on the selected rules.

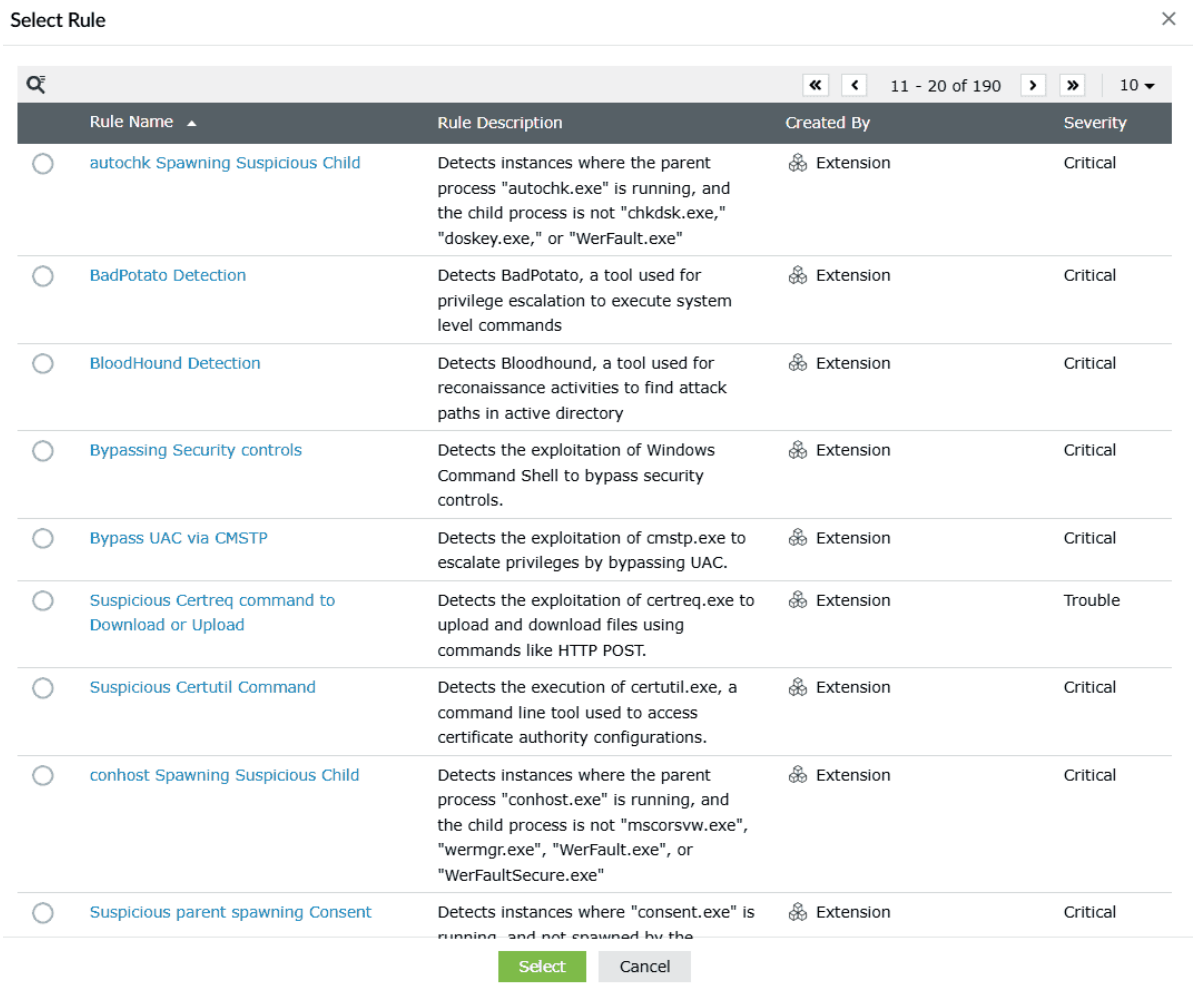
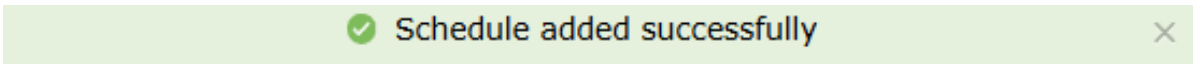


Image 4: Create scheduled reports in the manage rules module

3. Click on Save after making all the required configurations. Upon successful completion of action, the below pop-up appears.

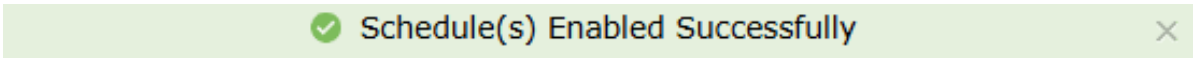


To enable/disable a schedule for report(s)

To enable/disable a schedule for report(s)

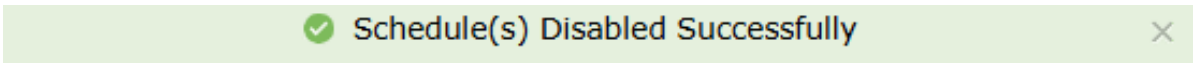
Enabling a schedule

1. Click on the currently disabled icon under the Actions column to enable the schedule.
2. As soon as you perform this action, the icon indicates that the schedule is now enabled and the below pop-up message appears briefly.



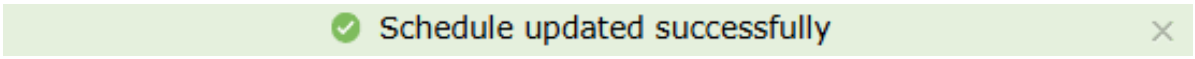
Disabling a schedule

1. Click on the currently enabled icon under the Actions column to disable the schedule.
2. As soon as you perform this action, the icon indicates that the schedule is now disabled and the below pop-up message appears briefly.



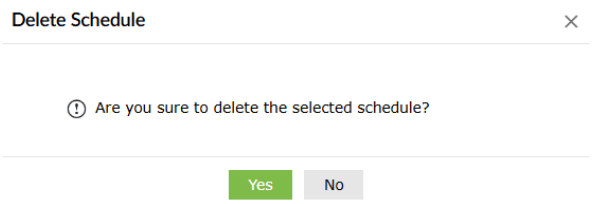
To edit a schedule for report(s)

1. In the Scheduled Reports module, click on the edit icon under the Actions column.
2. The Edit Scheduled Reports module appears on the screen.
3. Make the necessary edits and click on the Update button. Upon successful completion of action, the below pop-up appears.



To delete a schedule for report(s)

1. In the Scheduled Reports module, click on the delete icon under the Actions column.
2. A Delete Schedule pop-up appears to confirm the action. Click on Yes.



3. Upon successful completion of action, the below pop-up appears.



Read also

This document explained how to schedule detection reports, configure report details and notifications, and manage actions like enabling, disabling, editing, or deleting schedules.

- Rule management overview
- Understanding rules
- Creating custom rules
- Query grammar

- Managing rules

10.1.3.1. Object filtering for Active Directory for rule fine tuning

Last updated on: September 12, 2025

In this page

Overview

Feature Scope

Object Selection and Filtering

Active Directory object filter behaviors

Prerequisites

Workflow architecture

Use cases

Limitations

Overview

The object-filter based rule fine-tuning for Active Directory enables you to optimize the detection rules by applying it specifically to certain AD objects to reduce false positives, alert fatigue and improve the rule accuracy. Using this intuitive object-filtering interface, the solution lets you to you can define users, groups or OUs (Organizational Units), interactive through GUI (Graphical User Interface). This ensures monitoring adapts automatically to directory changes, simplifies rule deployment, and improves alert relevance.
With re-engineered detection, object filters reduce alert fatigue for SOC teams by helping them fine-tune detections to specific users, groups, or OUs, reducing false positives and ensuring alerts stay actionable.

> NOTE
>
> Currently, the object filter capability is available only for pre-defined Windows and Active Directory rules.

Feature scope

The Object FIlter feature is accessible from the below modules:

- Rule library
- Rule management
- Alerts

Object selection and filtering

Object selection and filtering

Object selection methods

1. Direct object selection

- You can select objects directly using Active DirectorySync data.
- The selection remains static for the chosen objects unless modified again.

2. Group or OU (Organizational Unit) based object selection

- Instead of selecting objects directly, you can assign specific OUs or groups.
- Membership objects within the OU or group are dynamically assigned based on the Active Directory sync data.

3. Manual values

- You can define manual values apart from value selection in the domain.
- The entered object name in manual values will be matched against criteria across all domains

Field specific object filters

Field	Available object filter options
User	User, Group based user, OU based user
Computer	• Computers, or • DCs (Domain Controllers), Member servers, Workstation
Group	Group, OU based group
OU	OU

Active Directory object filter behaviors

1. Domain object sync in the filter

Object syncing behavior varies based on the selected tabs in the object filter:

- Direct object selection
  - Sync is performed only for the selected object type.
- OU-based object selection
  - Sync includes both the OU and the associated object types within it.
  - For example, if it is OU-based user selection, both the OU and the user objects are synced accordingly.
- Group-based object selection
  - Membership sync is required to resolve group memberships accurately.

- As per the framework design, this involves syncing User, Computer, OUs and Group objects as mandatory components to complete the membership resolution process.

2. Domain selection in the Filter

Domain behavior in the object filter depends on the feature usage context:

- In Alert Profiles
  - Domains listed in the object filter are based on the selected domains in the alert profile.
- In Rules
  - All available domains are listed in the object filter.

Selection behaviors

- Empty checkbox
  - If no objects are selected for a domain, No objects selected will be displayed with an empty checkbox.
- Partial selection
  - If some objects are selected, the domain checkbox appears partially selected.
  - The object count is displayed, and only those selected objects are used for object matching.
- Full selection
  - If the checkbox is fully selected, it indicates that all objects from the domain are included for matching.
  - All Users (or the applicable object type) is displayed.
- No domain configured
  - If no domains are configured, Add Domain Manually will be displayed.

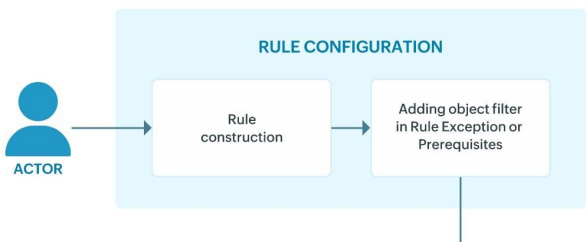
Prerequisites

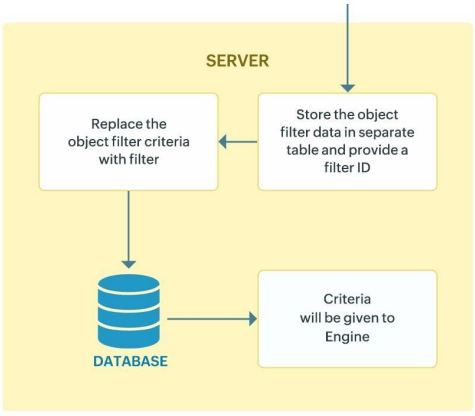
License coverage details

- Direct object selection & manual values are accessible to those with Free and Basic plans.
- Group-based object selection and OU-based selection is accessible to those with a Standard plan subscription or higher tiers.

Workflow architecture

The following diagram illustrates the workflow of how the Object Filter operates. For clarity, the instance highlights its implementation within the Rule Management module.





Use cases

1. Automated alert customization with group & OU-based filters

Use case
Security teams and other key operational divisions often struggle with high alert noise because rules apply broadly across all users and devices, generating unnecessary signals from non-critical accounts.
With object filtering
Analysts can assign rules to specific OUs or security groups, ensuring only critical accounts and systems are monitored. Membership updates are synced dynamically via Active Directory, eliminating the need for manual rule edits. This allows the various operational teams to maintain focus on sensitive entities while cutting down false positives from routine operations.

2. Streamlined rule deployment across business units

Use case
Global organizations with distributed Active Directory environments face challenges when deploying uniform rules since objects vary across regions and business units.
With object filtering
Rules can be installed with OU-based user grouping, automatically pulling the correct set of objects per region. This enables region-specific monitoring without separate configurations, reduces administrative overhead, and ensures each division has accurate, localized detection coverage.

3. Exception handling for authorized administrative actions

Use case
Routine IT maintenance tasks (e.g., patching, group policy updates) frequently overlap with suspicious behavior patterns and trigger unnecessary alerts.
With object filtering
The Exceptions section lets teams exclude trusted accounts, devices, or OUs from rule conditions. By suppressing benign activity, SOCs can prioritize high-fidelity alerts without compromising visibility into sensitive changes elsewhere.

Limitations

- General
  - Object filter is available only for the Equals and NotEquals operators.
  - Object filter works on the latest synced domain data. If changes occur in Active Directory but are not yet synced, the filter processes data based on the last synced state.
- Alerts and rules
  - Object Selection: Maximum of 25 objects per domain for a field

Read also

This document explained how the Active Directory-based object filtering works, including selection methods, behaviors, prerequisites, and common use cases. You also learned how it helps cut alert noise, streamline deployments, and handle exceptions effectively.

- Accessing and applying object filtering in Log360

10.1.3.2. Accessing and applying object filtering

Last updated on: September 12, 2025

In this page

Overview

Implementing object-filtering via

Rule library

Rule management

Alerts

Overview

Object filtering capability lets you refine rules using intuitive GUI (Graphical User Interface), for optimized functionality by allowing you to apply the rules for specific users, groups, or OUs (Organizational Units) of Active Directory for improved results. This helps ensure that monitoring and exceptions target the right entities without unnecessary noise.

> NOTE
>
> The object filter capability is available only for pre-defined Windows and Active Directory rules.

Implementing object-filtering

Object filtering can be applied at different points in the product to refine rule and alert configurations. You can set filters during rule installation via the Rule Library, adjust them in Rule Management by configuring Objects and Exceptions, apply them while enabling rules, and configure them within Alerts for precise monitoring.

Rule library

The solution lets you configure object filters for the rules even at the time of installation from the Rule Library. To do this,

1. Access the solution's web console, navigate to the Security tab to access the Security Analytics Dashboard and click on Manage Rules in the top-right corner.

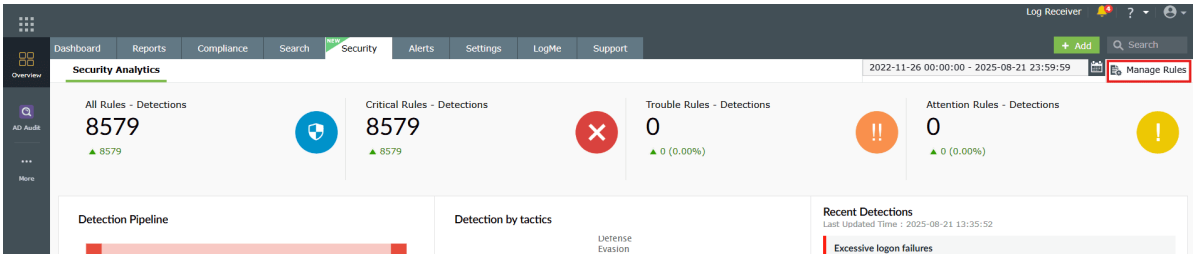




Image 1: Security dashboard widgets

2. In the Manage Rules module, click on Rule Library.

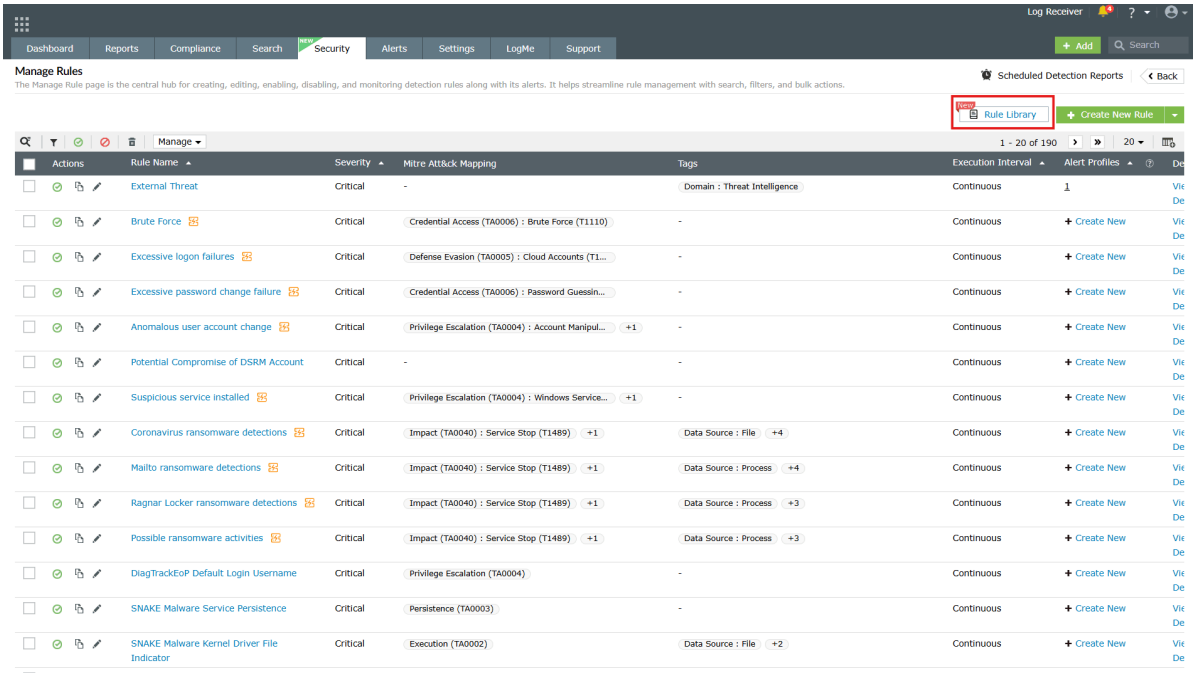
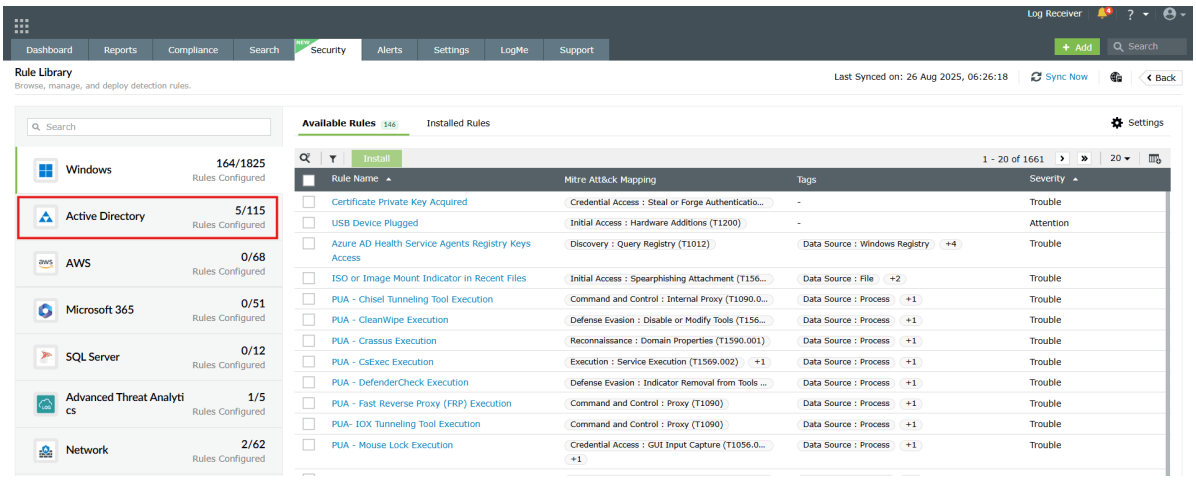


Image 2: Rule library in manage rules module

3. The object filter is available for both Windows and Active Directory rules. Click on the Active Directory category available in the left pane if you wish to apply the filter for these rules in specific.



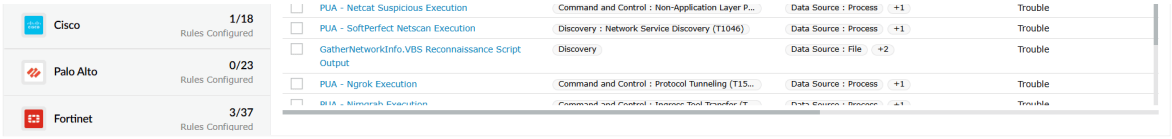


Image 3: Rule library in manage rules module

4. Click on the required rule name. You can use the search feature available to find the rule quickly.

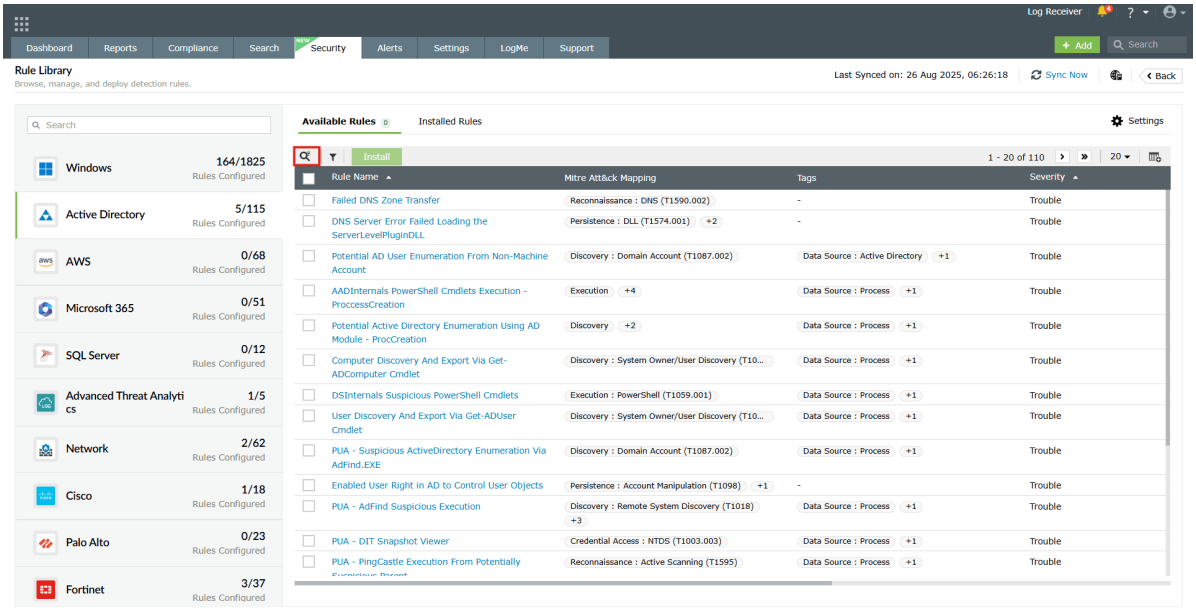


Image 4: Rule library in manage rules module

5. Clicking on the rule prompts open the Rule Summary box and the install button. Click on Install.

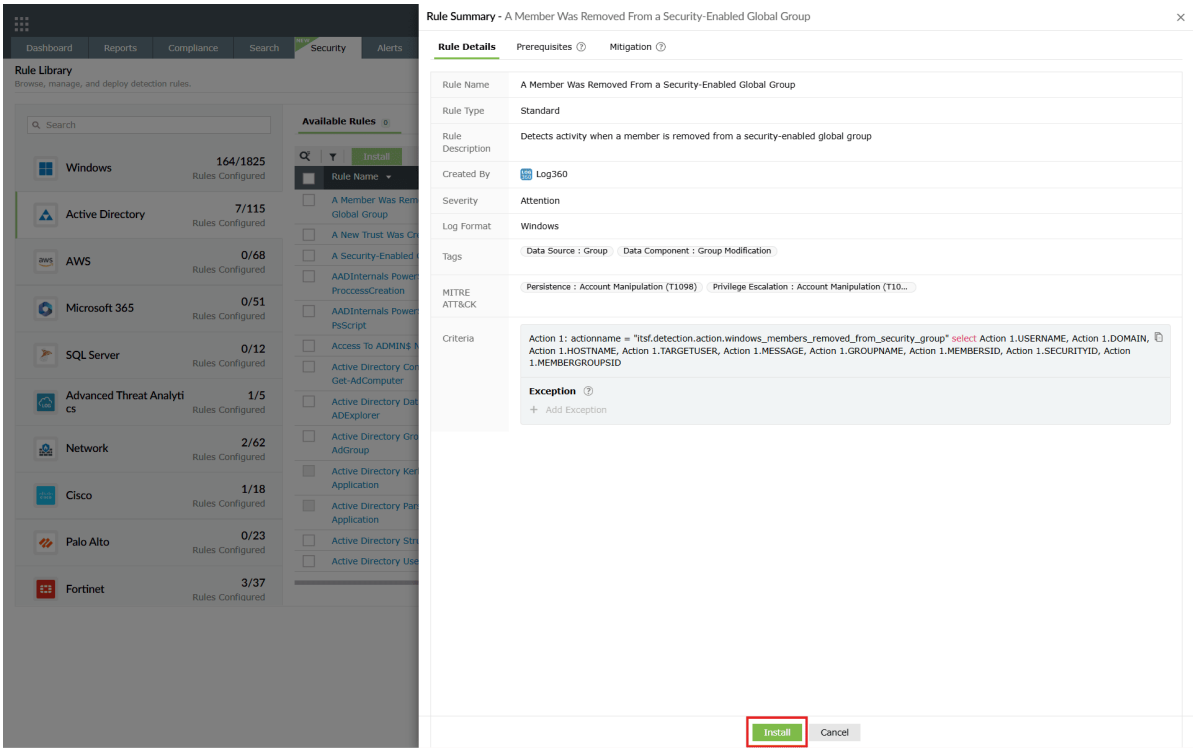


Image 5: Rule details in rule library

6. After clicking on Install, the Install Rules box slides open. Click on the add icon as highlighted below.

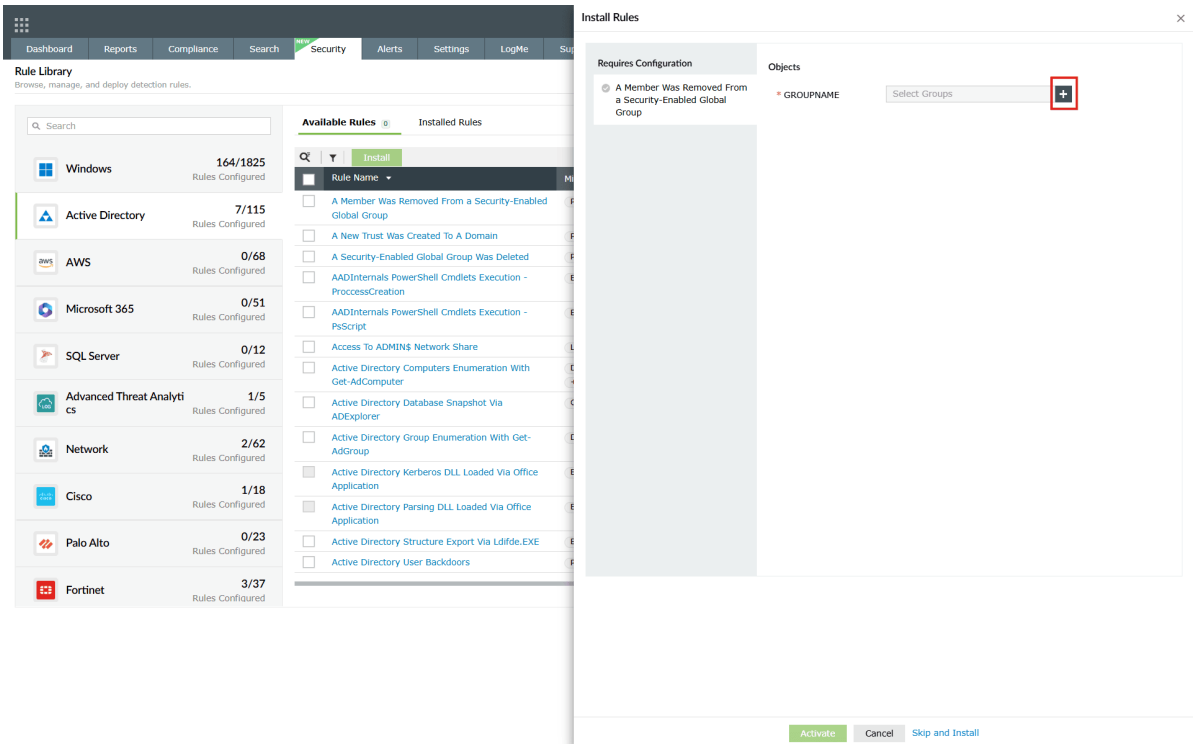


Image 6: Object filter in rule details in rule library

> **NOTE**
>
> You can choose to skip the below process by clicking on the Skip and Install option available in the Install Rules panel.

7. You will be taken to the Groups sub-tab displayed along with the object filter feature in order to be able to filter and choose what groups of users you wish to group under this rule before installation itself.

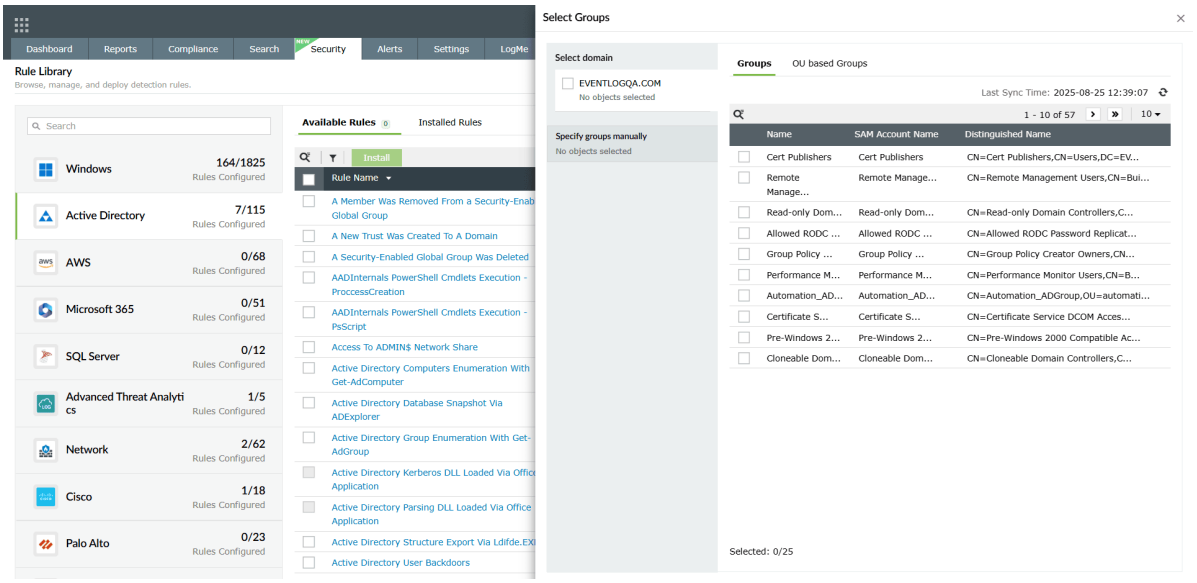




Image 7: Applying object filter in rule details in rule library

8. Similarly, the OU based Groups sub-tab also includes the filter for user selection.

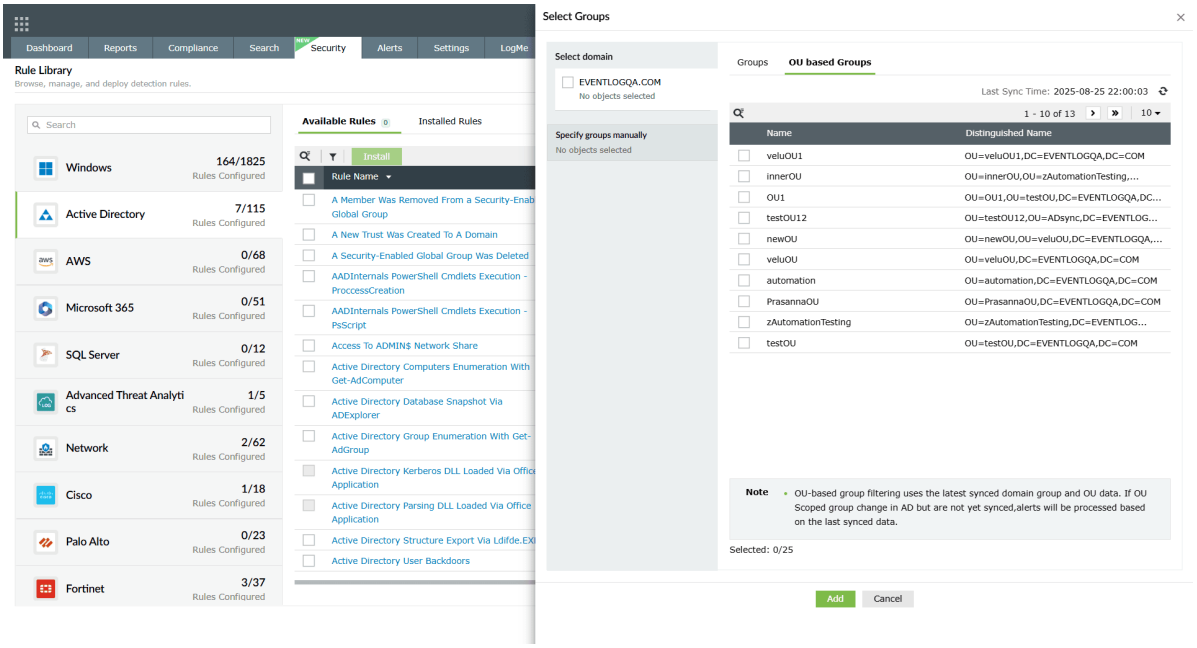


Image 8: Applying object filter in rule details in rule library

9. After selecting the preferred groups, you can view your selection by clicking on the View option below.

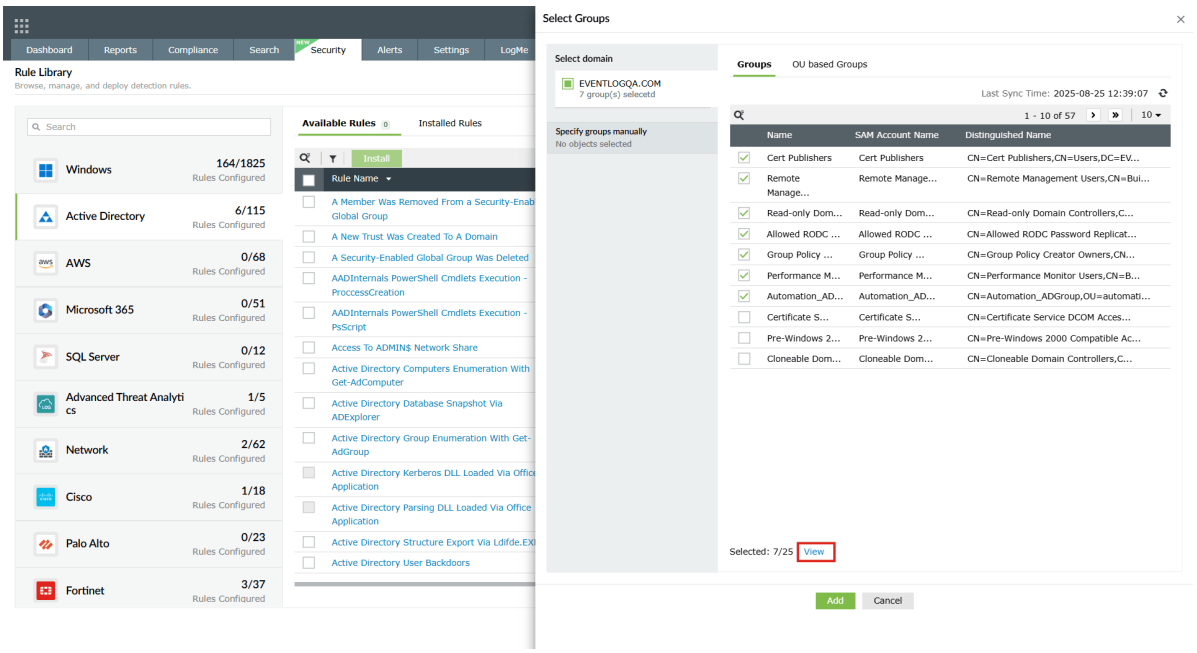
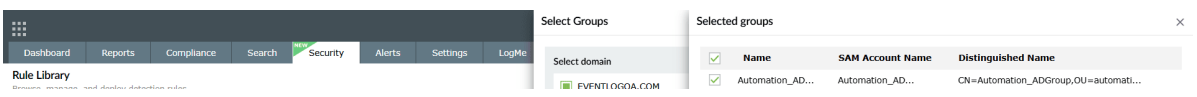


Image 9: Viewing the object filtering list

10. The list of selected user groups will be displayed.



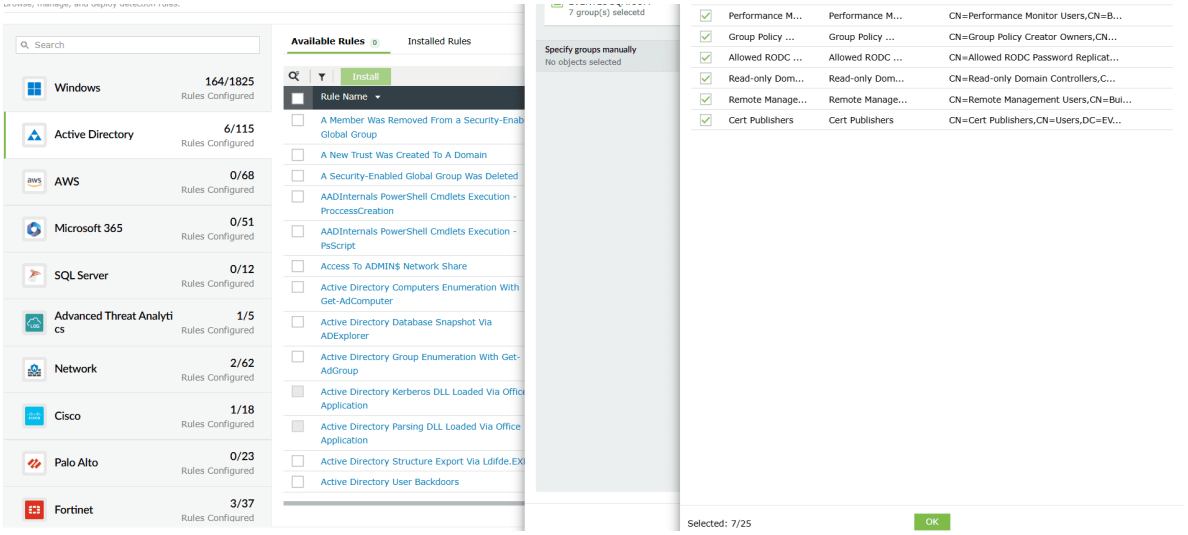


Image 10: Viewing list of configured object filter users/groups

11. Once the selection is done, click on OK in the selection list and then click on Add in the Select Groups pane. The Install Rules pane will display the Requires Configuration section with a green check mark.

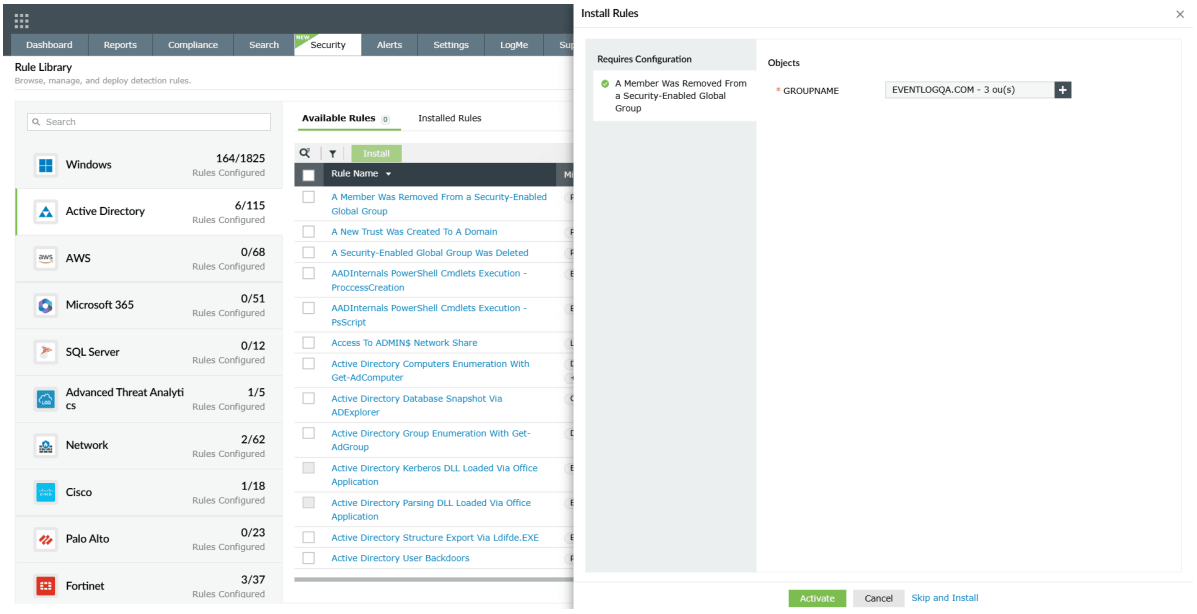
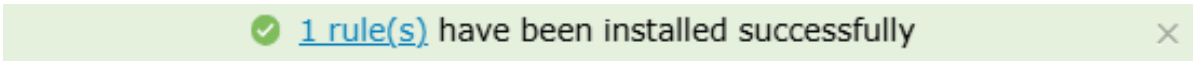


Image 11: Configuring object filter users/groups

12. Click on the Activate button. Upon successful completion of the action, the below pop-up appears.



To learn more about the Rule Library, refer to the help document.

Rule management

The solution allows you to configure or update object filters for existing rules through the Rule Management module. The filters can be applied in both the Objects and Exception sections of a rule's summary. To do this, follow the steps below:

1. In your account, navigate to the Security tab to access the Security Analytics Dashboard and click on Manage Rules in the top right corner.

Rules in the top-right corner.

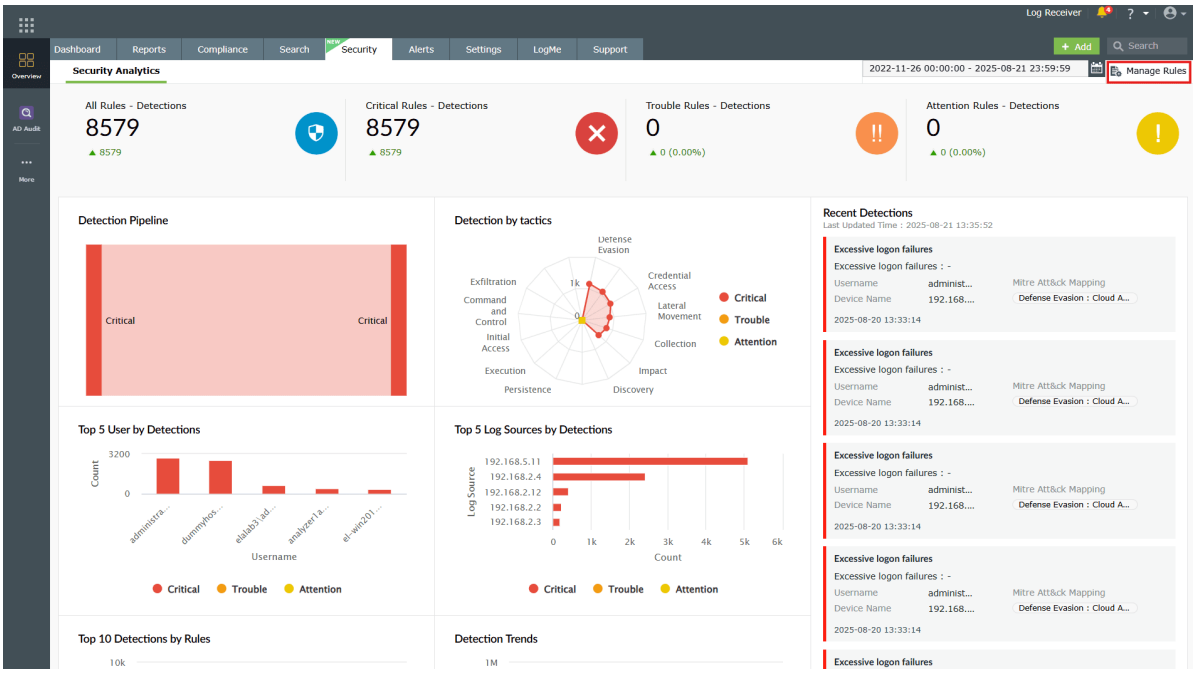


Image 12: Manage rules in the security dashboard

2. You will be taken to the Manage Rules module.

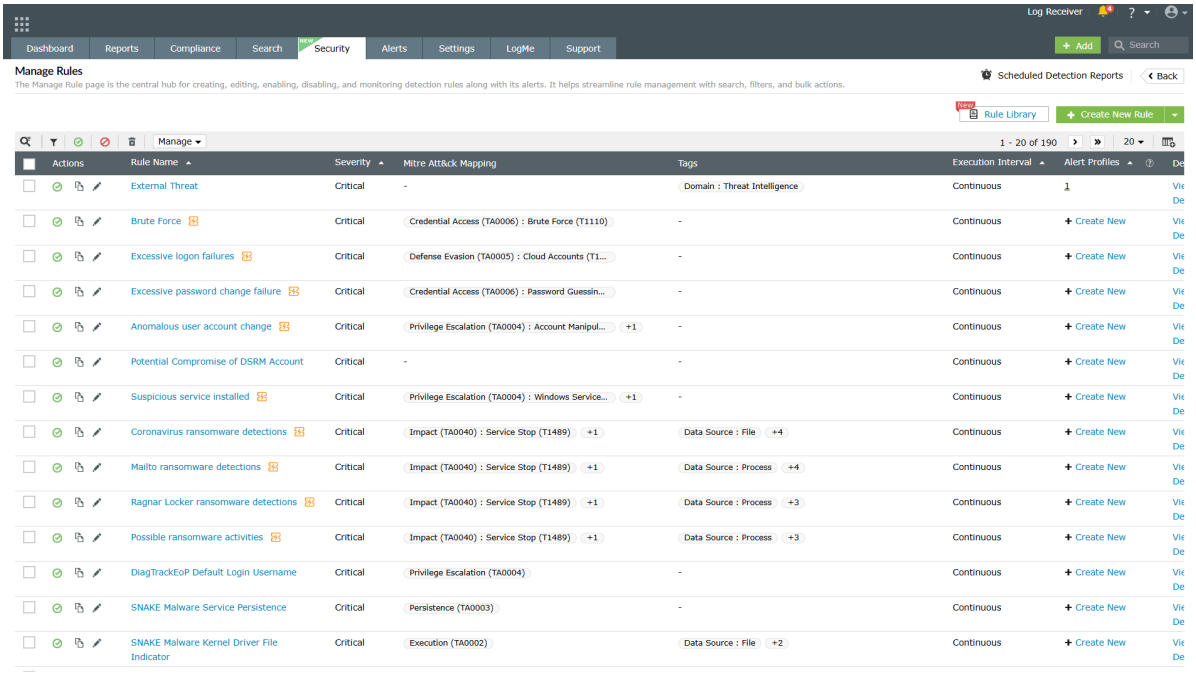
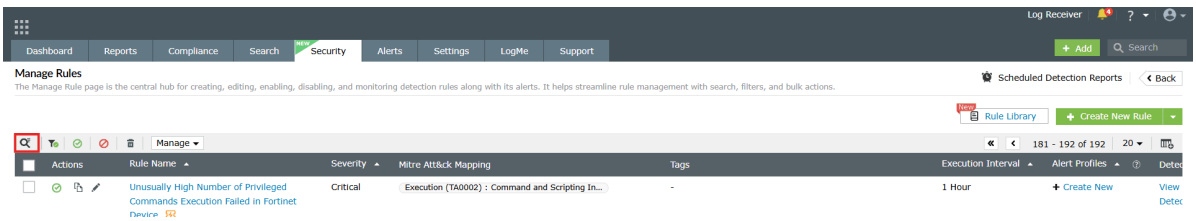


Image 13: Manage rules module

3. Click on the required rule name. You can use the search feature available to find the rule quickly.



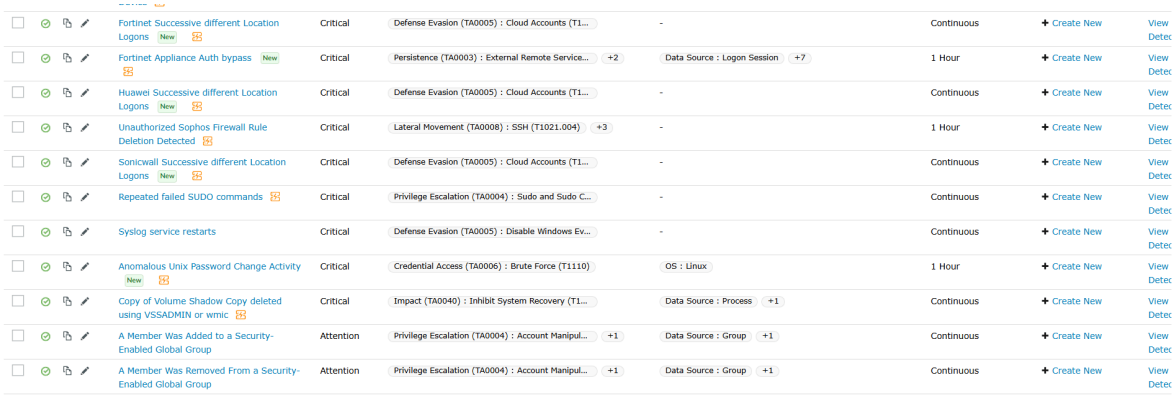


Image 14: Search option in manage rules module

4. Upon clicking on the rule name, the Rule Summary box slides open. The object filter feature is available for the below sections in the Rule Details sub-tab of Rule Summary.
   - Objects
   - Exception
   - Enabling rule

A. Objects section

1. Navigate to the Criteria section as highlighted below and click on the edit icon in Objects.

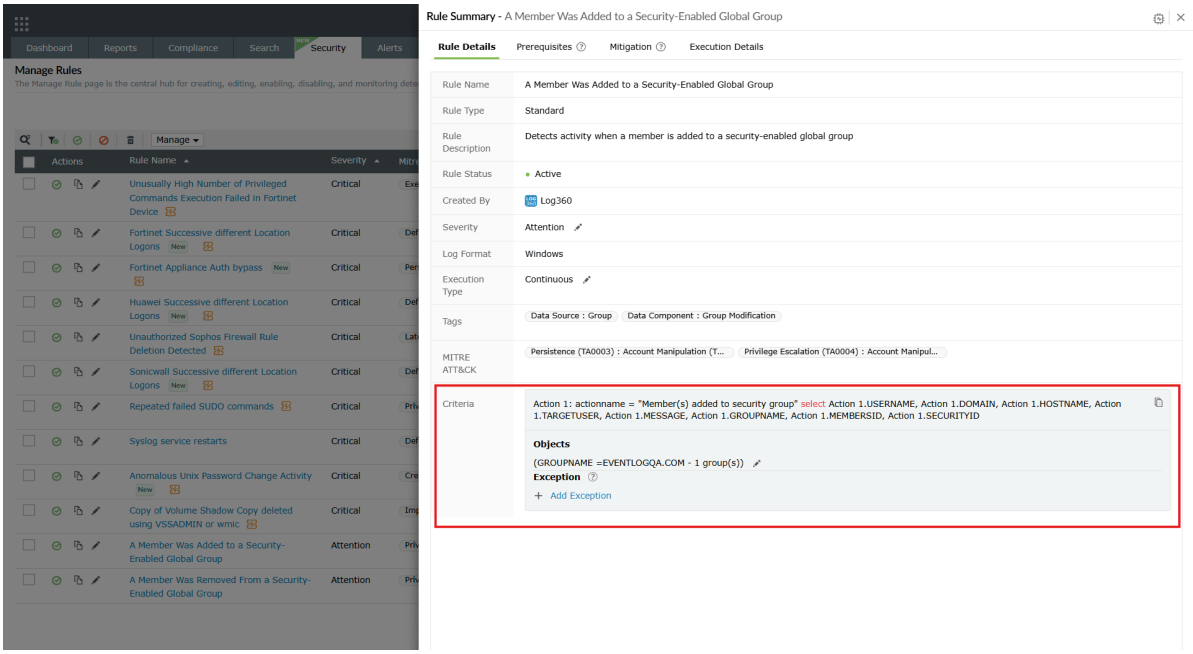


Image 15: Object filtering in rule summary in manage rules module

> NOTE
>
> - The edit icon will be available only if you have previously selected user groups during rule installation from the Rule Library.
> - In the case where you had chosen to Skip and Install rule, in the above mentioned Objects

field in the Criteria section, the option Add Objects will be visible. Click on it to access the object filter and follow the steps mentioned below to select user groups.

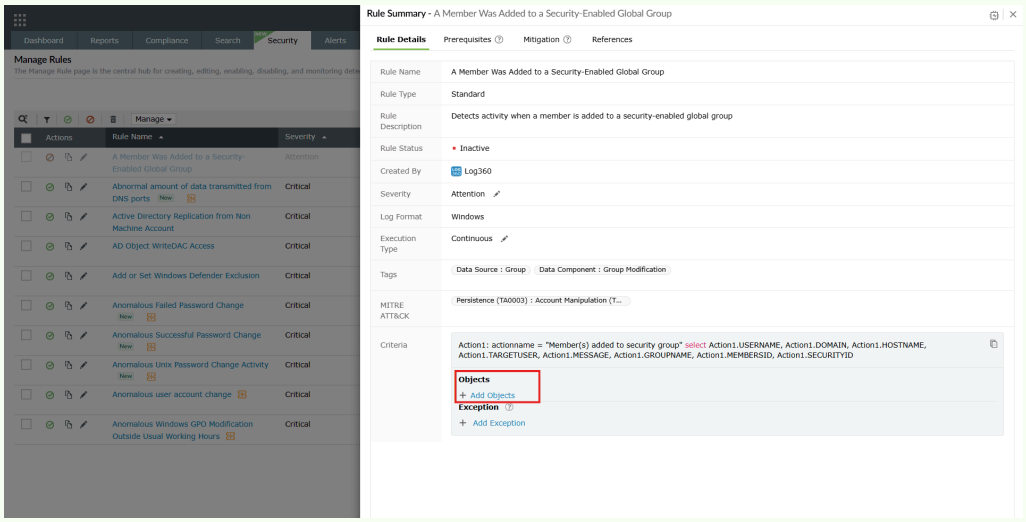


Image 16: Adding objects in rule summary

2. The Add Object pane slides open. Click on the add icon as highlighted below.

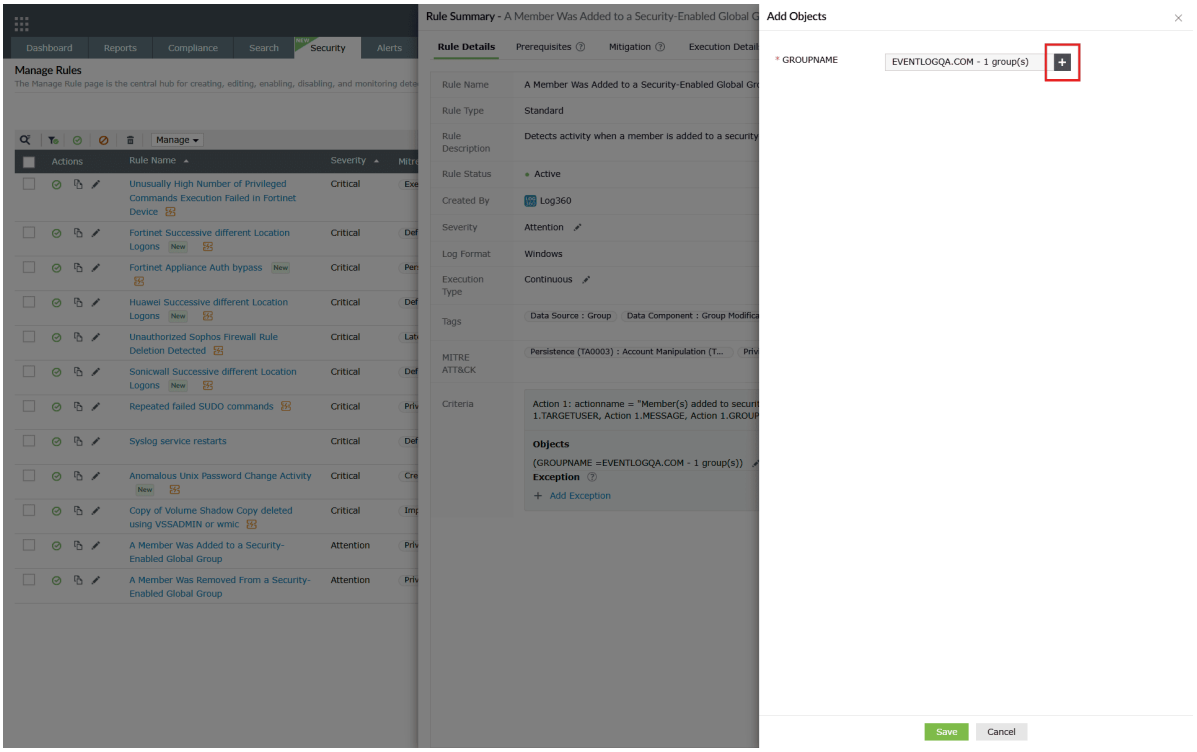
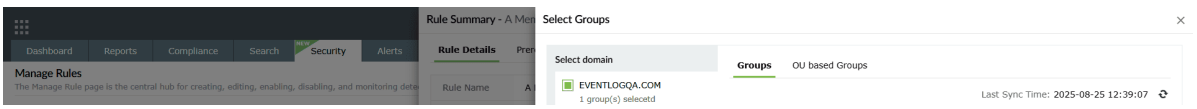


Image 17: Object filtering in rule summary

3. The Select Groups pane slides open. You will be taken to the Groups sub-tab displayed along with the object filter feature in order to be able to filter and choose what groups of users you wish to group under this rule.



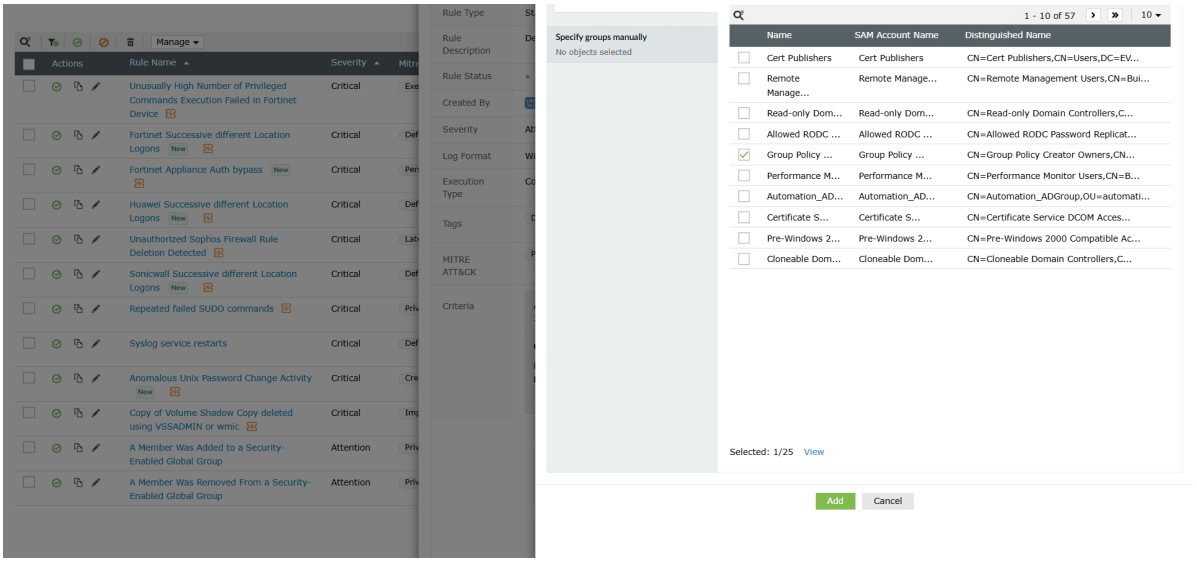


Image 18: Object filtering in rule management

4. Similarly, the OU based Groups sub-tab also includes the filter for user selection.

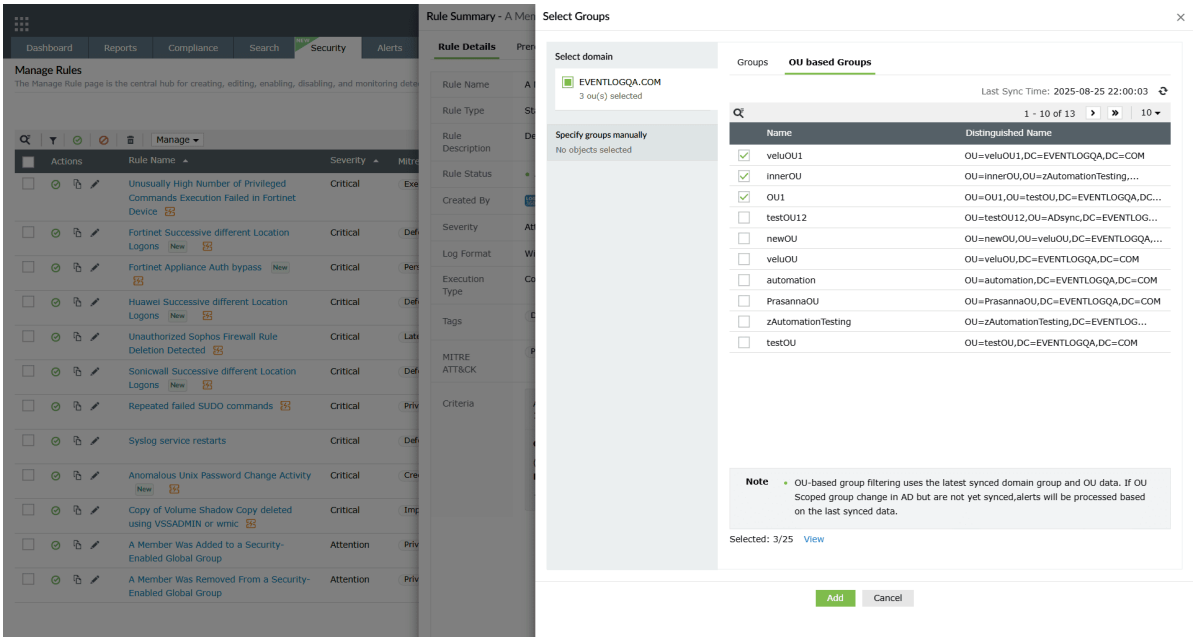


Image 19: Group selection in object filtering

5. After selecting the preferred groups, you can view your selection by clicking on the View option highlighted below.

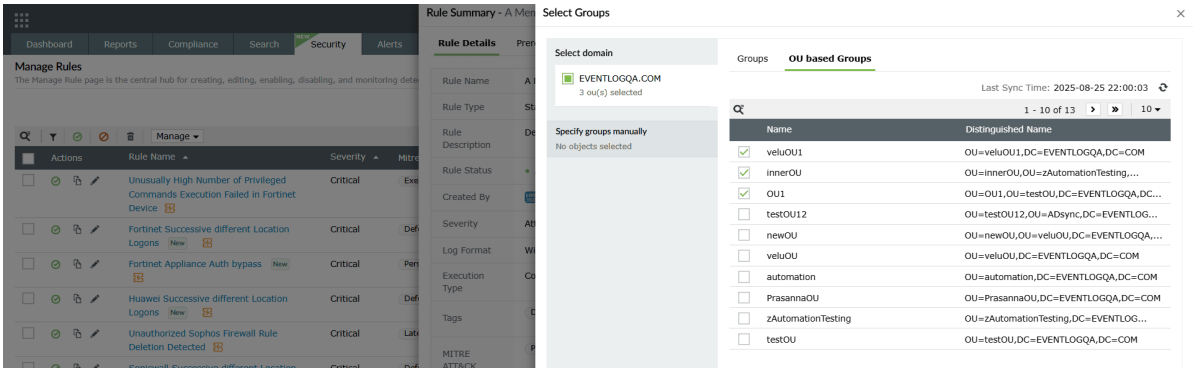




Image 20: Viewing list of configured object filter users/groups

6. The list of selected user groups will be displayed.

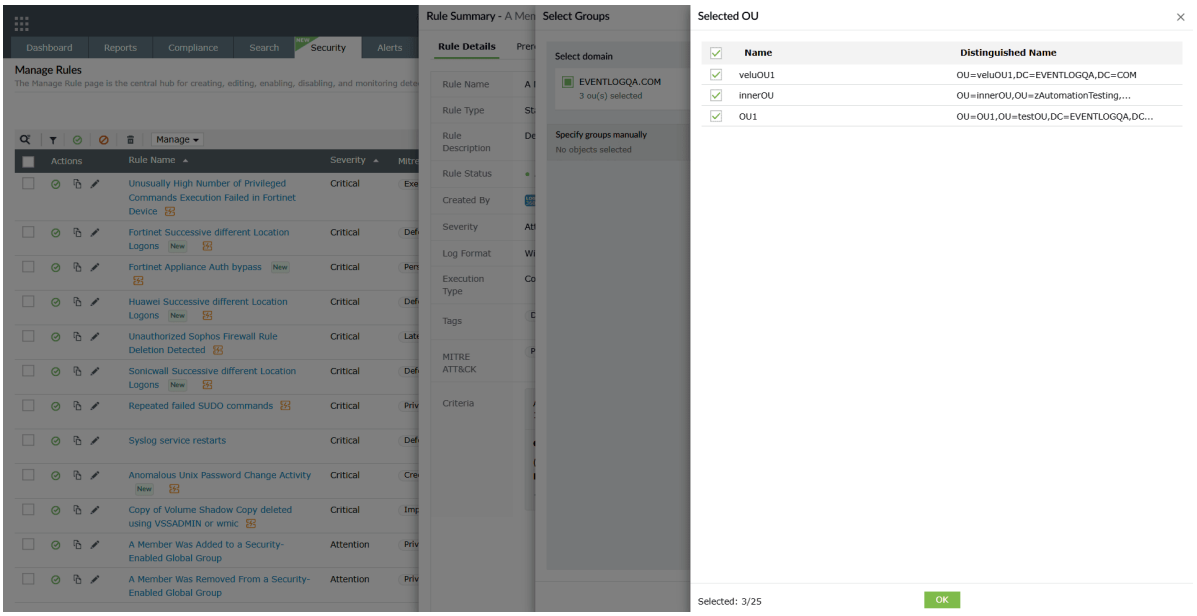


Image 21: Configuring object filter users/groups

7. Once the selection is done, click on OK in the selection list and then click on Add in the Select Groups pane. Click on the Save button in the Add Objects pane.

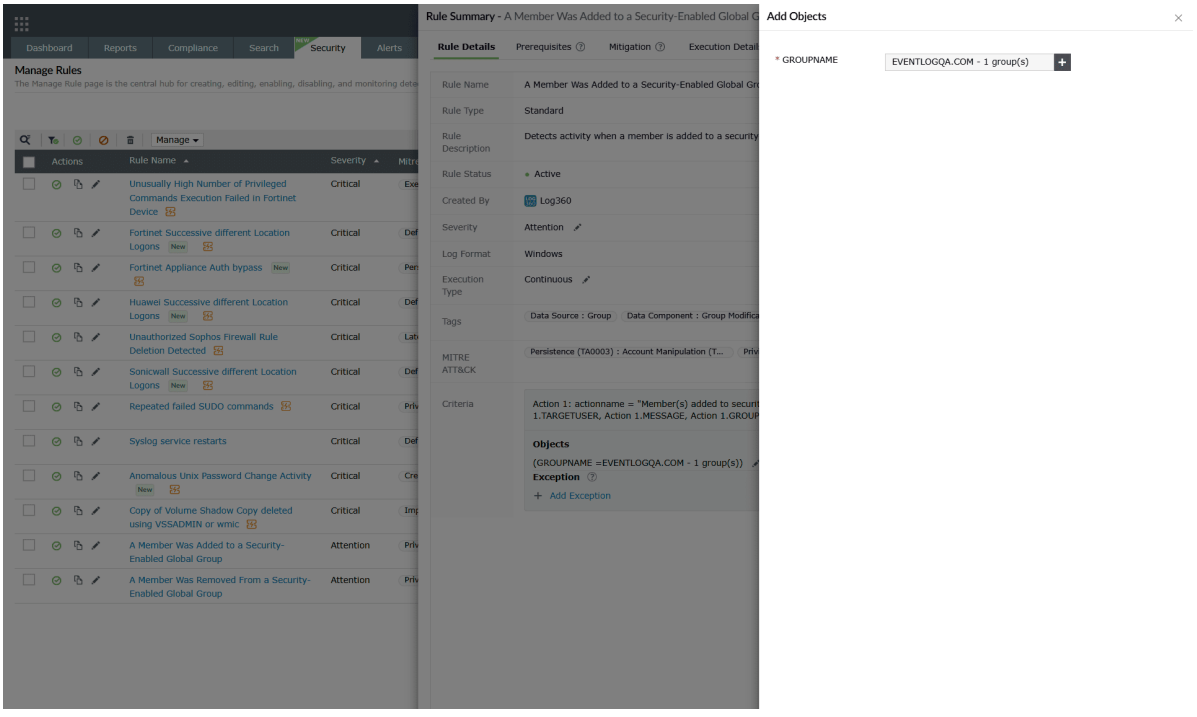




Image 22: Configuring object filter users/groups in rule management

8. Upon successful completion of action, a Success pop-up appears briefly, and the selection changes are instantly updated and are visible in the Objects section.

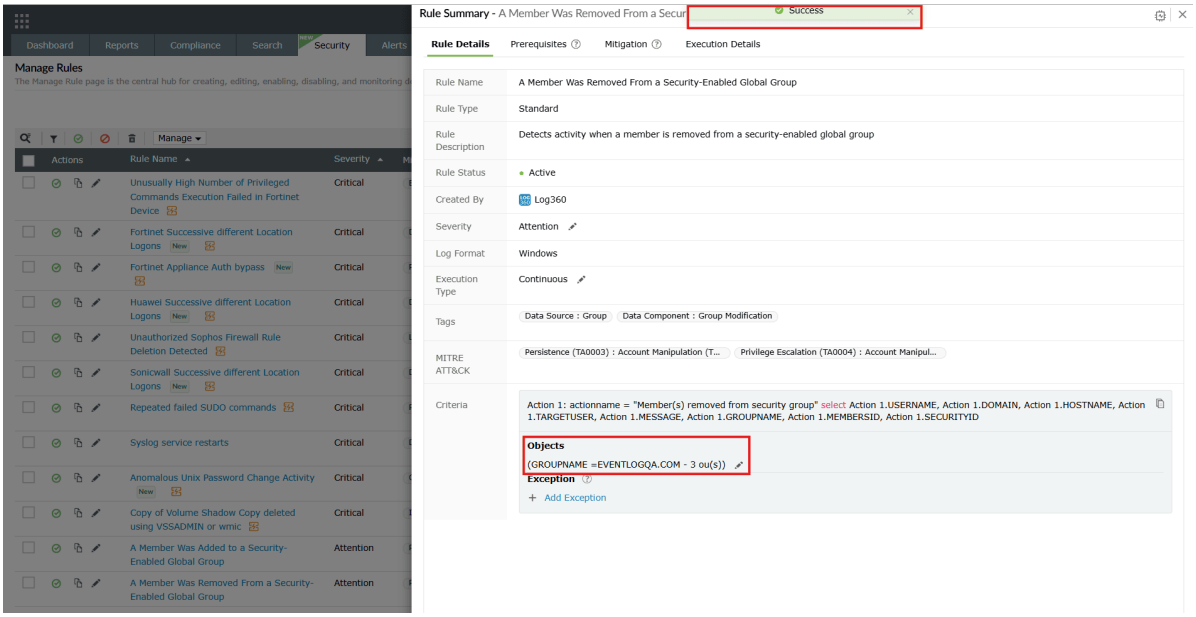


Image 23: Configuring object filter users/groups in rule management

B. Exception section

1. Navigate to the Criteria section as highlighted below and click on the Add Exception option as highlighted below.

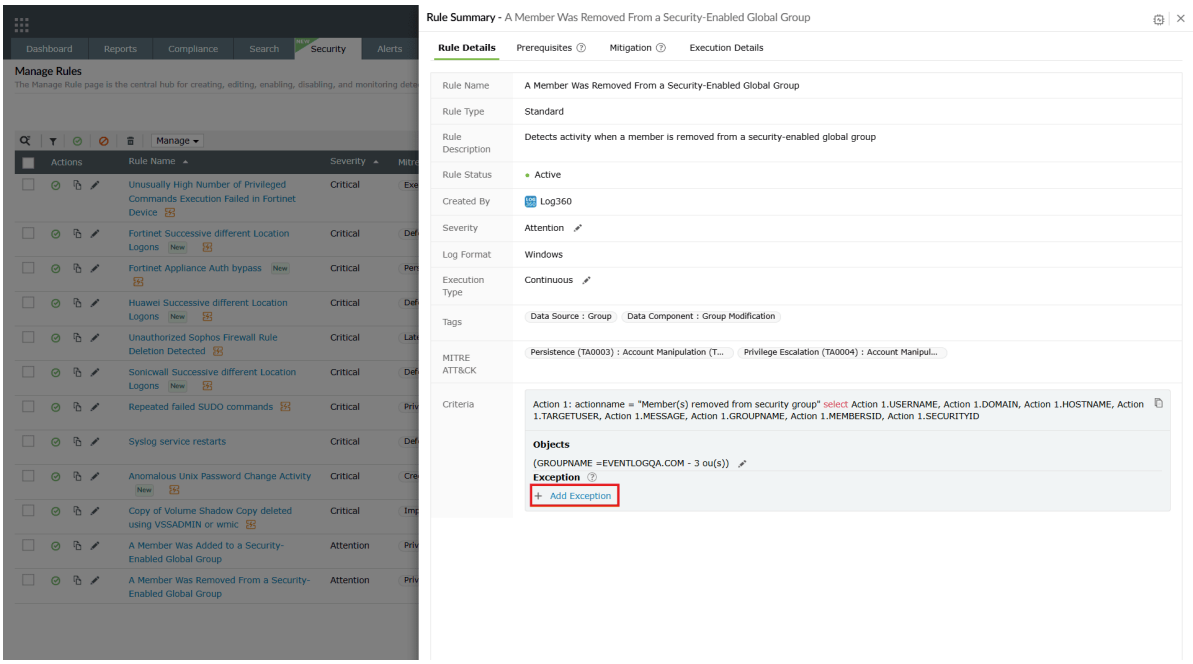


Image 24: Adding exceptions in rule summary

NOTE

- Rule exception can be configured only post installation.
- In case these configurations are made, you will be able to view the edit option to configure the exception instead of creating a new one.

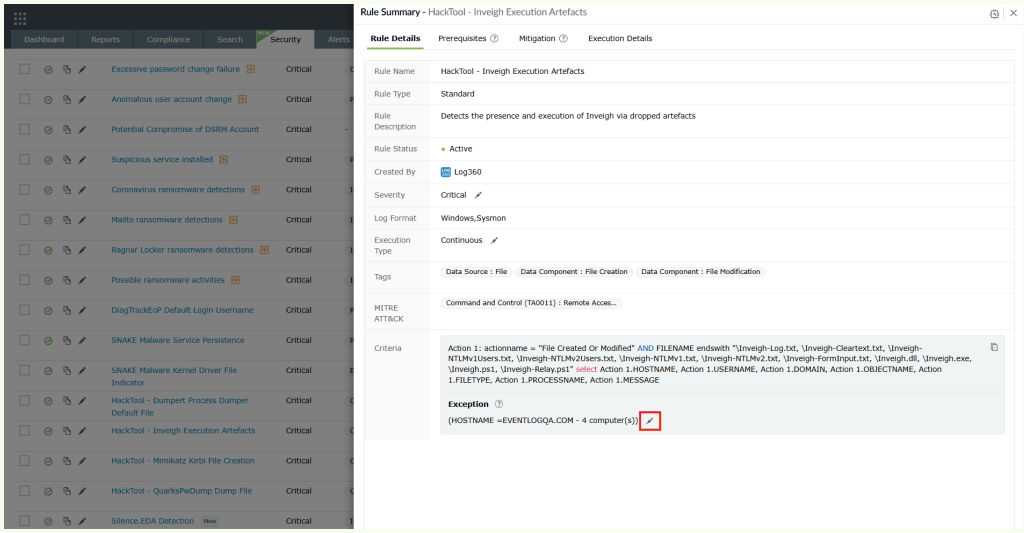


Image 25: Editing exceptions in rule summary

- Click on the edit icon as highlighted above and follow the steps given below.

2. The Add Rule Exception pane slides open. Make the necessary configurations with the preferred variables from the available drop-downs and then click on the add icon as highlighted below.
   This will allow you to filter through the devices and make selections as to which devices are to be configured for exceptions.

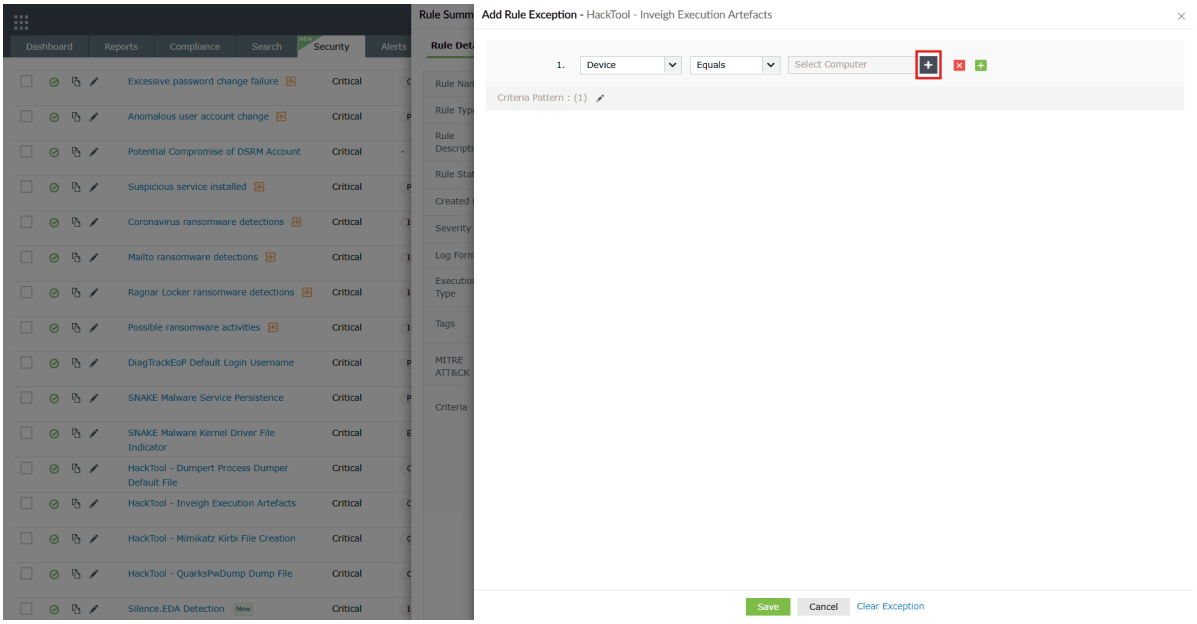


Image 26: Editing exceptions in rule summary with object filter

3. The Select Computer pane slides open. The device names will be displayed along with the object filter feature in order to be able to filter and choose what devices you wish to group under this rule.

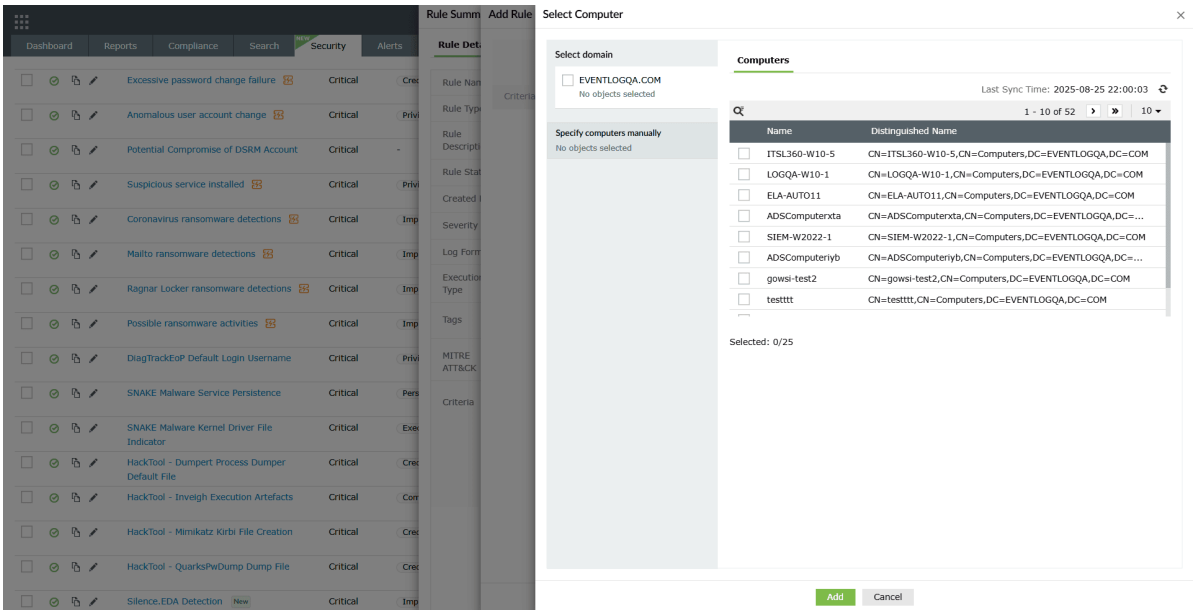


Image 27: Configuring object filter users/groups in exception

4. After selecting the preferred devices, you can view your selection by clicking on the View option as highlighted below.

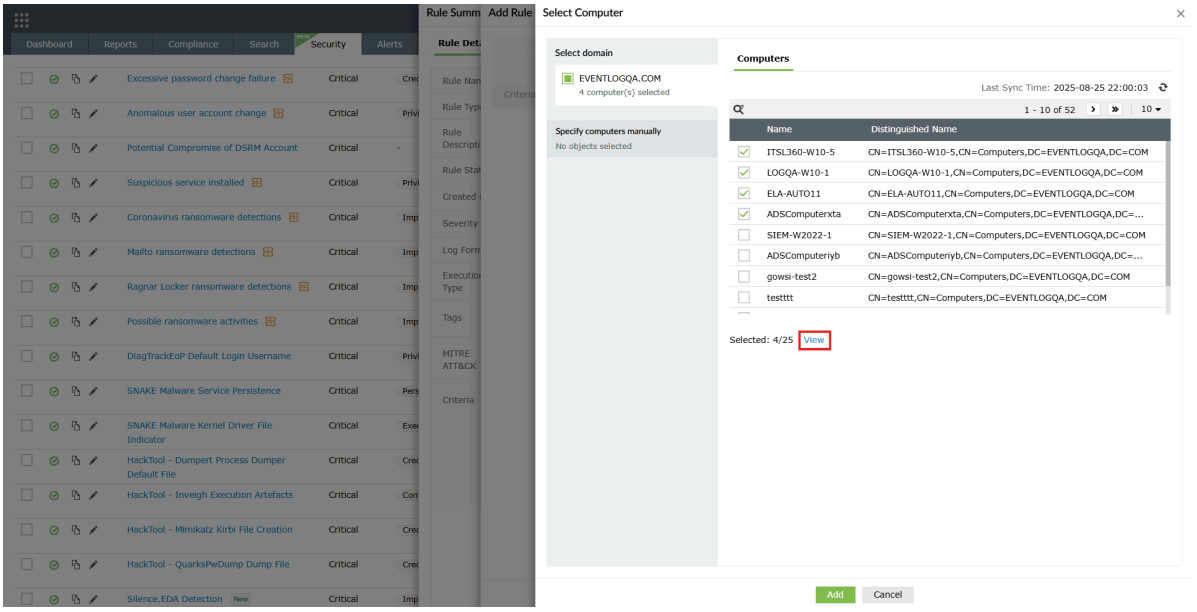
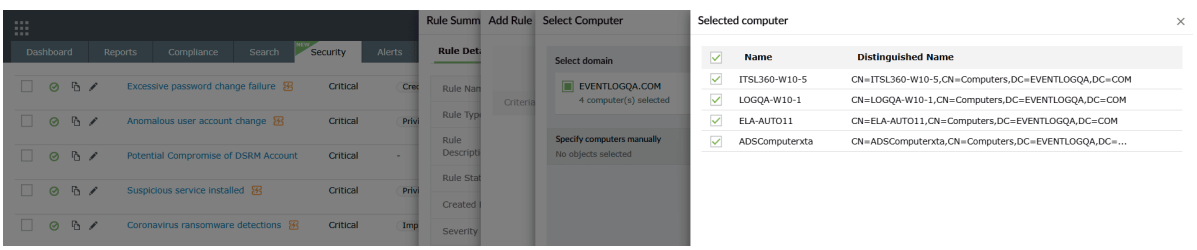


Image 28: Viewing list of configured object filter users/groups

5. The list of Selected computers will be displayed.



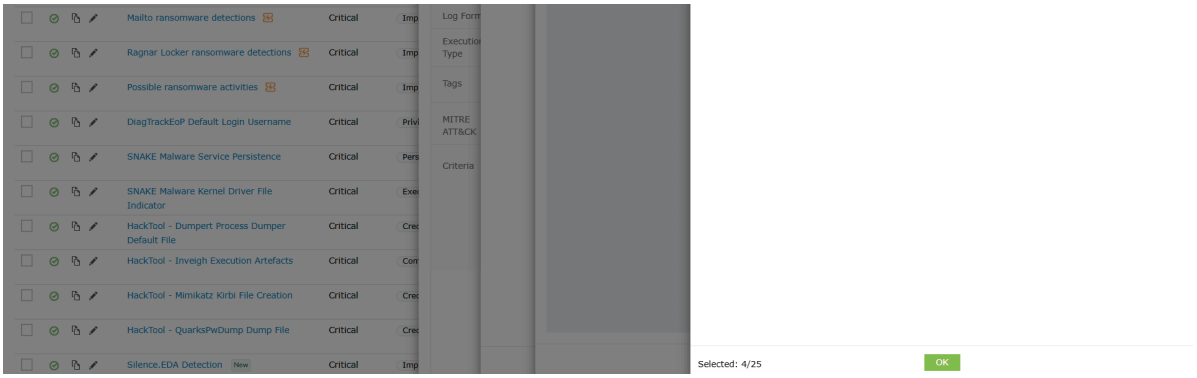


Image 29: Configuring object filter users/groups

6. Once the selection is done, click on OK in the selection list and then click on Add in the Select Computer pane. Click on the Save button in the Add Rule Exception pane as highlighted below. In case you wish to reset the exception configurations and redo them, click on Clear Exception.

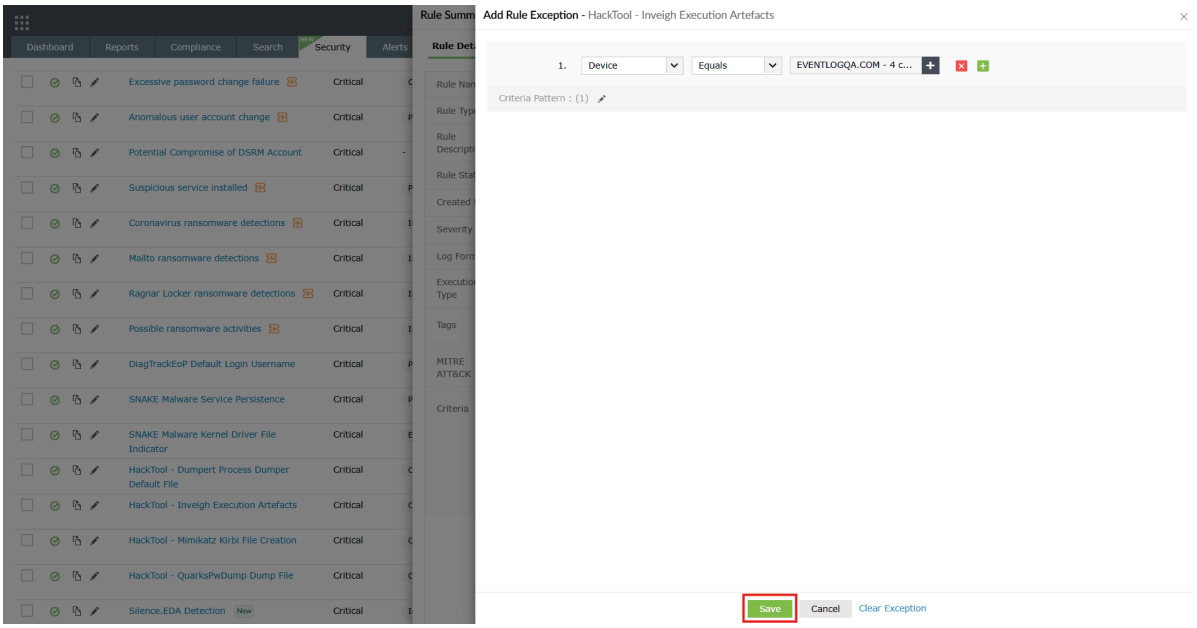
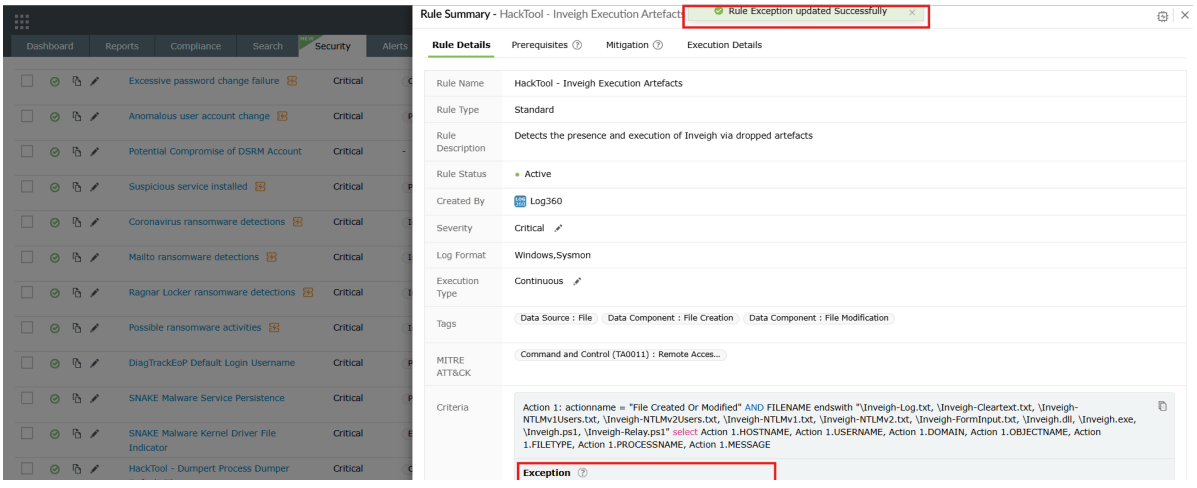


Image 30: Configuring object filter users/groups in rule management

7. Upon successful completion of action, a Rule Exception saved Successfully pop-up appears briefly, and the selection changes are instantly updated and are visible in the Exception section.



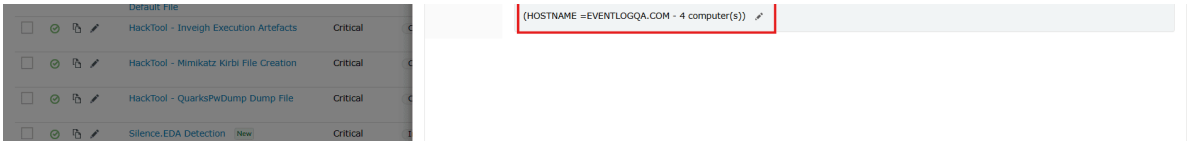


Image 31: Configuring object filter users/groups in rule exceptions

C. Enabling rule

When activating a rule, the object filter automatically slides open for that particular rule.

1. Click on the currently disabled icon ⊘ under the Actions column to enable the rule.

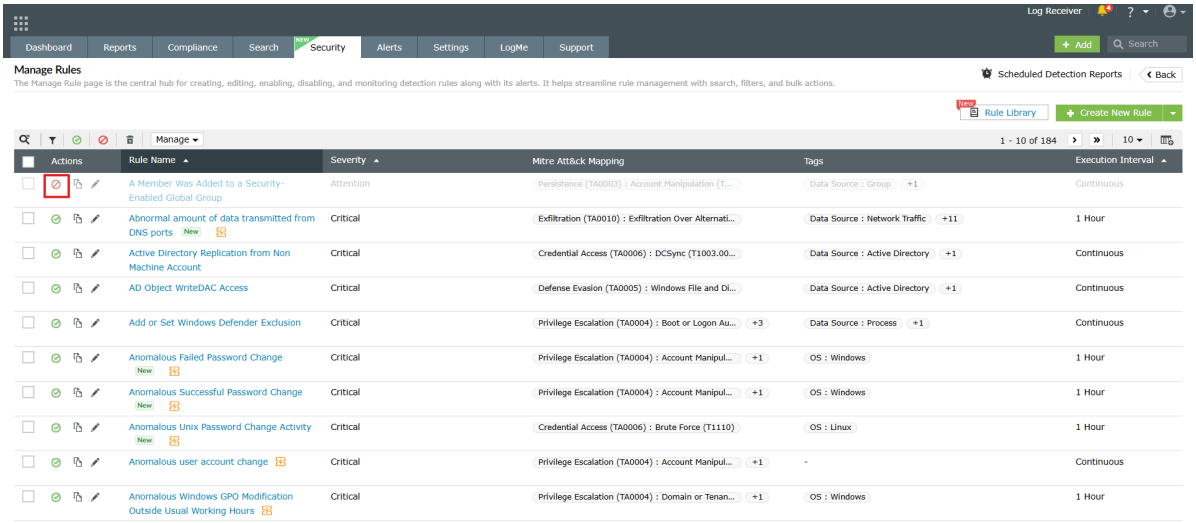


Image 32: Enabling a rule

2. The object filter pane slides open upon clicking on the disabled icon.

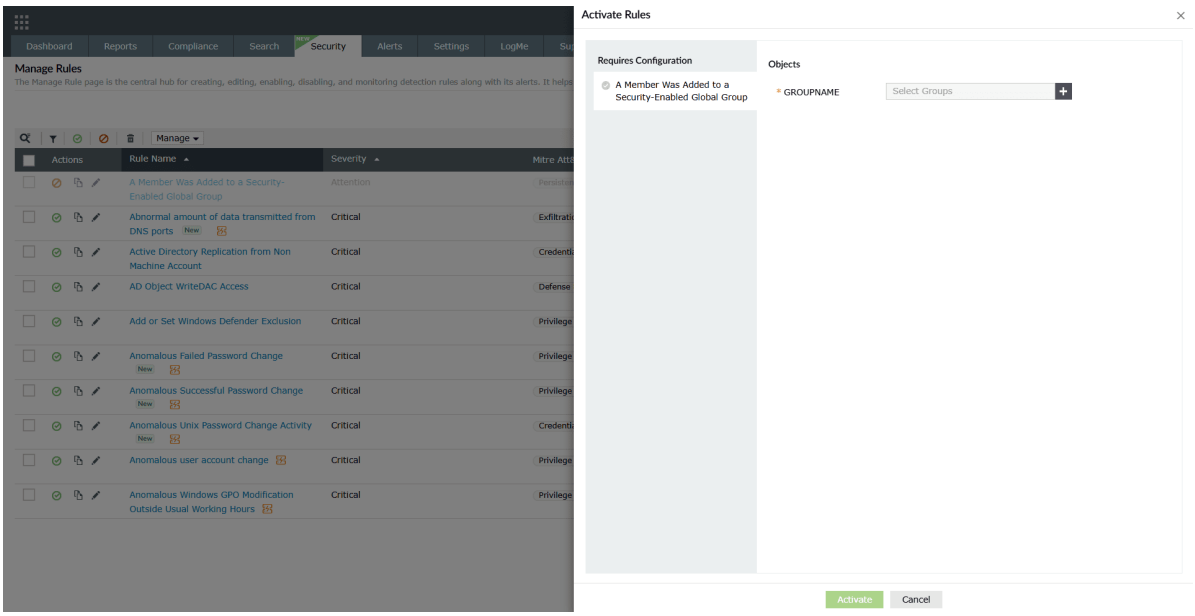


Image 33: Object filtering while enabling a rule

3. Select preferred users/groups and click on the Activate button.

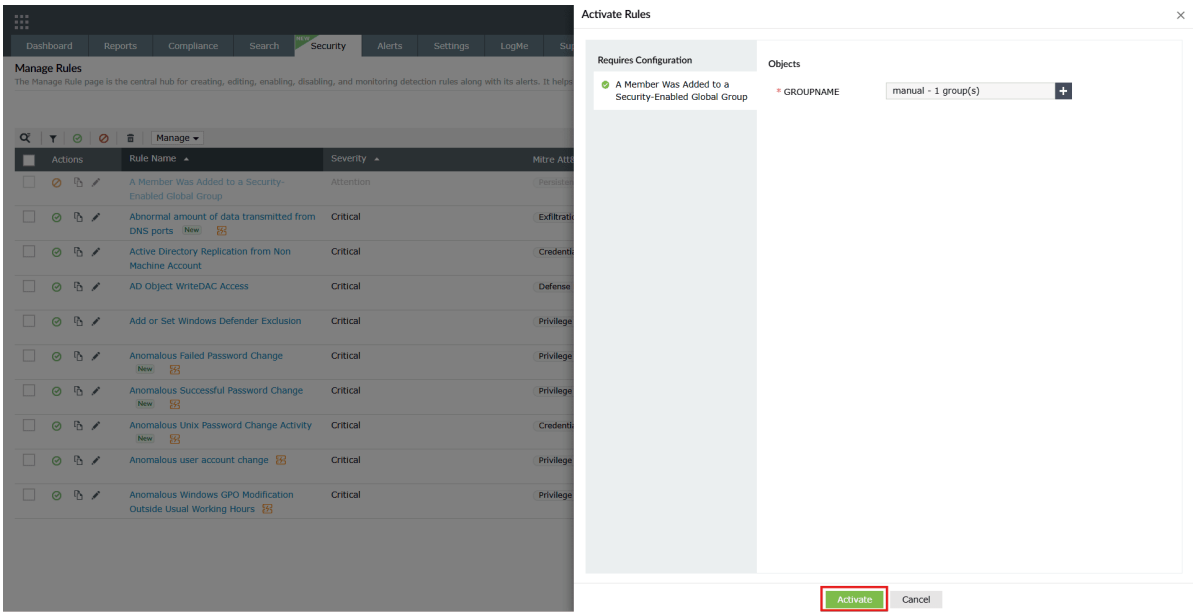


Image 34: Object filtering while enabling a rule

4. Upon successful completion of action, the below pop-up appears.

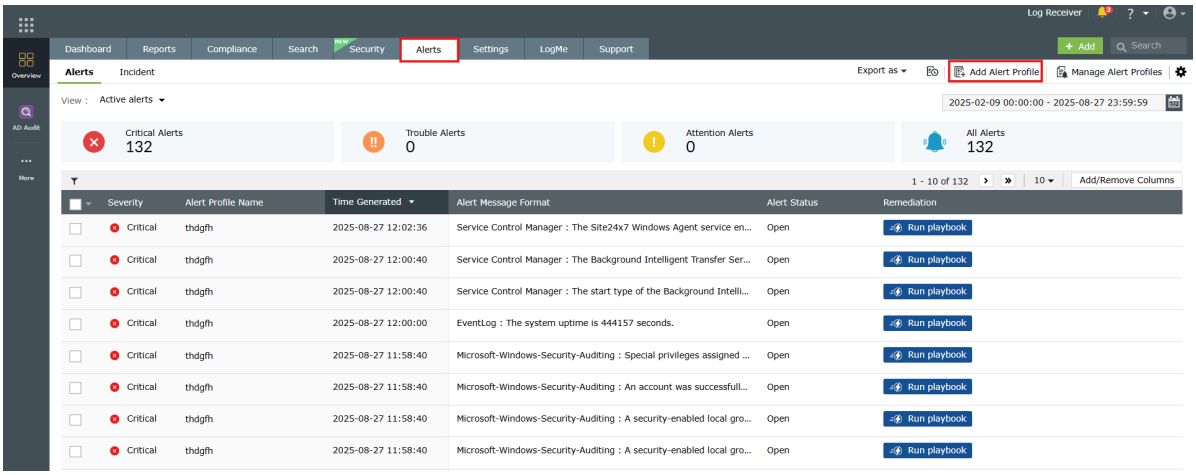


Alerts

The solution also supports object filters when creating or editing alert profiles, enabling you to refine Active Directory-based criteria with user, group, or OU selections. To do this, follow the steps below:

> **NOTE**
>
> The Active Directory object filter is accessible only for the rules and criteria under the Active Directory log type.

1. In the product console, navigate to the Alerts tab and click on Add Alert Profile.



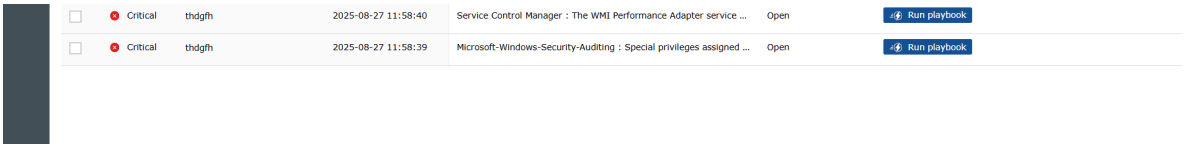


Image 35: Adding an alert profile

2. The Add Alert Profile module is displayed.

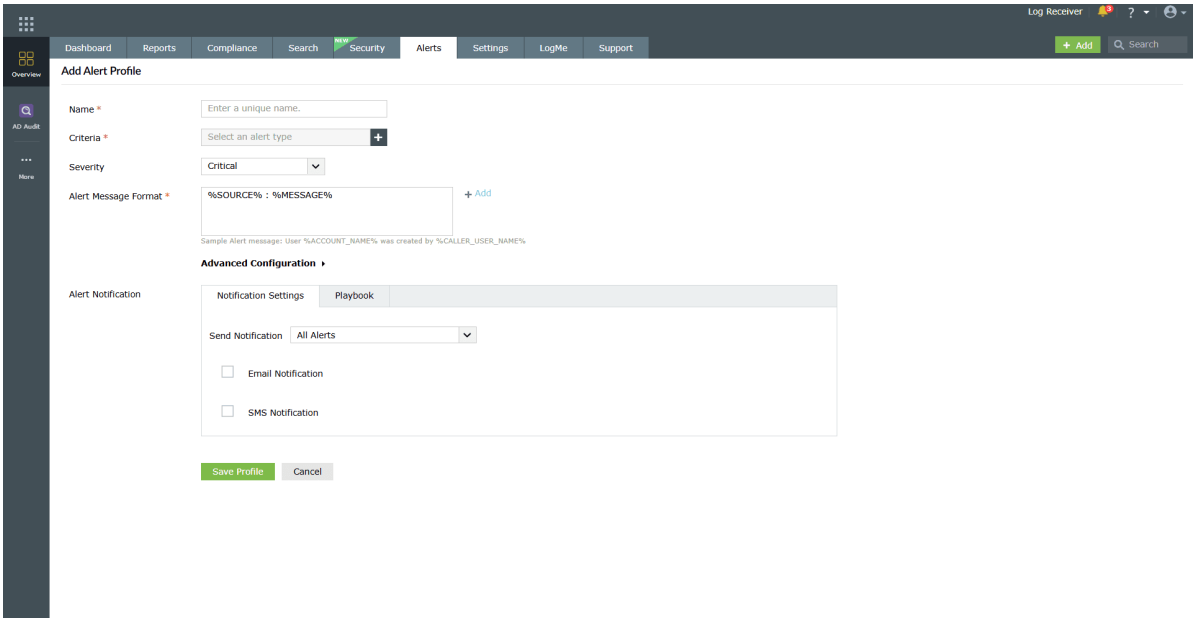


Image 36: Add alert profile module

3. Provide the Name for the alert. Add Active Directory specific Criteria by choosing Active Directory as the Log Type in the Rules sub-tab of the Alert Criteria Builder. Click on the Select button.

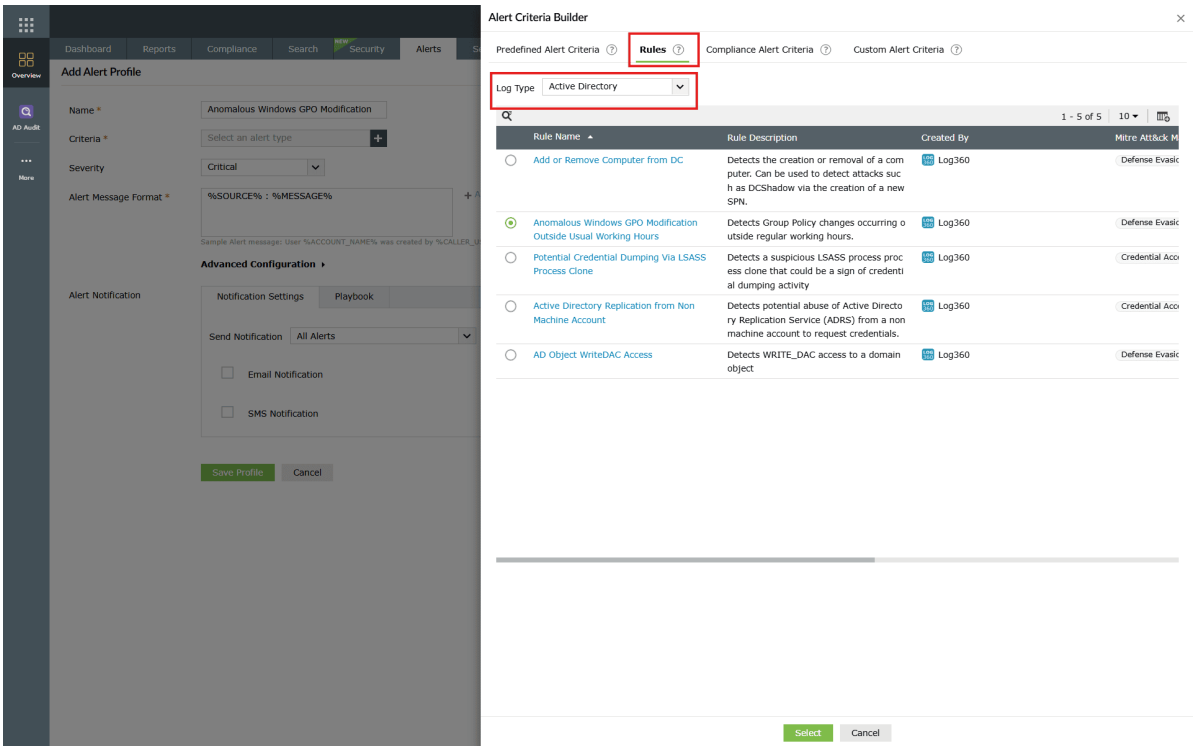


Image 37: Object filtering in the alerts module

4. Choose the domain under the Select Domain drop-down. Tick the Filter checkbox and then configure the filter based on your requirements. Click on the add button of the object filter to select users to be grouped under this.

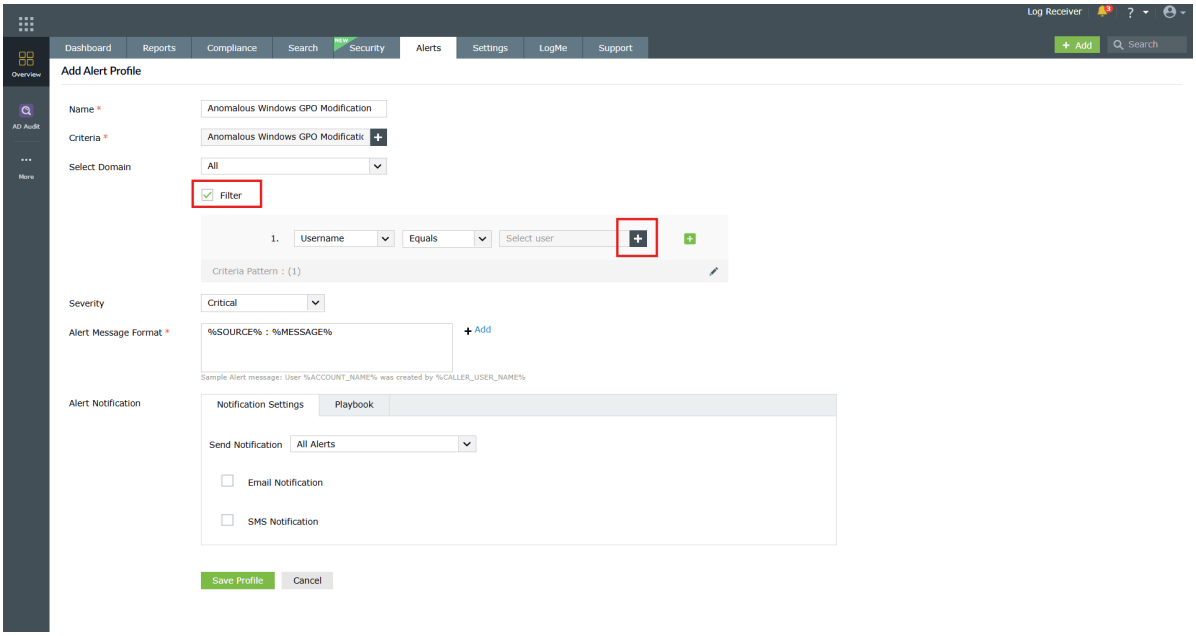


Image 38: Object filtering while adding an alerts profile

5. The Select user pane slides open. The user names will be displayed along with the object filter feature in order to be able to filter and choose which users you wish to group under this alert configuration.

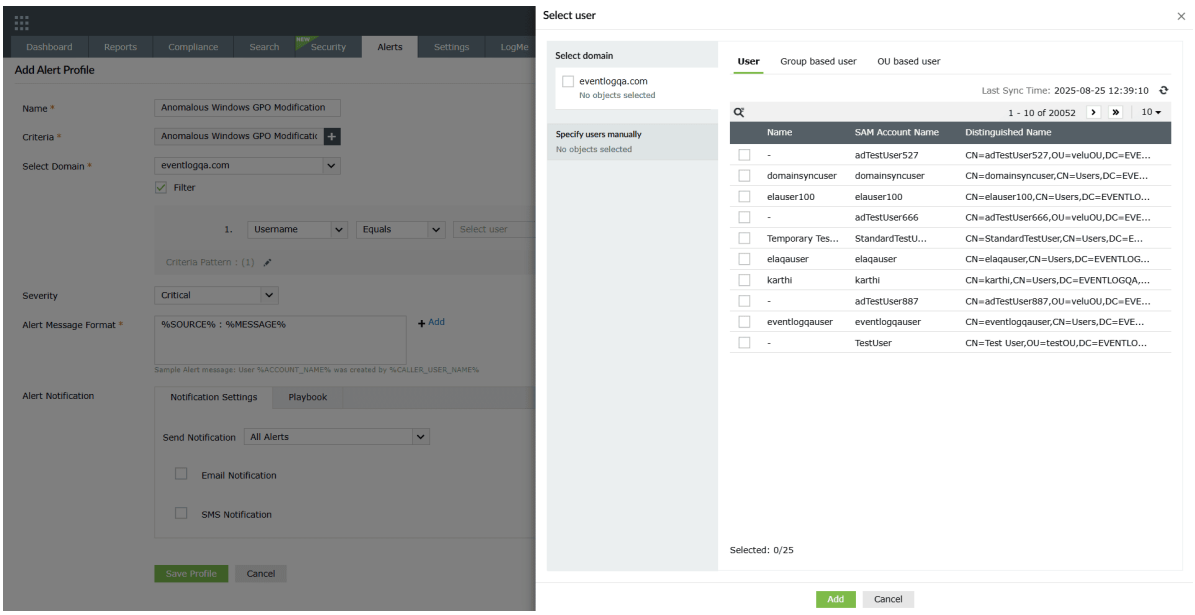
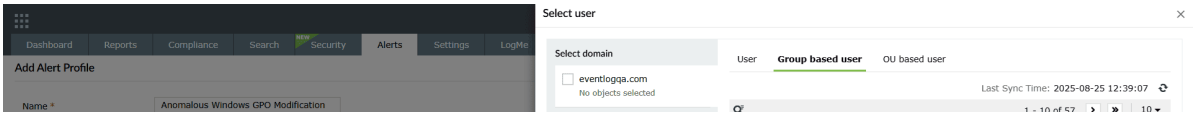


Image 39: Object filtering in the alerts module

6. Similarly, the Group based user sub-tab also includes the filter for user selection based on user groups.



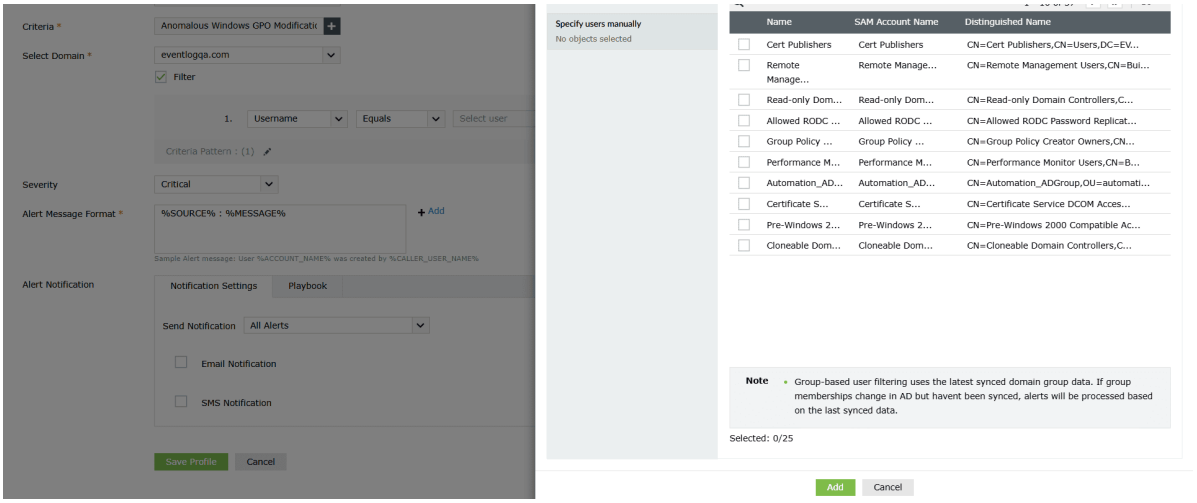


Image 40: Configuring object filter users/groups

7. The OU based user sub-tab also includes the filter for user selection where the users are listed categorized by their OUs.

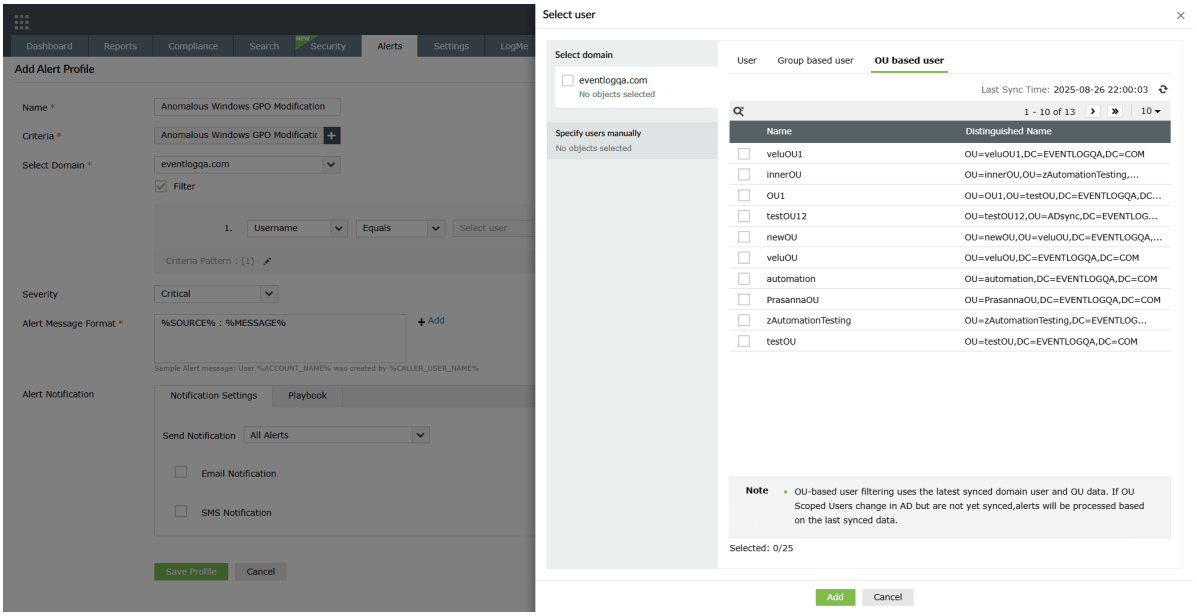
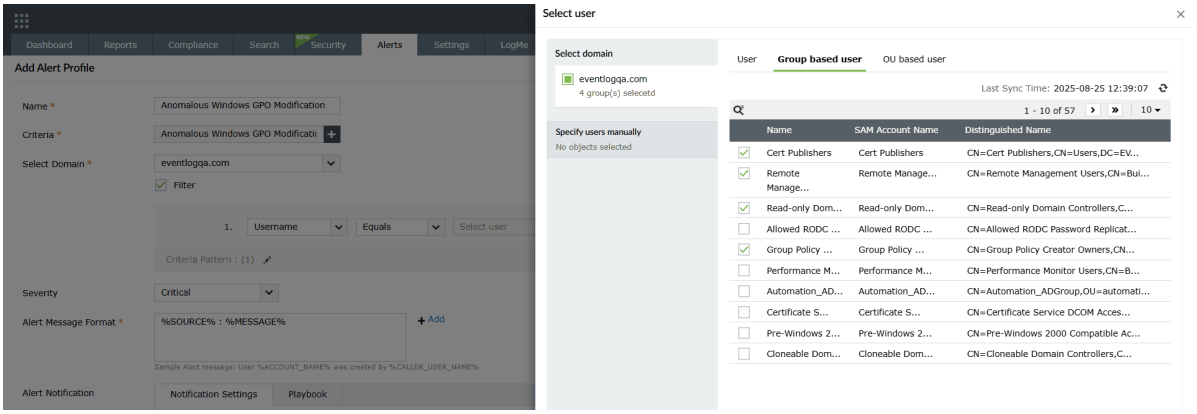


Image 41: Configuring object filter users/groups

8. After selecting the preferred users, you can view your selection by clicking on the View option as highlighted below.



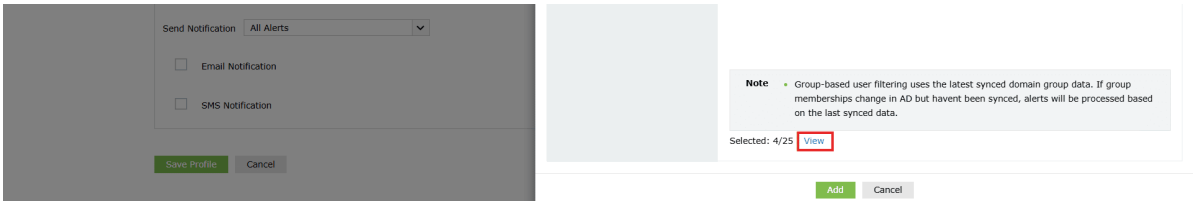


Image 42: Viewing list of configured object filter users/groups

9. The list of Selected users/groups will be displayed.

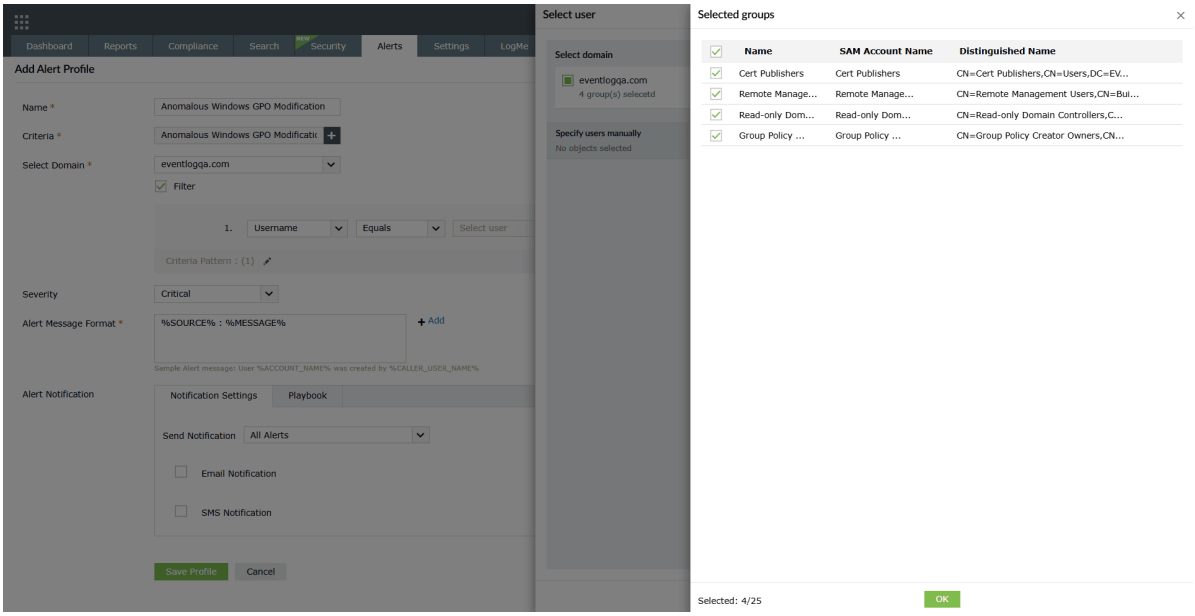


Image 43: Configuring object filter users/groups

10. Once the selection is done, click on OK in the selection list and then click on Add in the Select user pane.

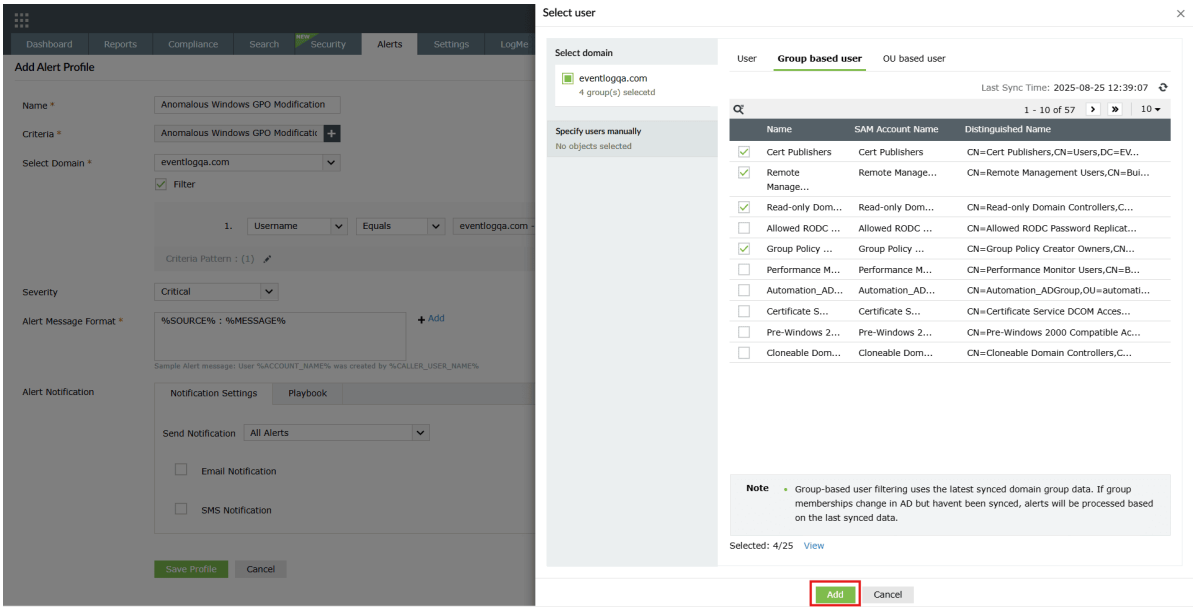


Image 44: Configuring object filter users/groups

11. Upon successful completion of action, the selection changes are instantly updated.

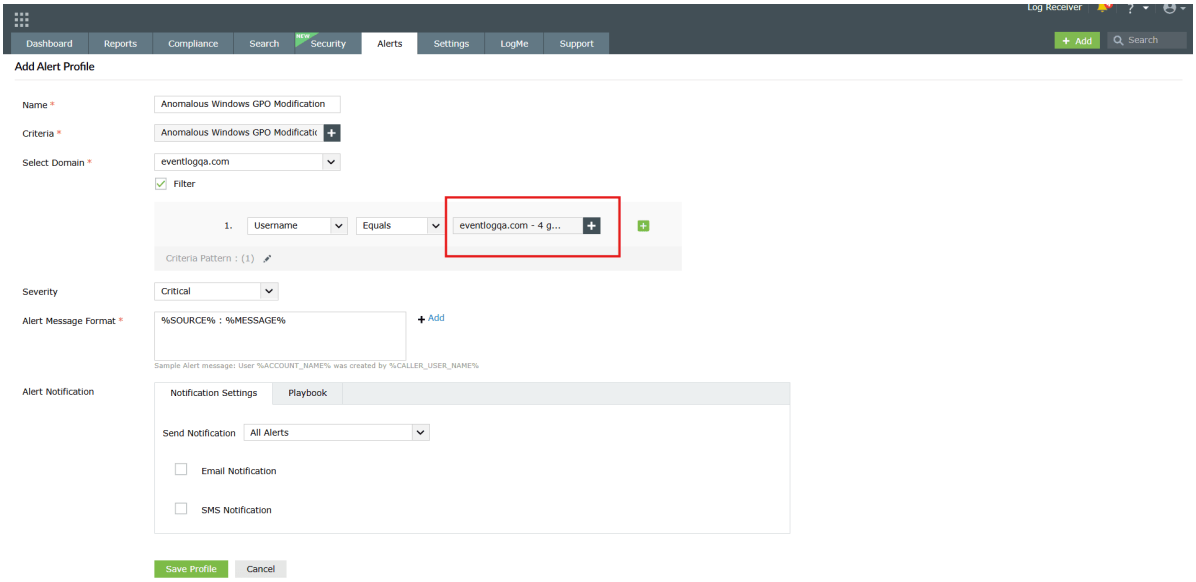


Image 45: Configuring object filter users/groups in alerts module

> **NOTE**
>
> The object filter can also be used in a existing alert profile by clicking on the edit icon of an alert profile and following the above mentioned steps. To learn more about creating and managing alert profiles, refer to the Alerts help document.

Read also

This document explained how to use the object filter during rule installation, rule management, and alert configuration. You also learned how it can be applied in the objects and exception sections, as well as in alert profiles, to improve accuracy in monitoring.

- Active Directory Object Filter Overview

10.1.4.1. About Rule Library

Last updated on: September 12, 2025

In this page

Highlights of Rule Library

Workflow

Log360's Rule Library is a centralized, cloud-delivered repository of security threat detection rules. It is designed to enhance Log360's ability to identify potential security threats. The rules within Log360's Rule Library are primarily based on two standards:

- MITRE ATT&CK® framework: The rules are directly mapped to tactics and techniques used by adversaries, allowing security teams to understand the context of an attack and anticipate the attacker's next move.
- Sigma rules: These are generic, open-source yet credible rules written in standardized format converted to Log360's query structure.

By leveraging a cloud-delivered rule library, security teams can receive up-to-date detection logic automatically without having to write or manually update every rule, thus staying ahead of emerging threats.

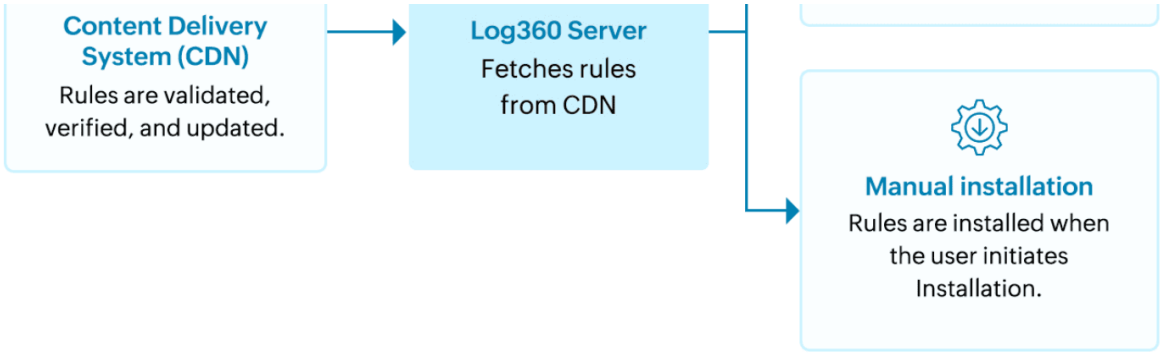
> NOTE
>
> Explore in depth the functionalities of Log360's rule library and its Security Intelligence Pack.

Highlights of Log360's Rule Library:

- Over 2,000 predefined threat detection rules to spot insider threat, external threats, malware, APTs and more.
- Rules are categorized based on the log sources they are associated with for easier implementation.
- Rules are also mapped to relevant MITRE ATT&CK® threat modelling framework.
- Option to automatically install new threat detection rules based on your security policies. This ensures your systems are immediately protected against the latest threats and attacks as soon as a new rule is released.

Workflow





The cloud delivered system of Log360, hosts the detection rules uploaded by ManageEngine. The rules are then delivered to the Log360 server.

Please note that the Log360 server should have an active internet connection for uninterrupted update of the detection rules. For offline or air-gapped environments, rule updates can be applied by downloading the latest Rule Library package and configuring the system to use it locally.

Once the rules are updated, the Available Rules tab in the solution's console lets you install and configure them. Our solution also provides auto-installation option which updates the rules in your environment as the rule gets pushed to the Rule Library by ManageEngine team.

This guide explores how you can selectively install rules or configure auto-updates of rules.

Understanding Rule Library

In the central view of the Rule Library, rule attributes are displayed in a table. Columns represent different fields, and additional columns can be added or removed to customize the view. The Rule Library is divided into two tabs: Available Rules and Installed Rules.

Key aspects of the Rule Library include:

- MITRE ATT&CK® Mapping: Each rule is aligned with tactics and techniques from the MITRE ATT&CK® framework, offering better visibility into adversarial behaviors.
- Severity classification: Rules are assigned severity levels to help users prioritize detections and response actions effectively.

Common components:

These components are present in both the Available Rules and Installed Rules tabs.

Component	Details
Rule Name	The name of the rule for identification.
Severity	Shows the rule's criticality level, such as Attention, Critical, or Trouble.
MITRE ATT&CK® Mapping	Displays the associated MITRE ATT&CK® tactic and techniques.

Component	Details
Tags	Lists related tags such as data source and data component associated with the rule.
Rule Type	Specifies whether the rule is Standard, Anomaly, or Advanced.
Created Time	The date and time when the rule was first added.
Last Modified Time	The date and time when the rule was last modified.
Description	Provides a detailed summary of what the rule detects, including its purpose and author information.

Components specific to the Installed Rules table

Field	Details
Execution Interval	Defines how criteria matching occurs. • Continuous: Matches incoming logs and raises detection directly if they match. • Intelligent: Runs the criteria on indexed logs and raises detection if matched from indexed logs.
Created By	Indicates the source of the rule. In this case, all rules are created by Log360.

Read also

This page introduced the Rule Library, its role in enhancing threat detection and architecture. To learn how to manage and configure these rules in your environment, refer to:

- Installing Rules
- Configuring Auto-Install Settings

10.1.4.2. Installing Rules

Last updated on: September 12, 2025

In this page

Overview

Steps to install Rules from the Rule Library

Overview

This page details how rules can be installed from the Rule Library. The rules can be installed automatically as ManageEngine develops and adds them to the cloud repository or can be browsed and installed manually. The below segment outlines the steps to install rules.

Steps to install Rules from the Rule Library

1. In your account, navigate to the Security tab to access the Security Analytics dashboard.
2. Click Manage Rule in the top-right corner.

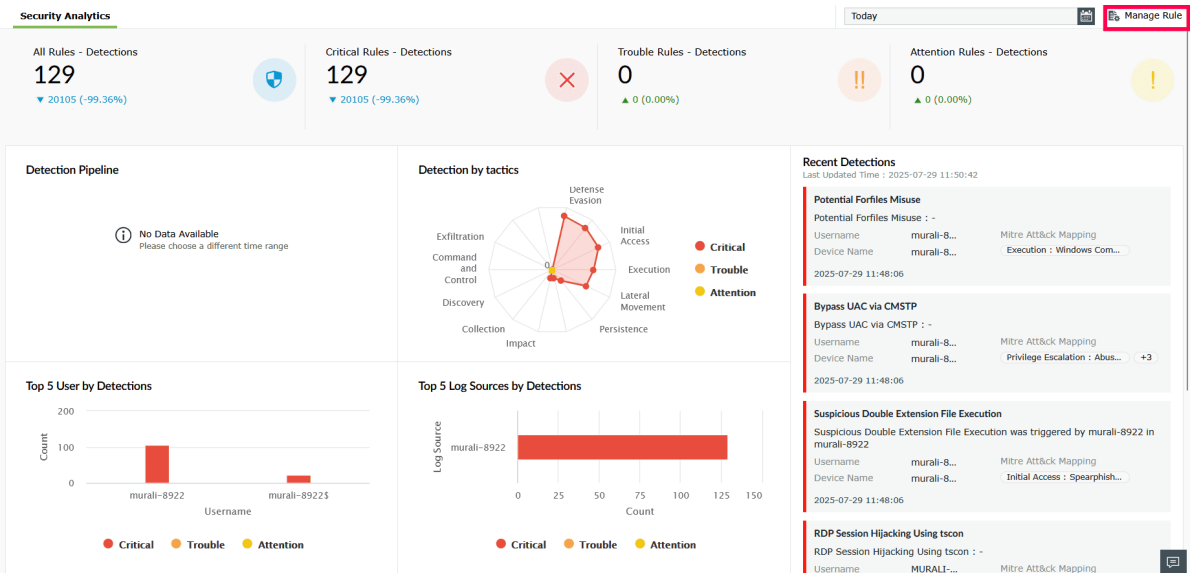
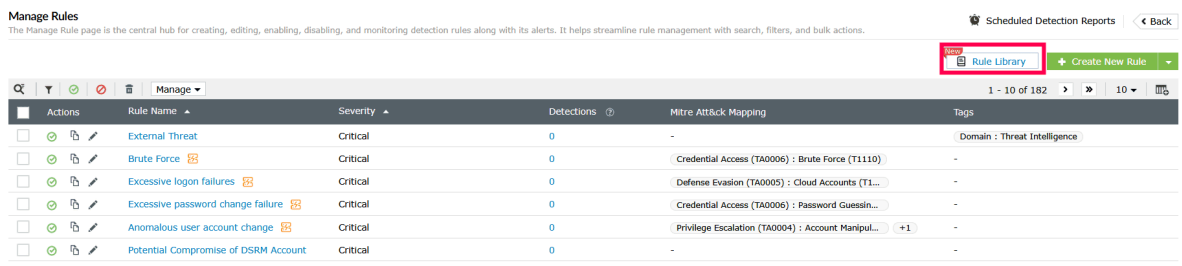


Figure 1: Navigating to the Rule Library

3. In the Manage Rules page, click Rule Library.



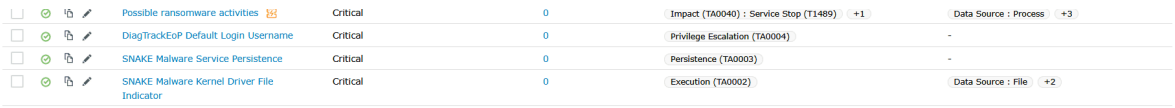


Figure 2: Navigating to the Rule Library

4. Select a category from the left panel to view its rules.
   - Available Rules tab: Displays rules that are available in the central repository but not yet installed.
   - Installed Rules tab: Displays already installed rules in your environment.

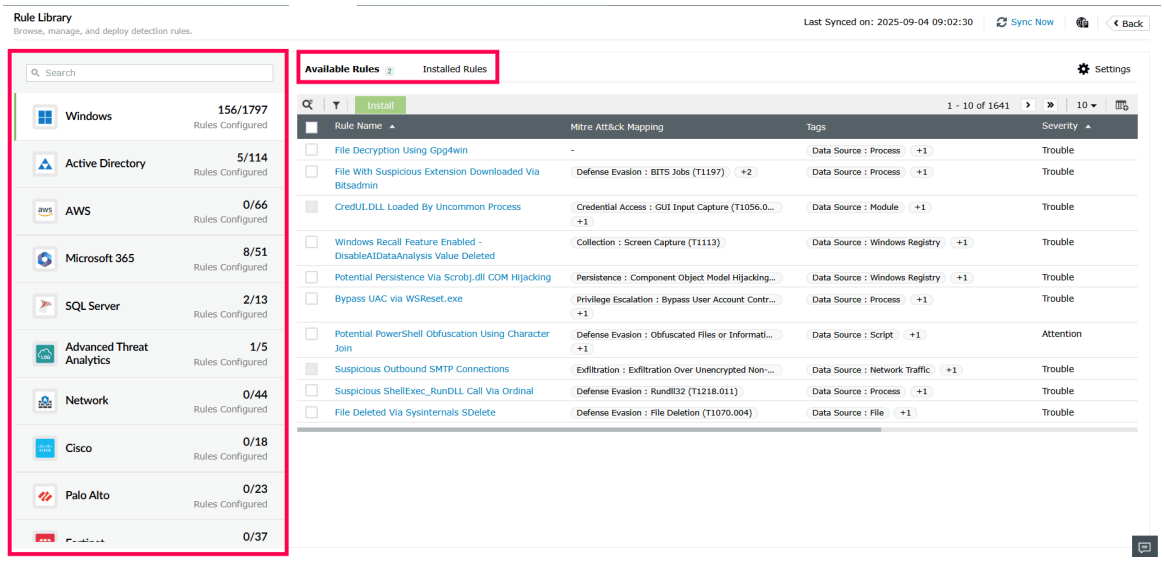
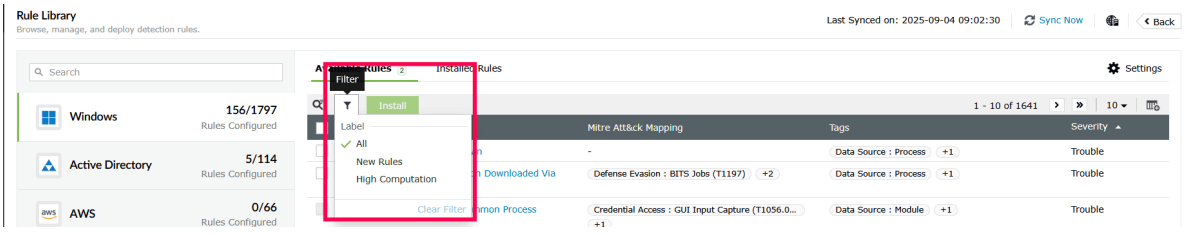


Figure 3: Selecting Rule Library categories

5. In the Available Rules tab, click the ⏷ icon to apply filters for rules. The filter works based on different criteria as outlined:
   - All Rules: Displays all rules.
   - New Rules: Recently added rules.
   - High Computational: Resource-intensive rules, such as:
     - Threshold Logic: Triggers alerts only when an event crosses a defined limit.
     - Anomaly Models: Detects deviations from normal behavior patterns.
     - Multi-action Logic: Correlates two or more events



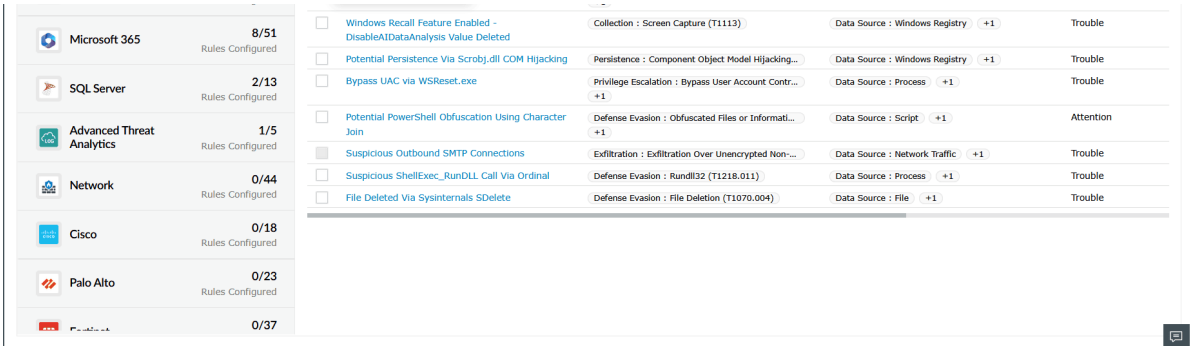


Figure 4: Applying filters in the Available Rules tab

6. Click Clear Filters to remove all applied filters.

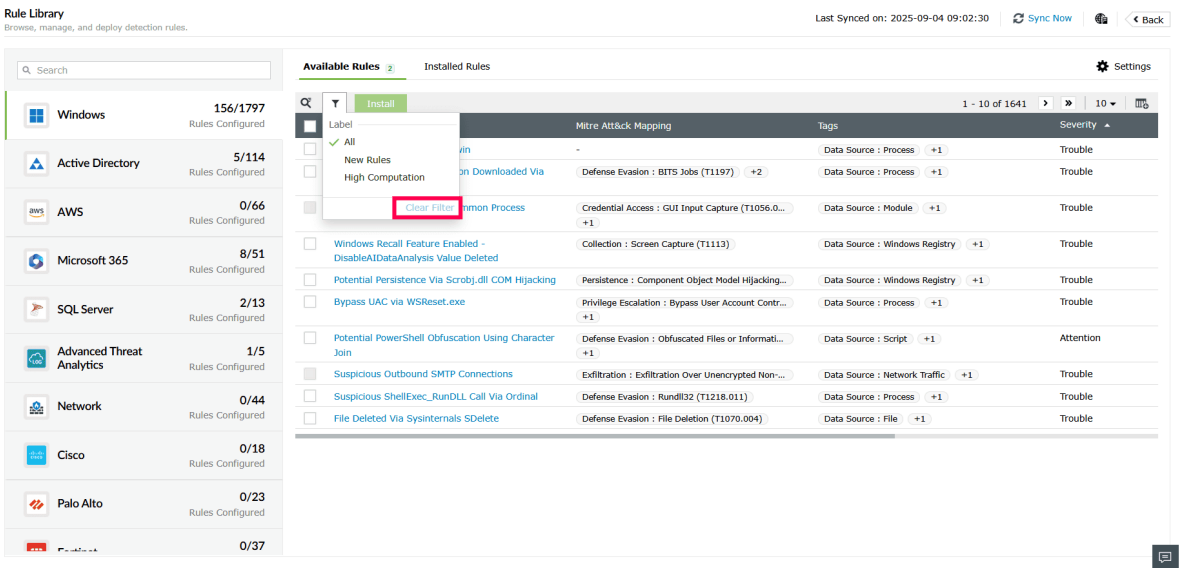


Figure 5: Removing applied filters

7. Click the icon in the top-right corner to customize the rule table view. Select the checkbox next to the fields to add or remove them, and then click Apply.

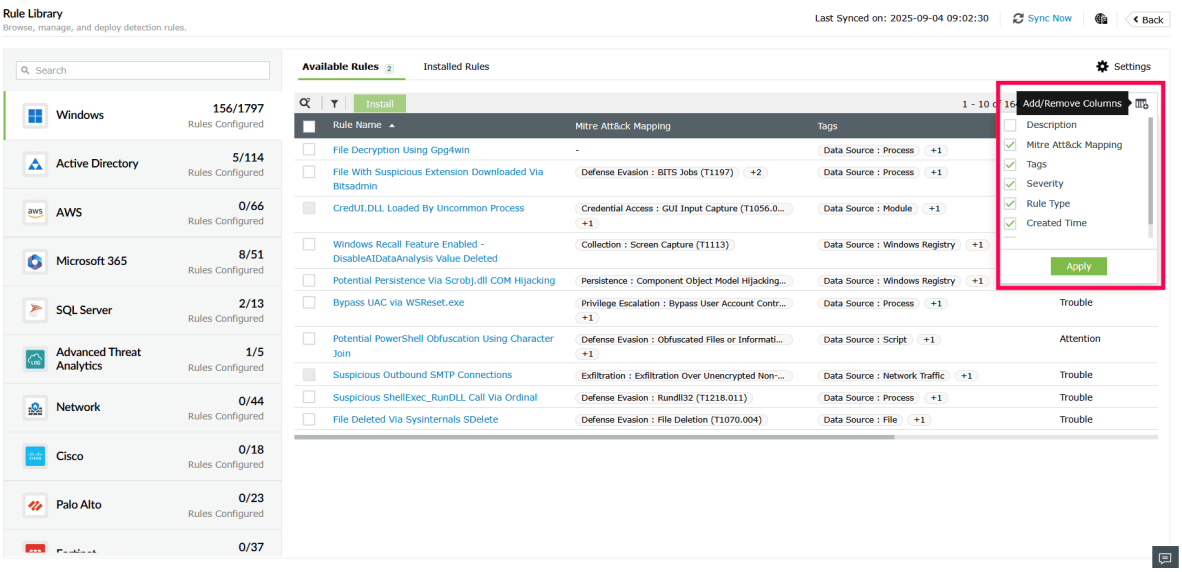


Figure 6: Customizing columns in the Available Rules tab

8. Click the icon to access Advanced Search and locate rules by severity, rule type, MITRE tags, tags, or rule name.
9. To close the search, click the icon again.

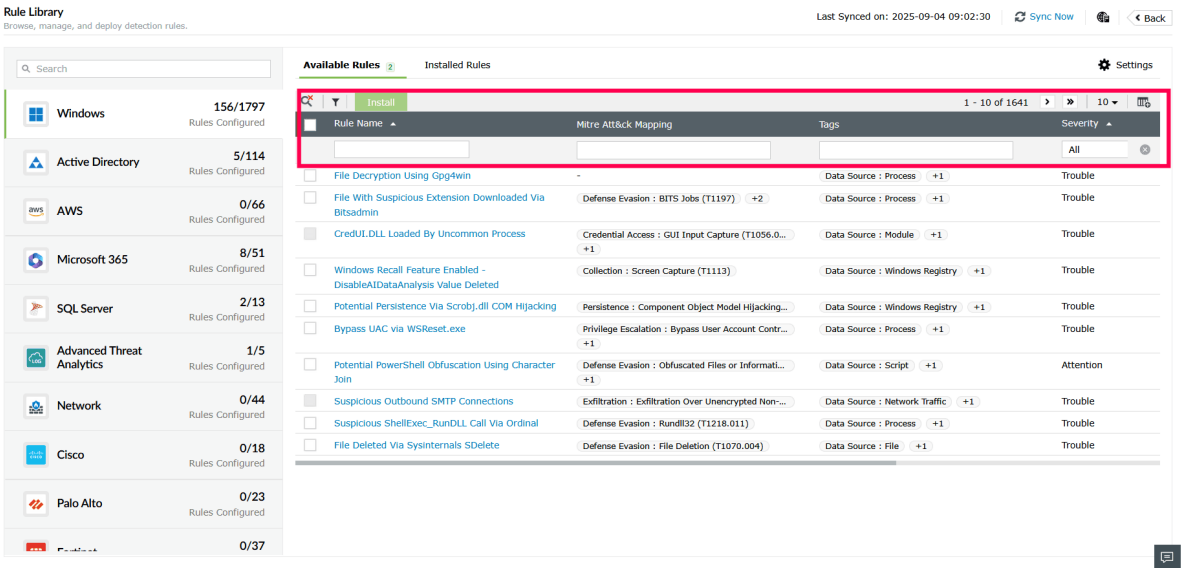


Figure 7: Using Advanced Search

10. Select the checkbox next to the rules you want to install from the Available Rules tab, then click Install.

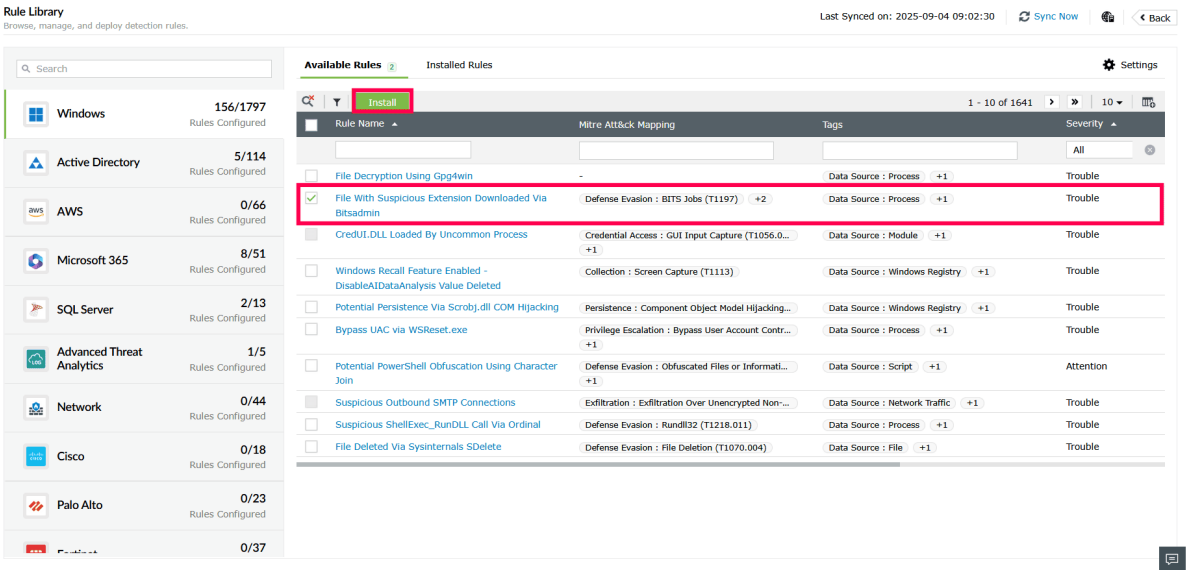


Figure 8: Installing rules from the Available Rules tab

> **NOTE**
>
> You can install multiple rules at once. Some rules require additional configuration during installation.
> - If you install such a rule individually, a popup will prompt you to either complete the additional configuration and install the rule, or skip it and have the rule installed in a disabled state.
> - If the same rule is installed as part of a bulk installation, it will be assumed that you chose to skip

the configuration, and the rule will be installed in a disabled state.
You can enable these rules later from the Manage Rule page after completing the necessary configurations.

11. In the Installed Rules tab, select the ▼ icon to apply the filters for rules, such as New Rules, High Computational, and Deprecated rules.

> **NOTE**
>
> Deprecated rules are rules that we no longer recommend for installation as they have been replaced, improved, or consolidated. If you have installed these rules, then they appear only in the Installed Rules tab.

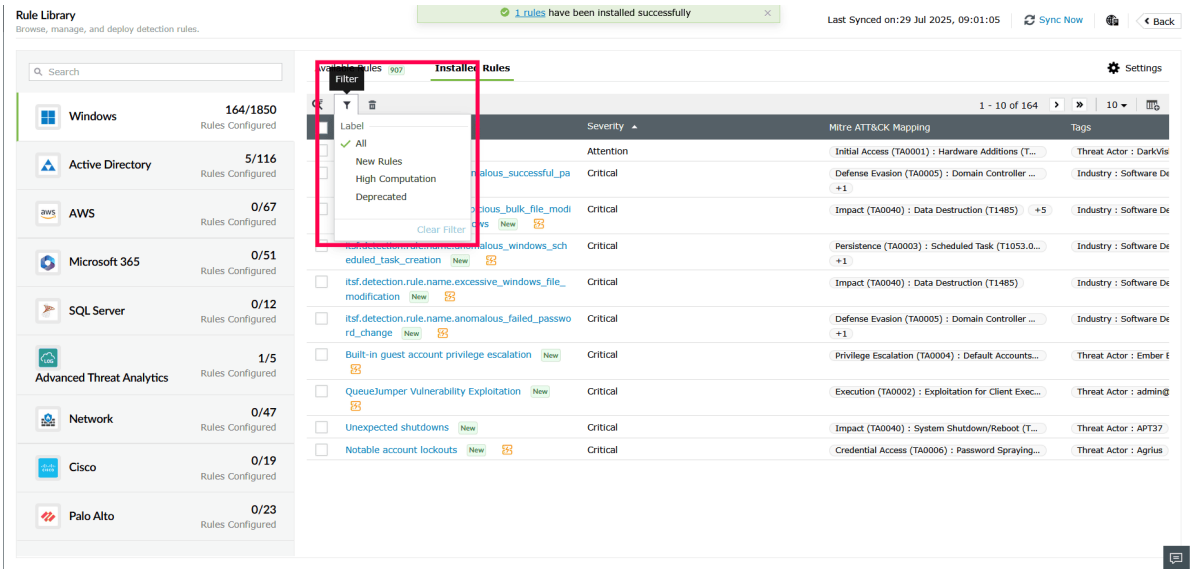


Figure 9: Applying filters in the Installed Rules tab

12. Click the icon to customize the table view. Select the checkboxes next to the fields you want to display, such as Created By, Installed Time, Last Updated Time, and then click Apply.

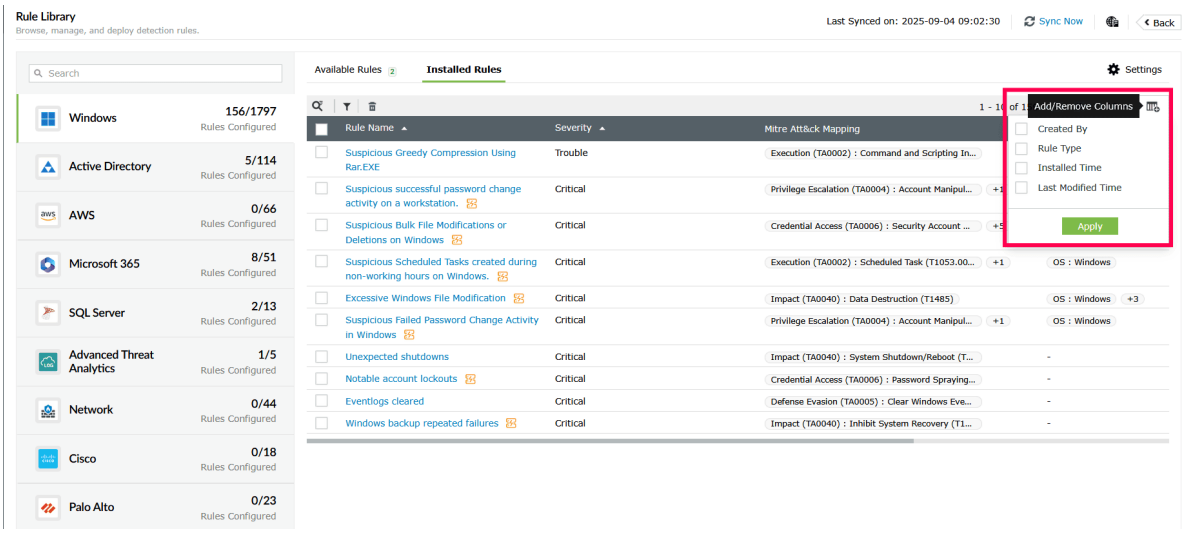




Figure 10: Customizing columns in the Installed Rules tab

13. Select the checkboxes next to the rules you want to delete and click the 🗑 icon.

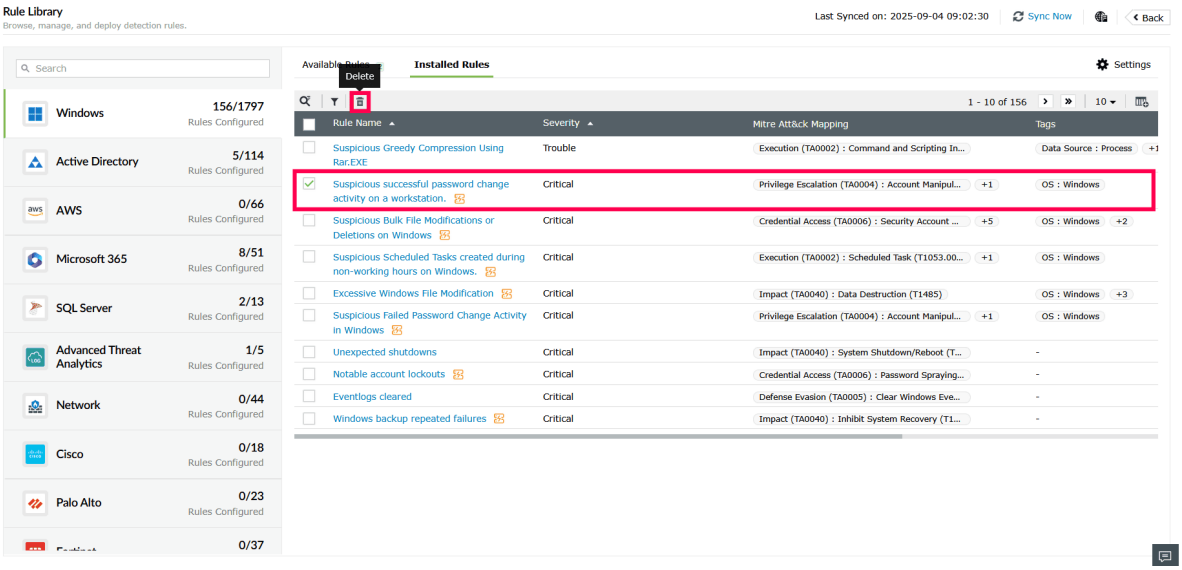


Figure 11: Deleting rules from the Installed Rules tab

14. In the pop-up that appears, click Yes to confirm the deletion.

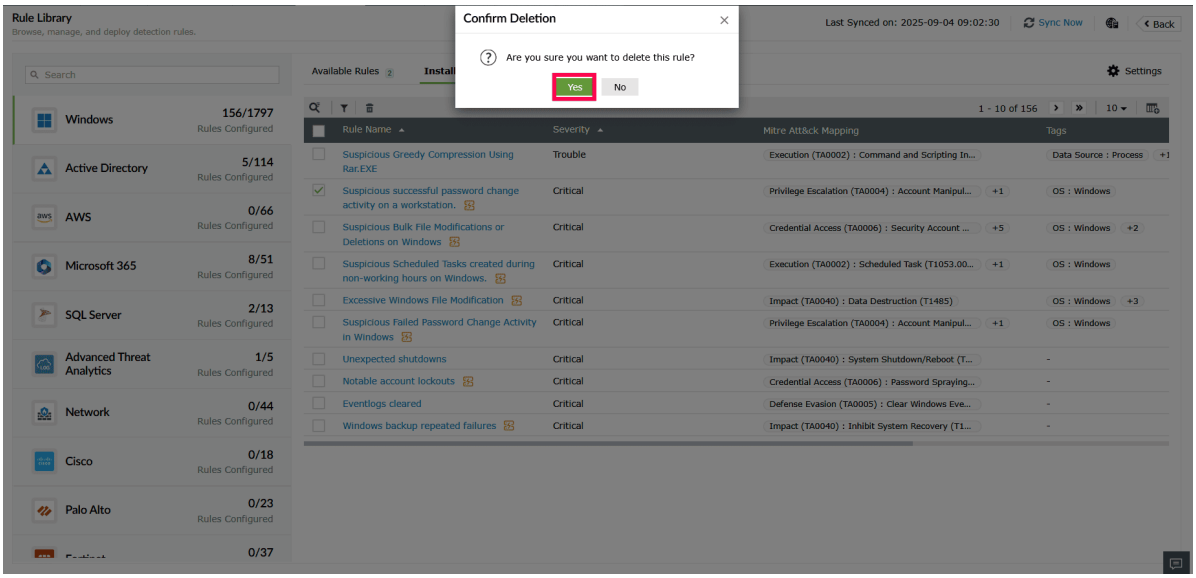


Figure 12: Deleting rules from the Installed Rules tab

Read also

This page detailed the steps to install rules from the Rule Library. To configure auto-install and rule update settings, refer to the following articles:

- Configuring auto-install settings
- Configuring Rule Update Settings

10.1.4.3. Configuring auto-install settings

Last updated on: September 12, 2025

In this page

Overview

Steps to configure auto-install settings

Overview

This page explains how to configure auto-install settings for rules in the Rule Library. This capability enables the automatic installation of rules based on their severity level.

Steps to configure auto-install settings

1. In the Rule Library page, navigate to Settings.

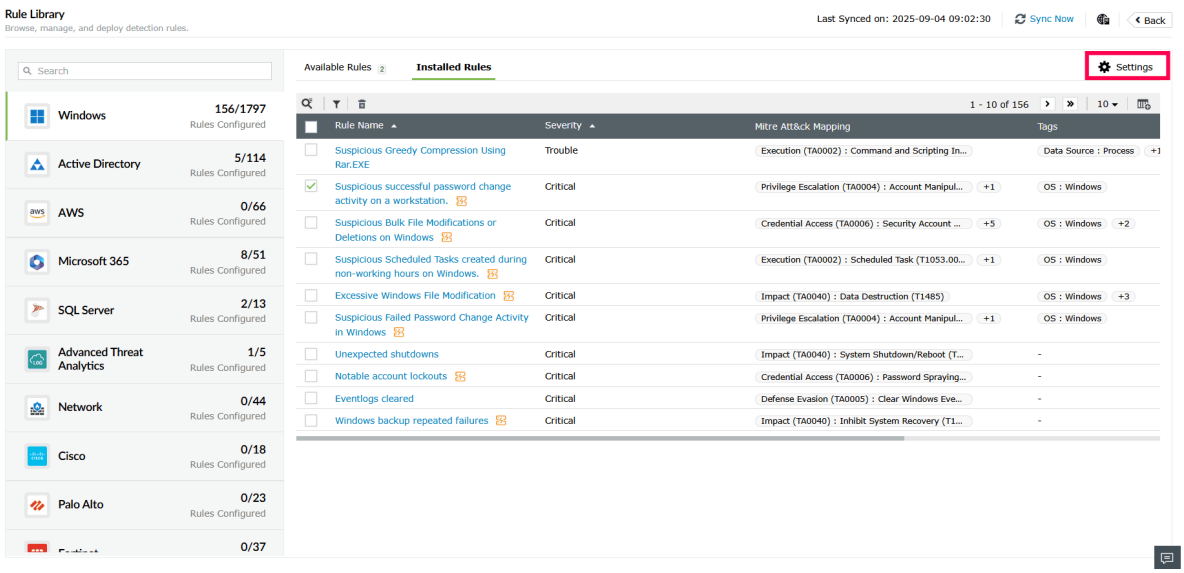
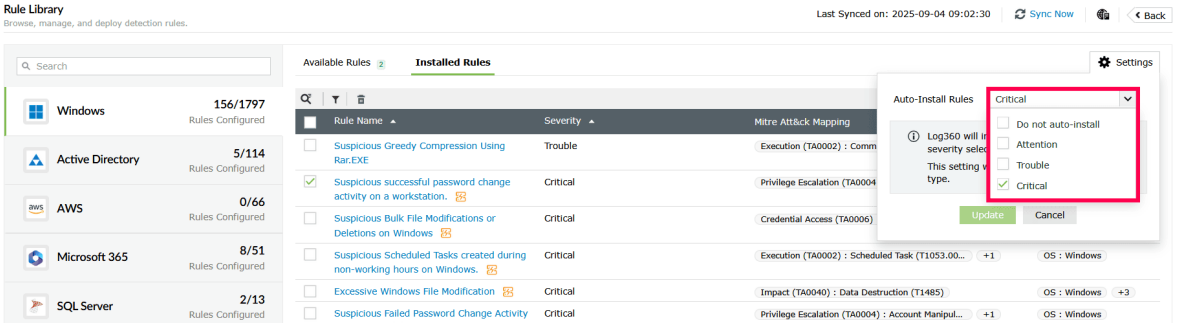


Figure 1: Configuring auto-install settings

2. From the Auto-Install Rules dropdown, select the severity levels for which rules should be automatically installed, such as Critical, Trouble, or Attention.



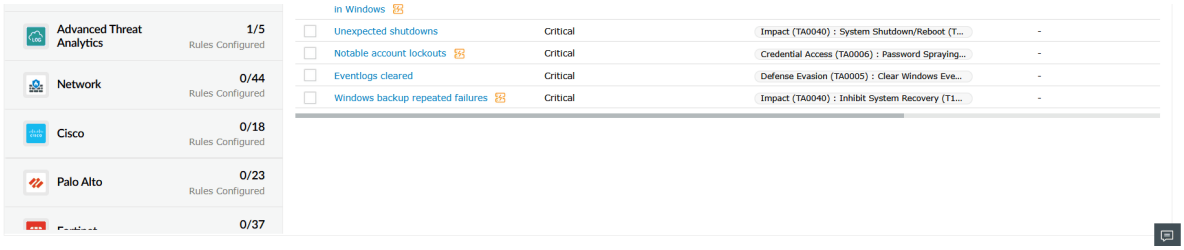


Figure 2: Configuring Auto-Install Rules

3. To disable auto-install, select Do not auto-install.
4. Click Update to save your changes.

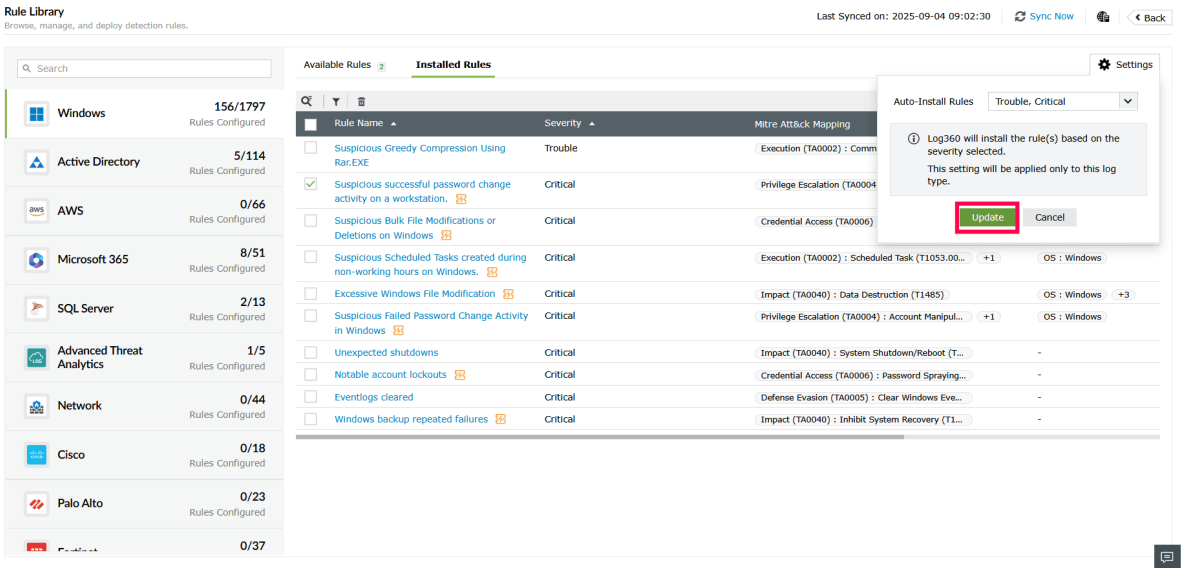


Figure 3: Configuring Auto-Install Rules

> NOTE
>
> Rules that are highly computational will be installed in a disabled state by default.

5. Auto-install settings are applied per Rule Library category, so configure them individually for each category as needed.
6. Rules installed through auto-install are activated automatically, but you must manually enable any associated alert profiles if required.

> NOTE
>
> Severity of the pre-defined rules is provided by ManageEngine Log360 team at the time of creation.

Read also

This page explained how to enable automatic installation of rules based on severity levels. To learn how to manage and configure these rules in your environment, refer to:

- Configuring Rule Update Settings
- Installing Rules

10.1.4.4. Configuring Rule Update Settings

Last updated on: September 12, 2025

In this page

Overview

Pre-requisites

Steps to configure Rule Update Settings for:

Environments connected to the internet

Offline or air-gapped environments

Overview

Rule Update Settings ensure that your system consistently receives the latest rule updates from Security Intelligence Pack, our cloud repository, enabling accurate and reliable threat detection. For environments with internet connectivity, you can configure automatic synchronization or perform manual updates from the cloud server. For offline or air-gapped environments, rule updates can be applied by downloading the latest Rule Library package and configuring the system to use it locally.

Pre-requisites

Before configuring Rule Update Settings, ensure the following:

- Whitelist the domain static.zohocdn.com in your firewall or network security settings to avoid any connection blocks.
- The user creating scheduled tasks must have the necessary permissions to:
  - Access the script file.
  - Access the directory specified by the -targetDir parameter.
- The user creating the cron job must have:
  - Read and execute permissions for the script file.
  - Write access to any directories the script interacts with, such as log or download folders.
- Ensure curl is installed and accessible for the user running the cron job, as it is required to download the ZIP files.

Steps to configure Rule Update Settings for:

Environments connected to the internet

1. Navigate to the Rule Library page.

2. In the top-right corner, click the icon and select static.zohocdn.com from the drop-down.
3. Click Save to apply the changes.
4. Click Sync Now to fetch the latest rules immediately.

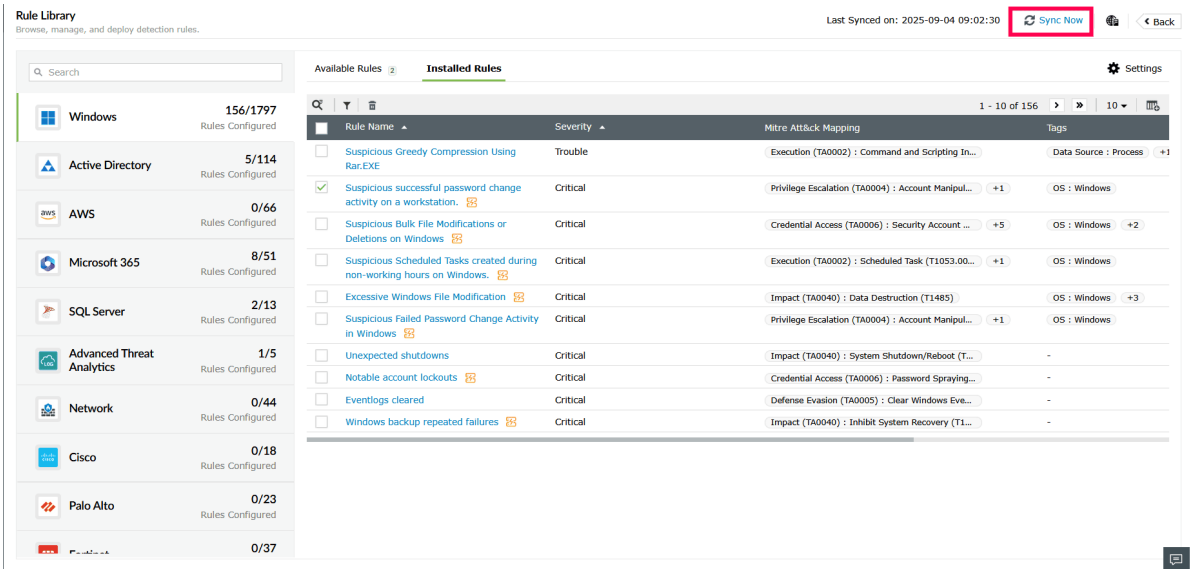


Figure 1: Syncing the Rule Library

5. A scheduled synchronization job also runs every 6 hours to update rules automatically.

Offline or air-gapped environments

1. Go to the Rule Library page.
2. In the top-right corner, select the icon and select Localhost from the drop-down.
3. Click Save to apply the changes.

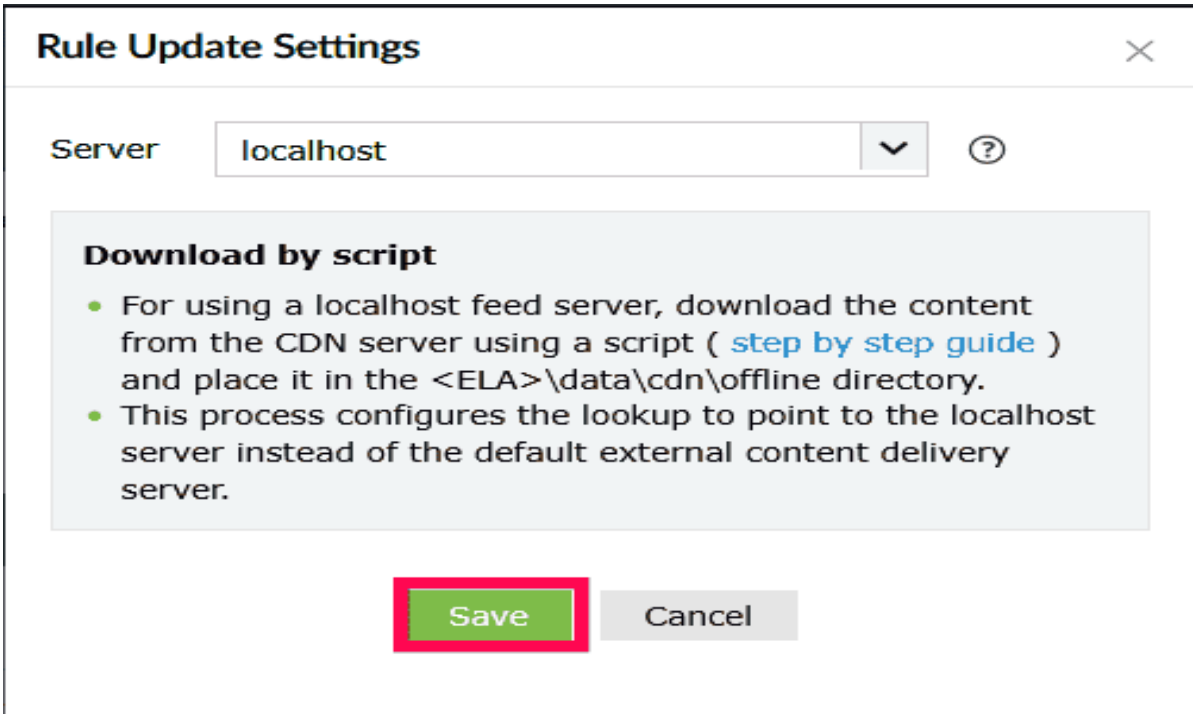


Figure 2: Configuring Rule Update Settings

4. Download the latest Rule Library ZIP file.
5. Place the downloaded log360library.lpm file in the following folder on the server: {server.home}\data\cdn\offline
6. The system extracts and applies the updated rules automatically.
7. If auto-install is enabled, rules matching the configured severity levels will be installed after syncing.

Downloading Rule Library ZIP files

1. Download the latest Rule Library file using the provided script:

> NOTE
>
> The following scripts are located in the path <Installed Dir>\Log360\tools\

- Windows: download-log360library.bat
- Linux: download-log360library.sh

2. Run script file to download the latest log360Library ZIP file.
3. To automate the download process, you can schedule the script to run at regular intervals using:
   - Task Scheduler on Windows
   - Cron Job on Linux

Steps to schedule a PowerShell script every 6 hours in Task Scheduler

1. Press Win + R to open the Run dialog box.
2. Type taskschd.msc, and click OK.

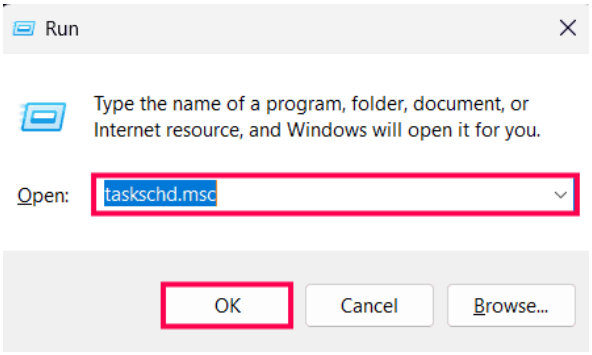


Figure 3: Opening the Task Scheduler

3. Click Create Task.

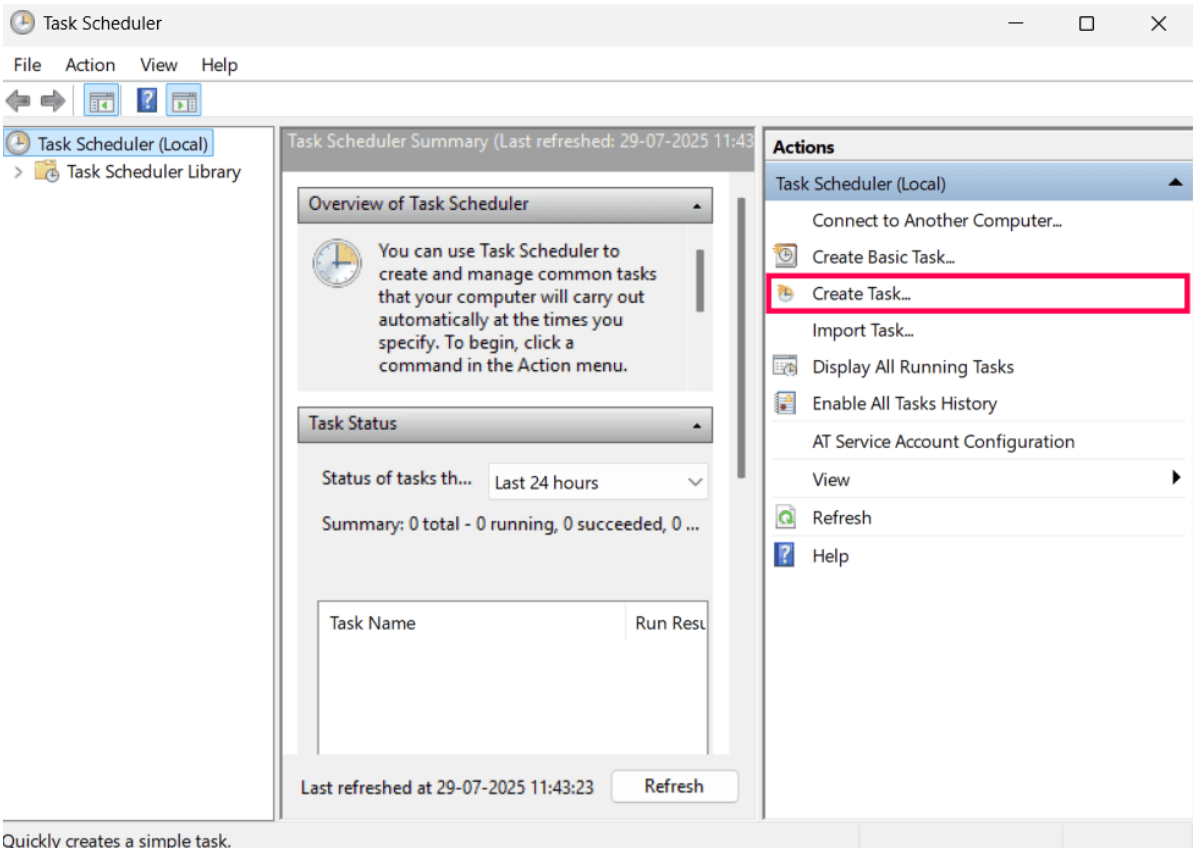


Figure 4: Creating a new task in Task Scheduler

4. In the General tab:
    - Enter a name.
    - (Optional) Add a description.
    - Select Run whether user is logged on or not.

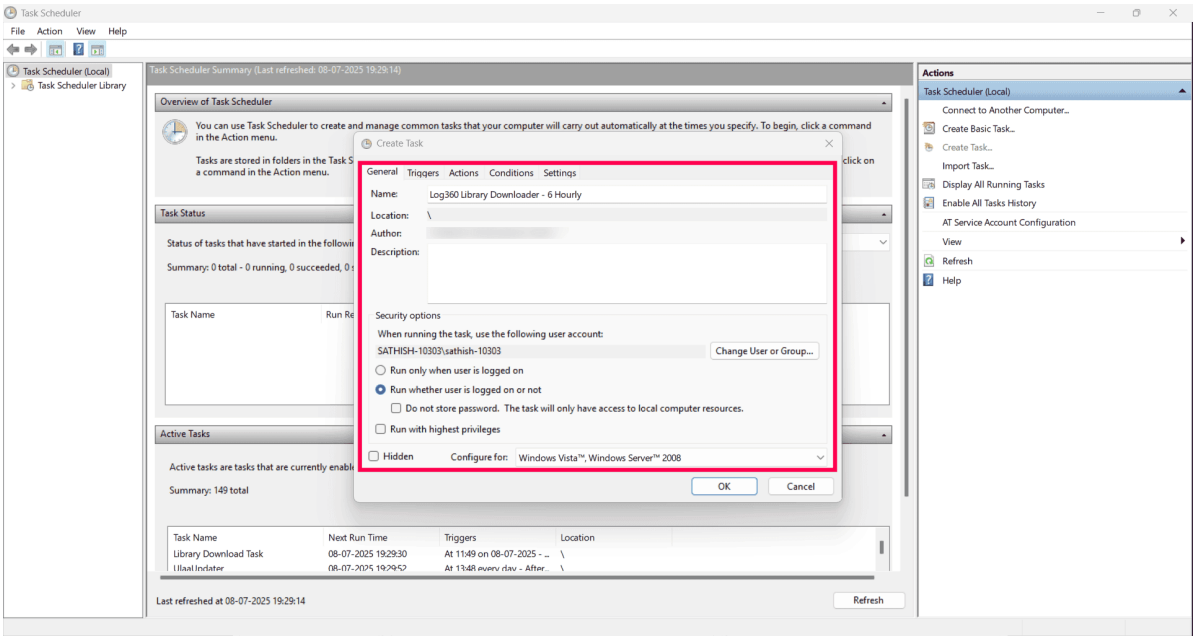


Figure 5: Configuring General settings

5. Go to the Triggers tab and click New.

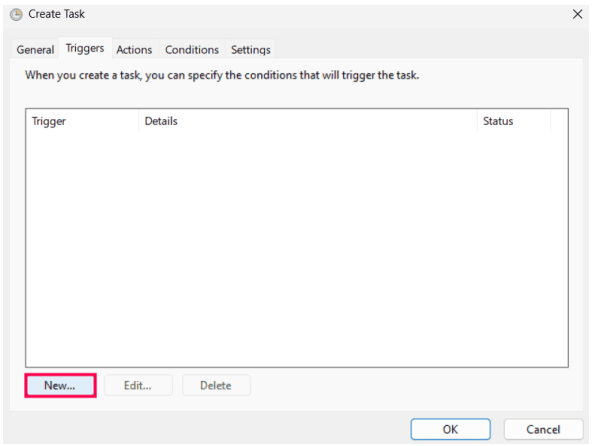


Figure 6: Creating a new Trigger

6. In the New Trigger window:
    - From the Begin the task dropdown, select On a schedule.
    - Under Settings, choose Daily and set the Start date and time.
    - Under Advanced settings, check Repeat task every and set it to 6 hours.
    - In the For a duration of field, select 1 day.
    - Enable Stop task if it runs longer than and set it to 30 minutes.

- Ensure the Enabled checkbox is selected.
- Click OK to save the changes.

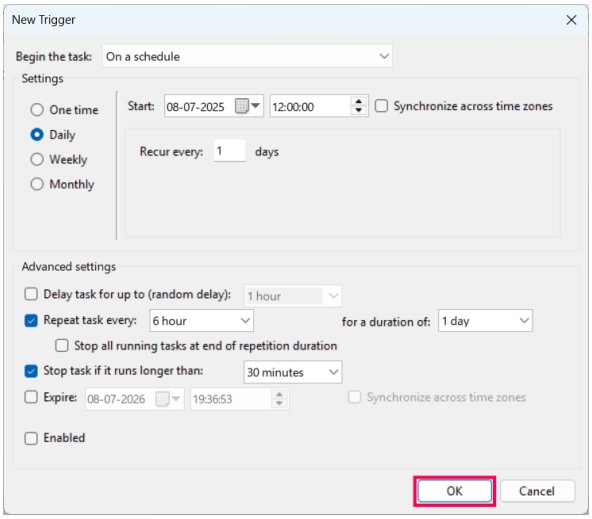


Figure 7: Configuring task triggers

7. Navigate to the Actions tab and click New.
8. In the Actions window:
   - In the Action dropdown, select Start a program.
   - In the Program/script field, enter cmd.
   - In the Add arguments (optional) field, enter: /c "<download_path>\download-log360library.bat -targetDir <folder where files need to be downloaded>"

> NOTE
>
> :If the -targetDir parameter is not provided, the files will be downloaded to the script file's parent directory by default.

   - Click OK.

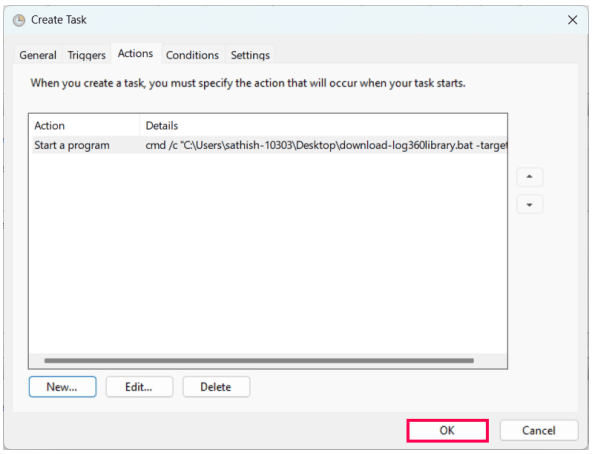


Figure 8: Configuring task actions

9. Navigate to the Conditions tab.
10. Go to the Settings tab.
11. In the Settings tab:
    - Select the checkbox next to Allow task to be run on demand.
    - Select the checkbox next to Stop the task if it runs longer than, and set the duration to 1 hour.
    - Select the checkbox next to If the running task does not end when requested, force it to stop.
    - In the If the task is already running, then the following rule is applied dropdown, choose Do not start a new instance.
    - Click OK to save the task.

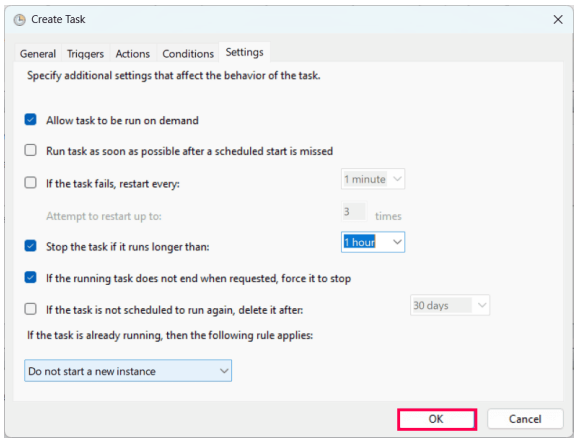


Figure 9: Configuring additional settings

- When prompted, enter your Windows username and password.
- To verify the configuration, right-click the task in Task Scheduler and select Run.

Steps to schedule a shell script for every 6 hours in Cron Job

1. Set the script as executable before running it by using the following command: chmod +x <script_file_path>/download-log360library.sh
2. Run the crontab -e command to open the crontab editor.
3. Insert the following cron entry to run the script every 6 hours: 0 */6 * * * <script_file_path>/download-log360library.sh --target-dir "<download_path>

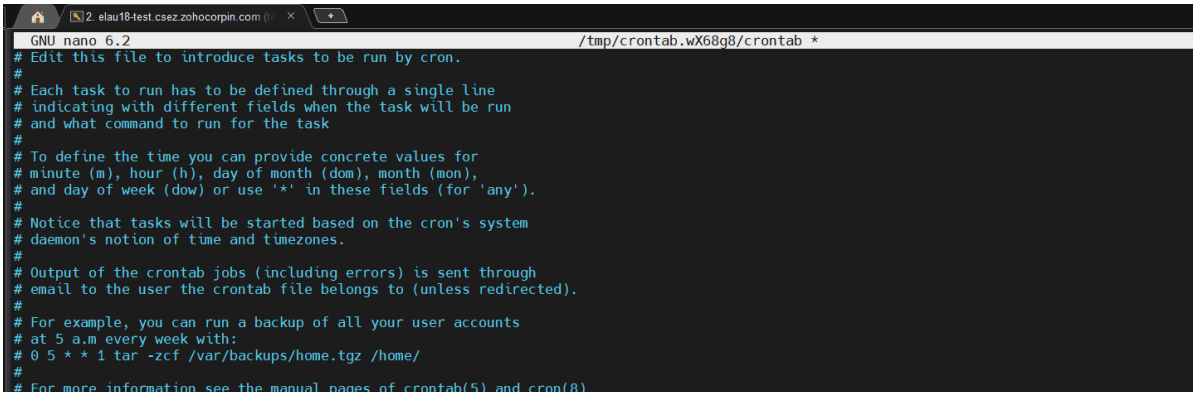




Figure 10: Adding the cron command

4. You can modify the path or time as required.
5. Save and exit the crontab editor:
   - Press Ctrl + O to save.
   - Press Ctrl + X to exit.
6. Verify the cron job installation by running the command: crontab -l

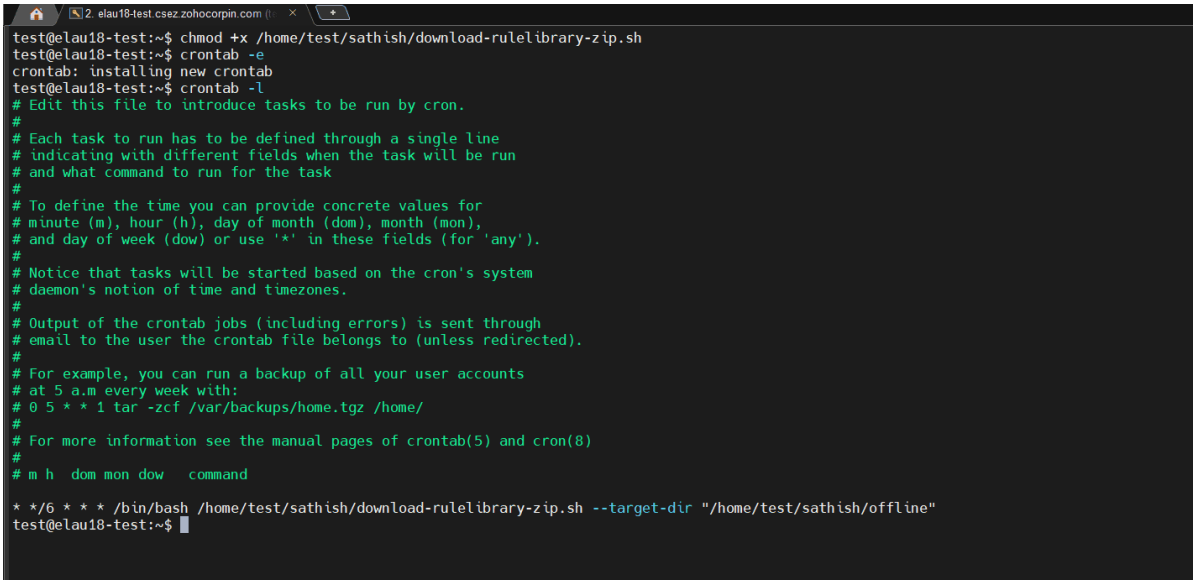


Figure 11: Saving and verifying the cron job

7. Check logs to confirm execution:
   - Review the script's log file: <download_path>/logs/download.log
   - Alternatively, review system logs such as var/log/cron.log depending on your operating system.

Read also

This page explained how to keep your Rule Library updated in online and offline environments. To learn more about the Rule Library and managing its capabilities, refer to:

- About Rule Library
- Installing Rules

10.1.5.1. Advanced Threat Analytics

Last updated on: September 12, 2025

In this page

Add users

Manage Users

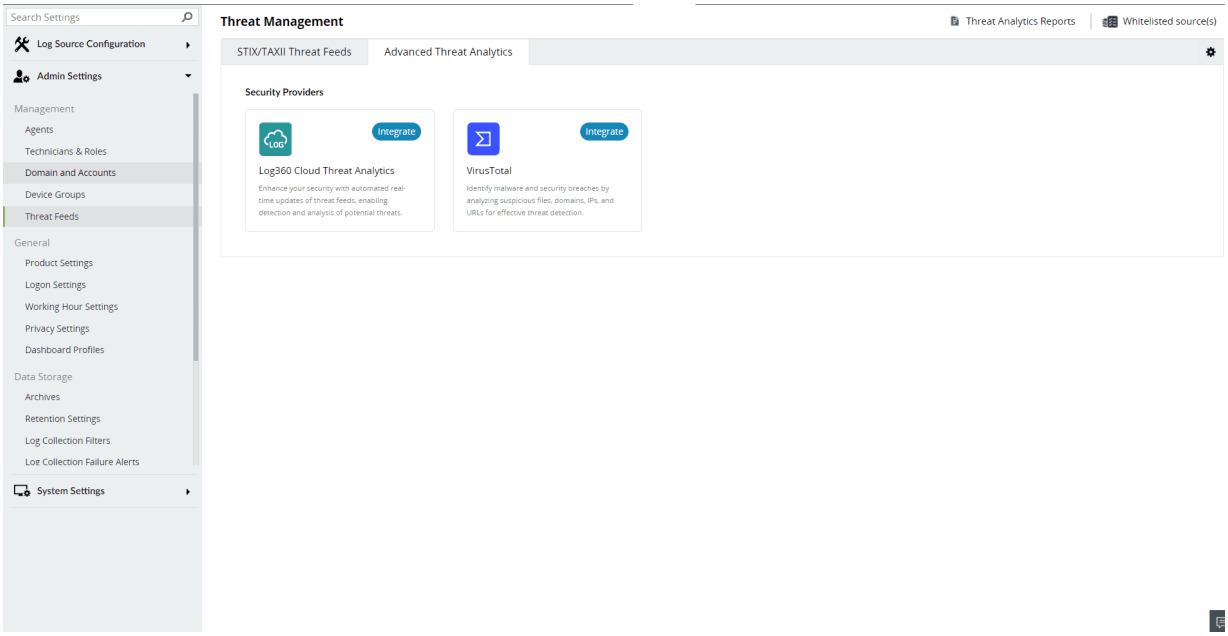
Import users from Active Directory

Creating custom user roles

The Advanced Threat Analytics feature gives valuable insights into the severity of threats using the reputation score for potentially malicious URLs, domains, and IP addresses. To utilize the Advanced Threat Analytics feature in EventLog Analyzer, an add-on has to be purchased.

Advanced Threat Analytics add-on purchase:

- To purchase the Advanced Threat Analytics add-on, please click here.
- After purchasing and applying the add-on license, go to Settings → Admin Settings → Management→ Threat Feeds. The Advanced Threat Analytics tab will be present next to the STIX/TAXII Threat Feeds tab. Configure the respective feeds to access the threat analytics data.



Overview

1. Vendor support:
   EventLog Analyzer supports the following vendors for the Advanced Threat Analytics data:
   - Log360 Cloud Threat Analytics

Default integration from Log360 Cloud suite. This can be accessed once the add-on is purchased.

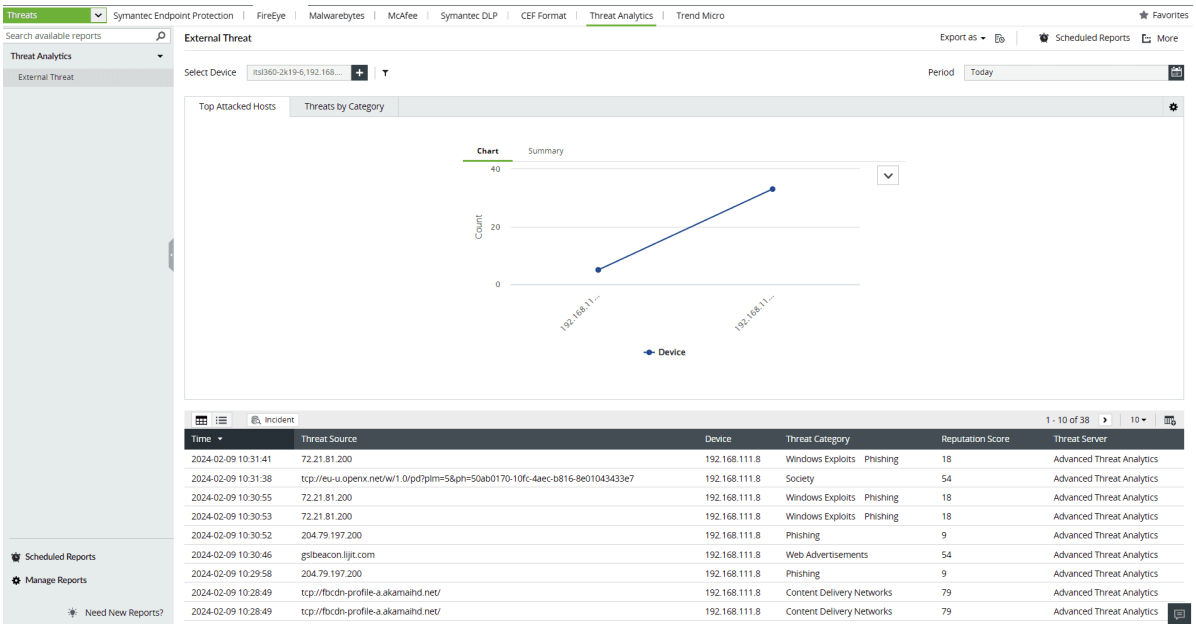
- VirusTotal
  Third-party threat feed integration. This follows the Bring Your Own Key(BYOK) model. If you have bought VirusTotal access separately, you can use your API key and get the threat analytics information in EventLog Analyzer.

2. Access
   Here's how users can access the Adavanced Threat Analytics information for different usecases:
   - For investigation: To investigate the external threat sources, the threat analytics information can be accessed through the External Threat report and the Incident Workbench.
   - Detection: The Default Threat alert criteria detects interaction with external threat sources. Once the Advanced Threat Analytics add-on is applied, the alerts will be accurately fine tuned to reduce false positives.

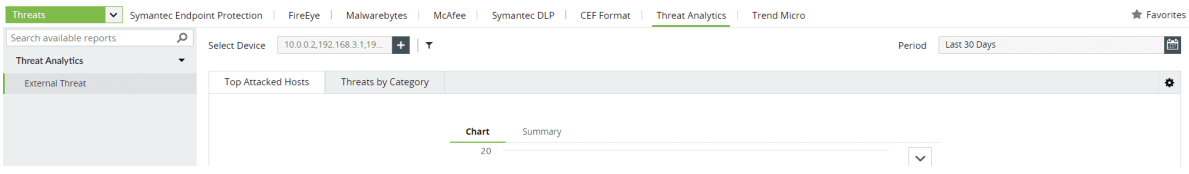
External Threat report

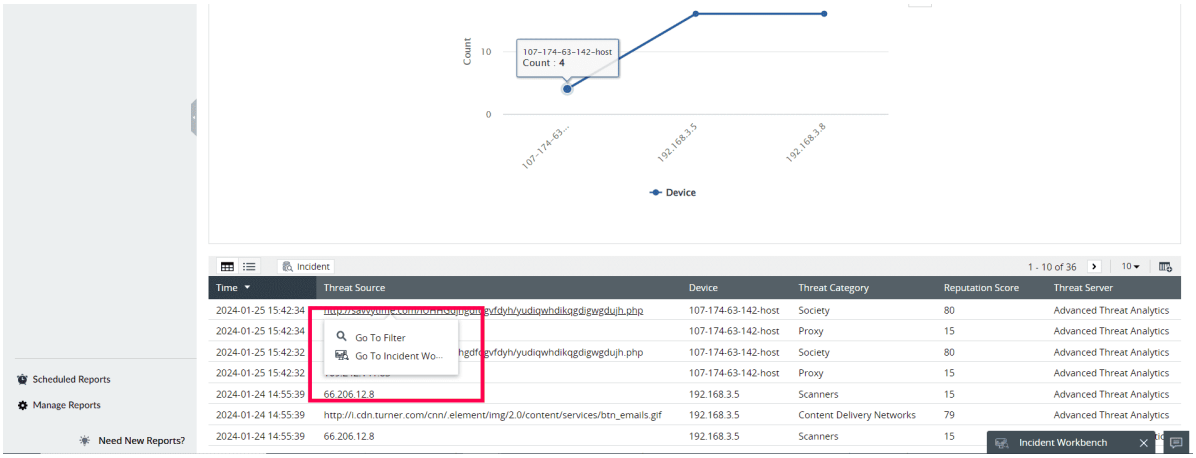
Navigation: EventLog Analyzer home > Reports > Select Threats from the drop-down in the top left corner > Threat Analytics > External Threat
The External Threat report contains the information on the source of the threat, severity, reputation score, and more.

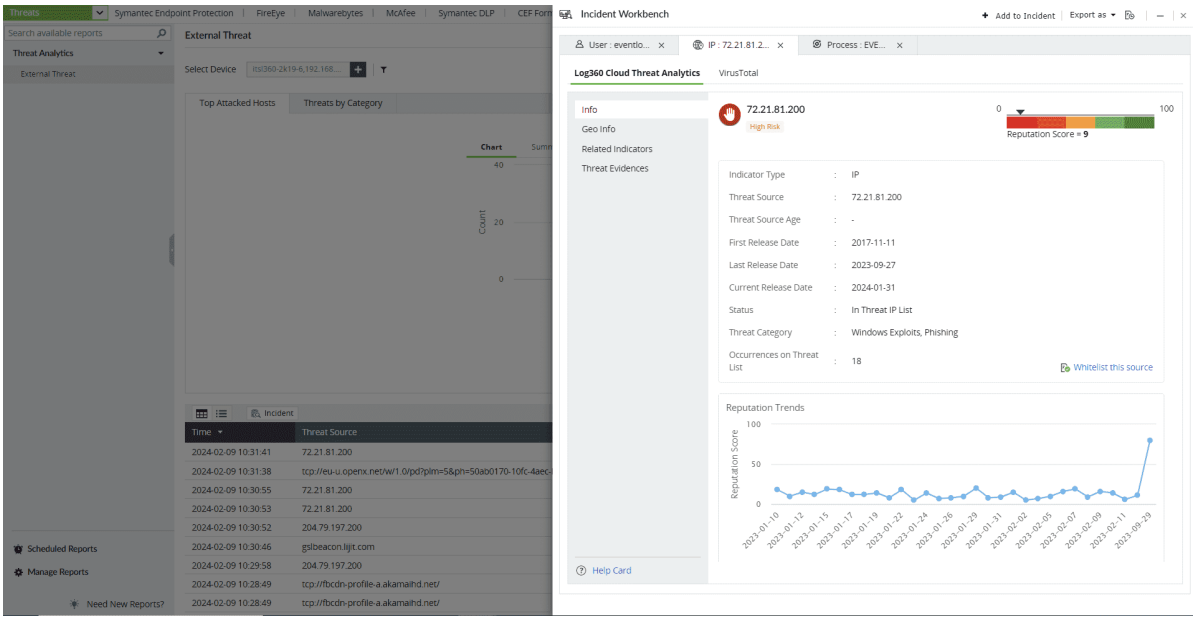
- View reports of Top Attacked Hosts and Threats by Category for the selected period.



- Click on URLs and IPs in the Threat Source column and select Go To Incident Workbench to get contextual risk data from the integrated threat feeds

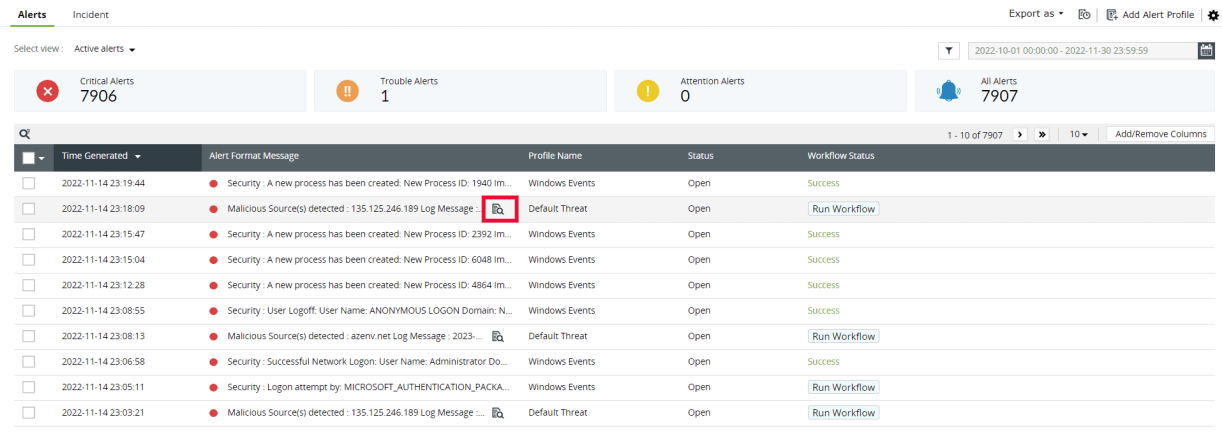






Alerts

View the generated alerts on the Alerts summary page, and click on the Threat Analysis icon to open the Incident Workbench and analyze further.





10.1.5.2. Constella Intelligence

Last updated on: September 12, 2025

In this page

Add users

Manage Users

Import users from Active Directory

Creating custom user roles

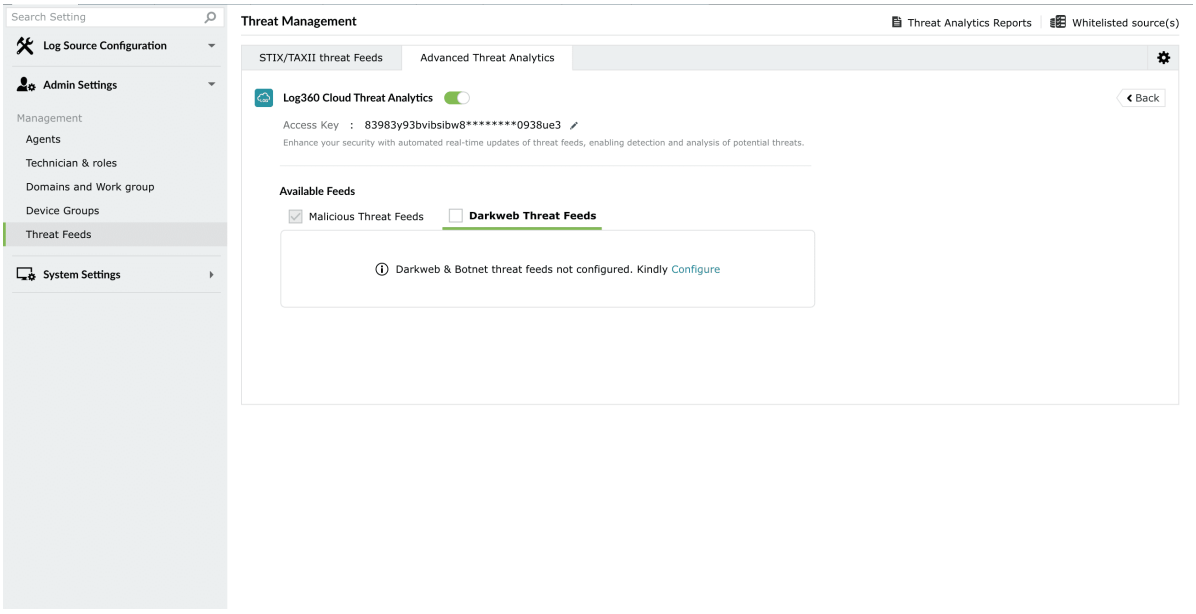
Constella Intelligence is a digital risk protection platform that provides dark web monitoring. This integration with EventLog Analyzer enables users to identify personal information such as credit card number, email information, usernames and credentials that are leaked in the dark web. Users can also

- Gain visibility into breaches using the Threat Analytics dashboard
- Get breach reports
- Get predefined alerts for supply chain breaches

Configuring Dark Web threat feeds

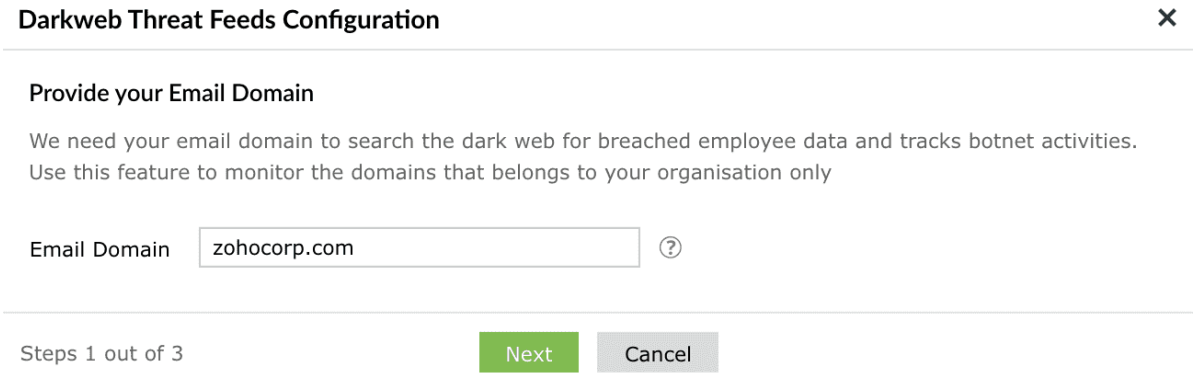
Once you have purchased the Advanced Threat Analytics add-on and applied the license, head to the Advanced Threat Analytics page.
Navigation: Settings → Admin Settings → Management → Threat Feeds → Advanced Threat Analytics → Log360 Cloud Threat Analytics → Integrate
To get the access key, please follow the steps (Until step 2) in this help document.

- After pasting the access key in the Access Key box, Malicious Threat Feeds will be enabled automatically. To enable dark web threat feeds, switch to Dark Web Threat Feeds and click the Configure button.

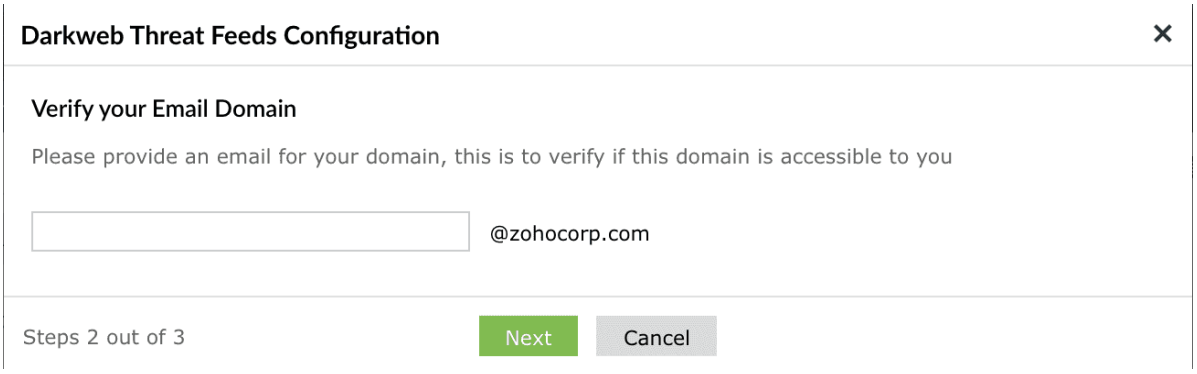


- Upon clicking Configure, a pop-up requesting an email domain to monitor for dark web exposure will be

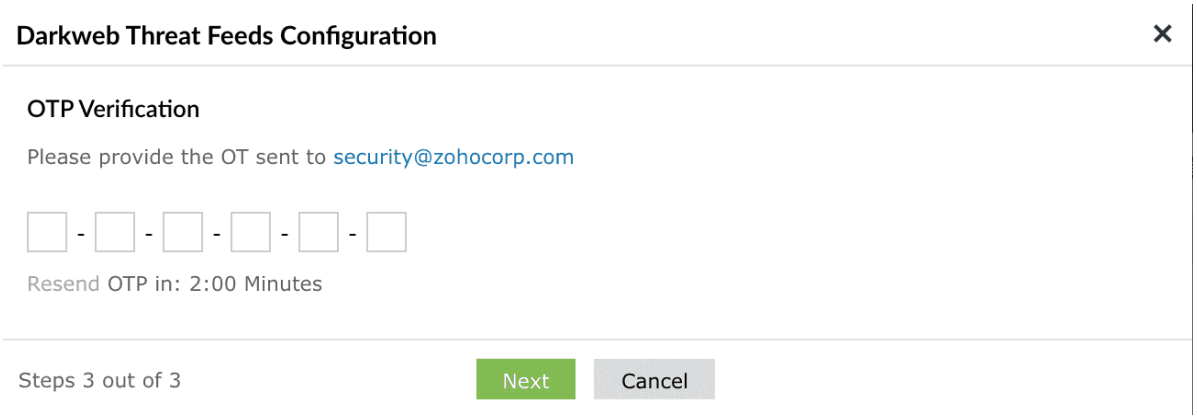
- Upon clicking Configure, a pop-up requesting an email domain to monitor for dark web exposure will be displayed. After entering the domain, you will be asked to provide a valid email address from that domain for verification.



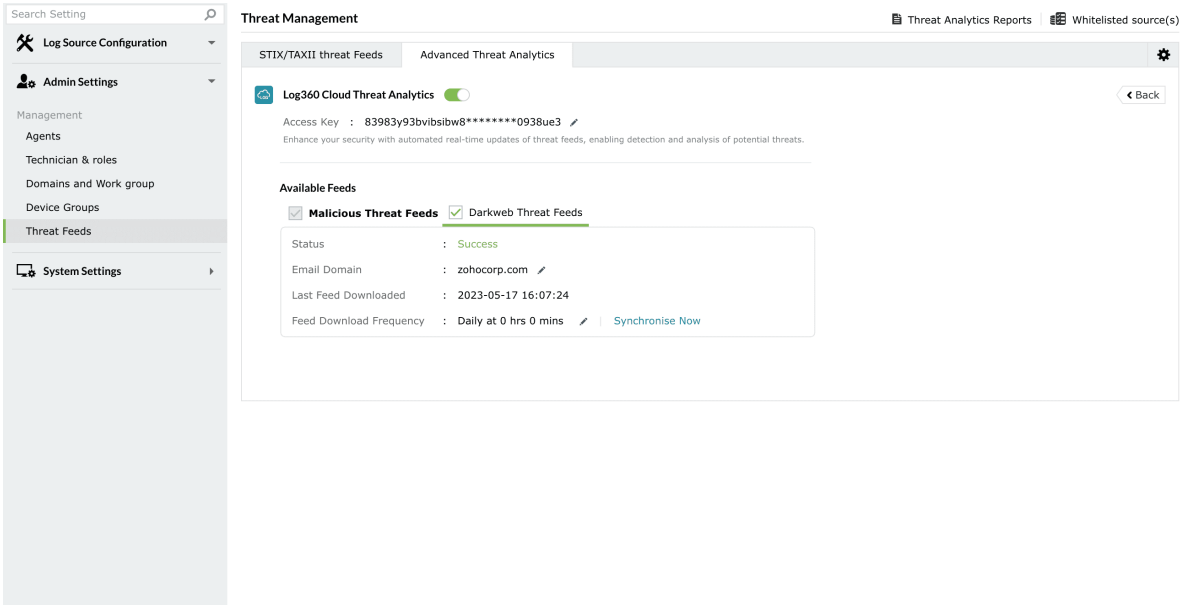
> **Note**
>
> Domain configuration for email is linked to licensing. You can only configure domains associated with licenses you have purchased.



- You will receive an OTP (One-Time Password) to the entered email address. Upon successful verification of the OTP, you will have successfully configured your domain for dark web breaches.



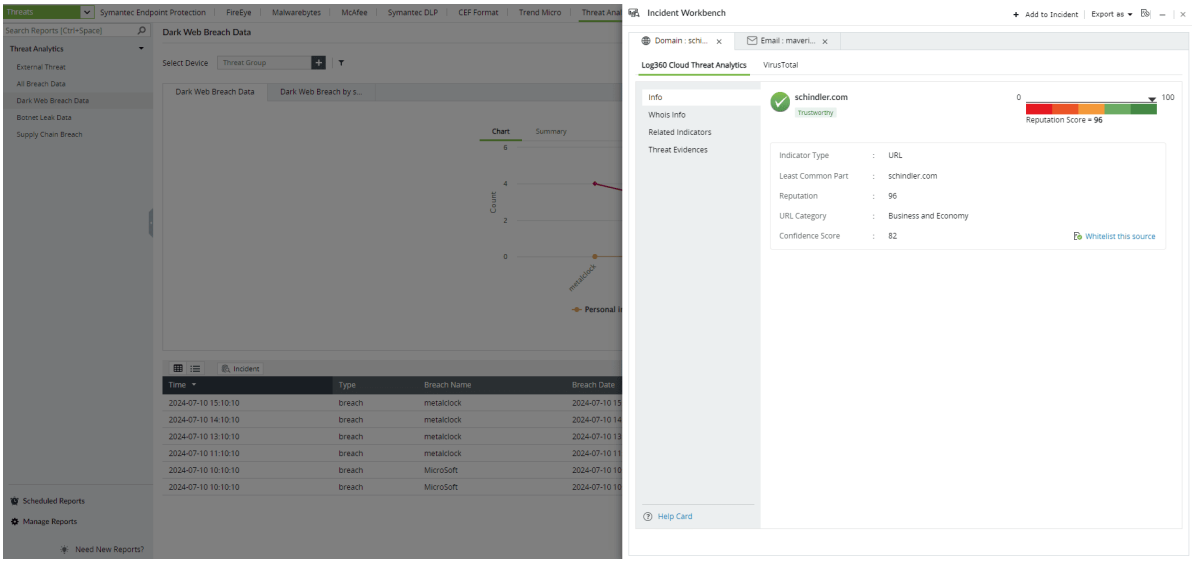
- You will see this page once your domain is successfully configured.



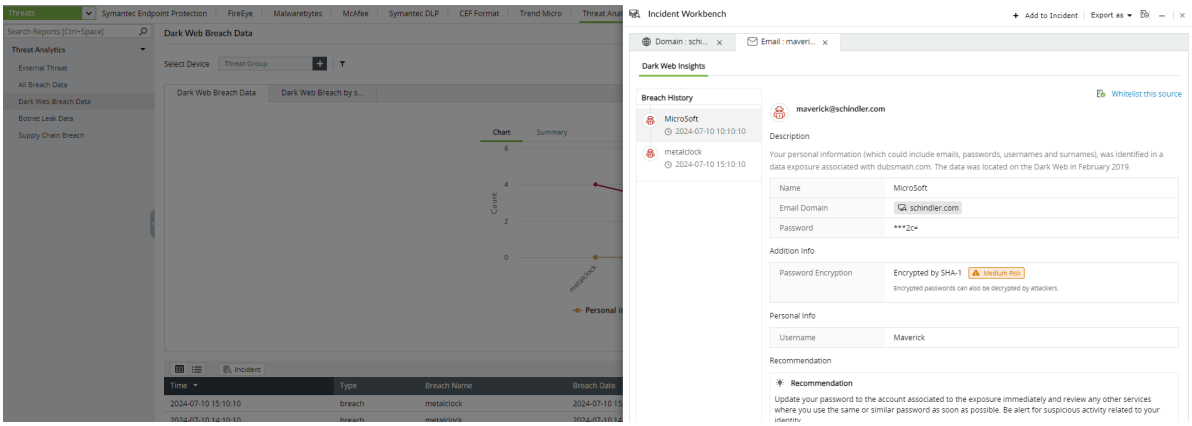
Analysis

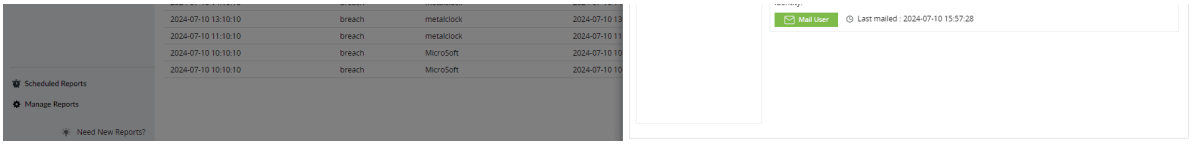
EventLog Analyzer provides both email and domain analysis for configured domains. Users will be able to send emails from the Incident Workbench to notify individuals whose data has been breached.

- Domain analysis for the configured domain



- Email analysis for the configured domain





EventLog Analyzer provides an alert profile for supply chain breaches. A supply chain breach refers to the breach where the email domain and the domain where the user's data was breached are different.

Troubleshooting tips:

- Ensure that L3C Feeds Server is reachable from ELA machine.
- Try reconfiguring Dark Web monitoring with your domain
- Ensure that the licensed domain and configured domain are the same.

For further information regarding configuring non-licensed domains, please contact support@eventloganalyzer.com

10.1.5.3. VirusTotal

Last updated on: September 12, 2025

In this page

Configuration

Analysis

Advanced threat analytics add-on in EventLog Analyzer

> **Note**
>
> VirusTotal is one of the largest live threat feeds that consolidates risk scores of IPs, URLs, Domains, and files from a wide range of security vendors. This integration in EventLog Analyzer follows the Bring Your Own Key(BYOK) model. If you have bought VirusTotal access separately, you can use your API key and analyze threat sources in EventLog Analyzer.

VirusTotal terms of service:

Users can access VirusTotal API in two ways:

1. Public API: Provides free access with specific limitations, including constraints on request frequency and access with lower priority.
2. Premium API: Provides exclusive access without limitations on request frequency and prioritized access, complemented by additional benefits.

Recommendation: For business workflows it is recommended to use Premium API for integration.
To learn more about VirusTotal, their terms of service, privacy policy, and API usage, please visit their website.

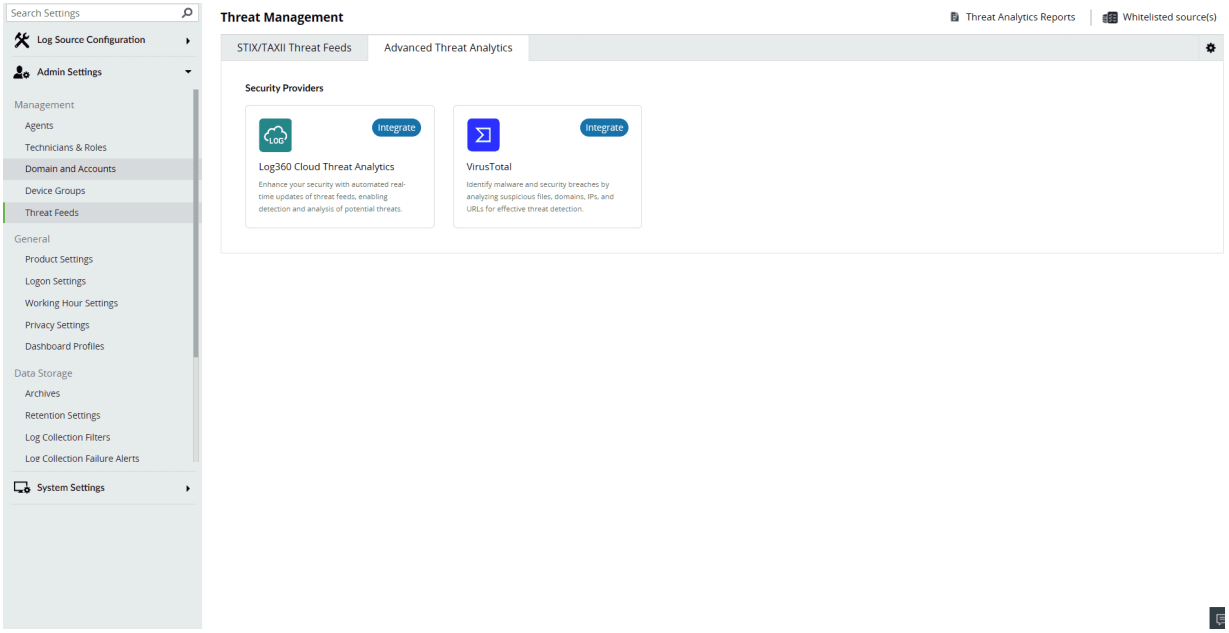
Configuration

> **Note**
>
> Please refer to VirusTotal's privacy policy to understand how user-submitted data is utilized for analysis, as well as their policies on data processing, sharing, retention, and deletion.

Once you have purchased the Advanced Threat Analytics add-on and applied the license, head to the Advanced Threat Analytics page.

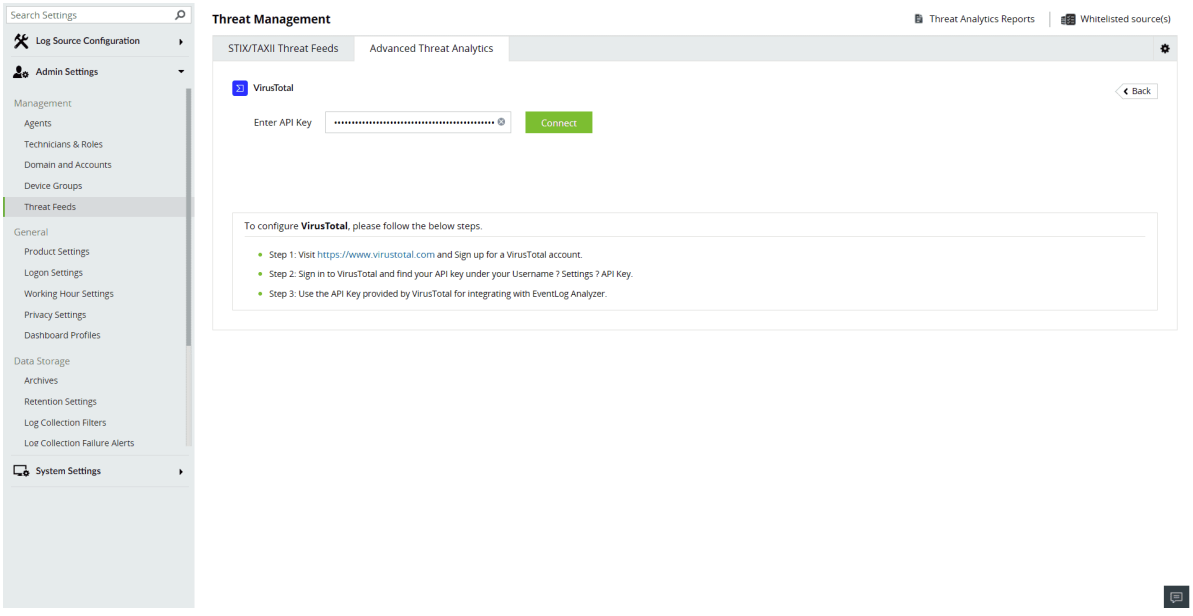
> Navigation: Settings → Admin Settings → Management→ Threat Feeds→Advanced Threat

Analytics → VirusTotal → Integrate

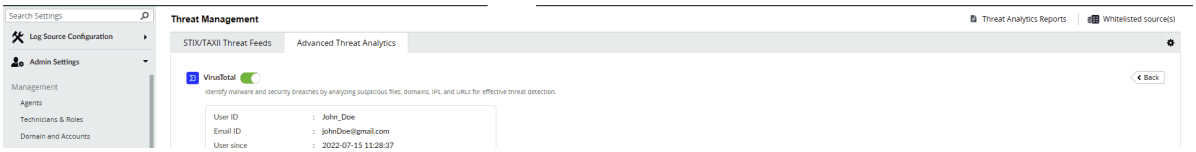


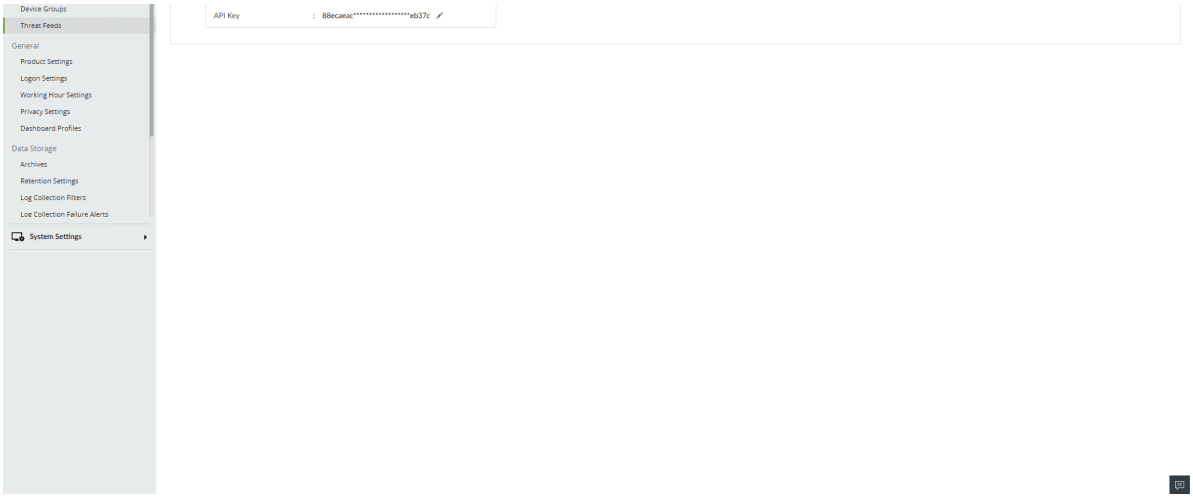
To get the API key:

1. Visit https://www.virustotal.com and sign up for a VirusTotal account.
2. Sign in to VirusTotal and find your API key and go to your Username→ Settings→API Key.
3. Use the API Key provided by VirusTotal for integrating with EventLog Analyzer.



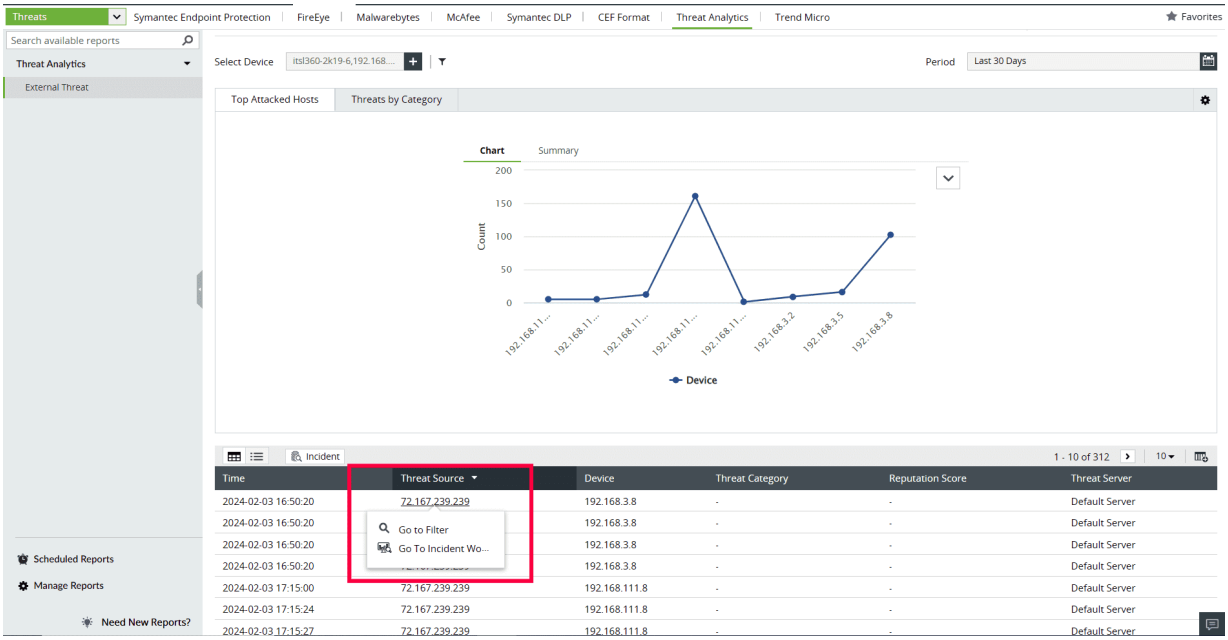
4. Paste the API key and click on Connect to finish configuring VirusTotal.





Analysis

In EventLog Analyzer, users can access the data from VirusTotal through the Incident Workbench. Learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer.

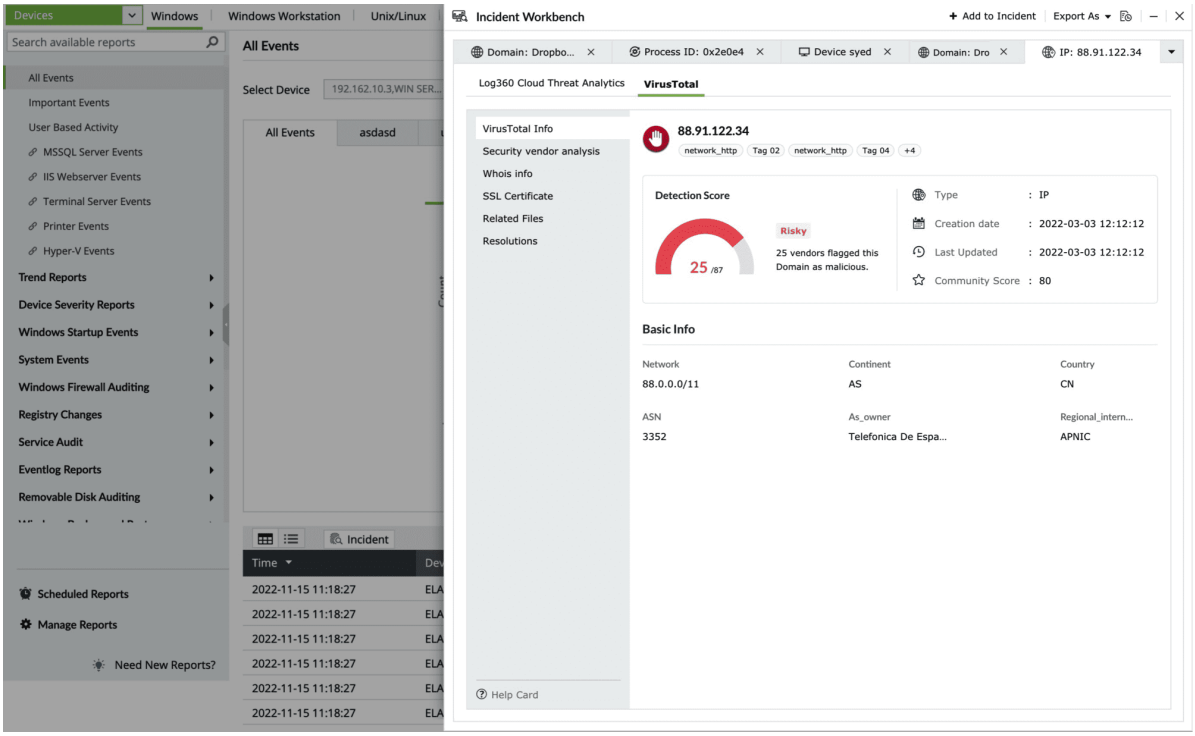


> **Note**
>
> To understand the different terminologies used in the VirusTotal reports, please use the Help Card in the bottom left corner.

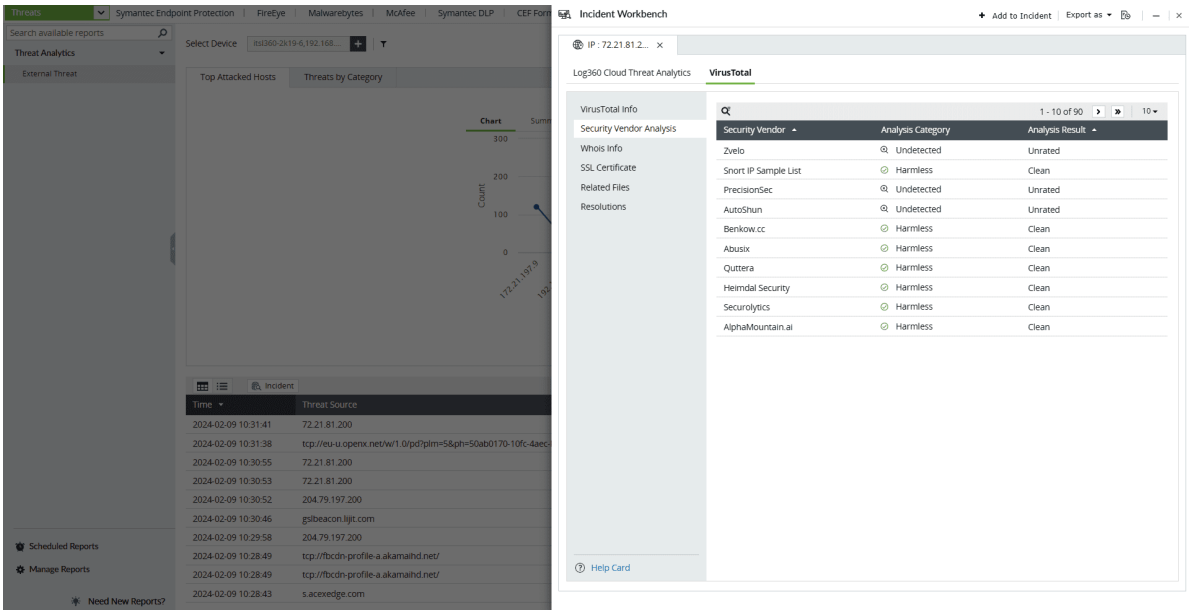
Select any IP, URL, or Domain to analyze in the Workbench. You can access the following data:

- VirusTotal note-box
  This section contains the Detection Score of the Threat Source, which is the number of security vendors who have flagged the source as risky out of all the security vendors. Along with this, the basic details and the geo note-box of the Threat Source are also available.

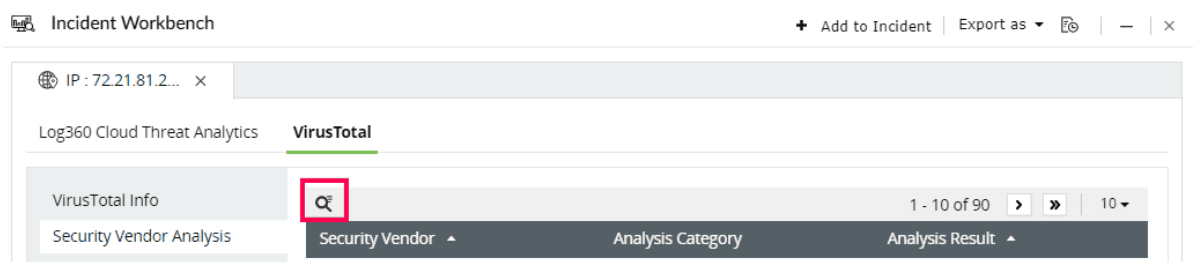
note-box of the Threat Source are also available.

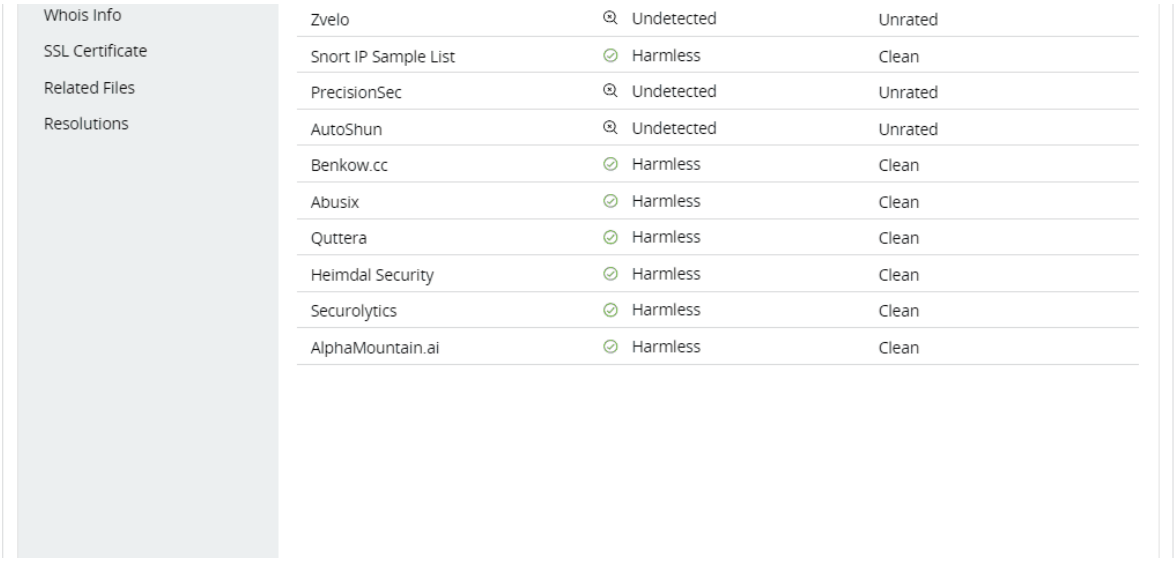


- Security Vendor analysis
  This section contains the individual analysis of 85+ security vendors such as SOCRadar, Fortinet, Forcepoint ThreatSeeker, and ArcSight Threat Intelligence.



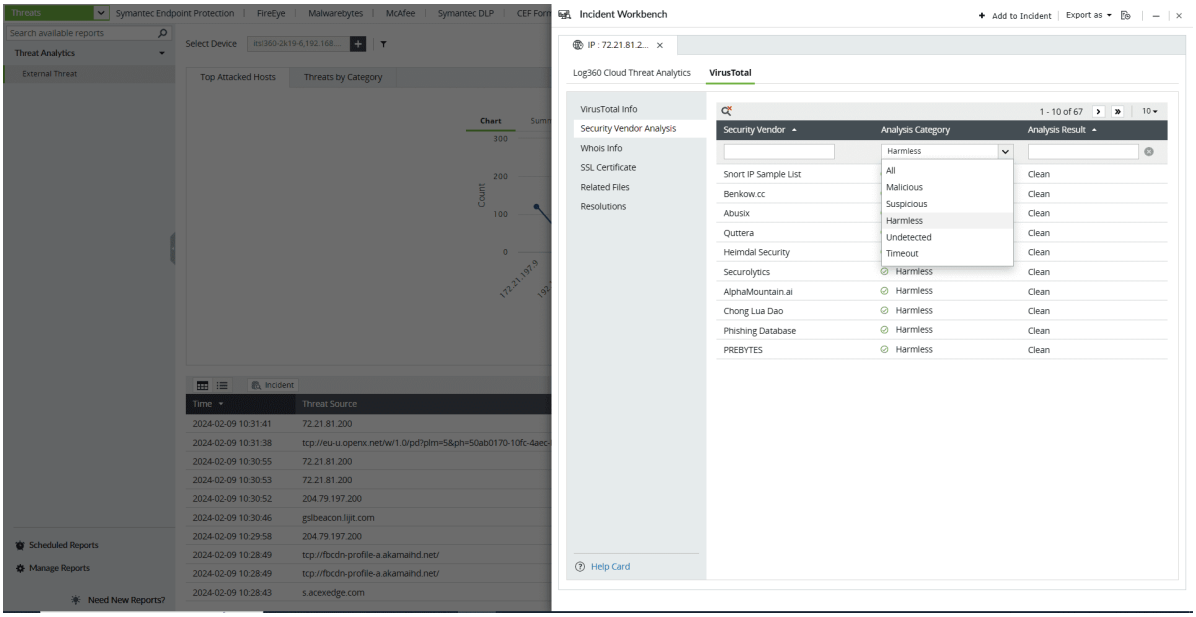
Click on the search icon in the top left corner to filter based on Security Vendor, Analysis Category, and Analysis Result.





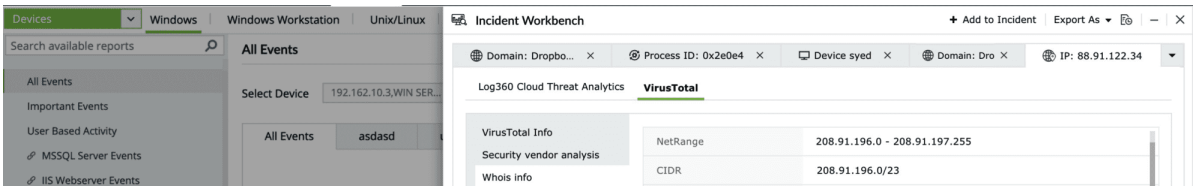
Here are the Analysis Categories:

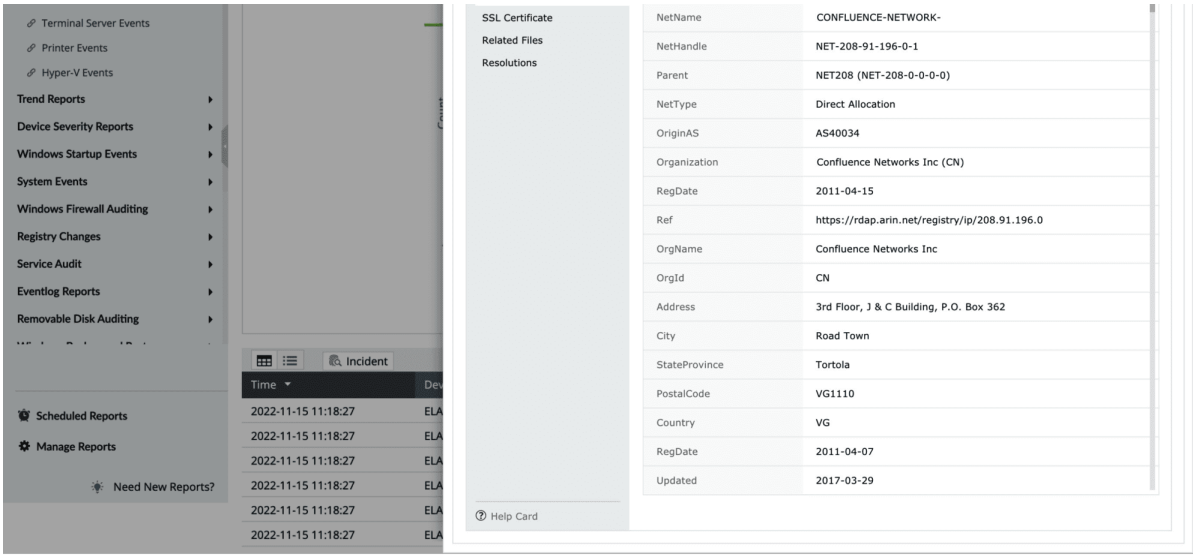
- Malicious
- Suspicious
- Harmless
- Undetected
- Timeout



- Whois note-box

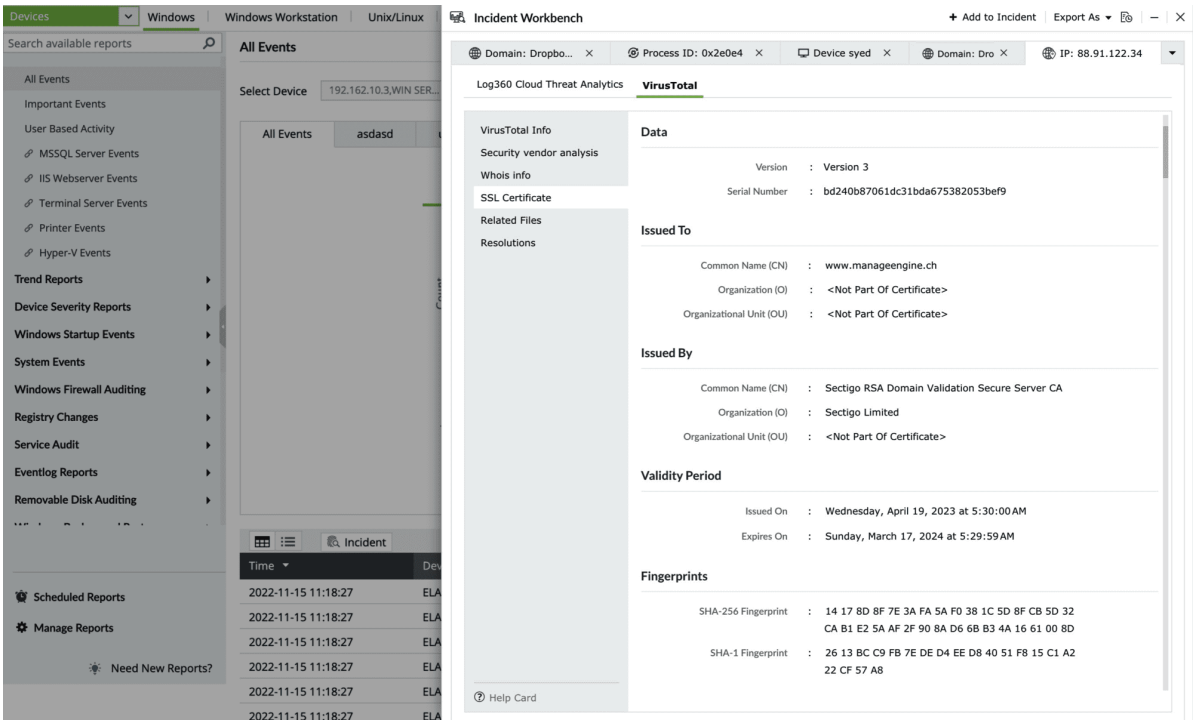
  This section contains the Whois note-boxrmation of the threat source domain.





- SSL Certificate

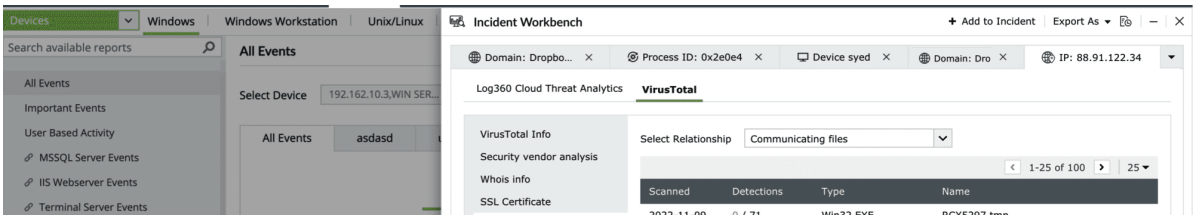
  This section contains details of the SSL certificate issued to the Threat Source and who issued it.

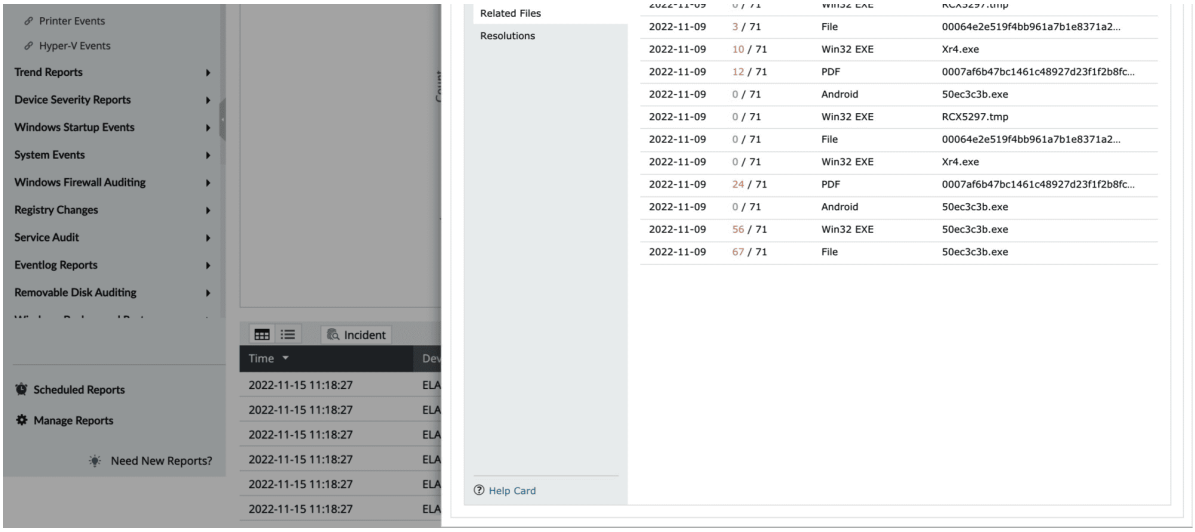


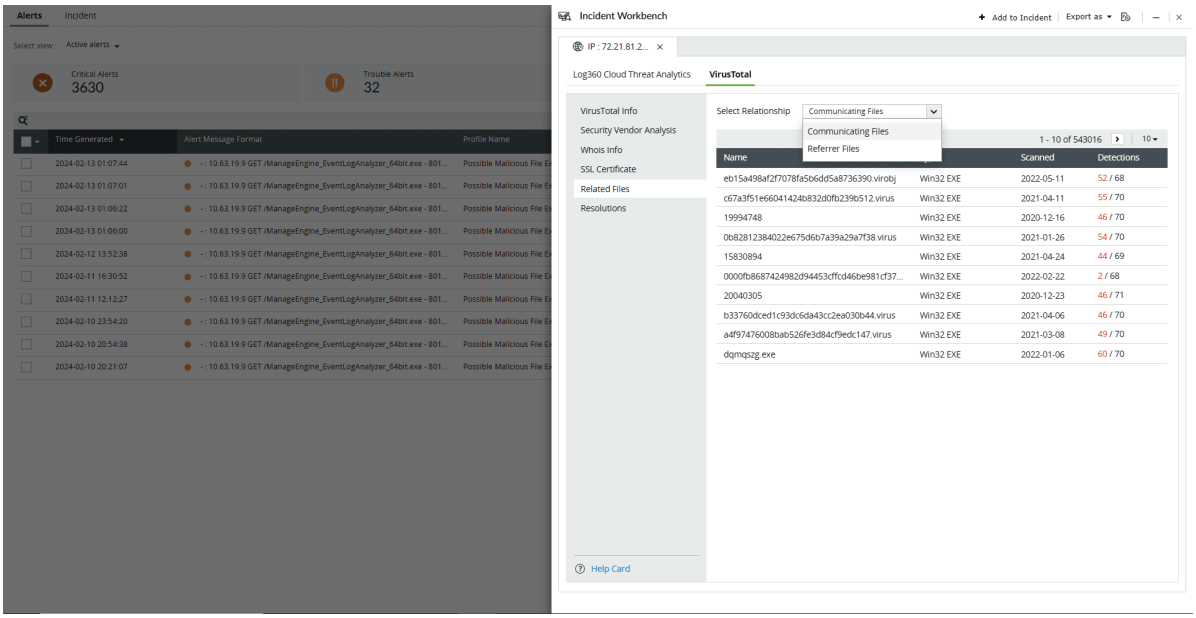
- Related Files

  This section maps the relationship of the files to the IP address in following ways:

  - Files communicating with the IP address
  - Files downloaded from the IP address
  - Files containing the IP address

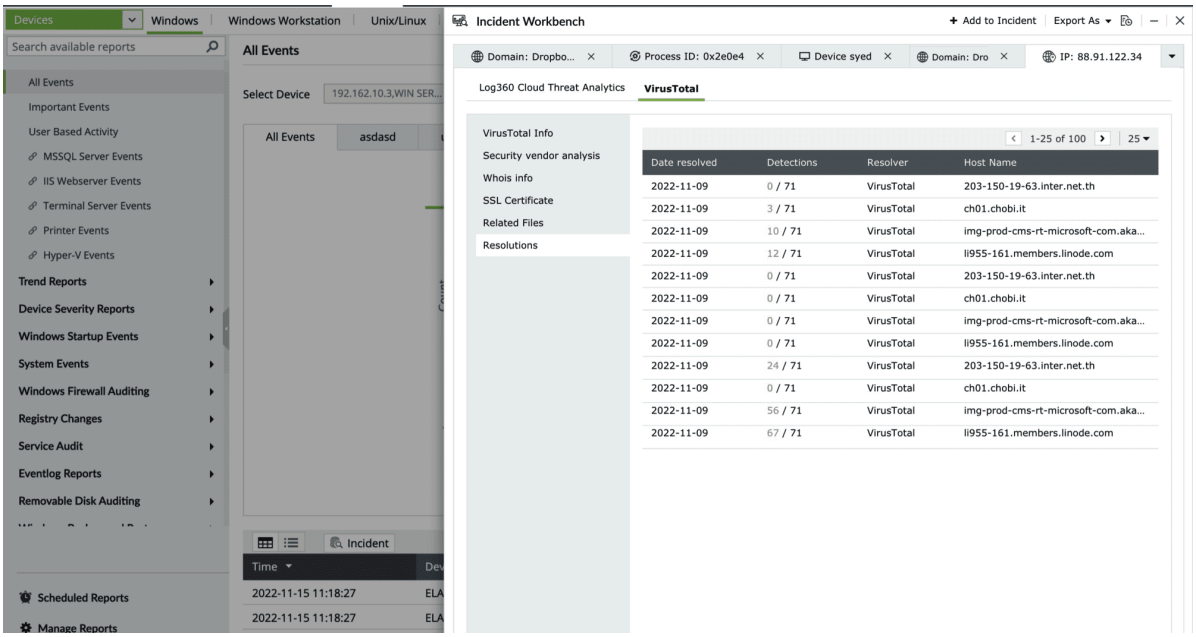






- Resolutions

  This section contains the past and current IP resolutions for a particular domain.




2022-11-15 11:18:27
2022-11-15 11:18:27
2022-11-15 11:18:27
2022-11-15 11:18:27
Need New Reports?
Help Card

10.1.5.4. Constella Intelligence

Last updated on: September 12, 2025

In this page

> How to whitelist a new source?
>
> Threat Alerting

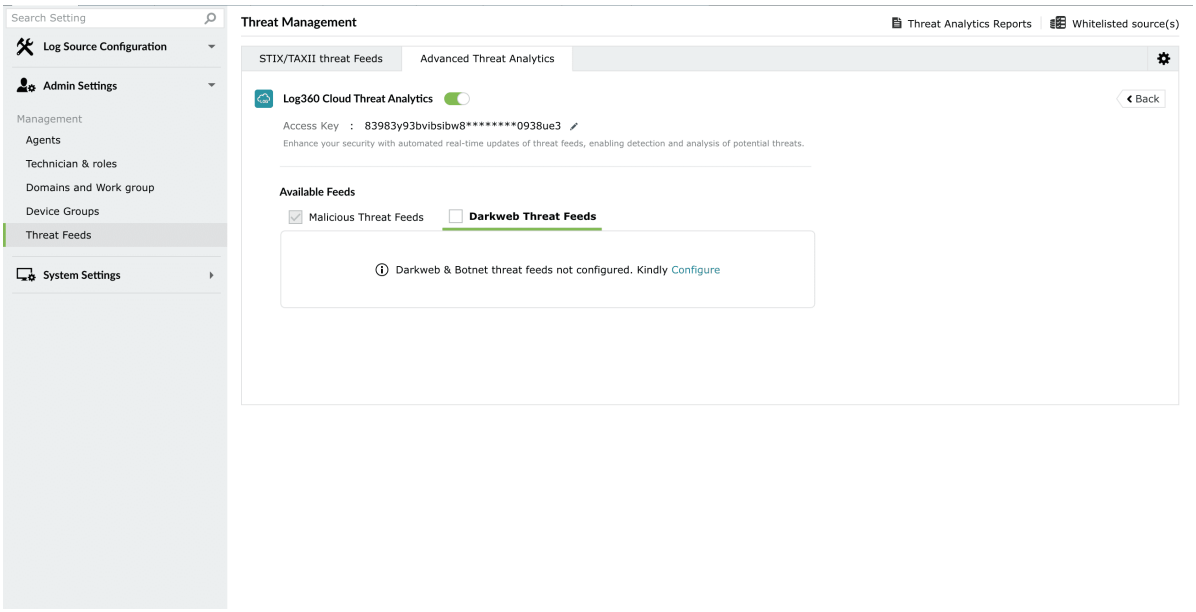
Constella Intelligence is a digital risk protection platform that provides dark web monitoring. This integration with EventLog Analyzer enables users to identify personal information such as credit card number, email information, usernames and credentials that are leaked in the dark web. Users can also

- Gain visibility into breaches using the Threat Analytics dashboard
- Get breach reports
- Get predefined alerts for supply chain breaches

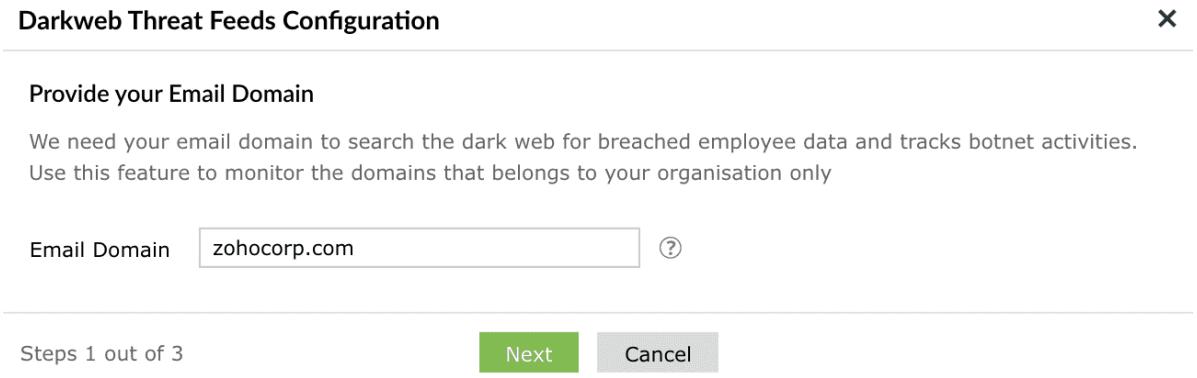
Configuring Dark Web threat feeds

Once you have purchased the Advanced Threat Analytics add-on and applied the license, head to the Advanced Threat Analytics page.
Navigation: Settings → Admin Settings → Management → Threat Feeds → Advanced Threat Analytics → Log360 Cloud Threat Analytics → Integrate
To get the access key, please follow the steps (Until step 2) in this help document.

- After pasting the access key in the Access Key box, Malicious Threat Feeds will be enabled automatically. To enable dark web threat feeds, switch to Dark Web Threat Feeds and click the Configure button.

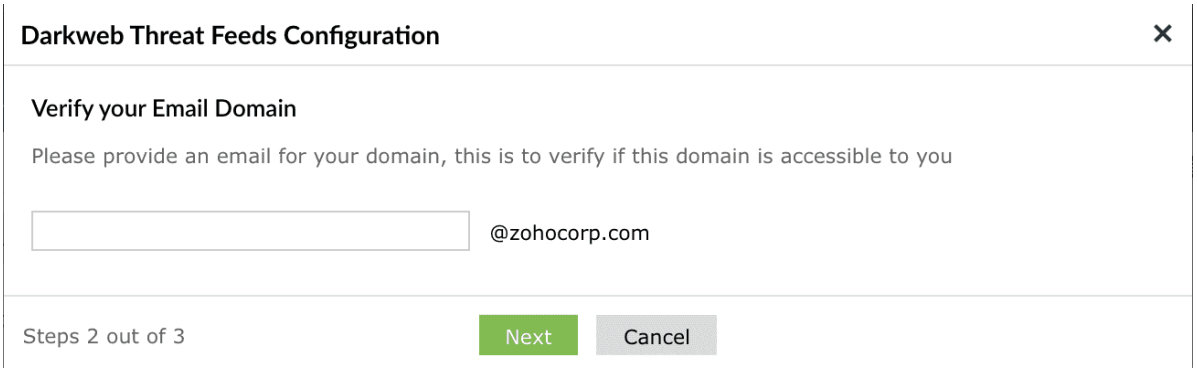


- Upon clicking Configure, a pop-up requesting an email domain to monitor for dark web exposure will be displayed. After entering the domain, you will be asked to provide a valid email address from that domain for verification.

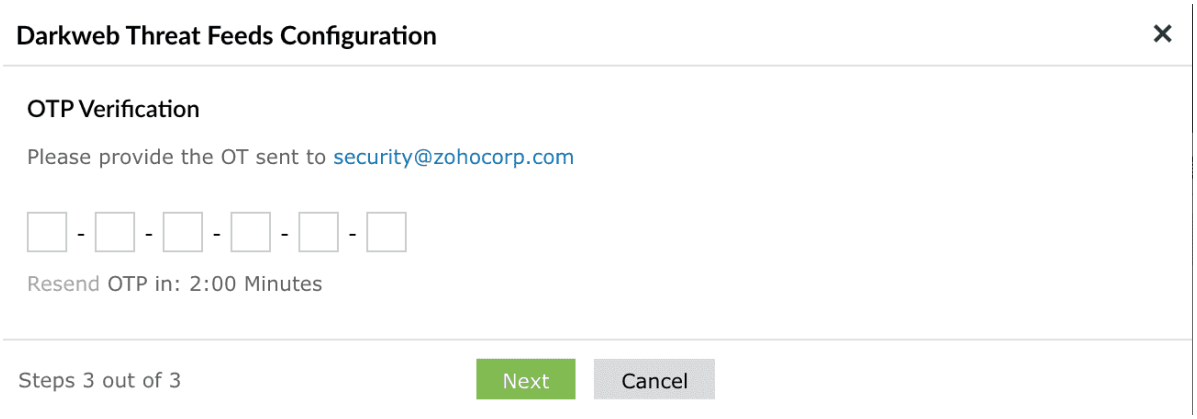


Note

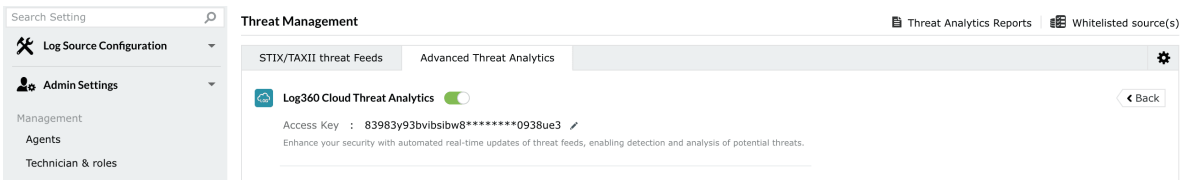
Domain configuration for email is linked to licensing. You can only configure domains associated with licenses you have purchased.

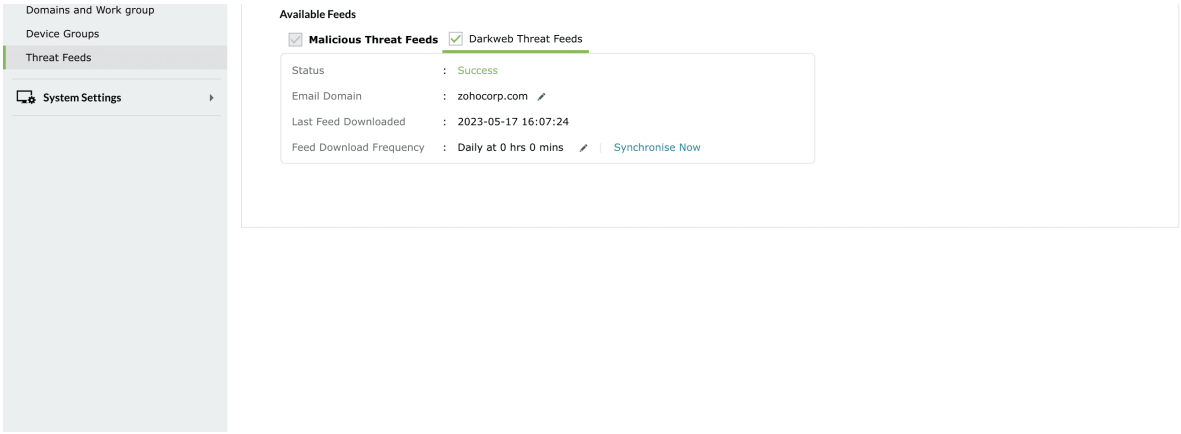


- You will receive an OTP (One-Time Password) to the entered email address. Upon successful verification of the OTP, you will have successfully configured your domain for dark web breaches.



- You will see this page once your domain is successfully configured.

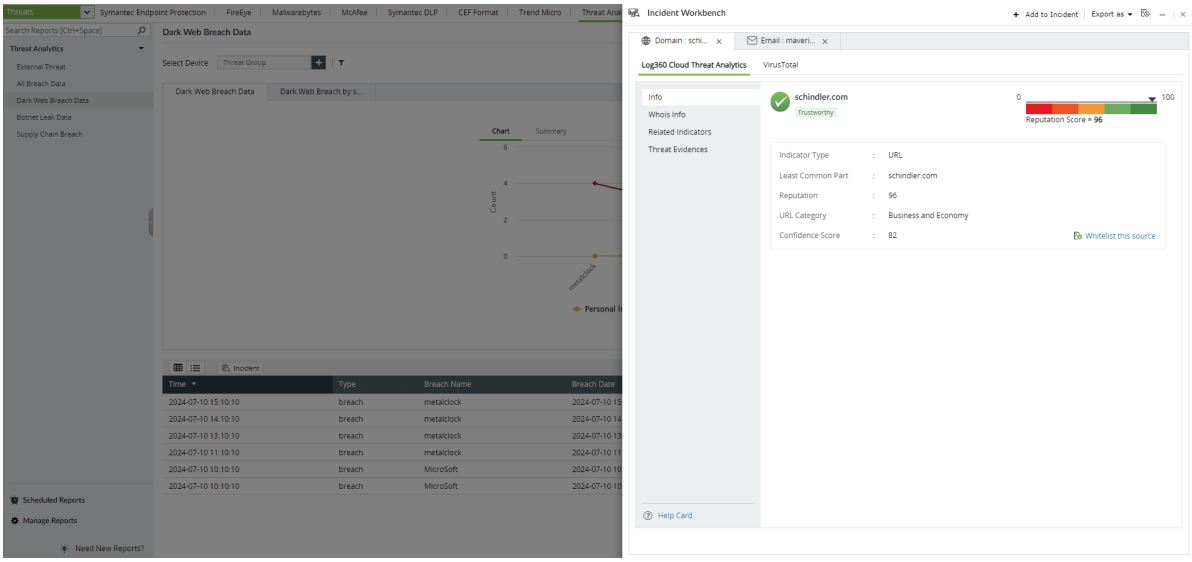




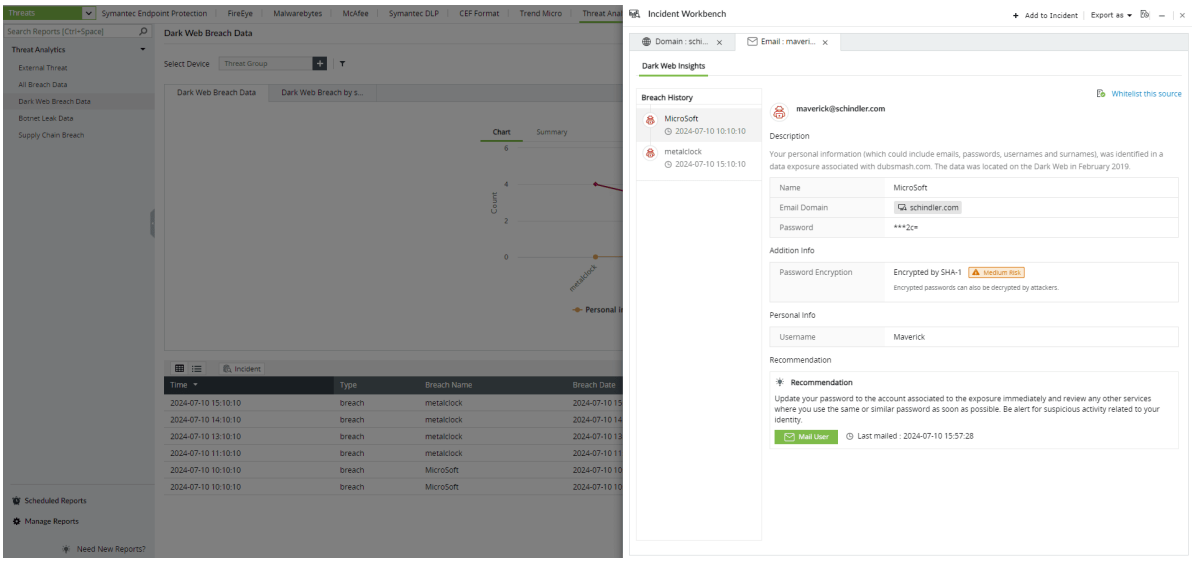
Analysis

EventLog Analyzer provides both email and domain analysis for configured domains. Users will be able to send emails from the Incident Workbench to notify individuals whose data has been breached.

- Domain analysis for the configured domain



- Email analysis for the configured domain



EventLog Analyzer provides an alert profile for supply chain breaches. A supply chain breach refers to the breach where the email domain and the domain where the user's data was breached are different.

Troubleshooting tips:

- Ensure that L3C Feeds Server is reachable from ELA machine.
- Try reconfiguring Dark Web monitoring with your domain
- Ensure that the licensed domain and configured domain are the same.

For further information regarding configuring non-licensed domains, please contact support@eventloganalyzer.com

10.1.5.5. Threat Whitelisting

Last updated on: September 12, 2025

In this page

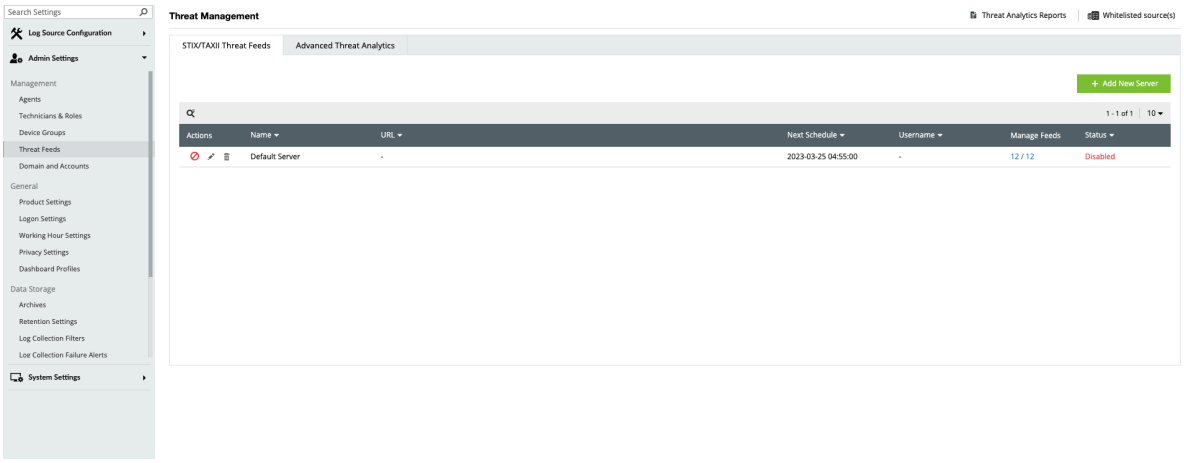
How to whitelist a new source?

Threat Alerting

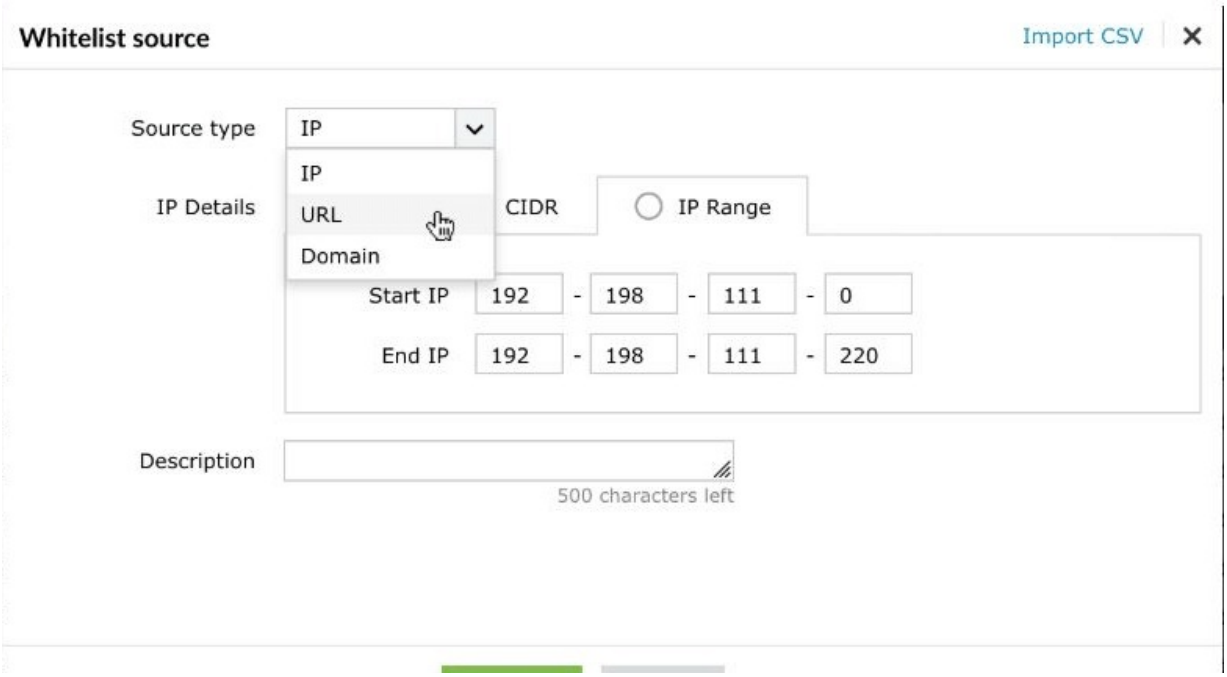
Threat whitelisting helps you to specify an index of approved IPs, URLs, and Domains.

How to whitelist a new source?

- Navigate to Settings > Admin Settings > Threat Feeds > Whitelisted Sources.
- Click the Whitelist Source option. (top right corner of Threat Feeds page).



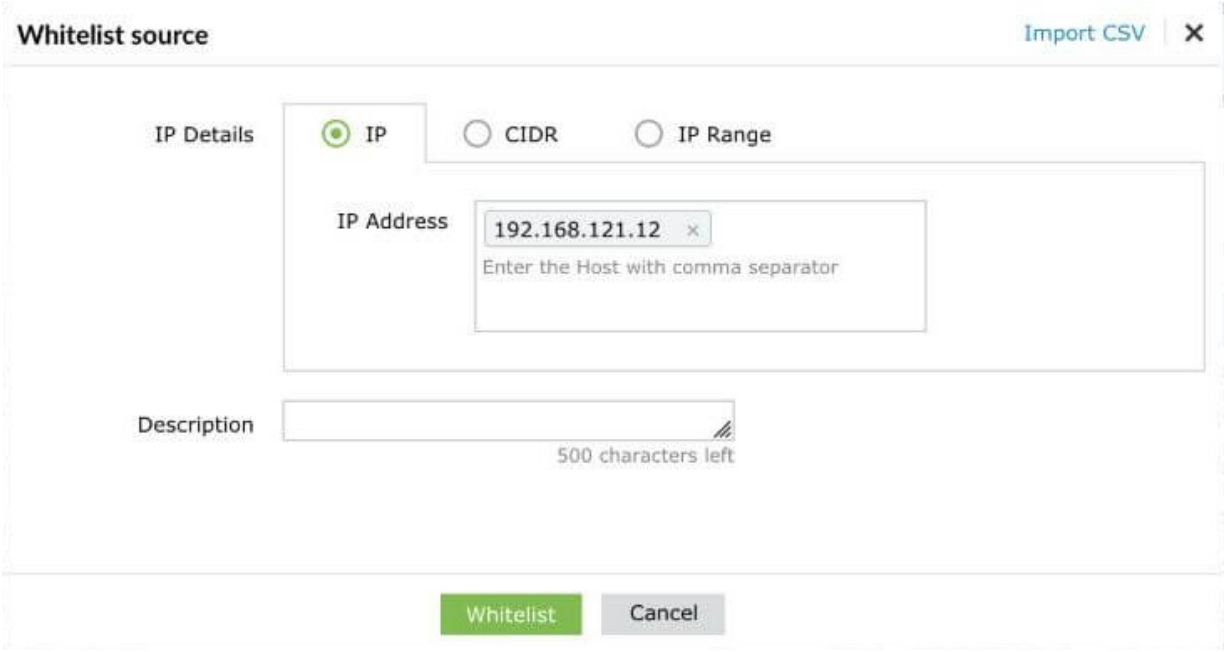
- Select the source type from the drop-down list.



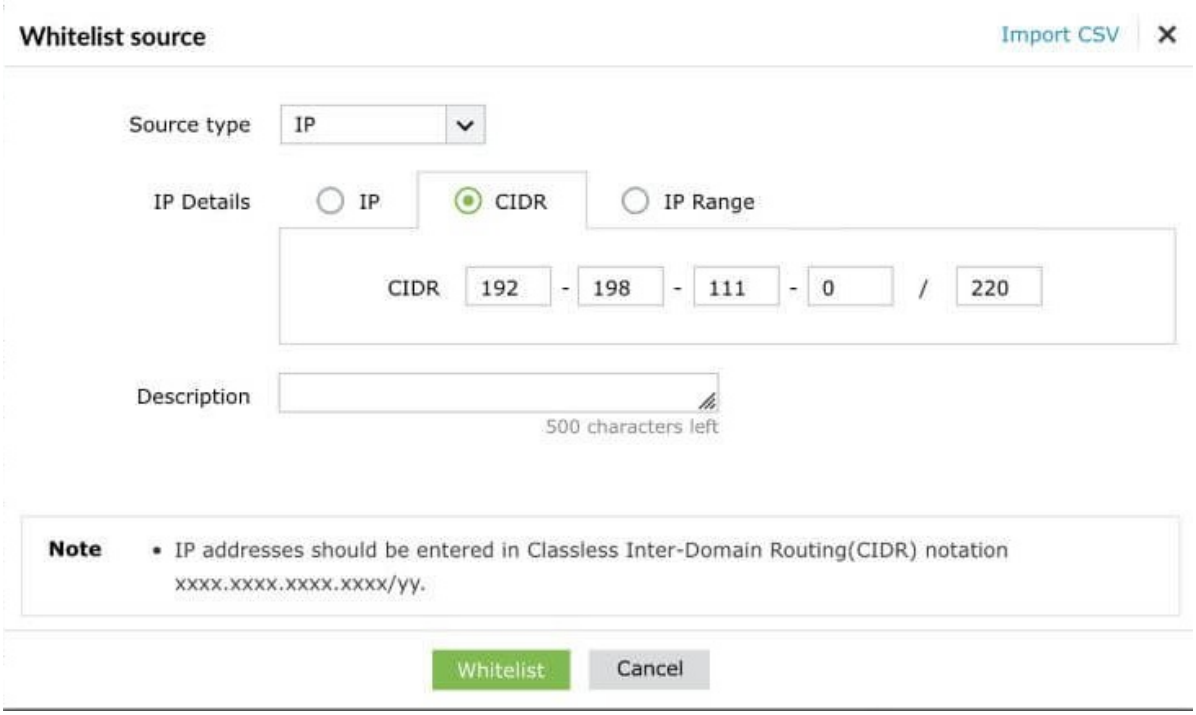


IP Details

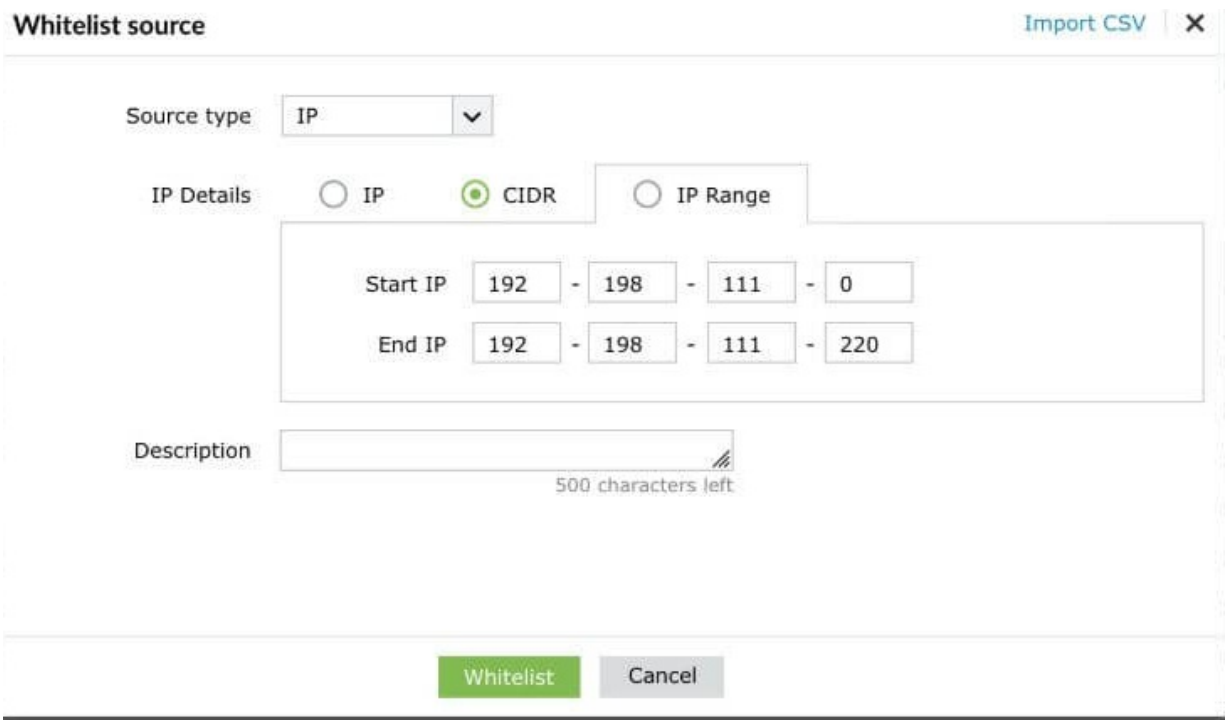
The value(s) entered should either be an IP address, CIDR, or an IP Range.



- The CIDR value can be entered using the '/' symbol. For instance, 192-198-111-0/220.

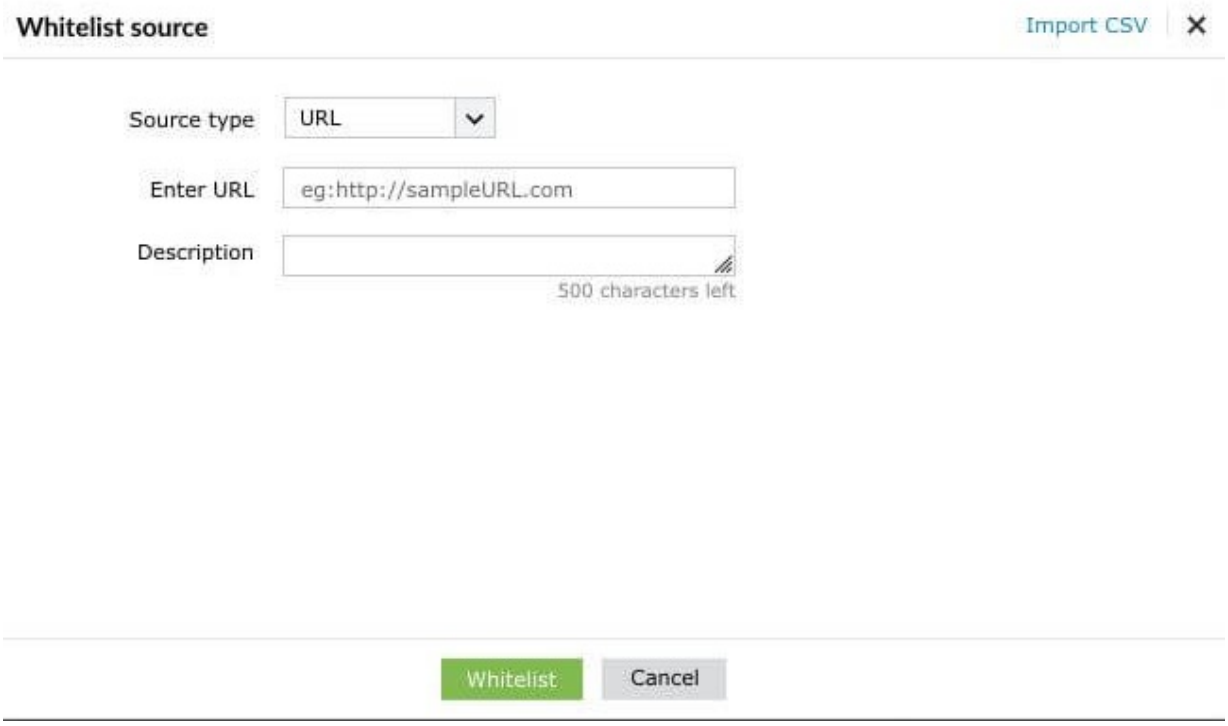


- IP Range can be entered by mentioning the Start and End IPs. For instance, 192-198-111-0 should be the Start IP and 192-198-111-220 should be the End IP, if you want the IPs in-between the range to be whitelisted.



URL

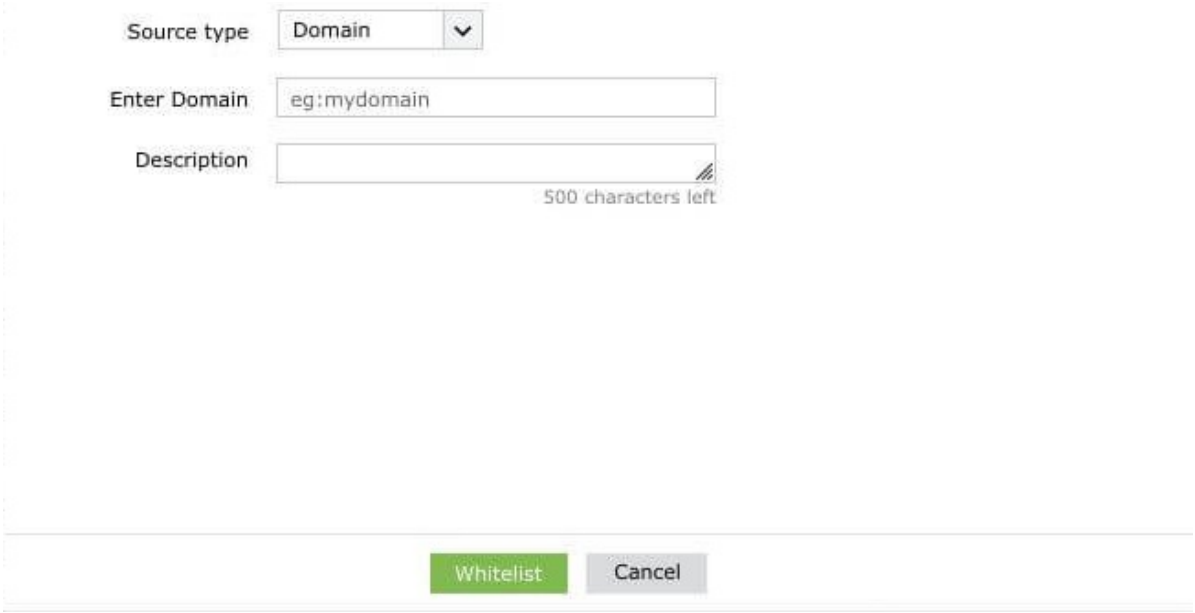
The URL can be whitelisted by mentioning the address in the text box. For instance, http://sampleURL.com



Domain

- A domain can be whitelisted by mentioning the domain address. For instance, 'mydomain'.

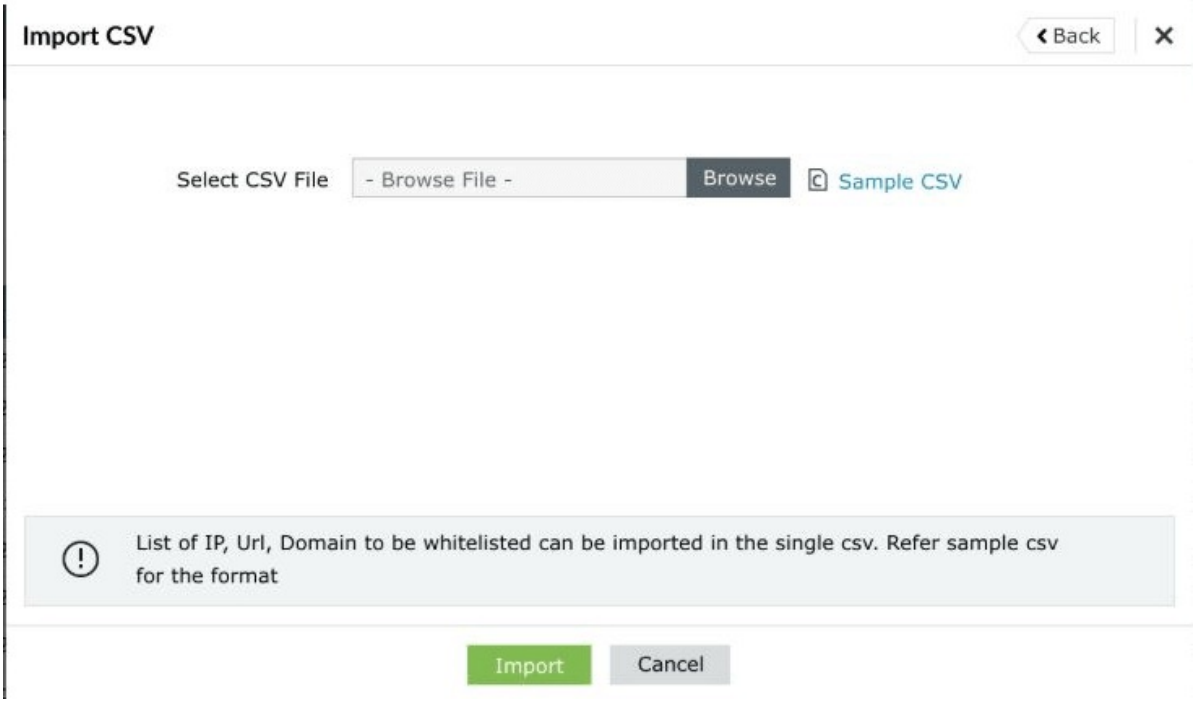




- Enter an appropriate value in the Description field. (Optional)

Import CSV

- To import an existing CSV file containing the source(s) to be whitelisted, click the Import CSV option on the top-right corner of the pop-up window.



- Refer the sample CSV for the file format.

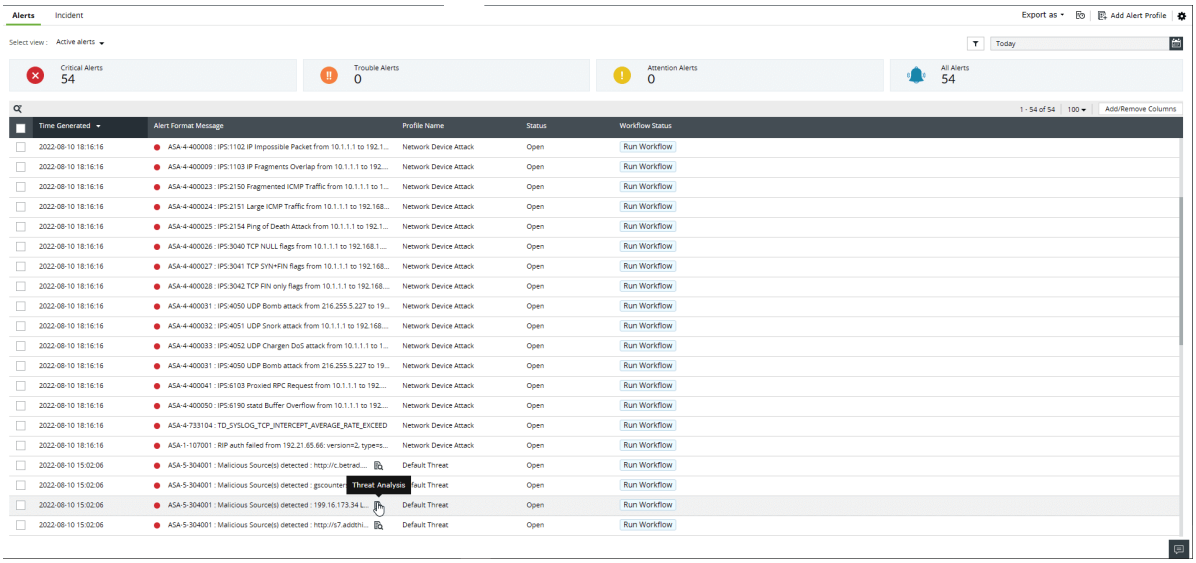
> Note
>
> Only CSV files are supported.

- The imported source(s) will be displayed in the list.
- To delete an existing source, click the bin icon displayed near the respective source(s) under Actions. Click the Yes button in the confirmation box that appears.

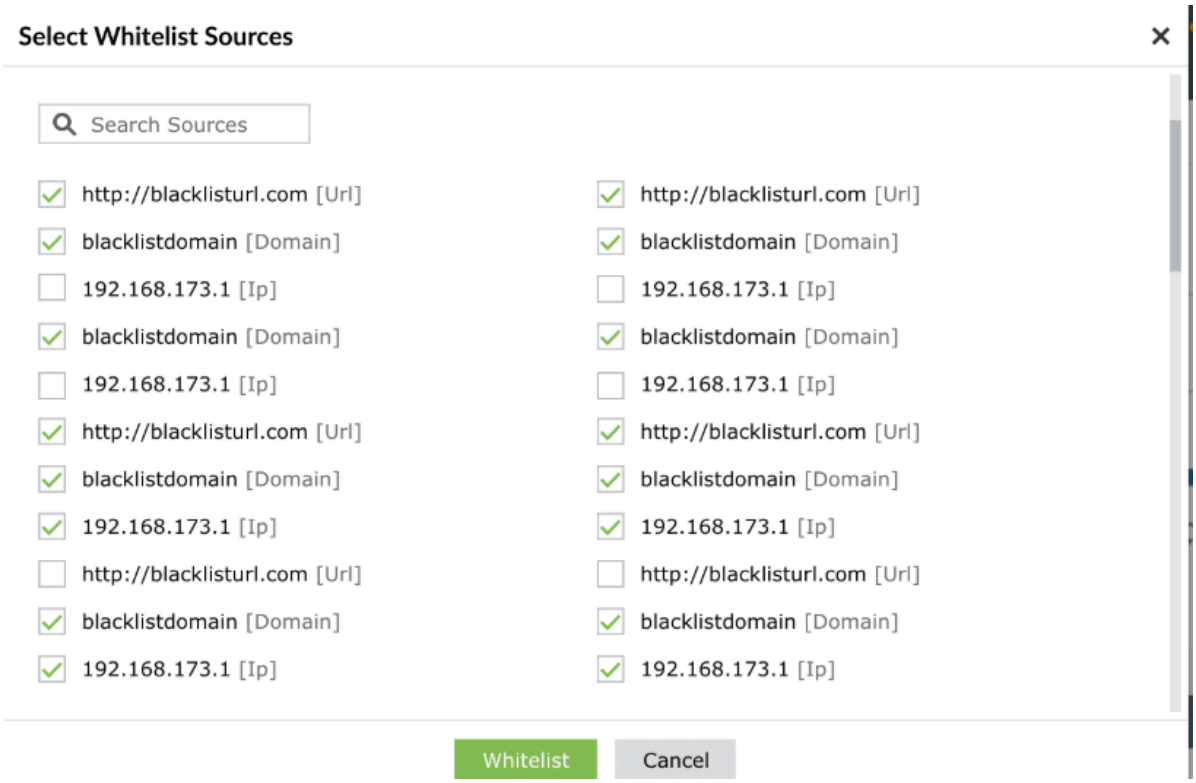
Threat Alerting

Threat Whitelisting has been integrated with Advanced Threat Analytics with the aim of reducing false positive alerts.

- Navigate to Alerts > Threat Alerts.



- To whitelist a particular source, select the desired source from the list (using checkbox) and click on the ellipsis (three dots stacked vertically) and select the Whitelist Source option.



- Click the Whitelist button. Click the Yes button in the confirmation box that appears.

> **Note**
>
> The whitelisted sources will be excluded from threat alerts and external threat reports.

10.1.5.6. Threat Import

Last updated on: September 12, 2025

In this page

How to whitelist a new source?

Threat Alerting

Threat import lets you import threat feed data into EventLog Analyzer from CSV files. This will help users to add any third-party threat data easily, and EventLog Analyzer processes the threat feed data present in the files for threat alerting.

> Note
>
> The CSV files should contain the list of threat sources in the first column. Download sample CSV file.

How to add files for Threat Import

- If you need to add Threat Sources for threat alerting, place the files in the <Dir>\EventLog Analyzer\data\za\threatfeeds\ThreatImport\Import folder.
- Files in the ThreatImport directory will be deleted once it is processed. If any files are not deleted, this may indicate that an exception has occurred. Check the log file for details and contact support at eventloganalyzer-support@manageengine.com for further assistance.

> Note
>
> If you need to remove any Threat Sources from flagging threat alerts, place the file containing the Threat Feeds to be removed in <Dir>\EventLog Analyzer\data\za\threatfeeds\ThreatImport\Delete folder.

Scheduling Threat Import

- Scheduling helps users import Threat data from files at the specified location automatically on a daily basis. This ensures that threat feeds are consistently updated and stay current. A threat Import schedule can be enabled by changing the threat.import.schedule.enable property in <dir>\EventLog Analyzer\conf\EventLogAnalyzer\threat folder\threatstore.properties file from "false" to "true".
- A schedule will run everyday at 8:00 AM to process the files placed under respective ThreatImport folder.

- Users can disable the threat schedule by changing the value of threat.import.schedule.enable property key from <dir>\EventLog Analyzer\conf\EventLogAnalyzer\threat folder\threatstore.properties file back to "false".
- If the threat.import.schedule.enable property key value changes from "false" to "true", the product must be restarted.
- Restarting the product will trigger the threat import operation immediately instead of waiting for the 8.00 AM schedule.
- You can find entries related to the threat Import feature in the product log file by searching for ThreatImportHandler.

10.1.5.7. Switching threat stores

Last updated on: September 12, 2025

In this page

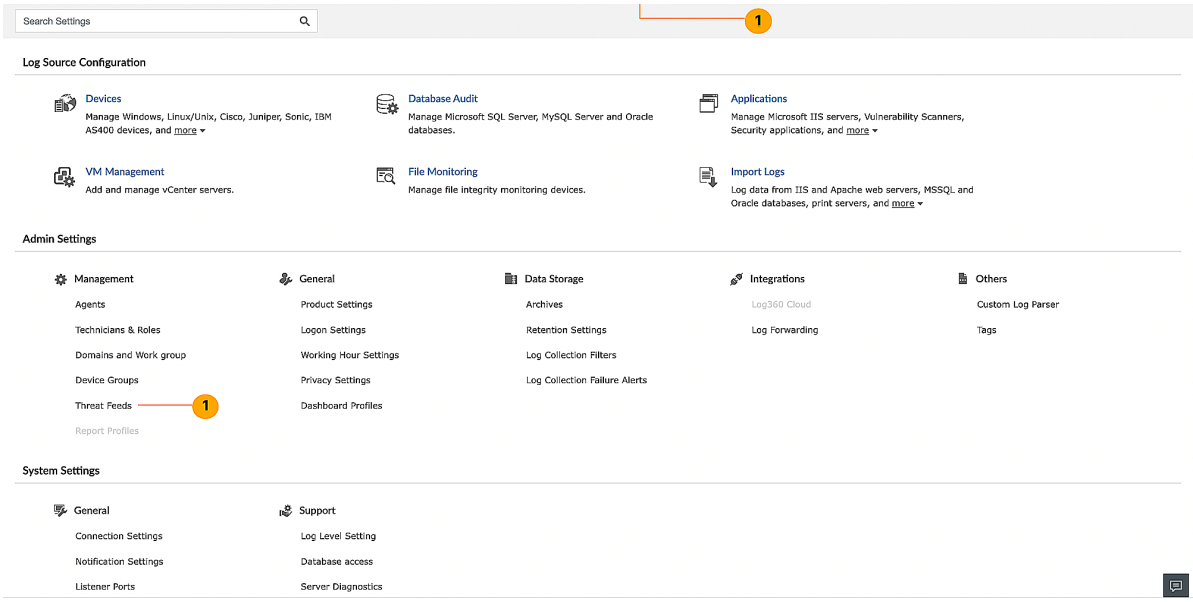
How to whitelist a new source?

Threat Alerting

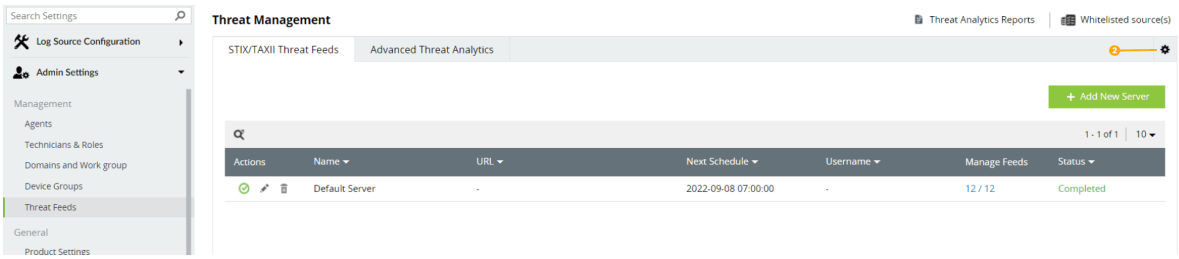
To switch between the two threat storage (in-memory threat storage and disk-based threat storage) available in EventLog Analyzer, please follow the steps given below.

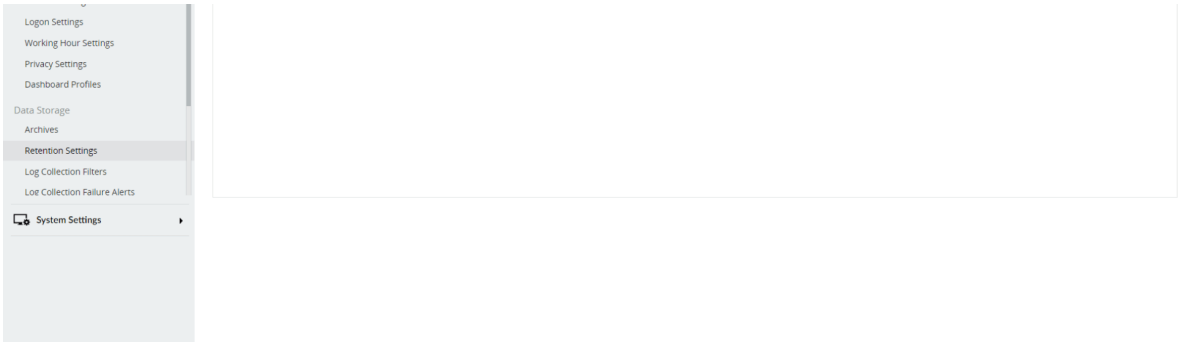
> **Note**
>
> - In-memory threat store requirements: The in-memory threat storage requires a minimum of 2 GB RAM to be allocated to EventLog Analyzer; of which at least 512 MB should be available for use.
> - Switching to in-memory threat storage is not possible in 32-bit systems.

1. Go to Settings → Admin Settings → Management → Threat Feeds.

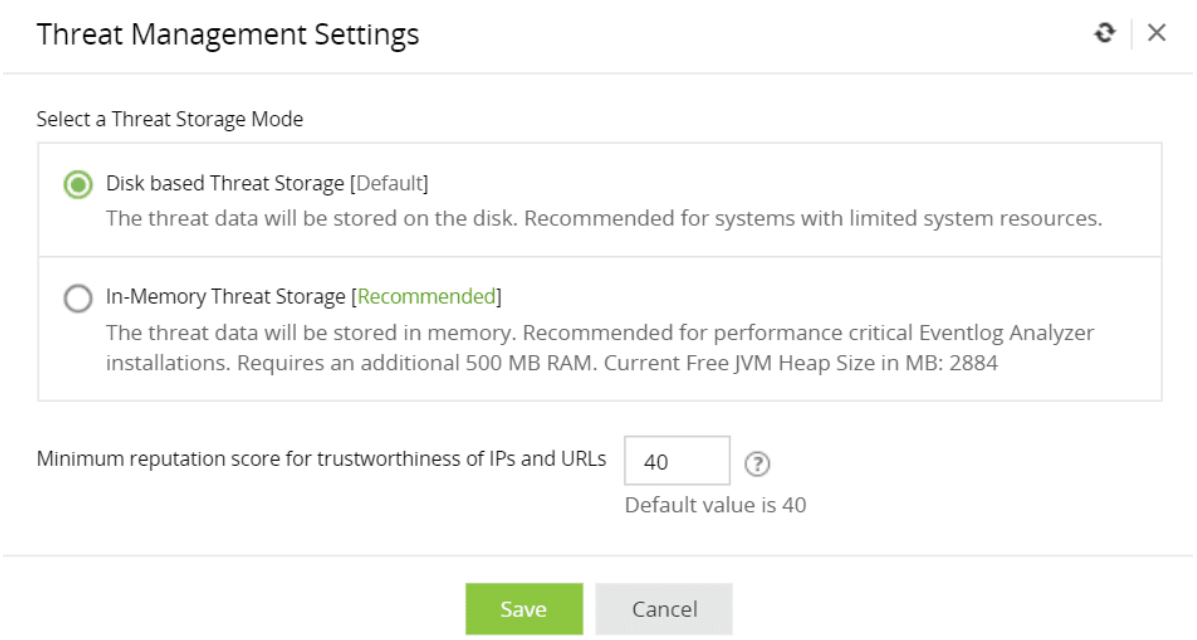


2. Under Threat Feeds sub section, click on Settings icon on the top right corner.





3. Choose between Disk based Threat Storage and In-Memory Threat Storage. You can also set a Minimum reputation score for trustworthiness of IPs and URLs. Click on Save.



10.1.5.8. Integrating and using the MITRE ATT&CK framework with EventLog Analyzer

Last updated on: September 12, 2025

In this page

What is the MITRE ATT&CK framework?

Pre-configurations required for integration

EventLog Analyzer helps spot adversaries, classify attacks, and single out attack tactics and techniques by integrating the MITRE ATT&CK framework to robustly monitor network security.

What is the MITRE ATT&CK framework?

The MITRE ATT&CK framework is a matrix of attack tactics mapped with various attack techniques that are constantly updated to serve as the attack encyclopedia for IT security professionals all across the globe.
The tactics signify the objectives of an attacker such as:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Various attack techniques such as account manipulation, access token manipulation, and brute force to name a few are associated with the tactics to help identify adverse events and anomalies. The framework is adopted globally to facilitate easier communication among cyber security enthusiasts about the latest attack patterns.

Pre-configurations required for integrating MITRE ATT&CK framework in EventLog Analyzer

Closely monitoring and tracking network events is of paramount importance to detect adversaries. You need to enable the advanced audit policy settings given under the following categories in your network to cohesively gain

insights from the framework:

- Account Logon
- Account Management
- Directory Service Access
- Logon/Logoff Events
- Object Access
- Policy Change
- Privilege Use
- Detailed Tracking
- System Events
- App Locker Auditing
- Windows Defender Attack Surface Reduction

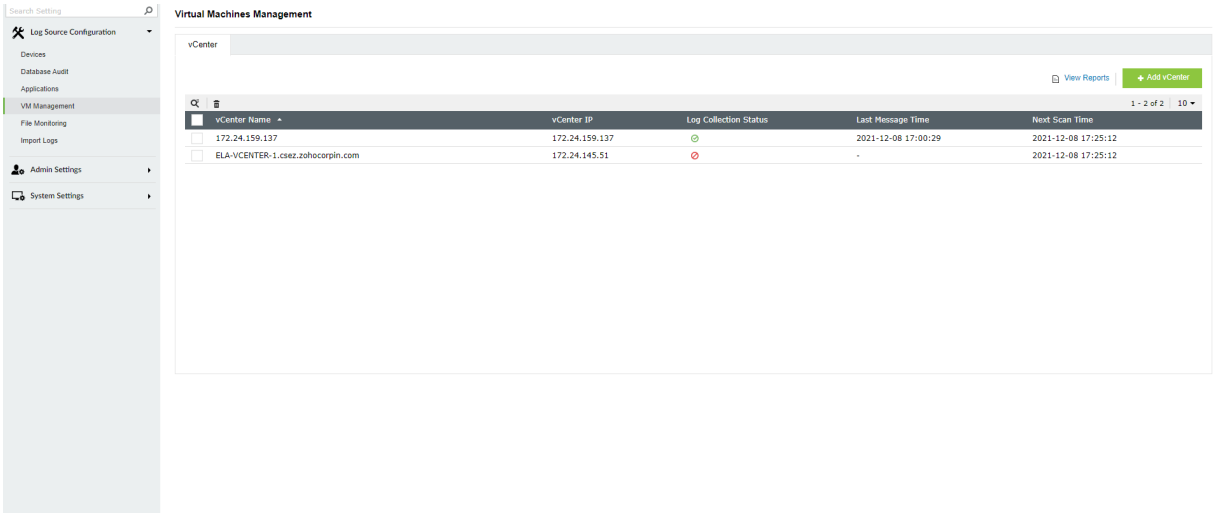
10.1.6. VM Management

Last updated on: September 12, 2025

The vCenter servers to be monitored by EventLog Analyzer can be managed in this section.
Settings > Log Source Configuration > VM Management
vCenter servers can be added and deleted. All the vCenter servers that are being monitored can also be viewed.

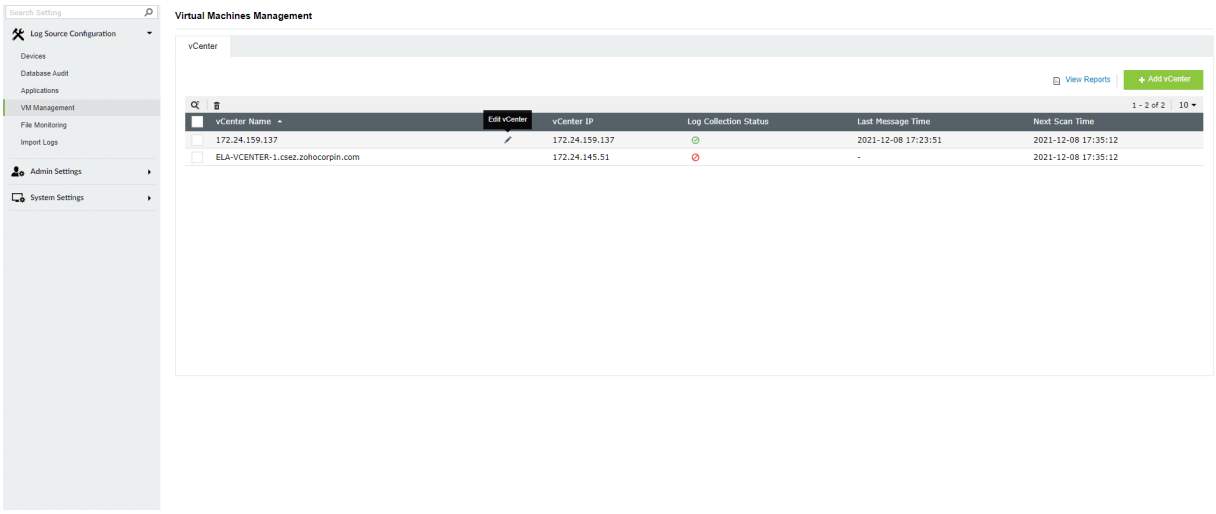
View vCenter

After you have added a vCenter server, you can view the added vCenter servers along with vCenter IP, log collection status, last message time, and next scan time.



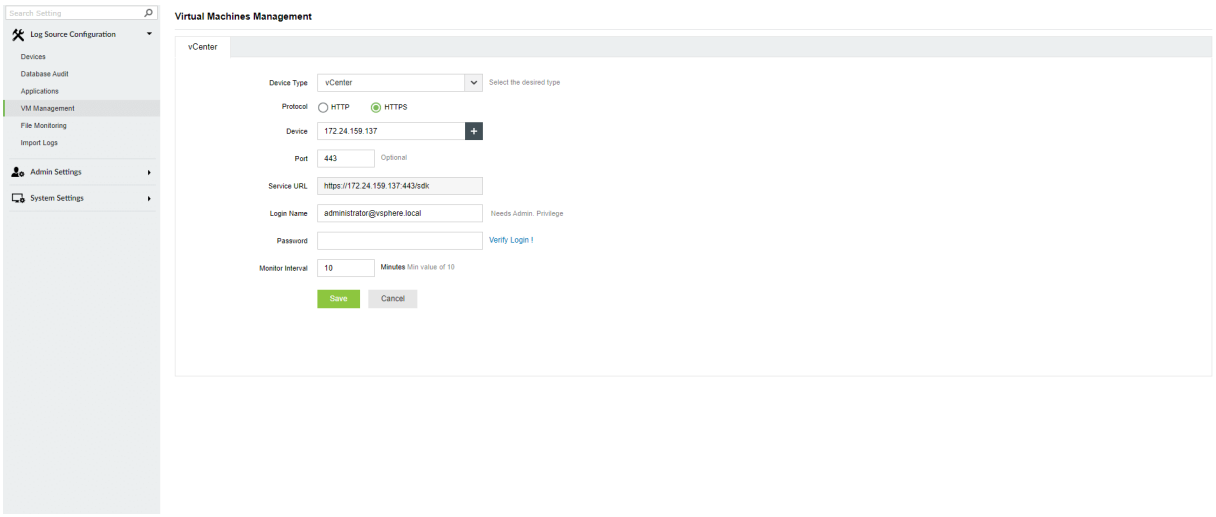
How to edit a vCenter server?

To edit a vCenter server, hover your mouse over the vCenter and click the Edit icon that appears.



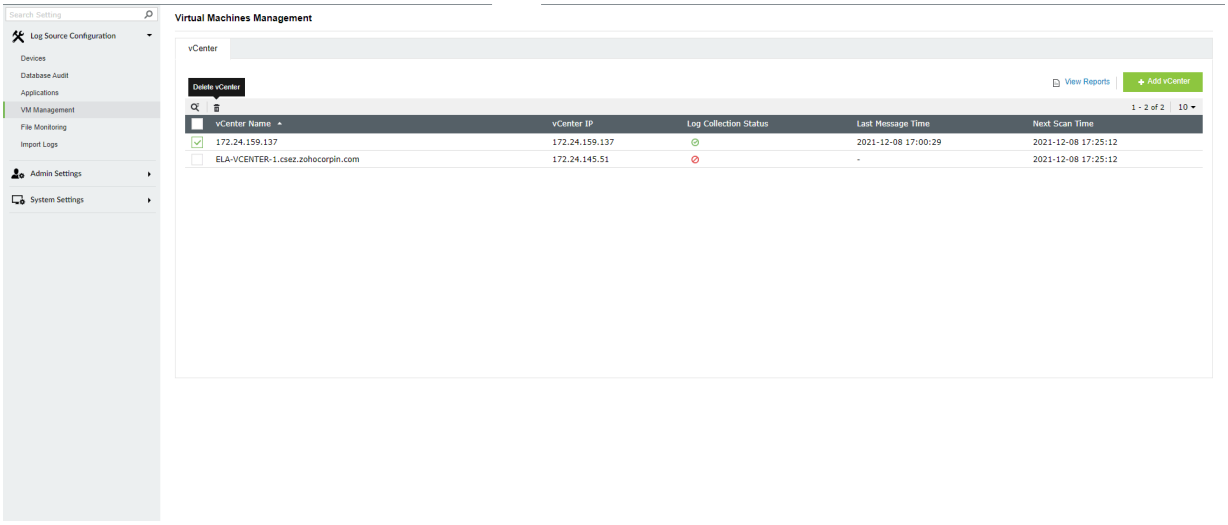
You can modify the Device type, Protocol, Device name, port number, and more

You can modify the Device type, Protocol, Device name, port number, and more.



How to delete a vCenter server?

To delete a vCenter server, select the vCenter you want to delete and click the Delete icon.



10.1.7. Manage Vulnerability Data

Last updated on: September 12, 2025

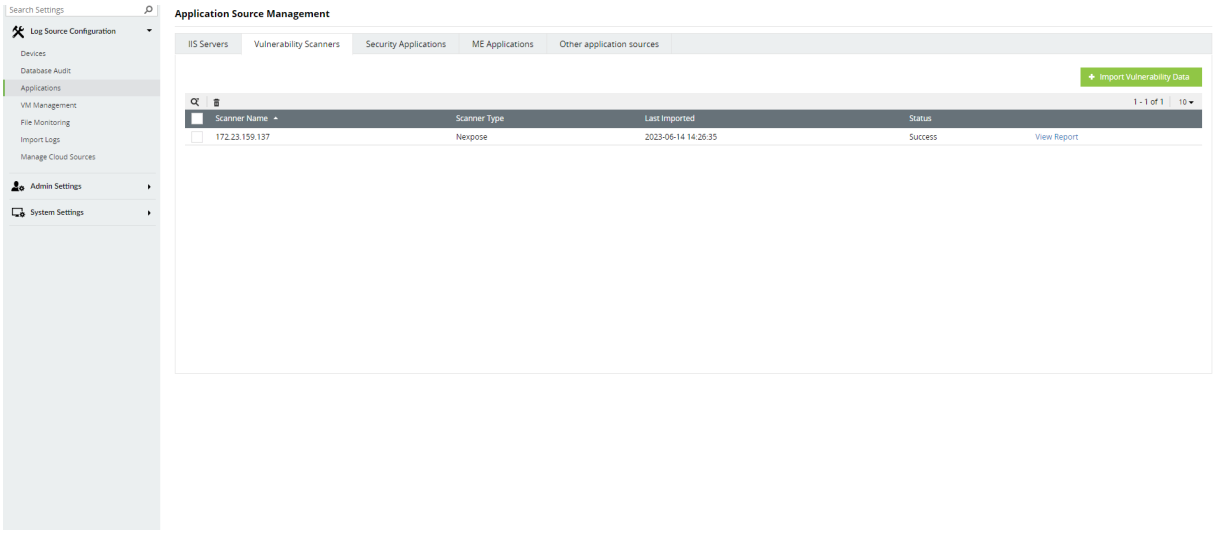
The vulnerability scanners to be monitored by EventLog Analyzer can be managed in this section. Vulnerability scanners can be added, deleted, and all the vulnerability scanners that are being monitored can be viewed.
Settings > Log Source Configuration > Applications

How to add a vulnerability scanner?

To add a vulnerability scanner, click the Import Vulnerability Data button.

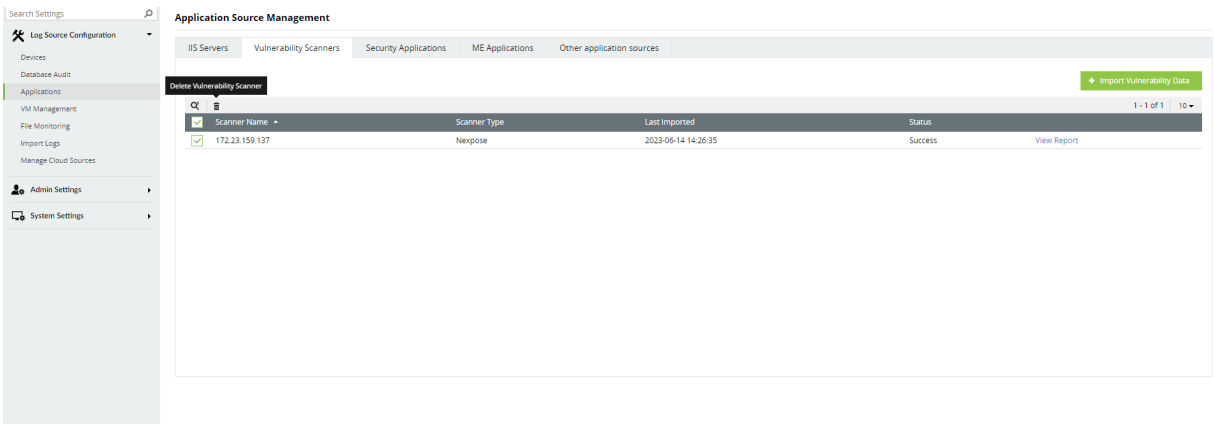
View Vulnerability Imports

After you import a vulnerability log, the vulnerability scanners will be displayed along with the name of the scanner, type, last import time, and status.



How to delete a Vulnerability Scanner?

To delete a threat solution, select the vulnerability scanner you want to delete and click the Delete icon.



10.2.1. Overview

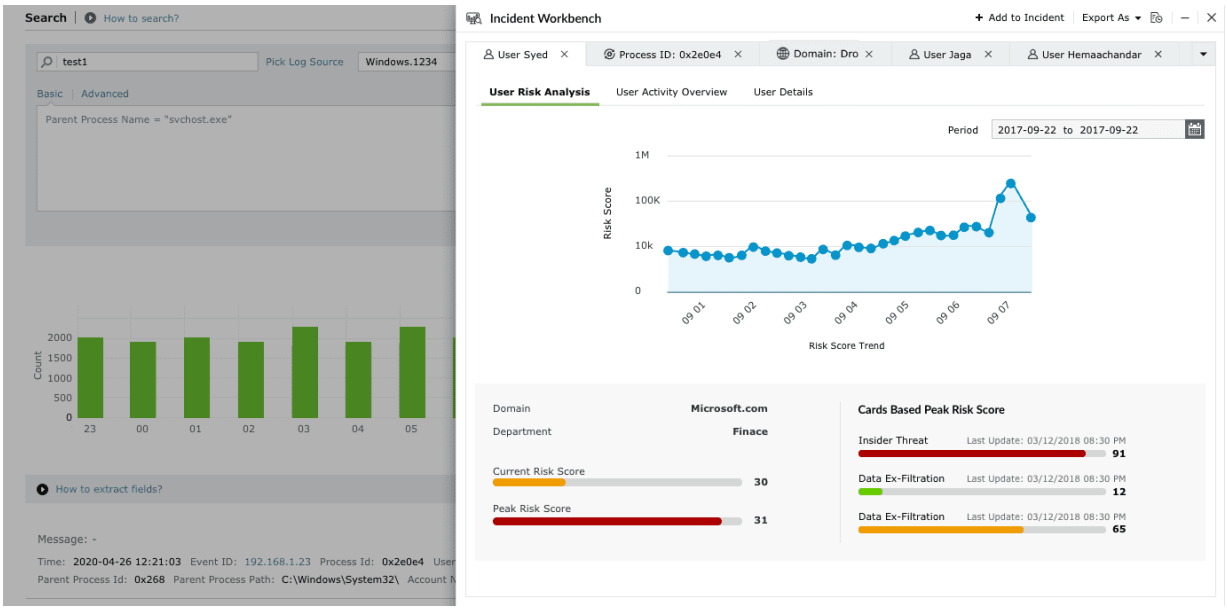
Last updated on: September 12, 2025

In this page

Features

Access and usability

- The Incident workbench is Eventlog Analyzer's investigation console that unifies analytics of the core entities such as users, processes, and threat sources.
- This feature facilitates users to add, compare, and analyze data with enriched integrations like UEBA and Advanced Threat Analytics.
- Utilize the contextual assesment with risk based profiling, conduct faster root cause analysis by probing the process trees, and minimize the overall time taken to investigate and resolve threats.



Features:

Here are the entities you can analyze using Incident Workbench:

- Users

  Analytics offered: ML-based user activity and risk score data compiled through UEBA integration from Log360's suite.

- Process

  Analytics offered: Process hunting tree with parent-child relationships and event timeline.

- Threat sources

  Analytics offered: Risk analysis from security vendors using Advanced Threat Analytics integration.

Access and usability:

- Roles and restrictions:
  - Operator and guest role members have no access to the Incident Workbench.
  - Custom roles can be created to provide access to the Incident Workbench.
- Access: Incident workbench can be invoked from multiple dashboards of EventLog Analyzer such as reports, log search, compliance, alerts, and more.
- Users can add upto 20 tabs in a single instance of the Incident Workbench and save it to an existing incident or create a new incident.

10.2.2.1. About Zoho's Zia Insights

Last updated on: September 12, 2025

In this page

How Zia Insights work

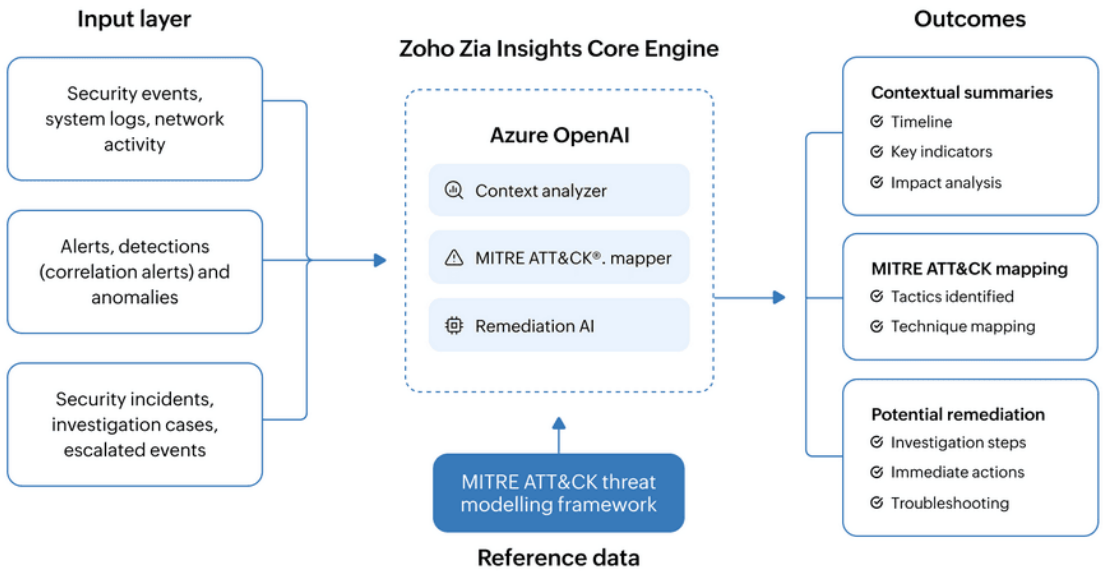
Zia Insights workflow

Benefits of integrated Zia Insights experience

ManageEngine Log360 uses Zoho's Zia Insights, an AI-powered engine to enhance log analysis, threat detection, and incident response. By leveraging contextual AI, Zia Insights transforms raw logs, security events, audit trails, alerts, and incidents into actionable insights, enabling you to quickly identify risks, get context on an event, possible mitigation steps, and add value by mapping MITRE ATT&CK® techniques to the events wherever possible for effective analysis.

How Zia Insights work

This section elaborates the underlying architecture and functioning of Zia Insights. Zia Insights capability works with bring your own key (BYOK) model with Azure Open AI. By processing logs, alerts, and incidents, Zia Insights delivers contextual summaries, highlights potential risks, maps relevant activities to MITRE ATT&CK® techniques, and suggests possible remediation steps. These insights enable security teams to understand the event context better, accelerate investigations, and strengthen response strategies.



Zia Insights workflow

1. Invoking Zia Insights

The workflow begins when a user initiates a request for insight by selecting a specific log, alert, or incident. This

The workflow begins when a user initiates a request for insight by selecting a specific log, alert, or incident. This action triggers the Zia Insights engine to begin its analysis.
Once invoked, the product console automatically retrieves all relevant data associated with the selected item. This includes raw logs, event metadata, alert context, or incident timelines, depending on the request initiated by the user. This collected information forms the input layer, which is critical to the insight generation process.
The input layer aggregates a wide range of security data sources, including:

- Security events, system logs, and network activity: Collected from endpoints, firewalls, cloud infrastructure, and other monitored systems
- Alerts and detections (correlation alerts): Triggered through rule-based correlation alerts.
- Security incidents, investigation cases, and escalated events: Data related to ongoing or historical threats under review by the SOC team

This comprehensive dataset ensures that Zia Insights has all the context it needs to generate actionable insights.

2. Insight generation

Once the relevant security data is collected, it is passed to the Zia Insights core engine, which leverages the capabilities of Azure OpenAI to transform raw data into contextual insights.
Zia Insights pairs the retrieved data with a predefined set of instructions known as a prompt. This prompt defines how Zia Insights should interpret the data and how the output should be structured.
Zia Insights then processes the data through several core components:

- Context analyzer
  Reconstructs the event timeline, identifies key actions, and potential threat classifications.
- MITRE ATT&CK® mapper
  Matches detected behaviors to known attacker tactics and techniques using the MITRE ATT&CK® framework, helping the SOC team understand potential threat stages.
- Remediation AI
  Suggests investigation steps, containment strategies, and recovery recommendations tailored to the specific scenario.

3. Outcomes from Zia Insights

After processing and analyzing the input data, Zia Insights produces a structured output that is both actionable and context-aware. The key components of the outcomesinclude:
Contextual summaries
Summarizes the event with a timeline, key indicators, and impact analysis

- Timeline: Reconstructs the sequence of related events to provide temporal clarity.
- Key indicators: Highlights important information such as source IPs, user accounts, and processes.
- Impact analysis: Evaluates the potential effect of the event on systems, users, or business operations, helping teams prioritize response.

MITRE ATT&CK® mapping

Based on the behaviors observed, Zia Insights maps the activity to corresponding MITRE ATT&CK® tactics and techniques. This enables standardized threat classification and aids in investigation and threat hunting.

Potential remediation

Zia Insights offers suggested investigation steps, immediate containment actions, and troubleshooting guidance to support timely and informed action.

Benefits of Zia Insights

Zia Insights empowers SOC team's investigation process and effectively mitigate or neutralize a threat with unprecedented speed. It allows SOC professionals to:

- Proactively hunt for subtle indicators: Leverage the Summary, Insights, and Timeline in Zia Insights to uncover subtle indicators of compromise proactively. These segments quickly highlight relevant events, actors, and entities.
- Accelerate Investigation: By automatically providing context, identifying actors, entities, and laying out the attack chain with MITRE ATT&CK® framework mapping.
- Enable Rapid Remediation: By offering specific, actionable steps tailored to the detected threat and log types.
- Enhance Threat Intelligence: By consistently mapping incidents to MITRE ATT&CK® , building institutional knowledge of adversary tactics.
- Optimize Analyst Productivity: By offloading initial analysis and information gathering to the AI, allowing human analysts to focus on critical decision-making and strategic defense.

Read also

This document detailed the working principles and key use cases of Zia Insights. For configuring and leveraging the capabilities of Zia Insights, refer to the articles below:

- Using Zia Insights
- Setting up Zia Insights

10.2.2.2. Using Zia Insights

Last updated on: September 12, 2025

In this page

Overview

Key insights provided by Zia

Overview

Zoho Zia, the AI-engine, delivers contextual insights from logs, alerts, and incidents by leveraging advanced summarization, threat mapping, and possible remediations. Using Universally Unique Identifiers (UUIDs) for logs, Alert IDs for alert data, and Incident IDs for incident data, Zia Insights processes raw data to streamline threat detection, investigation, remediation, and compliance audit.
This page explains how Zia Insights categorizes events, generates insights, and guides response actions within the product console.

Key insights provided by Zia

Zia Insights provides six key information for effective security operations. They are:

- Log categorization
- Summary
- Insights
- Timeline
- Potential MITRE ATT&CK® Mapping
- Mitigation guidance

Log categorization

To accelerate log analysis and generate remediation steps, Zia Insights categorizes log data and provides tailored recommendations based on the log type. Refer the below table to learn how Zia Insights categorizes the logs, the detection indicator it uses for log categorization, and the modules it assigns to each category.

> NOTE
>
> All logs in the Search and Alerts modules are categorized, and remediation steps are provided if the log falls into one of the predefined categories.

Log type	Detection indicators	Insights provided

Log type	Detection indicators	Insights provided
Error and crash logs	Error codes, "failed" or "fatal" keywords, or stack traces. Application crashes, or service failures that disrupt normal operations.	Troubleshooting Steps For example, application crashes will include recommendations to analyze application logs at the time of the crash to identify any correlated events, and debug using tools like WinDbg to trace access violations.
Security logs	Failed authorizations, suspicious activities such as User Account Control (UAC) modifications, or triggered security alerts.	Potential Mitigation Steps For example, office process launching PowerShell will include recommendations to investigate the source document, restrict script execution using Powershell's Constrained Language Mode, and block macros from untrusted sources.
Audit logs	Unauthorized access attempts, audit policy violations, or configuration changes.	Recommendations For example, changes to audit policies will include recommendations to enforce strict access controls and alert mechanisms for critical audit events.

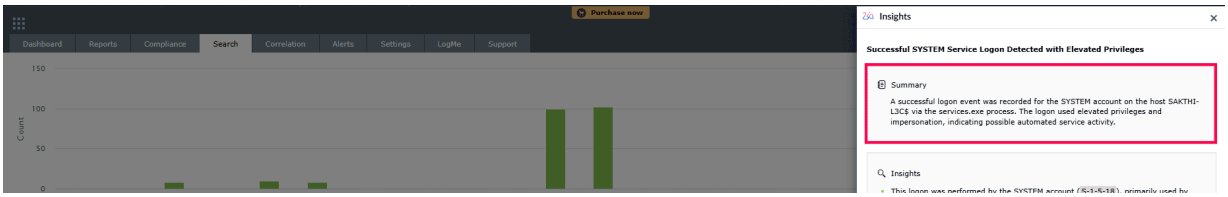
NOTE

If a log does not fall under one of the above mentioned categories, mitigation steps will not be available.

Summary

The Zia Insight's Summary segment provides a concise overview of logs, events, alerts, and incidents. It distils crucial information from logs and incidents by using structured inputs. For incidents, it gathers details like evidence, notes, activity logs, involved parties, and basic incident context to generate the summary.

NOTE Summary is generated for logs accessed via Search and Alerts consoles. While Zia provides a concise overview across both, the level of detail in the summary may depend on the context of the underlying data.



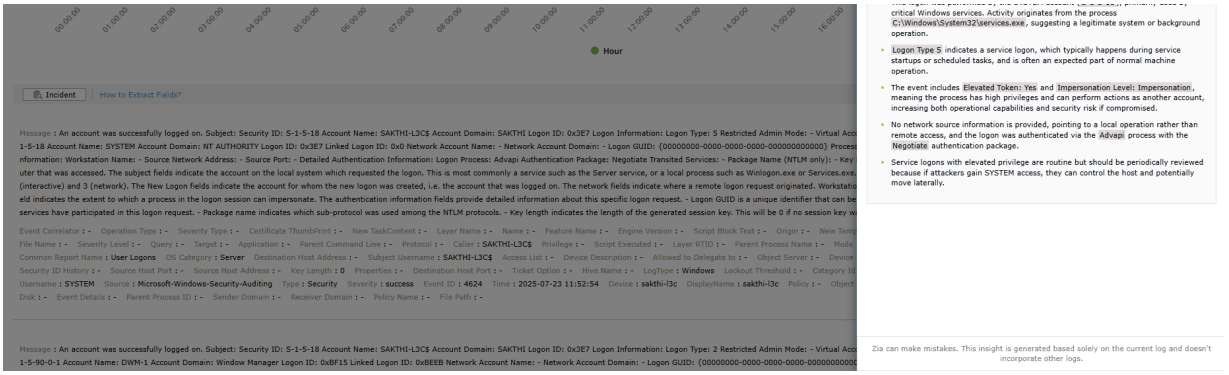


Figure 1: Zia Insights summary from Search

Insights

The Insights segment in Zia Insights provides actionable understanding derived from analyzing events leading to an alert, which enables the identification of key actors, source and destination IPs, user accounts, involved entities, example systems, and the detection of suspicious behaviors.

> **NOTE**
>
> Insights are generated only when you invoke Zia Insights from Search and Alerts consoles of the product. In the Incidents module, Insights are not available for workbench evidence.

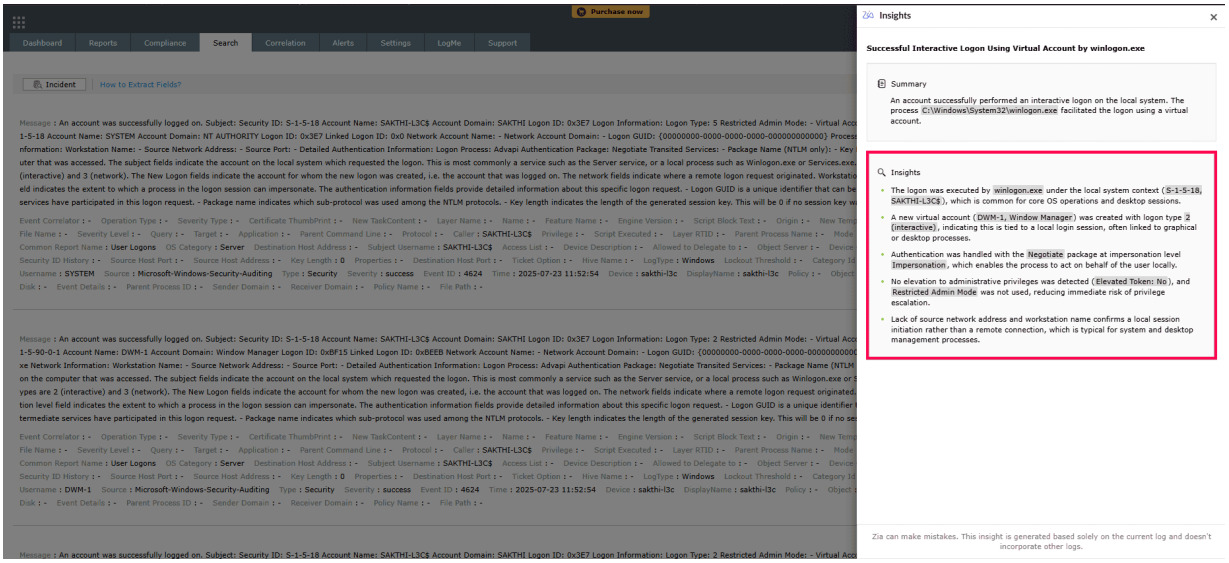


Figure 2: Insights generated by Zia based on Alert data

Timeline

Timeline segment of Zia Insights provides a chronological view of key events related to the alert or incident, including timestamps and specific actions or system behaviors that led up to or followed the incident. This helps reconstruct the attack chain, verify patterns, and correlate the activity with other events.

NOTE

The Timeline segment will be available in the following cases:
- In the Alerts module, when alerts are linked to correlation rules or alerts profiles that are defined based on thresholds.
- In the Incidents module.

1. Correlation rule-based alerts are alert profiles that get associated with specific detection rules. It results from the aggregation of multiple related events or alerts, which together reveal a broader and more significant security incident.
   Example: Events like login failures followed by successful logon and new services installed denote a sequence of activity by the same user. Timeline will be shown for these types of events.
2. Threshold-based alerts are triggered when a particular activity exceeds a predefined limit within a specified time frame, indicating potentially suspicious behavior.
   Example: An alert is generated when a login failure occurs 10 times within 5 minutes, which may suggest a brute-force attack. Timeline of the login failures will be graphically shown by Zia Insights.

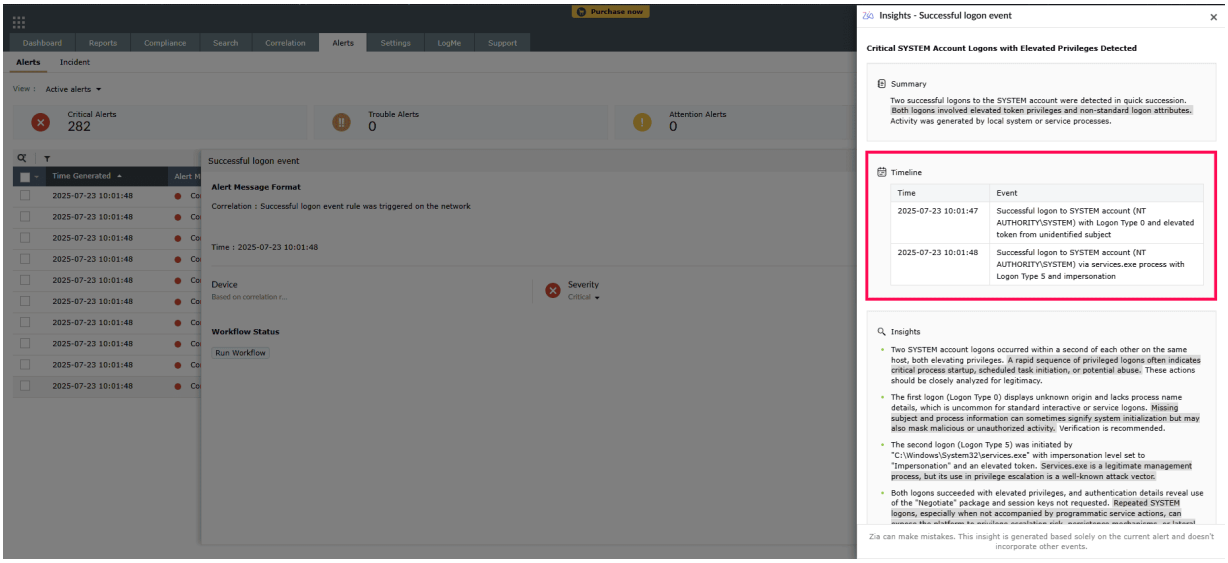


Figure 3: Overview of the event timeline by Zia Insights

Potential MITRE ATT&CK® Mapping

Zia Insights maps events and alerts with known tactics, techniques, and procedures (TTPs) from the MITRE ATT&CK® framework. This includes mapping the activity to the corresponding Tactic Name, Technique ID, and Technique Name.

NOTE

Potential MITRE ATT&CK® Mapping is displayed only when the log indicate suspicious or

malicious activity.

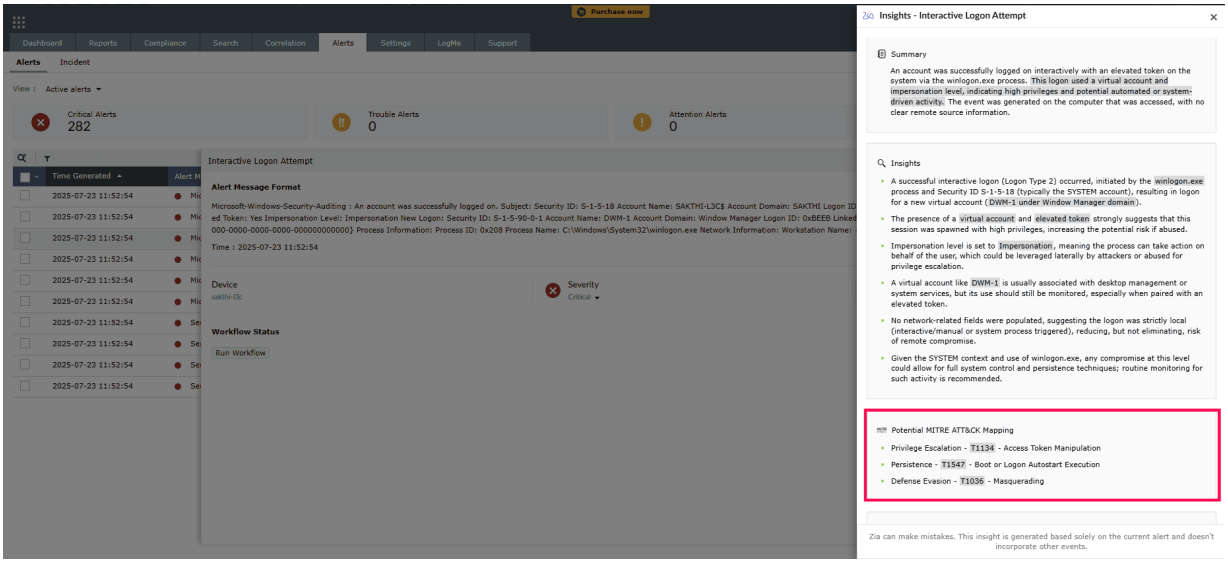


Figure 4: Mapped MITRE ATT&CK® techniques by Zia Insights

Mitigation guidance

Based on log categorization, Zia Insights provide actionable remediation steps that help contain the incident, restore normal operations, and reduce the risk of future occurrences. Recommendations are tailored to the type of log,such as crash, error, audit, and security.

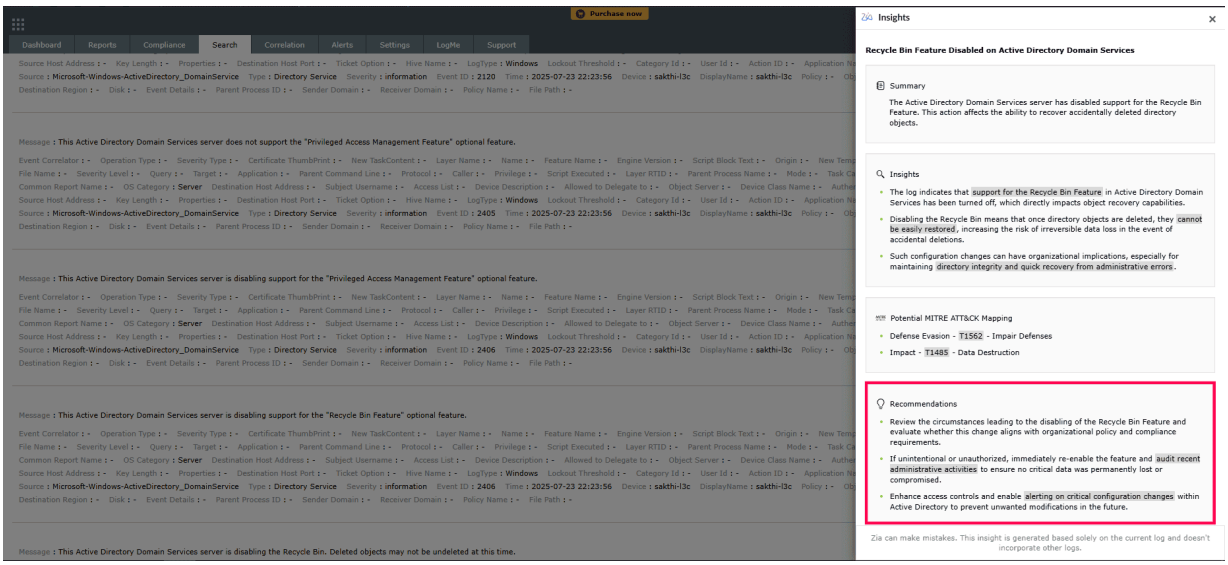


Figure 3: Overview of the event timeline by Zia Insights

Read also

This document elaborated on the overview, key insights, and use cases of Zia Insights. For configuring and leveraging the capabilities of Zia Insights, refer to the articles below:

- Setting up Zia Insights

- Invoking Zia Insights

10.2.2.3. Setting up Zia Insights

Last updated on: September 12, 2025

In this page

Overview

Pre-requisites

Accessing Zia Insights

Creating an Azure OpenAI resource

Steps to obtain Endpoint URL and API key

Deploying a model in Azure OpenAI

Overview

Zia Insights provides AI-powered actionable insights on incidents, alerts and logs using the Bring Your Own Key (BYOK) model, supporting integration with Azure OpenAI services.
This page elaborates on configurations that are essential to enable Zia Insights. It covers the creation of an Azure OpenAI resource, deployment of a compatible model, retrieval of necessary credentials such as the endpoint URL and API key, and integrating the AI service with the product console.

Pre-requisites

Before beginning the setup, ensure the following:

- You must have an active Azure subscription with access to the Azure OpenAI service.
- The following credentials are required from your Azure portal:
  - Endpoint URL
  - API key
  - Deployed model name

Accessing Zia Insights

1. Log in to your account.
2. Go to the Settings tab, and select Admin.
3. Navigate to Zia and select Insights.
4. To enable Zia Insights in, click Configure Now.



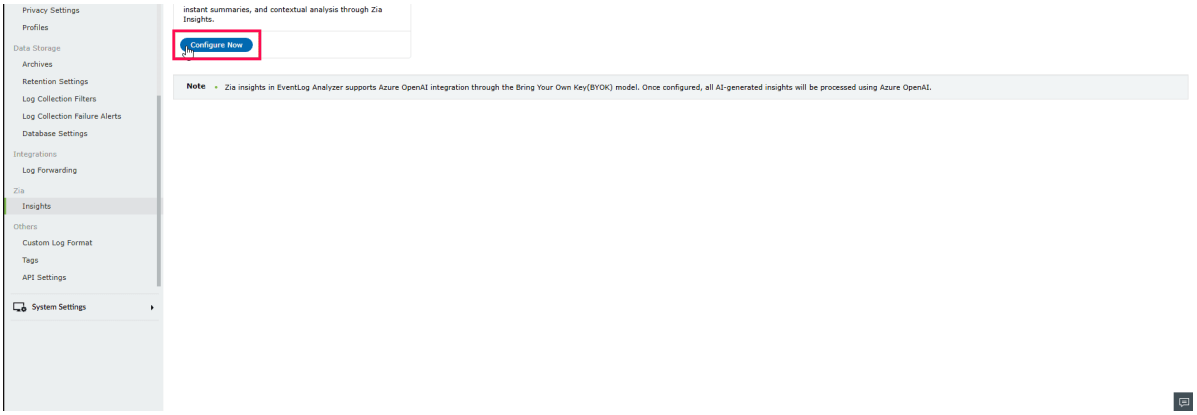


Figure 1: Configuring Azure OpenAI

5. Enter the following details obtained from your Azure Portal:
   - Endpoint URL
   - DeploymentName
   - API Key
6. Click Save to complete the initial setup.

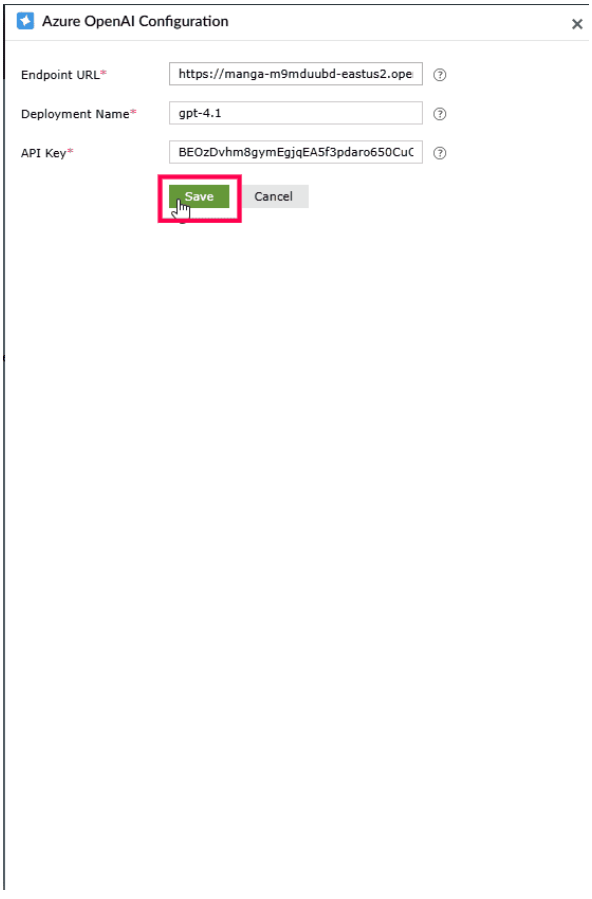


Figure 2: Configuring Azure OpenAI

7. In the pop-up window that appears, read the data privacy notice, select the I understand checkbox to acknowledge the terms, and then click Proceed to complete the OpenAI integration.



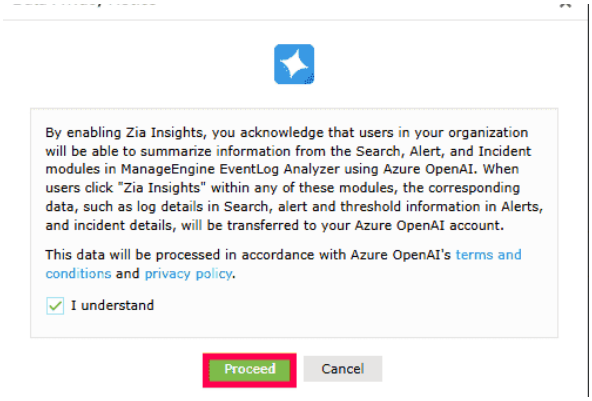


Figure 3: Azure OpenAI integration

8. Once the integration is complete, Zia Insights will be enabled.

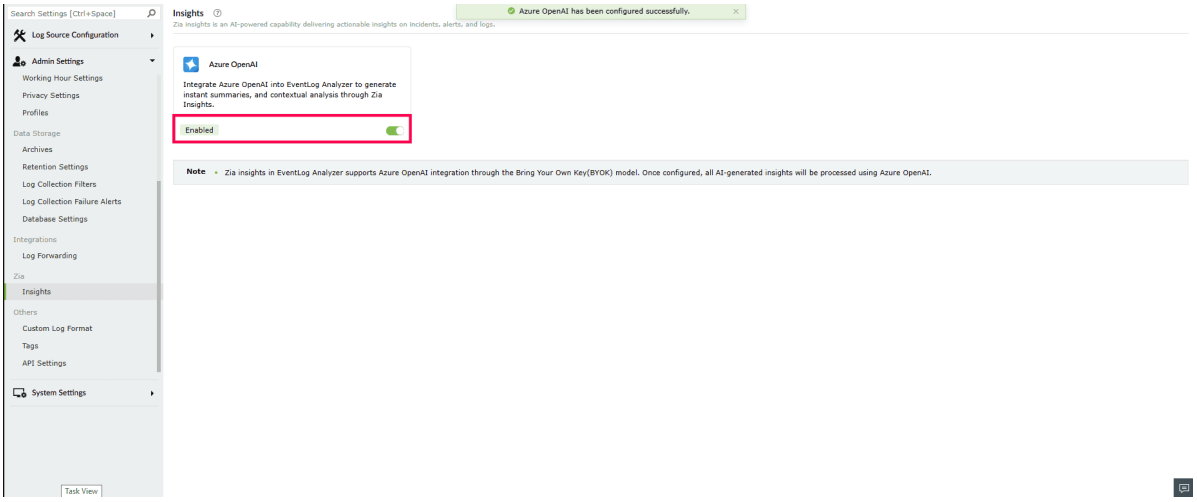


Figure 4: Azure OpenAI integration

- To disable or re-enable Zia Insights, use the toggle switch beside the Azure OpenAI option.
- A confirmation pop-up will appear when disabling.
- Click Yes to disable Zia Insights.
- To delete the Azure OpenAI configuration, select the checkbox “Delete existing Azure OpenAI configuration” before clicking Yes.

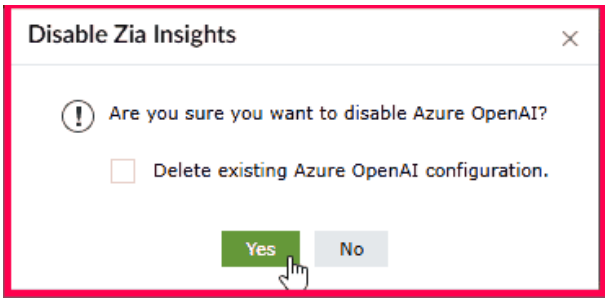


Figure 5: Disabling and deleting Azure OpenAI configuration

Creating an Azure OpenAI resource

If you do not already have an Azure OpenAI resource, follow these steps:

NOTE If you already have an Azure OpenAI resource, refer to this to obtain the API key and Endpoint URL.

1. Log in to Azure portal and click Create a resource.

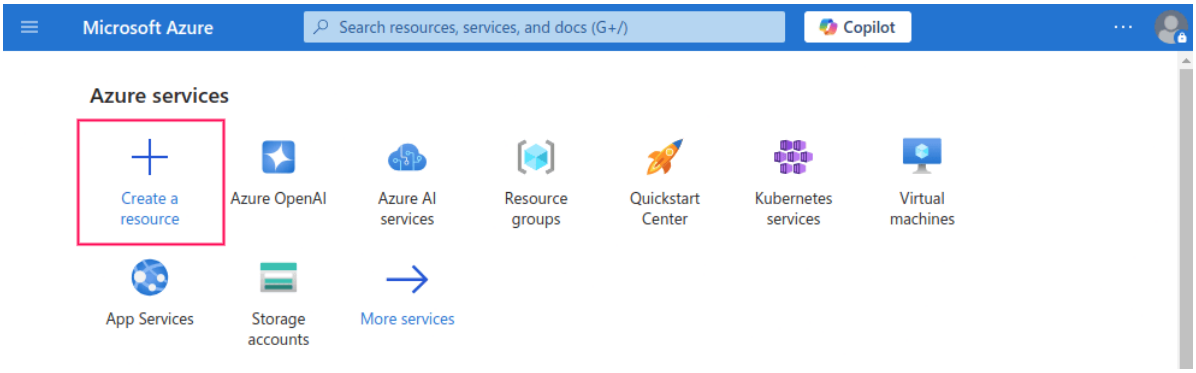
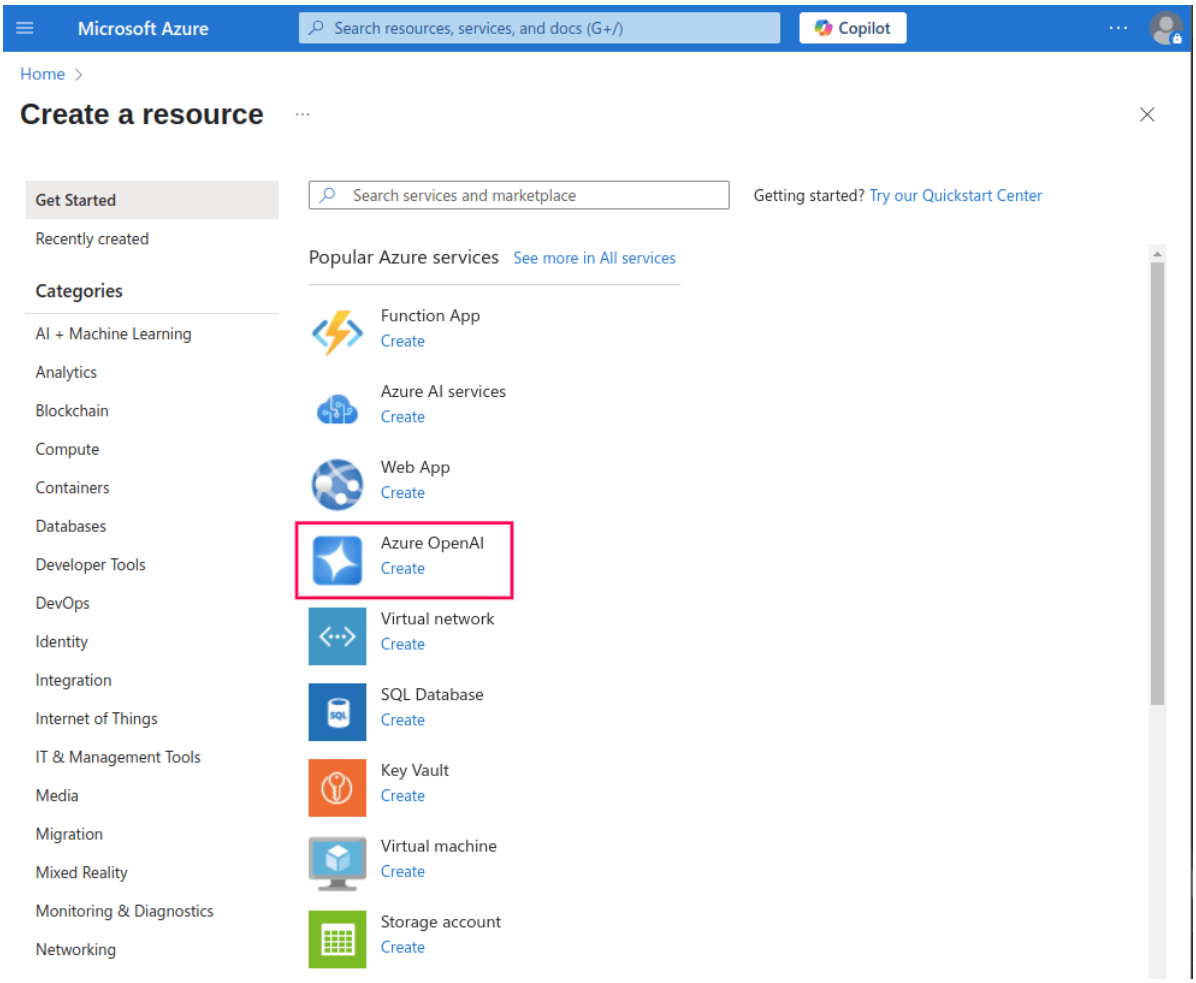


Figure 6: Creating a resource in Microsoft Azure

2. Select Azure OpenAI as the resource type.



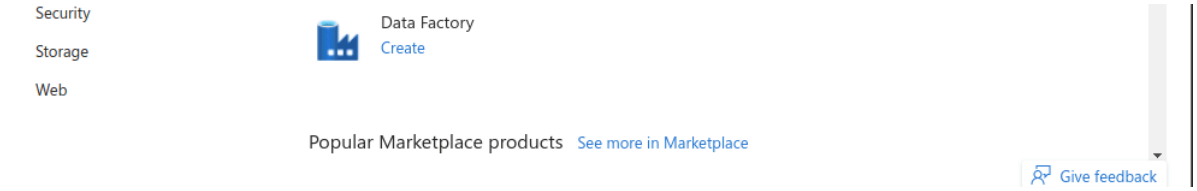


Figure 7: Creating an Azure OpenAI resource

3. Choose a Subscription of your choice.
4. Select an existing Resource group or create a new one.

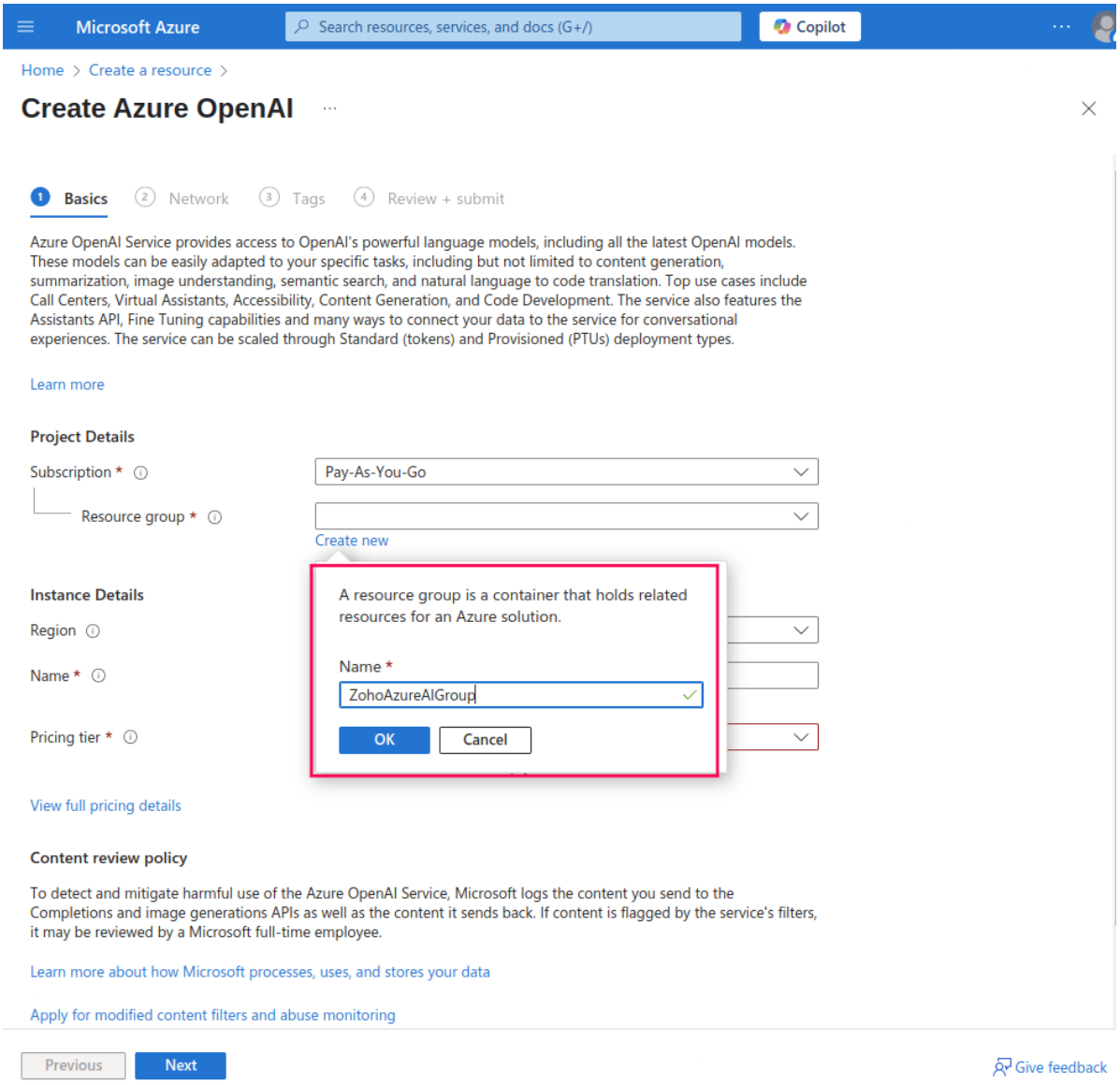
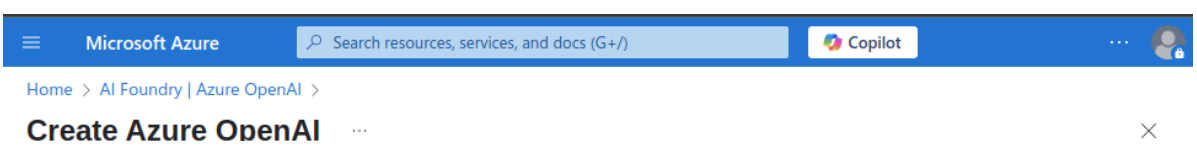


Figure 8: Creating a resource group in Microsoft Azure

5. Pick your desired Region and Pricing Tier.
6. Enter a suitable Name for the resource.



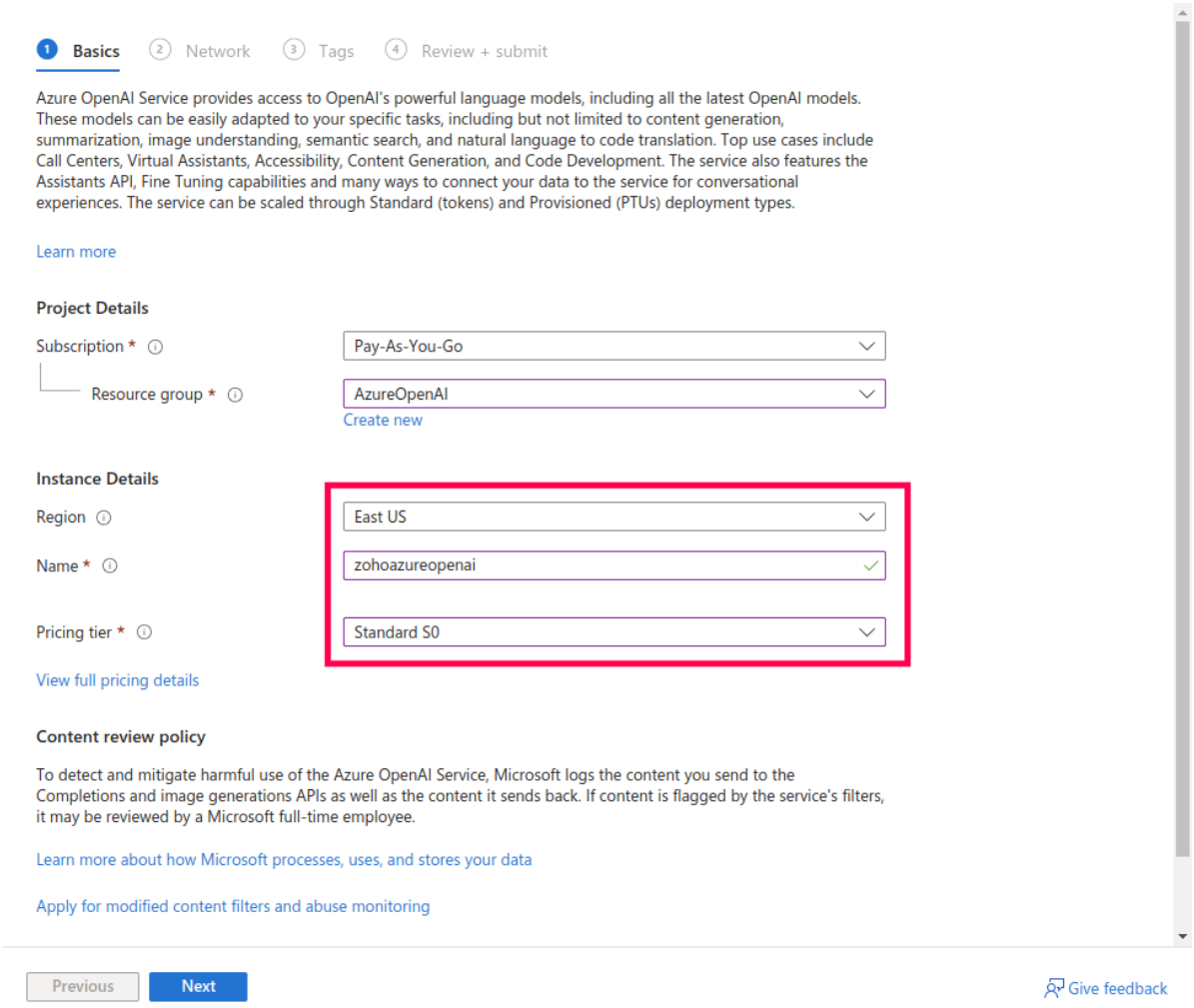
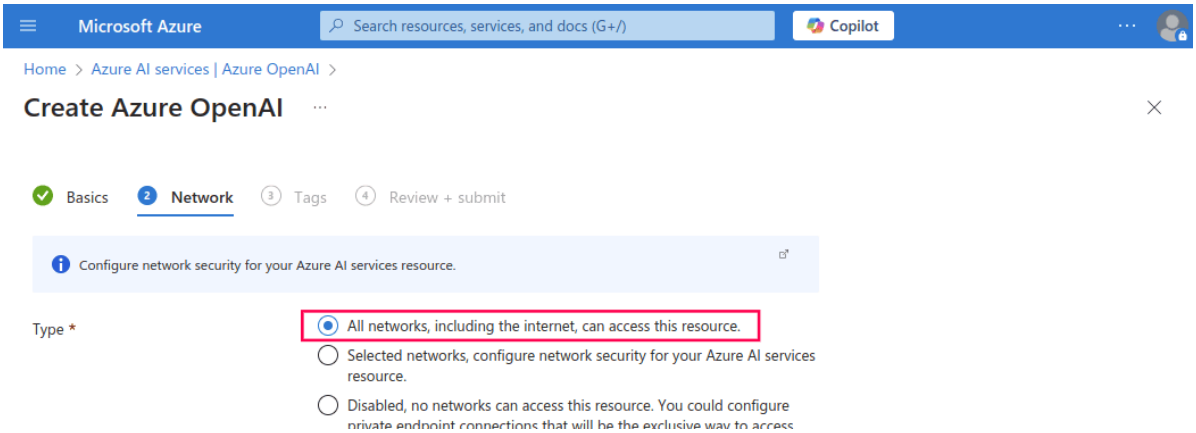


Figure 9: Instance details for Azure OpenAI service

7. Under Networking, select All networks, including the internet, can access this resource.

> **NOTE**
>
> The Azure OpenAI resource must be publicly available on the internet so that the product console can access the endpoint.



this resource.

Previous Next Give feedback

Figure 10: Configuring network security for Azure AI services resource

8. Click Next to configure Tags (optional).
9. Click Next again to move to the Review + Submit page.

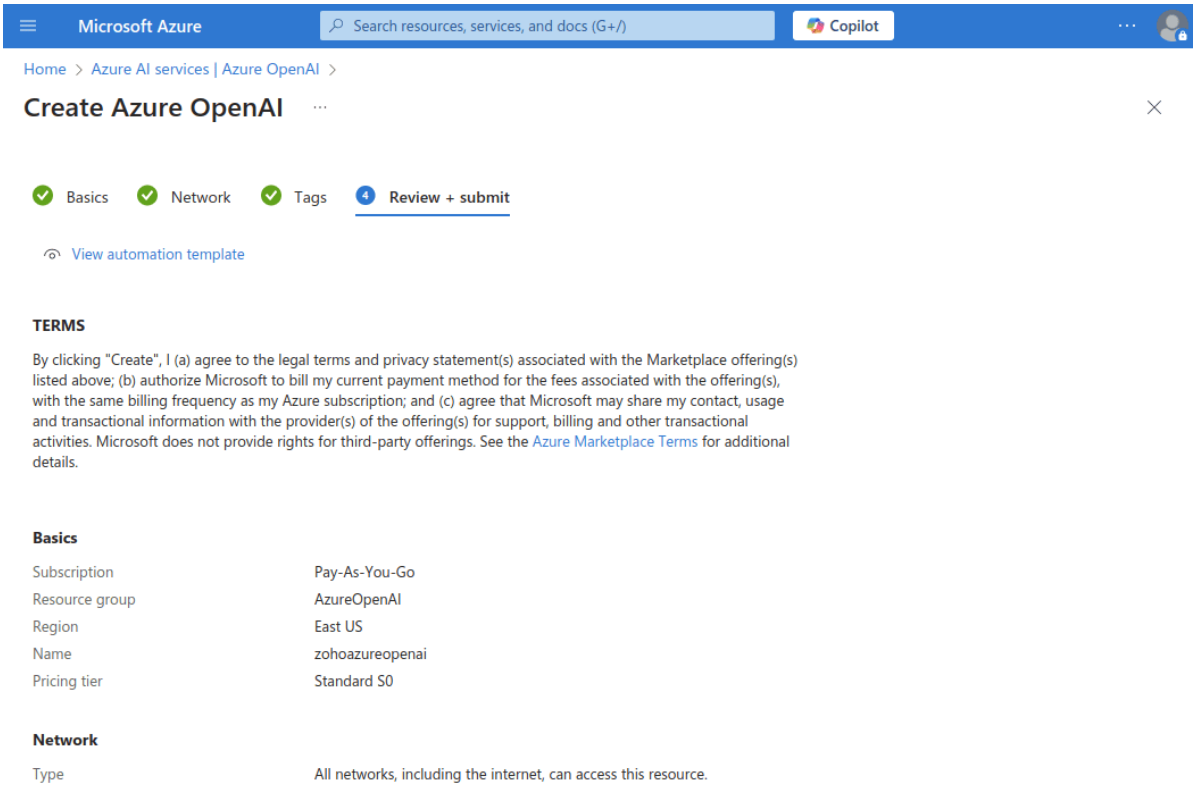




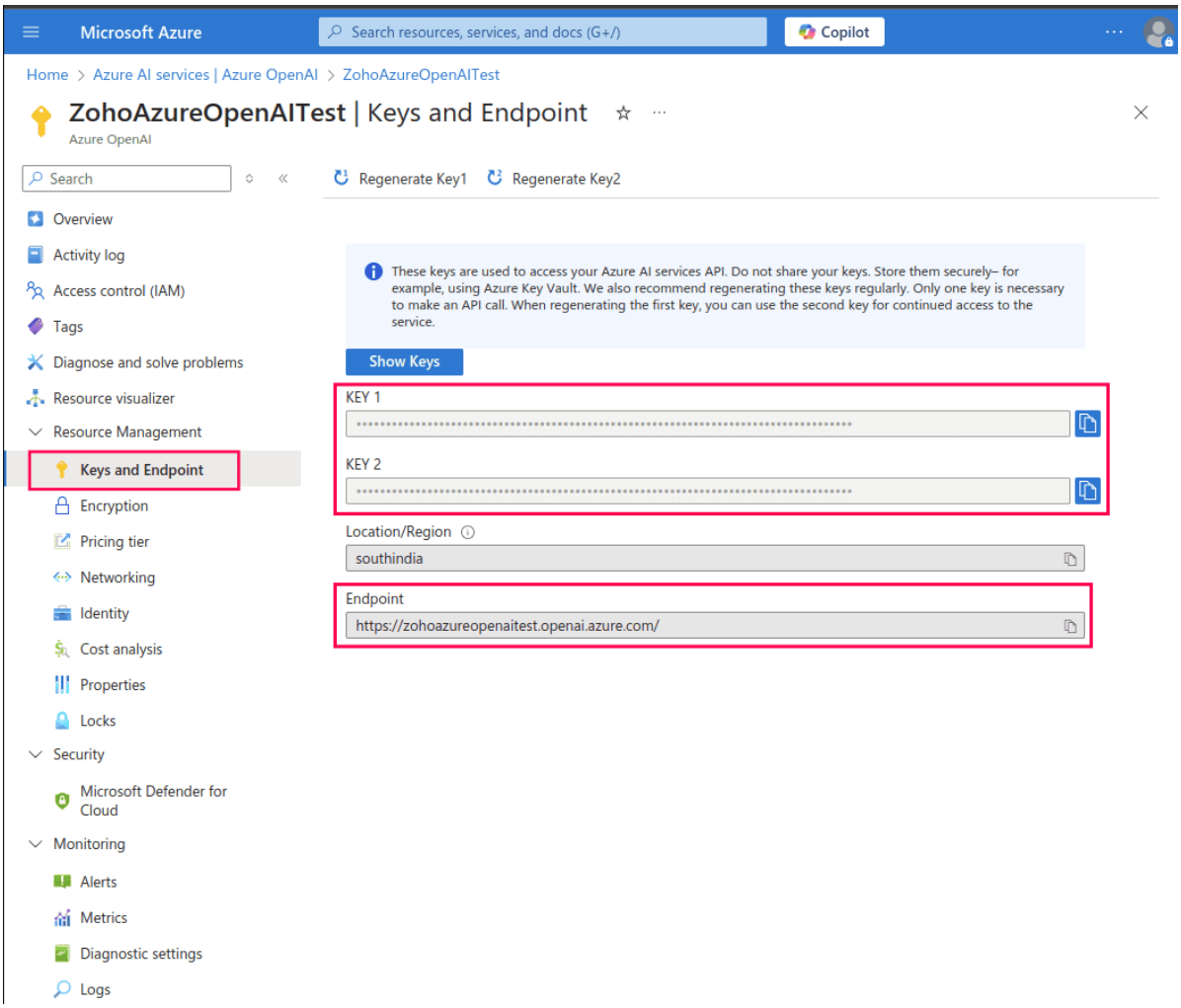
Figure 11: Final review to create resource

10. Review your settings and click Create to provision the resource.

Steps to obtain Endpoint URL and API key

If you already have an Endpoint URL and API key, skip to the next section. If not:

1. Log in to Azure portal and navigate to your Azure OpenAI resource.
2. In the left pane, under the Resource Management section, click on Keys and Endpoint. It will open Keys and Endpoint console.
3. In this window, you will find the Endpoint URL and API keys for your Azure OpenAI resource. Copy these details for use in the product.



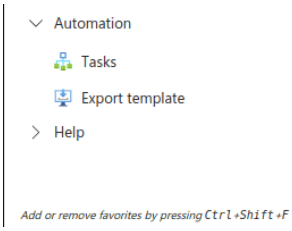


Figure 12: Obtaining API keys and Endpoint URL for Azure OpenAI resource

Deploying a model in Azure OpenAI

A deployed model is a version of an AI model (such as GPT-4o or GPT-4.1) that has been activated and made available for use within your Azure OpenAI resource. The product console will interact with the deployed model to generate AI-powered insights from your logs and alerts.

> NOTE
>
> If you already have a deployed model, you can directly use its deployment name when integrating with the product console. Ensure that the model is one of the following types:
>
> 1. The Chat Completion API model (models GPT-4o or newer). For better results, use latest available model such as GPT-4.1 or newer.
> 2. A non-reasoning model, excluding versions like o1-preview and o1-mini.

If you do not have a deployed model, follow the steps below.

Steps to deploy a model

1. Navigate to your Azure OpenAI resource and click Go to Azure AI Foundry portal.

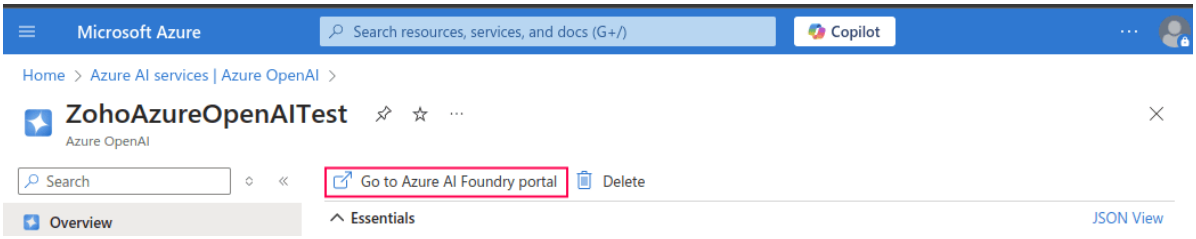
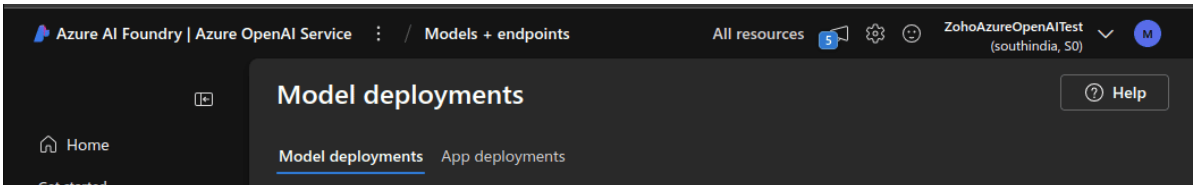


Figure 13: Deploying a model in the Azure AI Foundry portal

2. On the Azure AI Foundry portal, navigate to the Deployments section, click Deploy model, and select Deploy base model.



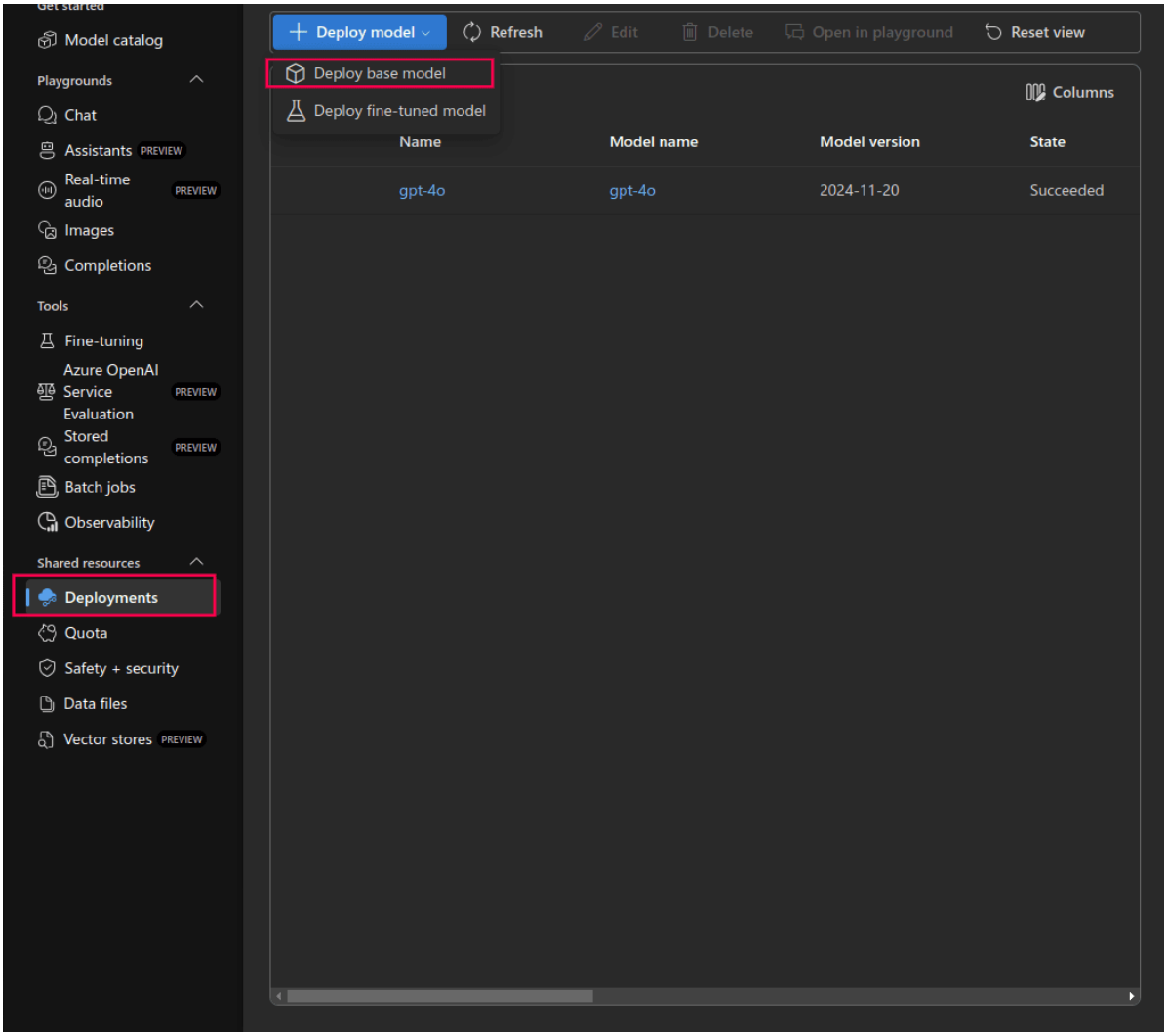
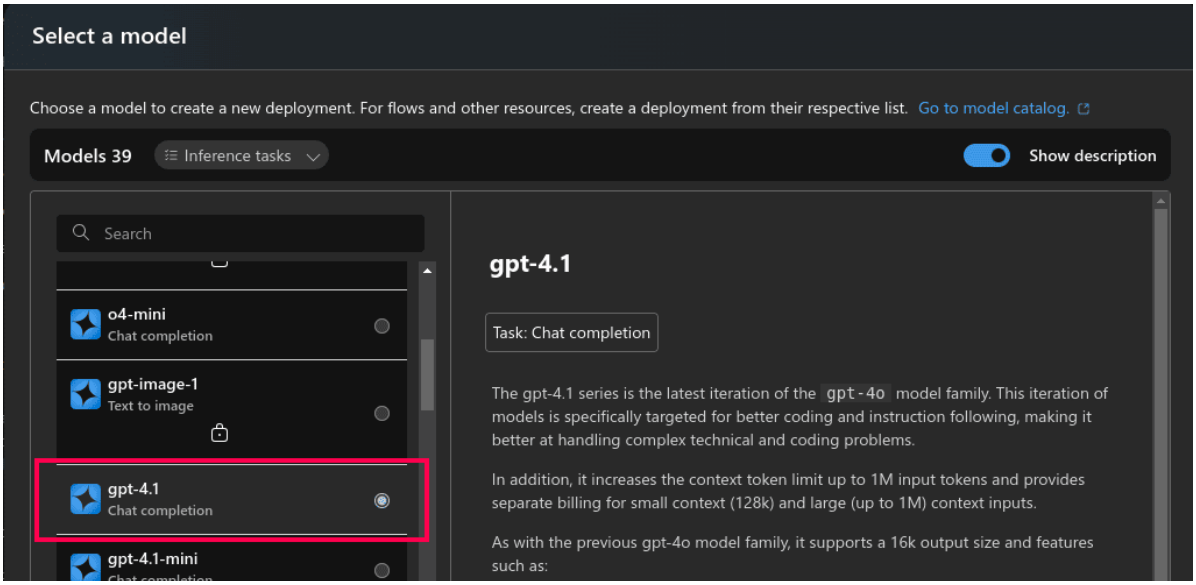


Figure 14: Deploying a model in Azure AI Foundry portal

3. Choose a model that meets the following constraints:

   - Must support the Chat Completion API (models GPT-4o or newer). For better results, use latest available model such as GPT-4.1 or newer. Avoid reasoning models like o1-preview and o1-mini because they do not support system prompts.



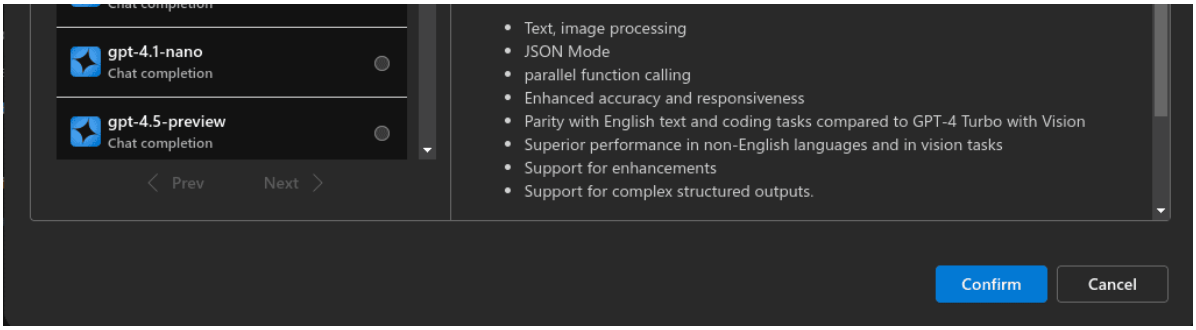


Figure 15: Available models for deployment in Azure AI Foundry portal

4. Enter a deployment name of your choice (defaults to the model name).

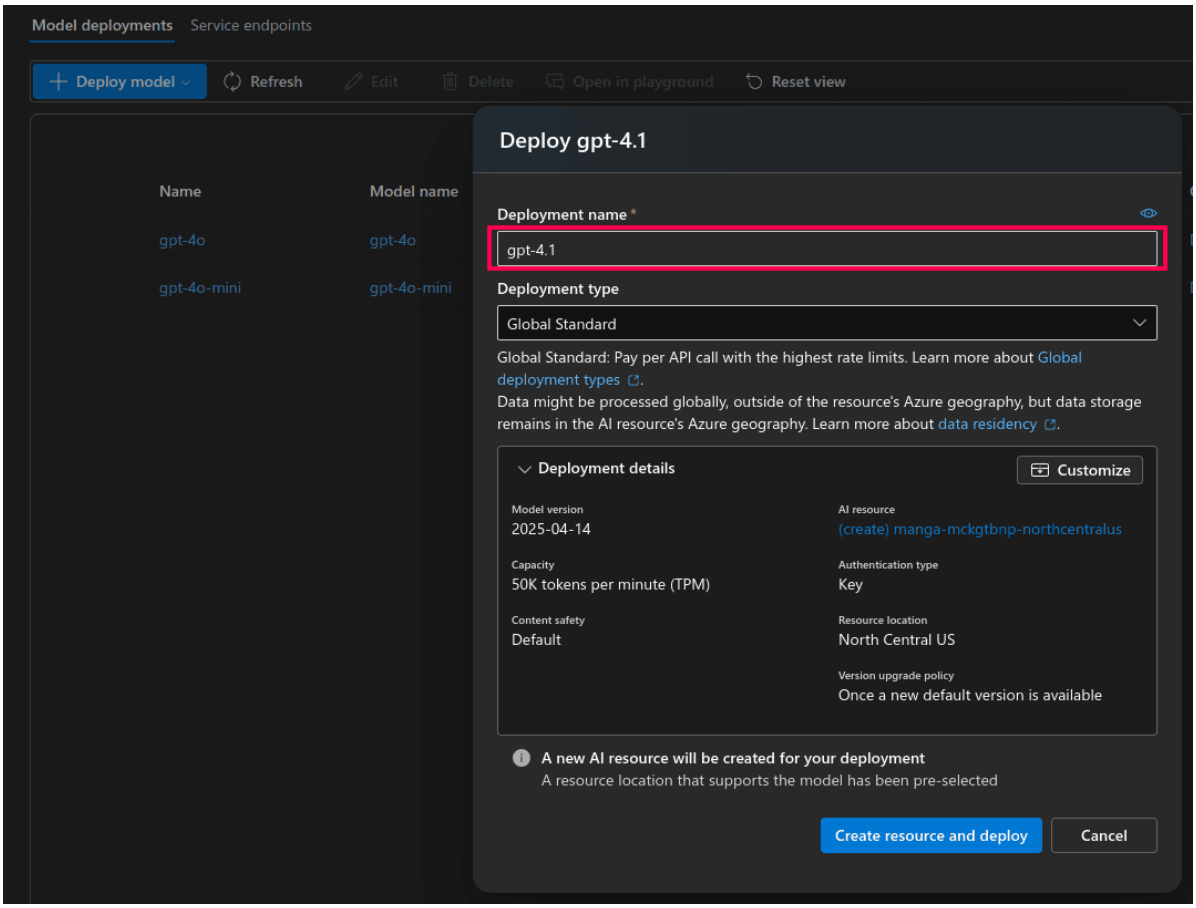
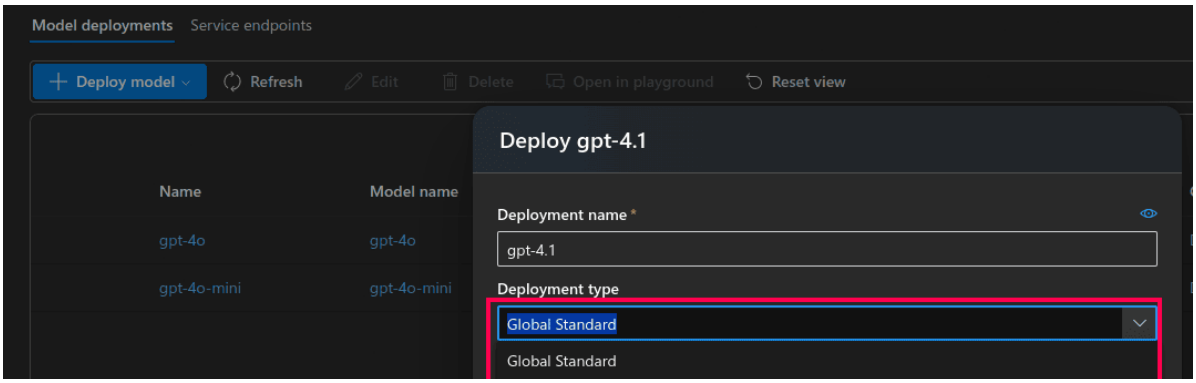


Figure 16: Deployment settings in Azure AI Foundry portal

5. Select the deployment type based on your data processing needs. Learn more about deployment types.



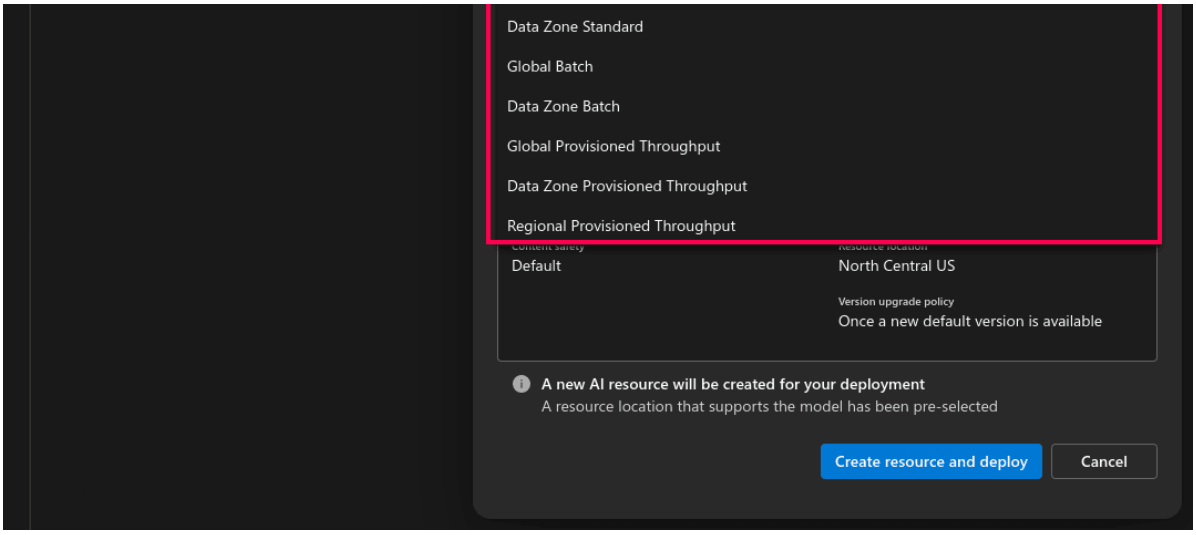


Figure 17: Deployment settings in Azure AI Foundry portal

6. Click Create resource and deploy to complete the model deployment.

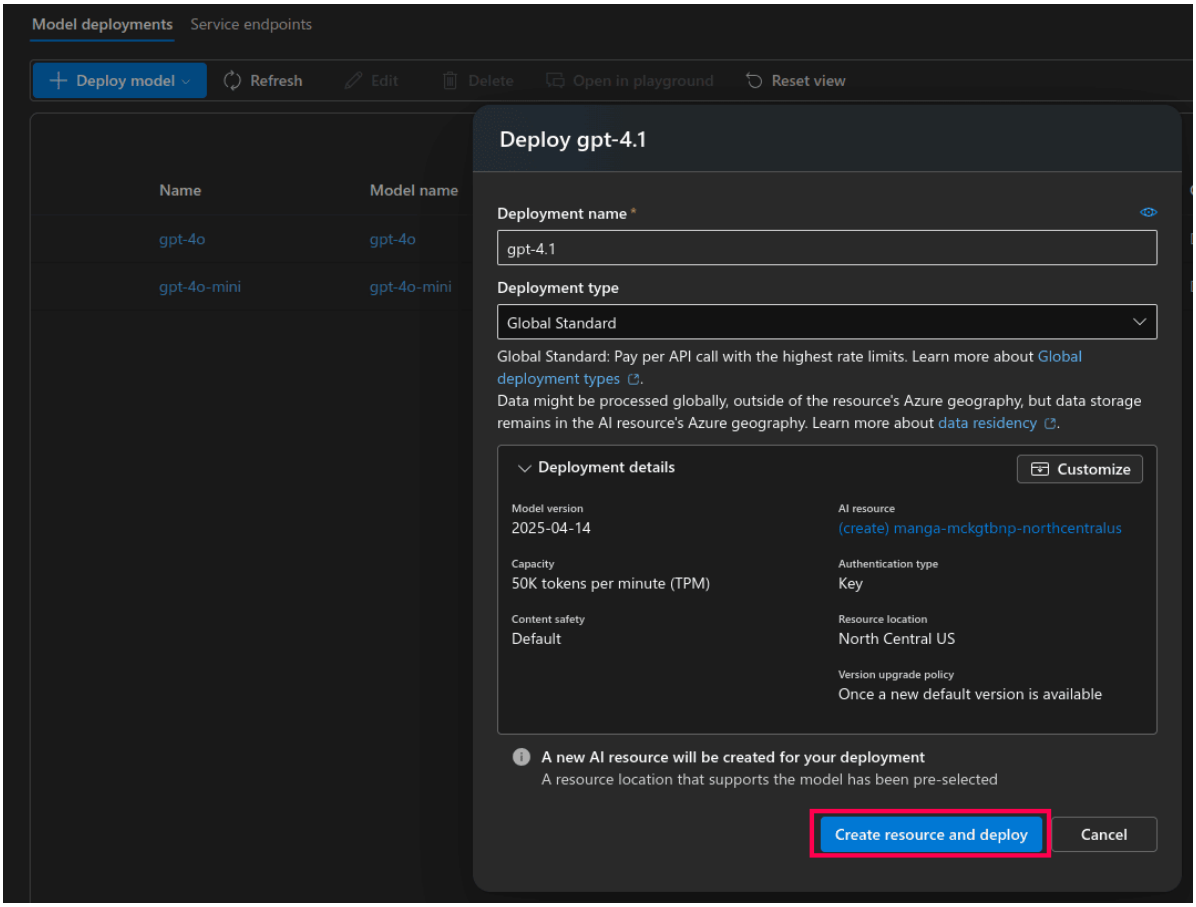


Figure 18: Model deployment in Azure AI Foundry portal

NOTE Once you've completed these steps and obtained your credentials, refer to this section to access Zia Insights.

Read also

This document detailed the configuration steps required to enable Zia Insights, including Azure OpenAI resource creation, model deployment, and integration setup. To leverage the capabilities of Zia Insights, refer to the following articles:

following articles:

- Using Zia Insights
- Invoking Zia Insights

10.2.2.4. Invoking Zia Insights

Last updated on: September 12, 2025

In this page

Overview

Invoking Zia Insights from Search

Invoking Zia Insights from Alerts

Invoking Zia Insights from Incidents

Overview

Zia Insights is an AI-powered capability that delivers contextual security insights by analyzing logs, alerts, and incidents. These insights help interpret security activity, identify impacted entities, map observed behavior to the MITRE ATT&CK® framework, and determine recommended response actions.
This page explains how to invoke Zia Insights from the Search, Alerts, and Incidents modules.

Invoking Zia Insights from Search

1. In your account, go to the Search tab.
2. Perform a search query using either the basic or advanced mode.

> NOTE
>
> Refer to this video to learn how to perform log searches.

3. In the search results, hover over a specific log entry.
4. Click on the zia icon on the top-right corner of the log entry to view insights generated by Zia.

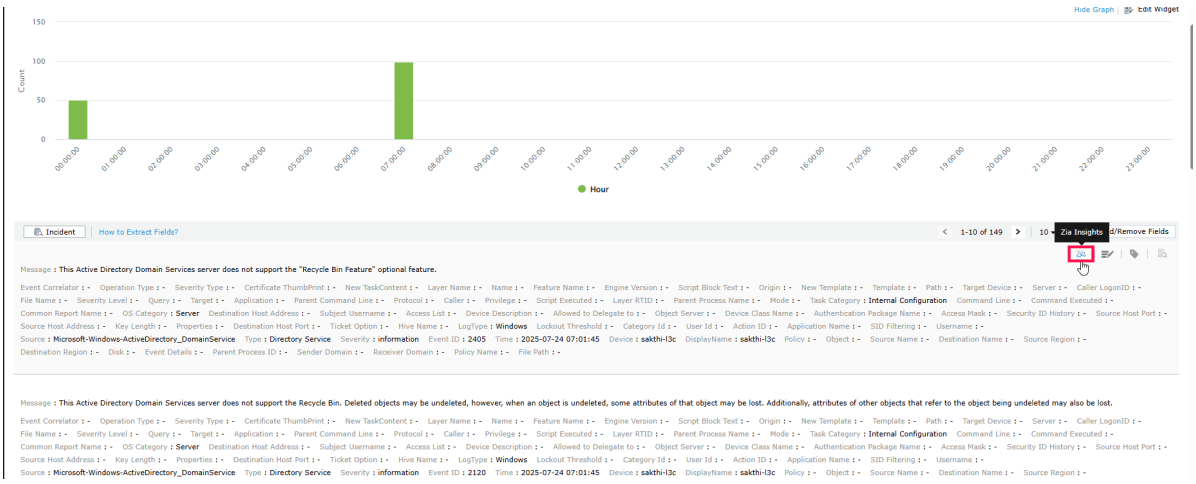
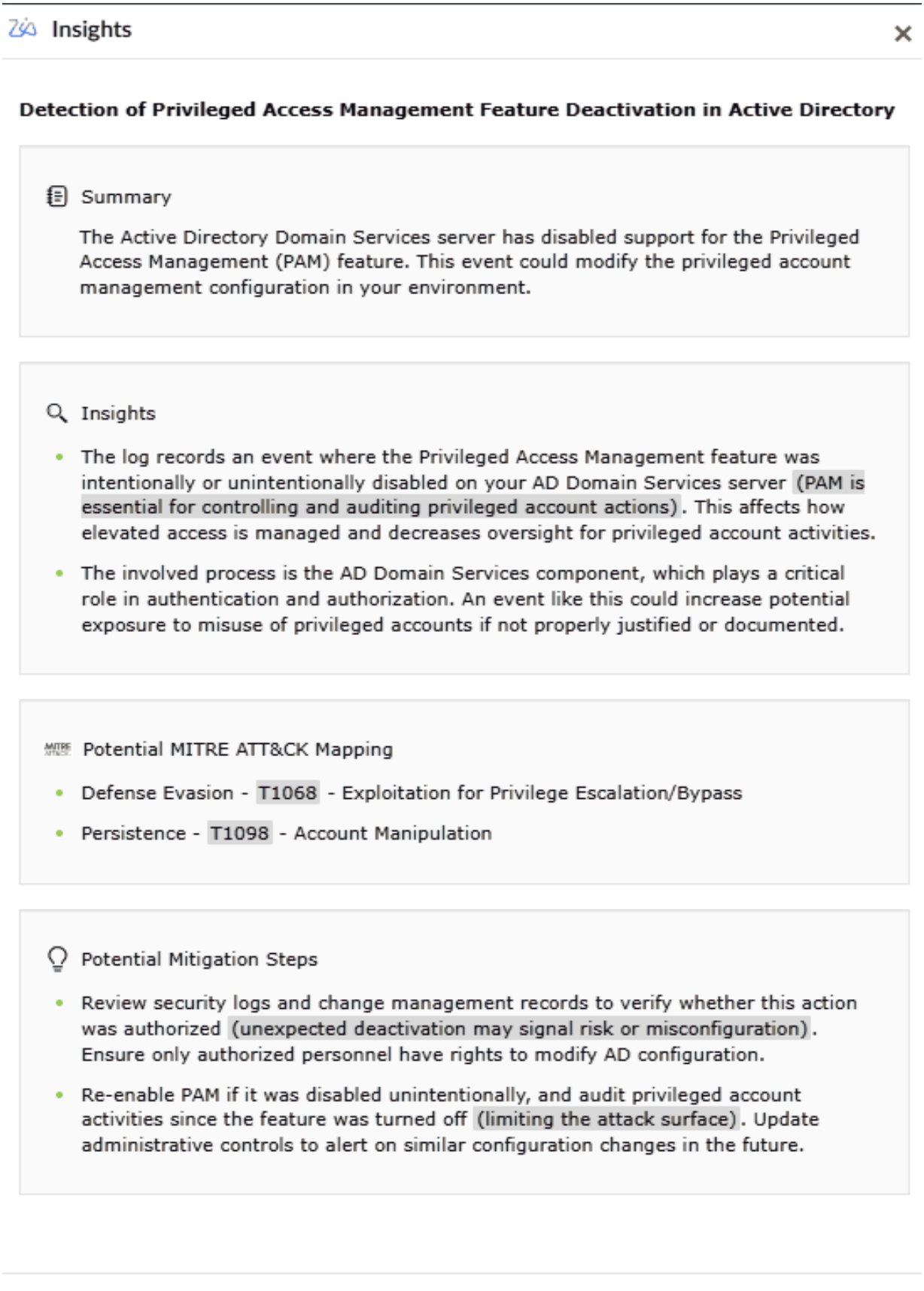


Figure 1: Invoking Zia Insights from Search

Insights provided by Zia Insights for Search

Zia will process the selected log and display contextual insights, including a summary, associated MITRE ATT&CK® techniques (if applicable), and suggested mitigation steps.



Zia can make mistakes. This insight is generated based solely on the current log and doesn't incorporate other logs.

Figure 2: Zia Insights generated for the selected log

Invoking Zia Insights from Alerts

1. In your account, go to the Alerts tab and select Alerts.
2. Select an alert from the list.
3. Click on the Zia insights icon displayed at the top-right corner to generate Zia Insights.

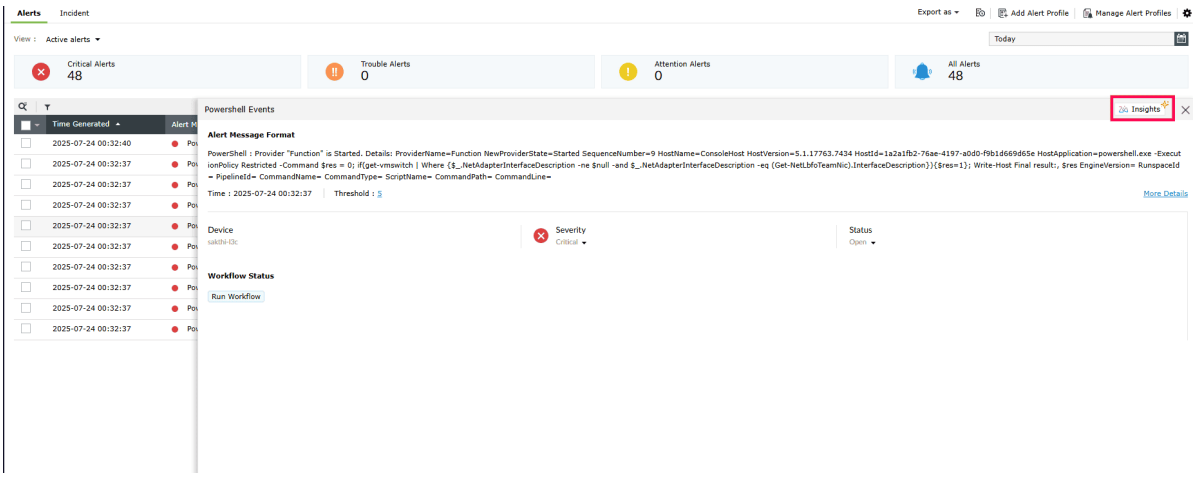


Figure 3: Invoking Zia Insights from Alerts

Insights provided by Zia Insights for Alerts

For alerts, Zia Insights provides contextual summary, attack timeline, relevant MITRE ATT&CK® techniques (if applicable), and mitigation steps based on the alert data.



2025-07-24 00:32:37	svchost process started a new database engine instance
2025-07-24 00:32:38	PowerShell engine state changed from None to Available
2025-07-24 00:32:39	Provider "Function" started in ConsoleHost
2025-07-24 00:32:40	Provider "Variable" started in ConsoleHost
2025-07-24 00:32:41	PowerShell engine state changed from Available to Stopped

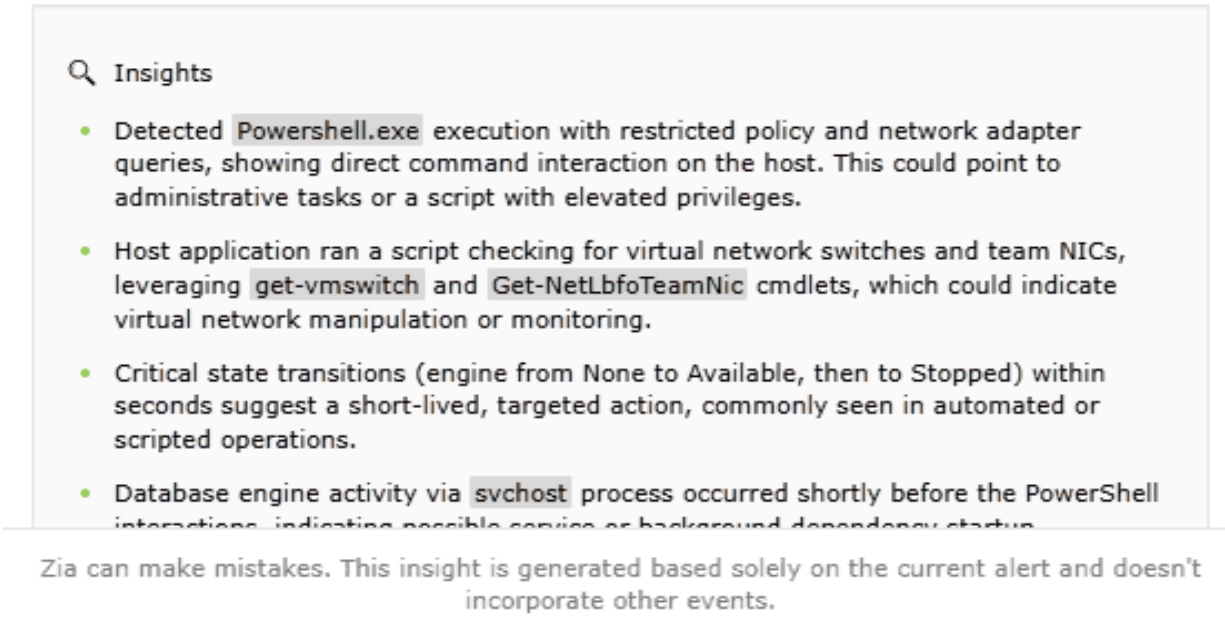


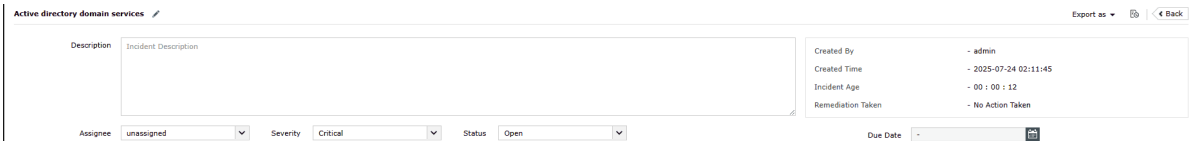
Figure 4: Zia Insights generated for Alerts

Invoking Zia Insights from Incidents

1. In your account, go to the Alerts tab and select Incident.

> NOTE
>
> Use the Select view dropdown to filter incidents. Select from All Incidents, Active Incidents, Critical Incidents, or create a new one using Add Custom View.

2. Select an incident from the list.
3. Click on the Zia insights icon to generate insights.



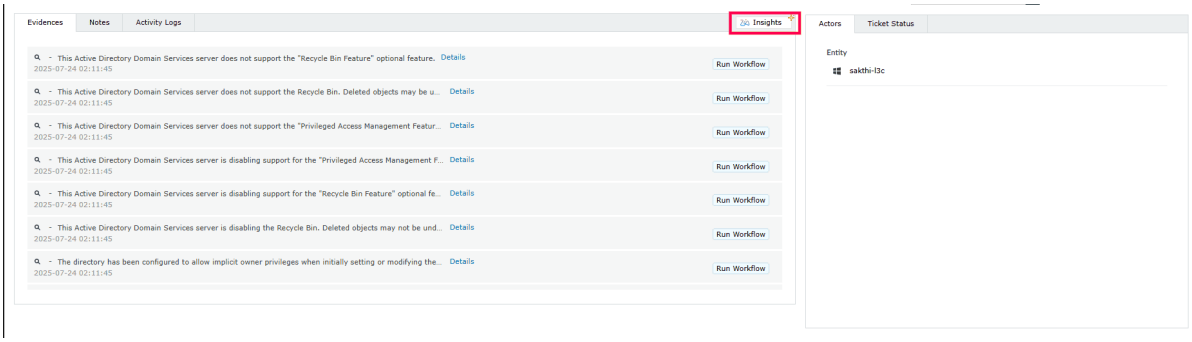


Figure 5: Invoking Zia Insights from Incidents

Insights provided by Zia Insights for Incidents

When invoked from the Incident console, Zia Insights provides details on involved actors, a chronological evidence timeline, evidence summary, and relevant MITRE ATT&CK® techniques based on the incident data.

Insights - Active directory domain services

Actors

- Entity involved: sakthi-l3c in Active Directory Domain Services operations.

Evidence Timeline

Time	Event
2025-07-24 07:01:45	Active Directory Domain Services server does not support the "Recycle Bin Feature" optional feature. (Count ≈ 1)
2025-07-24 07:01:45	Active Directory Domain Services server does not support the Recycle Bin. Deleted objects may be undeleted, but attribute loss can occur. (Count ≈ 1)
2025-07-24 07:01:45	Active Directory Domain Services server does not support the "Privileged Access Management Feature" optional feature. (Count ≈ 1)
2025-07-24 07:01:45	Active Directory Domain Services server is disabling support for the "Privileged Access Management Feature" optional feature. (Count ≈ 1)
2025-07-24 07:01:45	Active Directory Domain Services server is disabling support for the "Recycle Bin Feature" optional feature. (Count ≈ 1)
2025-07-24 07:01:45	Active Directory Domain Services server is disabling the Recycle Bin. Deleted objects may not be undeleted at this time. (Count ≈ 1)
2025-07-24 07:01:45	Directory is configured to allow implicit owner

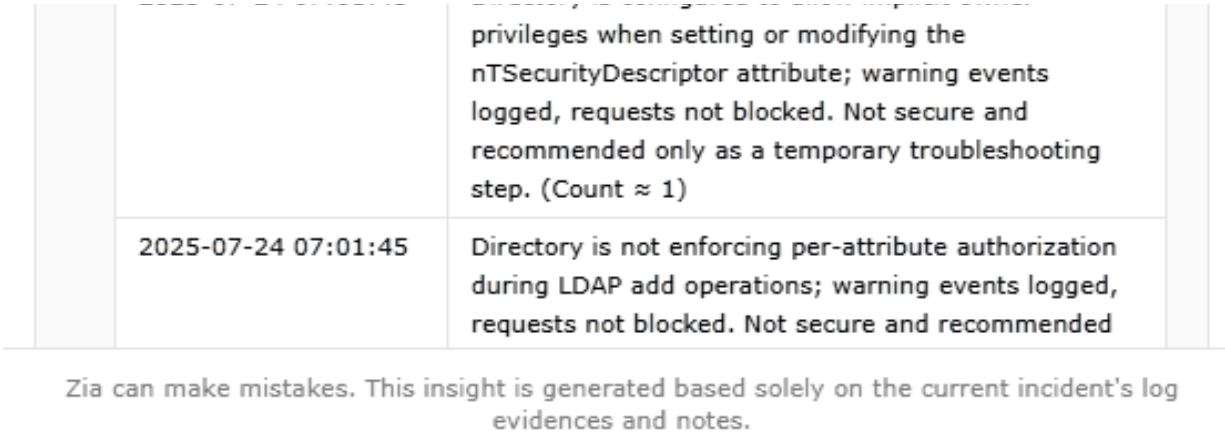


Figure 6: Zia Insights generated for Incidents

Read also

This document explained how to access Zia Insights from Search, Alerts, and Incidents within the product console to generate AI-powered security insights. For a comprehensive overview of Zia Insights and instructions on how to leverage its capabilities effectively, refer to the following articles:

- Using Zia Insights
- Setting up Zia Insights

10.2.3.1. Overview

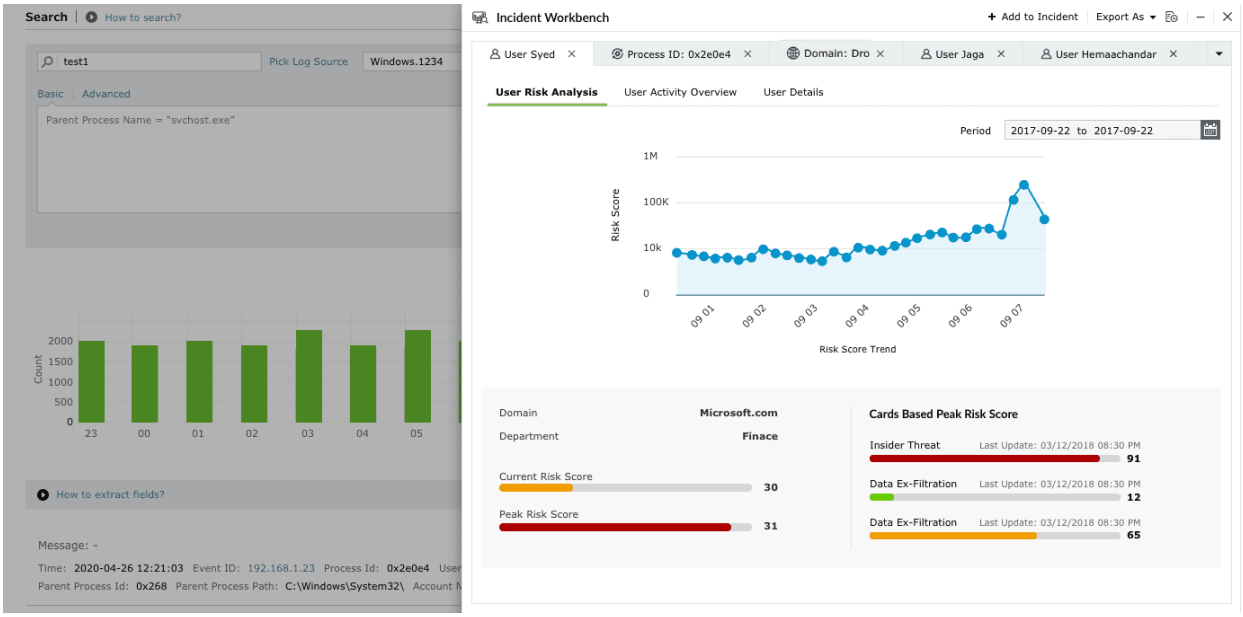
Last updated on: September 12, 2025

In this page

Access

Analysis

- The Incident workbench is Eventlog Analyzer's investigation console that unifies analytics of the core entities such as users, processes, and threat sources.
- This feature facilitates users to add, compare, and analyze data with enriched integrations like UEBA and Advanced Threat Analytics.
- Utilize the contextual assesment with risk based profiling, conduct faster root cause analysis by probing the process trees, and minimize the overall time taken to investigate and resolve threats.



Features:

Here are the entities you can analyze using Incident Workbench:

- Users

  Analytics offered: ML-based user activity and risk score data compiled through UEBA integration from Log360's suite.

- Process

  Analytics offered: Process hunting tree with parent-child relationships and event timeline.

- Threat sources

  Analytics offered: Risk analysis from security vendors using Advanced Threat Analytics integration.

Access and usability:

- Roles and restrictions:
  - Operator and guest role members have no access to the Incident Workbench.
  - Custom roles can be created to provide access to the Incident Workbench.
- Access: Incident workbench can be invoked from multiple dashboards of EventLog Analyzer such as reports, log search, compliance, alerts, and more.
- Users can add upto 20 tabs in a single instance of the Incident Workbench and save it to an existing incident or create a new incident.

10.2.3.2. Incident Workbench Access

Last updated on: September 12, 2025

> **Note**
>
> Please refer to the Incident Workbench Overview page to learn about Incident Workbench. This page details on how to access the workbench in EventLog Analyzer.

- Log fields you can click on to invoke the Incident Workbench:

  Users:

  - Username
  - Target User
  - VPN UserName
  - User Principal Name
  - Destination User
  - Sourceuser
  - Subject Username

  Process:

  - Process Id
  - Parent Process ID
  - Process GUID
  - Parent Process GUID
  - Process Name
  - Parent Process Name

  Domain analysis:

  - Domain
  - URL Site

  IP Analysis:

  - Source IP
  - Client IP Address
  - Server IP Address
  - Address
  - Destination IP

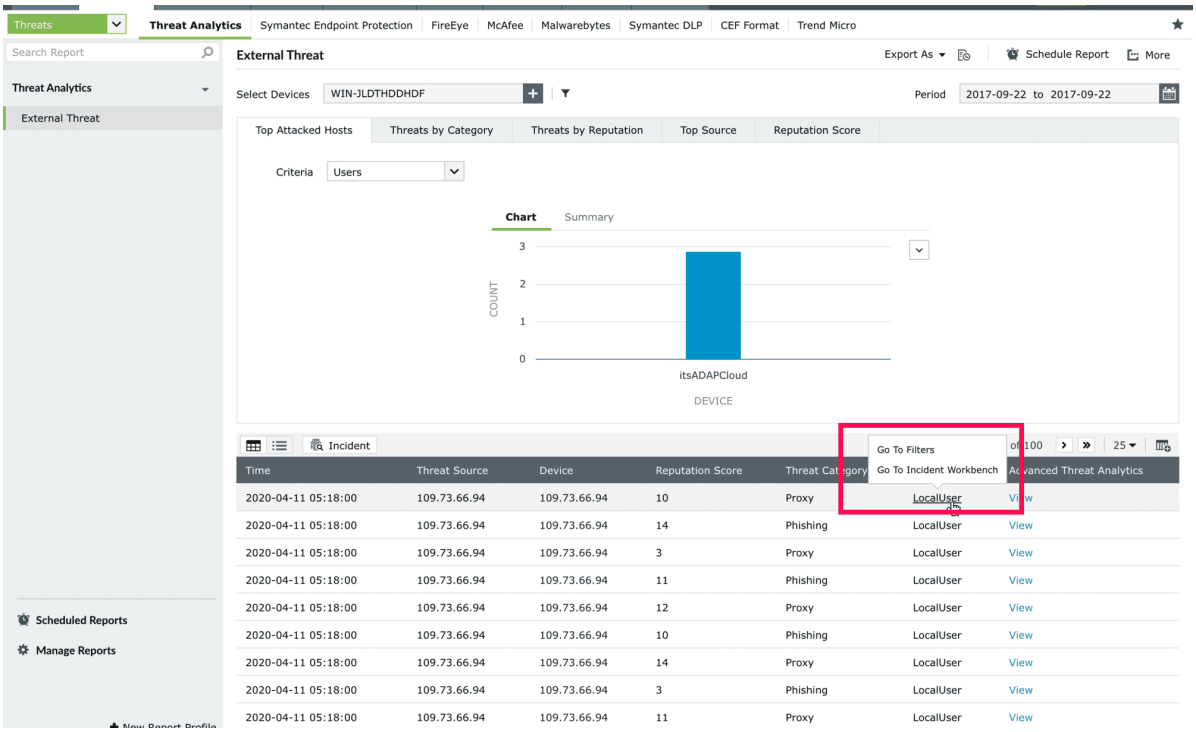
- Remote Ip
- Source Host Address
- NAT Source Address
- NAT Destination Address
- Destination IP
- Original Client IP
- IP Address
- Endpoint IP
- Private Ip
- Target Ip

URL Analysis:

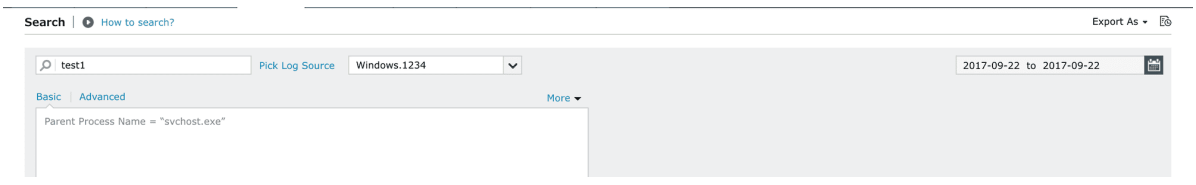
- Payload URL
- Object URL
- URL

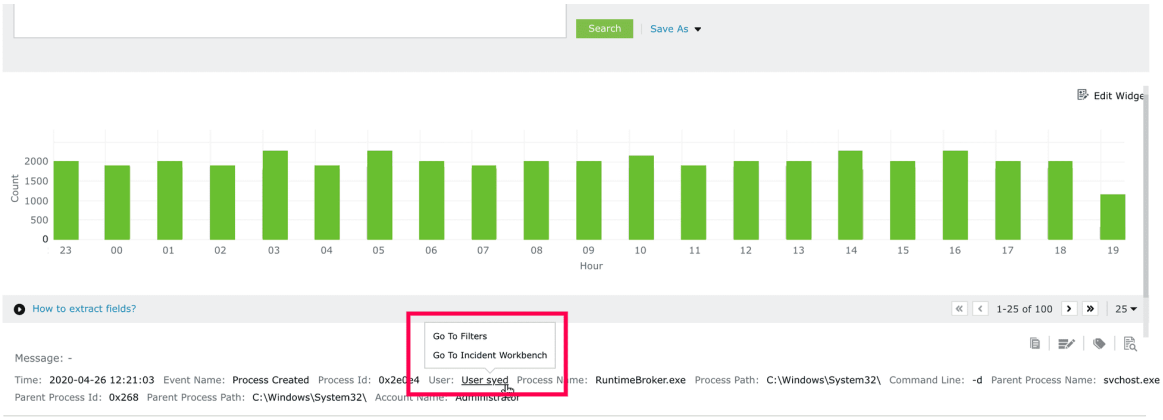
Invoking the Incident Workbench from different dashboards of EventLog Analyzer:

- From Reports

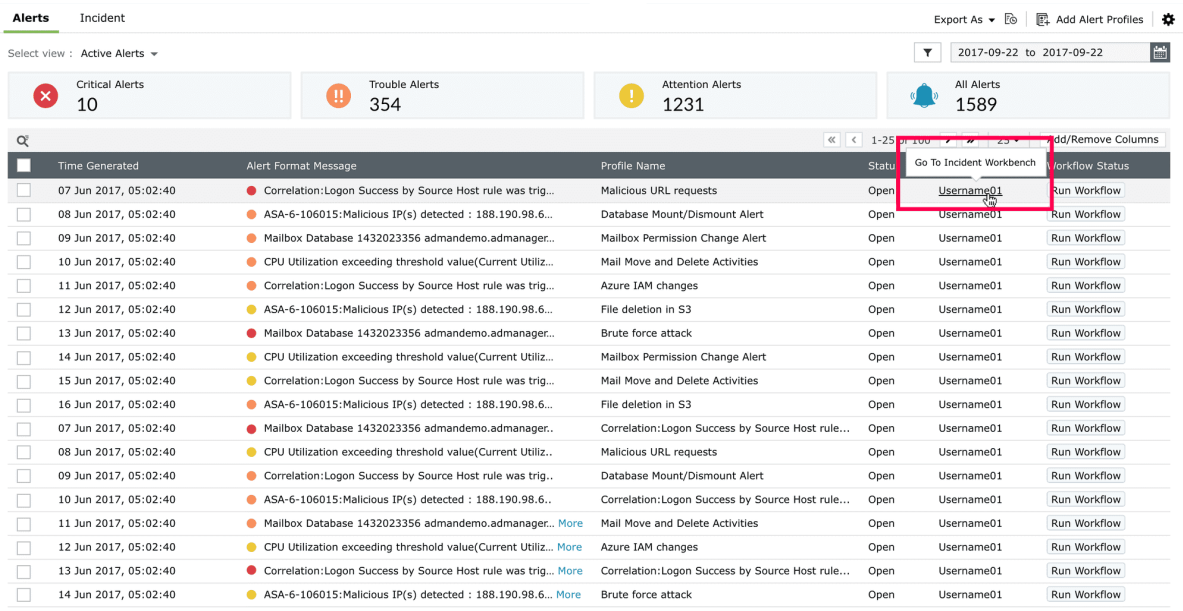


- From Log Search

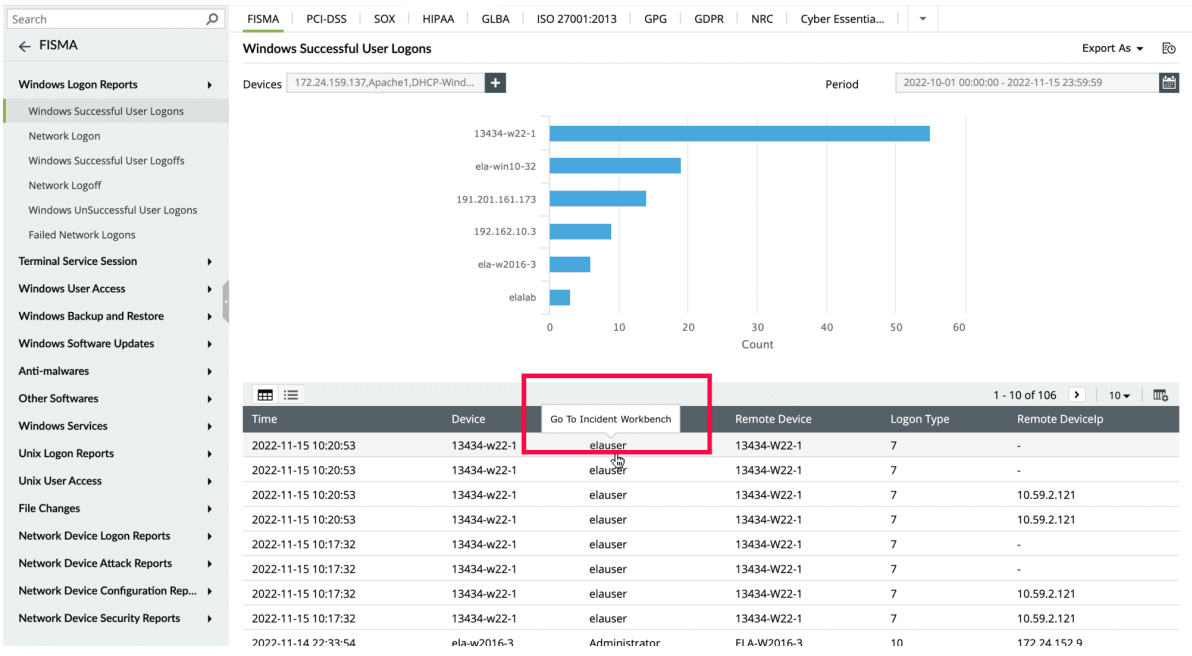




- From Alerts



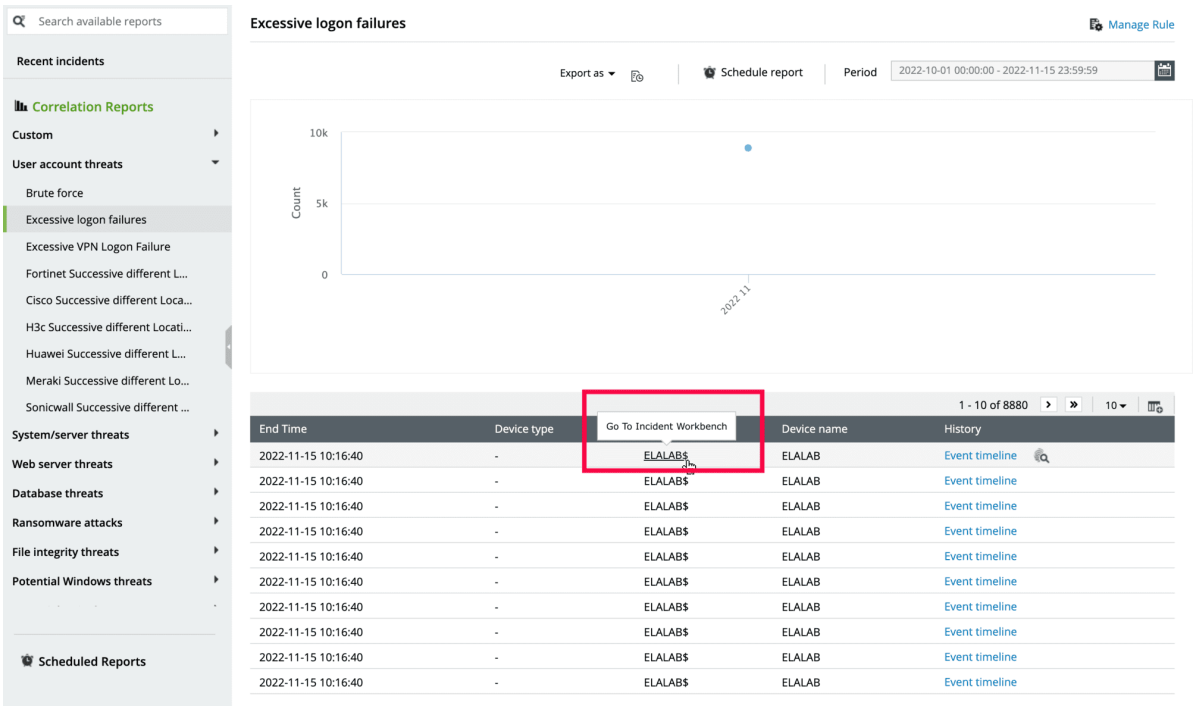
- From Compliance dashboard



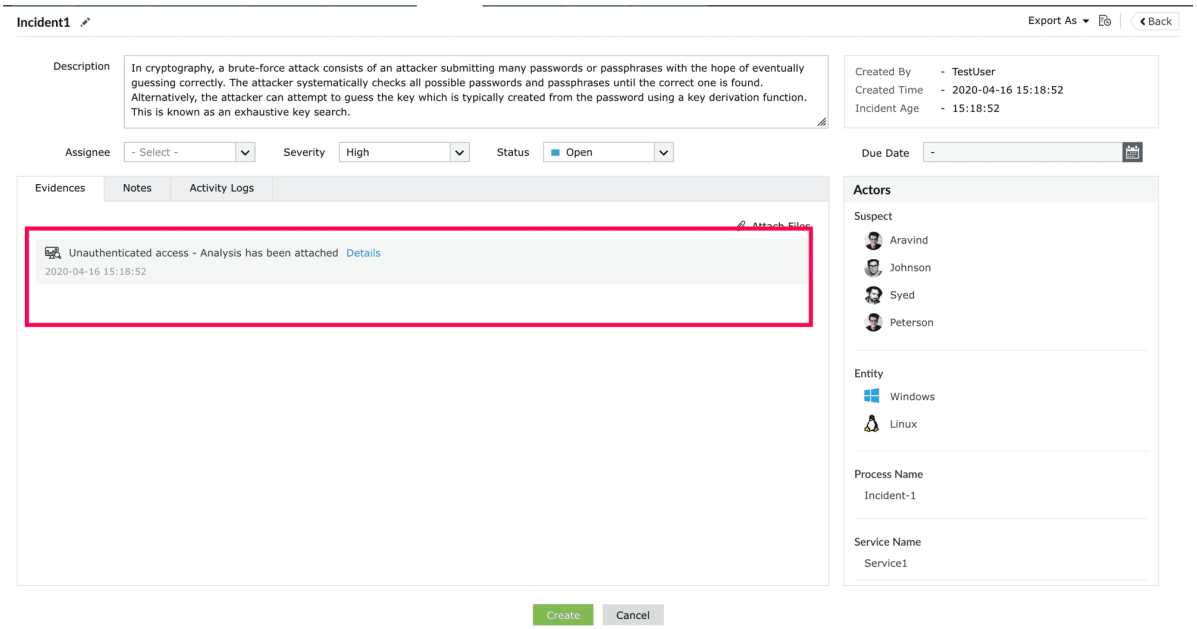


2022-11-14 22:33:32	ela-w2016-3	DWM-3	-	2	-

- From Correlation



- From Incident management console



> **Note**
>
> Minimize the tab to access Incident Workbench while you traverse through different pages in EventLog Analyzer. As long as you don't close the workbench, the analysis will be available even if you log out of EventLog Analyzer and login again. You can also save it to an existing incident or

create a new one.

10.2.3.3. User analytics in Incident Workbench

Last updated on: September 12, 2025

In this page

User Risk analysis

User Activity Overview

User Details

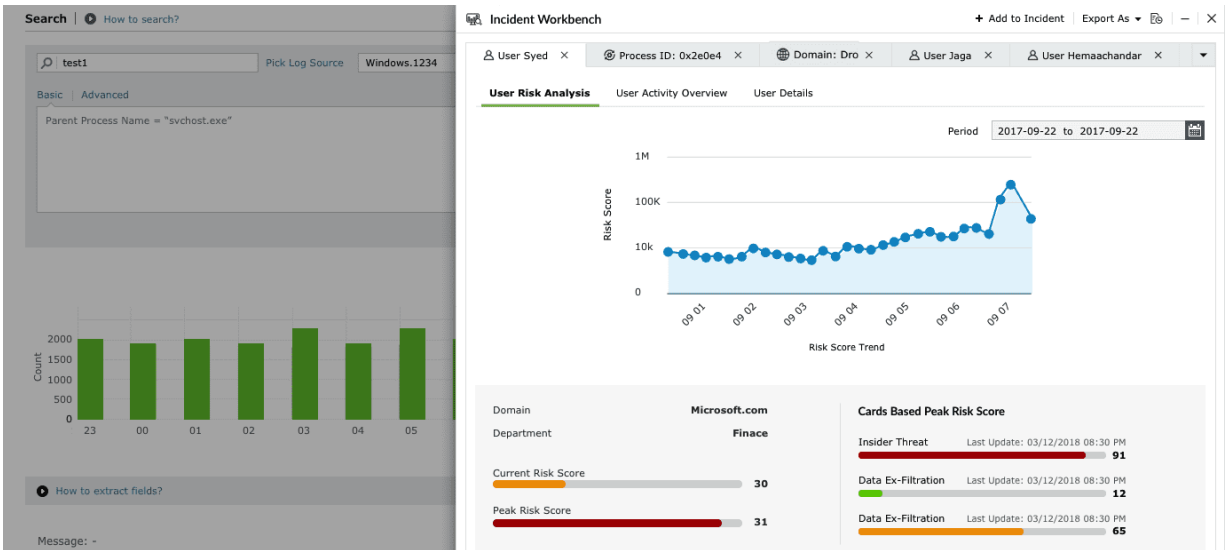
The user analytics data in Incident Workbench incorporates UEBA from the Log360 suite. It's necessary to purchase UEBA to get behaviour analytics and risk score trends of users.

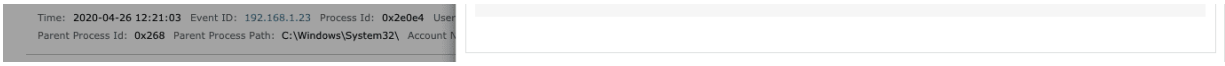
1. Please refer to the Incident Workbench Overview page to learn about the feature, and check the Access page to learn how to invoke Incident Workbench from different dashboards of EventLog Analyzer.
2. To get user analytics, you can click on any of the following fields that uniquely identify a user:
   - Username
   - Target User
   - VPN UserName
   - User Principal Name
   - Destination User
   - Sourceuser
   - Subject Username

The following data will be available in the user analytics section of the Incident Workbench:

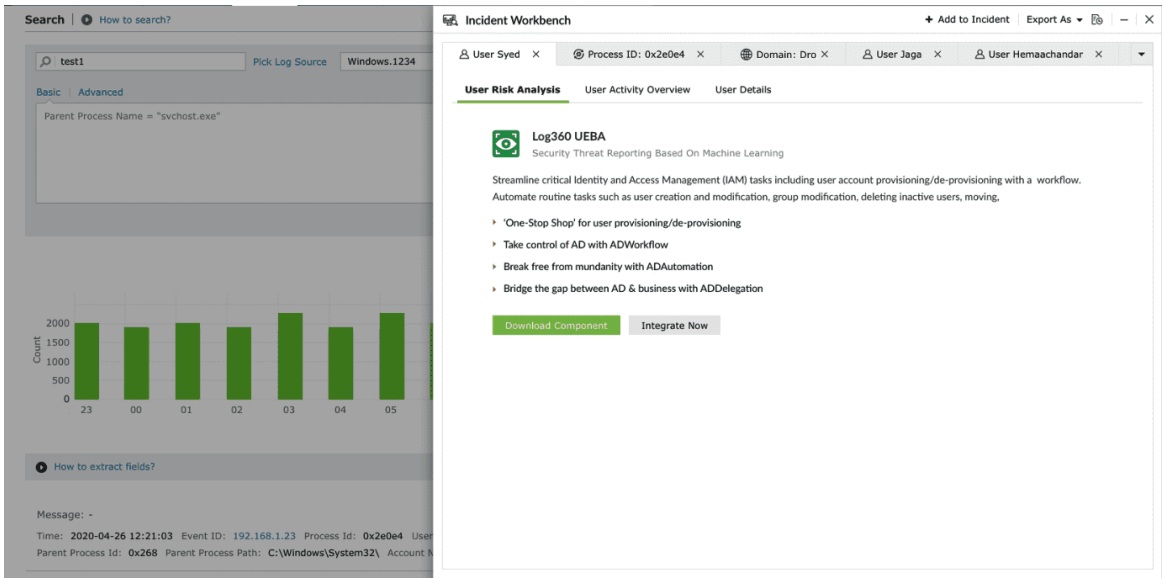
User Risk analysis

View the user's Risk Score Trend, Peak Risk Score and the Cards Based Peak Risk Score for possible insider threat and data exfiltration activities. Click on the Calendar icon and set the required period.

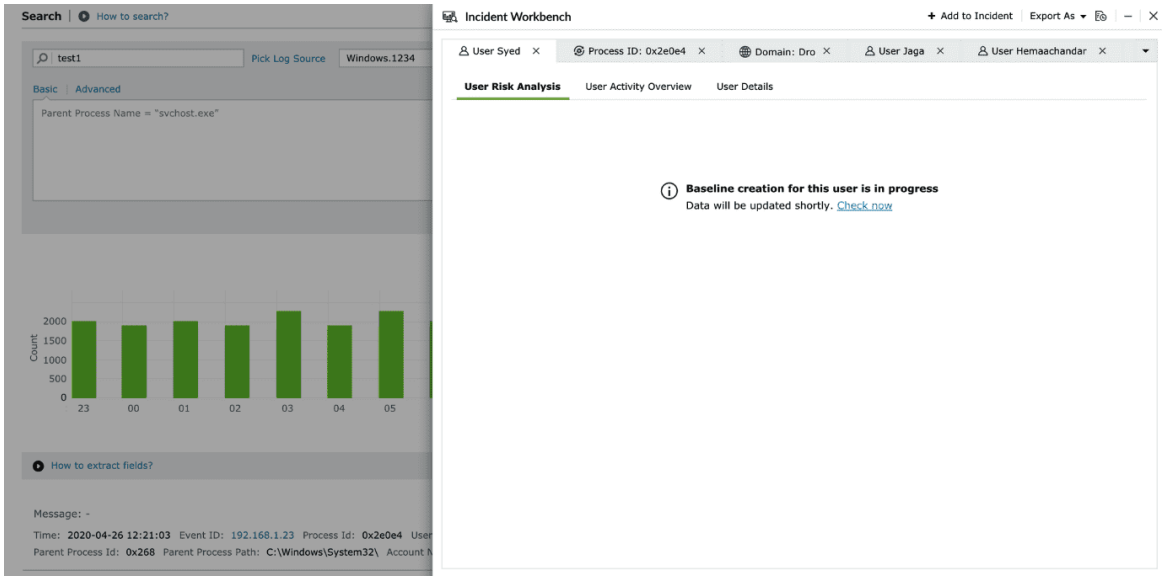




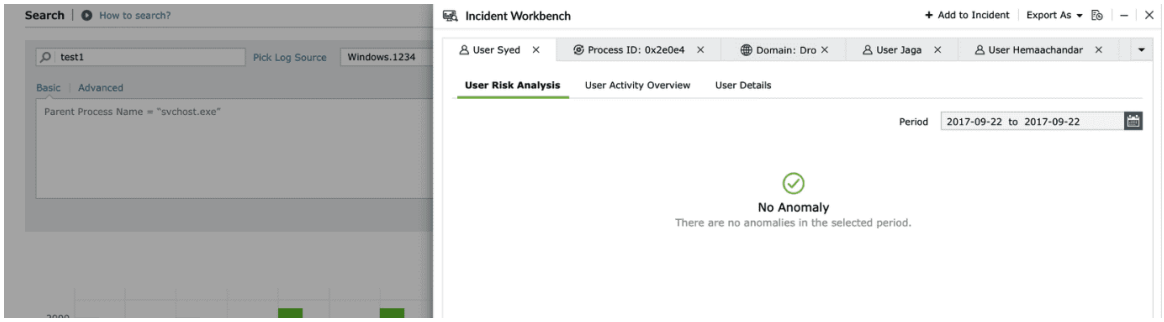
- Here are the possible messages that will be displayed in the User Risk Analysis section and the causes
  - Case 1: UEBA not purchased

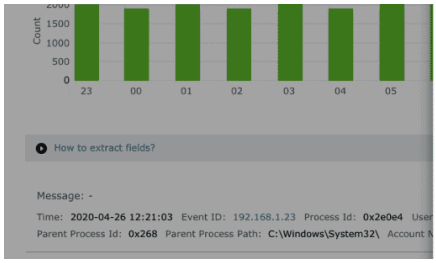


  - Case 2: Baseline creation is in progress as the model is training



  - Case 3: The particular user has no anomalies



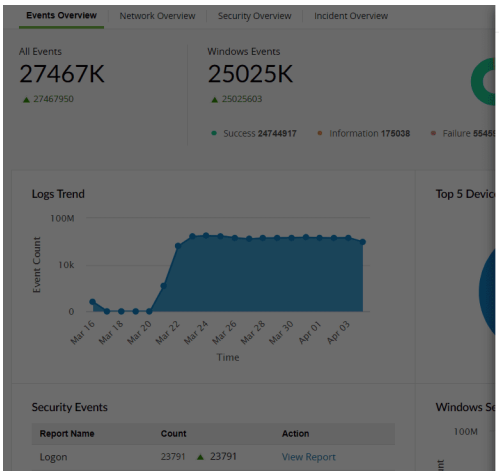


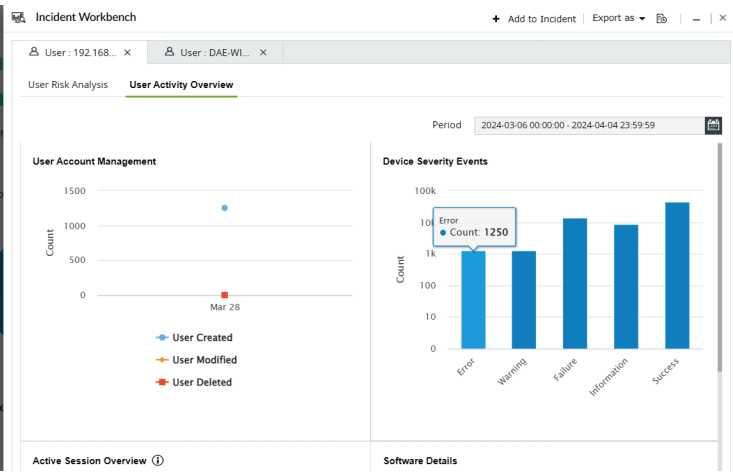
User Activity Overview

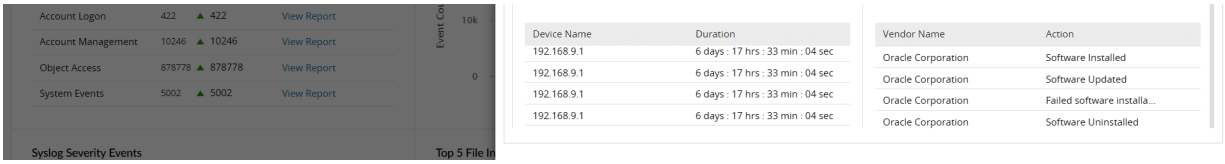
Note: The User Activity Overview section in the Incident Workbench does not require UEBA integration.

The User Activity Overview contains the following widgets:

User Account Management	Tracks create, modify, and delete actions related to the user account.
Device Severity Events	Consolidates the device severity events for the devices accessed by the user
Active Sessions Overview	Shows the list of active sessions on different devices and their duration
Software Installations and Updates	List of softwares installed, uninstalled and updated by the user during the selected period
Top 5 File Integrity Monitoring Events	Tracks events related to file creation, deletion, modification and access.
Process Tracking	Tracks process creation and termination activities





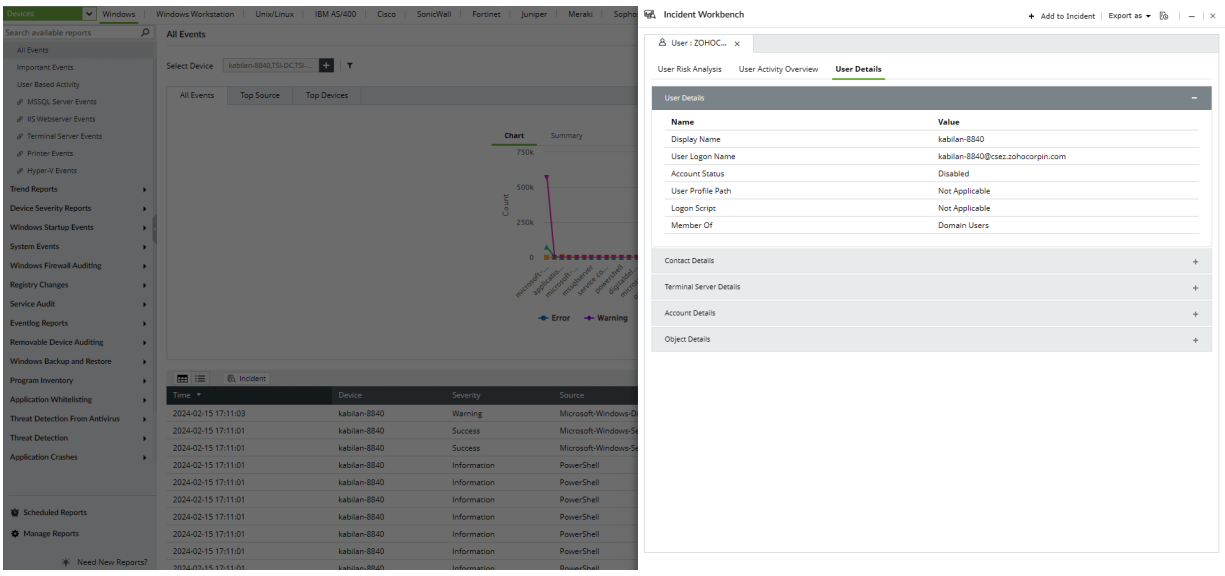


User Details

> **Note**
>
> The User Details section in the Incident Workbench doesn't require UEBA integration.

This sections fetches the Active Directory object details such as:

- User Details
- Contact Details
- Terminal Server Details
- Account Details and
- Object Details



> **Note:**
>
> Minimize the tab to access the Incident Workbench while you traverse through different pages in EventLog Analyzer. As long as you don't close the workbench, the analysis will be available even if you log out of EventLog Analyzer and login again. You can also save it to an existing incident or create a new one.

10.2.3.4. Process analytics in Incident Workbench

Last updated on: September 12, 2025

In this page

Process Analytics Views

Process Analytics Elements

The Process Analytics section of the Incident Workbench showcases process spawning with the parent child relationships and the process event details.

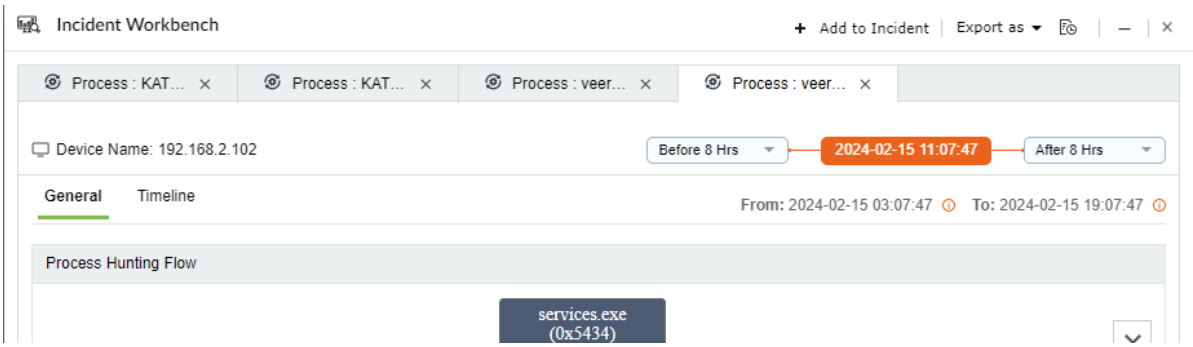
Note

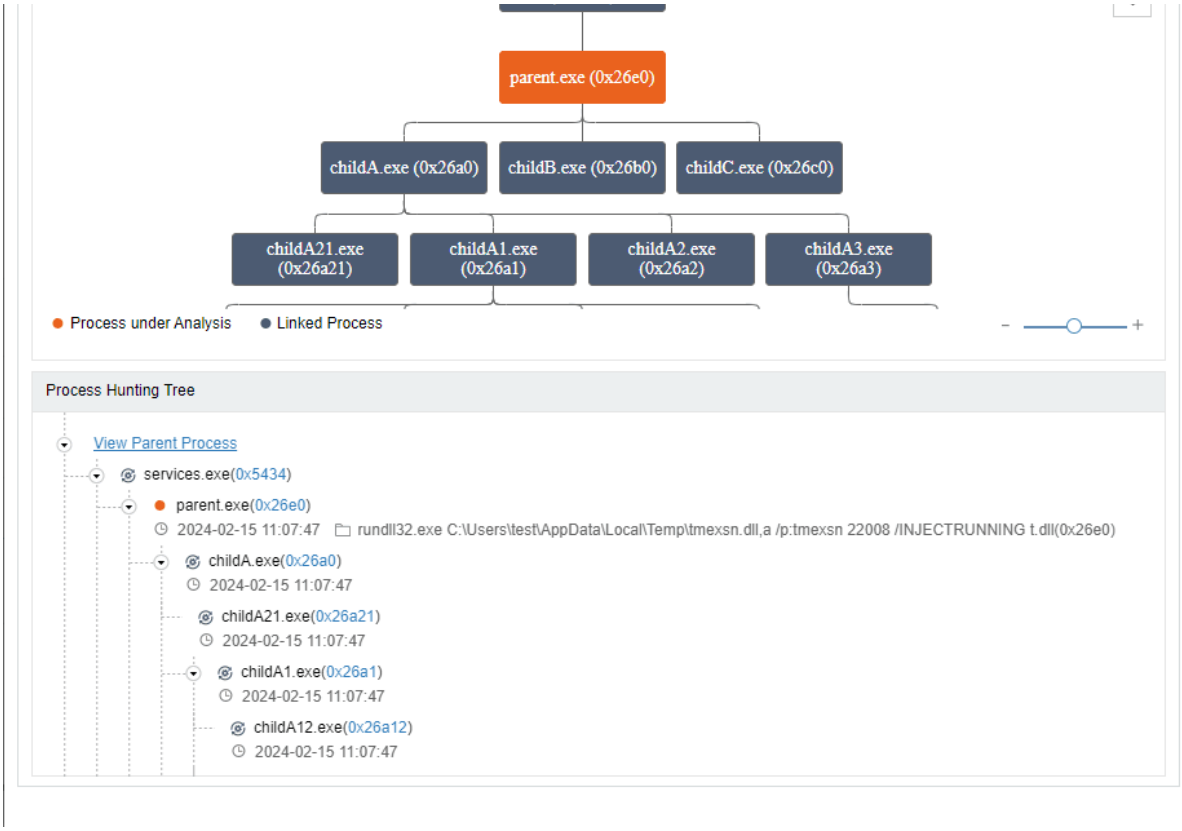
1. Please refer to the Incident Workbench Overview page to learn about the feature, and check the Access page to learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer.
2. To access the process hunting tree, you can click on any of the following fields that uniquely identify a process:
   - Process Id
   - Parent Process ID
   - Process GUID
   - Parent Process GUID
   - Process Name
   - Parent Process Name
3. The process spawning will be available in graphical format for upto 50 child processes.

Process analytics views

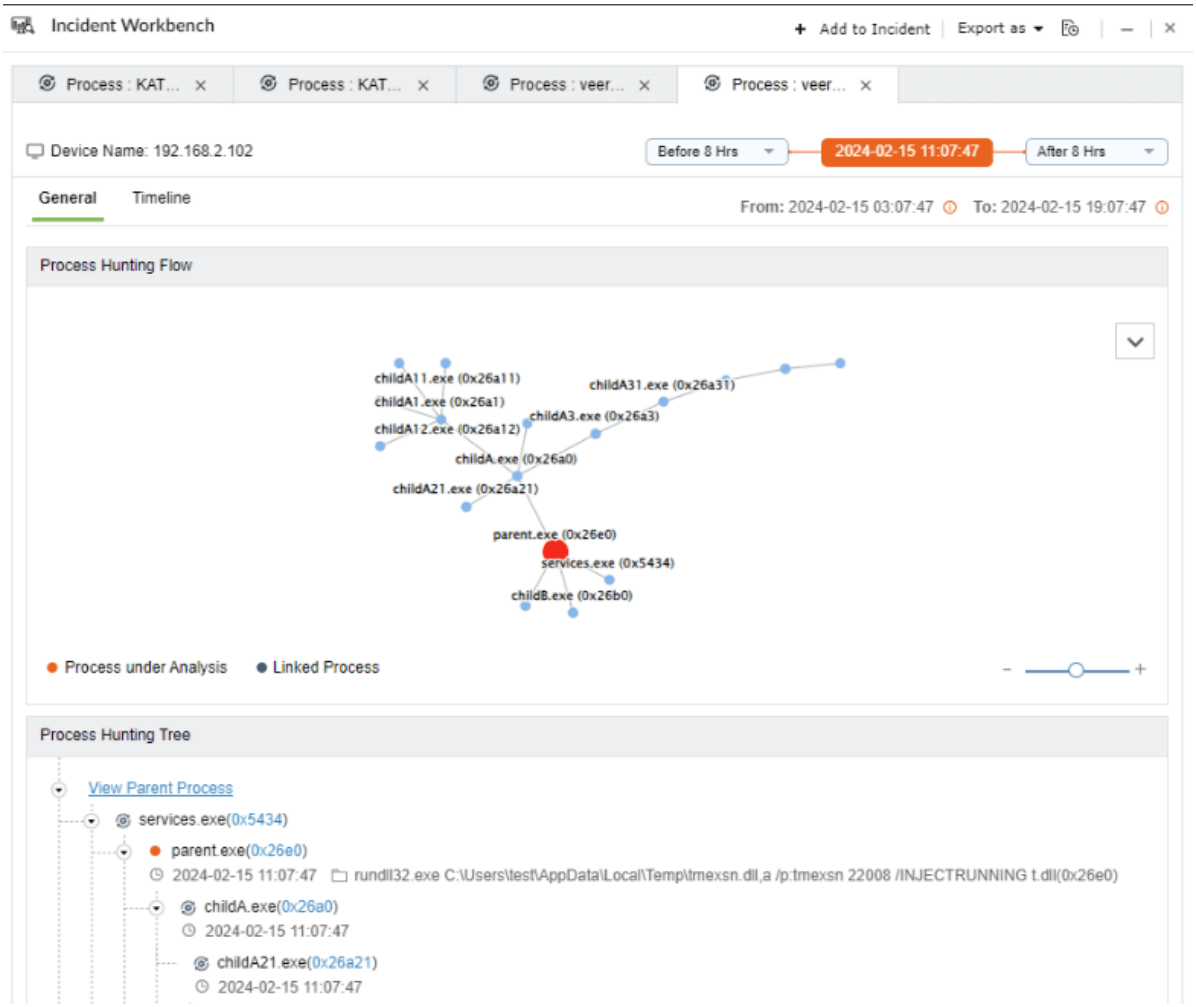
Here are the different graphical formats available in Incident Workbench to analyze process flow:

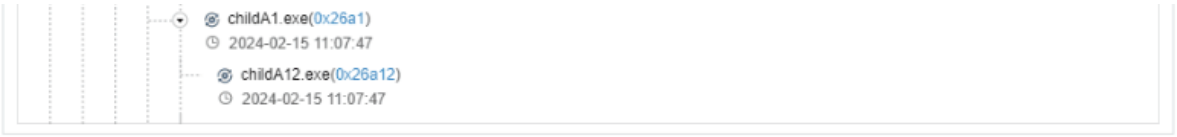
- Hierarchical tree with respective parent and children of the process



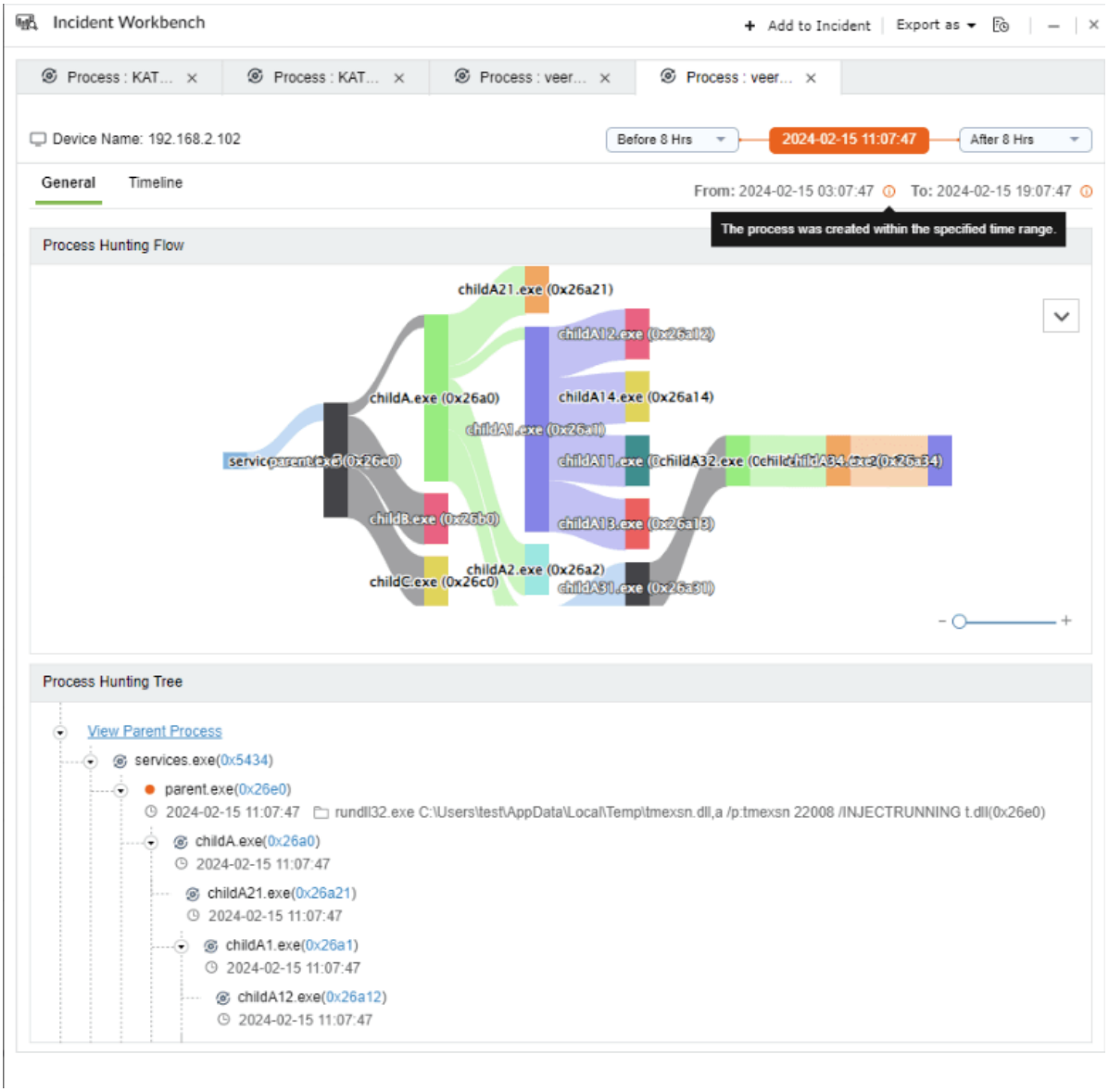


- Process cluster view



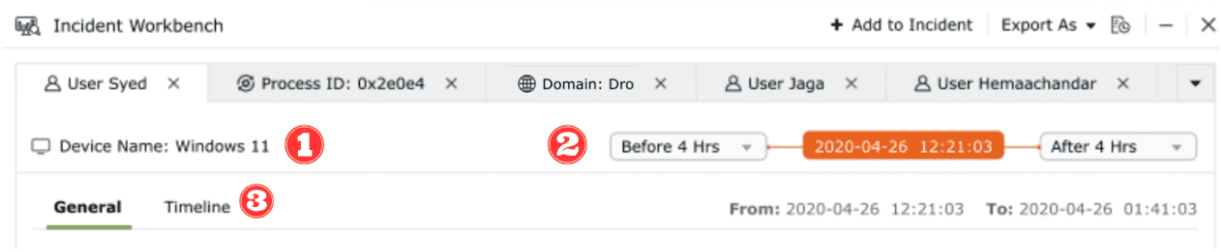


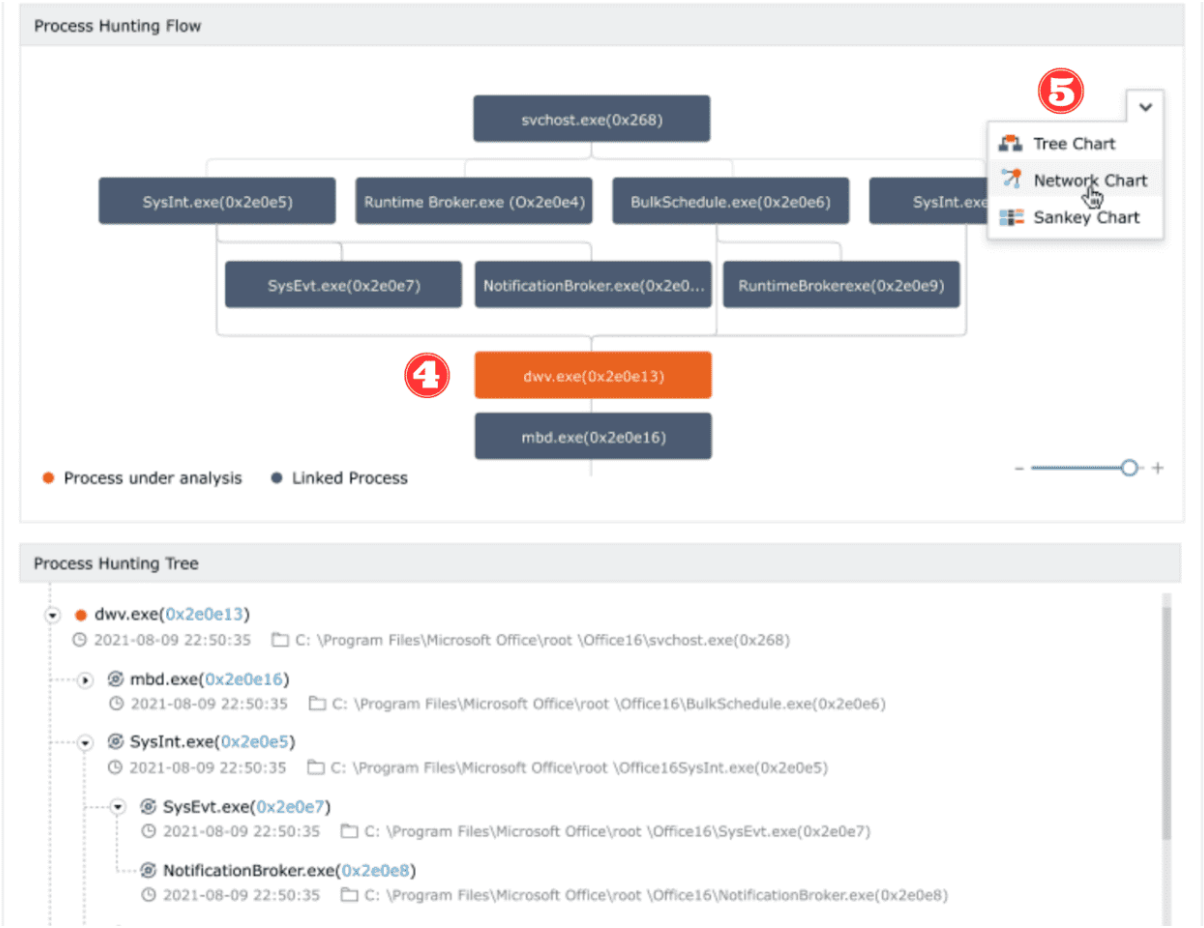
- Sankey Chart view with the process flow



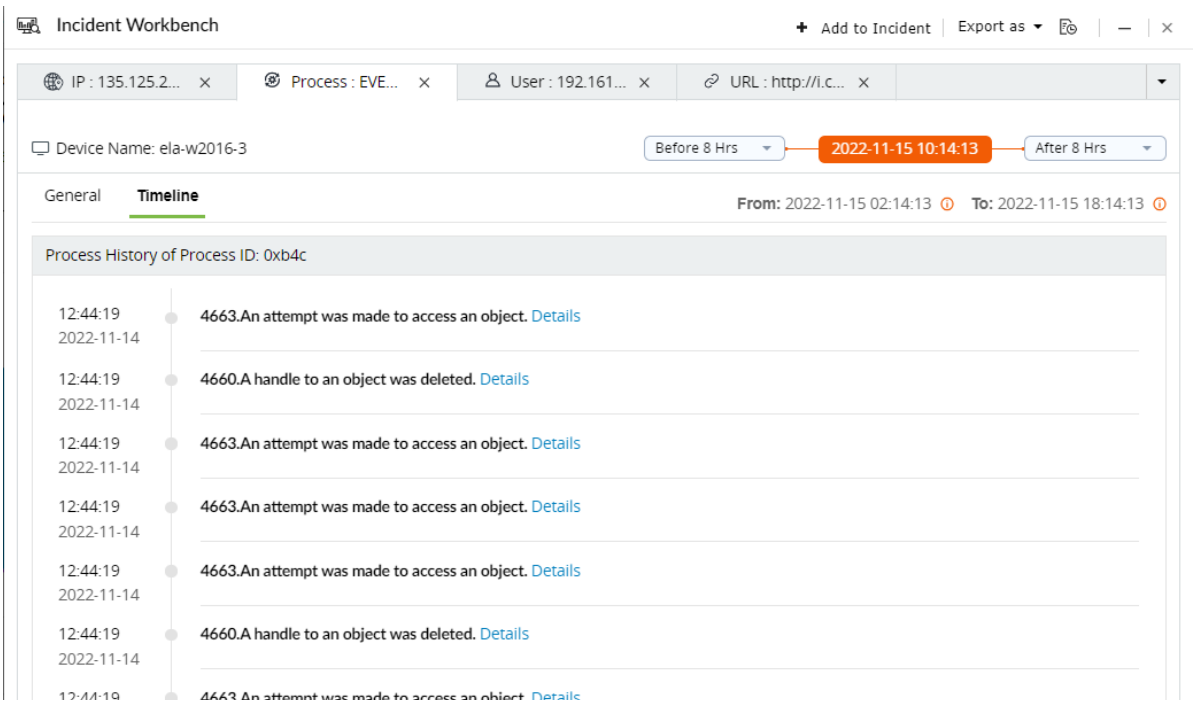
The process analytics tab explained.

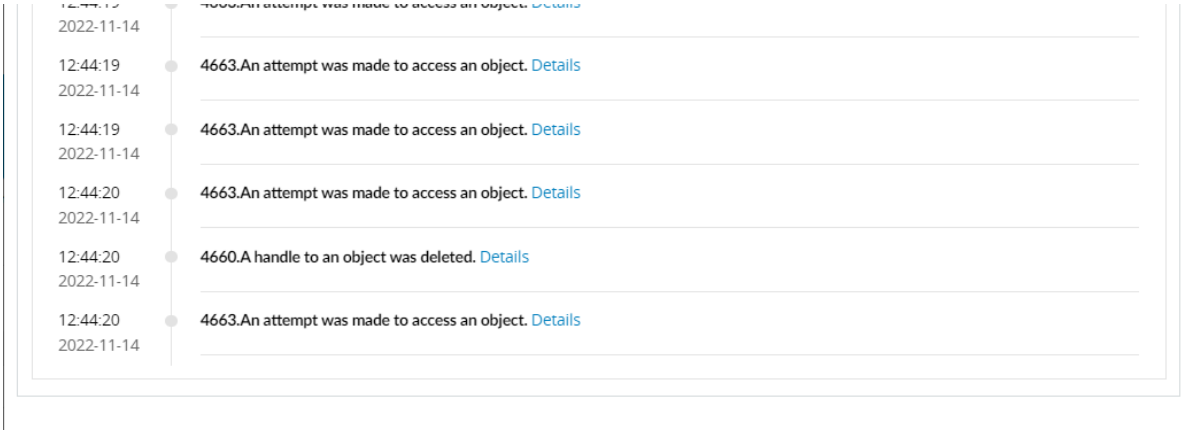
Process Analytics - Elements





1. Device Name: The device in which the process is active for the selected period.
2. Timeline adjuster: Use the timeline adjuster in the top right corner to view the process activities upto 8 hours prior to and after the selected event.
3. Views: Alternate between the General view and Timeline view. The General view has the graphical presentation of the process flow, and the Timeline view has the process history with list of events.





4. Highlighted process: The Process being analyzed currently will be highlighted in orange and the rest of the linked processes will be in a different color.
5. Graphical formats: Select the dropdown button next to the process tree to alternate between different graphical formats

> **Note**
>
> Minimize the tab to access the Incident Workbench while you traverse through different pages in EventLog Analyzer. As long as you don't close the workbench, the analysis will be available even if you log out of EventLog Analyzer and login again. You can also save it to an existing incident or create a new one.

10.2.3.5. Advanced Threat Analytics in Incident Workbench

Last updated on: September 12, 2025

In this page

Log360 Cloud Threat Analytics

Dark Web Monitoring

VirusTotal

Note

1. Please refer to the Incident Workbench Overview page to learn about the feature, and check the Access page to learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer.
2. To access Advanced Threat Analytics data, you can click on any of the following fields that uniquely identify the external sources:

Domain analysis:

- Domain
- Canonical Name
- Client Domain
- URL Site

IP Analysis:

- Remote DeviceIp
- Source IP
- Client IP Address
- Server IP Address
- Address
- Destination IP
- Device Ip
- Remote Ip
- Source Host Address
- NAT Source Address
- NAT Destination Address
- Destination IP
- Original Client IP
- IP Address

- Endpoint IP
- Private Ip
- Target Ip
- Source Device
- Target Machine
- Destination Host Address
- Target Device

URL Analysis:

- Payload URL
- Object Url
- URL

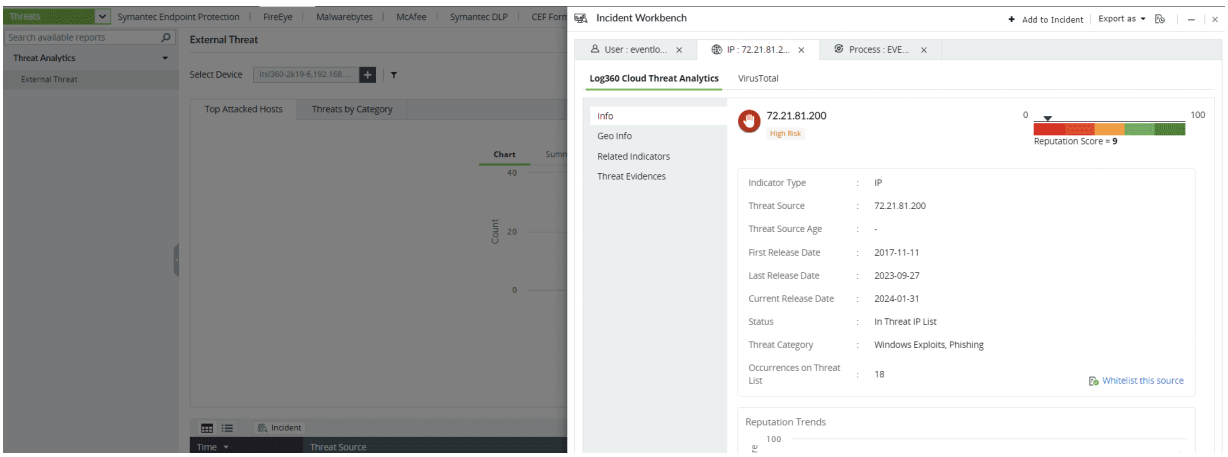
EventLog Analyzer supports the following vendors for the Advanced Threat Analytics in Incident Workbench:

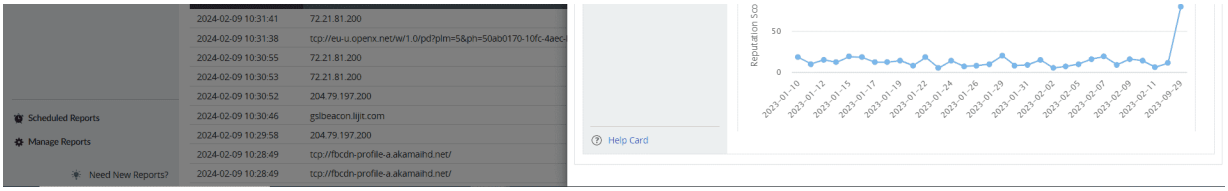
- Log360 Cloud Threat Analytics
- Dark Web Monitoring
- VirusTotal

Log360 Cloud Threat Analytics

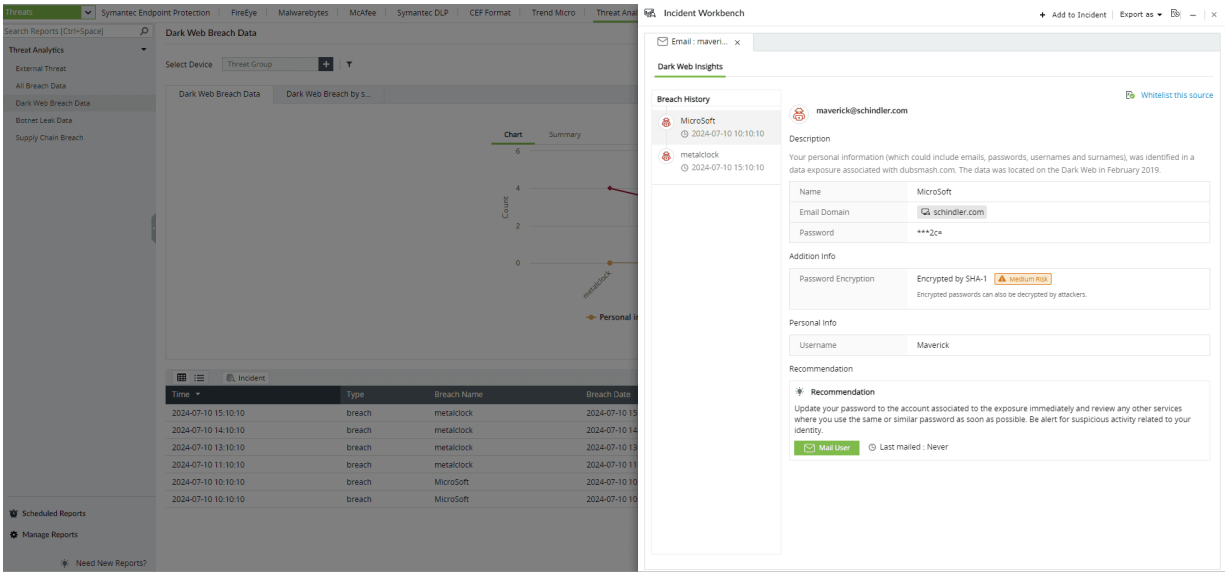
This is the default integration from Log360Cloud suite, and can be accessed once the Advanced Threat Analytics add-on from EventLog Analyzer is purchased.

> Note:
>
> Check out the Advanced Threat Analytics page to learn about the configuration and analysis.





Dark Web Monitoring

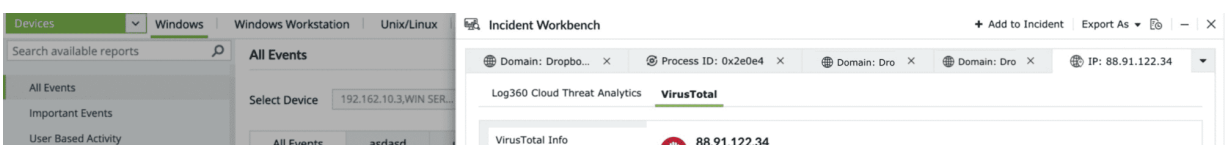


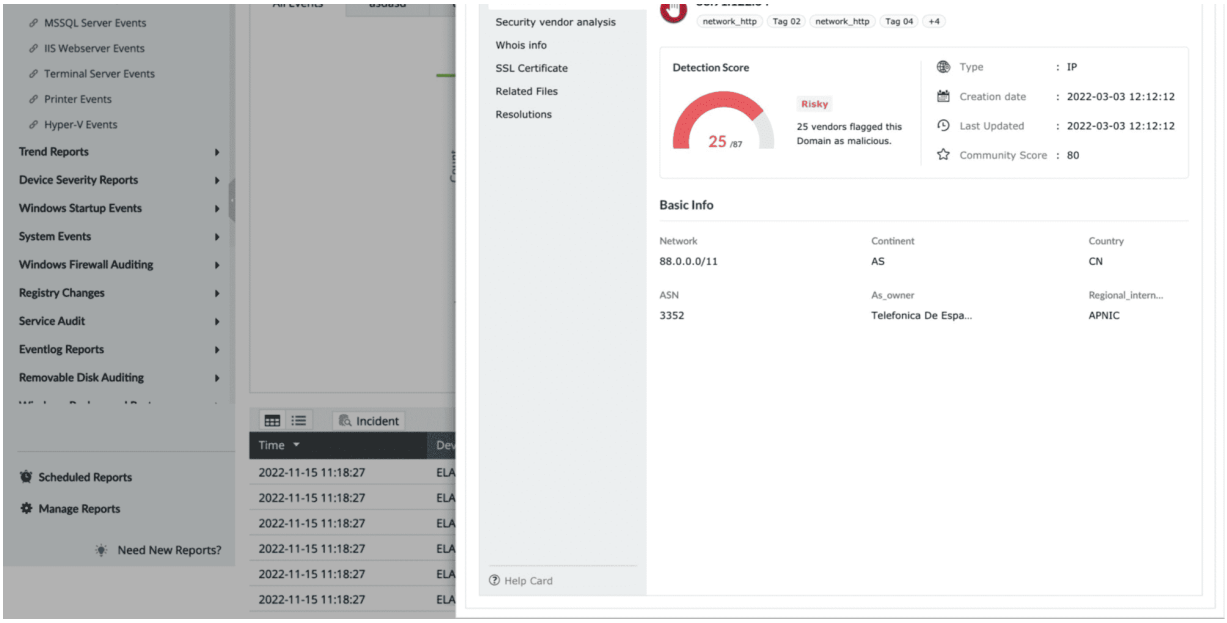
When you purchase Advanced Threat Analytics, you also gain access to Dark Web monitoring. You can use your domain to enable Dark Web monitoring. This feature actively scans for any compromise of user data on the Dark Web and sends alerts. Compromised data can include credentials, credit card information, and more. With this information, the security analyst can gain insight into the depth of the breach and the type of information that has been breached.

VirusTotal

This is a third-party threat feed integration, and follows the Bring Your Own Key (BYOK) model. If you have purchased VirusTotal access separately or if you own a public API key for free, you can use your the key and get the threat analytics information in EventLog Analyzer.

> Note:
>
> Check out the Advanced Threat Analytics page to learn about the configuration and analysis.





Note

Minimize the tab to access the Incident Workbench while you traverse through different pages in EventLog Analyzer. As long as you don't close the workbench, the analysis will be available even if you log out of EventLog Analyzer and login again. You can also save it to an existing incident or create a new one.

10.2.3.6. Incident building using the Incident Workbench

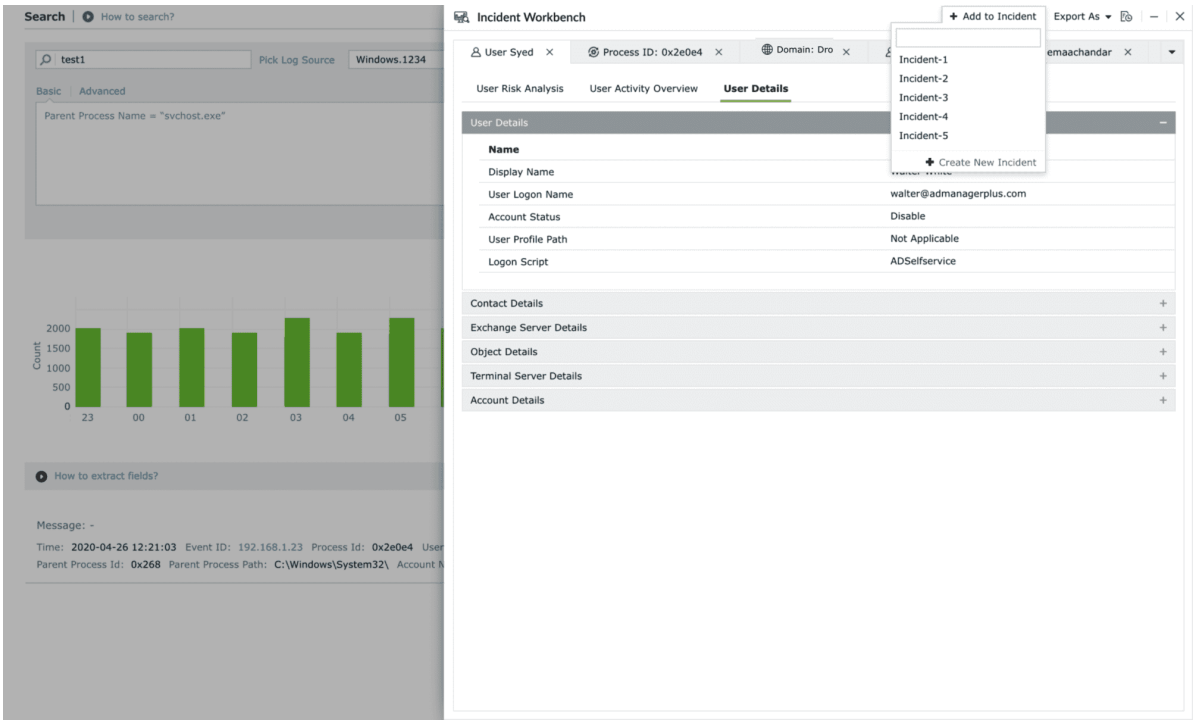
Last updated on: September 12, 2025

This page explains about building incidents using the instances of the Incident Workbench.

> **Note**
>
> 1. Please refer to the Incident Workbench Overview page to learn about the feature, and check the Access page to learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer
> 2. You can add upto 20 analysis tabs in a single instance of the Incident Workbench. If you want to analyze more entities you will have to close the current instance, and open a new one.

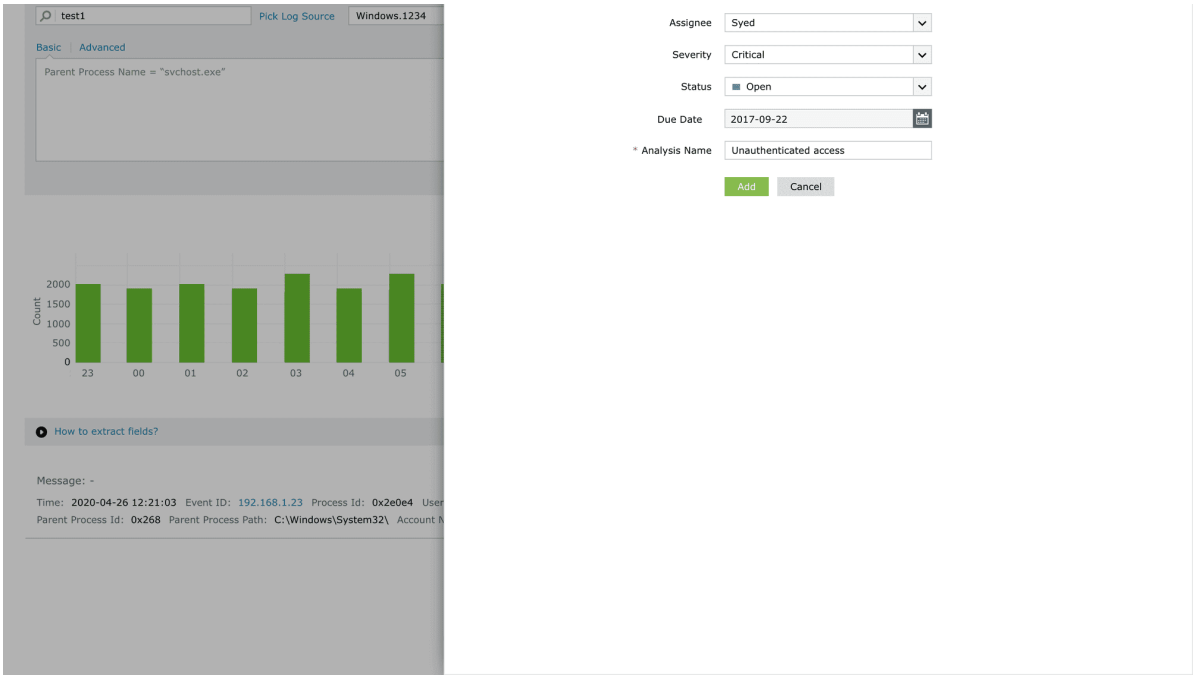
Steps to add the Incident Workbench instance to Incidents as evidence:

1. Click on Add to Incident in the top right corner of the Incident Workbench to save the instance.

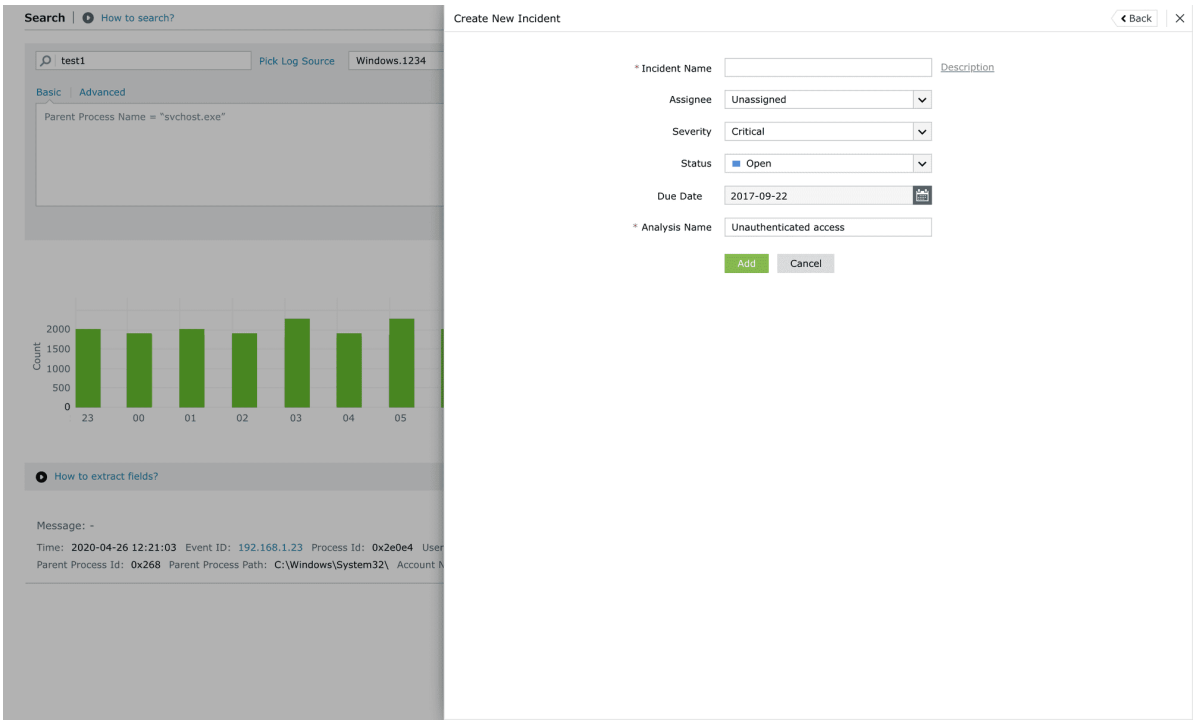


2. The dropdown contains the list of existing incidents. Use the search bar to find specifc incidents and add the Incident Workbench instance.
3. Once you select the incident, the following page will appear. Assign a person to handle the incident, add severity and status, and set the deadline to resolve the incident.

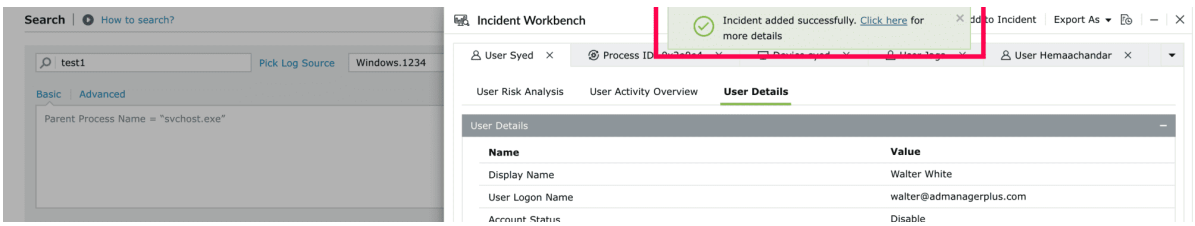


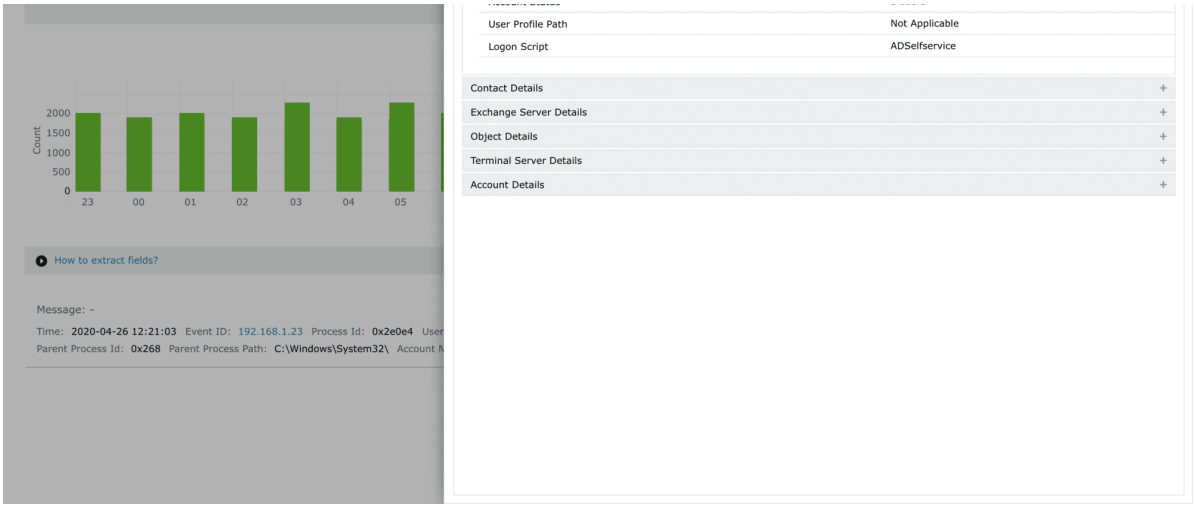


4. To create a new incident and add the instance, click on the Create New Incident button in the dropdown. You need to add the additional details of the Incident Name, and Description in the corresponding page.

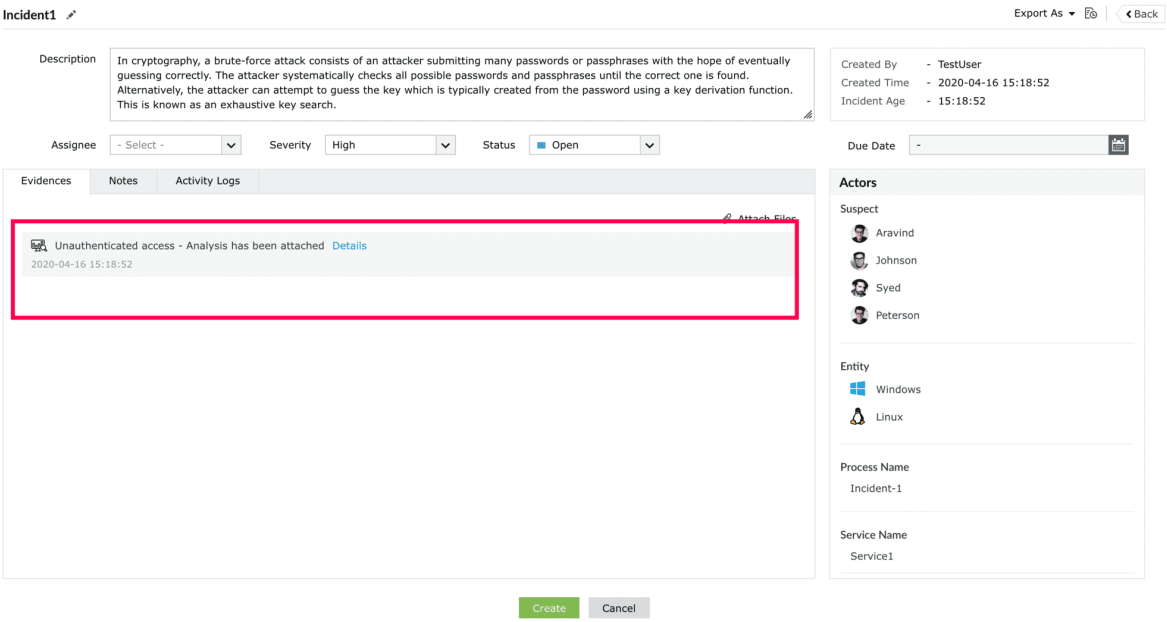


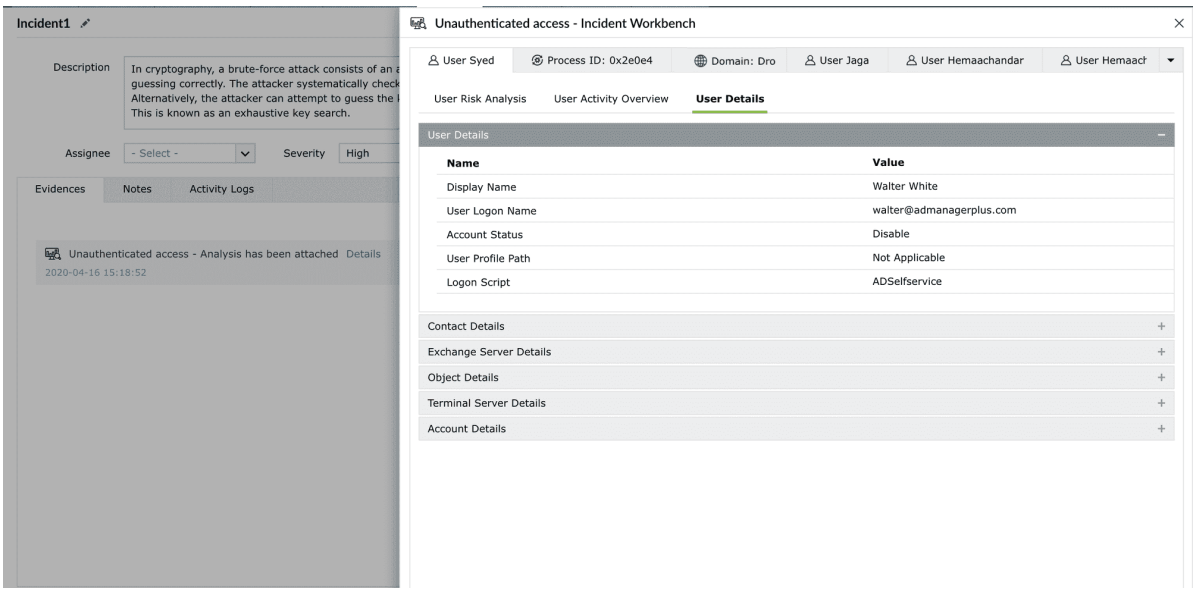
5. Once the instance has been saved, you'll get the success message notification. The Click here link in the notification will lead you to the incident management console.





6. Head to Alerts tab → Incident to view the list of incidents. Incident Workbench analysis are stored under the Evidences section in the incident management console. Click on Details to view the specific analysis.





Use the Incident Management help document to learn more about creating, accessing and managing incidents.

> **Note**
>
> Minimize the tab to access the Incident Workbench while you traverse through different pages in EventLog Analyzer. As long as you don't close the workbench, the analysis will be available even if you log out of EventLog Analyzer and login again.

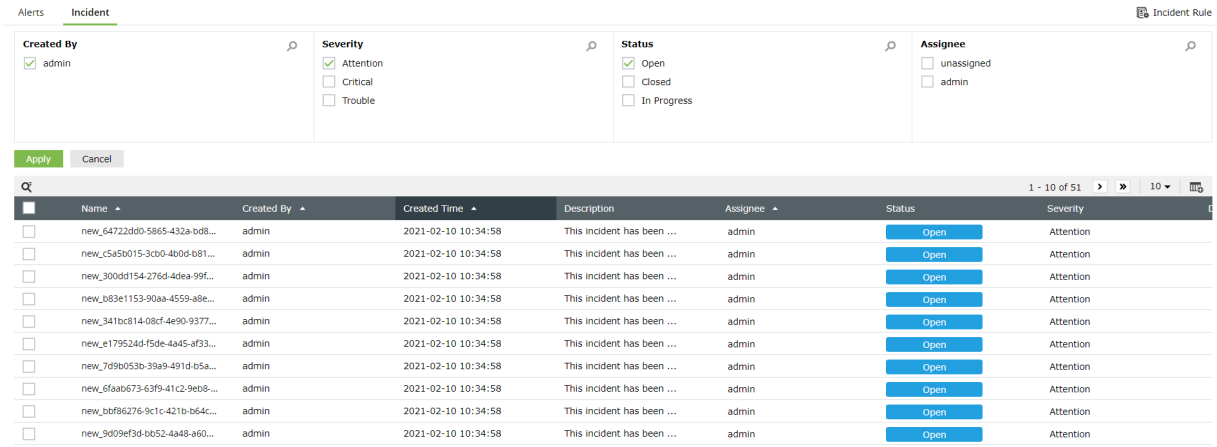
10.3.1.1. Incident management

Last updated on: September 12, 2025

EventLog Analyzer helps you streamline the process of managing and investigating security incidents.. You can track the status of security incidents by navigating to the Alerts tab → Incident.

Viewing and editing incidents

In the Incident page, you can view the list of all incidents in your network along with crucial information such as the assignee, status, and severity. You can click on any incident to view and edit the incident's name, description, assignee, status, and severity. The Evidence and Notes tab display the list of evidence and notes attached to an incident. The Activity Logs page records and displays the events pertaining to the creation, modification, and deletion of incidents.
The incident page displays details such as the age of the incident, who created it, and when it was created. The Actors widget contains the list of users, entities, services, and processes responsible for the incident to help the assignee quickly investigate the incident and take remedial action.

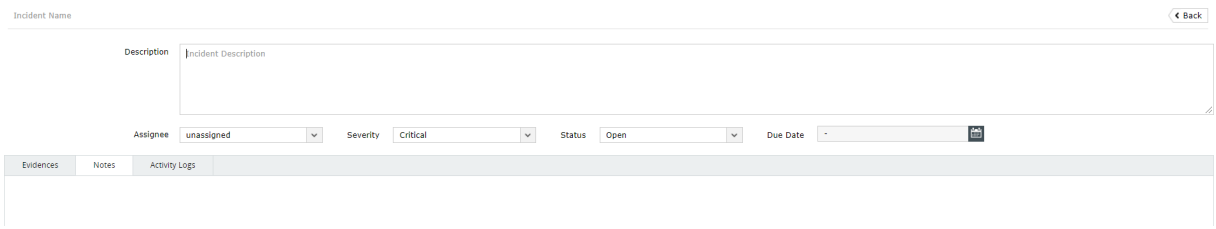


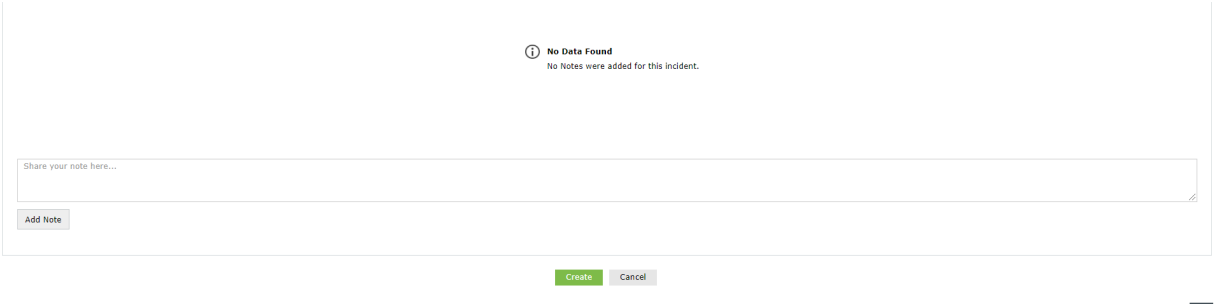
Steps to create an incident

You can create an incident in EventLog Analyzer by navigating to the Alerts tab → Incident → +Add Incident.

- In the Incident page, enter a name and description for your incident in the respective fields.
- Select the assignee, severity, and status of your incident from the respective drop-down menus.
- Click on Create.

You can view the incident creation event being logged in the Activity Logs pane.





Additionally, you can create incidents in EventLog Analyzer by:

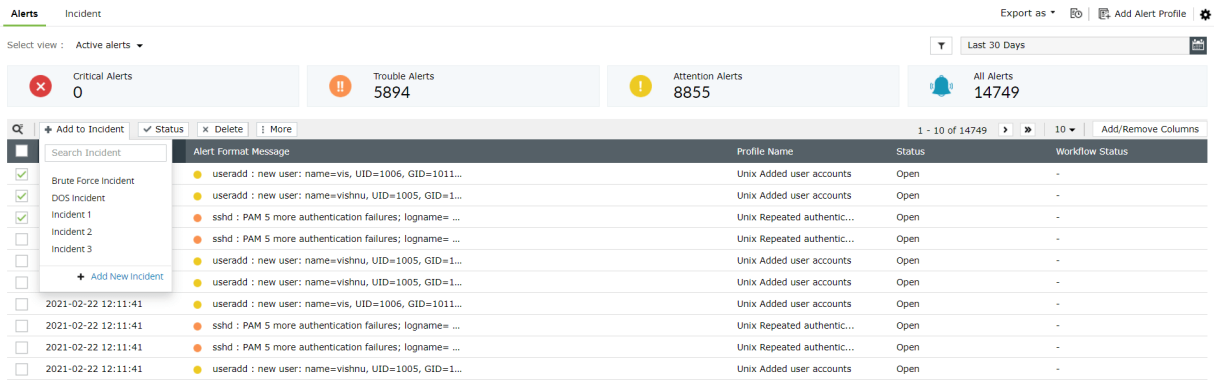
- Mapping alerts as incidents
- Mapping search results as incidents
- Mapping reports as incidents
- Automating incident creation by configuring incident rules

Steps to map alerts as incidents

In EventLog Analyzer, you can map a triggered alert as an incident, assign a security technician to respond to the incident, and track its status by following the steps given below:

- Navigate to the Alerts tab.
- Select the alert for which you want to create an incident.
- Click on the +Add to Incident button present at the top of the alerts table and click on the +Add New Incident option to create a new incident.
- Enter the name and description of the incident.
- Select the assignee, status, and severity of the incident from the respective drop-down menus.
- Click on Create.

You can also add an alert as evidence to an incident by selecting the alert, clicking on the +Add to Incident button, and selecting the required incident from the list displayed. The alert can now be viewed under the Evidence tab of the selected incident.



Steps to map search results as incidents

EventLog Analyzer allows you to map search results as incidents to help you backtrack an attack and conduct root cause analysis by following the steps given below:

- Navigate to the Search tab and execute the required search query.
- In the search results pane, click on the Incident button.
- Now, select the search result(s) you want to add to an incident.
- Click the +Add to Incident button and choose the incident to which you want to add the search result(s).
- Alternatively, you can also create a new incident to map the selected search results by clicking the +Add New Incident link.
- If you're creating a new incident, enter a name and description for the incident. Select the assignee, status, and severity from the respective drop-down menus.
- Click Create.

You can now view the search results added as evidence under the Evidence tab of the incident.



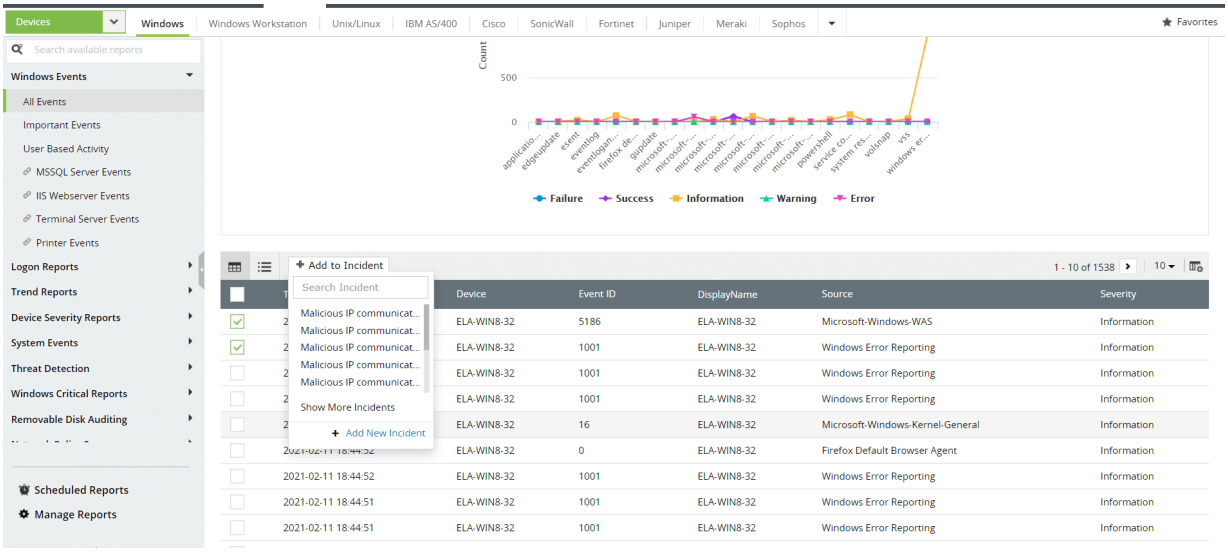
Steps to map reports as incidents

If anomalies are detected in a report, you can further investigate the deviant events specified in the report by mapping those events as incidents and thoroughly examining them by assigning a dedicated IT security professional. You can map reported events as incidents by following the steps given below:

- Navigate to the Reports tab and click the report you want to add as an incident.
- Click the Incident button and select the events of interest.
- Click the +Add to Incident button and select the name of the incident to which you want to add the selected events.
- Alternatively, you can also create a new incident by clicking the +Add New Incident link.
- If you're creating a new incident, enter a name and description for the incident. Select the assignee, status, and severity from the respective drop-down menus.

- Click Create.

You can now view the events of the report listed under the Evidence tab of the selected incidents.



Configuring incident rules

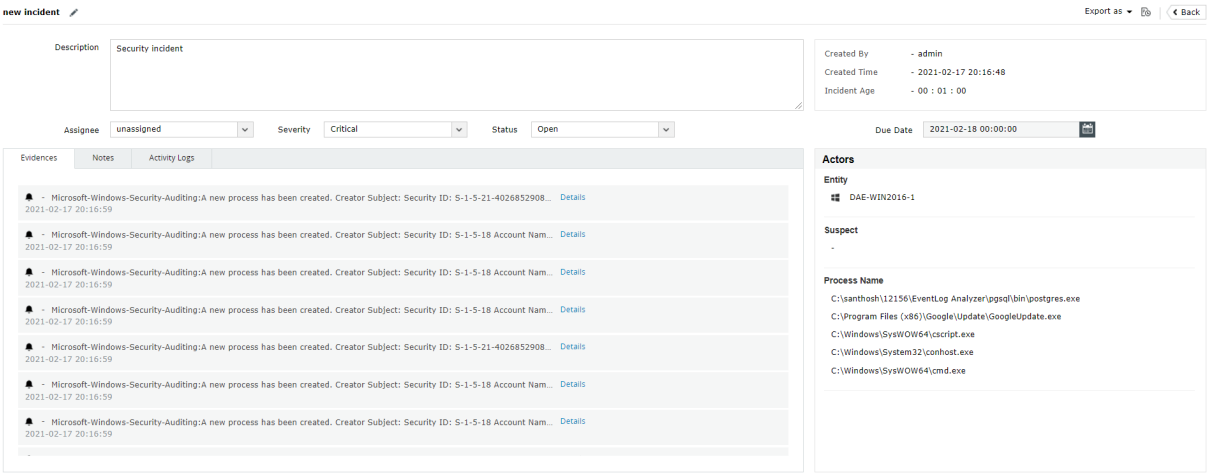
You can configure pre-defined incident rules for devices, device groups, and alert profiles to automatically create incidents when a specific number of alerts get triggered within a specified time span.

Steps to create an incident rule

- Navigate to the Alerts tab → Incident → Incident Rule → +Add Incident Rule.
- Enter a name and description for your incident rule.
- Assign the incidents created by this rule to a technician by selecting a name from the Assign To drop-down menu.
- Select the severity: Attention, Critical, or Trouble from the Severity field.
- Enter the threshold value to create the incident. An incident will be created when the specified number of alerts get triggered within the time frame.
- In the Criteria field, specify the Device, Device Group, or Alert Profile for which you want to create an incident. You can also create a criteria with multiple fields by clicking on the + icon to add another field and combine them using AND and OR logical operators.
- Click on Save.



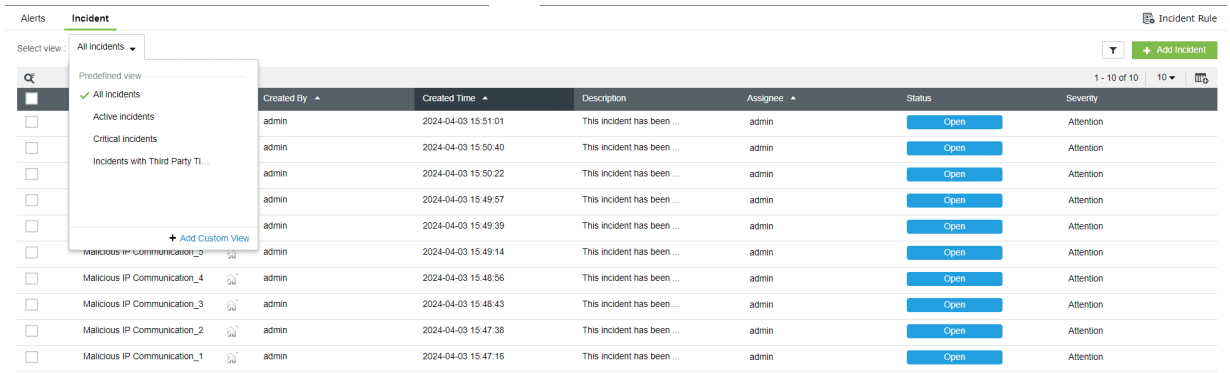
You can click on the Incident name to edit the name, description, assignee, severity, and status of the incident. You can view the Evidence, Notes, Activity Logs, and Actors of the incident. Additionally, you can also view who created the incident, when it was created, and the age of the incident in this page.



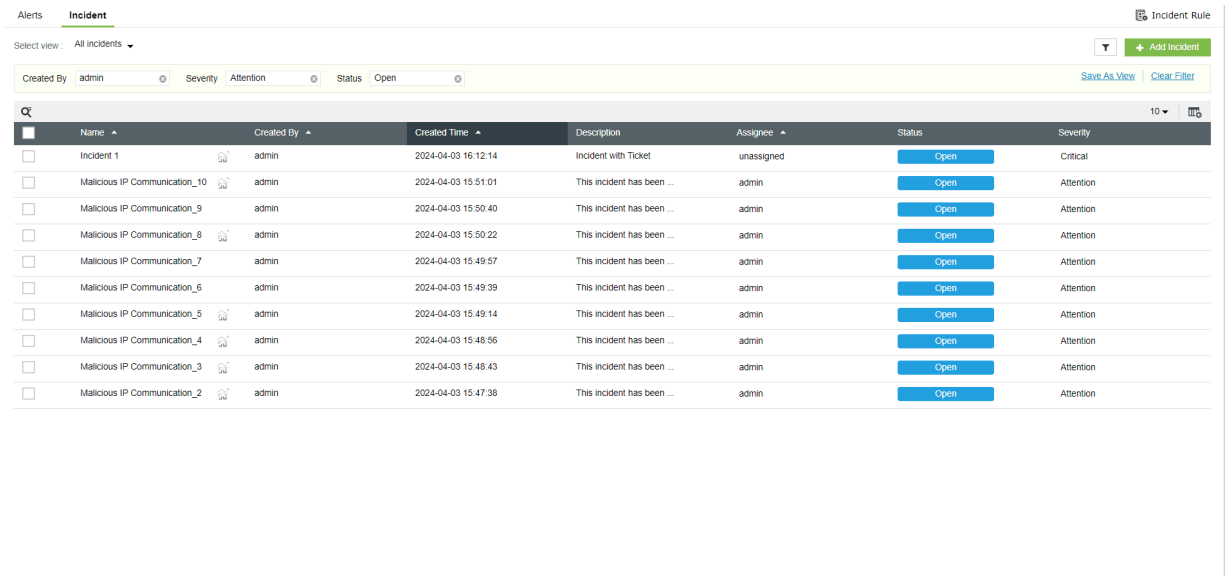
Note: You can create up to 10 incident rules in your EventLog Analyzer instance. The solution is capable of triggering up to fifty incidents per incident rule in a day.

Creating Incident views

You can view the incidents under various categories, such as All incidents, Active incidents, Critical incidents, and Incident with third-party ticketing tool by selecting the required view from the Select View drop-down menu. You can also create custom views by configuring a filter for the type of incidents you want to view.

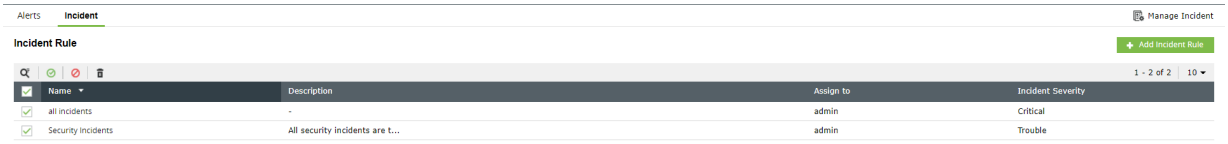


Apply the filter and click the Save as View link to enter a name for the view and click Save. Custom views are personal to the users who created them and can be viewed only by them. You can edit and delete the custom view by hovering your mouse pointer over the created view in the Select View drop-down menu.



Viewing and editing incident rules

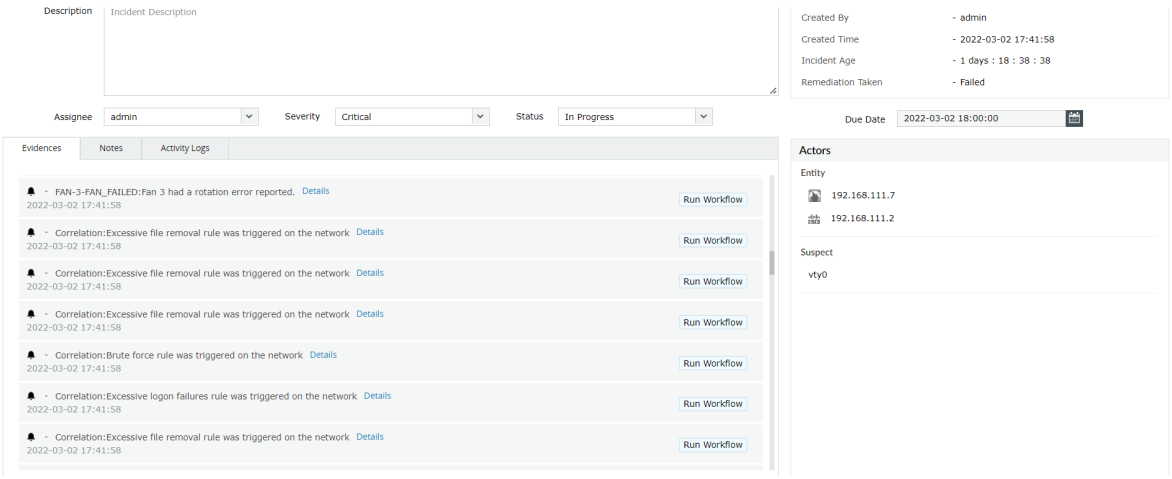
In the Incident Rule page, you can select incidents to enable, disable, and delete them.



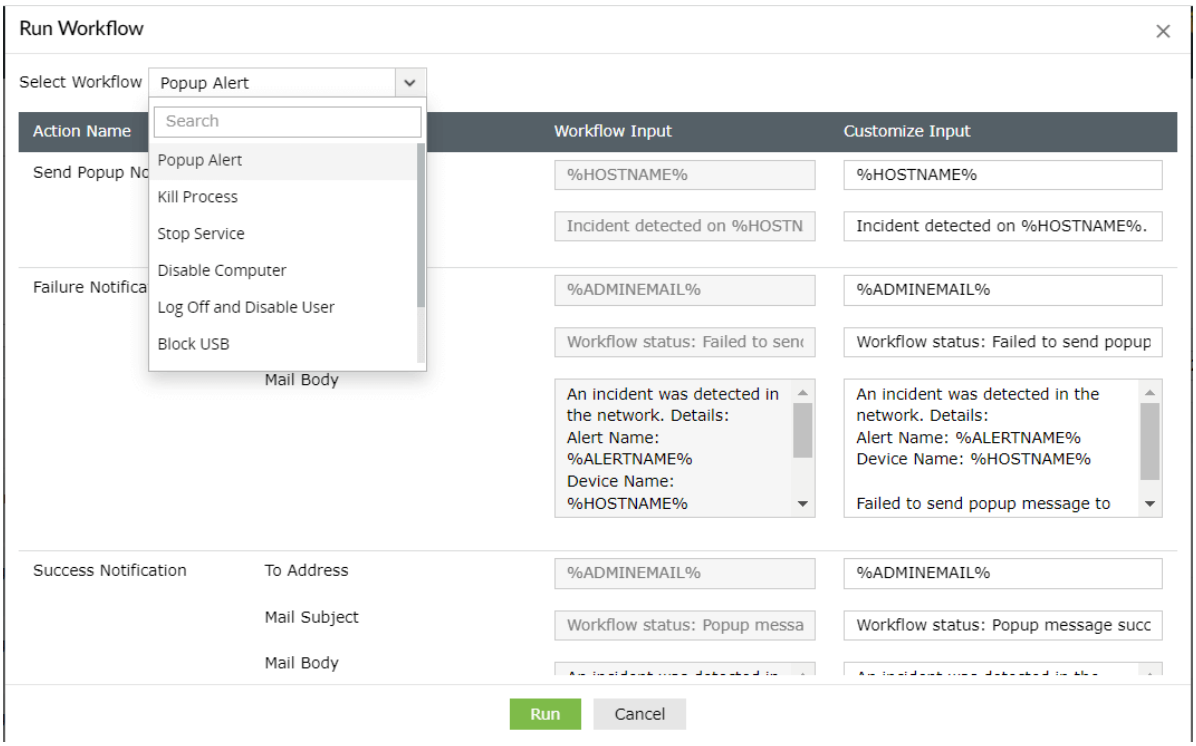
OnDemand Workflows

To run a workflow for an incident,

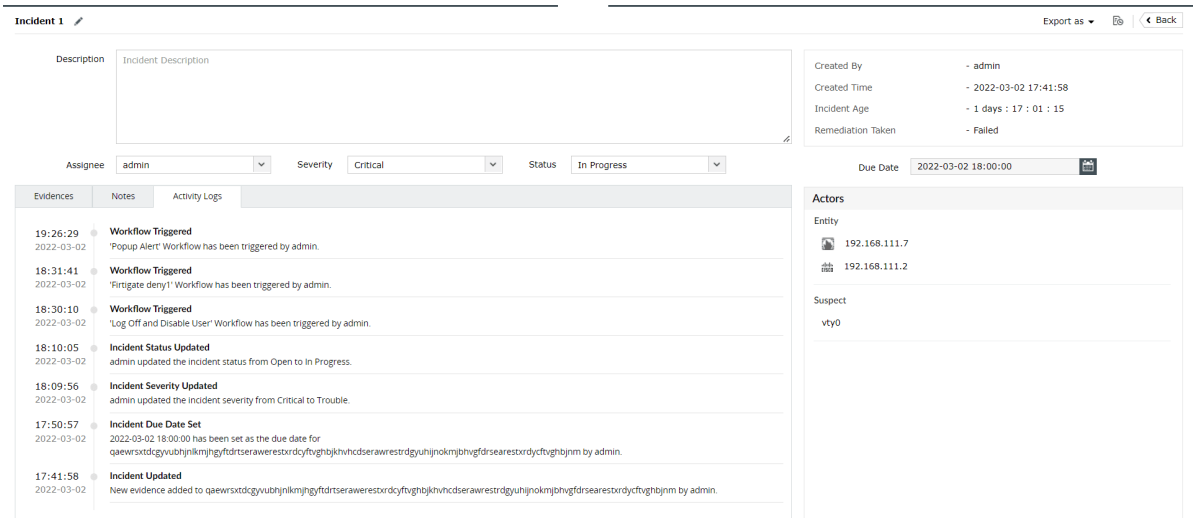
- Navigate to Incident and select the particular incident.
- Click the Run Workflow button for the particular evidence under the Evidences tab.



- Select a workflow from the drop down menu and click Run.



- Click Activity Logs to find the workflow history.

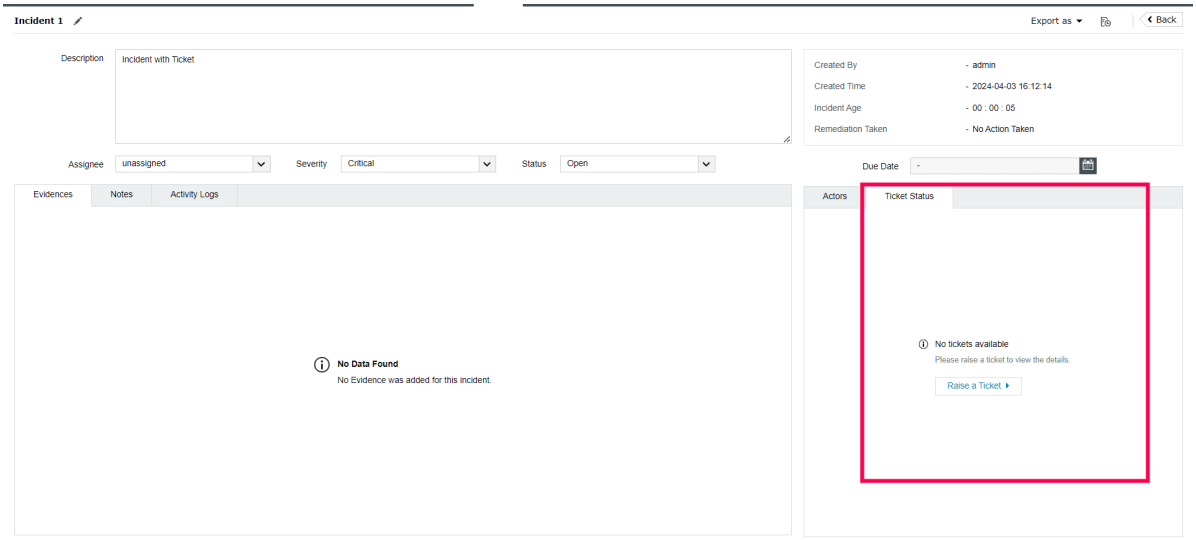


The status of the workflow will be displayed under Remediation Taken in the top-right corner. The same will be recorded in the exported report.
Note: Users can also run multiple workflows for a single alert or incident.

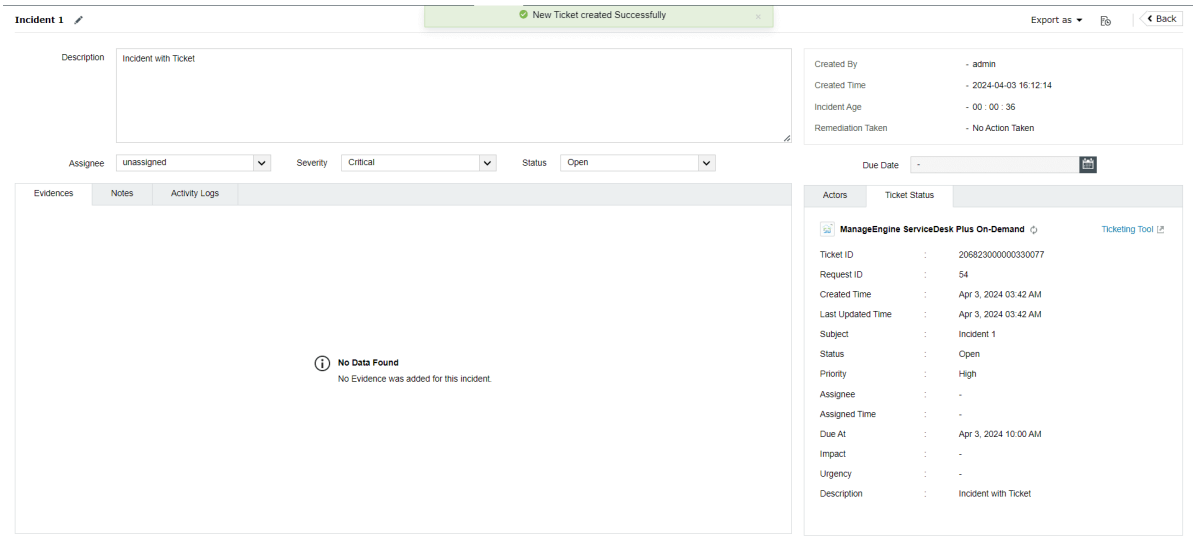
Creating Tickets for Incidents

To create a ticket for an incident,

- Navigate to the Incident section and select the required incident.
- Click the Raise a Ticket button under the Ticket Status tab to create a ticket in the configured ticketing tool; ticket details will be displayed immediately.



- The priority of the created ticket is set based on the current severity of the incident.



- Any changes to the status or severity of the incident will automatically update the ticket's status and severity in the ticketing tool according to the mapped values.

- Refer to this link for status/severity mapping details.

> **Note**
>
> Bidirectional synchronization is only available if the EventLog Analyzer app is installed in the ticketing tool. If not yet installed, follow the steps at this link to install the EventLog Analyzer app.

Incident Management Status/Severity Mapping with Ticketing Tool

Understanding how incident statuses and severities in EventLog Analyzer correspond to those in various ticketing tools is crucial for seamless integration and efficient incident management.

Default Status Mapping

The table below outlines the mapping between EventLog Analyzer incident statuses and the corresponding statuses in different ticketing tools:

Tool	EventLog Analyzer - Incident Status	Ticketing Tool - Ticket Status
Kayako	1. Open 2. In Progress 3. Closed	1. Open 2. Pending 3. Closed
Zendesk	1. Open 2. In Progress 3. Closed	1. Open 2. Pending 3. Solved
ServiceNow	1. Open 2. In Progress 1. Closed	1. New 2. In Progress / Active 3. Closed
Freshservice	1. Open 2. In Progress 3. Closed	1. Open 2. Pending 3. Closed
Jira Cloud	1. Open 2. In Progress	1. Open 2. Work in Progress

	3. Closed	3. Done
Jira Service Desk	1. Open 2. In Progress 3. Closed	1. Open 2. Work in Progress 3. Done
ServiceDesk Plus Cloud	1. Open 2. In Progress 1. Closed	1. Open 2. Open 3. Closed
ServiceDesk Plus	1. Open 2. In Progress 3. Closed	1. Open 2. In Progress 3. Closed
ServiceDesk Plus MSP	1. Open 2. In Progress 3. Closed	1. Open 2. In Progress 3. Closed

Default Severity Mapping

The following table illustrates how incident severities are mapped between EventLog Analyzer and various ticketing tools:

Tool	EventLog Analyzer - Incident Severity	Ticketing Tool - Ticket Severity
Kayako	1. Critical 2. Trouble 3. Attention	Impact: 1. Urgent 2. High 3. Normal
Zendesk	1. Critical 2. Trouble 3. Attention	Priority: 1. Urgent 2. High 3. Normal

ServiceNow	1. Critical 2. Trouble 3. Attention	Priority: 1. 1- Critical 2. 2 - High 3. 3 - Moderate
Jira Cloud	1. Critical 2. Trouble 3. Attention	Priority: 1. Highest 2. Medium 3. Low
Freshservice	1. Critical 2. Trouble 3. Attention	Priority: 1. Urgent 2. High 3. Low
Jira Service Desk	1. Critical 2. Trouble 3. Attention	Priority: 1. High 2. Medium 3. Low
ServiceDesk Plus Cloud	1. Critical 2. Trouble 3. Attention	Priority: 1. High 2. Medium 3. Normal
ServiceDesk Plus	1. Critical 2. Trouble 3. Attention	Priority: 1. High 2. Medium 3. Normal
ServiceDesk Plus MSP	1. Critical 2. Trouble 3. Attention	Priority: 1. High 2. Medium 3. Normal

AlarmsOne	1. Critical 2. Trouble 3. Attention	Priority: 1. Critical 2. Major 3. Info

By aligning incident statuses and severities between EventLog Analyzer and your ticketing tools, you can ensure consistent communication and efficient incident resolution across platforms.

10.3.2.1. Playbook management overview

Last updated on: September 12, 2025

In this page

- Overview
- What is playbook?
- Playbook recommendations
- Workflow architecture
- How is a playbook executed?
- When a playbook is associated to an alert profile
- On-Demand playbook execution
- Playbook history
- Pre-defined playbooks
- Use cases

Overview

Playbooks are automated response workflows designed to help mitigate security incidents as soon as alerts are triggered. Whether it's disabling compromised user accounts, blocking IPs, or enforcing USB policies, playbooks reduce response time and manual intervention through intelligent recommendations and predefined actions. This document explains how playbooks work, how to execute them, and how they align with real-world use cases mapped to the MITRE ATT&CK framework.

What is playbook?

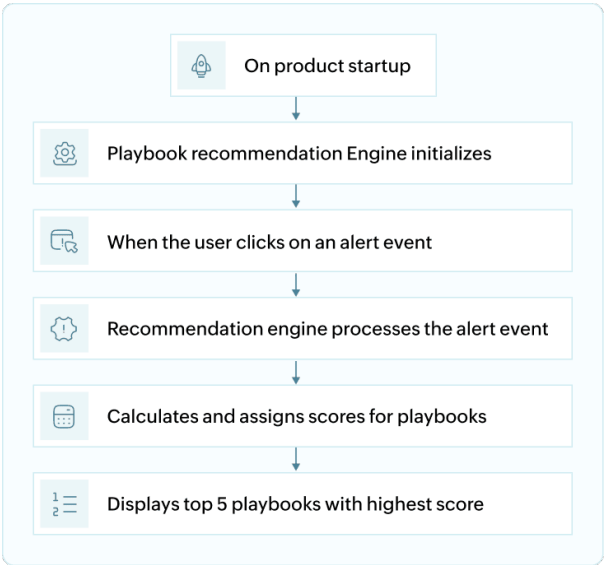
You can mitigate security incidents in your network before they result in a breach by automating response workflows when alerts are triggered. The product allows you to create such workflows to automatically perform actions such as disabling USB ports, shutting down systems, and changing firewall rules when security incidents are detected. This automated capability that provides remediation suggestions is called Playbook.

Playbook recommendations

Playbook recommendations are intelligent, context-aware response suggestions provided for every alert raised in the system. As soon as the product is launched, the playbook recommendation engine is initialized in the background. These recommendations are based on predefined logic that links specific alert types to optimal mitigation or investigation workflows, such as disabling a user account for suspicious login activity, or blocking an IP after detecting port scanning. This system ensures faster, guided incident response and minimizes manual decision-making during critical security events.

When you click on an alert, the engine processes the alert's event data and metadata including parameters like event type, source device, user behavior, and historical response patterns. Based on this context, it evaluates and maps the alert to the most relevant response workflows in the form of playbooks.
Each applicable playbook is assigned a relevance score that reflects how well it matches the characteristics of the alert. The top five scoring playbooks are then displayed under the Run Playbook section.

Workflow architecture



How is a playbook executed?

There are two ways in which a playbook can be executed:

- When a playbook is associated to an alert profile
- On-Demand playbook execution

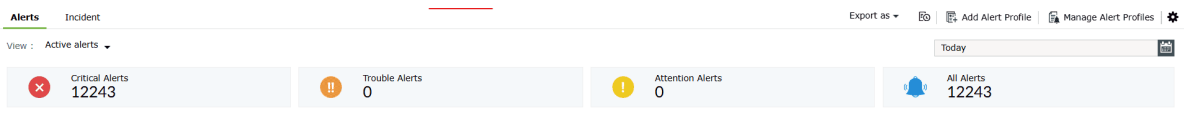
A. When a playbook is associated to an alert profile

When an event triggers an alert, and the alert profile has a playbook linked to it, the playbook runs automatically. In short, the event causes an alert, and the alert triggers the assigned playbook.
Refer to this document to learn how to associate a playbook to an alert profile.

B. On-Demand playbook execution

When an event occurrence is identified, you can manually execute a playbook- either from the list of Recommended Playbooks or Other Playbooks provided in the product console via the Alerts tab.
Below is the step-by-step guide on how to execute a playbook manually.

1. In the product console, navigate to the Alerts tab. The Run Playbook option is provided for each of the alerts generated. Click on the Run Playbook option associated with the alert you wish to execute the playbook for.



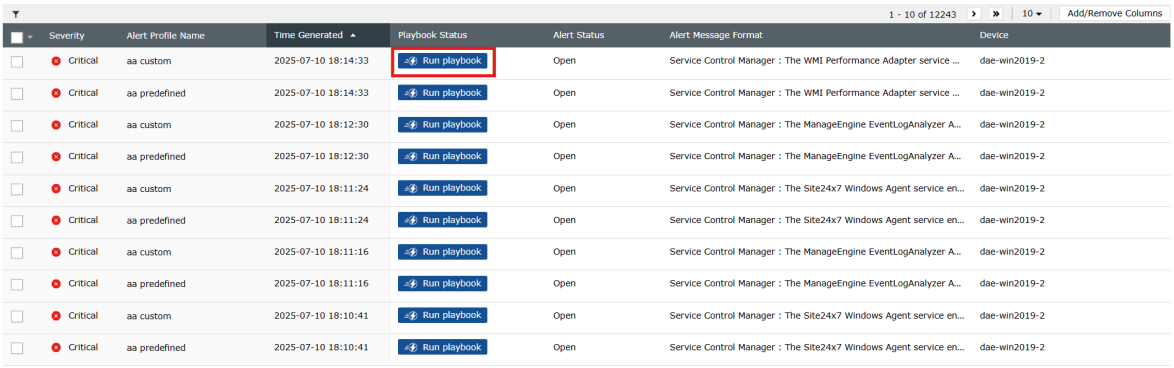
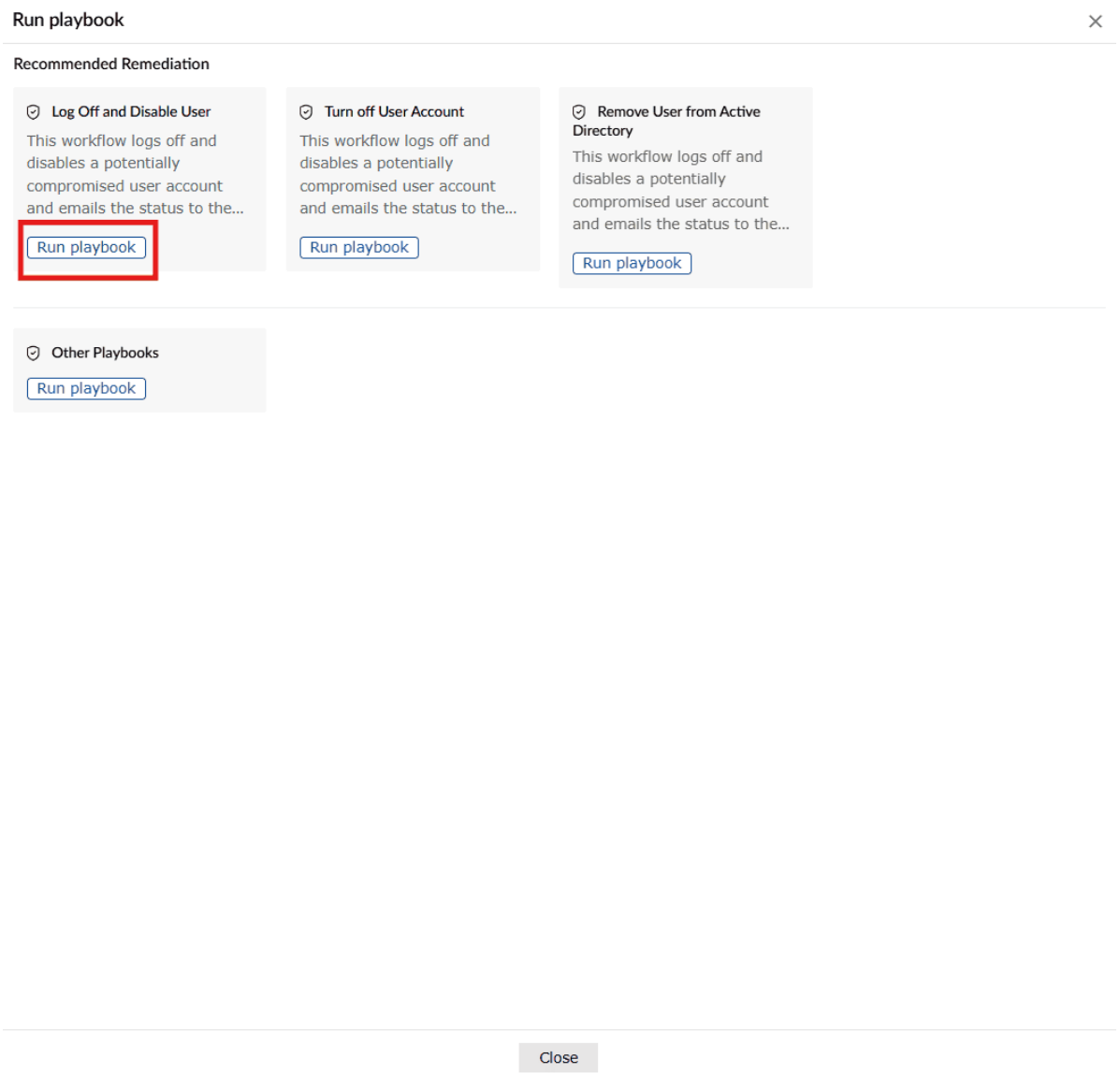
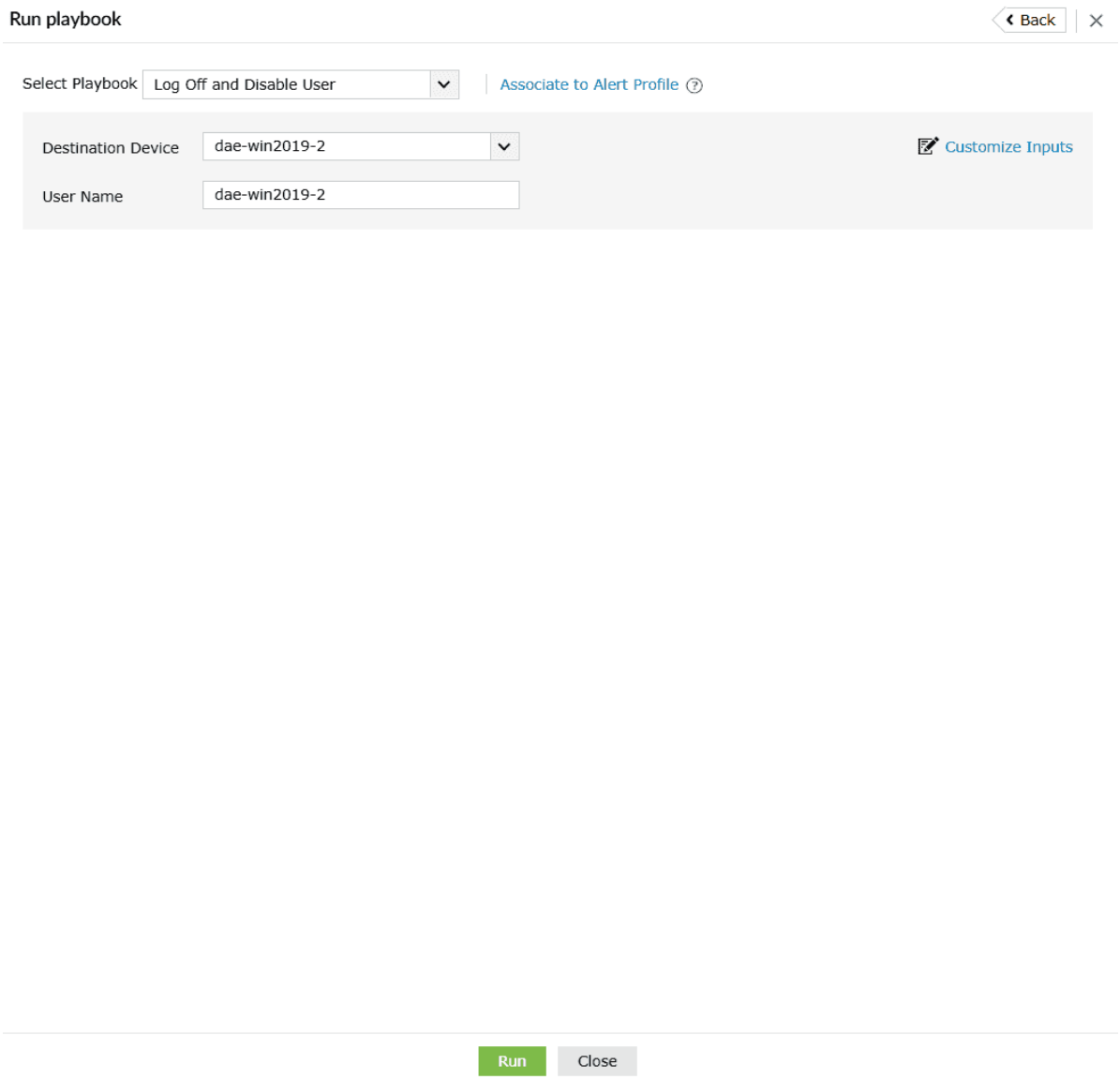


Image 1: Run playbook option for alerts in the alert profile

2. The Run playbook box with the available recommendations for that alert slides in. Click on the Run playbook button of any recommendation option you wish to execute as shown below.



3. The recommendations expand into fields as shown below.



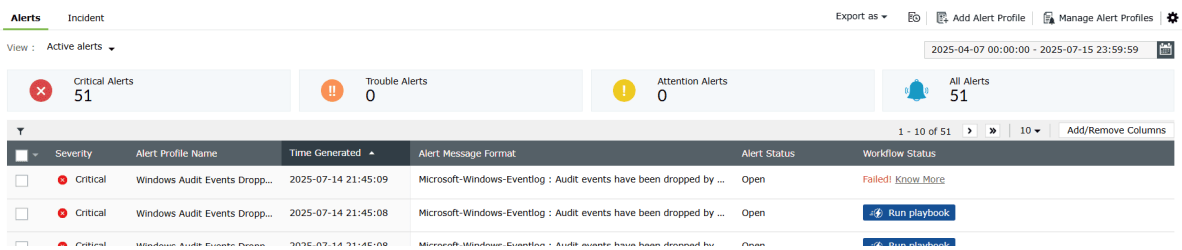
4. The fields in each playbook recommendation vary from playbook to playbook. Click on Run after providing all the necessary inputs. The playbook is executed, and the below pop-up appears.



Playbook history

You can access and view the list of playbooks used until now from the playbook history as explained below:

1. Click anywhere on the row of the required alert profile in the Alerts tab.



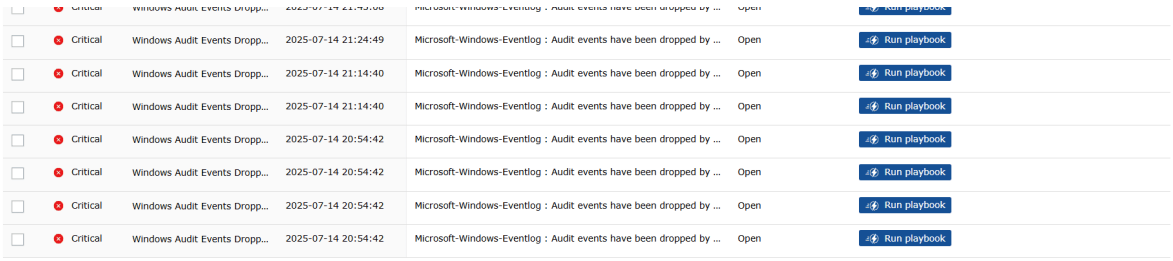


Image 2: Playbook remediations for alerts via the Alerts tab

2. When you click on an alert name, the details of the alert and the related playbooks appear. Under Remediation, you can see the history of the playbooks used for the same alert up until now.

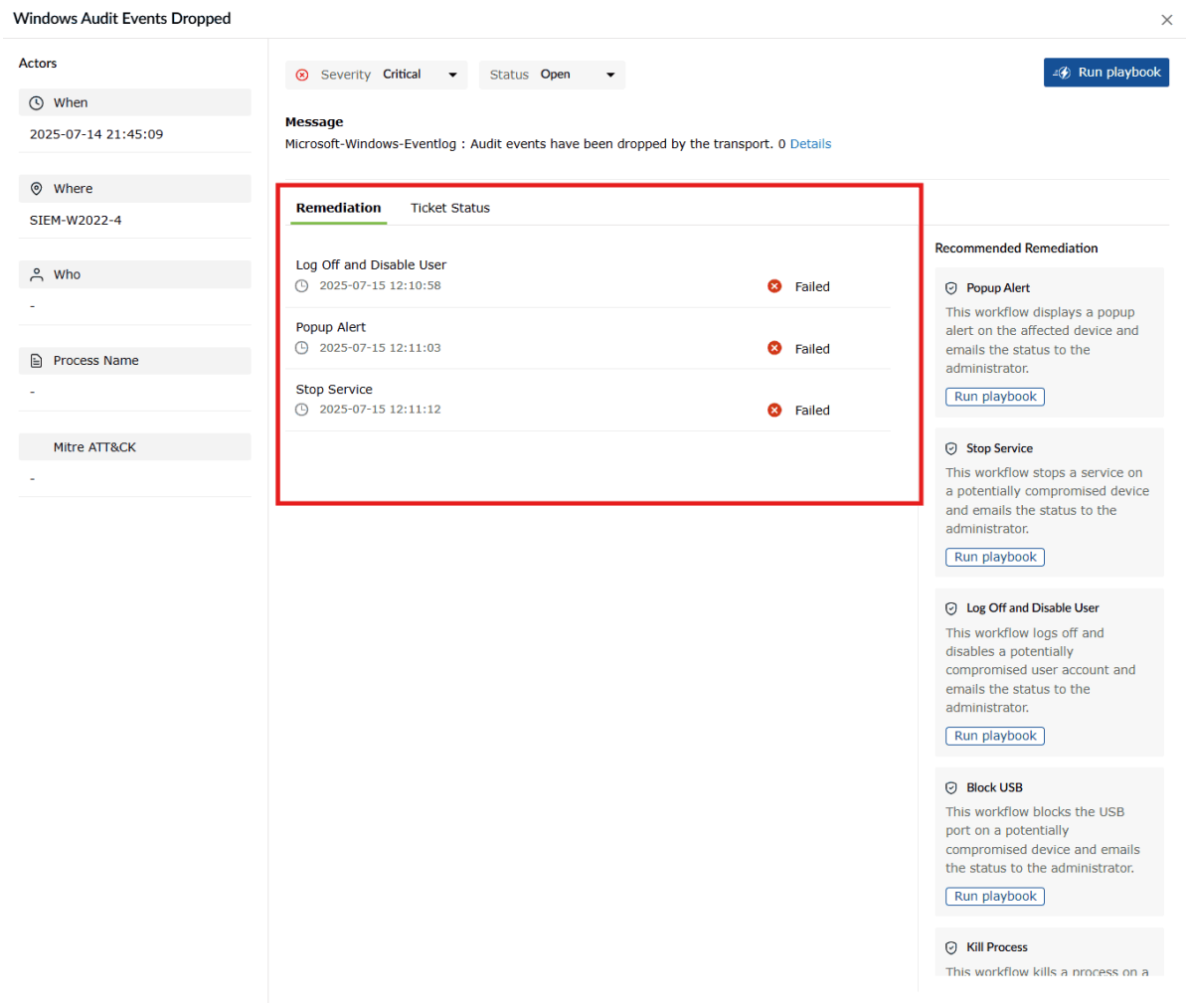


Image 3: Viewing playbooks history from the remediations

Pre-defined playbooks

The product offers 6 predefined playbooks for quick response to common security incidents. These ready-to-use

playbooks perform actions like blocking USB ports, disabling computers, killing processes, or logging off users. Though they can't be edited or deleted, you can run them on demand, link them to alert profiles, or use them as templates when creating custom playbooks. Below is the list of all 6 predefined playbooks and their description.

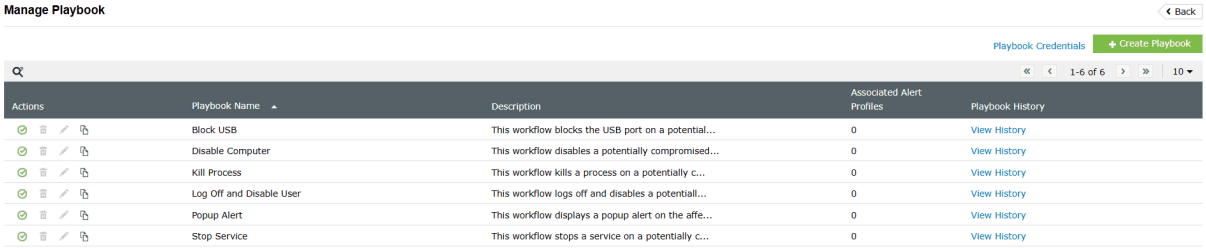


Image 4: List of predefined playbooks available in the product

Playbook name	Description
Block USB	This playbook blocks the USB port on a potentially compromised device and emails the status to the administrator.
Disable Computer	This playbook disables a potentially compromised computer and emails the status to the administrator.
Kill Process	This playbook kills a process on a potentially compromised device and emails the status to the administrator.
Log Off and Disable User	This playbook logs off and disables a potentially compromised user account and emails the status to the administrator.
Popup Alert	This playbook displays a popup alert on the affected device and emails the status to the administrator.
Stop Service	This playbook stops a service on a potentially compromised device and emails the status to the administrator.

Use cases

Use cases

1. Real-time ransomware containment in endpoint environments

Use case

Ransomware attacks usually begin with suspicious file activity or an unauthorized encryption process on the endpoints.

With Playbooks

Playbooks aid in effective remediation strategies when a potential ransomware attack attempt is detected. You can auto-trigger a playbook to disable USB ports, shut down infected systems, block lateral movement via firewall rules, and also notify SOC teams—all within seconds of detection. This helps in reducing the attack blast radius while ensuring business continuity.

MITRE Mapping

Tactic: Impact (TA0040), Execution (TA0002)

Technique: Data Encrypted for Impact (T1486), Command and Scripting Interpreter (T1059)

2. Adaptive firewall rule automation against emerging threats

Use case

A swift response is crucial after detection of Indicators of Compromise (IoCs) like malicious IPs or domains identified in threat intelligence feeds.

With Playbooks

The matching of alerts can trigger instant automated updates to firewall configurations like deny inbound/outbound rules for Cisco ASA, FortiGate, PaloAlto, SophosXG; etc and effectively blacklist malicious endpoints without the need for any manual rule entry thus, ensuring a rapid response across perimeter devices.

MITRE Mapping

Tactic: Defense Evasion (TA0005), Command and Control (TA0011)

Technique: Ingress Tool Transfer (T1105), Application Layer Protocol: Web Protocols (T1071.001)

3. Automatic user account lockdown during Brute-force attacks

Use case

User accounts are targeted during malicious attempts like brute force login attempts and password spraying.

With Playbooks

When an alert for multiple failed login attempts is triggered, a well configured playbook can instantly disable the associated account, block the source IP in the firewall and also notify the admins via alert notifications. This ensures instantaneous mitigation before the attacker(s) successfully authenticate

MITRE Mapping

Tactic: Credential Access (TA0006)
Technique: Brute Force (T1110), Password Spraying (T1110.003)

4. Smart patching of vulnerabilities through Endpoint Central

Use case
Unpatched systems are highly advantageous as entry points for attackers. In large organizations, coordination with IT teams for patching is often delayed/time-consuming.
With Playbooks
When a vulnerability is detected, a playbook can approve the patch and also initiate its deployment via Endpoint Central without requiring any human intervention. This closes critical vulnerabilities faster than any of the manual processes.

MITRE Mapping

Tactic: Initial Access (TA0001), Persistence (TA0003)
Technique: Exploit Public-Facing Application (T1190), Exploitation for Privilege Escalation (T1068)

5. Rogue device detection and network quarantine

Use case
Unknown devices can suddenly appear on the network, often behaving anomalously or bypassing the critical asset inventories.
With Playbooks
When an alert is triggered for such suspicious device activities, a traceroute can be run along with a ping test to assess network path, then disable that device account in AD and create deny access rules in firewalls. This ensures that suspicious assets are isolated immediately while preserving evidence for forensics simultaneously.

MITRE Mapping

Tactic: Discovery (TA0007), Lateral Movement (TA0008)
Technique: Remote System Discovery (T1018), Exploitation of Remote Services (T1210)

6. Centralized enforcement of USB security policies

Use case
Unmanaged USB ports on high-risk systems can act as entry points for attacks pertaining to data leaks
With Playbooks
Optimized configurations could be made in the playbooks to automatically disable USB ports on systems detected for anomalous behavior or based on policy violation alerts. This also ensures zero-trust enforcement even in distributed endpoint environments.

MITRE Mapping

Tactic: Collection (TA0009), Exfiltration (TA0010)

Technique: Data Staged (T1074), Exfiltration Over Physical Medium (T1052)

Read also

This document covered Playbook functionality, execution methods, and use cases. For related capabilities that enhance security orchestration and response, refer to

- Creating playbook
- Manage playbooks
- Update playbook credentials

10.3.2.2. Playbook management prerequisites

Last updated on: September 12, 2025

In this page

Overview

Prerequisites

List of devices supported

List of prerequisites

Overview

This document outlines the prerequisites for executing playbook actions, including supported OS platforms, necessary ports, protocols, and permission settings. It details the configurations required across Windows, Linux, AD, and firewall devices to ensure seamless response execution during security events.

Prerequisites

List of devices supported

- All types of Windows operating system.
- Linux operating systems:
  - Ubuntu
  - Debian
  - Fedora
  - CentOS
  - Red Hat Enterprise Linux (RHEL)
  - Arch Linux
  - SUSE Linux Enterprise Server (SLES)
  - openSUSE
  - Gentoo OS

Below are the necessary configurations to be made in order to access the playbook capability

Guide:
Port: Used for communication (this port should be open, free, and allowed in firewall)
Inbound: To which device/application the action is targeted towards.
Outbound: From where the action is raised.
Service: Which service/protocol will be used to execute this action.

NETWORK ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND
PING DEVICE	ICMP/No ports	Audited Windows / Linux Device	EventLog Analyzer Server
TRACE ROUTE WINDOWS	ICMP/No ports	Audited Windows Device	EventLog Analyzer Server
TRACE ROUTE LINUX	UDP/33434 -33534	Audited Linux Device	EventLog Analyzer Server

WINDOWS ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
LogOff	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: The computer should not include the EventLog Analyzer Installed server.
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: Distributed COM Users User Permissions: For root\cim v2 In WMI Properties:
	TCP/139	Audited Windows	EventLog Analyzer	NetBIOS session	

BLOCK	PORT	Device INBOUND	Server OUTBOUND	RPC/NP SERVICE	Additional Rights and Permissions
Shutdown and Restart	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	• Enable Account • Remote Enable • Read Security Environment Permission: The computer should not include EventLog Analyzer installed server
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
Execute Windows Script	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: The user should have read, write and modify access to the shared path in the script.
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
Disable USB	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: • Remote Registry
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	Service should be running. • Full Control permission to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
ALL SERVICE BLOCK	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users • Administrators User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
START PROCESS	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to	Audited Windows	EventLog Analyzer	RPC randomly allocated	

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
	TCP/1024 to 65,535	Windows Device	Analyzer Server	allocated high TCP ports	
STOP PROCESS	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
TEST PROCESS	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	

LINUX ACTIONS

BLOCK BLOCK	PORT PORT	INBOUND INBOUND	OUTBOUND OUTBOUND	SERVICE SERVICE	Additional Rights Additional Rights and Permissions and Permissions
Shutdown and Restart	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission : The user should be the root user.
Execute Windows Script	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission : Sudo permission for user.
ALL SERVICE BLOCK	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission : Sudo permission.
START PROCESS	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission : The permission to execute the command should be available for the user whose credentials are provided.
STOP PROCESS	Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission : The permission to execute the command should be available for the user whose credentials are provided.
TEST PROCESS	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	-

NOTIFICATIONS

BLOCK BLOCK	PORT PORT	INBOUND INBOUND	OUTBOUND OUTBOUND	SERVICE SERVICE	Additional Rights and Additional Rights and Permissions Permissions
Pop Up WINDOWS	TCP/135	Audited Linux Device	EventLog Analyzer Server	RPC	UserGroups: Distributed COM Users User Permissions For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: "AllowRemoteRPC" should be 1 for HKEY_ LOCAL_MACHINE\ SYSTEM\Current ControlSet\Control\Terminal Server.
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
Pop Up LINUX	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: Sudo permission for user.
Send Email WINDOWS & LINUX	TCP/Port mentioned while config using SMTP server	Audited Linux Device	EventLog Analyzer Server	-	Environment Permission: SMTP server should be configured on Event log analyzer server
Send SMS WINDOWS & LINUX	-	-	-	-	Environment Permission: SMS Server should be configured in the product.
Send SNMP Trap WINDOWS & LINUX	UDP/Port specified in workflow block	Audited Windows / Linux Device	EventLog Analyzer Server	-	Environment Permission: The port mentioned in workflow configuration should be open.

AD ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and

BLOCK BLOCK	PORT PORT	INBOUND INBOUND	OUTBOUND OUTBOUND	SERVICE SERVICE	Permissions Additional Rights and Permissions
DELETE AD USER WINDOWS	TCP/389	Audited Domain Controller	EventLog Analyzer Server	LDAP	User Permissions: • The user should have "Delete" Right in the AD to delete other Accounts. • The user to delete should not have "Protect Object from accidental deletion" checked.
DISABLE AD USER WINDOWS	TCP/389	Audited Domain Controller	EventLog Analyzer Server	LDAP	User Permissions: The User account provided should have "Read","Write ","modify owners" and "modify permissions" permissions enabled.
DISABLE USER COMPUTER WINDOWS & LINUX	TCP/389	Audited Domain Controller	EventLog Analyzer Server	LDAP	User Permission: The User account provided should have "Read", "Write" , "modify owners" and "modify permissions" permissions enabled.

MISCELLANEOUS ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
	TCP/135	Audited Windows Device	EventLog Analyzer Server	UserGroups: Distributed COM Users User Rights: • Act as part of the operating system • Log on as a batch job • Log on as a service • Replace a process level

BLOCK WRITE TO FILE WINDOWS	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	User Permissions: For root\cim v2 In Properties: • Execute Methods • Enable Account • Remote Enable • Read Security Environment Permission: The user should have read,write and modify access to the shared path.
WRITE TO FILE LINUX	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	Environment Permission: Sudo permission for user
HTTP WebHook	-	-	-	Environment Permission: A "connect" Socket Permission to the host/port combination of the destination URL or a "URL Permission" that permits this request.
FORWARD LOGS	TCP/Specified Port	Audited Windows / Linux Device	EventLog Analyzer Server	-
CSV LOOKUP	TCP/Specified Port	Audited Windows / Linux Device	EventLog Analyzer Server	User Permissions: Read permission to the specified CSV file.

FIREWALL ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
Cisco ASA deny inbound/Outbound rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: Refer to this page

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
Fortigate deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: Refer to this page
Palo Alto deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: Refer to this page
Sophos XG deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: Refer to this page
Barracuda deny Access rules	https/8443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: Refer to this page

Read also

This guide covers the groundwork for executing playbooks. For a deeper understanding of automation and orchestration in security response, refer to:

- Manage playbooks
- Update playbook credentials

10.3.2.3. Creating a playbook

Last updated on: September 12, 2025

In this page

Overview

Custom Create a Playbook

Reset Playbook

List of Playbook blocks

Overview

This document guides you through the steps to build custom playbooks using predefined logic blocks. These workflows automate security responses, ranging from system actions to AD user operations, helping you mitigate incidents more efficiently.

Creating a custom playbook

Steps to create a playbook

1. In the product console, navigate to the Alerts tab. Click on the More tools icon present at the top-right corner of the page as highlighted in the below image.

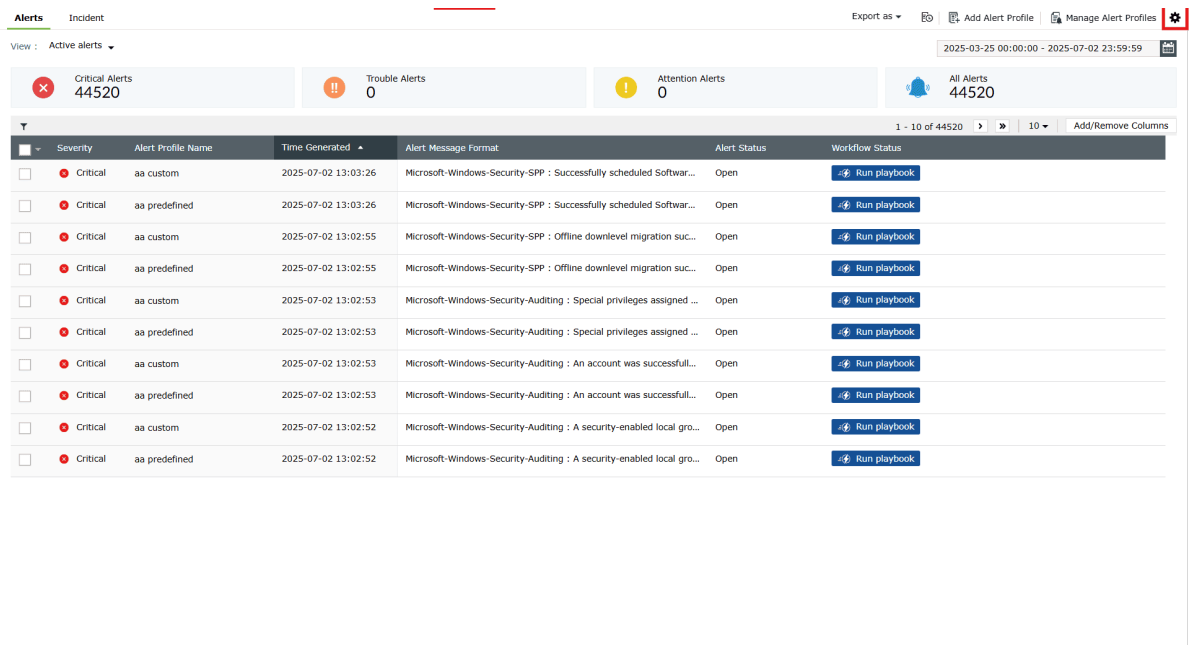
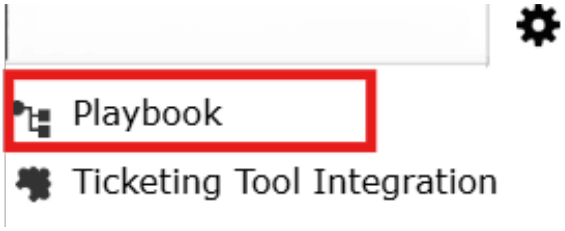


Image 1: More tools icon in the Alerts tab

2. Click on Playbook to open the Manage Playbook page.



3. Click on the +Create Playbook button.

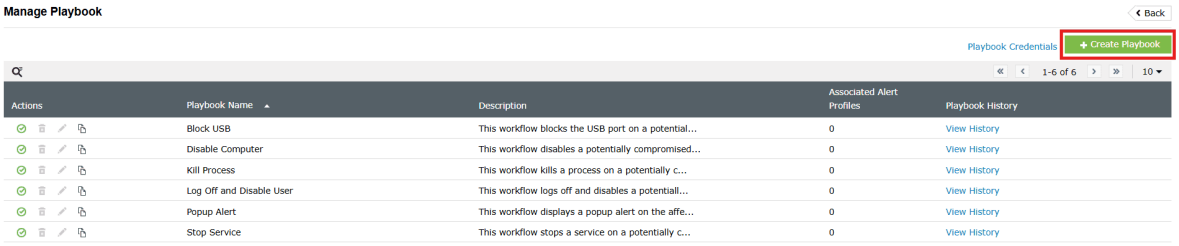


Image 2: Create Playbook button via the Alerts tab

4. Enter a name for the playbook in the Playbook Name field.

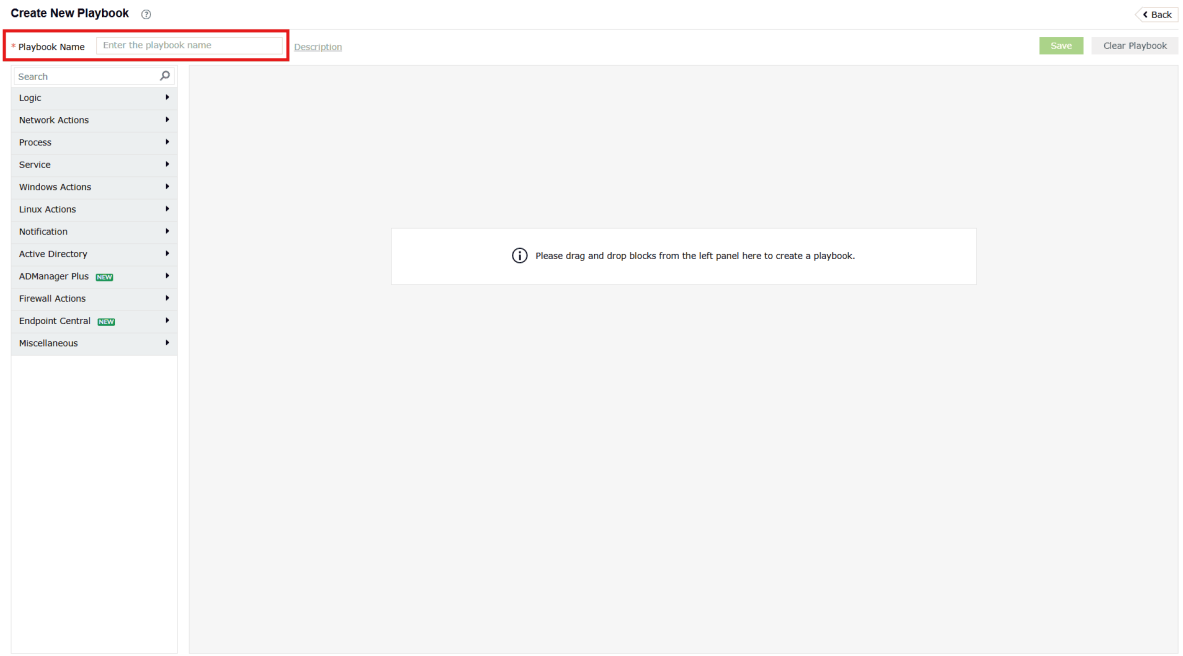
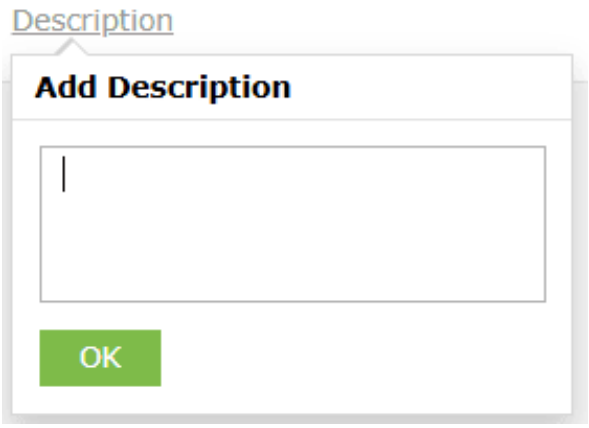


Image 3: Playbook name field during playbook creation

5. Click on Description (optional) beside the Playbook Name field to enter an appropriate description for the playbook. Click on OK.

playbook. Click on OK.



6. On the left pane, there are components provided for different event categories. Click on the respective drop-down icons in order to expand the actions. Create a playbook by dragging and dropping the playbook blocks from the left pane into the space provided. Ensure that these blocks are logically arranged to execute an event in your infrastructure.

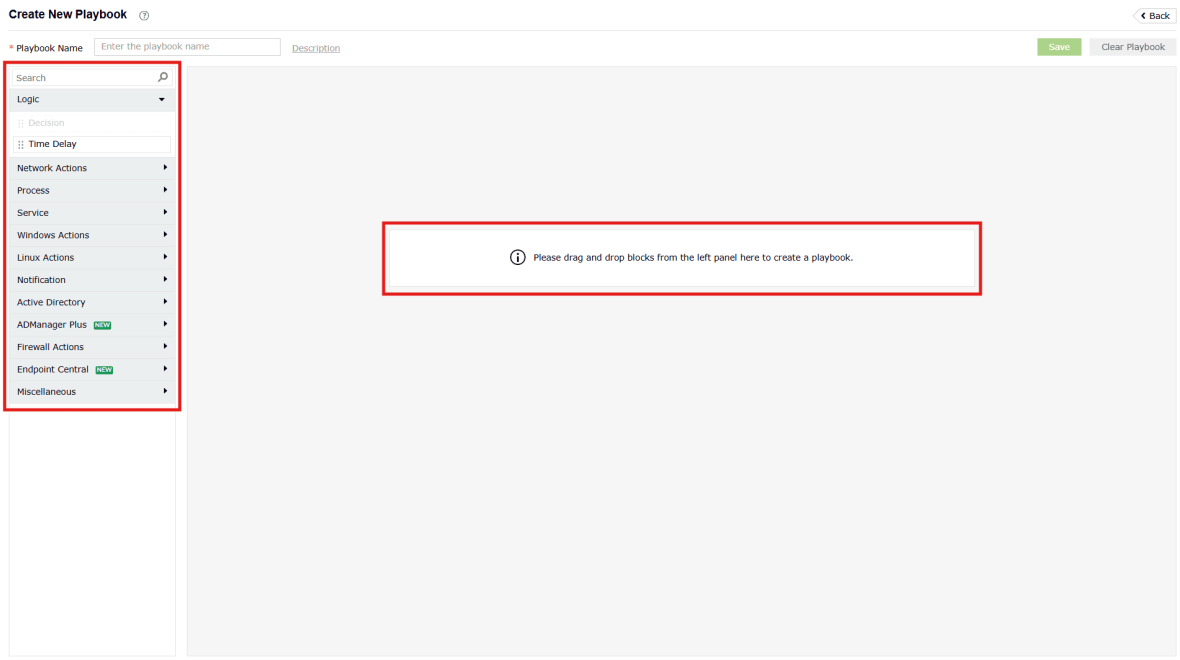
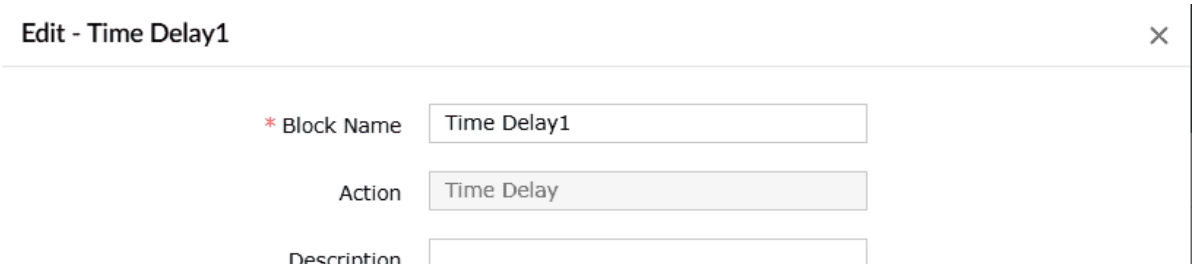


Image 4: Playbook blocks arrangement during playbook creation

7. The moment you finish the drag and drop action, an Edit pop-up appears with fields to configure that specific playbook block further. The fields to edit the playbook blocks vary from one block to another. After editing as per your requirements, click on OK. You can always come back and edit these blocks by clicking on the edit icon visible on the blocks in the drag and drop area.



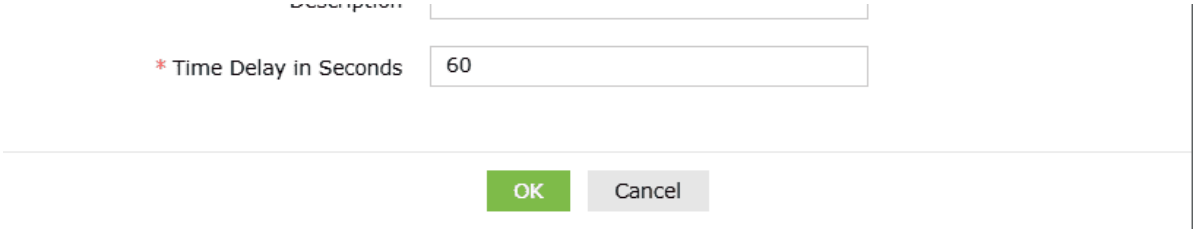


Image 5: Playbook blocks details during playbook creation

8. You can include multiple blocks in one playbook. Once you are done with the workflow design of your playbook, click on Save.

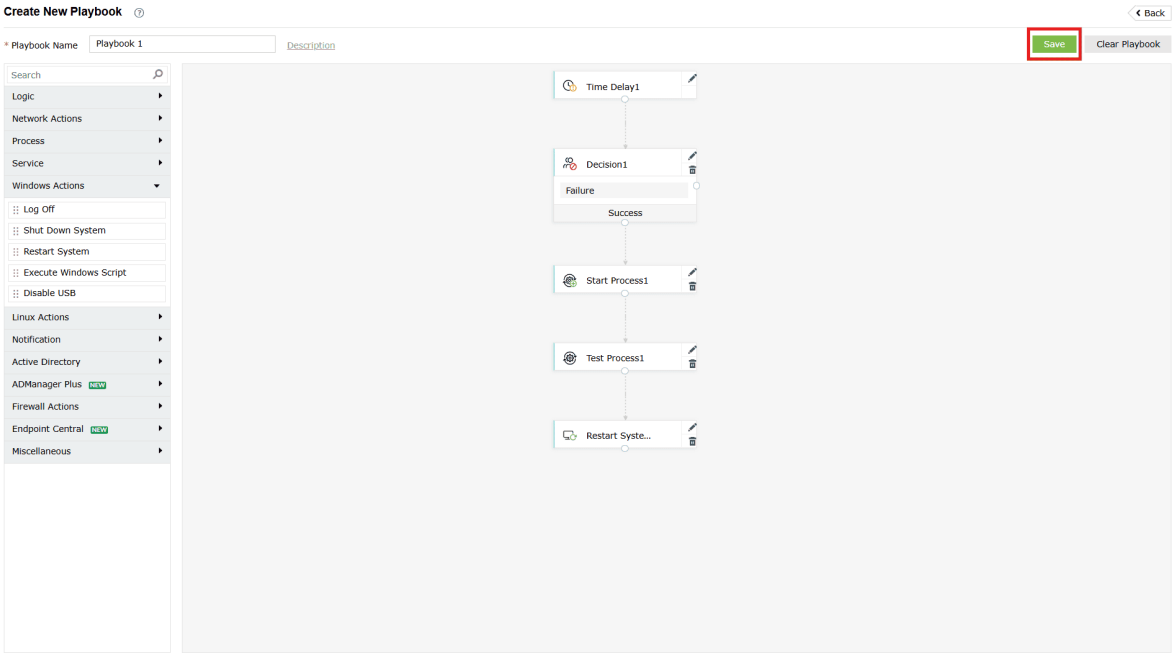
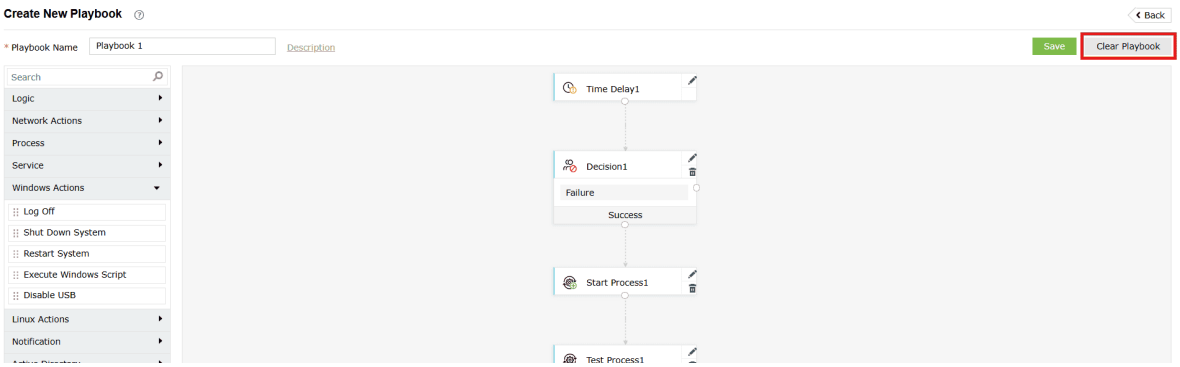


Image 6: Save a playbook after playbook creation

9. The playbook is saved instantly, and you will be taken back to the Manage Playbook tab with your newly created playbook listed under the playbooks list.

Reset playbook

1. In case you wish to reset the configurations set in the playbook creation up until now, click on the Clear Playbook button as highlighted in the below image.



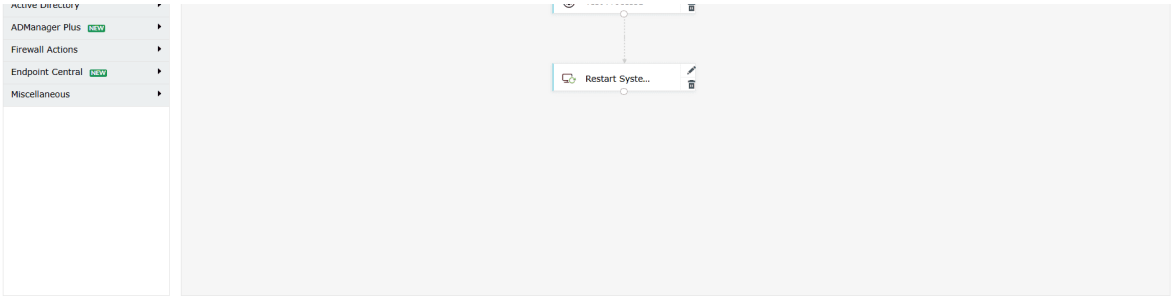
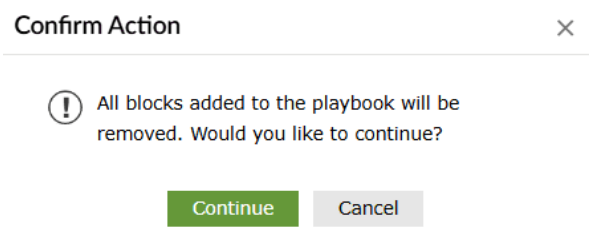


Image 7: Clear playbook option during playbook creation

2. A Confirm Action pop-up appears. Click on Continue.



3. All the configurations set in the playbook until then are cleared instantly, and you can see that the workspace becomes empty again.

List of playbook blocks

The product contains multiple playbook blocks to help you configure the playbooks to perform the required actions. The logic blocks are categorized under different sections.
The list of playbook blocks and the details to be specified while configuring playbooks using them are given below:

Component	Logic blocks	Details to be specified
Logic Actions	Decision Allows you to branch the playbook based on the status of the previous action.	Optional description
	Time Delay Allows you to introduce a time delay in the execution of the playbook.	The time delay in seconds.
	Ping Device Allows	• The name of the device to be pinged. • Number of echo request messages to be sent.

Component	Logic blocks	Details to be specified
	you to ping a device within your network to check connectivity	• Size of the packet to be sent. • Timeout for the action. • Number of action retries within the specified time.
Network actions	Trace Route Allows you to run a trace route function to a device in your network to identify the path.	• The name of the device you wish to trace the route to. • The maximum number of Hops. • Timeout for the action.
Process actions	Test Process Allows you to test whether a process is running on a device.	• The name of the device on which you want to test the process. • The process you want to test. • ExecutablePath and CommandLine to execute the process.
	Start Process Allows you to start a process on a device	• The name of the device on which you want to start a process. • The process working directory. • The command to start the process.
	Stop Process Allows you to stop a process on a device.	• The name of the device on which you want to stop the process. • The process you want to stop. • ExecutablePath and CommandLine to execute the process.
Service actions	Test Service Allows you to test whether a service is running on a device.	• The name of the device on which you want to test the service. • The service you want to test
	Start Service Allows you to start a service on a device.	• The name of the device on which you wish to start a service. • The service to be started.

Component	Logic blocks	Details to be specified
	Stop Service Allows you to stop a service on a device.	• The name of the device on which you wish to stop a service. • The service to be stopped
Windows actions	Log Off Allows you to log off from the currently active session on a device.	• The name of the device you want to log off from. • Select whether you'd like to force this action.
	Shut Down System Allows you to shut down a Windows device.	• The name of the device to be shut down. • Select whether you'd like to force this action.
	Restart System Allows you to restart a Windows device.	• The name of the device to be restarted. • Select whether you'd like to force this action.
	Execute Windows Script Allows you to execute a specified script file on a Windows device.	• The name of the device on which you want to execute the script file. • The type of script file. • Upload the script file to be executed. • Arguments to the script, if any. • You can separate multiple arguments using commas. • Timeout for the action. • The working directory for the script's execution.
	Disable USB Allows you to disable the USB port on a device.	The name of the device on which you want to disable the USB port.
	Shut Down Linux Allows you to shut down a Linux device.	• The name of the device to be shut down. • Select whether you'd like to force this action.

Component	Logic blocks	Details to be specified
Linux actions	Restart Linux Allows you to restart a Linux device.	• The name of the device to be restarted. • Select whether you'd like to force this action.
	Execute Linux Script Allows you to execute a specified script file on a Linux device.	• The name of the device on which you want to execute the script file. • The type of script file. • Upload the script file to be executed. • Arguments to the script, if any. • You can separate multiple arguments using commas. • Timeout for the action. • The working directory for the script's execution.
Notification actions	Send Pop-Up Message Allows you to display a pop-up message on a device.	• The name of the device on which you want to display the message. • The message to be displayed.
	Send Email Allows you to send an email message.	• The recipient's email address. • The email subject and body.
	Send SMS Allows you to send an SMS message.	• The recipient's mobile number. • The SMS content.
	Send SNMP Trap Allows you to send SNMP traps to the required destination.	• Enterprise OID. • SNMP Manager. • Message content.
	Disable User Allows you to disable a user's account.	The name of the user account you want to disable.

Component	Logic blocks	Details to be specified
Active Directory actions	Delete User Allows you to delete a user account.	The name of the user account you want to delete.
	Disable Computer Allows you to disable a computer account.	The name of the computer account you want to disable
Firewall Actions	Cisco ASA Deny Inbound Rule Allows you to add an deny inbound rule.	• The name of the firewall device. • The Interface name. • Source address. • Destination address.
	Cisco ASA Deny Outbound Rule Allows you to add an deny outbound rule.	• The name of the firewall device. • The Interface name. • Source address. • Destination address.
	Fortigate Deny Access Rule Allows you to add an deny access rule.	• Name of the firewall device. Source address. • Destination address. • Name of the source interface. • Name of the destination interface.
	PaloAlto Deny Access Rule Allows you to add an deny access rule.	• Name of the firewall device. Source address. • Destination address. • Name of the source zone. • Name of the destination zone. • Type of Rule (Universal, Intrazone or Interzone).
	SophosXG Deny Access Rule Allows you to add an deny access rule.	• Name of the firewall device. • Source address. • Destination address.

Component	SophosXG Update Logic blocks Deny Access Rule	• The name of the firewall device. Details to be specified • The rule name.
	Allows you to update an deny access rule.	• Source address. • Destination address.
	Barracuda CloudGen Deny Access Rule Allows you to add an deny access rule.	• Name of the firewall device. • Source address. • Destination address. • Name of the source interface. • Name of the destination interface. • Type of Rule (Inbound or Outbound).
Miscellaneous actions	Write to File Allows you to write a message to a file	• The name of the device on which the file is located. • The file name. • The absolute file path. • The text to be written to the file. • Select whether you would like to append to or overwrite a file if it already exists.
	CSV Lookup Allows you to search for values within a CSV file.	• Upload the CSV file to perform by clicking on "Browse". • Specify the header or column number. • Select the field to be matched.
	Forward Logs Allows you to forward logs to the required destination.	• Name of the destination server. • The protocol to be used. • Port number and standard.
	HTTP Request Allows you to send an HTTP request to a URL.	• The URL to which you want to send an HTTP request to. • Specify the Method you want to use (Get or Post). • Add the required headers. • Add the required parameters.

Component	Logic blocks	Details to be specified
	Disable User Allows you to disable a user account	• The name of the block. • The action to be performed (here, Disable User). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to disable.
	Delete User Allows you to delete a user account	• The name of the block. • The action to be performed (here, Delete User). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to delete.
	Disable Computer Allows you to disable a computer account.	• The name of the block. • The action to be performed (here, Disable Computer). • A brief description for this block to record its purpose in the workflow. • The device name of the computer account you want to disable.
	Reset user password Allows the user to reset their password	• The name of the block. • The action to be performed (here, Reset user password). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to reset the password. • The type of password that you want: Random or Custom.
	Add user to group Allows you to add a user to a particular group	• The name of the block. • The action to be performed (here, Add user to group). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to add to

Component	Logic blocks	Details to be specified
		the group. • The name of the group you want to add the user.
ADManager Plus actions		
	Remove user from group Allows you to remove a user from a particular group	• The name of the block. • The action to be performed(here, Remove user from group). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to remove from the group. • The name of the group that you want to remove the user from, or remove the user from all the groups that are available.
	Enable user Allows you to enable a disabled user account	• The name of the block. • The action to be performed(here, Enable user). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to enable.
	Unlock user Allows you to unlock a locked user account	• The name of the block. • The action to be performed(here, Unlock user). • A brief description for logic block to record its purpose in the playbook. • The username of the user account you want to unlock.
	Update user Allows you to update an attribute of a user	• The name of the block. • The action to be performed(here, Update user). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to update. • The attribute that you want to update in the user account's data. • The value of the attribute that needs to be updated.

Component	Logic blocks	• The name of the block. Details to be specified • The action to be performed(here, Delete Computer).
	Delete Computer Allows you to delete a computer account	• A brief description for this block to record its purpose in the playbook. • The device name of the computer account you want to delete.
	Enable computer Allows you to enable a disabled computer account	• The name of the block. • The action to be performed(here, Enable Computer). • A brief description for this block to record its purpose in the playbook. • The device name of the computer account you want to enable.
Endpoint Central actions	Install Patch Allows you to install a patch on a specific device for a detected vulnerability.	• The name of the block. • Name/IP of the destination device to install patch. • Name of the deployment configuration. • Description for the deployment configuration. • Vulnerability identifier will be extracted from alert criteria. • Deployment policy to be applied.
	Approve Patch Allows you to approve patches for the detected vulnerability.	The name of the block Vulnerability identifier will be extracted from alert criteria.

Read also

This document covered how to create custom playbooks, including workflow components and supported actions. For related capabilities that enhance security orchestration and automation, refer to:

- Manage playbooks
- Update playbook credentials

10.3.2.4. Managing playbooks

Last updated on: September 12, 2025

In this page

Overview

Managing Playbooks

Enable/Disable

Delete

Edit

Copy a playbook

Overview

The manage playbook section provides an overview of all configured playbooks along with their status, associated alert profiles, and execution history. Custom playbooks can be edited, deleted, copied, or toggled on/off. Predefined playbooks, however, can only be enabled, disabled, or duplicated—not edited or deleted.

Managing playbooks

1. In the product console, navigate to the Alerts tab. Click on the More tools icon present at the top-right corner of the page as highlighted in the below image.

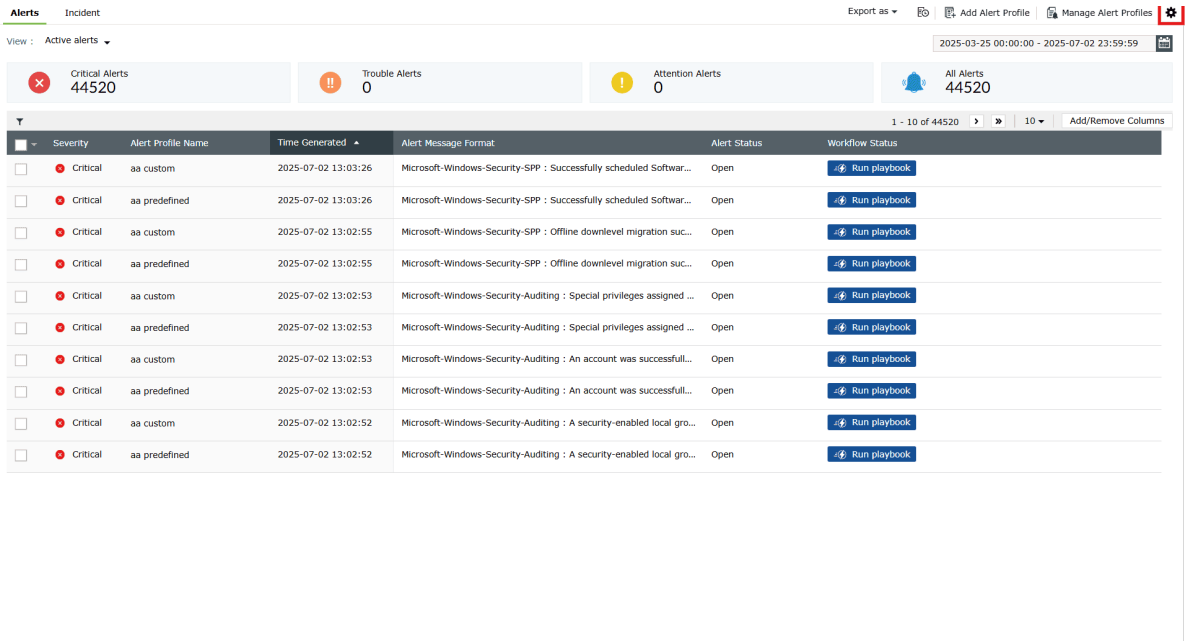
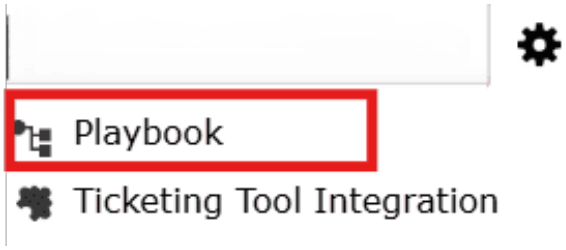


Image 1: More tools option in the Alerts tab

2. Click on Playbook to open the Manage Playbook page.



3. The Manage Playbook page displays the list of all playbooks, their descriptions, the number of alert profiles associated with each playbook, and their histories. You can:
   - Enable/disable
   - Delete
   - Edit
   - Copy a playbook

Enable/disable a playbook

Enabling a playbook

1. Click on the currently disabled icon under the Actions column to enable the playbook.
2. As soon as you perform this action, the icon indicates that the playbook is now enabled and the below pop-up message appears briefly.



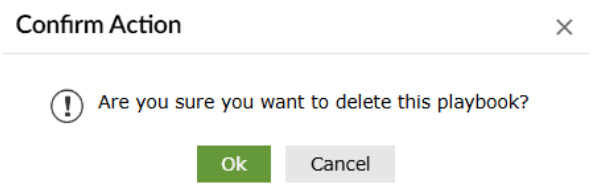
Disabling a playbook

1. Click on the currently enabled icon under the Actions column to disable the playbook.
2. As soon as you perform this action, the icon indicates that the playbook is now disabled and the below pop-up message appears briefly.



Delete a playbook

1. Click on the Delete icon under the Actions column to delete the playbook.
2. A Confirm Action pop-up appears. Click on Ok.



3. Upon successful completion of the action, the below pop-up appears.



NOTE

Only custom created playbooks can be deleted. Pre-defined playbooks can only be enabled/disabled or copied.

Edit a playbook

1. Click on the Edit icon under the Actions column to edit the respective playbook.
2. You will be taken to the Edit Playbook page. Make the necessary edits by changing the playbook blocks if needed and/or editing the playbook blocks' details, and click on Save.

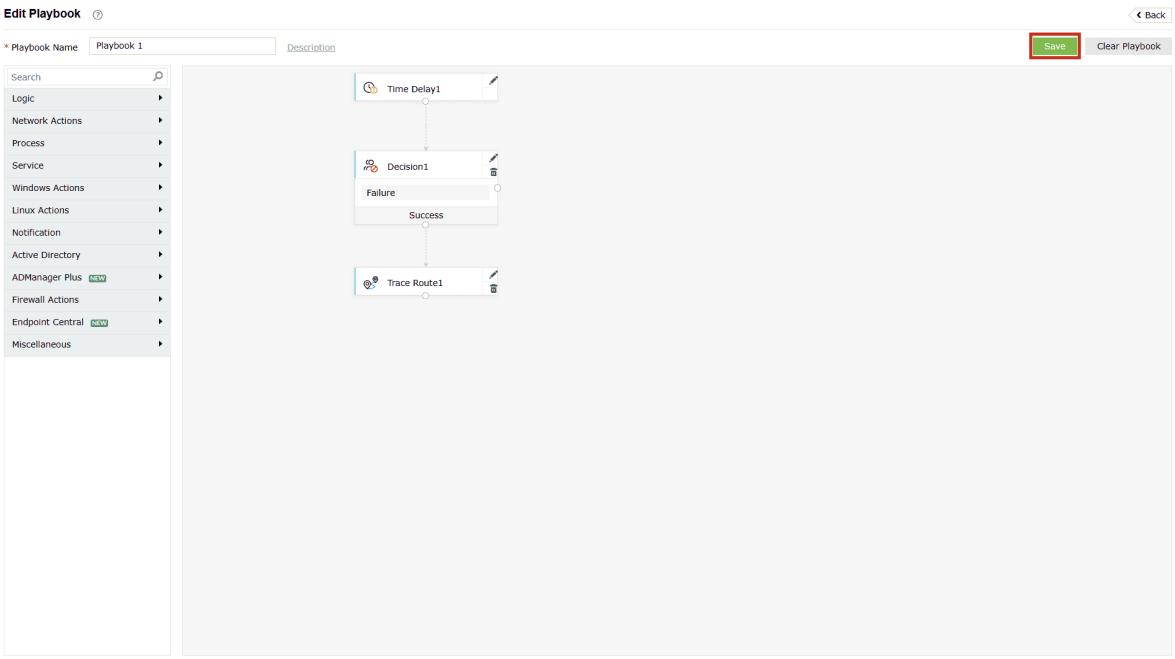


Image 2: Editing a playbook and saving the changes

3. The playbook is saved instantly, and you will be taken back to the Manage Playbook tab with your updated playbook listed under the playbooks list.

Copy a playbook

1. Click on the Copy icon under the Actions column to duplicate the respective playbook.
2. That playbook is instantly duplicated, and you can see the cloned version with the Playbook Name "Copy of (name of the playbook you have cloned)".

Read also

To get the most out of Playbooks, learn how to create custom ones using drag-and-drop blocks and how to associate them with alert profiles for automated incident response. You may also want to explore supported playbook actions and prerequisite configurations.

- Update playbook credentials
- Creating playbook

- Creating playbook
- Prerequisites for playbook configuration

10.3.2.5. Updating playbook credentials

Last updated on: September 12, 2025

In this page

Overview

Update playbook credentials

Accessing Playbook credentials

Windows devices

Linux devices

Cisco devices

Fortigate devices

PaloAlto devices

SophosXG devices

Barracuda CloudGen devices

ADManager Plus

SNMP TRAP

Overview

To ensure successful playbook execution across your infrastructure, credentials for supported devices must be securely configured within the product. You can set global or device-specific credentials for Windows, Linux, and major firewall vendors. Some integrations, like ADManager Plus and SNMP Traps, require additional setup to enable action-based responses.
Only users with admin privileges can manage playbook credentials.

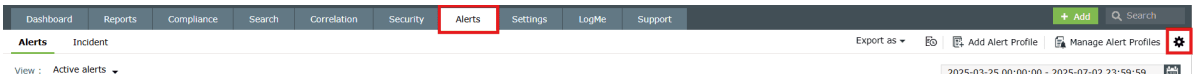
Updating playbook credentials

Pre-requisites to update playbook credentials:

- You can automate playbooks on Windows, Linux, and Cisco devices. But in order to perform this action, you must have administrative privileges.
- The credentials of these devices must also be updated in Log360 for seamless execution of the playbooks.

Accessing playbook credentials

1. In the product console, navigate to the Alerts tab. Click on the More tools icon present at the top-right corner of the page as highlighted in the below image.



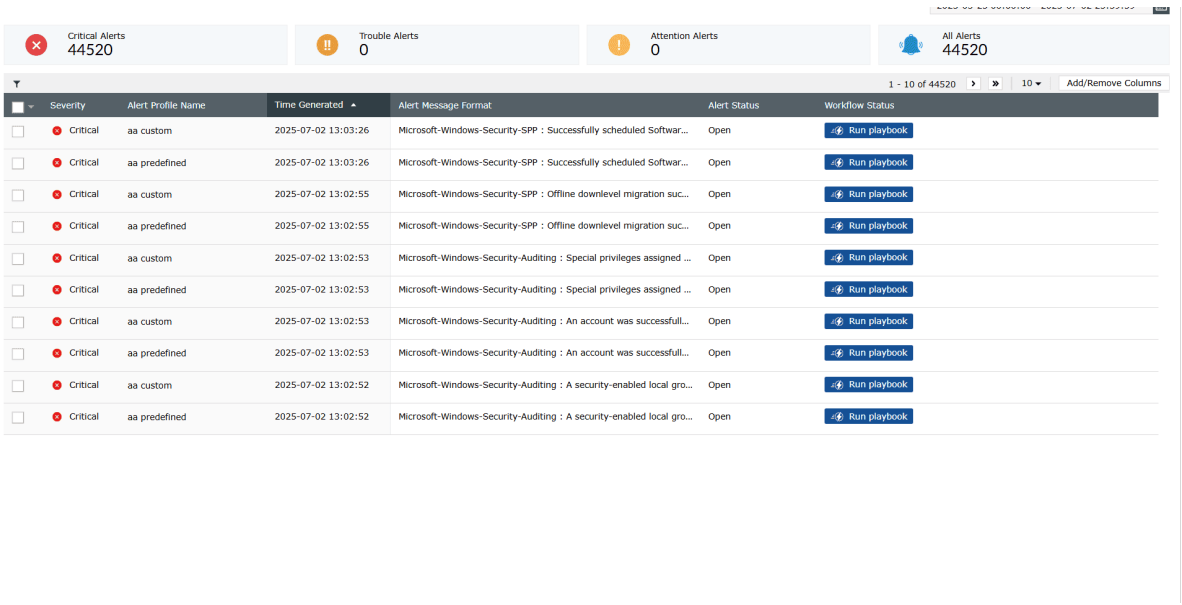
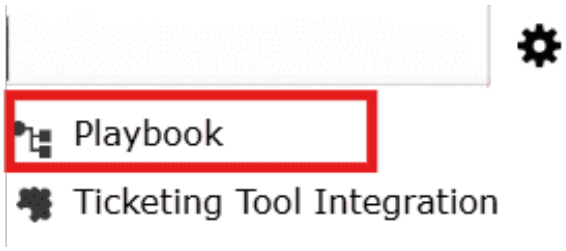


Image 1: More tools icon present in the Alerts tab

2. Click on Playbook to open the Manage Playbook page.



3. Click on the Playbook Credentials present in the Manage Playbook page.

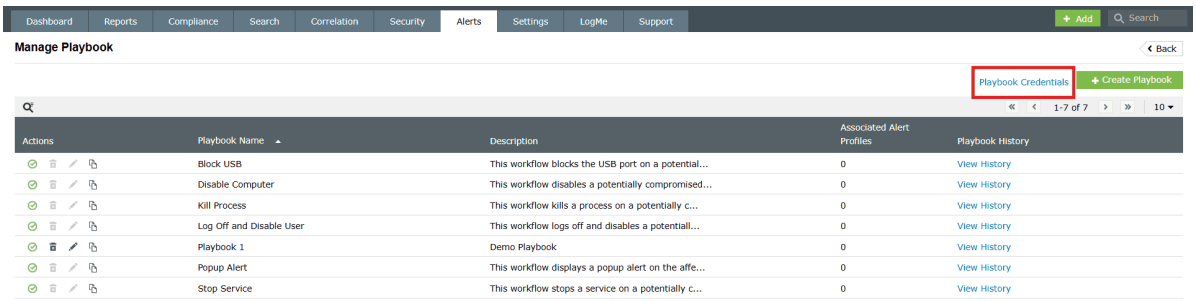
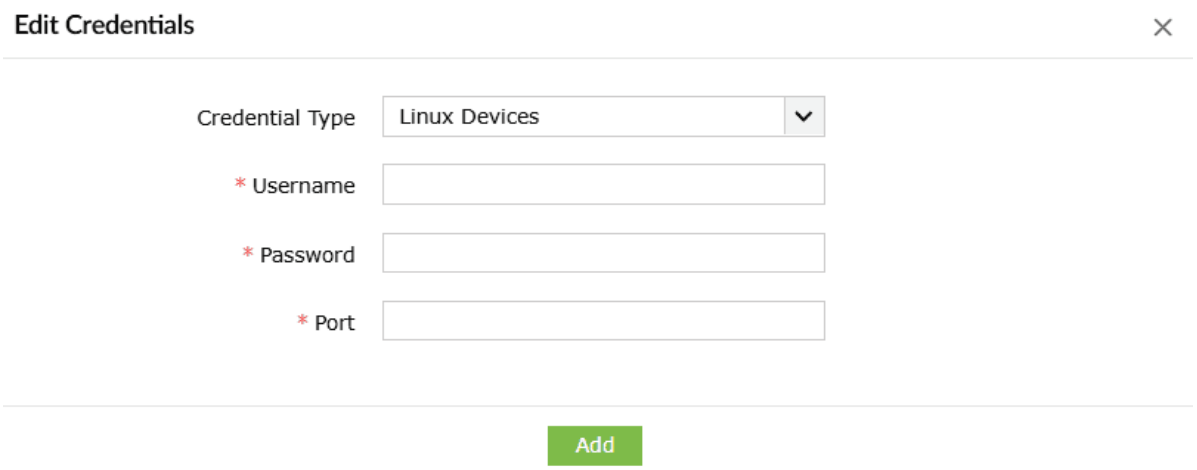
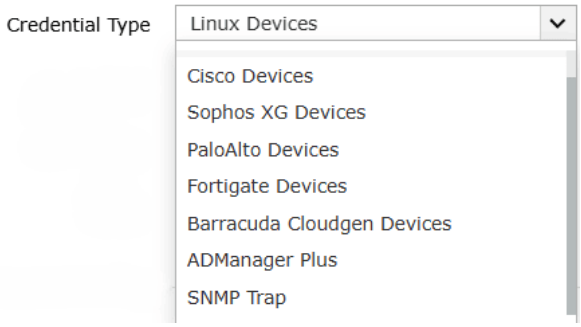


Image 2: Playbook credentials in the Alerts tab

4. When you click on Playbook Credentials, a pop-up appears to Edit Credentials.



5. Based on the device types, choose the Credential Type from the drop-down as shown below.



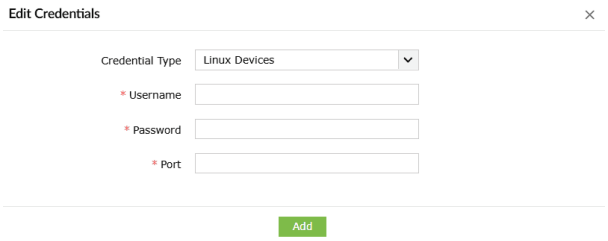
Continue reading to understand the step-by-step device specific guide to update playbook credentials.

To automate playbooks in Windows devices:

If the Windows devices have already been added to the product, playbooks can be executed by using the device credentials or the domain credentials of the devices. So, you need not manually update credentials for Windows devices.

To automate playbooks in Linux devices:

You can configure a set of common credentials for executing playbooks on all Linux devices.



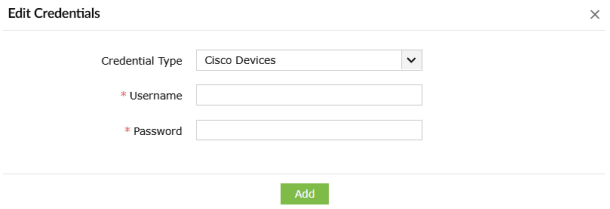
1. Enter the Username, Password, and Port number.
2. Click on Add to store and use these credentials to execute playbooks on all Linux devices.

To automate playbooks in Cisco devices

You must configure the REST API agent in the Cisco firewall to execute playbooks by following the steps given

in this link. (The Cisco REST API supported versions are listed here).

You can configure a set of common credentials for executing playbooks in all Cisco devices as elaborated below:



1. Enter the Username and Password.
2. Click on Add to store and use these credentials to execute playbooks on all Cisco devices.

If the common credentials do not work for certain Cisco Devices

You need to configure the credentials for those devices by following the steps given below:

1. In the product console, navigate to Settings → Devices.

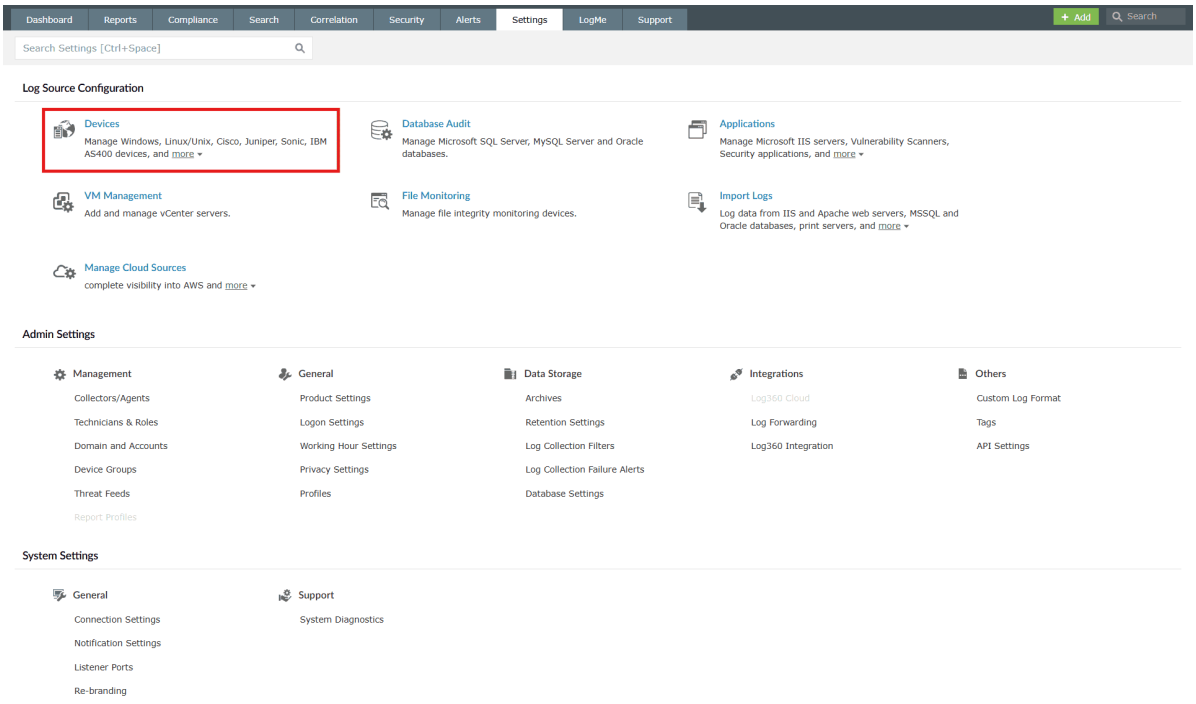


Image 3: Device settings via the Settings tab

2. Go to the Syslog Devices tab and hover your mouse pointer near the device on which you want to execute playbooks and click on the Edit icon.

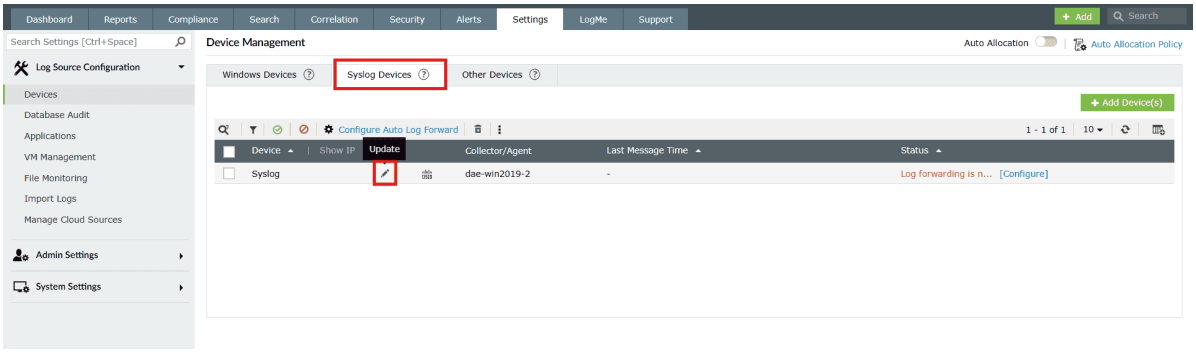
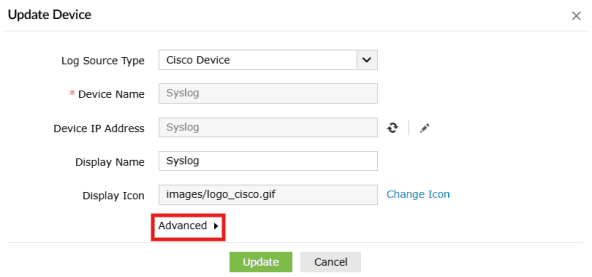
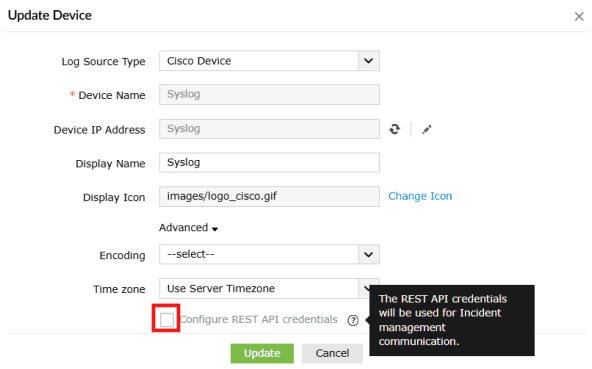


Image 4: Update Syslog device settings via the Settings tab

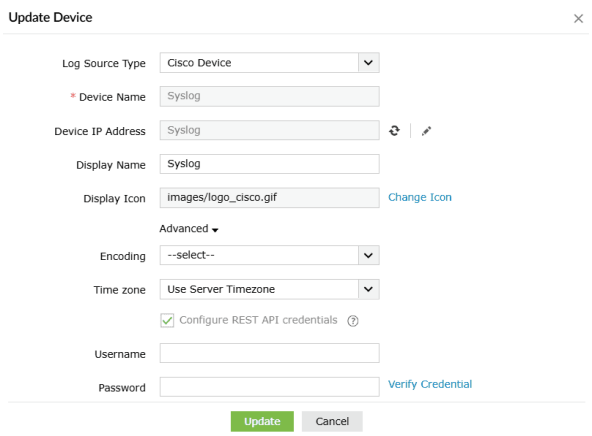
3. In the Update Device pop-up menu, click on Advanced.



4. Select the Configure REST API Credentials check box.



5. Enter a Username and Password and click on Verify Credential to send a REST API call to the Cisco device to verify if the credentials are valid. Once the verification is complete, click on Update to store and use the specified credentials for executing playbooks.



To automate workflows in Fortigate devices

In order to generate an API token to execute playbooks on Fortigate devices, you need to create a new REST API Admin on your device using the steps given below:

Phase 1: Create Administrator profile

1. Navigate to System from the sections listed on the left in the dashboard.
2. Click on the Admin Profiles under the System section.
3. Click the Create icon to start creating a new admin profile.
4. You will see the New Admin Profile window open.
5. Enter an appropriate name for your admin profile.
6. Select access control permissions for different functionalities between None, Read, Read/Write or Custom.
7. Select Read/Write for both Policy and Address options under Firewall Option.
8. Click OK to create your new admin profile

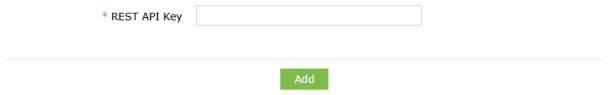
Phase 2: Create a REST API Admin and generate an API key

1. Navigate to System from the sections listed on the left in the dashboard.
2. Select Administrators under the System section.
3. Click on the Create New icon.
4. Select the REST API Admin option.
5. You will see the New REST API Admin window open.
6. Enter an appropriate username for your REST API admin profile.
7. Select your previously created Administrator Profile from the drop-down menu.
8. Click on OK to confirm your New REST API Admin .
9. Once you are done with this process, the system will automatically generate a new API key, which will be displayed only once.
10. Copy the generated API key before shutting it down.

> **NOTE**
>
> In case you lose your newly generated API key, you can go back to the Administrator section and click on the Regenerate icon.

After this process, You can configure a set of common credentials for executing playbooks in all Fortigate devices by following the steps given below:





1. Enter the Username and the REST API Key.
2. Click on Add to store and use these credentials to execute playbooks on all Fortigate devices.

To automate playbooks in PaloAlto devices

Pre-requisites:
To execute playbooks successfully, API access should be enabled by following the steps given below.
Phase 1:

1. Choose an Admin Role profile.
2. Navigate to Device → Admin Roles and either pick an existing role or set up a new one.

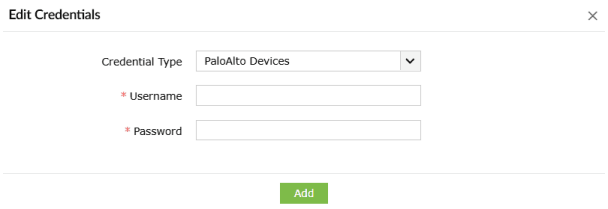
Phase 2:

1. Define the permissions available for the selected admin role.
2. Open the XML API section.
3. Turn on or off specific XML API capabilities like Report, Log, and Configuration.
4. Click OK to apply and save your changes.

Phase 3:
Assign the configured admin role to the desired administrator account.
Please note that the required permissions for the user under XML API are:

- Configuration
- Operational Requests
- Commit

You can configure a set of common credentials for executing playbooks in all PaloAlto devices by following the steps given below:

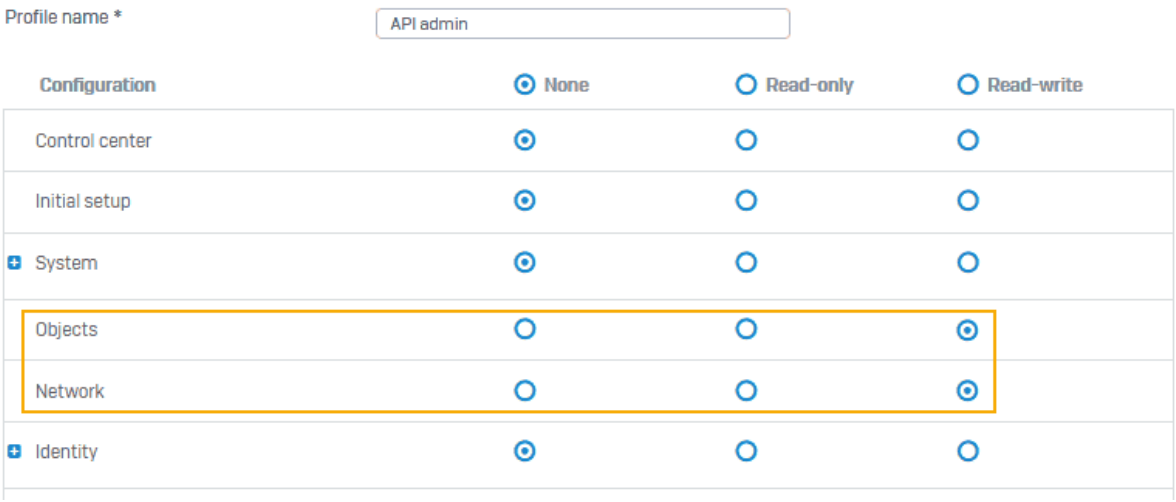


1. Enter the Username and Password.
2. Click on Add to store and use these credentials to execute playbooks on all PaloAlto devices.

To automate playbooks in SophosXG devices

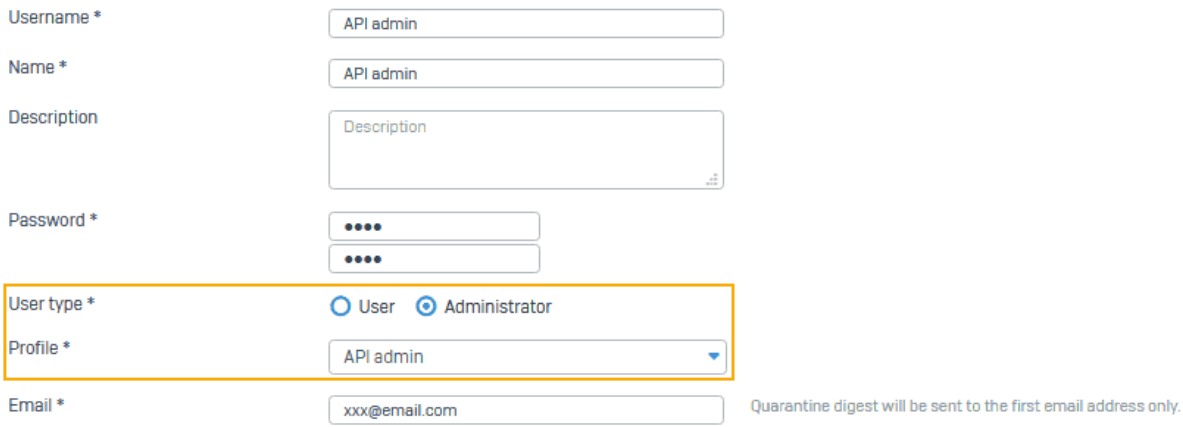
You must configure the encrypted password to execute playbooks on SophosXG devices. You can generate the encrypted password using the steps given below:
Phase 1: Create an administrator profile
Log in to your Sophos application and create an administrator profile with read-write permission for objects and network

1. Go to Profiles > Device access and create an administrator profile with specific rights.
2. Click Save.



Phase 2: Create an administrator

1. Create a user and add the administrator profile.
2. When you add a user with the API administrator profile, you can limit the administrator's rights based on the profile. Alternatively, you can use an existing administrator account.
3. Go to Authentication > Users and click Add.
4. Set User type to Administrator.
5. Select the API administrator profile created in step 1.
6. To allow access for a specific time, select the Access time.
7. To allow access only from specific IP addresses, select an option for Login restriction for device access.
8. Click Save.

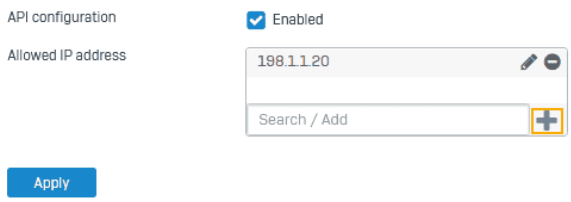


Phase 3: Allow API access

Turn on API configuration and allow API access from the administrator's IP address:

1. Go to Backup and firmware > API.
2. Select API configuration.

3. For Allowed IP address, enter the IP address from which you'll make the API request and click the add icon.
4. Click Apply.

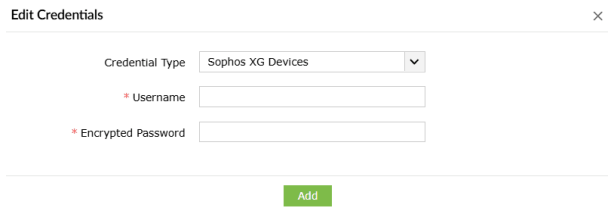


Phase 4: To generate encrypted password

1. Log in to advanced shell in the firewall.
2. Execute the following command:
   -aes-128-cbc-tool -k Th1s1Ss1mPlygR8API -t 1 -s <password>-
3. Copy the password and use it in the API configuration.

> NOTE
>
> The product will continue to support Sophos XG devices up to SFOS v19.0.
> If you wish to integrate with newer versions of Sophos XG, please contact us. We can make the necessary adjustments in the database to accommodate the new API credentials mechanism.
> All Sophos-related actions will continue to be supported.

After generating the encrypted password, you can configure a set of common credentials for executing playbooks in all SophosXG devices by following the steps given below:



1. Enter the Username and Encrypted Password.
2. Click on Add to store and use these credentials to execute playbooks on all SophosXG devices.

To automate playbooks in Barracuda CloudGen devices

In order to execute playbooks in Barracuda CloudGen devices, you need to create an X-API Token using the steps given below:

Phase 1: Enable the REST API for HTTPS

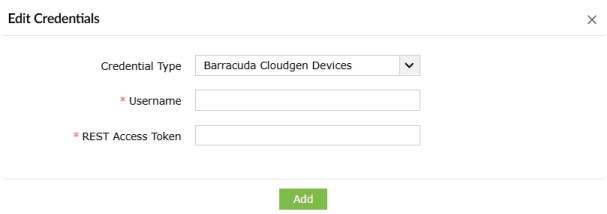
1. Navigate to CONFIGURATION > Configuration Tree > Box > Infrastructure Services > REST API Service.
2. Click the Lock button to enable editing.
3. In the HTTP interface section, enable the HTTPS interface option.
4. Specify the port number you'd like to use for API requests in the HTTPS Port field.

5. (Optional) To allow API requests through management IPs rather than the loopback address, enable the Bind to Management IPs setting.
6. Click New Key to generate a private key of your preferred key length, or import your existing key.
7. Click Ex/Import to either generate a self-signed certificate or upload an already existing one.

> NOTE
>
> Ensure that the certificate's common name matches the URI of your API request. For instance, if you're sending a request to https://CGF1.example:8443, the common name in the certificate should be CGF1.example.

Phase 2: Create an administrator profile for REST API authentication.
To authenticate with the REST API, a user account with the required privileges must exist, either in the Control Center for centrally managed firewalls or directly on the individual firewall for standalone setups. This user must hold the Manager role in both scenarios.
If you need a read-only user, you can duplicate the Observer role under the Control Center's Administrative Roles section, enable the Access to REST API option, and then create a new user under CC-Admin with this custom role assigned.
Phase 3: Create an X-API Token for authentication.
1. Navigate to CONFIGURATION > Configuration Tree > Box > Infrastructure Services > REST API Service.
2. Select Lock to begin editing.
3. From the left-hand panel, choose Access Tokens.
4. Click the + icon in the Access Tokens area.
5. Provide a name for the new token and click OK to proceed.
6. In the window that appears, click Generate New Token.
7. Specify the Admin username that will be used for authentication.
8. Set the validity period in days under the Time to live field.
9. Click OK to finalize and create the token.

After finishing the process, you can configure a set of common credentials for executing playbooks in all Barracuda CloudGen devices by following the steps given below:



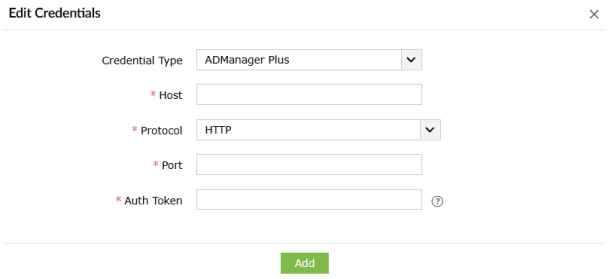
1. Enter the Username along with the generated REST Access Token.
2. Click on Add to store and use these credentials to execute playbooks in all Barracuda CloudGen devices.

Automating playbooks in ADManager Plus

ADManager Plus , an IGA solution with hybrid Active Directory management, reporting, and automation capabilities, must be integrated with Log360 for the successful execution of response playbooks. The list of actions that can be added to the playbook are called playbook blocks. These actions include:

- Enabling, disabling, updating, and deleting a user
- Enabling, disabling, and deleting a computer
- Resetting a user's password
- Adding to, and removing users from a group

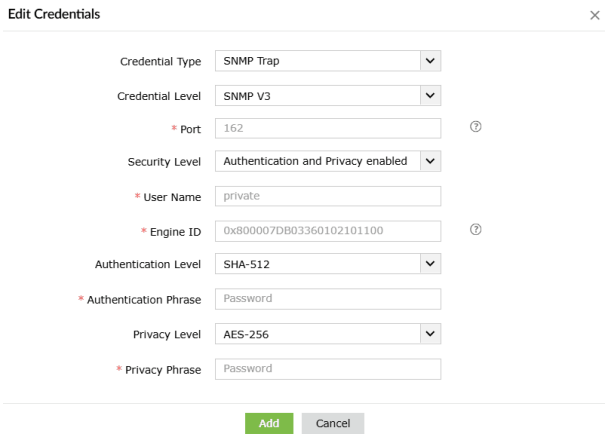
Only after the integration is complete can any of these actions be carried out.
You can set up an integration in the product to execute actions via ADManager Plus. Here are the steps:



1. After selecting the credential type as ADManager Plus, fill in the required details about the Host, Protocol, Port and Auth Token.
2. Click on Add, to integrate ADManager Plus with the product.

Automating playbooks in SNMP TRAP

To automate all SNMP Trap playbooks, you can configure a common credential by following these steps:



1. After choosing SNMP Trap as the credential type, enter the SNMP credential.
2. Click Add to save. This credential will now be used to execute all SNMP Trap playbooks.

NOTE

Refer to the port management page for details on how to update credentials.

Read also

This document elaborated on a simple and step-by-step guide on how to update playbook credentials. If you're building workflows, explore how to create custom playbooks and assign device actions.

- Creating playbook
- Manage playbooks

10.3.3. Ticketing Tool configuration

Last updated on: September 12, 2025

With EventLog Analyzer, you can efficiently manage security incidents by raising tickets and assigning them to administrators for alerts that are generated. You can easily manage the incident within the EventLog Analyzer console itself or use an external help desk software for raising tickets. Under Alert Configurations, click on ticketing tool integration to configure an external help desk - ServiceNow, ManageEngine ServiceDesk Plus, ManageEngine ServiceDesk Plus On-Demand, ManageEngine ServiceDeskPlus MSP, ManageEngine AlarmsOne, Jira Service Desk, Jira Service Desk On-Demand, Zendesk, Freshservice, Kayako, or BMC Remedy Service Desk.

Manage Ticketing Tool Configuration

To configure incident management with ticketing tools, click on ticketing tool integration under Alert Configuration. From the Ticketing Tool drop-down list, select the ticketing tool that you want to configure EventLog Analyzer with. Then, follow the following steps based on the ticketing tool used.

For ManageEngine ServiceDesk Plus On-Demand:

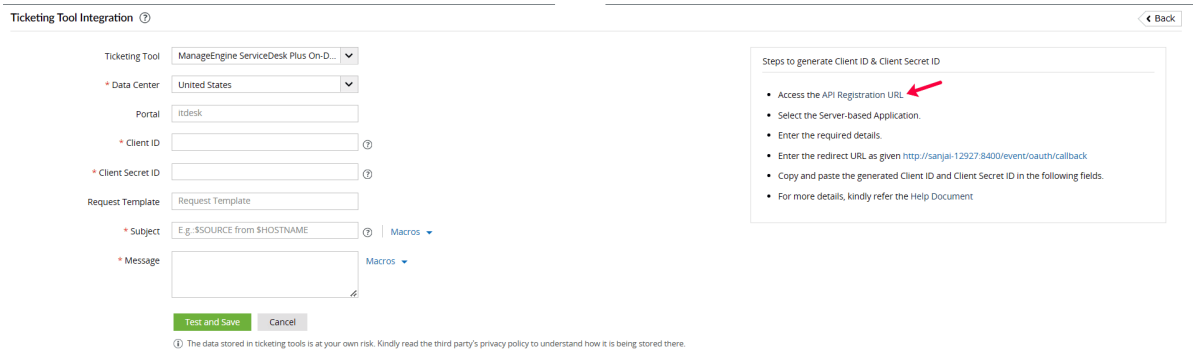
> **Note**
>
> Only users with permissions to view and edit requests can proceed with the configuration.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select ManageEngine ServiceDesk Plus On-Demand.

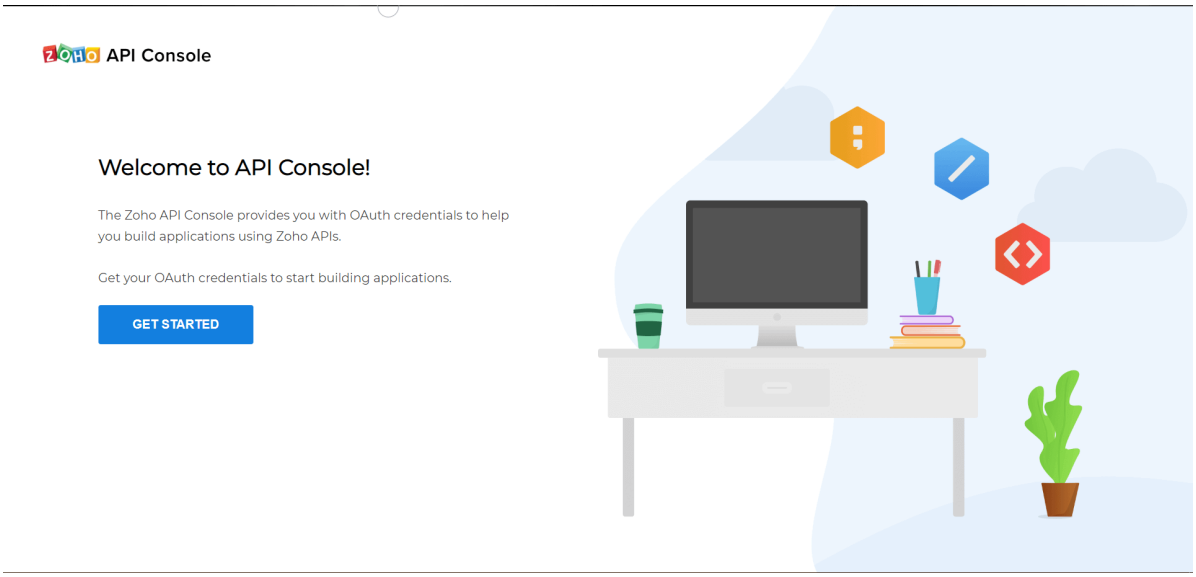
1. Choose the Data Center where your ServiceDesk Plus account is hosted. Kindly refer to the table below to find the corresponding Data Center for your ServiceDesk Plus account.

ServiceDesk Plus URL	Region	Data Center to be selected
https://sdpondemand.manageengine.com	United States	US
https://sdpondemand.manageengine.eu	Europe	EU
https://sdpondemand.manageengine.in	India	IN
https://servicedeskplus.cn	China	CN
https://servicedeskplus.net.au	Australia	AU

ServiceDesk Plus URL	Region	Data Center to be selected
~~https://servicedeskplus.jp~~	~~Japan~~	~~JP~~
https://servicedeskplus.ca	Canada	CA
https://servicedeskplus.uk	United Kingdom	UK
https://servicedeskplus.sa	Saudi Arabia	SA

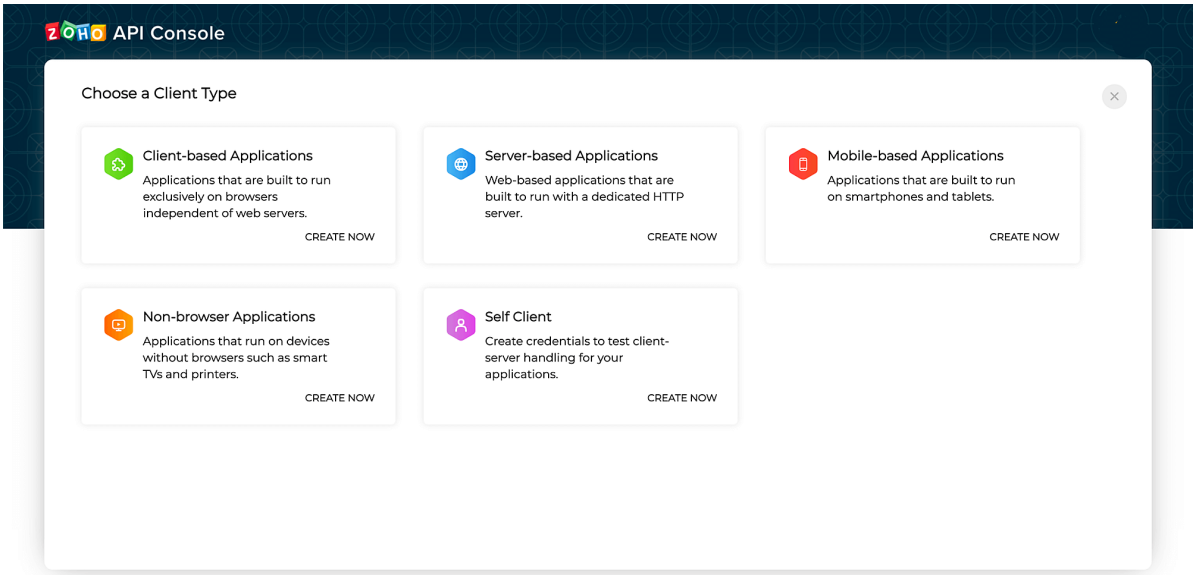


2. Click the API Registration URL to generate the Client ID and Client Secret ID.
3. Once the Zoho API Console is opened, click GET STARTED.

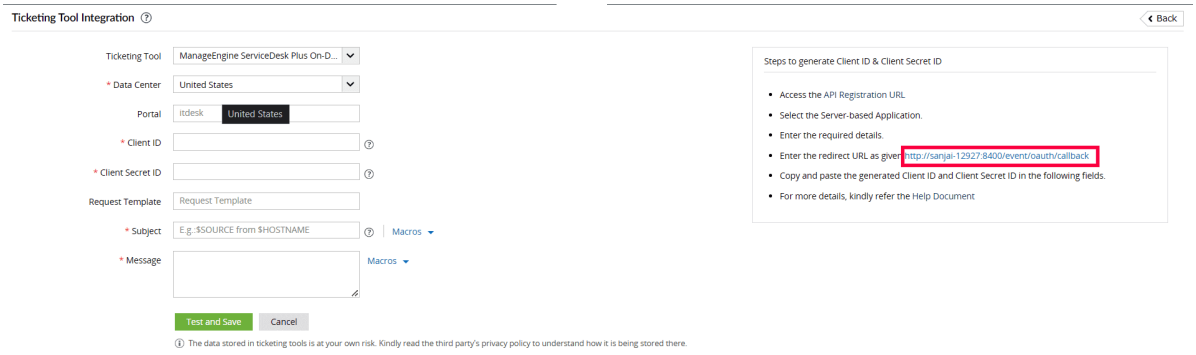


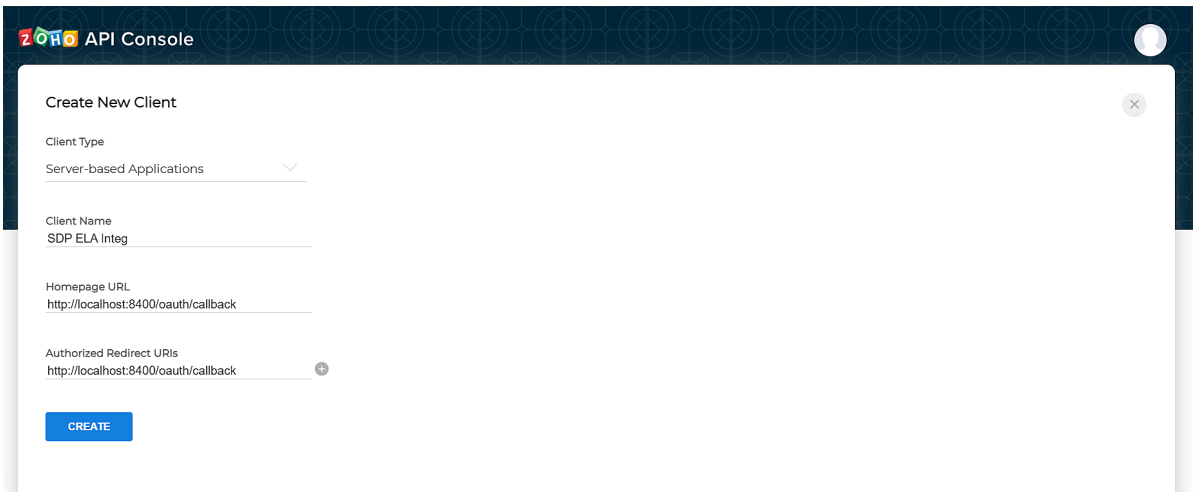
4. Select the Server-based Applications tile.



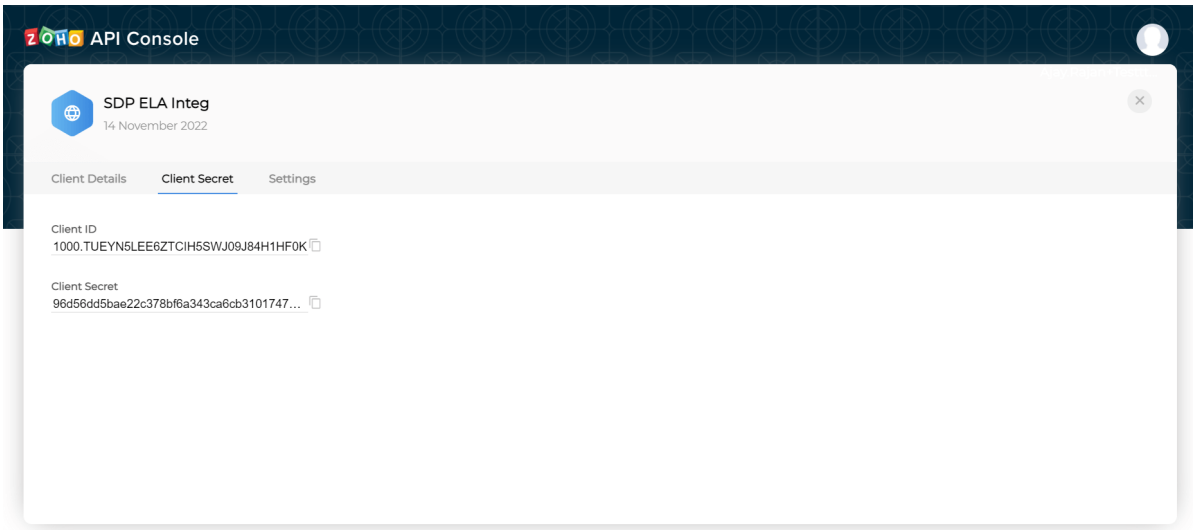


5. To create a new client, enter the required details. Enter the redirect URL as given in the EventLog Analyzer console and click Create.

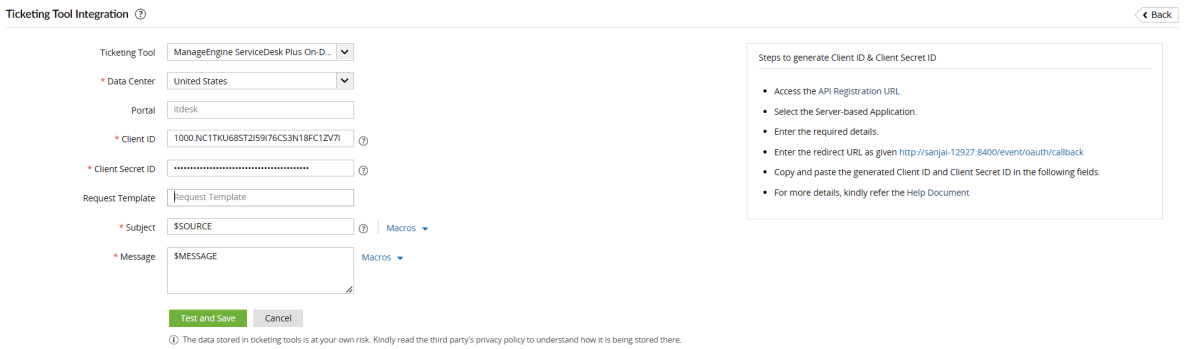




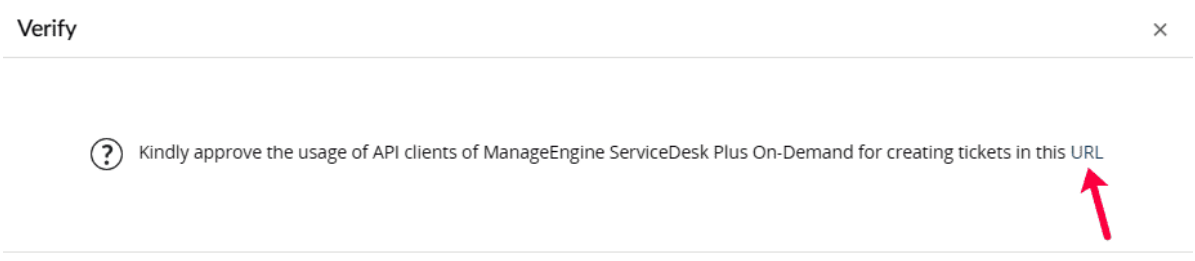
6. Copy the generated Client ID and Client Secret ID.



7. Back in the ELA console, paste the Client ID and Client Secret ID in the corresponding fields.

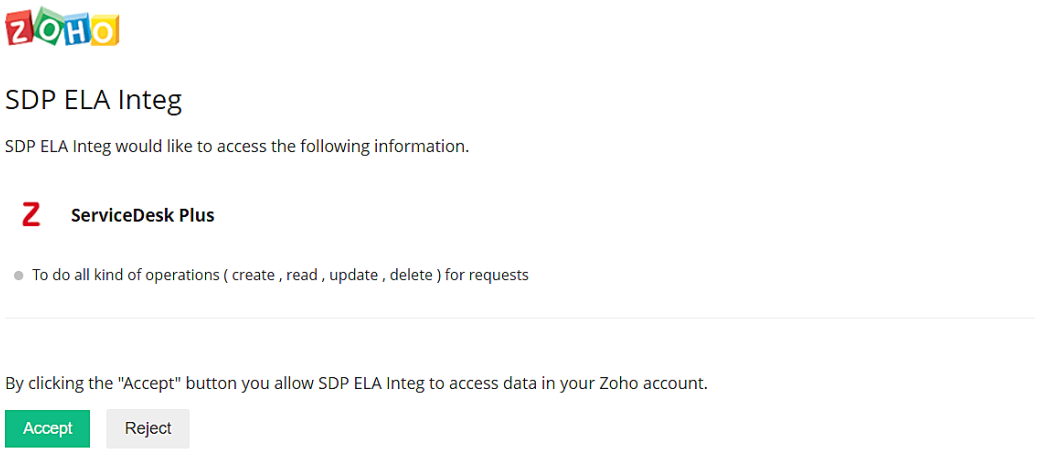


8. Please specify the Request Template you want to use for creating tickets in ServiceDeskPlus OnDemand. Leaving it empty would raise tickets using the Default Template.
9. Provide the Subject and Message for the alert—these can be selected from a predefined list under Macros or entered manually as per your requirements. Click the Test and Save button to proceed. Upon clicking, a verification popup will appear—click the URL provided to approve the integration with ServiceDesk Plus On-Demand clients.





10. Click Accept for API approval.



11. Click the Verify button in ELA console. The ticketing tool will now be configured successfully.

> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

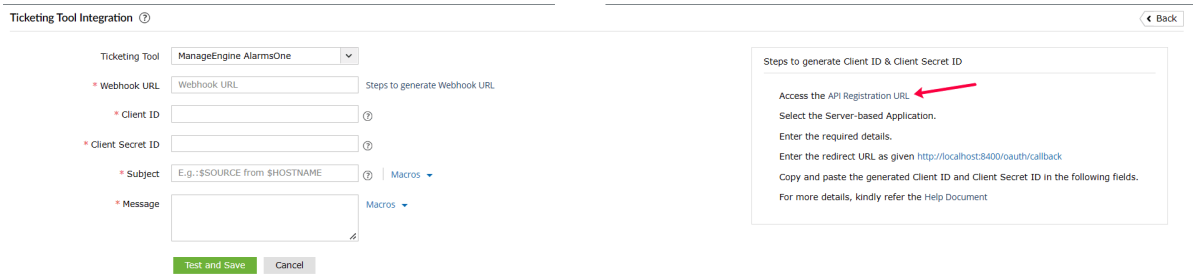
For ManageEngine AlarmsOne

> **Note**
>
> Only users with the super admin or the alarm admin role can proceed with the configuration.

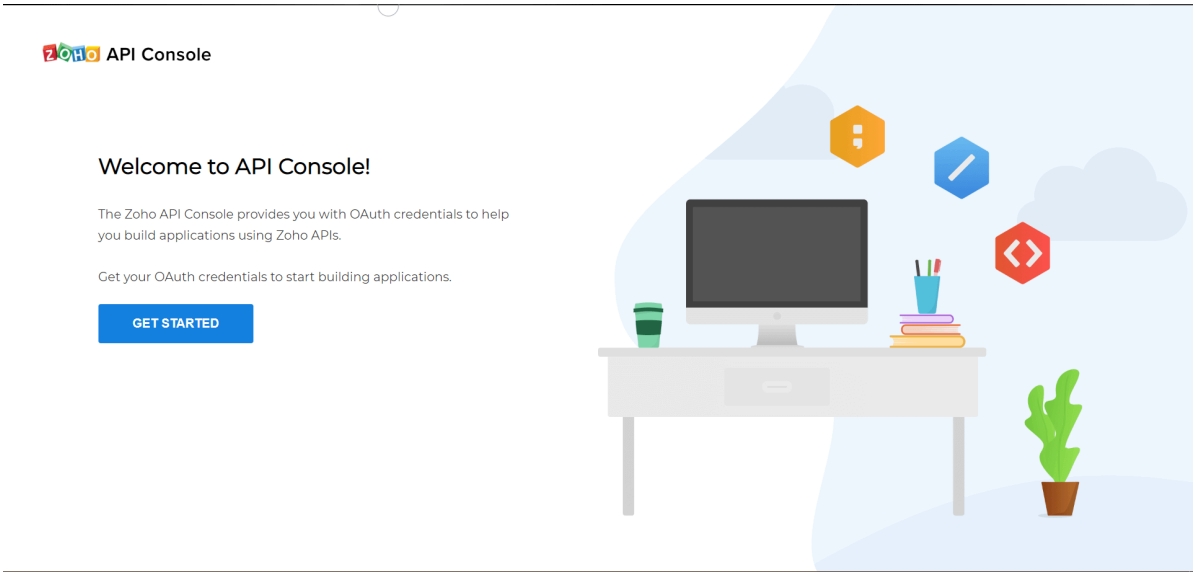
In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select ManageEngine AlarmsOne.

1. Open ManageEngine AlarmsOne and click the Applications icon, then click Applications(+) button in the left panel. From the list displayed, select Custom API Integration.
2. Enter an Application Label and Application Name. If a notification profile is already configured, select it. Click Add. You can also associate a notification profile later.
3. A Webhook URL specific to your custom app is generated.
4. Click API Registration URL in EventLog Analyzer to generate a Client ID and Client Secret ID.

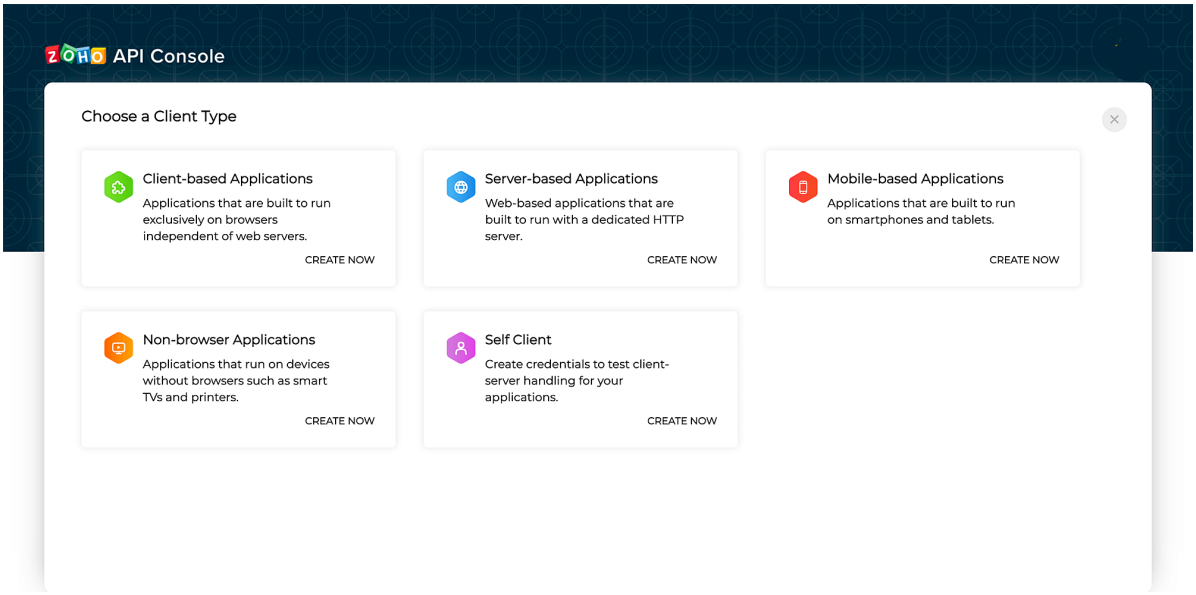
4. Click API Registration URL in EventLog Analyzer, to generate a Client ID and Client Secret ID.



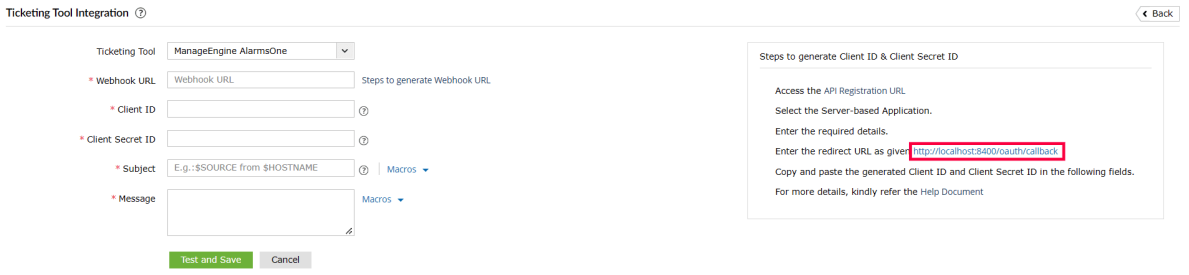
5. Once the Zoho API Console is opened, click GET STARTED.



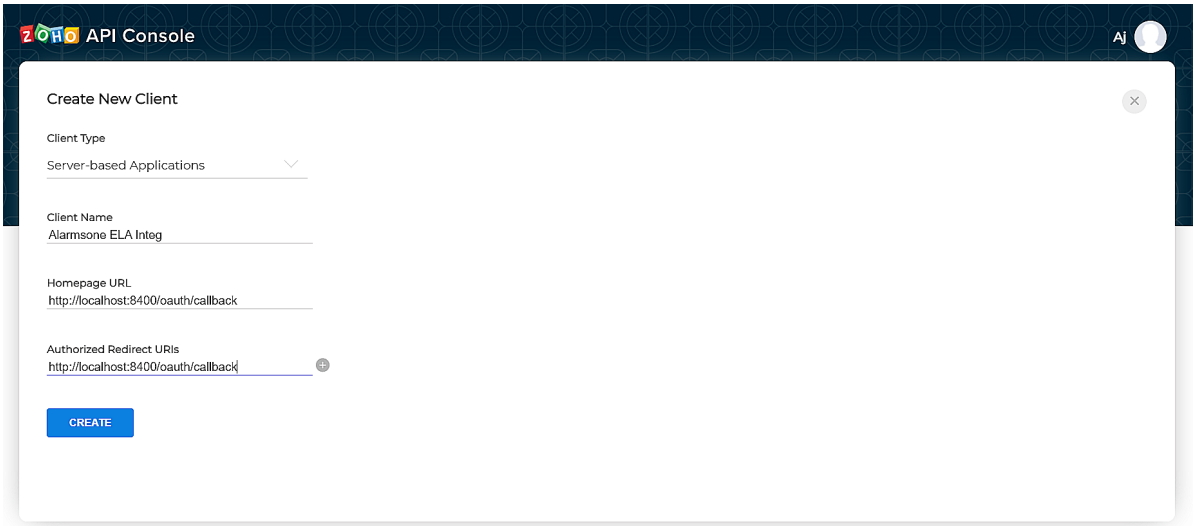
6. Select the Server-based Applications tile.



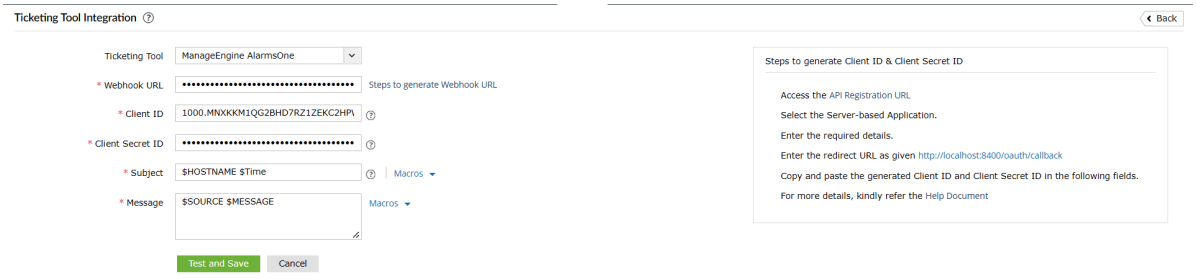
7. To create a new client, enter the required details. Enter the redirect URL as given in the EventLog Analyzer console and click Create.



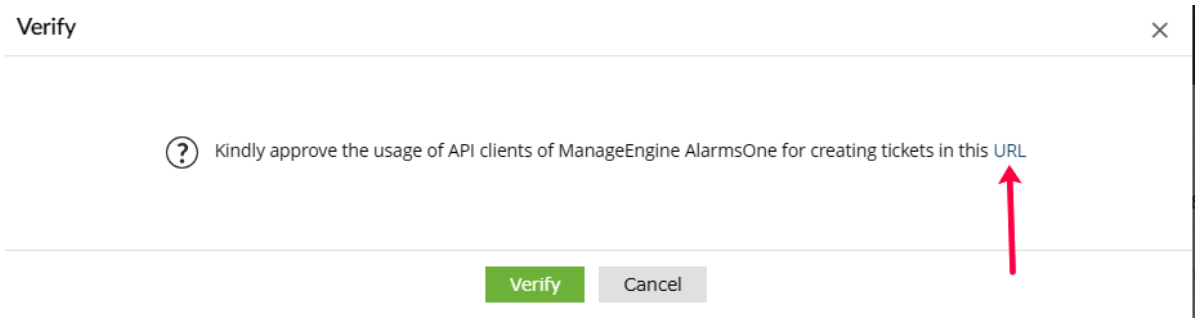
8. Copy the generated Client ID and Client Secret ID.



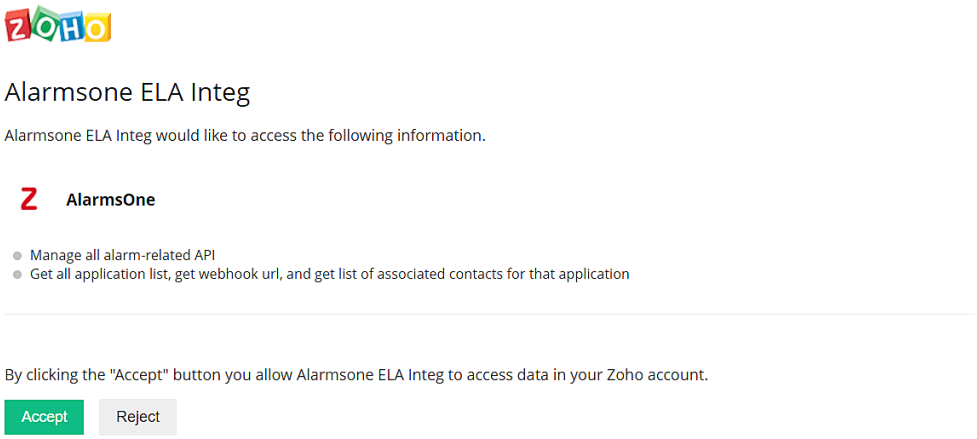
9. Back in the ELA console, paste the Webhooks URL, Client ID, and Client Secret ID in the required fields.



10. Enter the Subject and the Message for the alert. You can select them from the predefined list available under Macros or type your own. Click the Test and Save button. On clicking the Test and Save button, a verify popup will be displayed. Click the URL to approve the usage of the clients of ManageEngine AlarmsOne.



11. Click Accept for API approval.



Click Verify button in ELA. The ticketing tool will now be configured successfully.

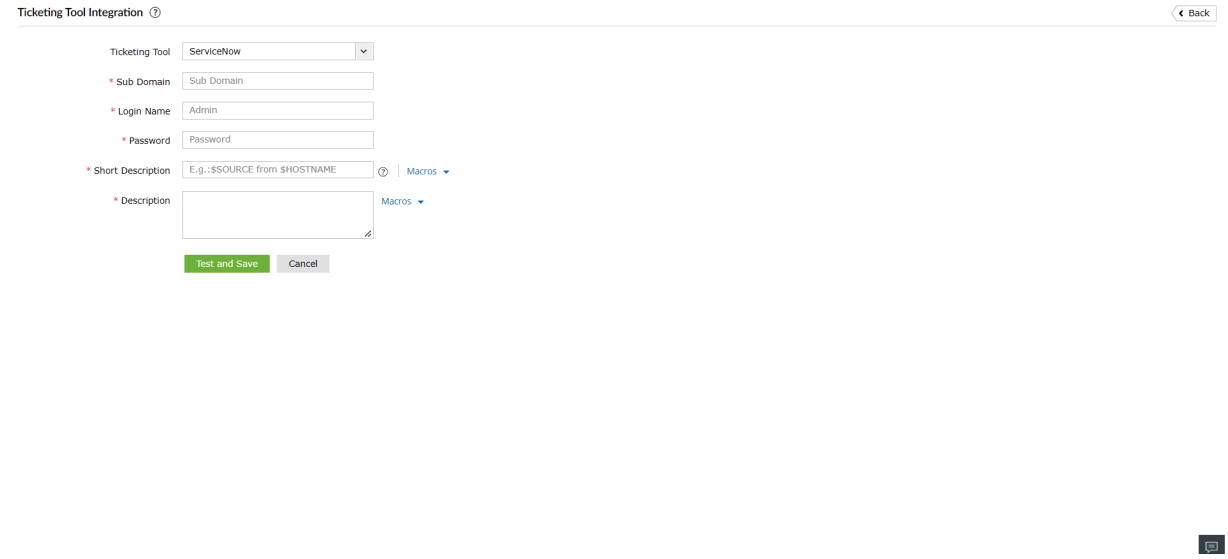
> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For ServiceNow

> **Note**

Only users with permissions to view and edit requests can proceed with the configuration.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select ServiceNow.



1. Enter the ServiceNow subdomain name or IP address.
2. Enter the login name and password of a valid account in the ticketing tool.
3. Enter the Short Description and the Description for the alert. You can select them from the predefined list available under Macros or type your own.
4. Click the Test and Save button to establish communication and complete configuration.

> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For JIRA Service Desk On-Demand

> **Note**
>
> Only users with permissions to view and edit requests can proceed with the configuration.

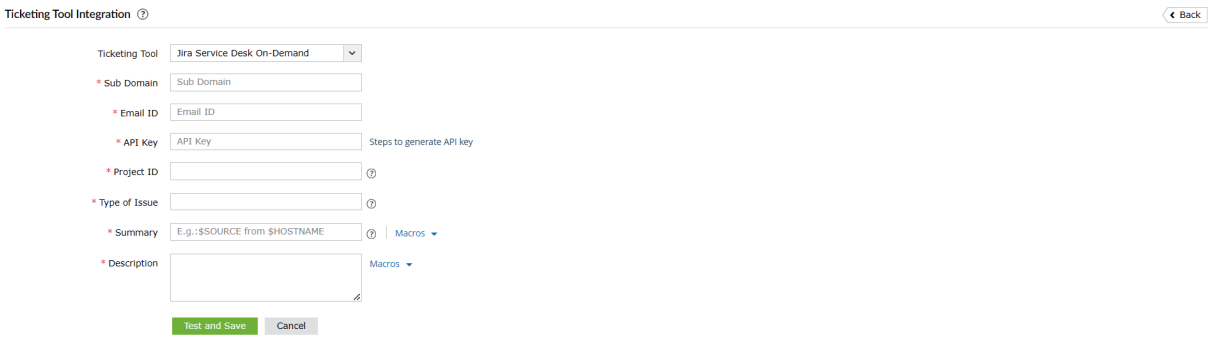
To configure EventLog Analyzer with Jira Service Desk On-Demand, you need to first get some details from your Jira ticketing tool. Go to the Official JIRA Cloud Doc to get the API Token.

1. After logging into your Jira Service Desk On-Demand account, click the settings icon on the top right corner

and select Projects.

2. In the project list, note down the Key corresponding to the project in which you want your tickets to be raised.
3. Click the settings icon on the top right corner and select Issues.
4. Note down the type of issues that the particular project can hold. The issues raised from EventLog Analyzer should have the same type for a ticket to be successfully raised in Jira Service Desk On-Demand.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select Jira Service Desk On-Demand.



1. Enter the Jira Service Desk On-Demand Subdomain.
2. Enter your JIRA Account Email ID.
3. Enter the API key that we got in the previous step.
4. Enter the Project ID. This is the Key of the particular project noted from the ticketing tool.
5. Enter the type of issue. This has to be the same issue type that the project has been configured to hold.
6. Enter the Summary and the Description for the alert. You can select them from the predefined list available under Macros or type your own.
7. Click the Test and Save button to establish communication and complete configuration.

> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For Zendesk

> **Note**

Only users with Admin/Agent privilege can proceed with the configuration.

Configuring Zendesk with OneAuth authentication:

> **Note**
>
> If your EventLog Analyzer server is running on HTTP, you can configure Zendesk using OAuth only from the installed machine.

To configure EventLog Analyzer with Zendesk, you will need to retrieve some information from your Zendesk ticketing tool:

1. After logging into your Zendesk account, click the tray icon in the top bar and click Admin Center.
2. In Admin Center, click Apps and integrations in the sidebar > select APIs > Zendesk API > OAuth Clients.
3. Click the + icon to create a new OAuth Client
4. Enter the client name, description, and name of the company. Select a logo.
5. Select Confidential for Client Kind field.
6. Enter the redirect URL as given in the EventLog Analyzer console in Redirect URLs field.
7. Copy the value that appears corresponding to Unique Identifier and save it in a separate document.
8. Once you click Save, a secret code will appear above the Save button. Click Copy and save it in a separate document. This would also be needed while configuring Zendesk in EventLog Analyzer.
9. Click Close and open EventLog Analyzer to complete the configuration process.

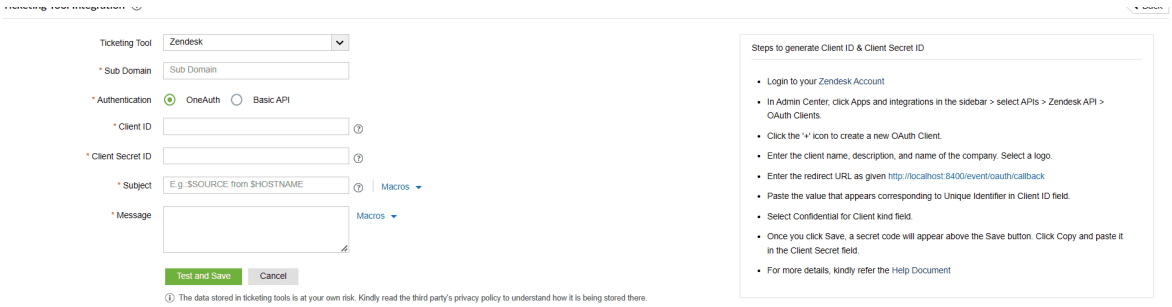
Configuring Zendesk with Basic API authentication:

1. Click the Admin icon in the sidebar, then select Channels → API.
2. Click the Settings tab, and make sure Token Access is enabled.
3. Click the + button to the right of Active API Tokens.
4. Optionally, enter a description under API Token Description. The token is generated, and displayed.
5. Copy the token, and paste it somewhere secure. Once you close this window, the full token will never be displayed again.
6. Click Save to return to the API page. A truncated version of the token is displayed.

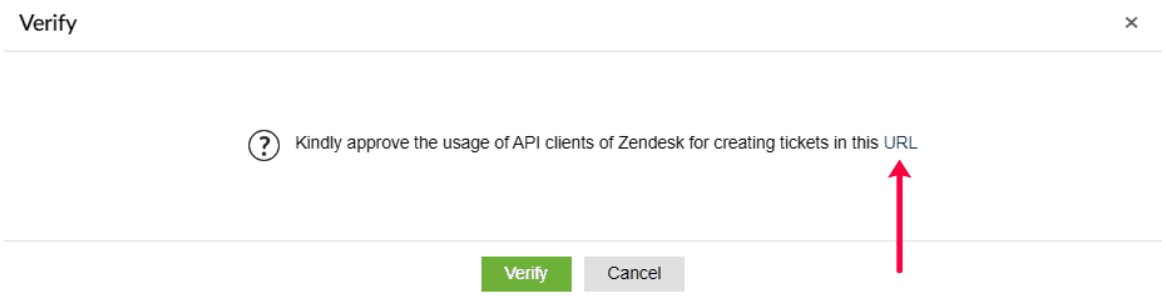
Configuration in EventLog Analyzer for Zendesk integration:

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select Zendesk.

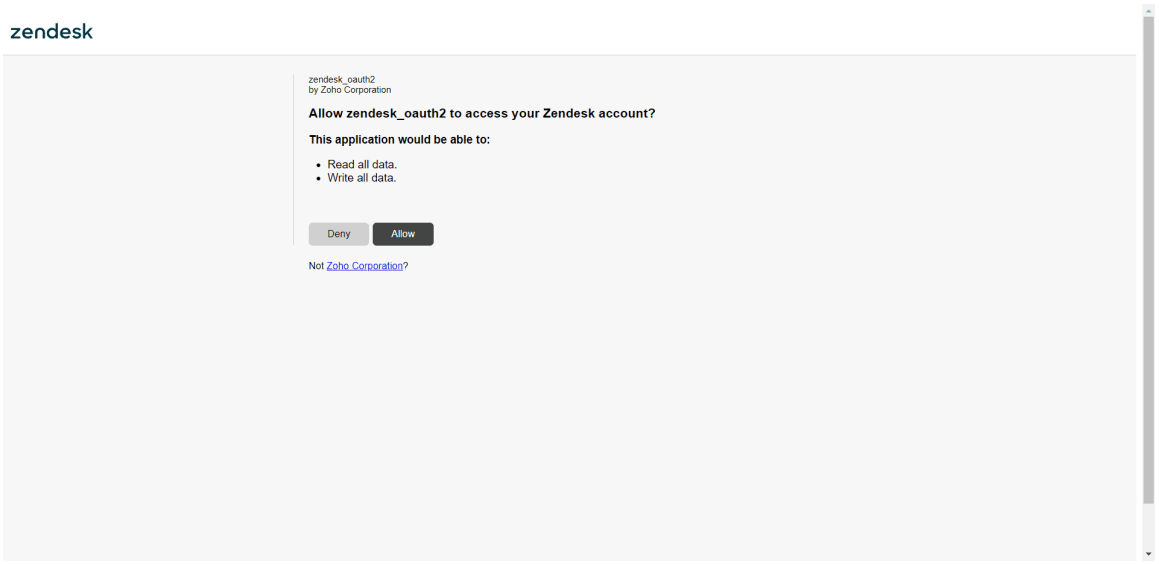
1. Enter the Zendesk subdomain name in the given field.
2. Under Authentication, you can choose either OneAuth or Basic API.
3. If you choose OneAuth under Authentication, follow the steps given below.



- Enter the Client ID in the corresponding field. This is value of the Unique Identifier noted from the ticketing tool.
- Enter the Client Secret ID in the corresponding field. This is the value of the secret code obtained from the ticketing tool.
- Enter the Subject and the Message for the alert. You can either select them from the predefined list available under Macros or enter your own. Click the Test and Save button. On clicking the Test and Save button, a verify popup will be displayed. Click the URL to approve the usage of the clients of Zendesk.

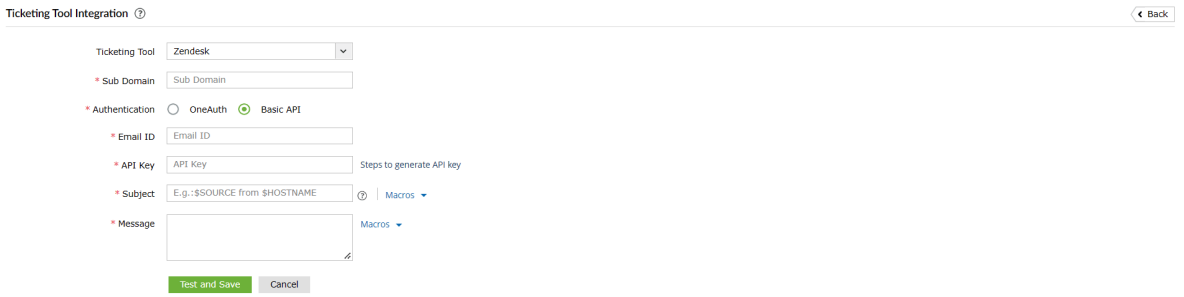


- Click Allow for API approval.



- Click the Verify button in EventLog Analyzer console. The ticketing tool will now be configured successfully.

4. If you choose Basic API under Authentication, follow the steps given below:



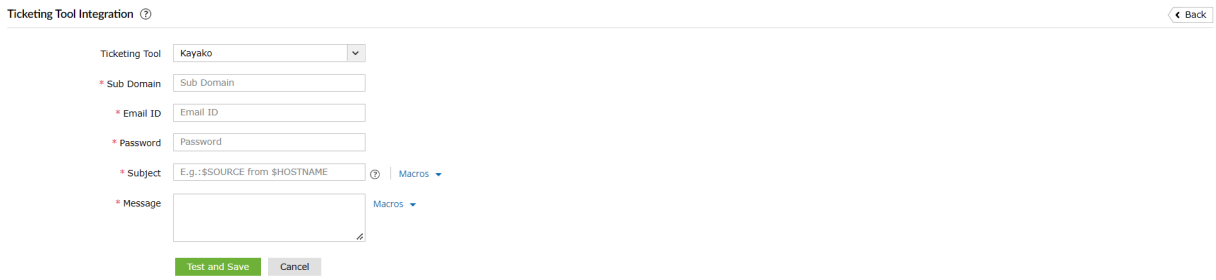
- Provide the Email Id in the given field.
- Click on Steps to Generate API Key for steps to generate an API key.
- Follow the given steps to generate the API key. After generation, provide the API key in the corresponding field.

5. Enter the Subject and the Message for the alert. You can select them from the predefined list available under Macros or provide your own.
6. Click the Test and Save button to establish communication and complete configuration.

> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For Kayako

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select Kayako.



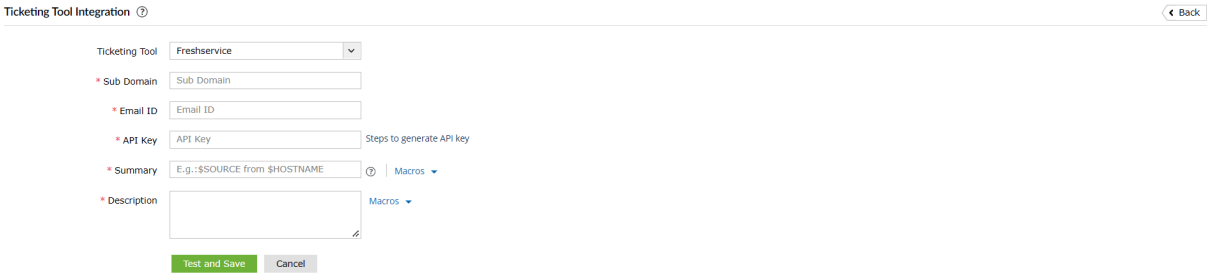
1. Enter the Kayako subdomain name.
2. Enter the emailId and password of a valid user in the ticketing tool.
3. Enter the Subject and the Message for the alert. You can select them from a predefined list available under Macros or type your own.
4. Click the Test and Save button to establish communication and complete configuration.

> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For FreshService

> **Note**
>
> Only users with either of the following privileges can proceed with the configuration:
>
> - Permissions to create, reply, edit, and delete tickets.
>
> Or
>
> - SD Agent, SD Supervisor, Admin, or Account admin role.

To configure EventLog Analyzer with FreshService, you need to first get some details from your FreshService ticketing tool. Go to the official Freshservice Doc to get the API Token.
In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select Freshservice.



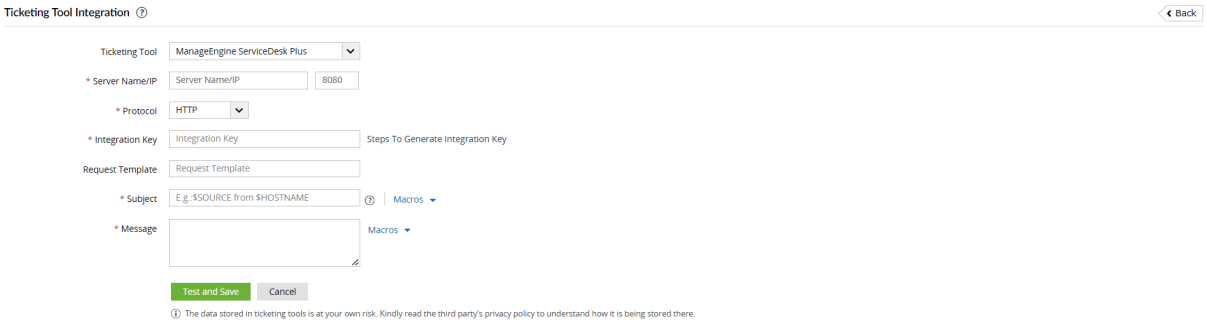
1. Enter the Freshservice Subdomain.
2. Enter Freshservice account Email ID.
3. Enter the API key that we got in the previous step.
4. Enter the Summary and the Description for the alert. You can select them from the predefined list available under Macros or type your own.
5. Click the Test and Save button to establish communication and complete configuration.

> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For ManageEngine ServiceDesk Plus

> **Note**
>
> Only users with permissions to view and edit requests can proceed with the configuration.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select ManageEngine ServiceDesk Plus.



1. Enter the ManageEngine ServiceDesk Plus server name or IP address.
2. Enter the port number.

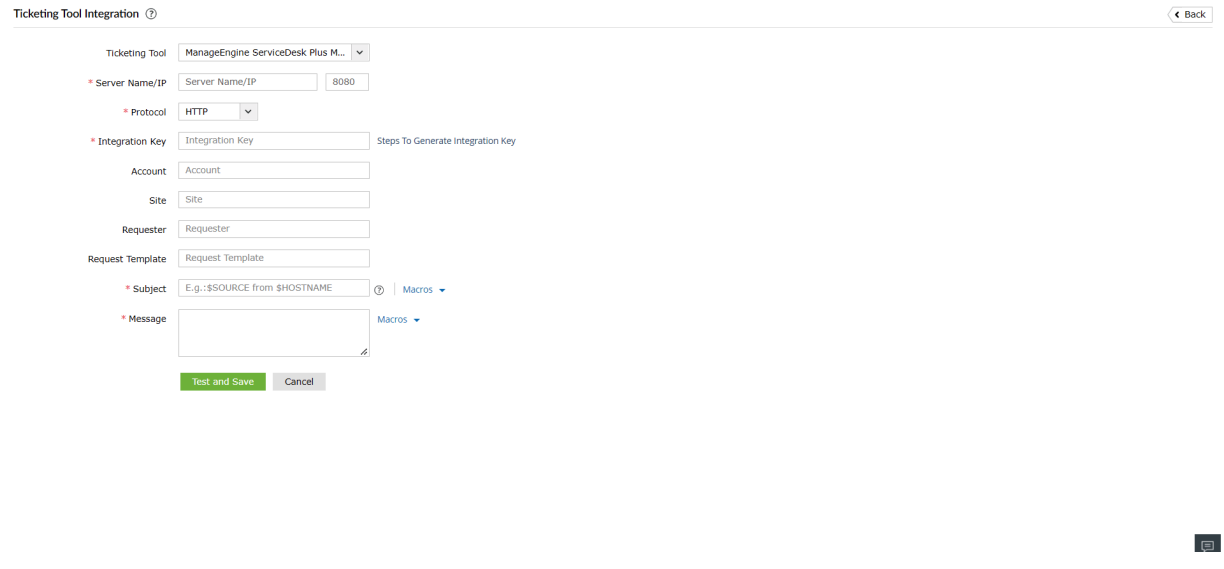
2. Enter the port number.
3. Choose the protocol for communication - HTTP/HTTPS.
4. Enter the Integration Key in the appropriate column. If you do not have an API key click on Steps to Generate API Key for instructions on generating an API key in ServiceDesk Plus.
5. Please specify the Request Template you want to use for creating tickets in ServiceDesk Plus. Leaving it empty would raise tickets using the Default Template.
6. Provide the Subject and Message for the alert—these can be selected from a predefined list under Macros or entered manually as per your requirements.
7. Click the Test and Save button.

> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For ManageEngine ServiceDesk Plus MSP

> **Note**
>
> Only users with permissions to view and edit requests can proceed with the configuration.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select ManageEngine ServiceDesk Plus MSP.



1. Enter the ManageEngine ServiceDesk Plus MSP server name or IP address.
2. Enter the port number.

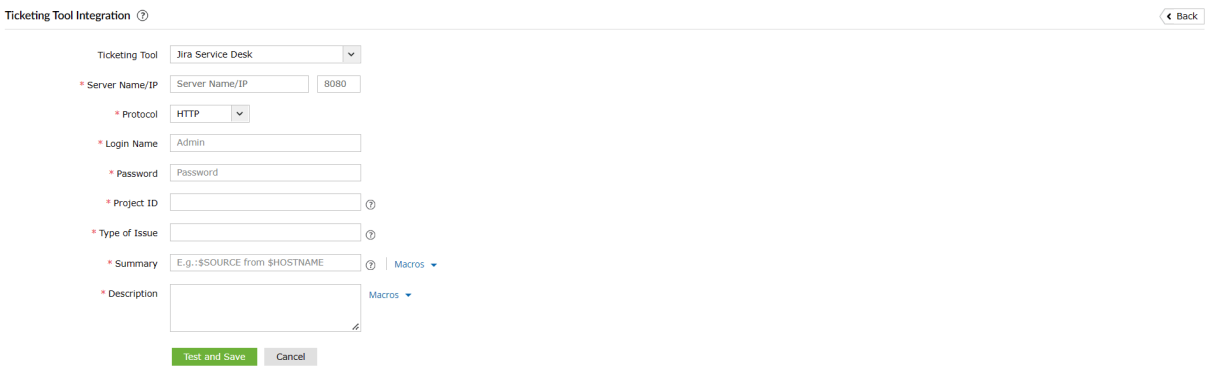
3. Choose the protocol for communication - HTTP/HTTPS.
4. Enter the API key in the appropriate column. If you do not have an API key, click Steps to Generate API Key for instructions on generating an API key in ServiceDesk Plus MSP.
5. If applicable, you may provide the following optional details:
   - Account – Denotes the account to which this request belongs
   - Site – Denotes the site associated with this request
   - Requester – Indicates the requester of the request
   - Request Template – Indicates the template used to create the request
6. Enter the Subject and the Message for the alert. You can choose them from the predefined list available under Macros or type your own.
7. Click the Test and Save button.

> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For JIRA Service Desk

To configure EventLog Analyzer with Jira Service Desk, you would first need to get a few details from your Jira ticketing tool.

1. After logging into your Jira Service Desk account, click the settings icon on the top right corner and select Projects.
2. In the project list, note down the Key corresponding to the project in which you want your tickets to be raised.
3. Navigate to the Issues tab and reenter your username and password when prompted.
4. Note down the type of issues that the particular project can hold. The issues raised from EventLog Analyzer should have the same type for a ticket to be successfully raised in Jira Service Desk.
5. Close Jira Service Desk and open EventLog Analyzer to complete the configuration process.



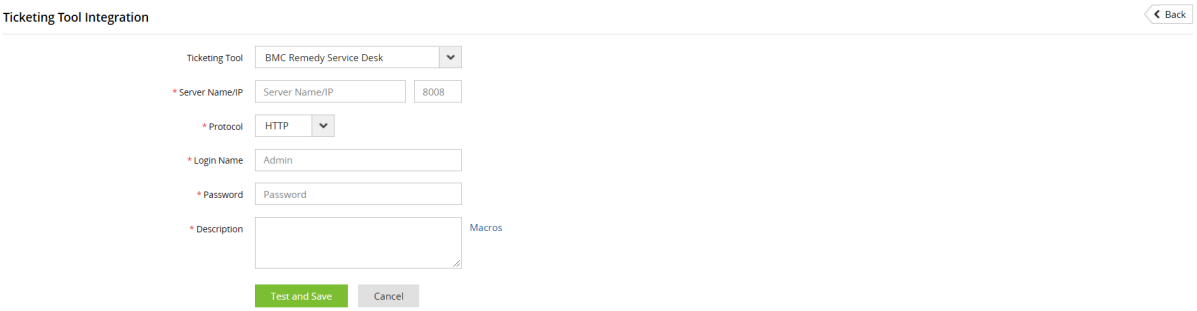
In EventLog Analyzer, navigate to the Alerts tab and click on ticketing tool integration under Alert Configuration. From the Ticketing Tool drop-down list, select Jira Service Desk.

1. Enter the Jira Service Desk server name or IP address.
2. Enter the port number.
3. Choose the protocol for communication - HTTP/HTTPS.
4. Enter the login name and password of the account having admin privileges.
5. Enter the project ID. This is the Key of the particular project noted from the ticketing tool.
6. Enter the type of issue. This needs to be same as the issue type that the project has been configured to hold.
7. Enter the Summary and the Description for the alert. You can select them from a predefined list available under Macros or type your own.
8. Click the Test and Save button to establish communication and complete configuration.

> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For BMC Remedy Service Desk

In EventLog Analyzer, navigate to the Alerts tab and click on ticketing tool integration under Alert Configuration. From the Ticketing Tool drop-down list, select BMC Remedy Service Desk.

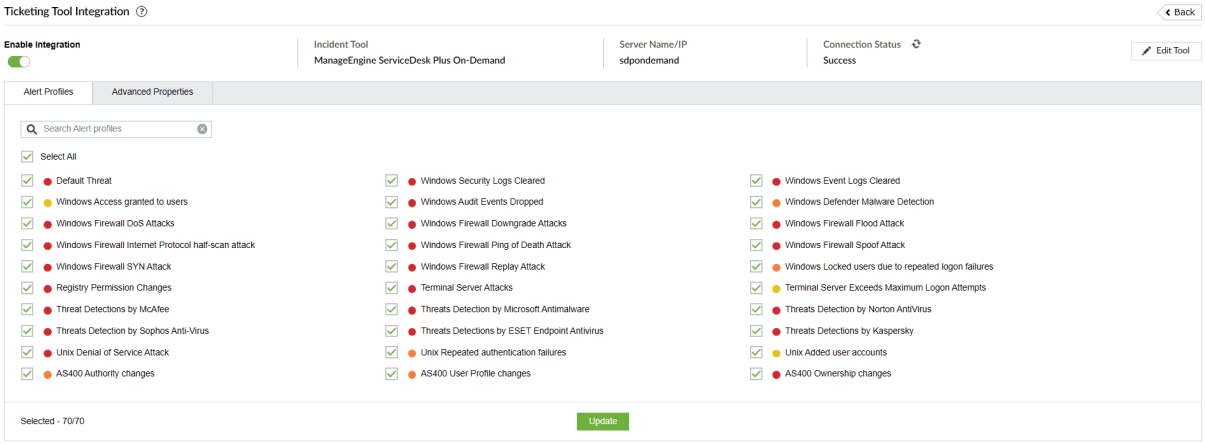


1. Enter the BMC Remedy Service Desk server name or IP address.
2. Enter the port number.
3. Choose the protocol for communication - HTTP/HTTPS.

4. Enter the login name and password of the account having admin privileges.
5. Enter the Description for the alert. You can choose it from a predefined list available under Macros or type your own.
6. Click the Test and Save button to establish communication and complete the configuration.

> **Note**
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

Mapping Alert Profiles with Configured Ticketing Tools



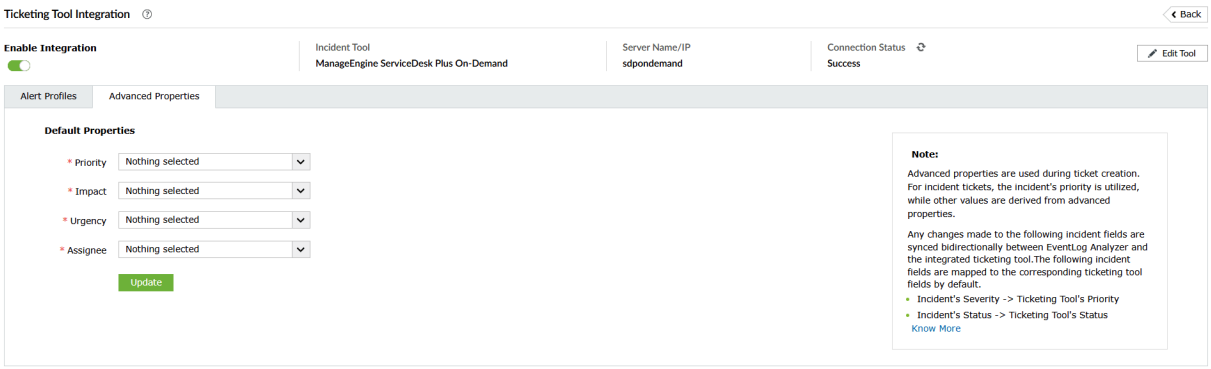
After configuring EventLog Analyzer with the ticketing tool, you can select specific alert profiles from where tickets should be created.

1. Access the Ticketing Tool Integration page - Here, you'll find a list of existing alert profiles.
2. Select Alert Profiles:
   - To select specific profiles for which tickets should be raised, use the search box to find them.
   - To select all alert profiles, check the Select All box. Any future profiles will also be automatically selected.
3. Update Settings: Once you've made your selections, click Update to apply the changes.
4. Manage Ticketing Tool Integration:
   - Enable/Disable Integration: Toggle the integration on or off as needed.
   - Check Connection Status: Click the Refresh icon next to the connection status to verify if Eventlog Analyzer is successfully connected to the ticketing tool.

Advanced Properties Configuration

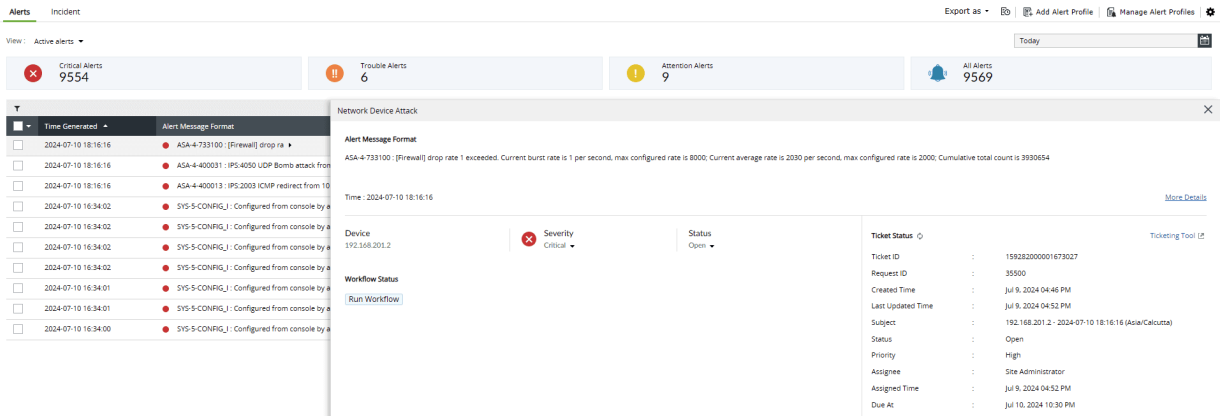
1. Navigate to the Advanced Properties tab to begin customization.
2. Configure each property by entering the desired values. These settings will be applied to any new tickets in the ticketing tool.

> **Note**
>
> 1. The Priority selected under Advanced Properties will not be applicable for tickets created from Incidents.
> 2. For seamless functioning of Advanced Properties, users integrating with Freshservice must disable the Priority Matrix in their Freshservice account.



Ticketing Tool Status

With EventLog Analyzer, you can efficiently manage security incidents by raising tickets and assigning them to administrators for alerts that are generated. After successfully configuring the ticketing tool, the ticket details can be viewed in Alerts tab by clicking the specific alert.




Impact : Affects Department
Urgency : High
Description : [Firewall] drop rate 1 exceeded. Current burst rate is 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max configured rate is 2000; Cumulative total count is 393065... More

11.1.1. Automatic database backup

Last updated on: September 12, 2025

Log360 can automatically back up its database and the databases used in the integrated products at regular intervals, as scheduled by you. Using this option, you can back up the built-in PostgreSQL DB or external PostgreSQL and MS SQL databases configured in the product.

Supported DB versions for auto backup

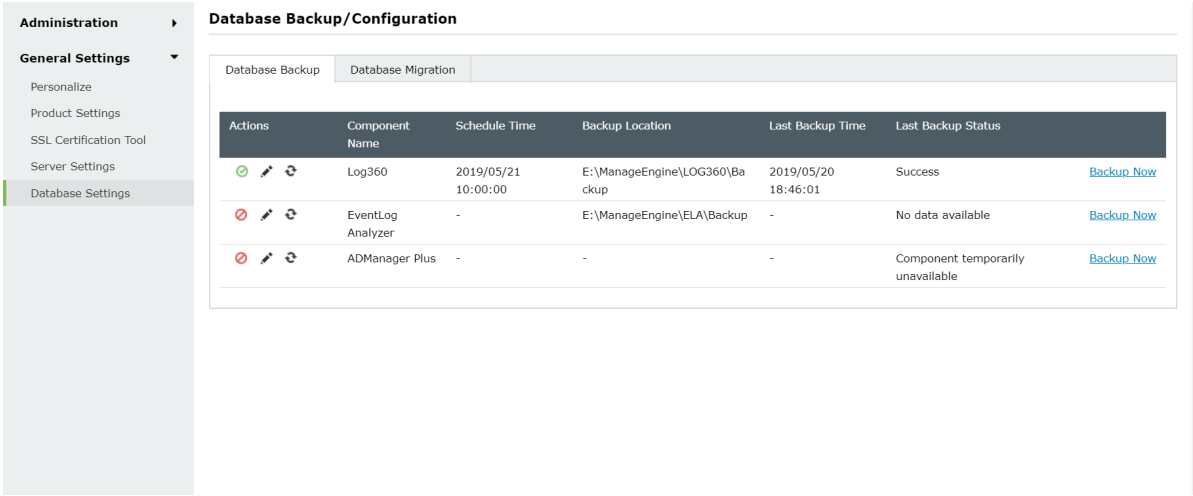
- PostgreSQL: Version 10 to 14
- MS SQL: Version 2008 and above

Prerequisite for backing up external PostgreSQL

1. In the machine where PostgreSQL is installed, go to <postgresql_installdir>/data and open the posgresql.conf file. Search for wal_level entry. Uncomment the entry and change its value to archive.
2. Copy all the files in <postgresql_installdir>/lib and <postgresql_installdir>/bin folders and paste them in <product_home>/pgsql/lib and <product_home>/pgsql/bin folders respectively. <product_home> refers to the home directory of Log360 or the integrated products for which you're configuring the auto backup scheduler.
3. Restart the external PostgreSQL server.
4. Repeat the steps 1 to 3 from above whenever you update the PostgreSQL server.

Steps to schedule database backup

1. Navigate to Admin → General Settings → Database Settings → Database Backup.
2. Choose Log360 or an integrated product for which you want to schedule auto backup, and click the edit icon.

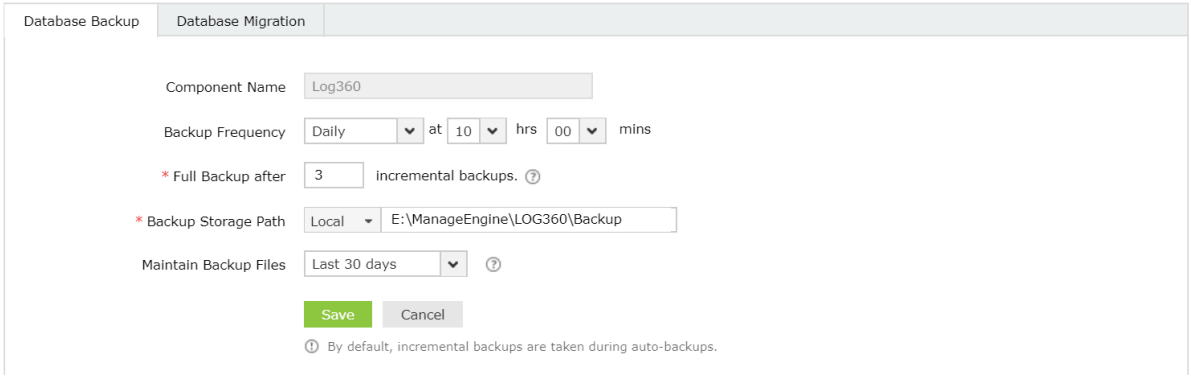


3. Select whether you want to schedule the backup daily, weekly, or monthly and at what time from the Backup Frequency drop-down.
4. Enter the number of incremental backups to take for every full backup in the Full Backup after __ incremental backups box. Enter 0 if you want to take only full backups.
5. Enter the Backup Storage Path.
   - You can either choose a local folder or shared folder to store the backups.
   - If the shared folder you've chosen needs permission to store the backups, then put a check against the Authentication Required box, and enter the necessary credentials.

> **Note 1**
>
> If the shared folder is located in a workgroup computer, then create a new domain account in AD. This new account should have the same username and password as that of a local account in the workgroup computer. Use the credentials of this new account for authentication.

> **Note 2**
>
> If the specified path is wrong or unreachable, the backup will be stored in the default backup folder (<Installation_Folder\Backup>).

6. Set a retention period for the backup files from the Maintain Backup Files drop-down.



7. Click Save.

Other settings

- To disable auto backup for Log360 or a particular integrated product, click the icon located in the Actions column of the auto backup configuration table.
- To get the status of the latest backup, click the icon.
- To edit the backup schedule for a particular component, click on the icon located in the action column of

the component.

- Use the Backup Now option to initiate a backup instantly.
- Use the Recent Backups icon in the status column to view all available backups.

Restoring backup from an old version of MS SQL server to new MS SQL server

If you've installed a new version of MS SQL server and want to configure it in Log360 or its integrated products in place of the old MS SQL server, you can do so by using the backup you've taken using Log360. Just note that, in addition to the backup you've taken using Log360, you need to copy the files in <MS_SQL_Old_Version>/Backup to <MS_SQL_New_Version>/backup.

Troubleshooting tips

If you get an error while backing up the database, please check whether:

- The database server is running.
- There is sufficient space in the backup storage location.

11.1.2. Database Migration

Last updated on: September 12, 2025

In this page

Important points to remember

Prerequisites for MSSQL migration

Prerequisites for PostgreSQL migration

Database backup for External PostgreSQL

Steps for Migration

Using this option you can change the built-in database server (PostgreSQL) of Log360 to MS SQL Server or another instance of a PostgreSQL Server.

Important points to remember

- Supported database migrations:
  - PostgreSQL Server to MS SQL Server or another instance of PostgreSQL Server.
  - MS SQL Server to PostgreSQL Server or another instance of MS SQL Server.
- Supported database versions:
  - PostgreSQL: 10 to 14
  - MS SQL: 2008 and above
- Take a backup of the database before you proceed.
- We recommend applying the Windows service packs and cumulative updates suggested by Microsoft during your migration to MS SQL Server.

Prerequisites for MSSQL migration

1. Copy the bcp.exe and bcp.rll files from the installed SQL Server directory and paste them in the Log360 bin folder (<Log360_installed_directory/bin).
   - Location of the bcp.exe file: <MSSQL_installed_folder>\Client SDK\ODBC\...\Tools\Binn\bcp.exe. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\...\Tools\Binn\bcp.exe.
   - Location of the bcp.rll file: <MSSQL_installed_folder>\Client SDK\ODBC\...\Tools\Binn\Resources\1033\bcp.rll. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\...\Tools\Binn\Resources\1033\bcp.rll
2. For migration to MS SQL, please install the corresponding SQL Native Client in the Log360 machine as per the MS SQL Server version.

MS SQL Server Version	Native Client
2008	Download
2012	Download
2014	Download
2017	Download
2019	Download

> Note
>
> MS SQL server version 2022 is also supported by Log360.

3. If firewall is enabled in the MS SQL Server machine, the TCP and UDP ports must be opened.
4. If the MS SQL server you wish to migrate to has Force encryption enabled, follow the steps mentioned below.

- Convert your certificate to .cer format.
  - Open IIS Manager.
  - In the middle pane, click Server Certificates.
  - Open the certificate you want to use, and click the Details tab.
  - Click Copy to file.
  - Click Next in the Certificate Export Wizard that appears.
  - On the Export Private Key screen, select No, do not export the private key, and click Next.
  - On the Export File Format screen, select either DER encoded binary X.509 (.CER) or Base-64 encoded X.509 (.CER), and click Next.
  - Enter a name for the file and click Next, and then Finish.
- Open Command Prompt and navigate to <Installation directory>\jre\bin. Use the command below to associate the certificate with the Java KeyStore.
  keytool -import -v -trustcacerts -alias myserver -file pathofthecert\certname.cer -keystore "..\lib\security\cacerts" -keypass changeit -storepass changeit -noprompt
  where pathofthecert is the location where the certificate has been stored and certname is the certificate name.
  The certificate will be added to your Java KeyStore.

Prerequisites for PostgreSQL migration

1. Open the remote machine where the product is installed & navigate to Product Home\ pgsql\ data\ pg_hba.conf
2. Open pg_hba.conf file and add an entry of the host IP address and its subnet mask as 0.0.0.0/0 (Refer Pic).

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
host    all             all             0.0.0.0/0               md5
```

3. Navigate to Product Home\ pgsql\ data \ postgresql.conf
4. Open postgresql.conf and change the Listen_addresses as '*' & remove the # in the start of the line. (Refer Pic)

```
# - Connection Settings -

listen_addresses = '*'          # what IP address(es) to listen on;
# comma-separated list of addresses;
# defaults to 'localhost'; use '*' for all
```

Database backup for External PostgreSQL

- In the machine where PostgreSQL is installed, go to <postgresql_installdir>/data and open the posgresql.conf file. Search for wal_level entry. Uncomment the entry and change its value to archive.
- Copy all the files in <postgresql_installdir>/lib and <postgresql_installdir>/bin folders and paste them in <product_home>/pgsql/lib and <product_home>/pgsql/bin folders respectively. Here, <product_home> refers to the home directory of Log360 or the integrated products for which you're configuring the auto backup scheduler.
- Restart the external PostgreSQL server.

Repeat the steps 1 to 3 from above whenever you update the PostgreSQL server.

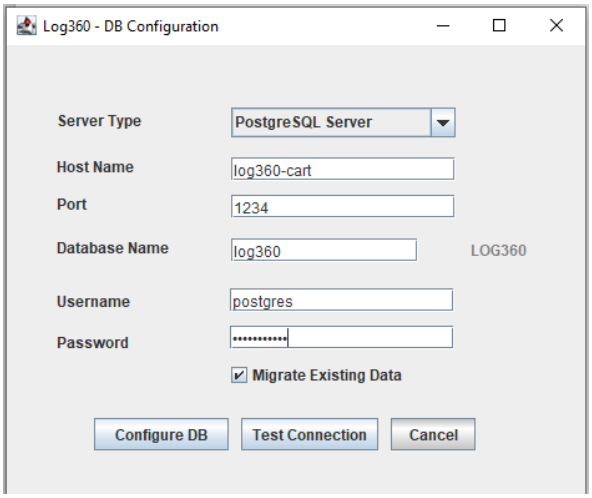
Steps for Migration

> **Note**
>
> Take a Backup/Snapshot of Log360 before proceeding with the steps (Important)

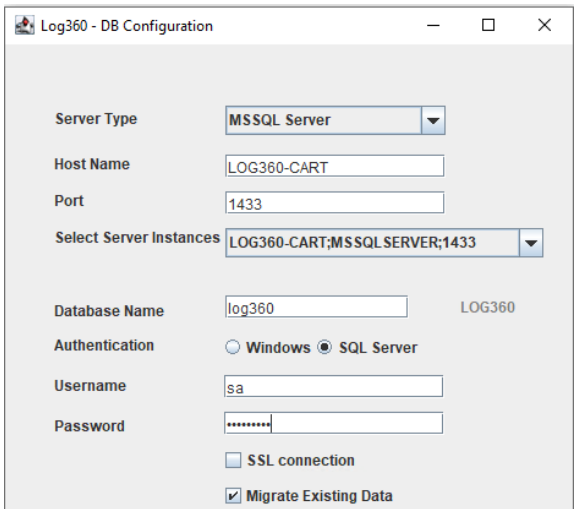
1. Open the Command Prompt and navigate to <Log360 home\bin> (Here, Log360 home is the location where Log360 is installed)

Log360 is installed).

2. Stop Log360 by running shutdown.bat.
3. Run the ChangeDB.bat.
4. From the Server Type menu, select the database server you plan to switch to.
5. If you select PostgreSQL Server, then:
   - In the Host Name and Port field, enter the host name or IP address and the port number of the PostgreSQL database server.
   - Enter the username and password of a user with the necessary permissions to create a new database.

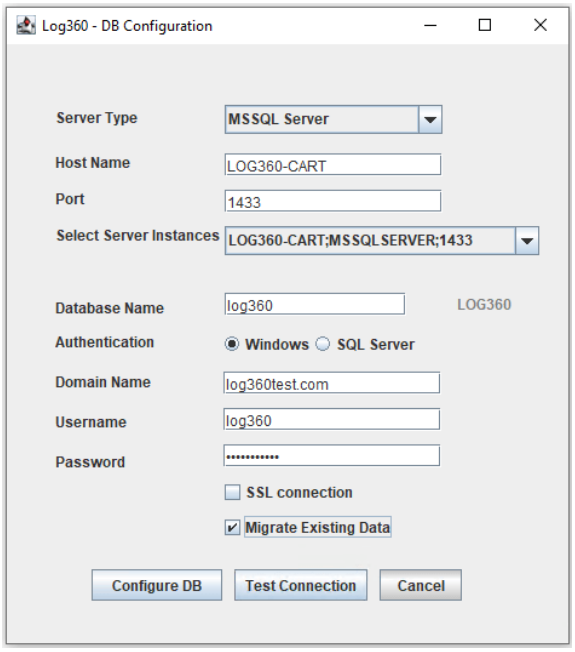


6. If you select MS SQL Server, then:
   - Move the bcp.exe and bcp.rll files into the bin folder manually.
   - In the Host Name and Port field, enter the host name or IP address and the port number of the MS SQL database server.
   - In the Select Server Instance field, select the SQL Server instance you want to use.
   - For Authentication, you can use either Windows credentials or a SQL Server user account.
   - If you want to use a SQL Server user account, then select SQL Authentication and enter the Username and Password.





- If you want to use Windows authentication, select Windows Authentication, and enter the username and password of a Windows domain user account.

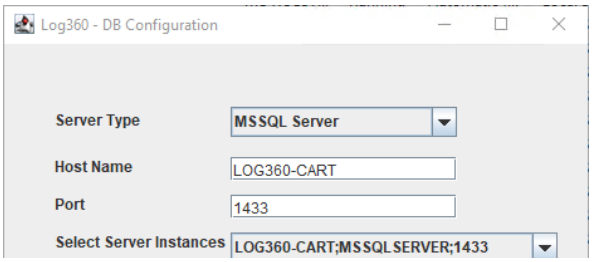


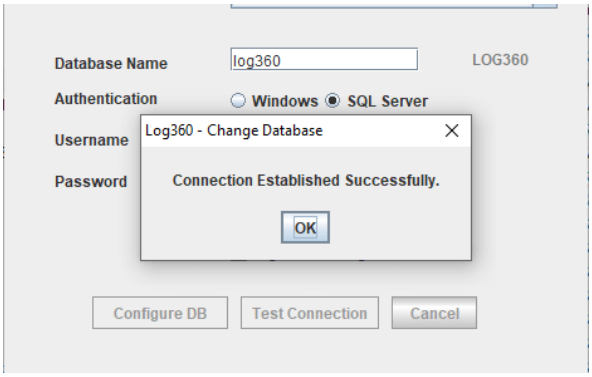
> **Note**
>
> The user account used must have permission to create a database in the selected MS SQL Server.

7. Check the box next to Migrate Existing Data to copy the data from your old database to the new database.

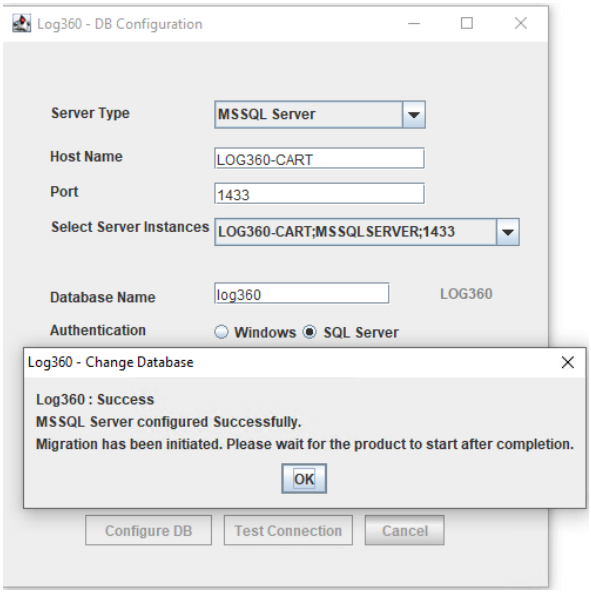
> **IMPORTANT**
>
> Leave this box unchecked only if you are changing the database of a fresh installation of Log360.

8. If the MS SQL server you wish to migrate to has Force encryption enabled, check the box next to SSL connection.
9. Click Test Connection and wait for the connection to be established.





10. Once Test Connection has been established successfully, click Configure DB to initiate migration.



11.1.3. Database Settings

Last updated on: September 12, 2025

Log360 allows you to configure periodic backup of the database that comes built-in with it and the integrated components. The product also allows you to migrate from the built-in database (PostgreSQL) to MS SQL.

- Database Auto Backup
- Database Migration

11.2. Database Access

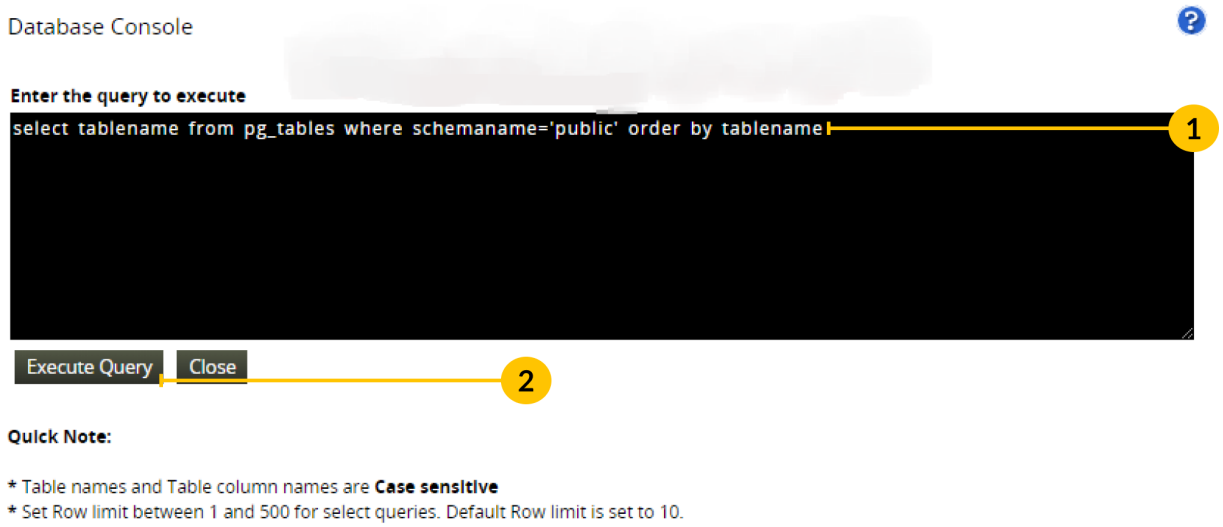
Last updated on: September 12, 2025

To access the EventLog Analyzer database, use the Access Database menu.

How to query the EventLog Analyzer database?

Use the following menu option:

- Settings tab > System Settings > System Diagnostics > Database Access



1. Enter the database query in the console.
2. Click the Execute Query button.

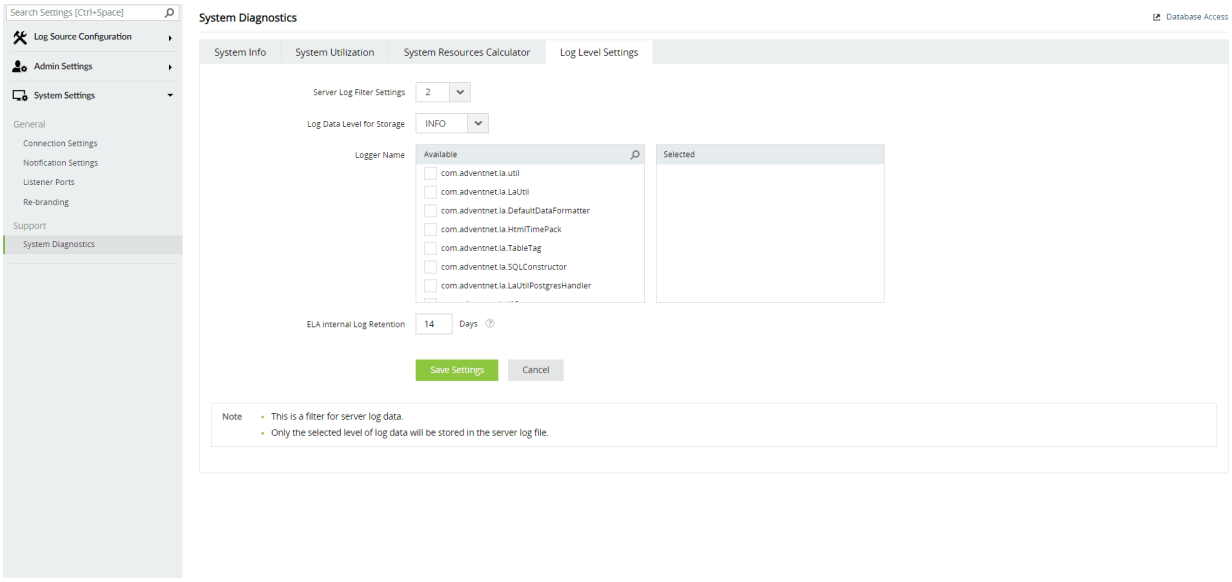
> Note
>
> - Only 'read queries' can be executed.
> - Create, Alter, Insert queries cannot be executed.
> - Table and Column names are case sensitive.

11.3. Log Level Settings

Last updated on: September 12, 2025

Log Level Settings is used to set the granularity level of EventLog Analyzer server logs. The logs will form part of the support information file (SIF) generated for sending to ZOHO Corp. These logs will be used for debugging EventLog Analyzer server issues.

- In the Settings tab, navigate to System Settings > System Diagnostics > Log Level Settings.



- Select the Server Log Filter Settings (values from 2 to 5).
- Select the Level of Log data to be stored.
- Select the Logger Name from the list. For each available logger or set of loggers, you can set the log filter level and log level independently.
- Click Save Settings to save the selected log level settings.

11.4. Log Forwarder

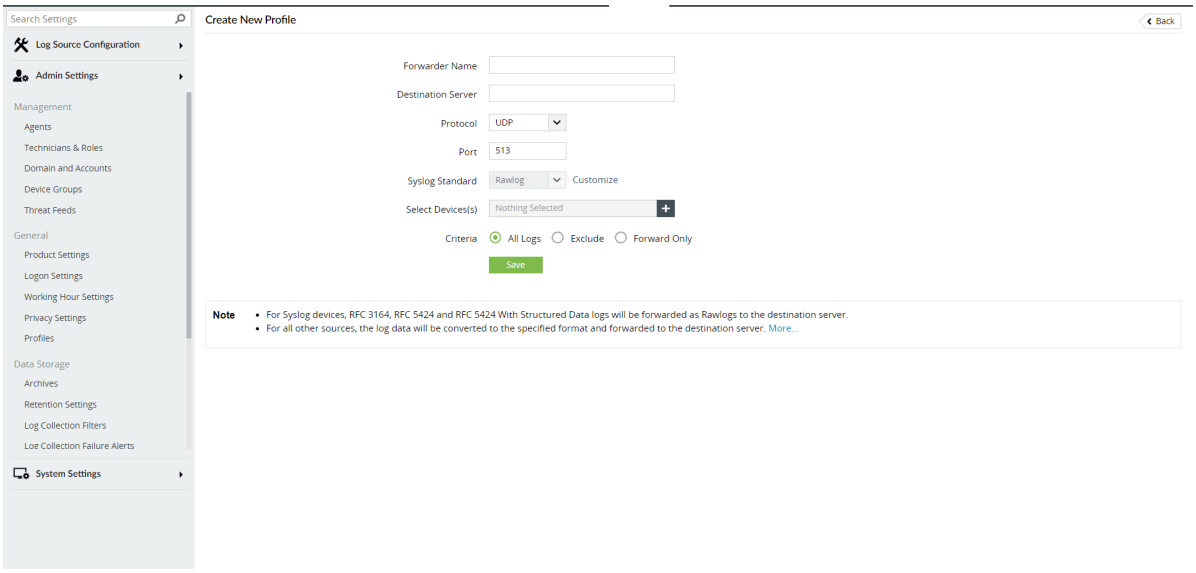
Last updated on: September 12, 2025

EventLog Analyzer's Syslog Forwarder transmits logs from various sources to a destination server. Logs from syslog devices are forwarded as raw logs, whereas logs from other sources are converted to specific formats such as JSON, RFC 5424, RFC 5424 With Structured Data, and RFC 3164, or a custom format, and then forwarded to the destination server.

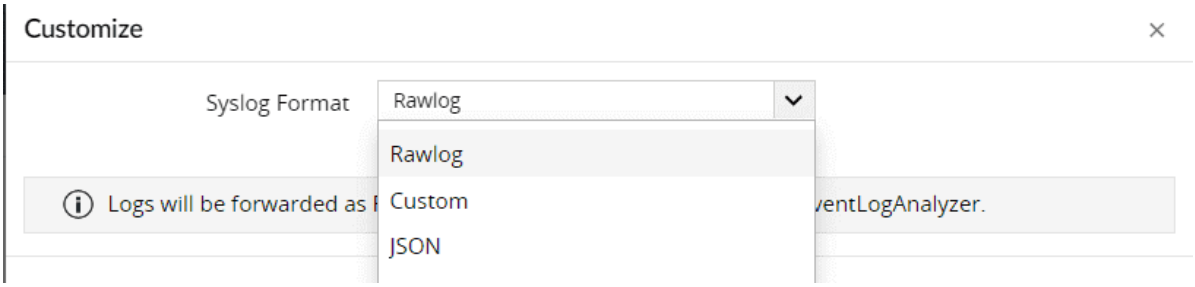
Steps to start forwarding logs

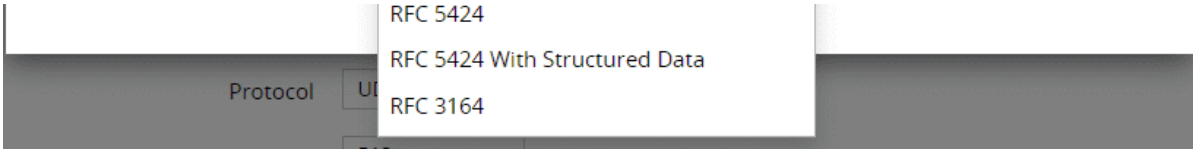
Creating a new profile

1. Navigate to Settings → Admin Settings → Integrations → Log Forwarding.
2. To add a new forwarder profile, click on Add New Profile on the top right corner of the page.
3. Enter the Forwarder Name.
4. Enter the Destination Server to which the logs have to be forwarded to.
5. Select the required Protocol, either UDP or TCP from the drop down.

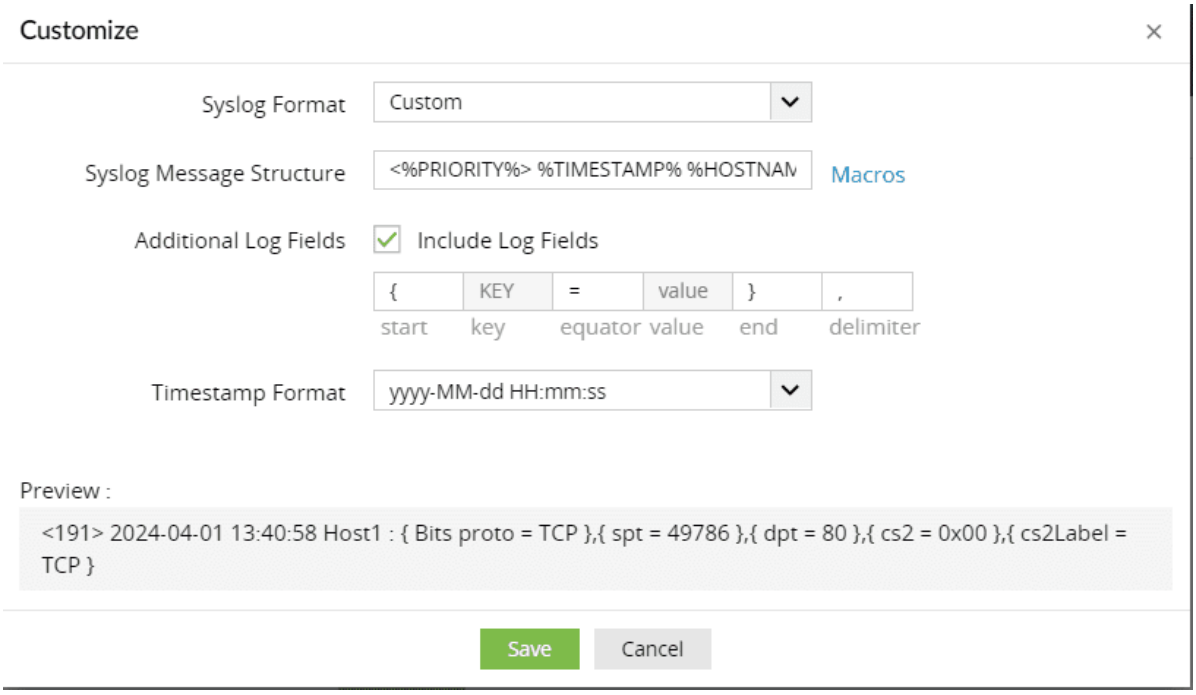


6. Enter the Port number. The default port number is 513.
7. Select the required Syslog Standard by clicking on Customize. The formats include Rawlog, JSON, RFC 5424, RFC 5424 With Structured Data, RFC 3164 and Custom.

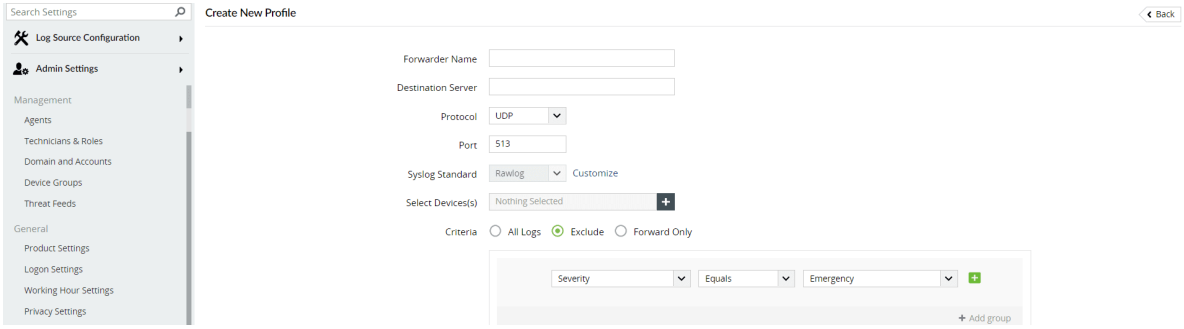


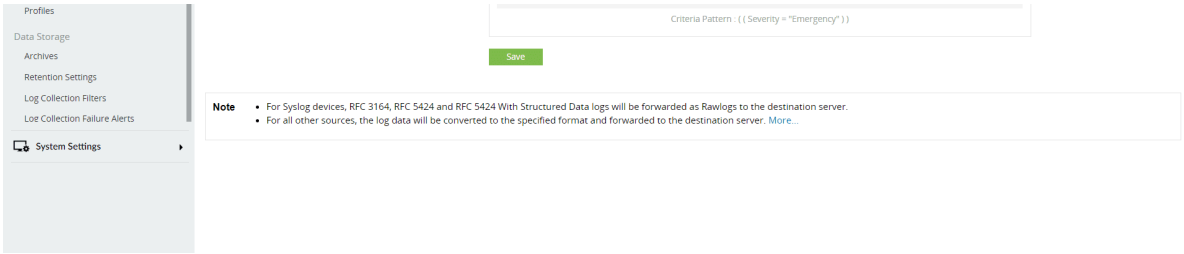


8. Select the required format and click Save.
9. To create a custom Syslog Format, select Custom from the drop-down.
   - Enter the Syslog Format.
   - Enter the Syslog Message Structure.
   - Enable Additional Log Fields.
   - Enter the Timestamp Format.
   - Click Save.



10. Under Select Devices, add the source devices from which logs have to be fetched.
11. Select the required Criteria.
    - All logs - It forwards all incoming logs.
    - Exclude - It excludes specific logs based on the given criteria before forwarding.
    - Forward Only - It forwards only specific logs based on the given criteria.

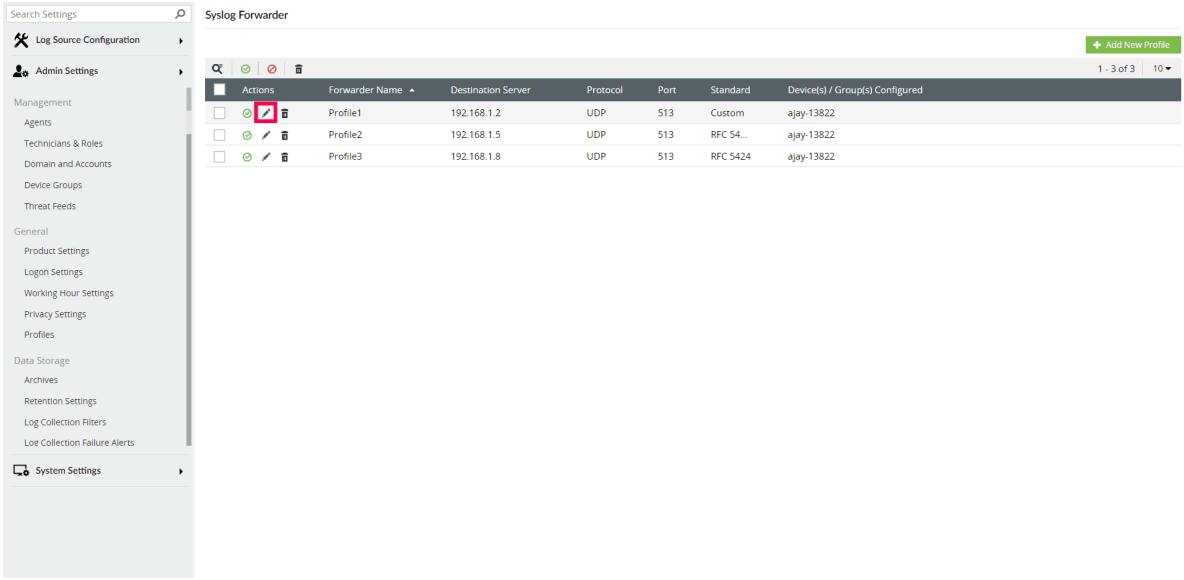




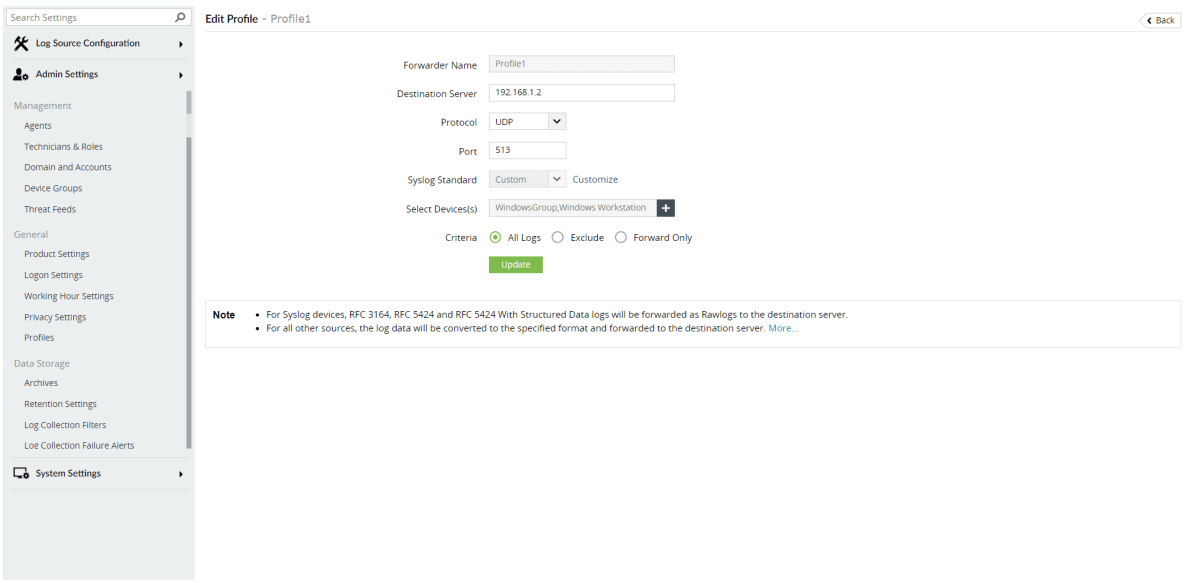
12. Click Save.

Updating an existing profile

1. Navigate to Settings → Admin Settings → Integrations → Log Forwarding.
2. Click on the Update Profile icon on the profile that has to be updated.

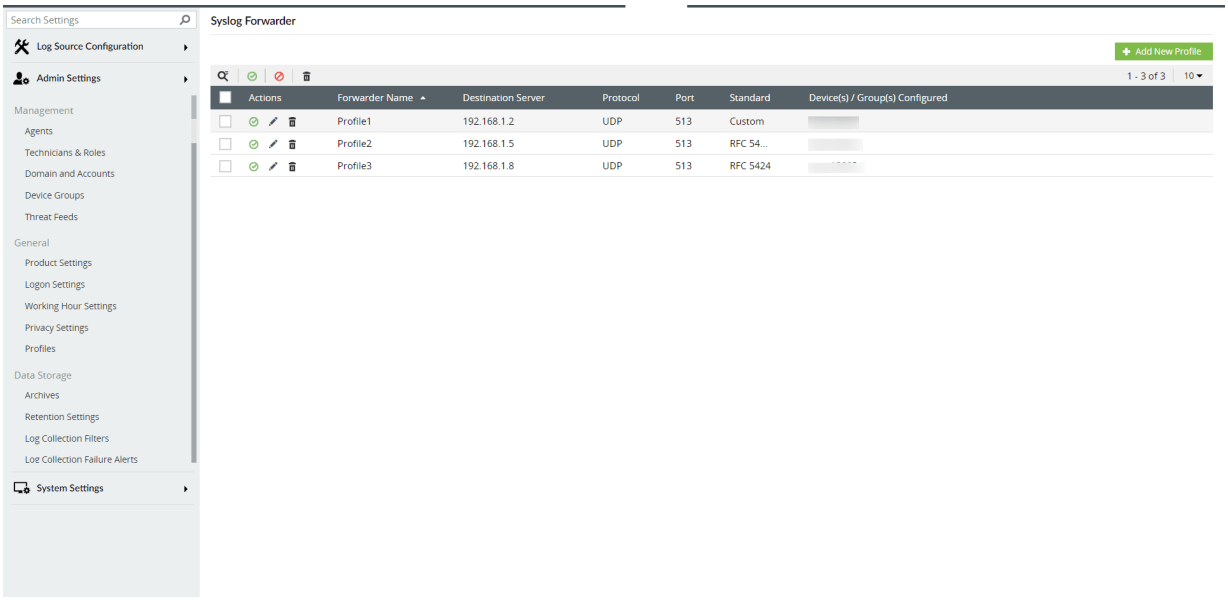


3. The Forwarder Name would already exist here.
4. Refer to steps 4 to 11 under Creating a new profile.
5. Click Update.



Managing forwarder profiles

EventLog Analyzer allows you to create up to 5 distinct profiles to enable seamless log forwarding. The profile dashboard allows you to enable, disable, update and delete the forwarder profiles.



11.5. Product Settings

Last updated on: September 12, 2025

In this page

Overview

Product Configurations

Product Notifications

Security Hardening

Overview

This document provides a comprehensive walkthrough of the Product Settings module in Log360, allowing administrators to tailor how the product behaves and responds to operational needs. From configuring product notifications to enforcing security measures, these settings offer granular control over performance and protection.

These configurations provide numerous customization capabilities, including limits for emails and SMSs, alert email formats, correlation permissions, and notification settings. The Product Settings tab has three sub-tabs, each having certain customization options:

- Product Configurations
- Product Notifications
- Security Hardening

Product Configurations

To configure settings such as views per page, number of rows displayed in reports, and so on in the product, follow the steps given below.

1. Navigate to the Settings tab and click on Product Settings listed under General in Admin Settings as highlighted below.

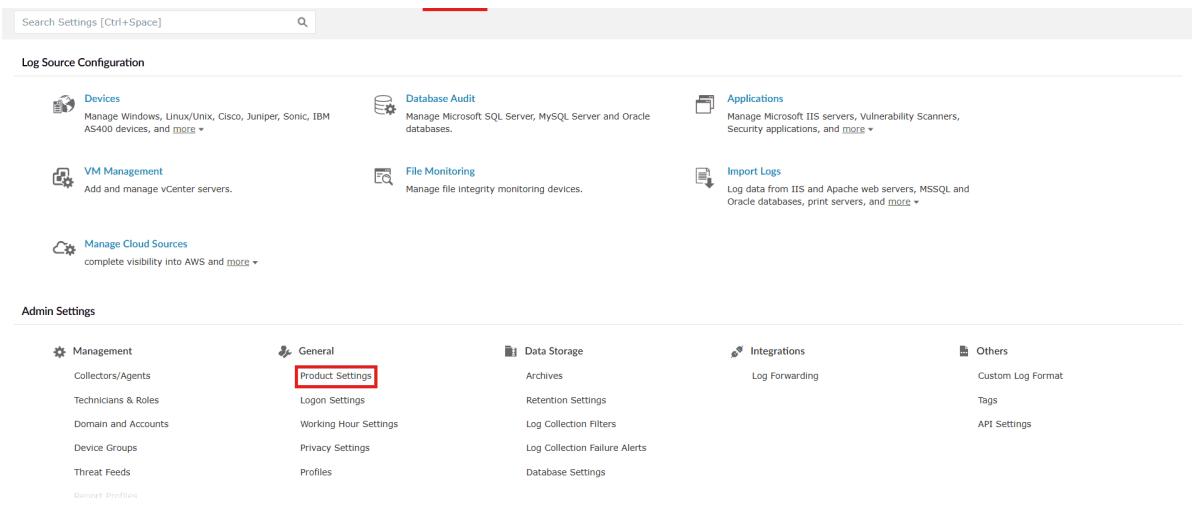




Image 1: Product settings via the Settings tab

2. You will be taken to the Product Settings module with the Product Configurations sub-tab displayed.

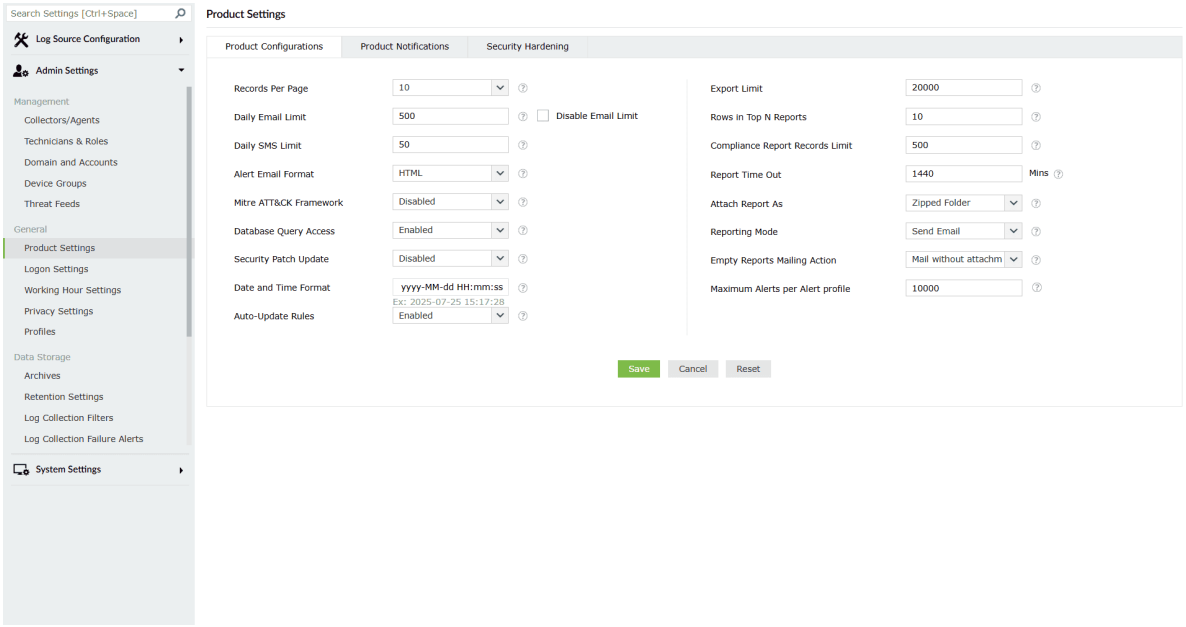


Image 2: Product Configurations sub-tab via the Product Settings tab

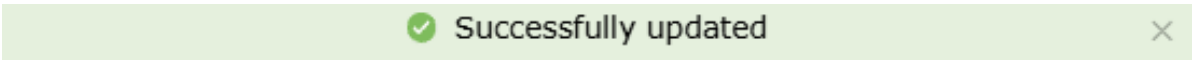
Below is the detailed list of all the fields present in these settings.

Configurations	Default Values	Description
Records Per Page	10	Select the number of records to be displayed in the pages of the user interface. The options available are: 10, 20, 50, and 100.
Daily Email Limit	500	Set the maximum permissible number of emails that can be sent per day. Enable or disable the mail limit alert by selecting the Enable/Disable Mail Limit Alert checkbox. There could be a mail server or client limitation for sending the emails.
Disable Email Limit (checkbox)	Empty checkbox	Ticking the checkbox will allow you to remove any limits for the maximum permissible number of emails that can be sent per day.
Daily SMS Limit	50	Set the maximum permissible number of SMS messages to be sent per day. The telecom service provider often sets a limit to the number of SMSs that can be sent per day.

Configurations	Default Values	Description
Alert Email Format	HTML	Select whether the alert emails are sent in HTML or plaintext format.
Mitre ATT&CK Framework	Disabled	Consolidated data from the Mitre reports will be displayed on the new dashboard tab Mitre Overview when this option has been enabled.Note: This feature will increase log processing and it might affect the performance.
Database Query Access	Enabled	Configure whether access to the product's database is allowed or denied. The product's database can be queried to access product data stored in it.
Security Patch Update	Disabled	Option to Automatically download Critical Security Patch to your Instance
Date and Time Format	yyyy-MM-dd HH:mm:ss	Set the format of date and time that needs to be displayed throughout the product. Other than the few predefined formats available, you can also create formats of your own. There are a few rules to be followed while creating your own date and time format: • The permitted separators are hyphen(-), slash (/), full stop(.), colon(:), comma(,), and space. • A space is the only separator that can be used between the date and the time. • There should not be any separators at the beginning or at the end. • Two continuous separators are not allowed. • Entering two digits for the month will display the month in numbers, whereas entering three digits will display it in words. Ex. 'MM' will display June as 06 and 'MMM' will display it as Jun.
Auto-Update Rules	Enabled	Option to Automatically download Critical Security Patch to your Instance
Export Limit	20000	Set the maximum number of records to be included in an exported report.
Rows in Top N	10	Set the number of rows to be displayed for reports under the Top

Reports Configurations	Default Values	N Reports section. Description
Compliance		
Report Record Limit	500	Set the maximum number of records to be included in a Scheduled Compliance Report.
Report Time Out	1440 mins	Set the maximum time allowed to generate a report.
Attach Report As	Zipped Folder	Select the report format to be attached in email. The available options are: PDF/CSV Report and Zipped Folder.
Reporting Mode	Send Email	Configure whether you want to save the reports in a folder in the machine, send them as mail attachments, or both. For Save to Location and Send Email & Save to Location options, you have to enter the location to save the reports in the text box. The reporting mode options available are Send Email, Save to Location, and Send Email & Save to Location.
Empty Reports Mailing Action	Mail without attachment	Configure whether you want to receive a mail or not when the reports are empty. There are two types of mail that you can receive. By selecting Mail without attachment, you will receive a mail without the empty reports. Mail with attachment, will let you receive a mail with the empty reports attached. You can choose not to receive a mail by selecting Don't mail reports.
Maximum Alerts per Alert profile	10000	Maximum number of alerts that will be triggered for an alert profile in a day. The recommended value is a maximum of 10,000.

3. After making the necessary changes, click on Save.
4. Upon successful completion of action, the below pop-up appears.



5. Click on the Reset button if you wish to reset all the configurations made in the fields and redo them.

Product Notifications

To configure the scenarios for which you want to receive notifications from the product, follow the steps given below.

1. Navigate to the Settings tab and click on Product Settings listed under General in Admin Settings as highlighted below.

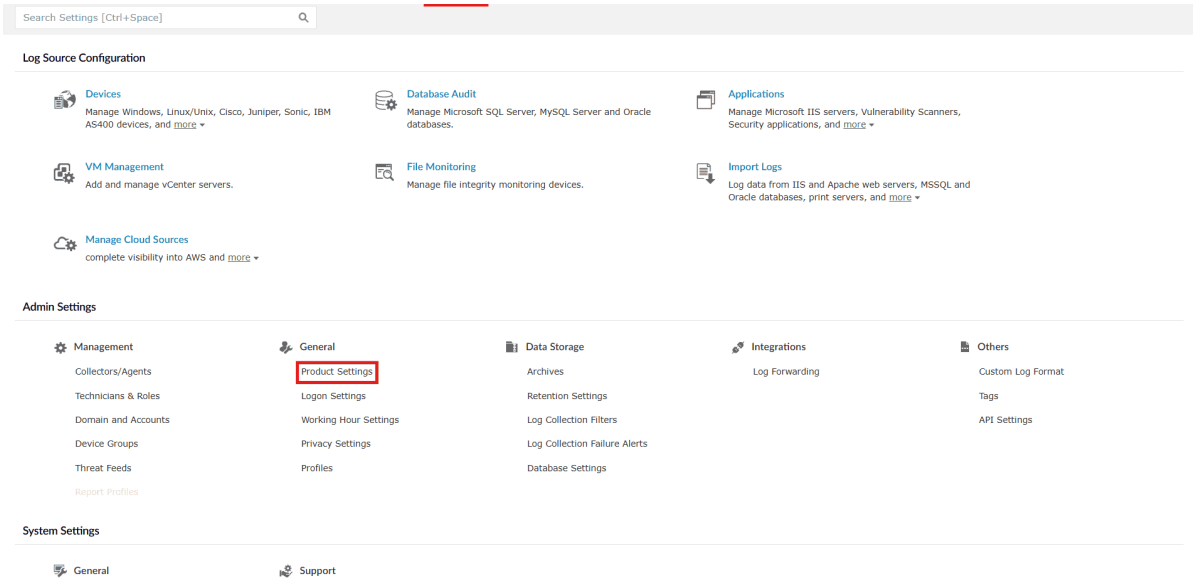


Image 3: Product settings via the Settings tab

2. You will be taken to the Product Settings module with the Product Configurations sub-tab displayed. Click on the Product Notifications sub-tab.

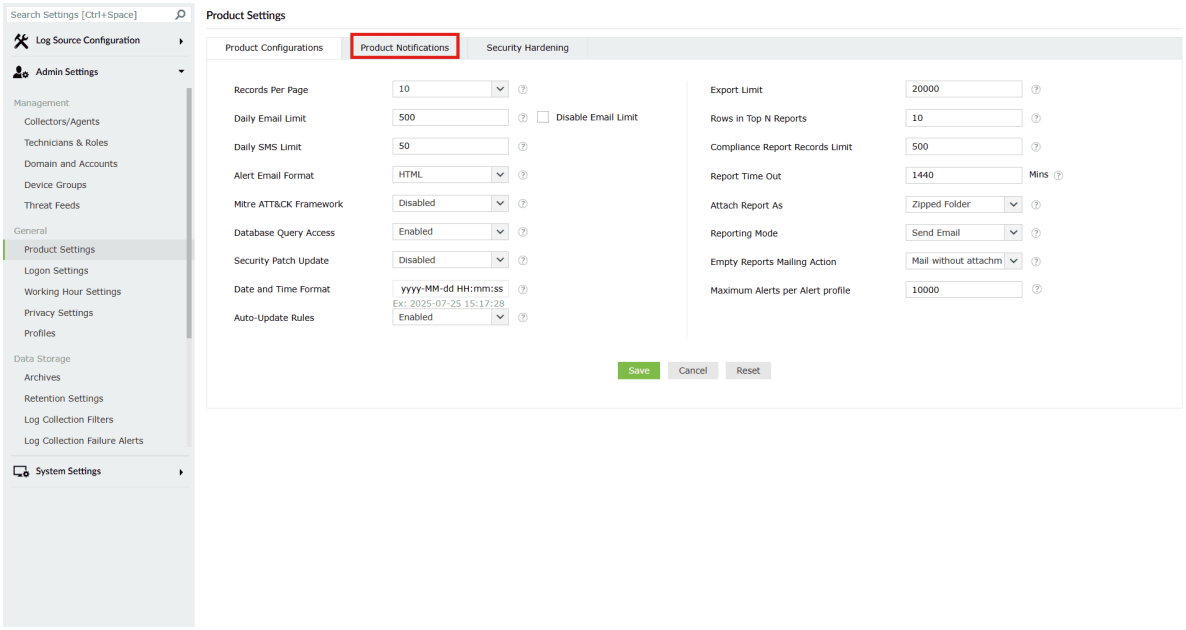
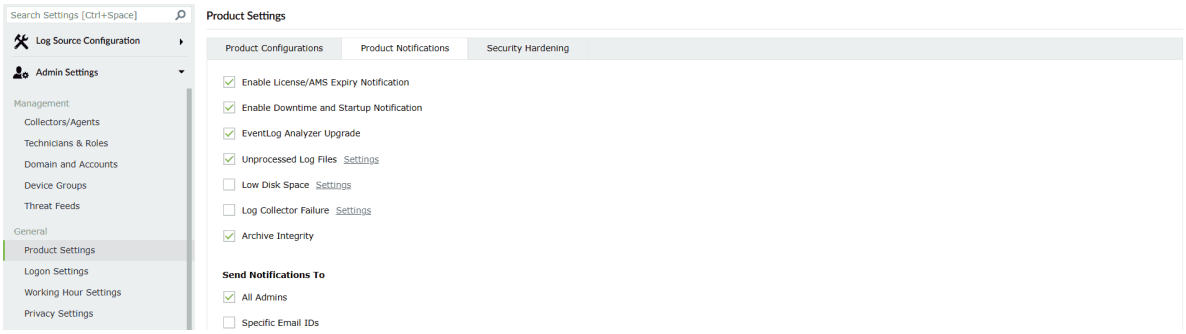


Image 4: Product Notifications sub-tab highlighted

3. The Product Notifications sub-tab opens as shown below.



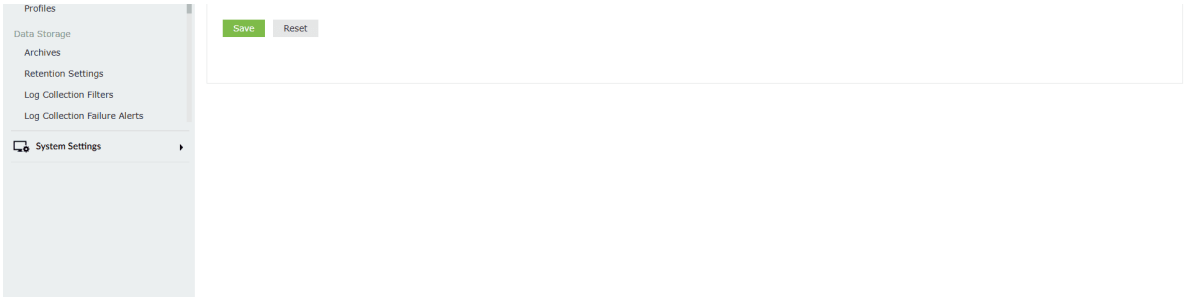


Image 5: Product Notifications sub-tab via the Product Settings tab

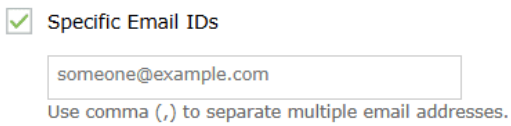
The different settings for enabling or disabling alerts have been listed below.

Configurations	Default configuration	Description
Enable License/AMS Expiry Notification	Enabled	You will be notified that your Log360 license is about to expire exactly 30 days, 7 days, and 1 day prior to the expiry date, as well as on the day of expiry.
Enable Downtime and StartUp Notification	Enabled	You will be notified when the Log360 service shuts down or is started.
Enable product Upgrade	Enabled	You will be notified when Log360 has been successfully upgraded.
Unprocessed Log Files	Enabled	When Log360 is unable to process the incoming logs fast enough, the unprocessed logs will be added to files. They will be processed one after the other once Log360 can process logs. You can set a limit on the number of files that get filled with unprocessed logs. You will be notified once the limit is exceeded.In a new installation of Log360, the default value for Unprocessed Log Files is 100.
Low Disk Space	Disabled	You will be notified when the free space available in the disk on which Log360 is installed goes below a certain value. You can set the limit in terms of GB of free disk space and give a suitable subject for the email that will get triggered.
Log Collector Failure	Disabled	You will be notified when Log360's log collector is unable to collect logs. You can configure the subject of the email that will get triggered.

Configurations	Default Enabled configuration	Description
Archive Integrity		You will be notified when the archive files are deleted or tampered via an email notification.

> NOTE
>
> In a new installation of Log360, notifications will be turned on by default for Enable License/AMS Expiry Notification, Enable Downtime and StartUp Notification, Enable Product Upgrade, and Unprocessed Log Files.

4. Choose the mode for Send Notifications To:
   - After configuring the necessary notification settings, select if those notification emails need to be sent to all the product designated Admins. This option is enabled by default. You can click on the checkbox to disable this option.
   - Alternatively, you can choose to send the notification mails to specific email addresses. This option is disabled by default. Click on the checkbox to enable it.
     - Upon enabling, a box to enter the mail address(es) appears as the below.



   - You can opt for both modes at the same time.
5. After making the necessary configurations, click on the Save button.
6. Upon successful completion of action, the below pop-up appears.



Security Hardening

Security hardening feature helps you manage and configure the security settings of the product console. This tab also displays a security score, which is calculated based upon the weightage given to each configuration.
To manage individual settings, click the Configure or Enable option corresponding to that security setting and make the required changes. Once configured, the setting will have a green ticked Configured/Enabled icon next to it.

Enabling Security Hardening:

1. Navigate to the Settings tab and click on Product Settings listed under General in Admin Settings as highlighted below.



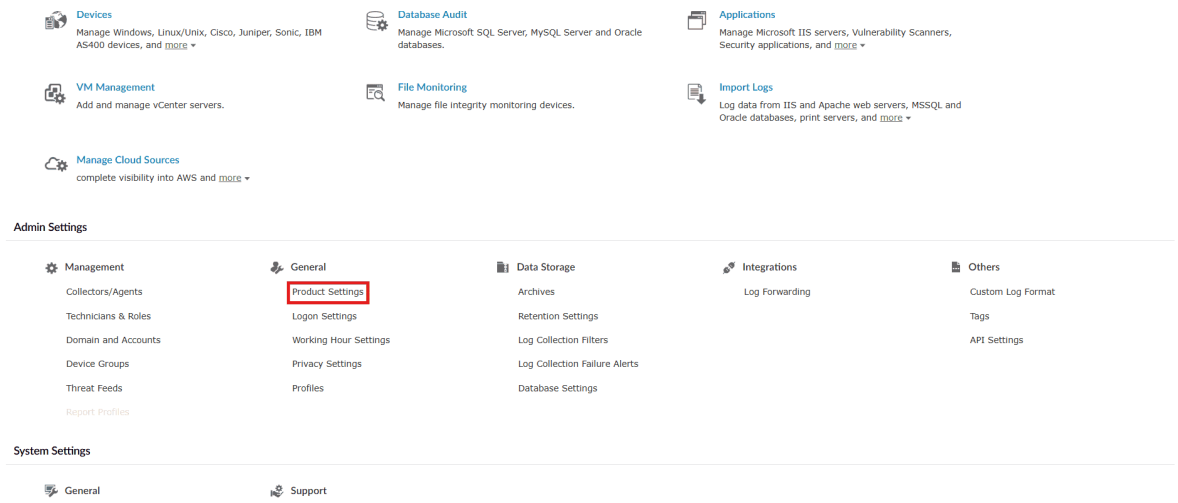


Image 6: Product settings via the Settings tab

2. You will be taken to the Product Settings module with the Product Configurations sub-tab displayed. Click on the Security Hardening sub-tab.

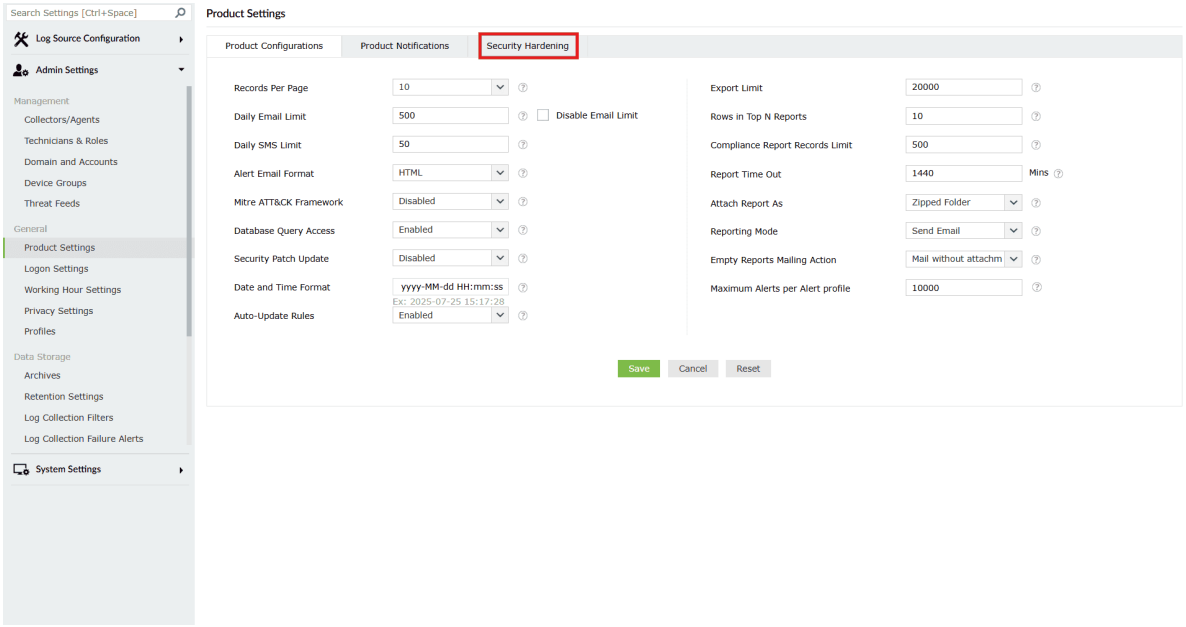
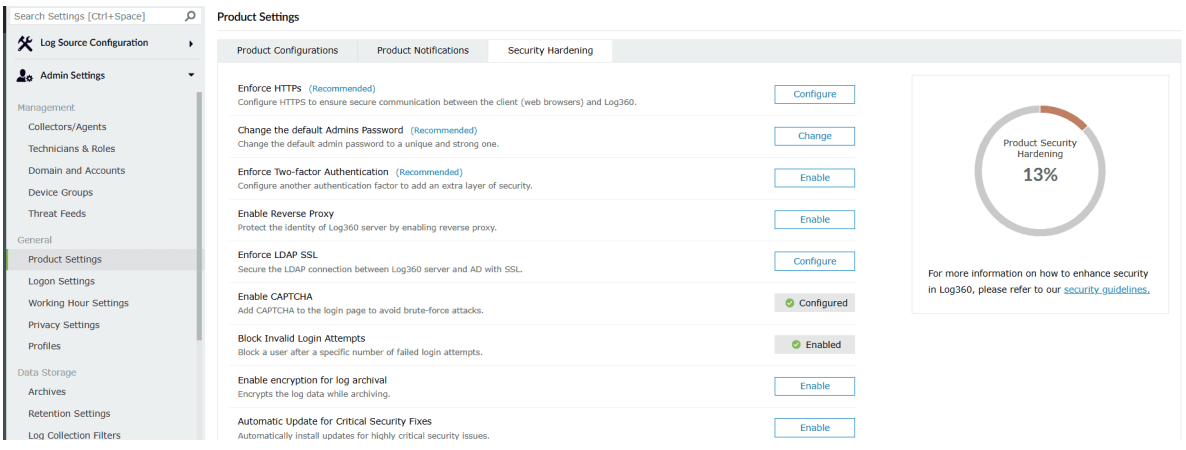


Image 7: Security Hardening sub-tab highlighted

3. The Security Hardening sub-tab opens as shown below.



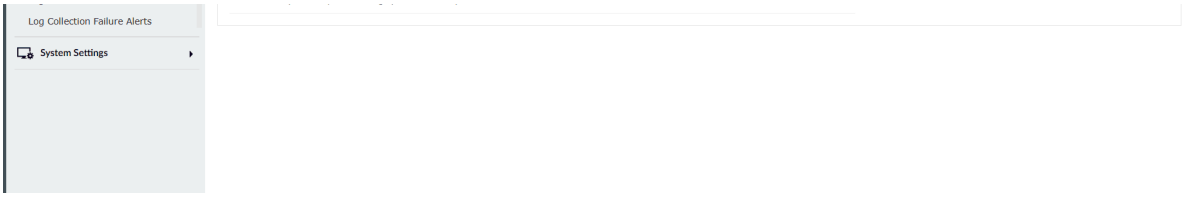


Image 8: Security Hardening sub-tab via the Product Settings tab

We recommend you configure all the settings and ensure your product security score is 100%. The security settings alert will be displayed in the notification center (□ icon on the top-right corner) until a security score of 100% is reached.

> NOTE
>
> For licensed customers, the alert will also be displayed after every successful login until all the mandatory security configurations (marked with * under List of security settings) are done.

List of available settings

- Enforce HTTPS: Configuring HTTPS helps you secure a connection between the web browser and the product's server. See how to enable HTTPS.
- Change the default Admins Password : It is recommended to use a strong password to access the product's dashboard. Use this setting to change both the admin and operator passwords.
- Enforce Two-factor Authentication: Two-factor authentication adds an additional layer of security. See how to configure two-factor authentication.
- Enable Reverse Proxy: Enabling reverse proxy helps protect the identity of the product's server. Click on Configure to navigate to the reverse proxy settings tab. See how to enable reverse proxy settings.
- Enforce LDAP SSL: This setting lets you secure the LDAP (Lightweight Directory Access Protocol) connection between the product server and Active Directory with SSL (Secure Sockets Layer). See how to enable LDAP SSL.
- Enable CAPTCHA: This setting adds a captcha to the login page to avoid brute-force attacks. See how to add captcha.
- Block Invalid Login Attempts: This setting allows you to block a specific user who fails to login after a specific number of attempts. See how to block invalid login attempts.
- Enable encryption for log archival: Enable this setting to encrypt the log data every time while archiving.
- Automatic Update for Critical Security Fixes: Enable this setting to automatically update your product to the latest build. See how to enable auto-update.

> NOTE
>
> The first three settings given in the above list are mandatory for Log360.

To ensure that you don't miss configuring any important security settings, Log360 sends the following alerts:

- Licensed users will receive a popup after every successful login to complete the mandatory security configurations.
- Admin accounts will be prompted to change the default admin password.
- A security alert will be displayed in the notification center until the security score reaches 100%.

Why we recommended Security Hardening?

To understand this, below is the breakdown of all the settings that the security hardening feature recommends:

1. Enforce HTTPS:

- This helps in preventing MITM attacks by encrypting the session between the browser and the Log360 server.
- Compliances like GDPR mandate organizations to use SSL encryption for secure data transmission.

2. Change the default Admins Password:

- Default passwords are publicly known and thus, can be easily exploited by attackers.
- Regular changes into strong passwords not only enhance security but also reduces the risk of privilege escalation.

3. Enforce two-factor authentication:

- In case the password does get compromised, attackers can still not login without the second factor.
- Also prevents unauthorized remote access.
- Some compliances make it mandatory to enable two-factor authentication.

4. Enable Reverse Proxy:

This conceals the actual IP addresses of the integrated components, making it hard for attackers to target them directly.

5. Enforce LDAP SSL:

Makes the connection secure by encrypting the traffic between Log360 and Active Directory.

6. Enable CAPTCHA:

Prevents automated brute force attacks by making manual human interaction necessary.

7. Block Invalid Login Attempts:

- Protects you against password guessing attacks and brute force attacks.
- Disables accounts temporarily after multiple repeated failed attempts.
- Flags suspicious login attempts for investigation and improves overall security monitoring.

8. Enable encryption for log archival:

Enable flat file encryption to encrypt the log data while archiving.

9. Automatic Update for Critical Security Fixes:

- Ensures that Log360 stays up to date with the latest builds and fixes for any vulnerabilities without needing any administrative burden.
- Ensures delivery of the latest security protocols of the comprehensive SIEM tool.
- Prevents exploitation of known vulnerabilities.

Security patch updates

Whenever critical vulnerabilities are discovered in the product, a security patch update is pushed to help mitigate any security threats. This option has to be enabled for automatic download of security patches whenever available.

Prerequisites for the security patch updates:

- Internet connection should be available
- Zoho creator website should be whitelisted as the patches will download from here.

Read also

This document detailed the configuration of product settings, including customization, notification preferences, and security hardening best practices. For additional features that help enhance security, administration, and automation, refer to:

- Administration settings
- Agent administration and settings

12.1.1. Extensions

Last updated on: September 12, 2025

In this page

Third-party Application Extensions

How to download and install extensions

Updating an Extension

Uninstalling an Extension

Modifying an Extension

Troubleshooting Steps for Extension Installation Failure

Extensions are pre-built software components that can either add a set of custom features into EventLog Analyzer or integrate other third-party applications into EventLog Analyzer. EventLog Analyzer's flexible platform enables it to address a wide-range of industry specific use cases.

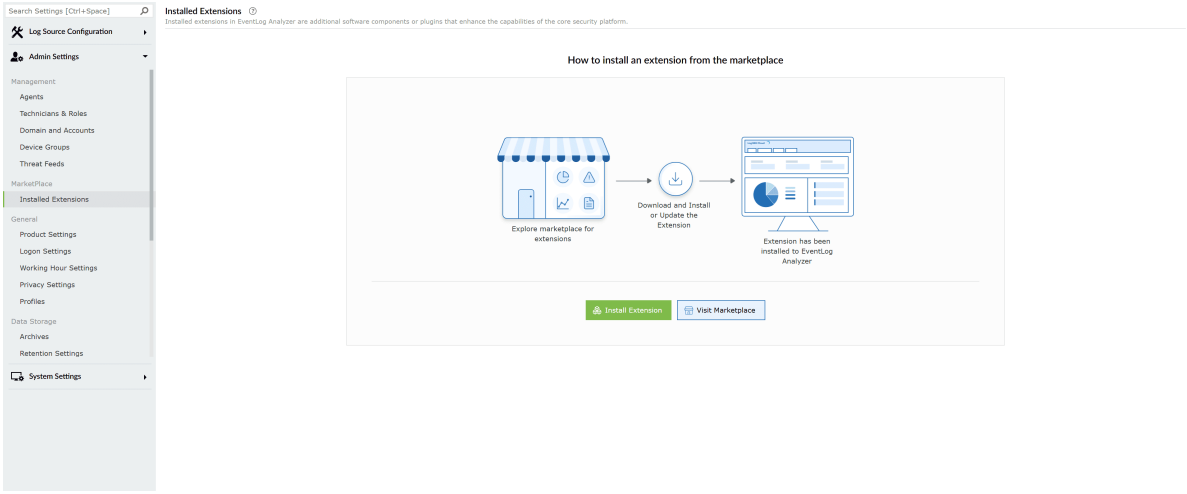
Third-party Application Extensions

Third-party application extensions enable users to integrate data from external security or business applications into EventLog Analyzer. Customers can download the extension for the application they use in their organization from the Marketplace, install it, and utilize it seamlessly.

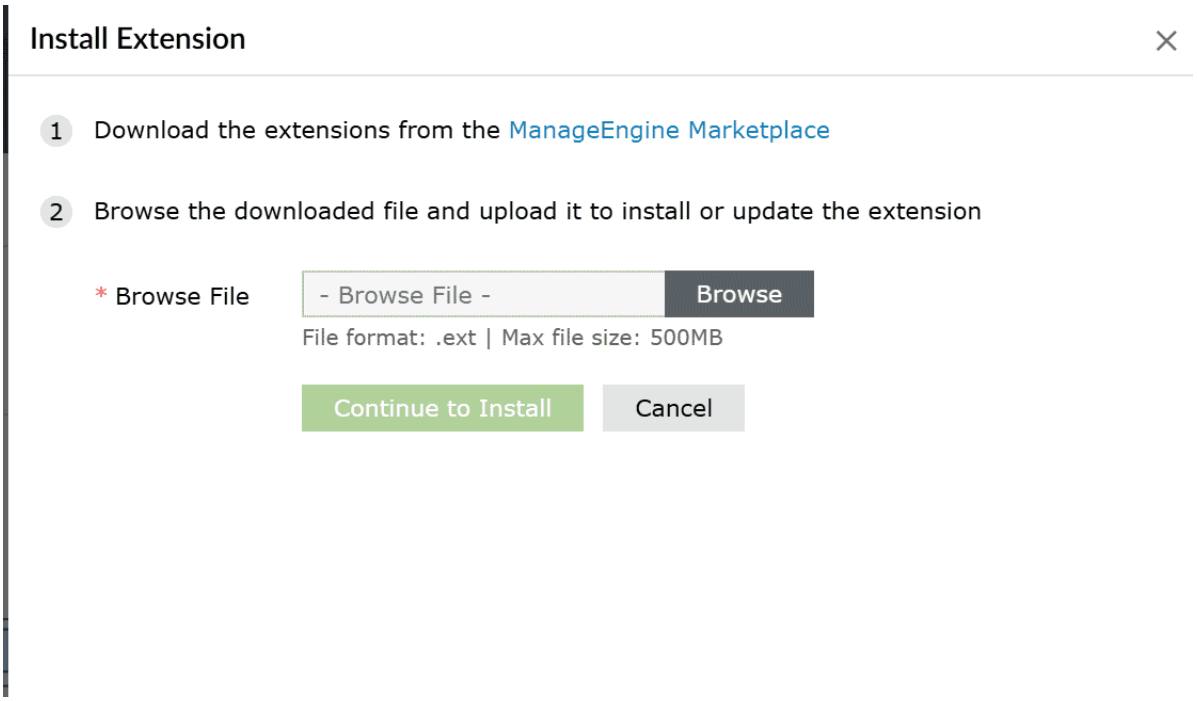
How to download and install extensions

To install an extension for EventLog Analyzer, you need to first download the extension from the Marketplace and must be uploaded to EventLog Analyzer. Here's how you can achieve this.

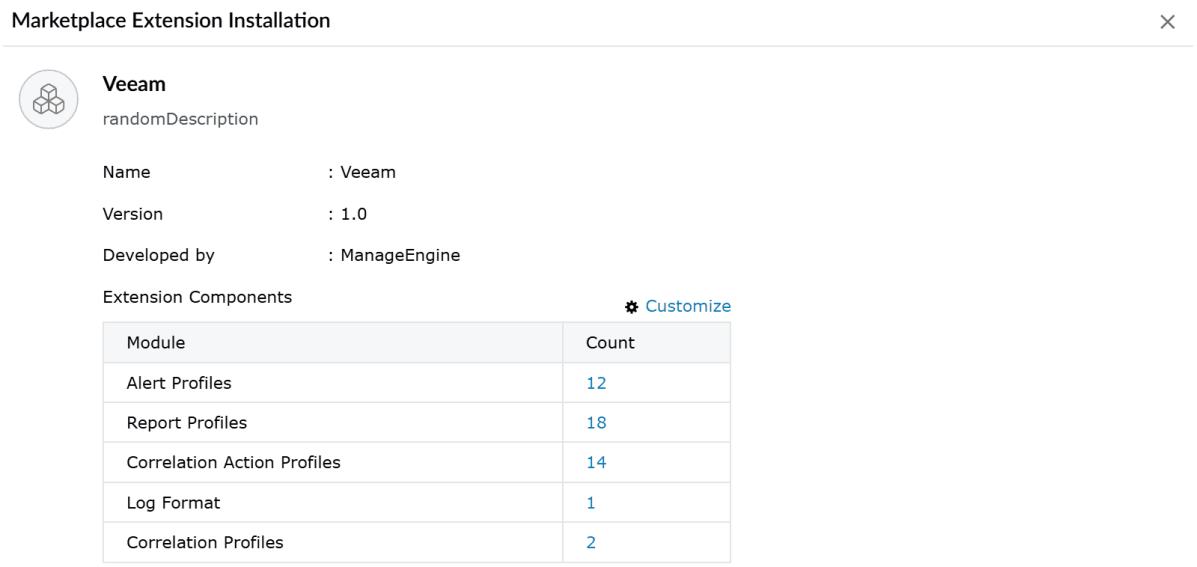
1. Download the required EventLog Analyzer extension from the Marketplace.
2. Once the download is completed, open EventLog Analyzer and navigate to Settings > Admin Settings > Marketplace > Installed Extensions.

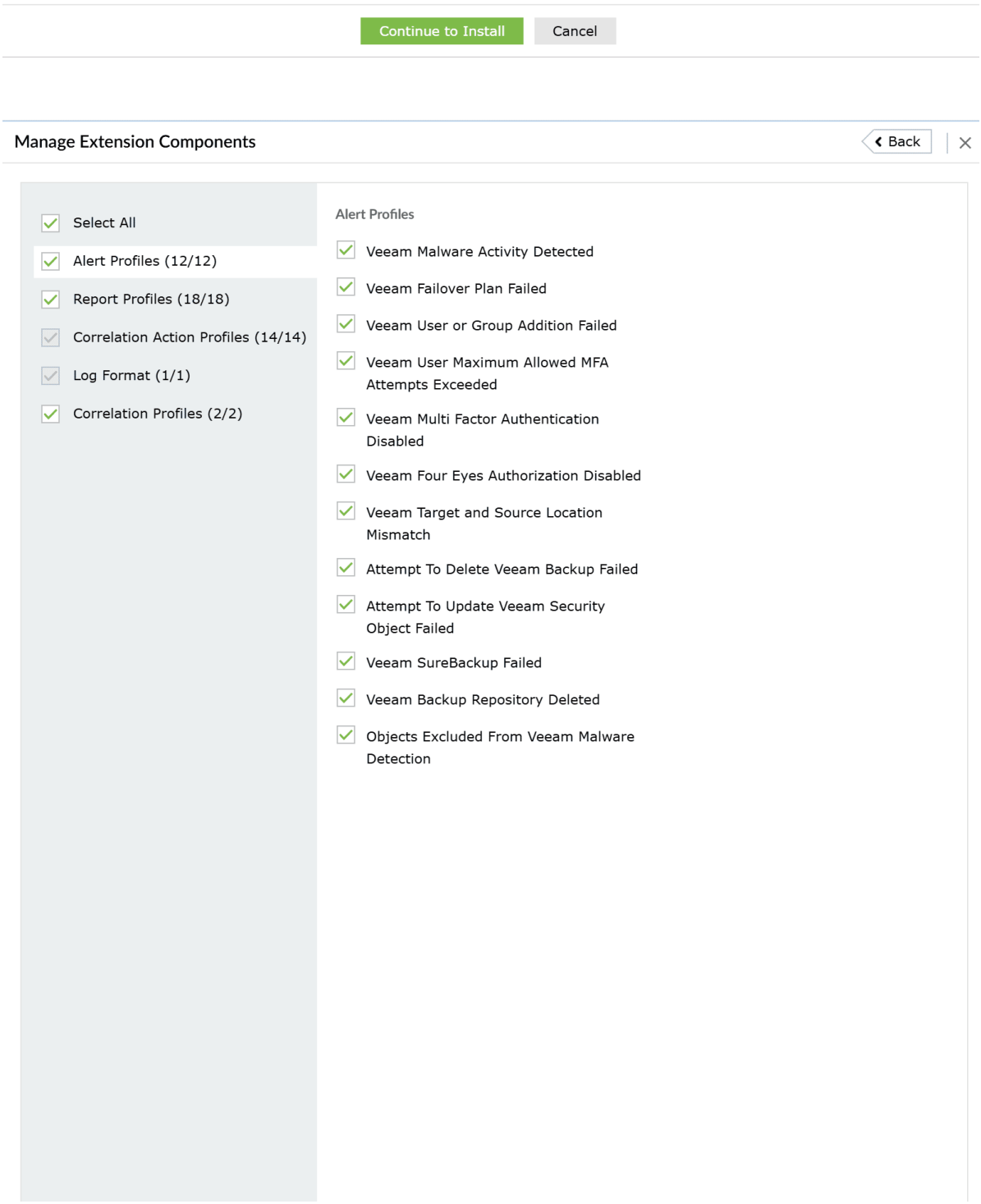


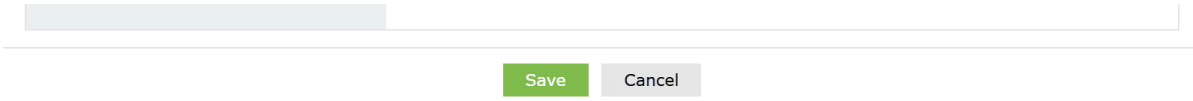
3. Click Install Extension and upload the extension.



4. Click Continue to Install to finalise the installation.
5. Before installing, you can customize extension components such as reports, log formats, and other configurations using the Customize feature.

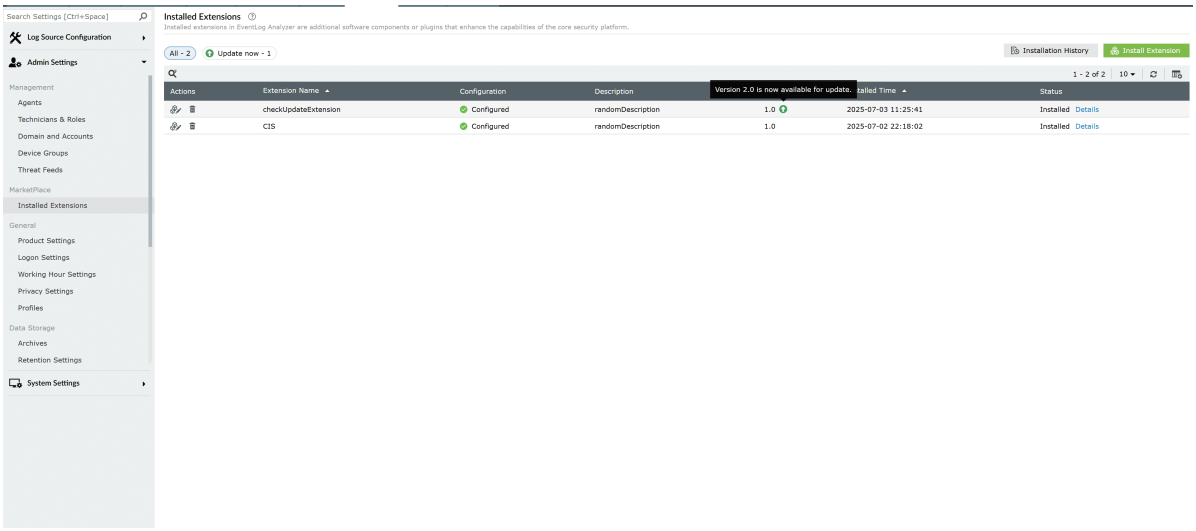


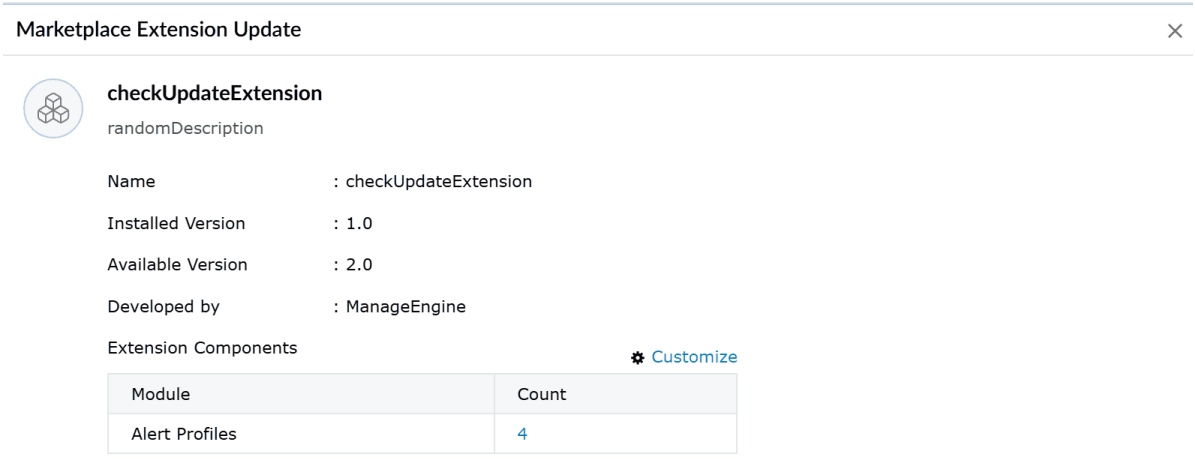

Continue to Install
Cancel
Manage Extension Components
Back
Select All
Alert Profiles (12/12)
Report Profiles (18/18)
Correlation Action Profiles (14/14)
Log Format (1/1)
Correlation Profiles (2/2)
Alert Profiles
Veeam Malware Activity Detected
Veeam Failover Plan Failed
Veeam User or Group Addition Failed
Veeam User Maximum Allowed MFA Attempts Exceeded
Veeam Multi Factor Authentication Disabled
Veeam Four Eyes Authorization Disabled
Veeam Target and Source Location Mismatch
Attempt To Delete Veeam Backup Failed
Attempt To Update Veeam Security Object Failed
Veeam SureBackup Failed
Veeam Backup Repository Deleted
Objects Excluded From Veeam Malware Detection



Updating an Extension

1. If an update is available for an installed extension, an Update icon will appear in the Installed Extensions table.





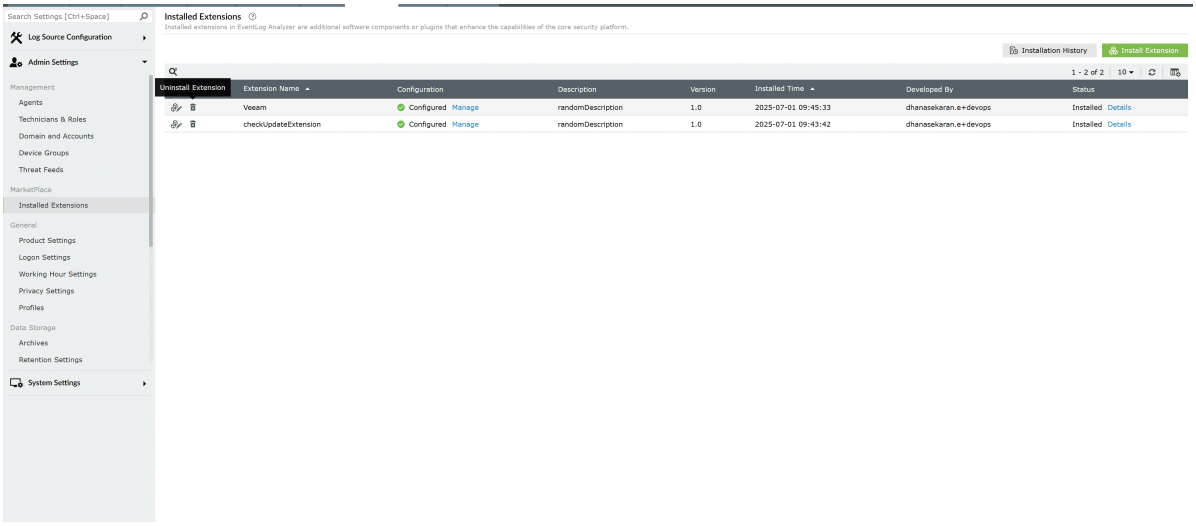


2. Click the Update icon to update the extension. You can customize the components that need to be updated.
3. The user can also manually update the extension by uploading the updated version, following the same steps used during extension installation.

Uninstalling an Extension

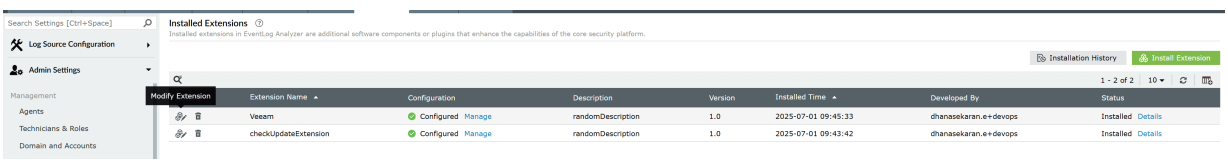
To uninstall an extension:

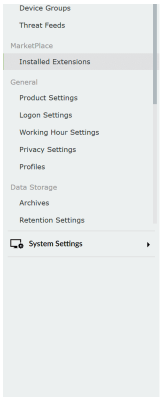
1. Click the Delete icon in the Manage Extensions table.
2. When an extension is deleted, all configurations associated with it will also be removed.



Modifying an Extension

After an extension has been customized and installed, users can reinstall components that were not initially installed by clicking the Modify icon in the Manage Extensions table.





Extension Details

To view an extension's summary, usage statistics, installation history, and contents, click Details in the Manage Extensions table.

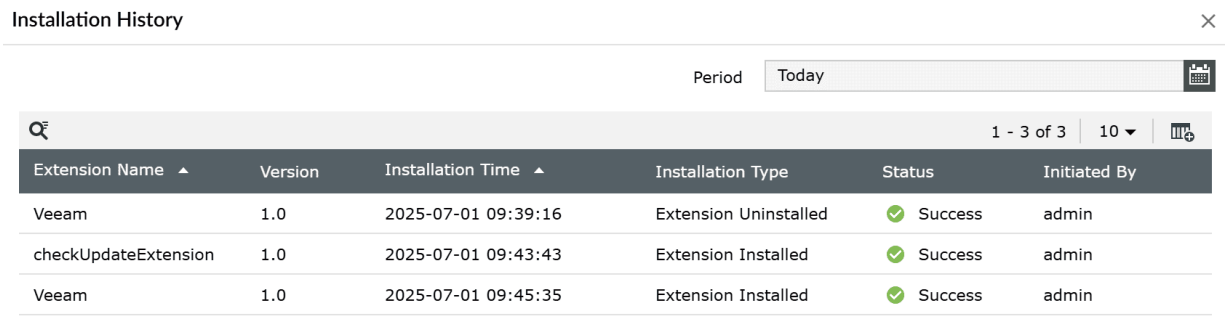
Extension Configurations

To configure applications or log sources for an extension:

1. Click Manage in the Manage Extensions table.
2. The configuration details window will open, allowing users to configure applications or log sources.

Installation History

To view the installation history of an extension, click the Installation History button.

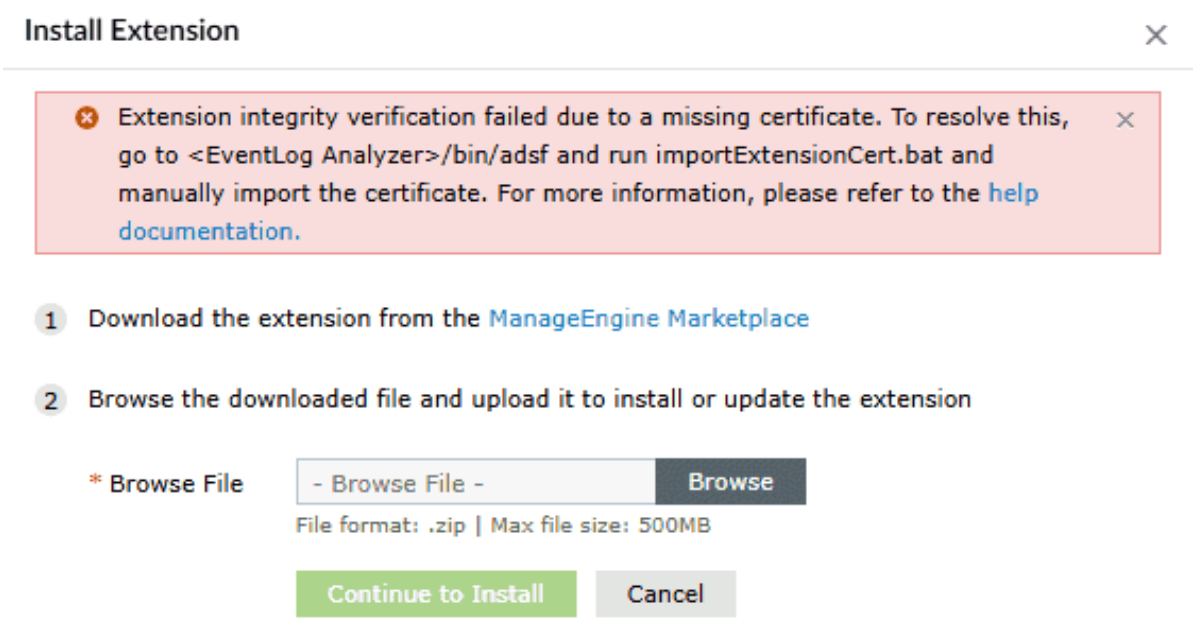


Troubleshooting Steps for Extension Installation Failure

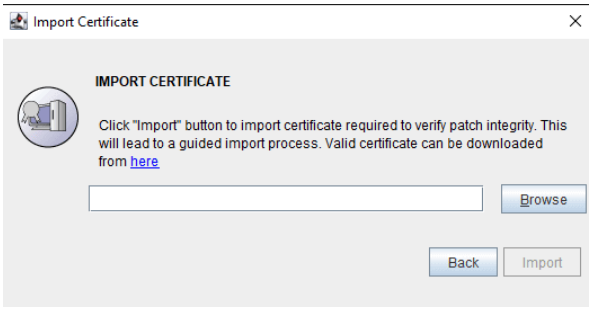
Step 1: Verify that the extension is compatible with your application's version.
Step 2: Clear your browser cache and retry the installation.
Step 3: Check the failure status in the Installation History for more details.
Step 4: If the issue persists, contact our support team or the extension developer for further assistance.

Manual Certificate Sync if Automatic Certificate Download Fails:

- If automatic certificate synchronization fails due to network issues, extension integrity verification will not occur. In such cases, the following error will appear:



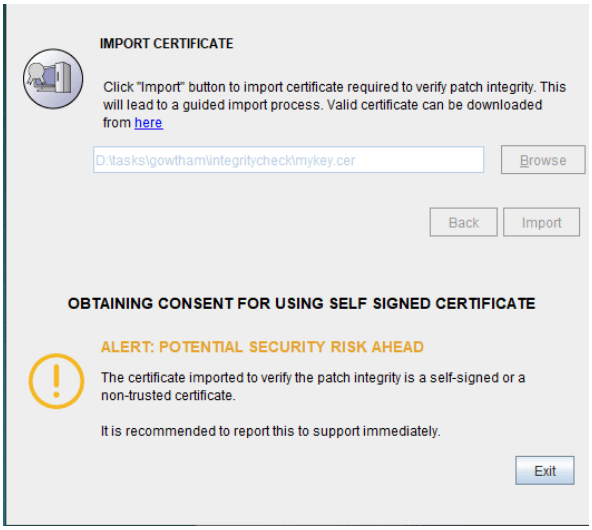
- To import the certificate manually, navigate to server_home/bin/adsf and execute importCertificate.bat (for Windows) or importCertificate.sh (for Linux/macOS).



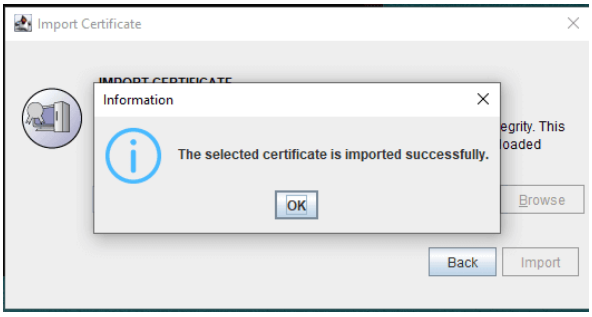
- The certificate download link will be available within the popup. Once downloaded, browse to the file and import the certificate.

> **Note**
>
> Only the certificate downloaded from the provided link can be synced. Attempting to import any other certificate will result in an error.





- After importing the appropriate certificate, a success popup will appear.



- Once the certificate is successfully imported, you can retry installing the same extension.

12.1.2. Compliance Extensions

Last updated on: September 12, 2025

In this page

Overview

Two-Factor Authentication

Email Verification

SMS Verification

Google Authenticator

RSA SecurID

Duo Security

Microsoft Authenticator

Custom TOTP Authenticator

Backup Verification Codes

Overview

Compliance Extensions provide predefined support to help you adhere to industry standards and regulatory requirements. Below are the compliance extensions available for EventLog Analyzer.

Supported Compliance Extensions

- DORA (Digital Operational Resilience Act)
  - DORA is an EU regulation designed to enhance the financial sector's ability to withstand cyber threats by establishing strict ICT risk management, incident reporting, and resilience testing requirements. To download the DORA extensions, visit marketplace.
- DPDP (Digital Personal Data Protection Act)
  - The DPDP Act is India's comprehensive data protection law that governs the processing of personal data, ensuring user rights, lawful data handling, and corporate accountability. To download the DPDP extensions, visit marketplace.
- CJIS (Criminal Justice Information Services)
  - The CJIS Security Policy sets standards for protecting sensitive law enforcement data in the U.S., ensuring strict access control, encryption, and auditing requirements for agencies and service providers. To download the CJIS extensions, visit marketplace.
- CIS (Center for Internet Security Controls)
  - CIS Controls are a set of best practices and security guidelines designed to help organizations protect

against cyber threats by implementing essential security measures and system hardening techniques. To download the CIS extensions, visit marketplace.

- Standard Framework for Education
  - The Standard Framework for Education provides guidelines and best practices for educational institutions to ensure compliance with relevant regulations and standards. To download the Standard Framework for Education extensions, visit marketplace.

Related resources

1. How to install an extension

12.1.3. Veeam

Last updated on: September 12, 2025

In this page

Overview

Veeam extension scope

Audited Veeam events

How to configure Veeam log source

Enabling event forwarding

Enabling correlation profiles

Enabling alert profiles

Viewing Veeam reports

Veeam events

Overview

Veeam is a data protection and disaster recovery solution designed for modern IT environments. It provides backup, replication, and recovery capabilities for virtual, physical, cloud, and SaaS workloads.

Veeam extension scope

The Veeam extension for EventLog Analyzer is designed to enable seamless integration of log data from Veeam Backup & Replication or Veeam ONE into the EventLog Analyzer ecosystem. This extension provides features such as log collection, parsing, reporting, alerting, correlation, and advanced log search capabilities.

Audited Veeam events

Authentication and authorization

- MFA management
- Password and credential management
- Four-eyes authorization events

Identity management

- User and group management

Malware detection

- Malware detection configuration changes
- Malware detection session completion events
- Malware activity detection events
- Malware remediation actions

Configuration management

- Global network traffic rule changes
- Global VM exclusion changes
- General settings changes
- Host configurations

Jobs

- Job sessions history
- Job configurations
- Restore sessions history

Infrastructure management

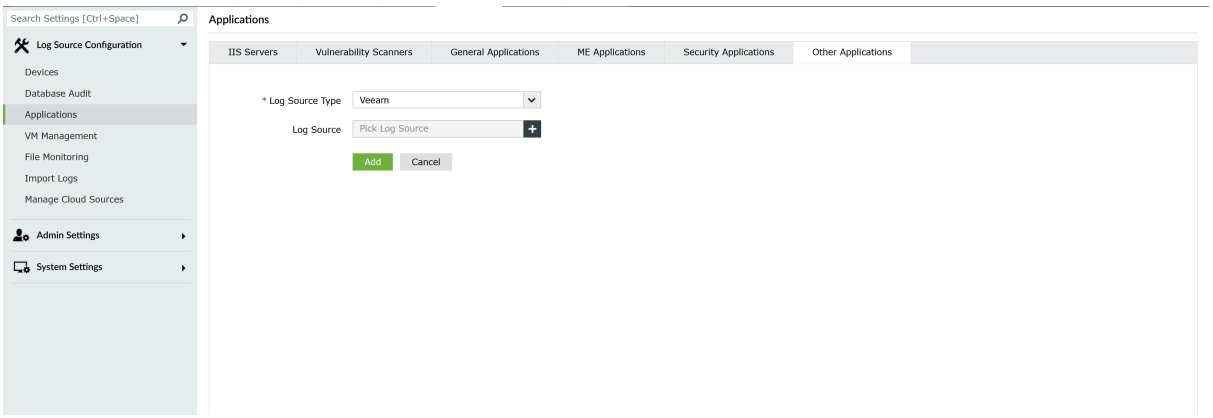
- Failover plan management
- Failover plan execution history
- Infrastructure location changes

Licensing

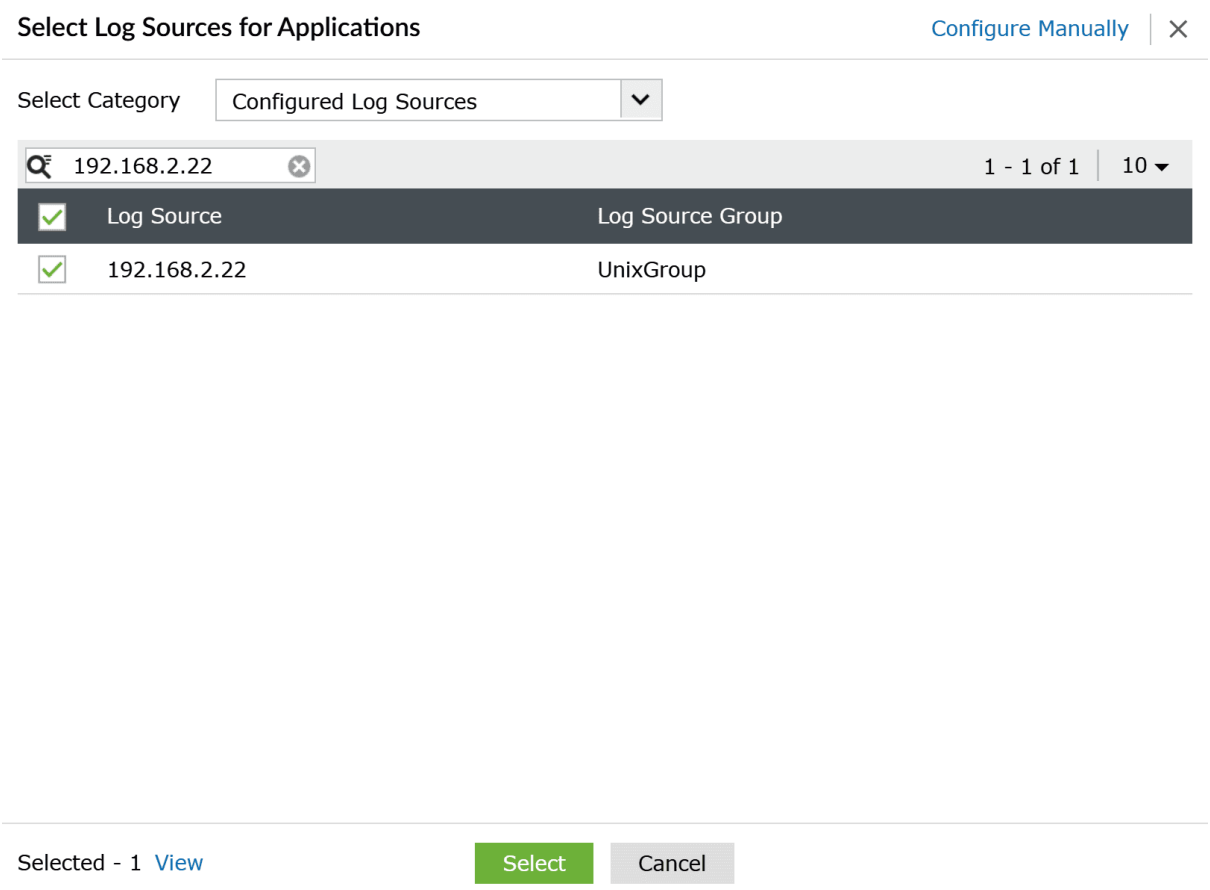
- License updates

How to configure Veeam log source

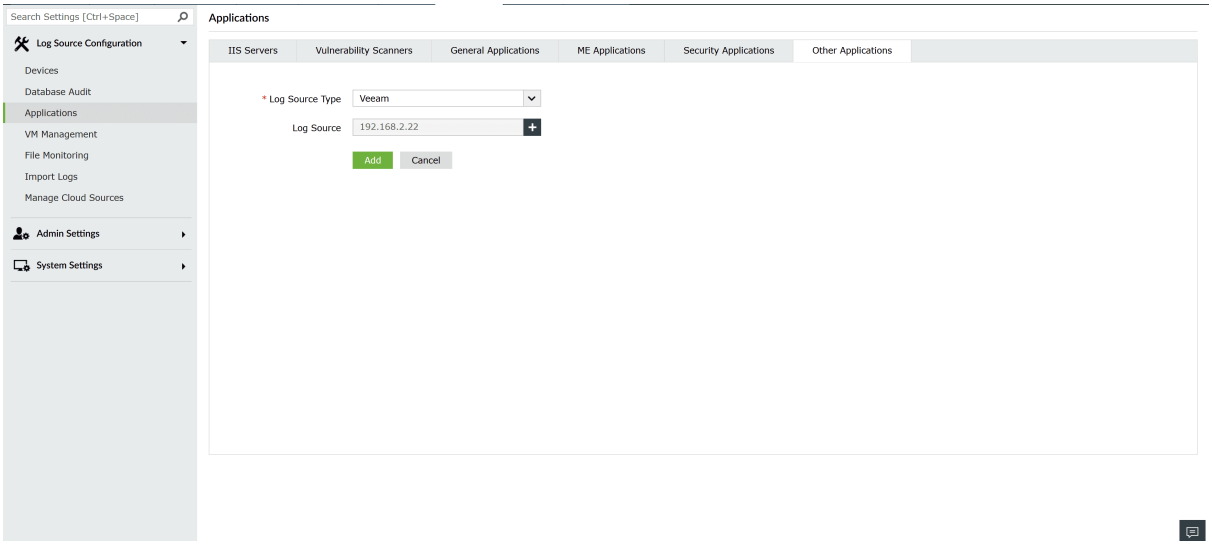
1. After installing the Veeam extension, configure the log sources by navigating to Settings > Applications > Other Applications.
2. Select Veeam from the Log Source Type dropdown.
3. Click the + icon to add a new device.



4. Choose a pre-configured host where Veeam Backup & Replication Server or Veeam ONE Server is installed. If the host is not pre-configured, click Configure Manually and enter the hostname or IP.



5. Click Add to save the configuration.



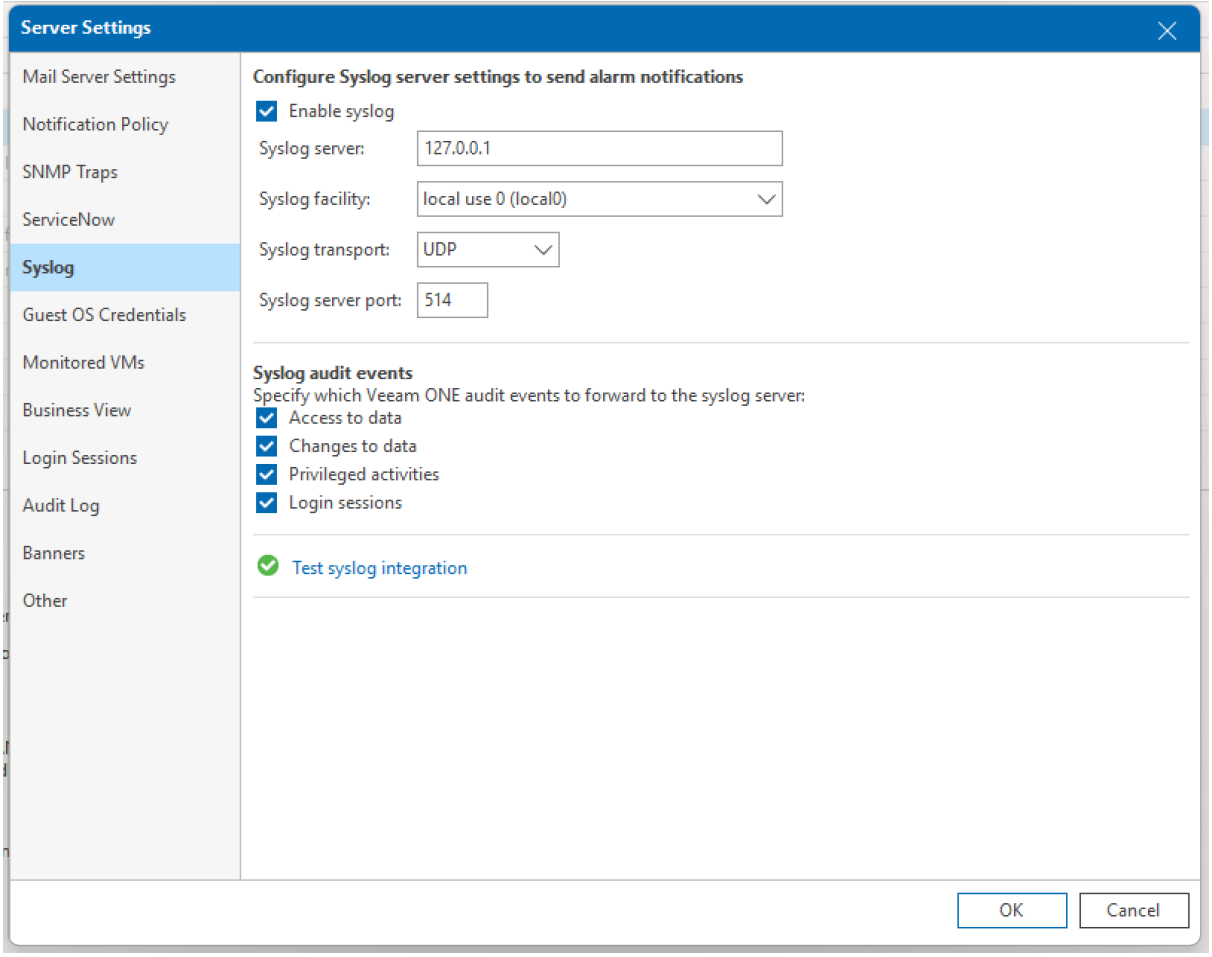
Enabling event forwarding

After configuring the log source, enable event forwarding in either Veeam ONE or Veeam Backup & Replication

to send events to EventLog Analyzer. This requires a Veeam Data Platform Advanced or Premium license that supports syslog event forwarding.

Event forwarding in Veeam ONE

1. Open Veeam ONE Client and navigate to Server Settings > Syslog.
2. Check Enable Syslog.
3. In Syslog server, enter the Hostname or IP of the EventLog Analyzer server in the log source.
4. Select mail under the Syslog facility dropdown.
5. Choose UDP or TCP under the Syslog transport dropdown.
6. Enter a port in which the EventLog Analyzer server is listening for Syslogs.
7. Check all options under Syslog audit events to enable comprehensive search and reporting in EventLog Analyzer.
8. Click OK to save the configuration.

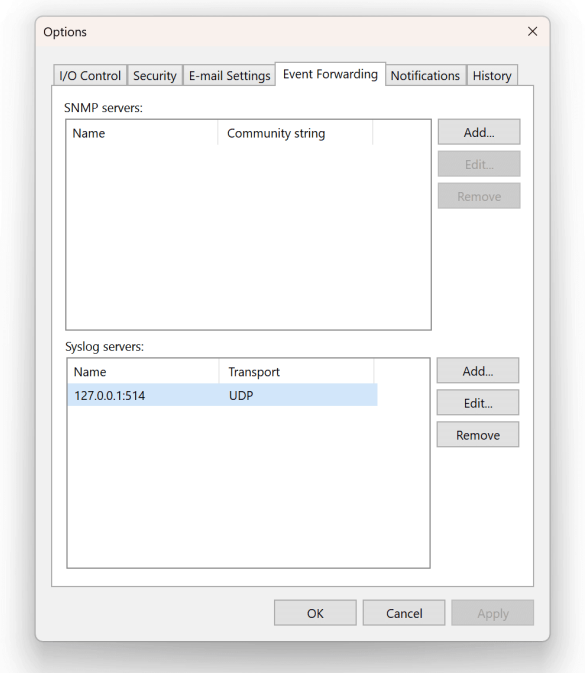


For detailed steps, refer to the official guide on Syslog integration in Veeam ONE.

Event forwarding in Veeam Backup & Replication

1. Open Veeam Backup & Replication Console and go to Options > Event Forwarding.
2. Click Add under Syslog servers to configure a Syslog server.
3. In the Server field, provide the Hostname or IP of the EventLog Analyzer server.

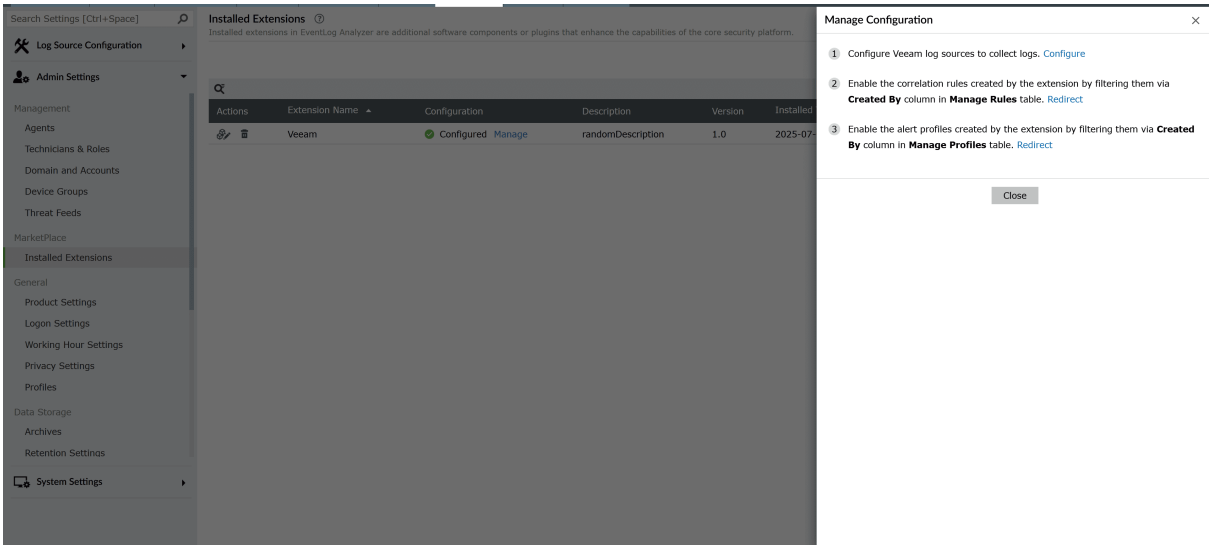
4. Enter a port in which the EventLog Analyzer server is listening for Syslogs.
5. Select UDP or TCP under the Transport dropdown.
6. Click OK to add the syslog server, then click Apply to save changes.



For more details, refer to the official guide on Syslog integration in Veeam Backup & Replication.

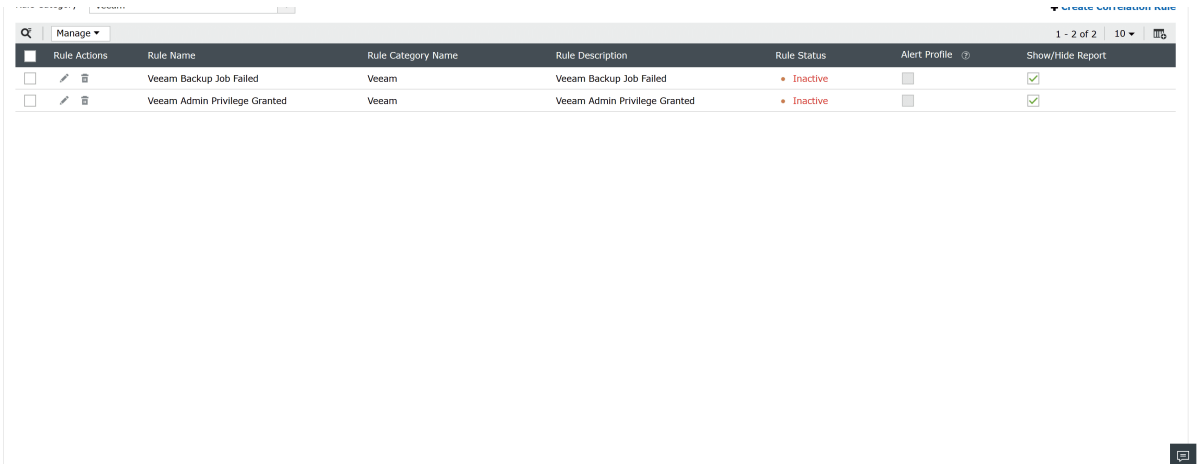
Enabling correlation profiles

1. Go to Settings > Marketplace > Installed Extensions. Click Manage under Configuration to open the Manage Configuration page.



2. Click Redirect next to Correlation Rules to open the Correlation tab. Select Veeam from the Rule Category selector to view the available correlation rules.

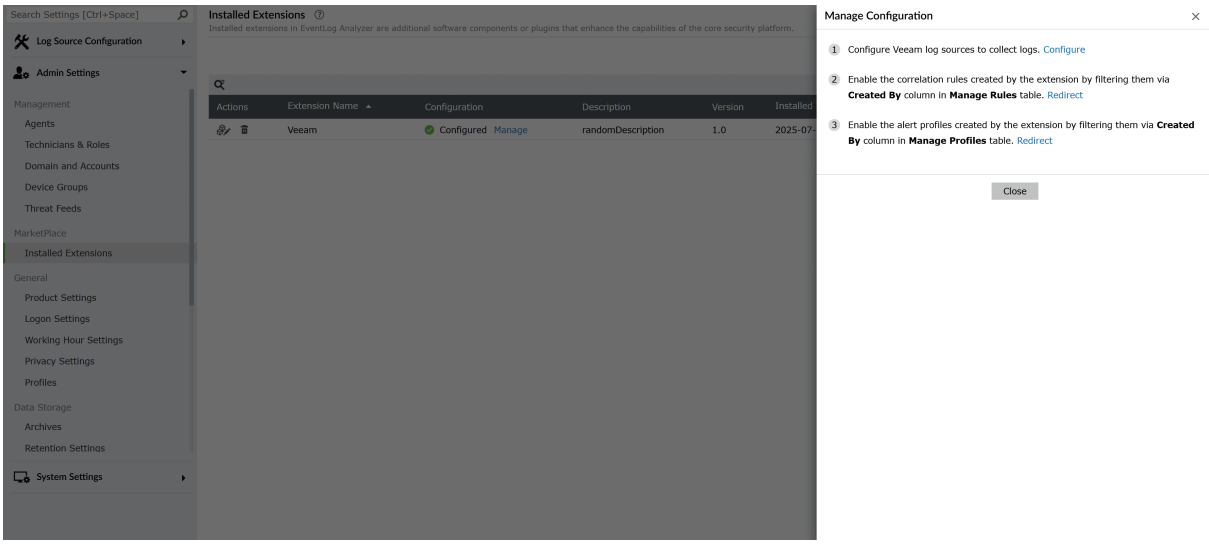




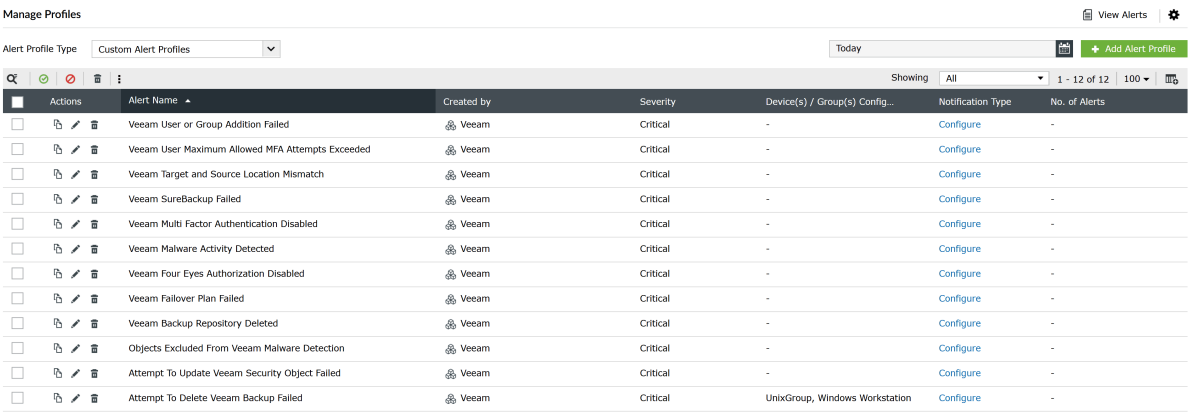
3. Review the available correlation rules and enable the required ones.

Enabling alert profiles

1. After configuring the log source, navigate to Settings > Marketplace > Installed Extensions. Click Manage under configuration to open the Manage Configuration page.



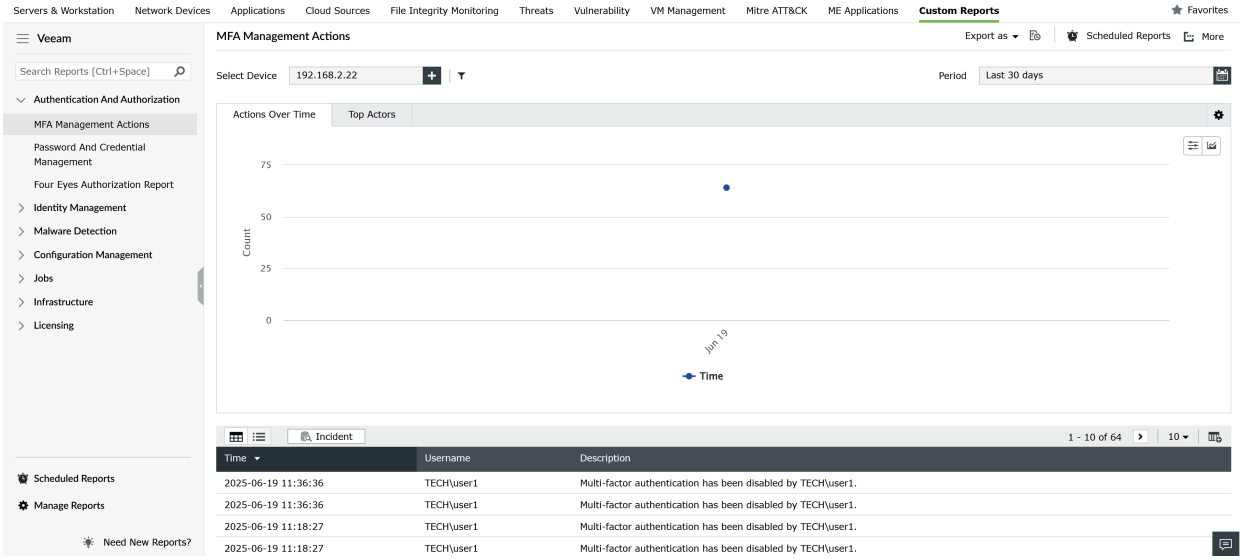
2. Click Redirect next to Alert Profiles to navigate to the Alerts tab. Extension alert profiles appear under Custom Alert Profiles. Use the Created By column to identify Veeam alert profiles.



3. Browse the available alert profiles and enable the required ones.

Viewing Veeam reports

To view Veeam reports, navigate to the Reports tab and select Veeam under custom reports.



Veeam events

Below is a list of Veeam events that EventLog Analyzer can track, helping you monitor backup and recovery activities effectively.

Instance ID	Event name
151	File Backup Job Finished
190	Backup Job Finished
194	File to Tape Job Finished
195	Tape Erase Job Finished
199	Tape Export Job Finished
200	Tape Copy Job Finished
203	Tape Eject Job Finished

205	Move To Media Pool Job Finished
206	Delete From Library Job Finished
208	Tape Import Job Finished
23010	Job Created
23050	Job Settings Updated
23090	Job Deleted
23110	Objects for Job Added
23130	Objects for Job Changed
23210	SureBackup Job Created
23220	SureBackup Job Settings Updated
23230	SureBackup Job Deleted
23310	Objects for SureBackup Job Added
23320	Objects for SureBackup Job Deleted
23410	Job Assigned as Secondary Destination
23420	Job No Longer Used as Secondary Destination
23440	Tape Job Created
23450	Tape Job Settings Updated
23490	Tape Job Deleted
23510	Objects for Tape Job Added

23520	Objects for Tape Job Deleted
23530	Objects for Tape Job Changed
24010	License Installed
24030	License Expired
24050	License Support Expired
24060	License Grace Period Started
24070	License Limit Exceeded
24080	License Removed
25300	Credential Record Added
25400	Credential Record Updated
25500	Credential Record Deleted
25900	Failover Plan Created
26000	Failover Plan Settings Updated
26010	Target Location Does Not Match Source Location
26100	Failover Plan Deleted
26110	Failover Plan Failed
26600	Failover Plan Started
26700	Failover Plan Stopped

28300	Host Added
28400	Host Settings Updated
28500	Host Deleted
31000	General Settings Updated
31100	Global Settings for Network Traffic Rules Updated
31200	User or Group Added
31210	Adding User or Group Failed
31400	User or Group Deleted
31600	Encryption Password Added
31700	Encryption Password Updated
31800	Encryption Password Deleted
31900	SSH Credentials Changed
32120	Objects for Job Deleted
32300	Global Network Traffic Rules Added
32400	Global Network Traffic Rules Deleted
32500	Global Network Traffic Rules Updated
32600	Preferred Networks Updated
32700	Preferred Networks Added

32800	Preferred Networks Deleted
36022	Backup Job for Application Backup Policy Finished
36026	Log Backup Job for Application Backup Policy Finished
390	SureBackup Job Finished
40200	Multi-Factor Authentication Enabled
40201	Multi-Factor Authentication Disabled
40202	Multi-Factor Authentication Token Revoked
40203	Multi-Factor Authentication for User Enabled
40204	Multi-Factor Authentication for User Disabled
40206	Allowed Attempts for Multi-Factor Authentication Exceeded
40290	Restore Session Finished
40400	Global VM Exclusions Added
40500	Global VM Exclusions Deleted
40600	Global VM Exclusions Changed
40700	Configuration Backup Job Finished
40900	Location Added
40901	Location Settings Updated
40902	Location Deleted

40903	Object Location Changed
41600	Malware Activity Detected
41710	Health Check Job Finished
41800	Attempt to Delete Backup Failed
41810	Attempt To Update Security Object Failed
42210	Malware Detection Session Finished
42260	Objects Added to Malware Detection Exclusions
42270	Objects Deleted from Malware Detection Exclusions
42280	Malware Detection Exclusions List Updated
42290	Malware Detection Settings Updated
42400	Four-Eyes Authorization Enabled
42401	Four-Eyes Authorization Disabled
42402	Four-Eyes Authorization Request Created
42403	Four-Eyes Authorization Request Approved
42404	Four-Eyes Authorization Request Rejected
42405	Four-Eyes Authorization Request Expired
451	File Backup Copy Job Finished
490	Backup Copy Job Finished
590	File Copy Job Finished

592	VM Copy Job Finished
610	Quick Migration Finished
28200	Backup Repository Deleted
42260	Objects Added to Malware Detection Exclusions
41610	Object Marked as Clean
42220	Restore Point Marked as Infected
42230	Restore Point Marked as Clean

Related resources

1. How to install an extension

12.1.4. Dropbox

Last updated on: September 12, 2025

Dropbox is a cloud-based file storage and collaboration platform that enables users to securely store, sync, and share files across multiple devices. It provides businesses and individuals with easy access to files from anywhere, ensuring seamless collaboration and data protection.

Dropbox extension scope

The Dropbox Audit Log Monitoring Extension empowers organizations to monitor continuously and analyze Dropbox audit logs, ensuring comprehensive visibility into critical activities. By capturing and evaluating events such as user actions, access patterns, and security changes, this extension helps mitigate risks, ensure compliance, and enhance operational efficiency. It enables organizations to detect unusual login attempts, identify potential insider threats, and stay ahead of evolving security challenges.

Audited Dropbox events

Security events

- Ransomware and admin alerts
- Authentications and sessions
- Passwords and TFA
- Encryption and key management

File and folder events

- File and folder operations
- File request and transfer events

Integrations and apps

- Integrations and apps events

Members and groups

- Invite link activity
- Member management activity
- Group management activity

Device management

- Device link and status Changes

Legal holds

- Legal hold events

Reports management

- Report management activity

Sharing

- Shared content
- Link actions

Team policies

- Web session policy
- Password and TFA policy
- Sharing and smart sync policy
- Signature policy
- Member and team policy
- Third party policy
- File and backup policy
- Governance policy

Team profile

- Data residency migration
- Team profile customization actions

Signatures

- Signature management Activity

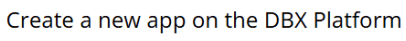
Trusted teams

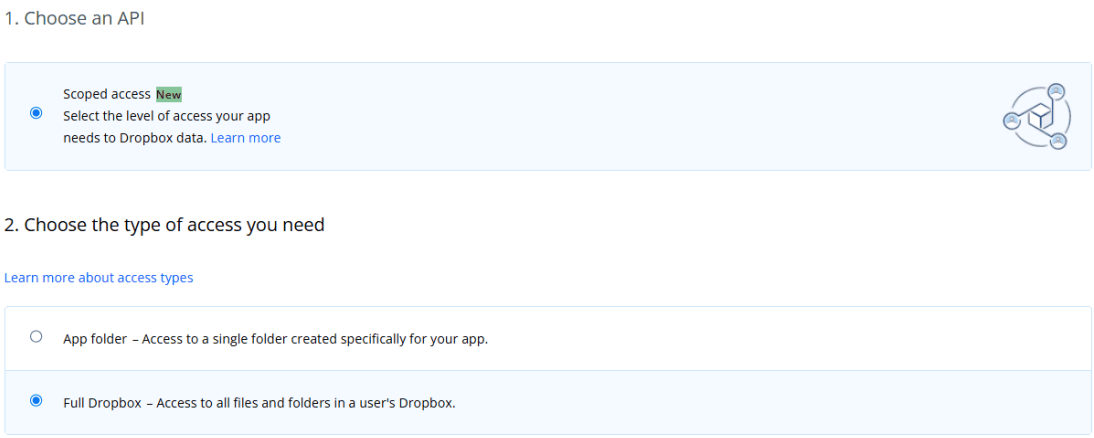
- Enterprise management activity
- Team merge activity

Configuring Dropbox integration

Setting up a Dropbox account and application

1. Sign in to your Dropbox account and navigate to the Dropbox Developers Console.
2. Click Create New App and select Scoped Access.
3. Choose Full Dropbox Access as the access type.

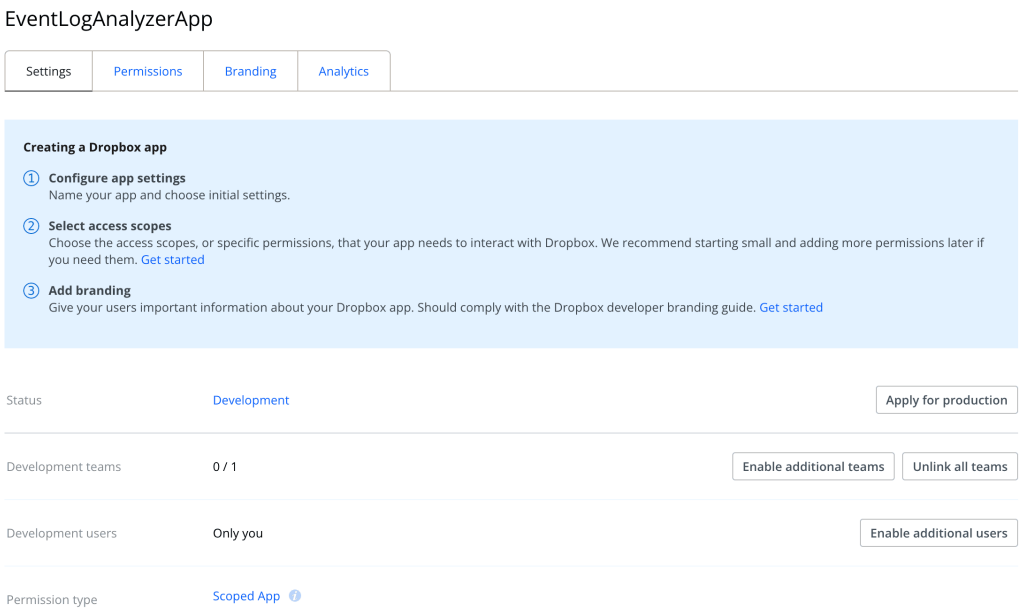




4. Provide a name for your app, agree to the Dropbox terms and conditions, and then click Create App.

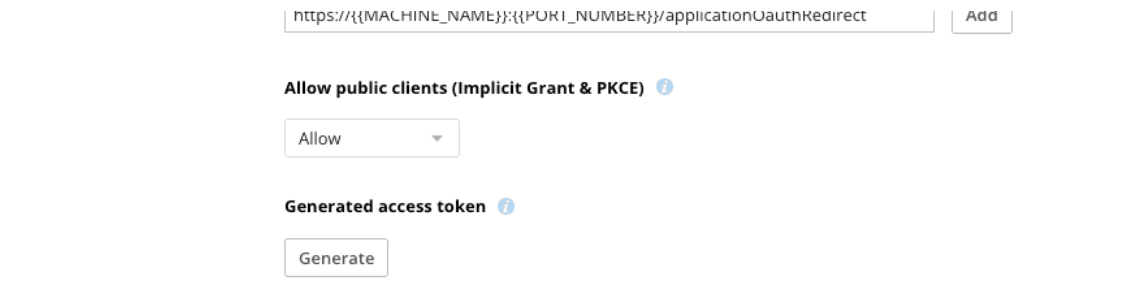


5. Once the app is created, the App Settings page will be displayed.

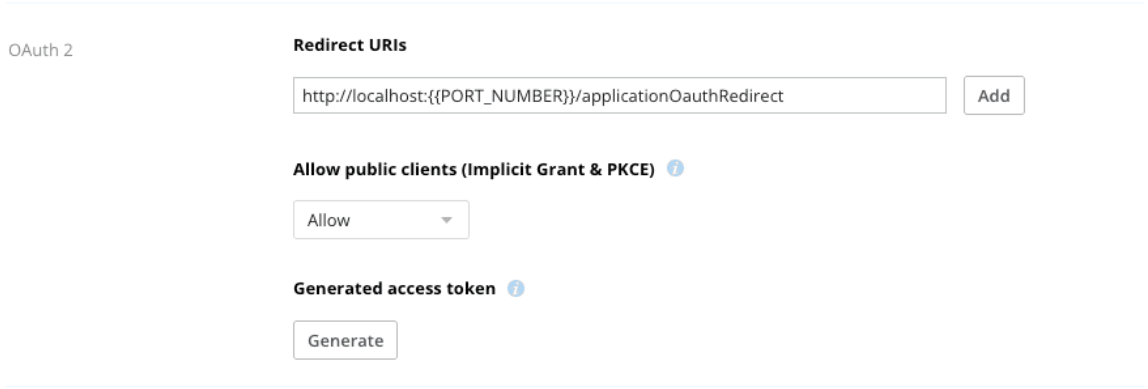


6. In the App Settings tab, enter the specified Redirect URL in the Redirect URLs textbox. Replace {{MACHINE_NAME}} and {{PORT_NUMBER}} with the actual machine name and the port number where the EventLog Analyzer instance is running.

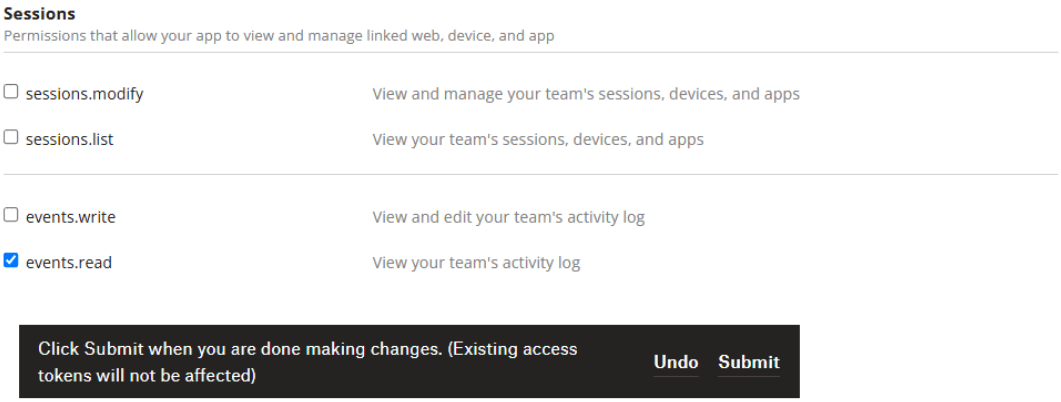




- If EventLog Analyzer is running in HTTP mode, use localhost as the machine name along with the appropriate {{PORT_NUMBER}}.



7. Navigate to the Permissions tab, scroll down, and enable team_data.member, events.read, members.read, files.metadata.read, sharing.read and sessions.list permissions.

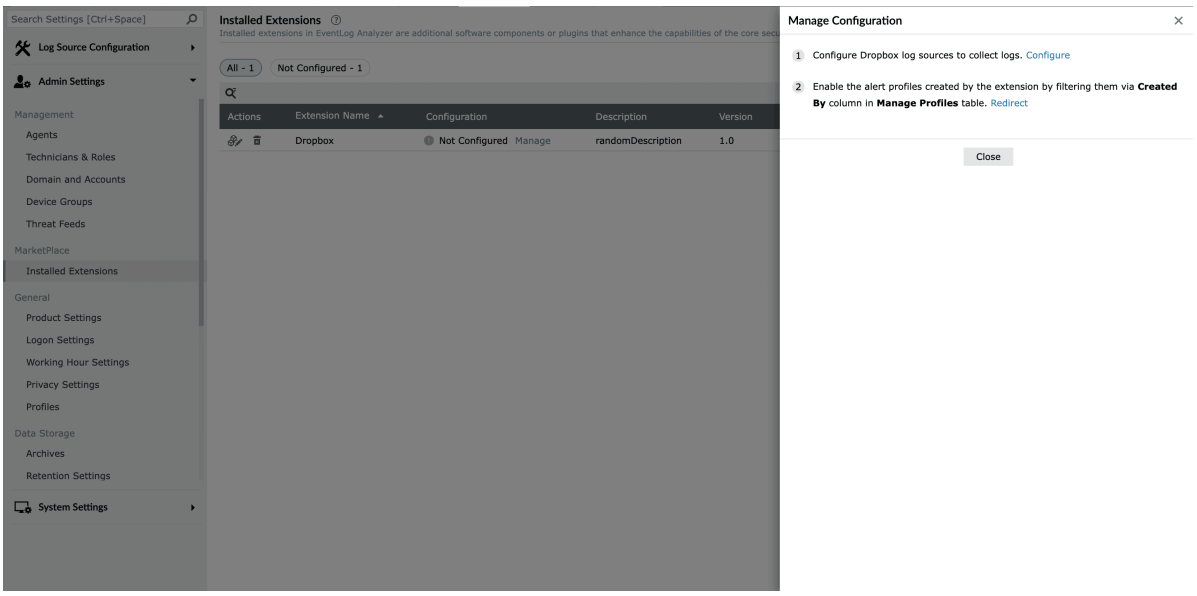


8. Click Submit to complete the Dropbox app configuration.
9. From the Settings tab, copy the Client ID and Client Secret values from the App ID and App Secret fields. These will be needed later while configuring Dropbox in EventLog Analyzer.

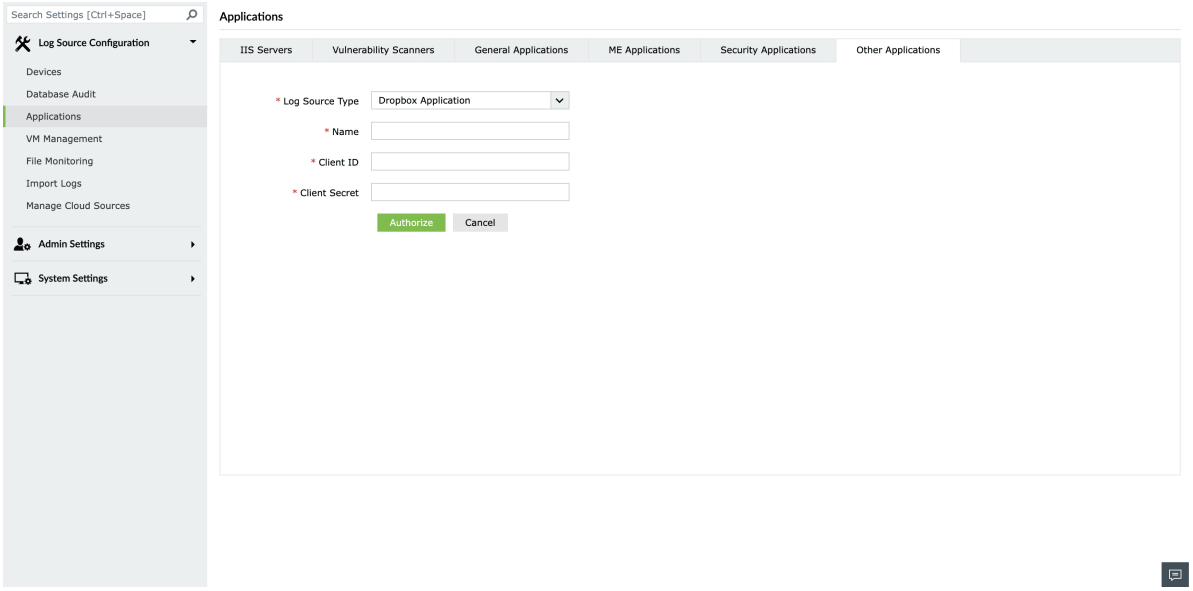
Configuring Dropbox in EventLog Analyzer

- In EventLog Analyzer, navigate to Settings → Marketplace.
- Locate and install the Dropbox Extension from the Marketplace.
- To verify installation, go to Settings → Marketplace → Installed Extensions and ensure Dropbox is listed.

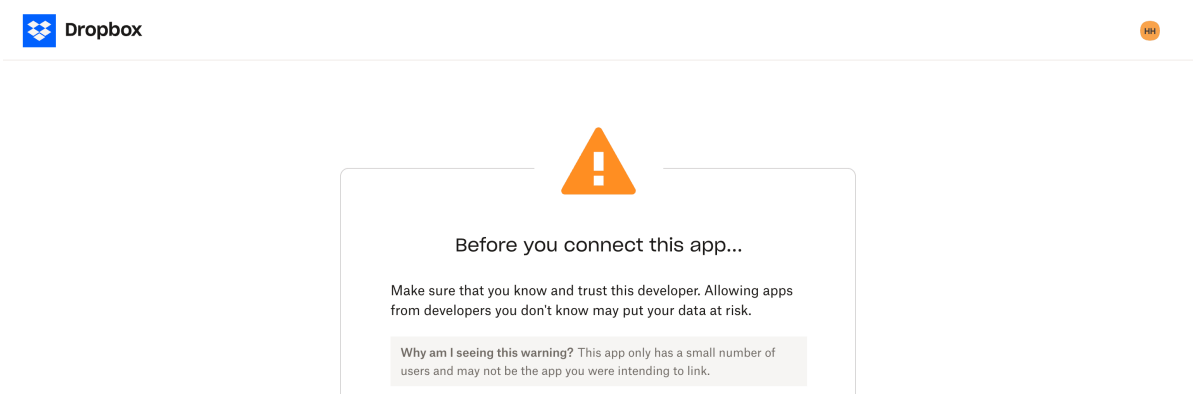
- Click Manage under the Dropbox extension to open the Manage Configuration page.

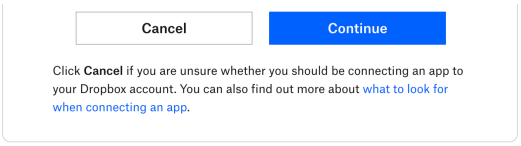


- Click Configure to open the configuration page or navigate to Settings → Applications → Other Applications.

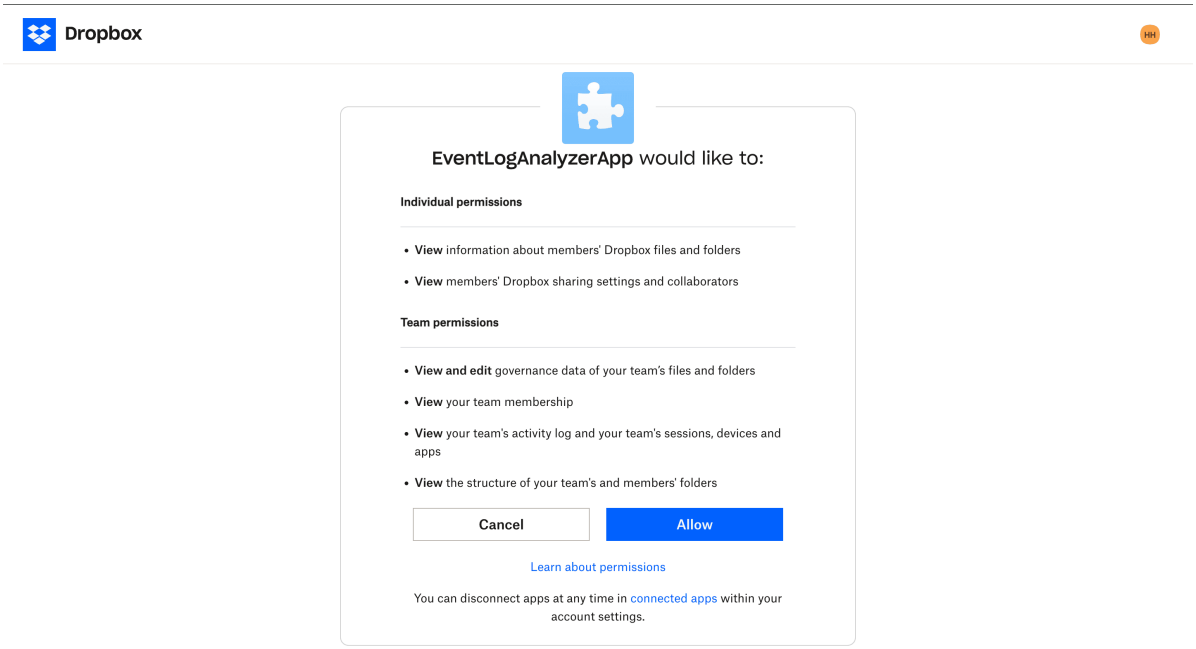


- Enter the Client ID and Client Secret obtained from the Dropbox Developer Console.
- Click Authorize. A pop-up will appear requesting consent.



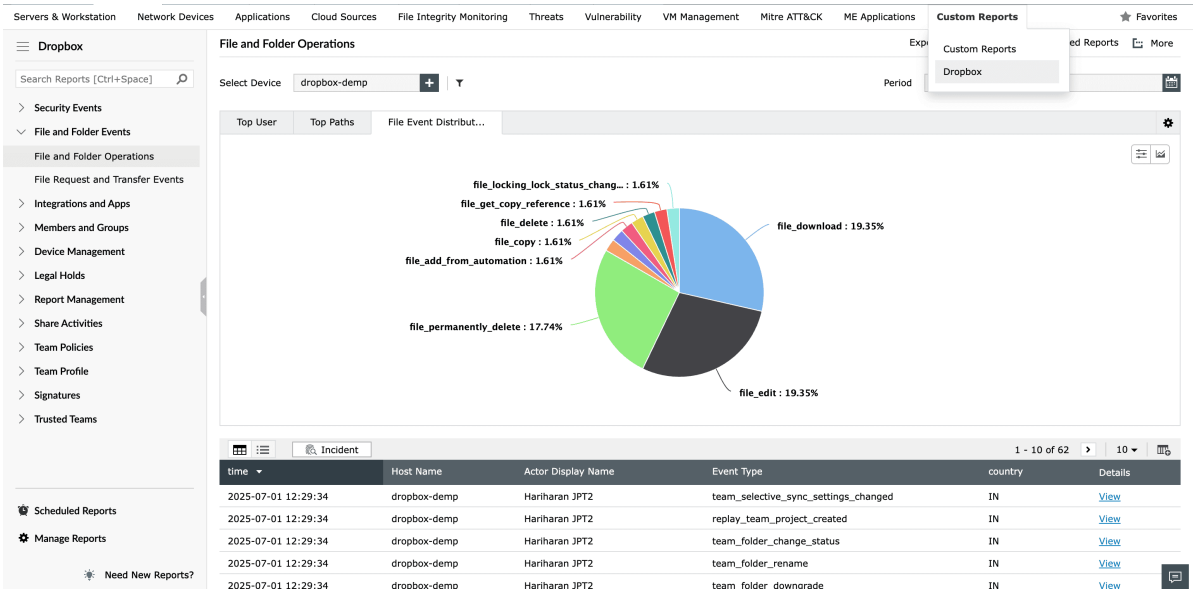


- Accept the consent request to complete the configuration.



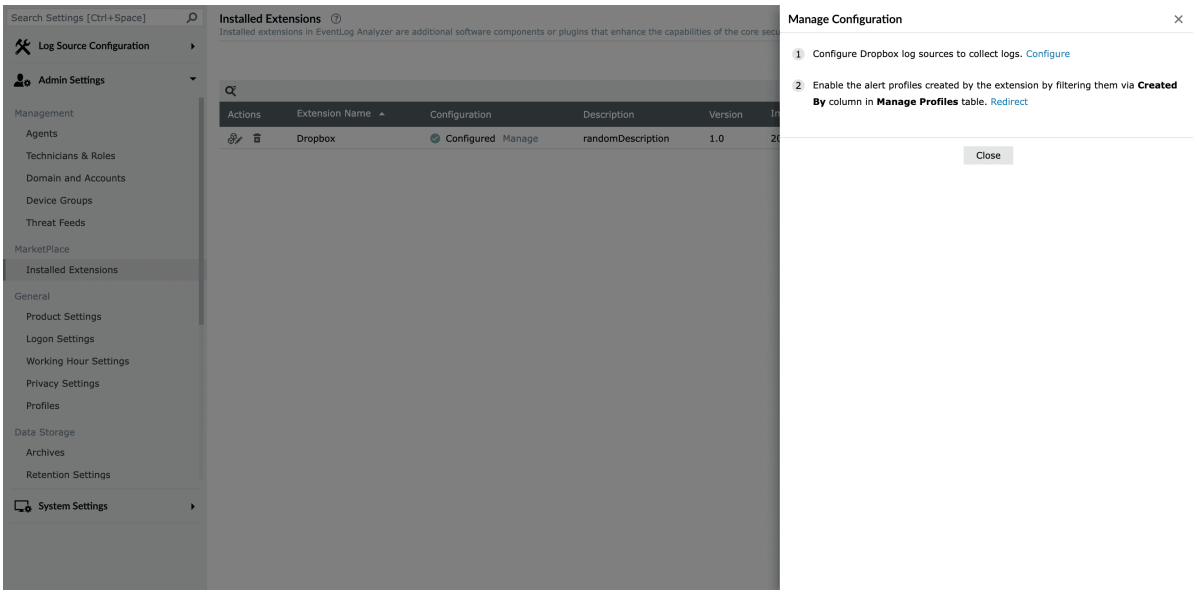
Accessing Dropbox reports

- Navigate to Reports → Custom Reports → Dropbox to view Dropbox-related reports.

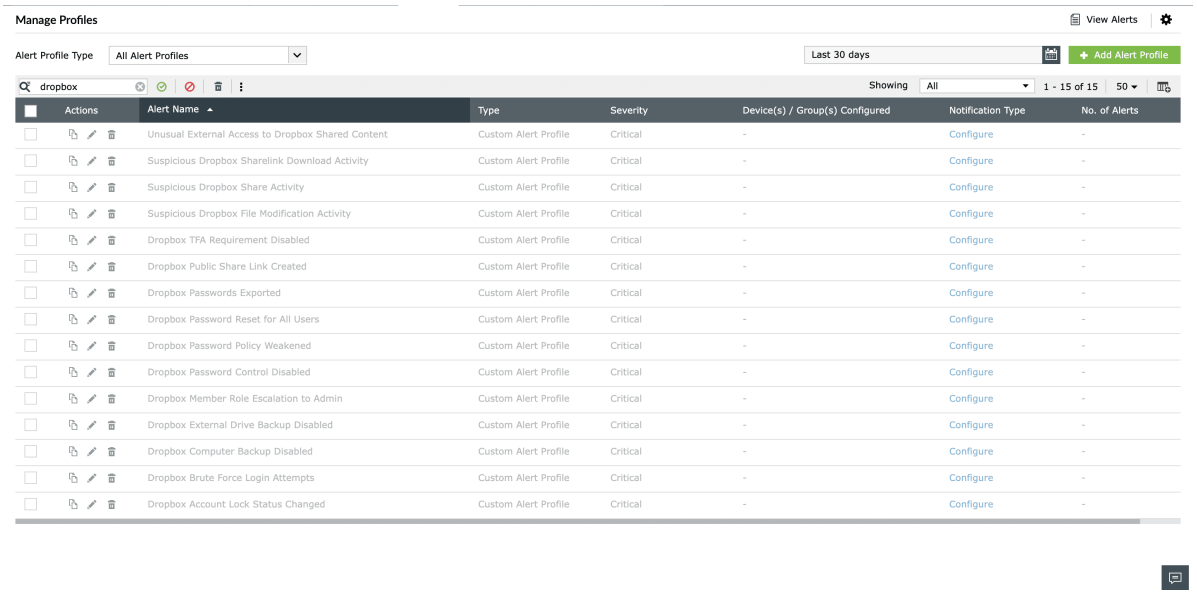


Configuring Dropbox alerts

- After configuring the log source, go to Settings → Marketplace → Installed Extensions.
- Click Manage under the Dropbox extension to open the Manage Configuration page.



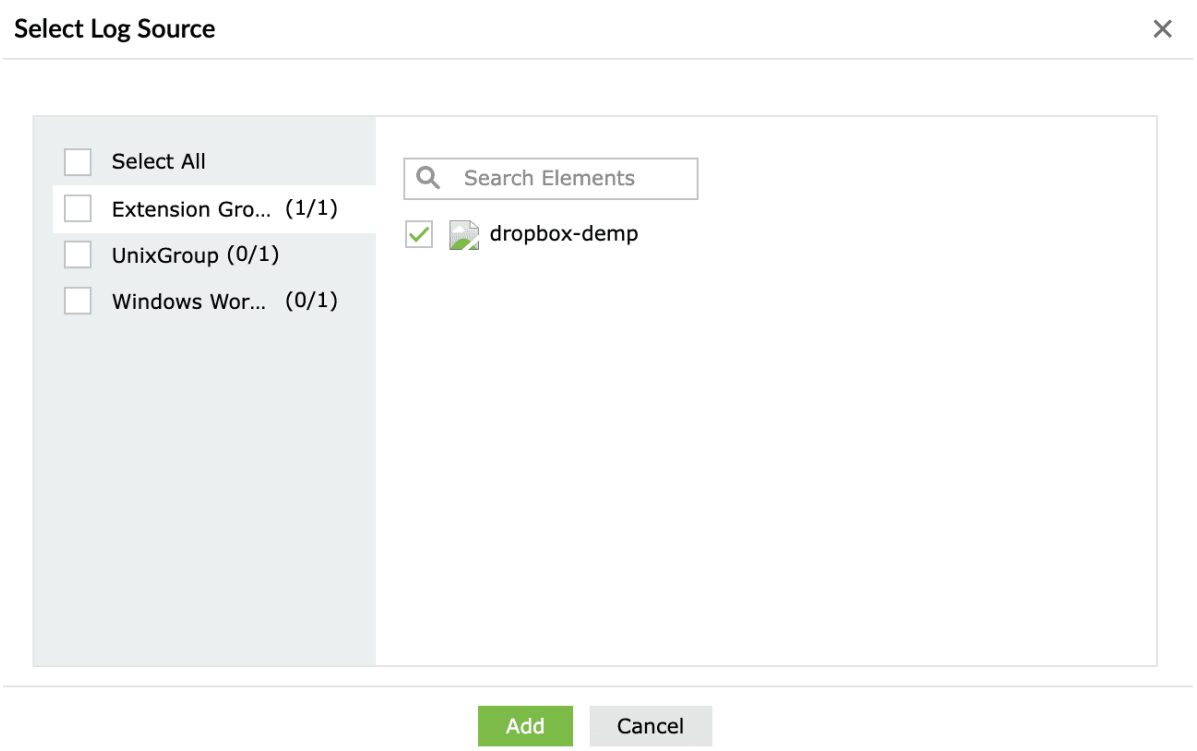
- Click Redirect next to Alert Profiles to open the Alerts tab. Browse the available Dropbox alert profiles and enable the required ones.



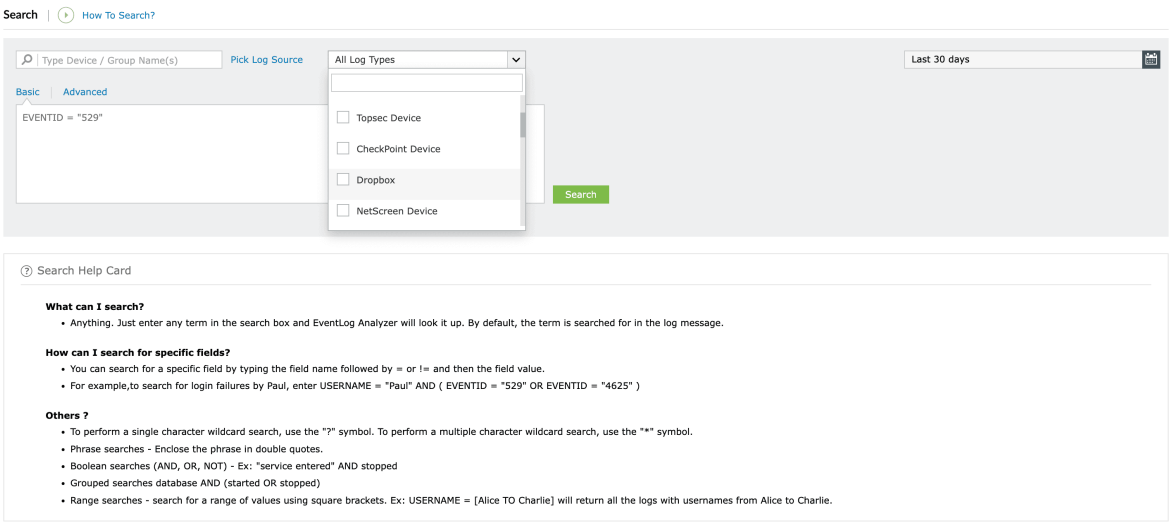
- Alternatively, go to the Alerts → Manage Profiles and choose Custom Alert Profiles under Alert Profile Type.
- Enable the required alert profiles.

Searching Dropbox Logs

- To search for Dropbox logs, select Dropbox Application under Extensions Group as the log source.



- Alternatively, filter logs by selecting Dropbox as the log type.



13.1. Data Upgrade

Last updated on: September 12, 2025

Overview

All the live and searchable logs processed by EventLog Analyzer are stored in Elasticsearch (ES), an open-source search engine, also referred to as Search Node. The processing of logs and preparation for search is called indexing. All the indexed data are stored in Elasticsearch data search.
From release 12040, EventLog Analyzer uses Elasticsearch version 5.6.4 to store all data. But soon this will be upgraded to ES version 6.5.4. ES has backward compatibility but only by one version; so all EventLog Analyzer installations pre Build 12040 need to be upgraded as they use ES version 2. This has raised a need to upgrade, or rather reindex, all older versions.
Reindexing is the process of extracting data from the source index and feeding it into the destination index.
Since ES 2 index is not compatible with ES 6.5.4, we are reindexing source index created in ES 2 (for versions before 12040) to destination index ES 5.6.4, so that it is compatible with ES 6.5.4.
The steps to reindex are as follows:
Note: All EventLog Analyzer installations post version 12040 needn't be reindexed as they already have the upgraded version.

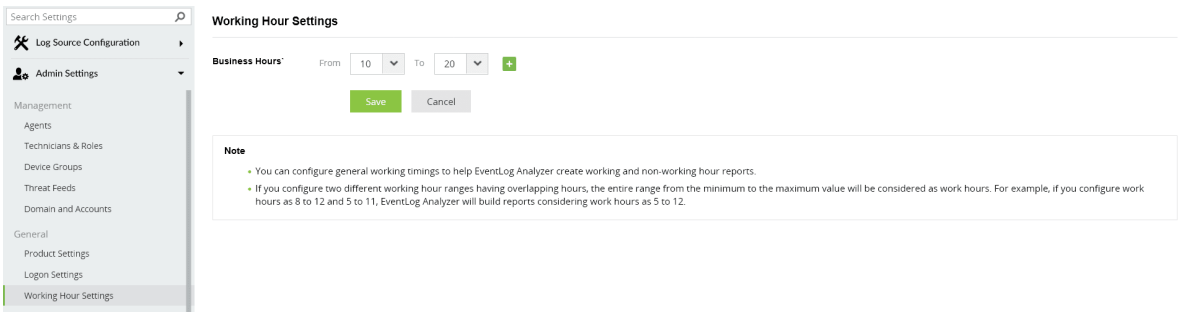
Prerequisites

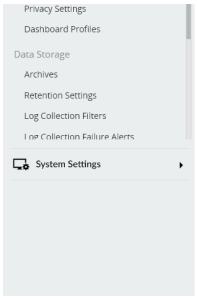
- At least 20GB of disk space or a minimum of [1x largest index size] or [3x largest archive size] and 5 GB on the Elasticsearch node. Reindexing will fail if the disk space is lesser than the specs mentioned above and you will receive a notification as mentioned here.

Data Upgrade (Reindexing)

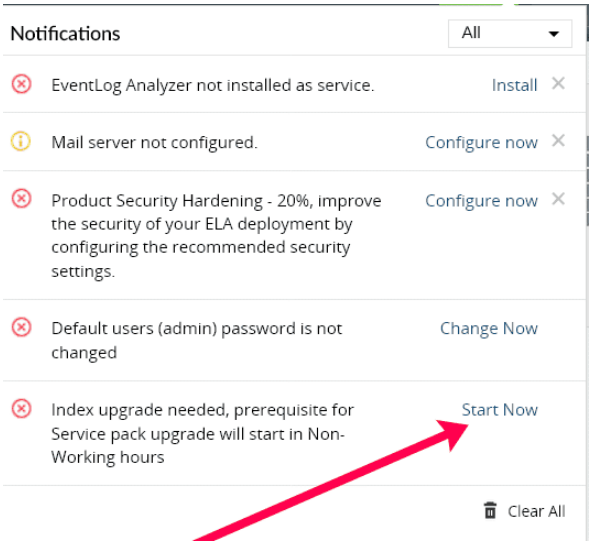
Data Upgrade (Reindexing) is a resource consuming process. Hence, it is better if the process is set to begin automatically during non-working hours. However, the user can force start at any time of the day if they don't mind high resource consumption.
The different way to Reindex are as follows:

- Automatic Reindexing
  The Reindexing process will automatically be triggered based on non working hours. This will be will be identified by EventLog Analyzer from Working Hour Setting set previously by the user.



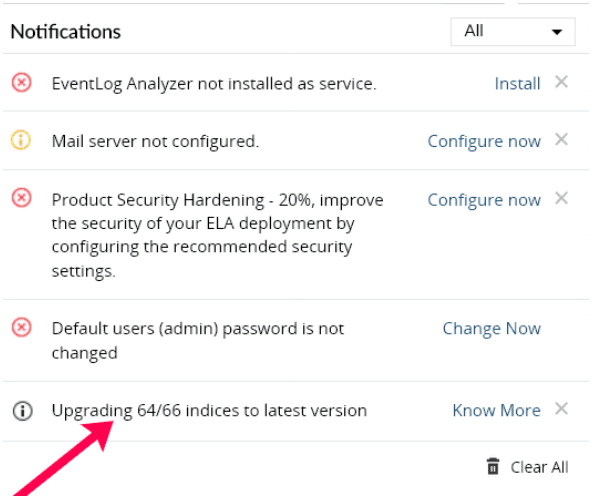


- Forced reindexing
  User can force Reindexing by clicking on the Start Now link in the following notification. By doing this, the Reindexing process will begin immediately.



Upgrade Status

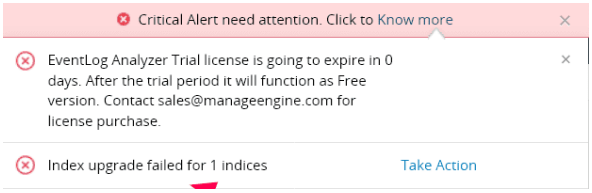
- COMPLETED
  The COMPLETED indices count will be shown in the notifications tab as shown in the image below. Here, 64/66 indicates COMPLETED COUNT/TOTAL COUNT, which means a total of 64 indices out of 66 has been successfully updated.



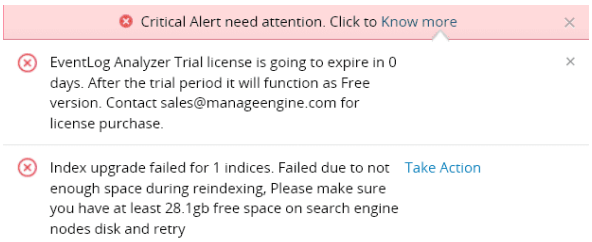
- FAILED

- FAILED

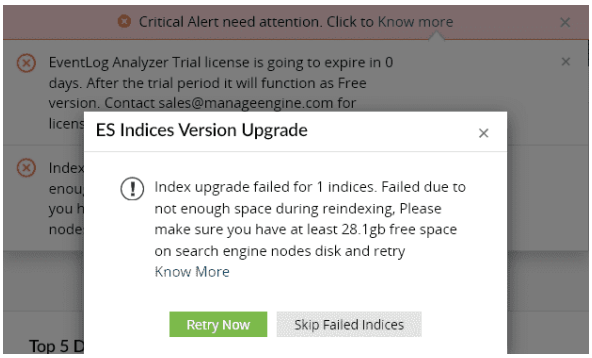
  The index upgrade sometimes fails, and these indices will be shown as FAILED indices in the notifications tab. These indices will automatically be updated after the current upgrading queue is completed. If not, it can also be triggered manually by clicking on the Take Action notification as shown in the image below.



  Sometimes, the failure can also be due to space constraints. If so, the following notification will pop up.



  By clicking on Take Action, user will be provided with two options: One, to retry Reindexing, or two, to skip those indices in case it is failing too many times. Skipping indices in this context mean the indices wont be reindexed/upgraded and those data will permanently be deleted as soon as the upgrade is complete. So, it is important that the user ensures that the skipped data isn't necessary.



In case none of this works for you and you are concerned about data loss, reach out to EventLog Analyzer team at eventlog-support@manageengine.com.

14.1. Custom Widgets

Last updated on: September 12, 2025

In this page

Types of Widgets in EventLog Analyzer

Dashboard Widget

Custom Report Widget

Incident Workbench Widget

Adding a custom widget in EventLog Analyzer

Installing the CLI for Zoho Extension Toolkit (ZET)

Including Resources in Your Widget Project

Validating and Packaging the Application

Adding the Created Widget to EventLog Analyzer

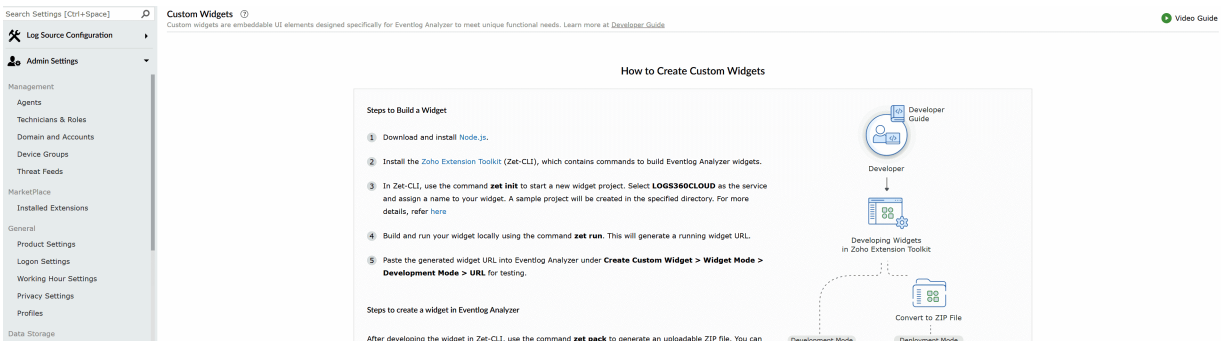
How to Include a Custom Widget in EventLog Analyzer

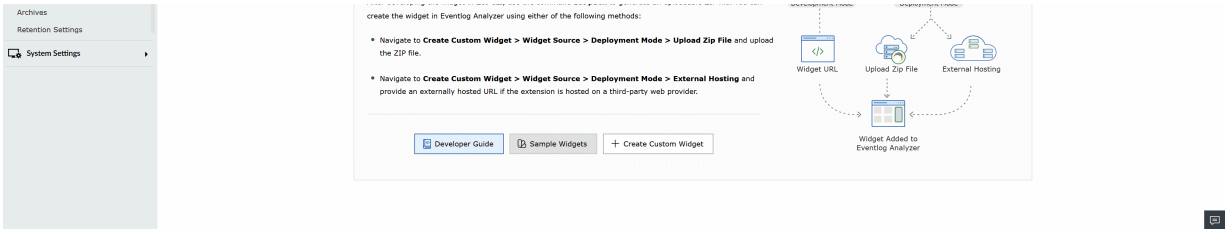
Passing Log Data to Custom Widgets in Incident Workbench

JS SDK

Widgets in ManageEngine EventLog Analyzer are embeddable UI components that you can create on your own, using our JS Software Development Kit. These widgets can be used to perform certain functions that utilize data from third-party applications seamlessly.
For example, with a custom widget in EventLog Analyzer, you can seamlessly integrate data from your EDR or email security solution into EventLog Analyzer, enabling you to monitor, analyze, and take necessary actions—all from a single platform.

> **Note**
>
> - Custom widgets can be created in all editions of EventLog Analyzer.
> - You can create up to a maximum of 200 widgets in EventLog Analyzer.





> **Note**
>
> These steps will be replaced by the widget list after you create your first widget. Refer to this image to follow the setup steps easily.
> Reference URLs:
> 1. Node.js
> 2. Zoho Extension Toolkit

Types of Widgets in EventLog Analyzer

- Dashboard Widget
- Custom Report Widget
- Incident Workbench Widget

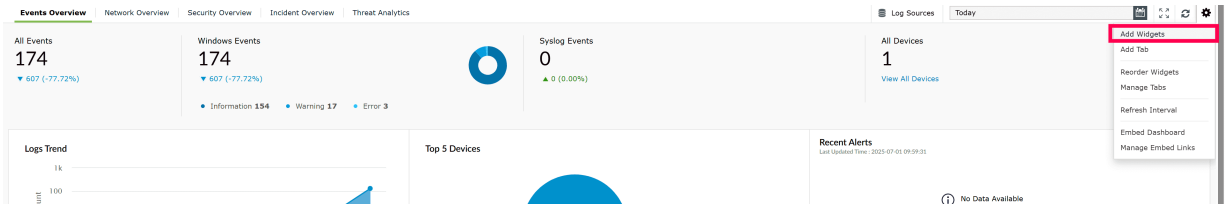
Dashboard Widget

You can build a custom widget for your dashboard in EventLog Analyzer. After creating the custom widget under Settings → Admin Settings → Developer Space → Custom Widgets, you can add it to your dashboard by using the Add Tab menu, where it will be listed in the dashboard settings.

> **Note**
>
> Only users with access to view or create widgets in a dashboard can view custom widgets.

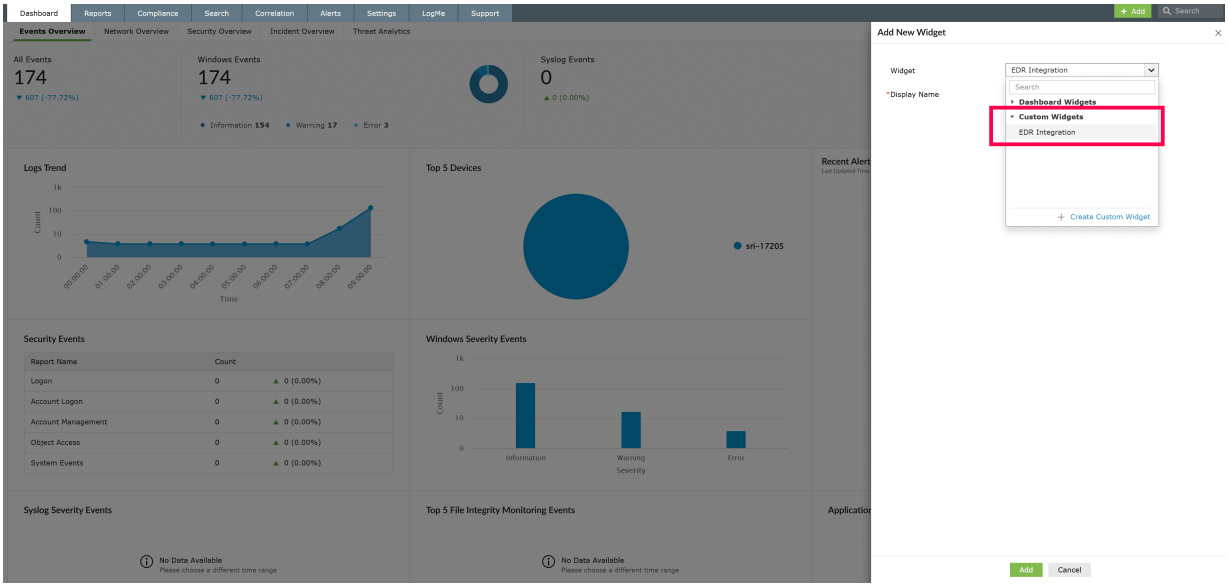
The user who have access to view or create widgets in dashboard can view the custom widgets.

How to create a custom widget in Dashboard





From the dropdown menu in the top right corner, choose Add widgets.



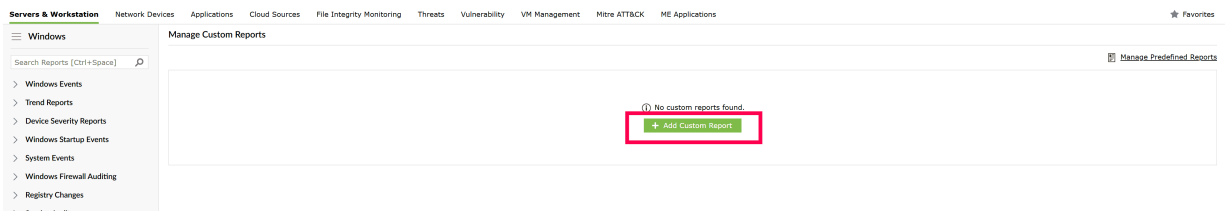
Select the custom widget that you want to add to the dashboard, and then click Add.

Custom Report Widget

A widget can be added as a custom report in EventLog Analyzer. After creating the custom widget under Settings → Admin → Developer Space → Custom Widgets, you can add it as a custom report by navigating to Reports → Manage Custom Reports → Add Report, and then selecting the Report Type as Custom Widget.

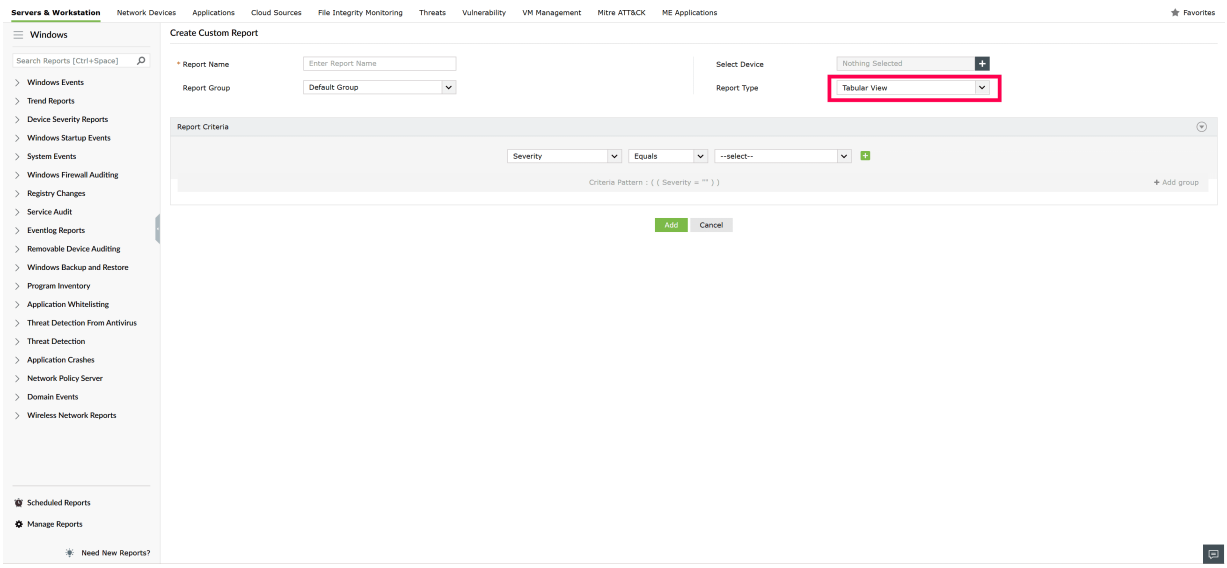
> Note: Only users with access to view or create reports in custom reports can view custom widgets.

How to create a custom widget in Custom Reports

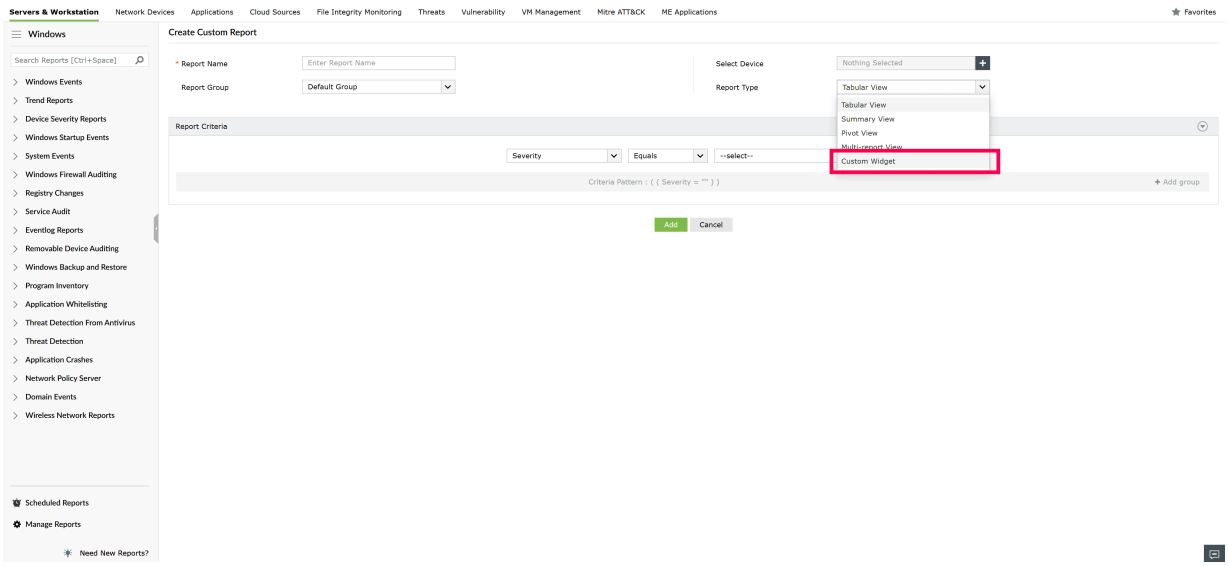




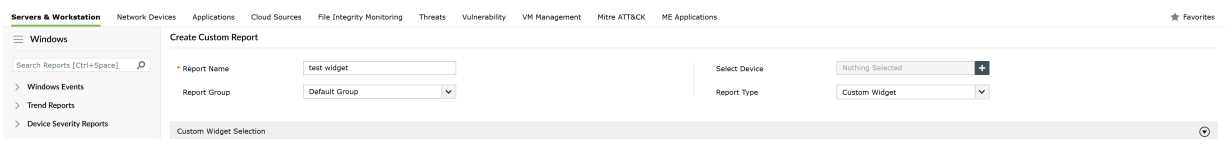
Click the Add Custom Report button.

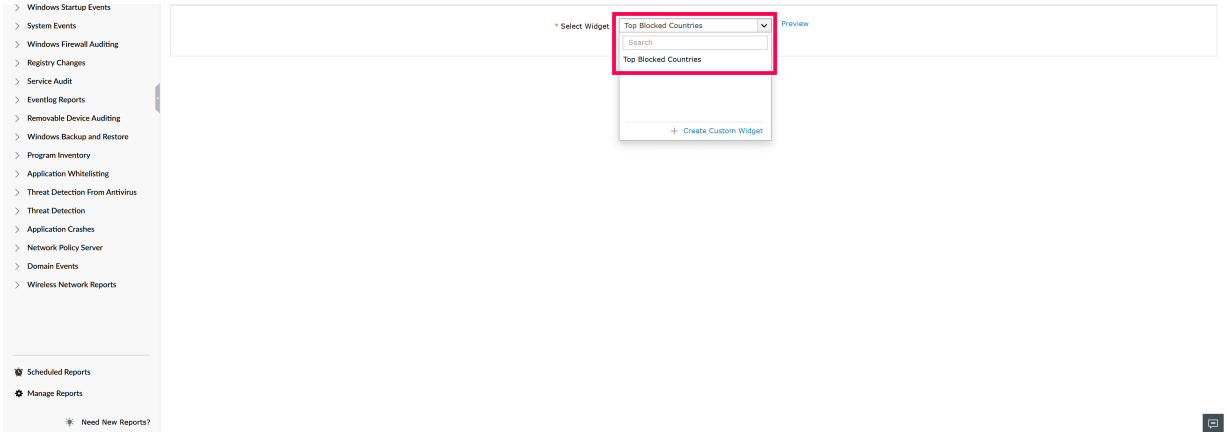


Click the Report type dropdown.

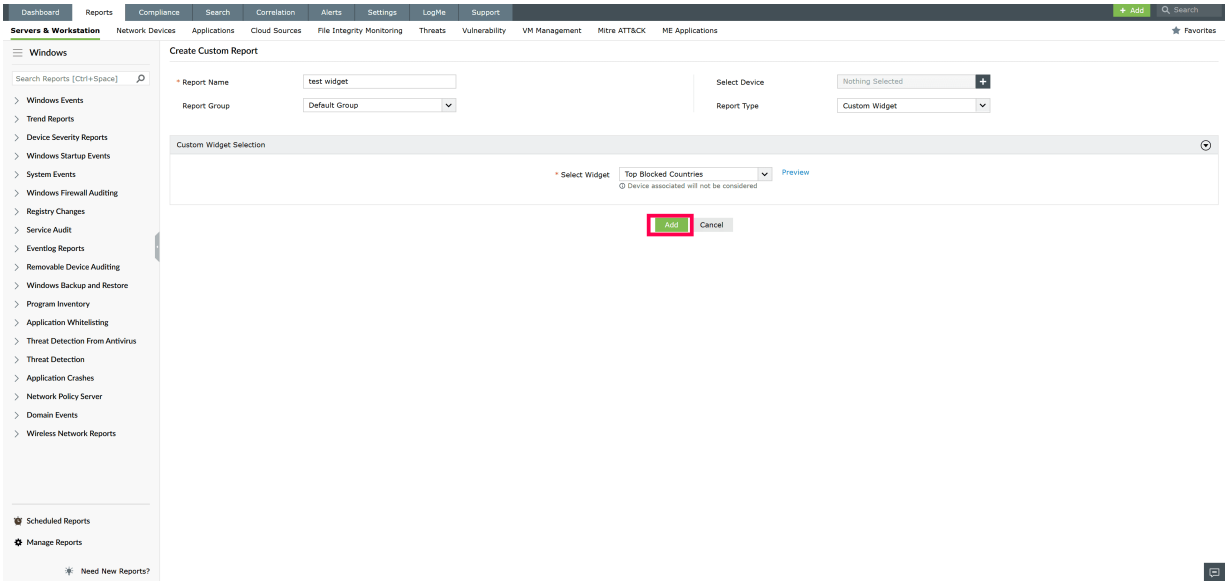


In the Report Type dropdown, select Custom Widget.





Under Custom Widgets, select the desired custom widget.



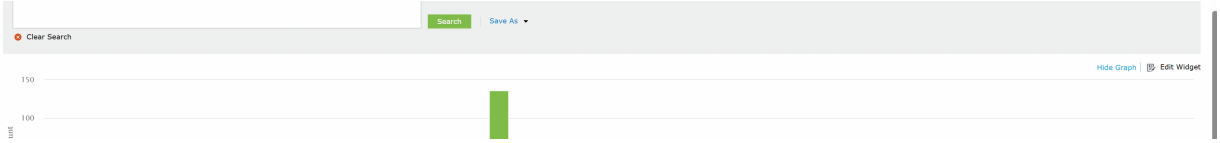
Then, click Add to create the custom report with the custom widget.

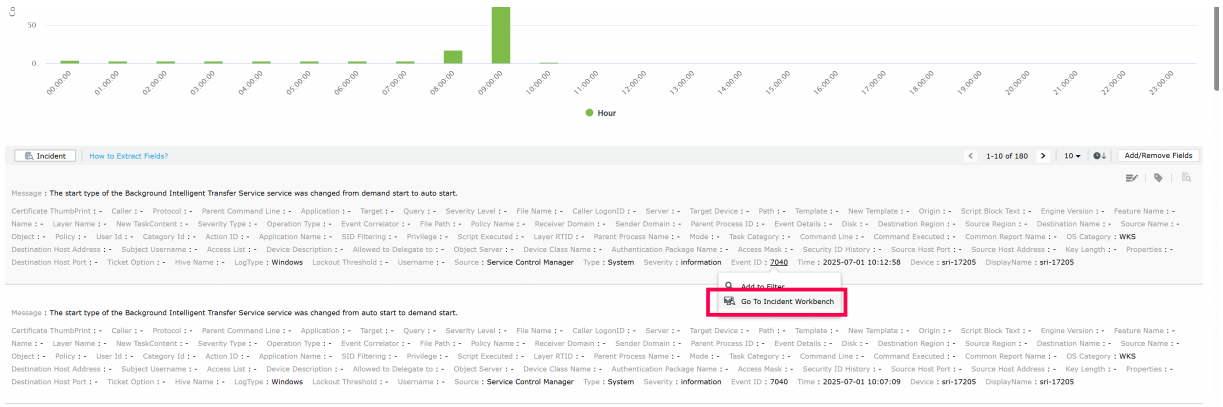
Incident Workbench Widget

A widget can be added to the Incident Workbench in EventLog Analyzer. This can be done directly from the Custom Widgets tab in the Settings, allowing you to integrate the custom widget seamlessly into the Incident Workbench.

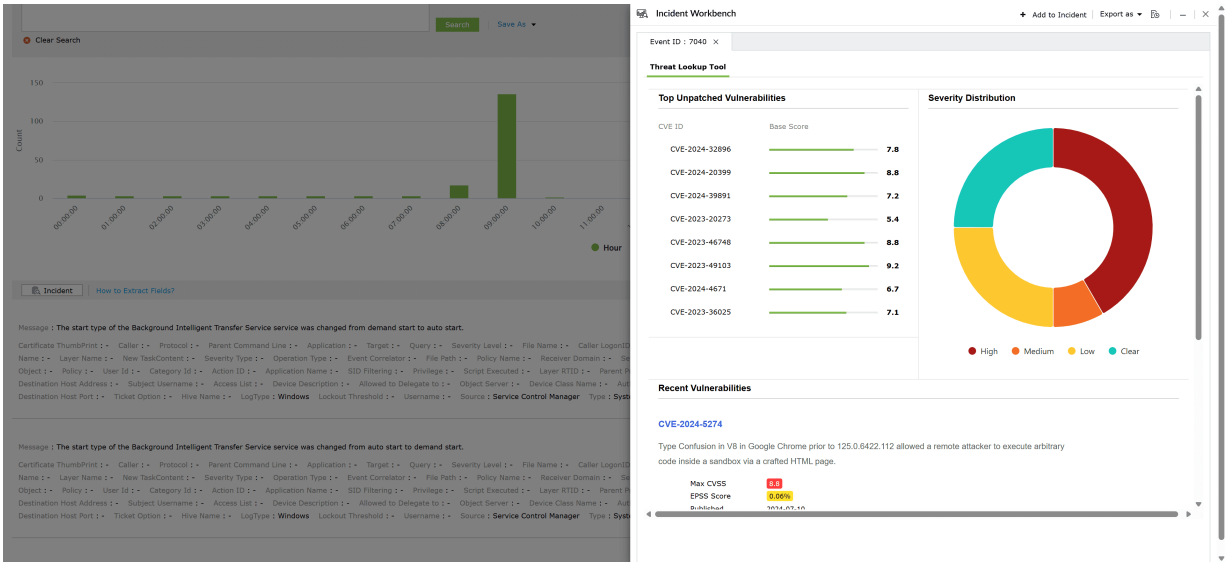
> Note: Only users with access to view incident workbench can view custom widgets.

How to view a custom widget in Incident Workbench





Select the field you need to analyze, then click Go to Incident Workbench.



The available widgets for the selected fields, including any custom widgets, are displayed in tabs.

Adding a custom widget in EventLog Analyzer

A custom widget can be added to EventLog Analyzer using the Zoho Extension Toolkit (ZET).

Create a custom widget using ZET

ZET, or the Zoho Extension Toolkit, is a command-line interface (CLI) designed to help developers build and package custom widgets for ManageEngine EventLog Analyzer.

A CLI is a text-based interface that allows users to interact with software by typing specific commands, receiving responses, and executing actions directly from the terminal or command prompt. While graphical user interfaces (GUIs) offer visual interaction, CLIs provide a simpler and more efficient way for developers to work, particularly when it comes to creating applications, managing software, or even building operating systems.

Here's how you can build custom widgets using ZET and package and integrate these widgets with ManageEngine EventLog Analyzer for enhanced functionality.

Install the necessary components

Prerequisites

.

- Visit the official Node.js website: https://nodejs.org/en/download/
- Choose the appropriate version for your operating system (Windows, macOS, or Linux) and download the installer.
- Once the installation is complete, verify that Node.js and npm are correctly installed by running the following commands in your terminal:

Check Node.js version
This will return the installed version of Node.js, e.g., v14.18.1.
Check npm version
This will return the installed version of npm, e.g., 6.14.12.
If both commands return a version number, it means Node.js and npm have been successfully installed.

Installing the CLI for Zoho Extension Toolkit (ZET)

To install the Zoho Extension Toolkit (ZET) CLI, follow these steps:

Install the ZET CLI package

Run the following command to install the zapps CLI node package:

Verify the installation

Once installed, run the following command to ensure that the installation was successful:
If the installation is successful, help information related to the zet command will be displayed.
Creating a New Project Using ZET
Follow these steps to create a new project using the Zoho Extension Toolkit (ZET):
Initialize a New Project
Run the following command to create a new project:
This command will display a list of available Zoho and ManageEngine services. Select the Log360 Cloud service for which you want to create a project template.

Verify the Server Startup

Once the project is created and the local development server starts running, verify its status by opening one of the following URLs in your browser:

- Manifest File: https://localhost:5000/plugin-manifest.json
- Widget Preview: https://localhost:5000/app/widget.html

If these URLs load correctly, your project has been successfully created and the local server is running.

Including Resources in Your Widget Project

All necessary files required for rendering your custom widget are stored inside the "app" folder of your project.

Starting the Server

To run your app locally and test it in your sandbox instance, start a local HTTPS server using the following

command:
This will start the HTTPS server on your local machine at port 5000. Ensure that this port is not occupied by any other process before running the command.

Verify the Server

Once the server starts, open the following URL in your web browser to check if it is running successfully:
https://127.0.0.1:5000/app/widget.html
If the page loads correctly, your widget is now running in a local environment and is ready for testing.

Validating and Packaging the Application

Before uploading your application, it is essential to validate and package it correctly. Follow these steps:

Validate the Application

Run the following command to check for any issues in your app package:
This will scan your application for any violations. If issues are detected, they must be resolved before proceeding with the upload.

Package the Application

Once validation is successful, generate an uploadable ZIP file by running:
This will create a ZIP file inside the "dist" folder of your project directory. The packaged file can then be uploaded to EventLog Analyzer for deployment.

Adding the Created Widget to EventLog Analyzer

Follow these steps to add the custom widget to EventLog Analyzer:

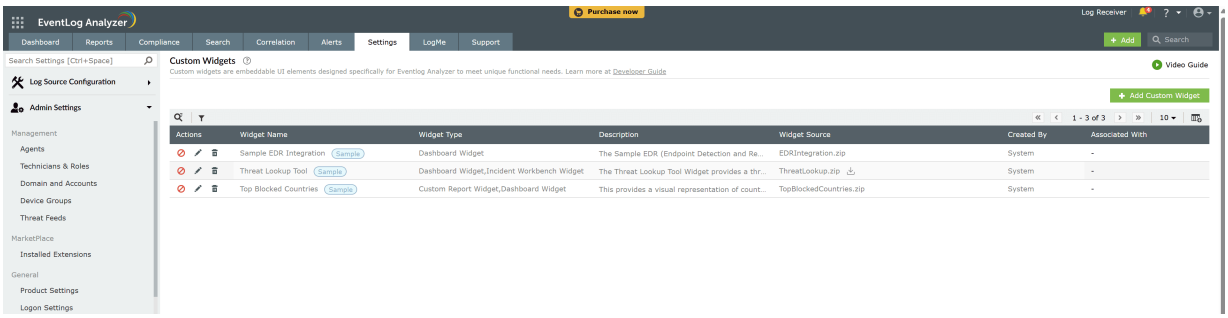
a) Navigate to Developer Space

Go to Settings → Developer Space → Custom Widgets in EventLog Analyzer.

b) Check Sample Widgets

The Sample Widgets section takes you to pre-created widgets within EventLog Analyzer.

- These default widgets serve as examples, helping you understand how custom widgets can be designed and used.
- You can download and unzip the sample widgets, then open them in a code editor to see how they work.

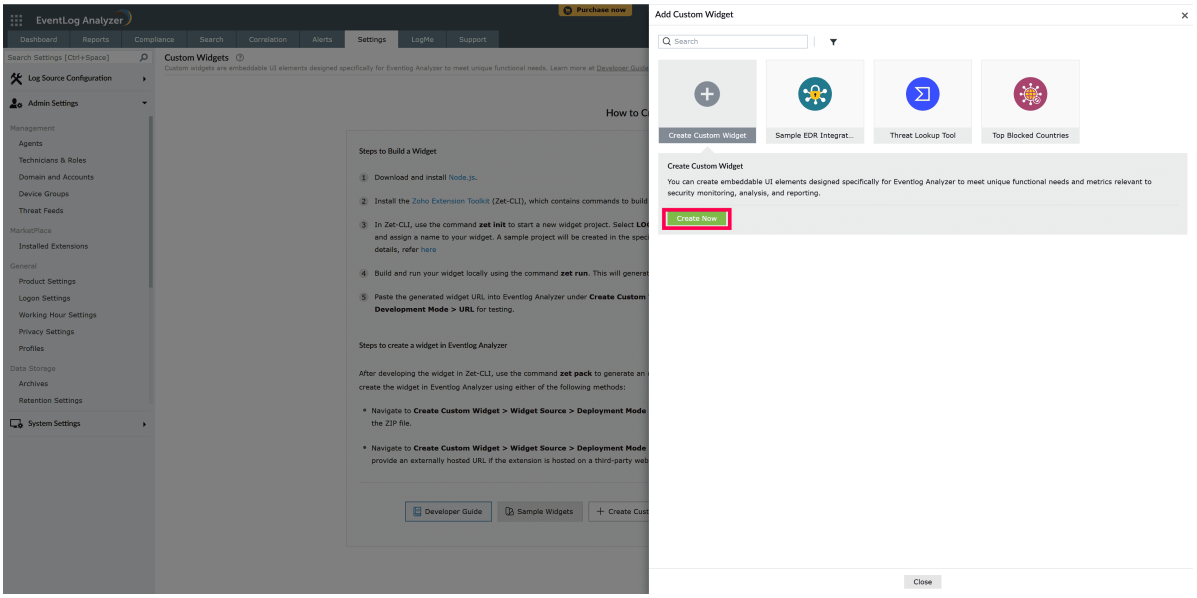


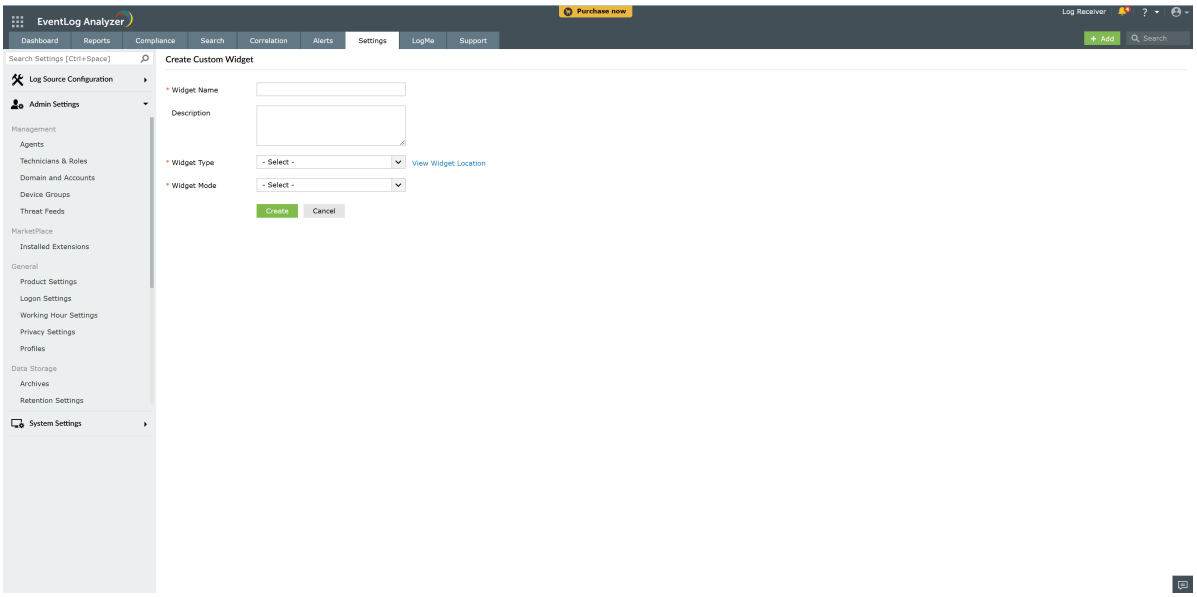


c) Create a New Widget

To create a new widget, click on Create Custom Widget → Create Now.

- EventLog Analyzer also offers a list of available widgets that you can add by selecting the custom widget.

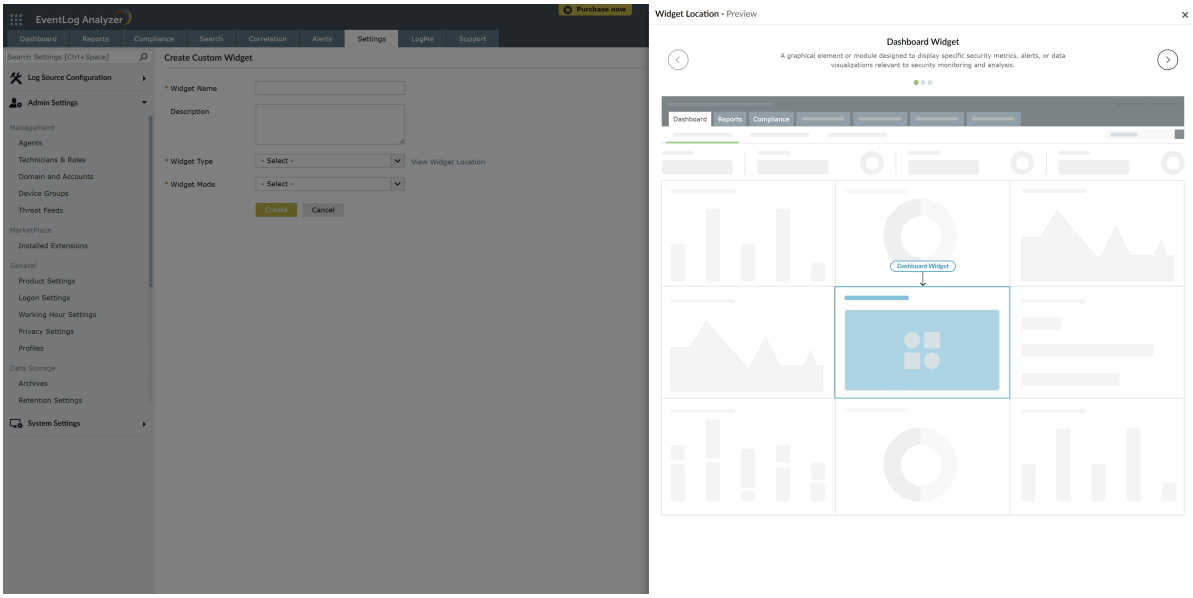


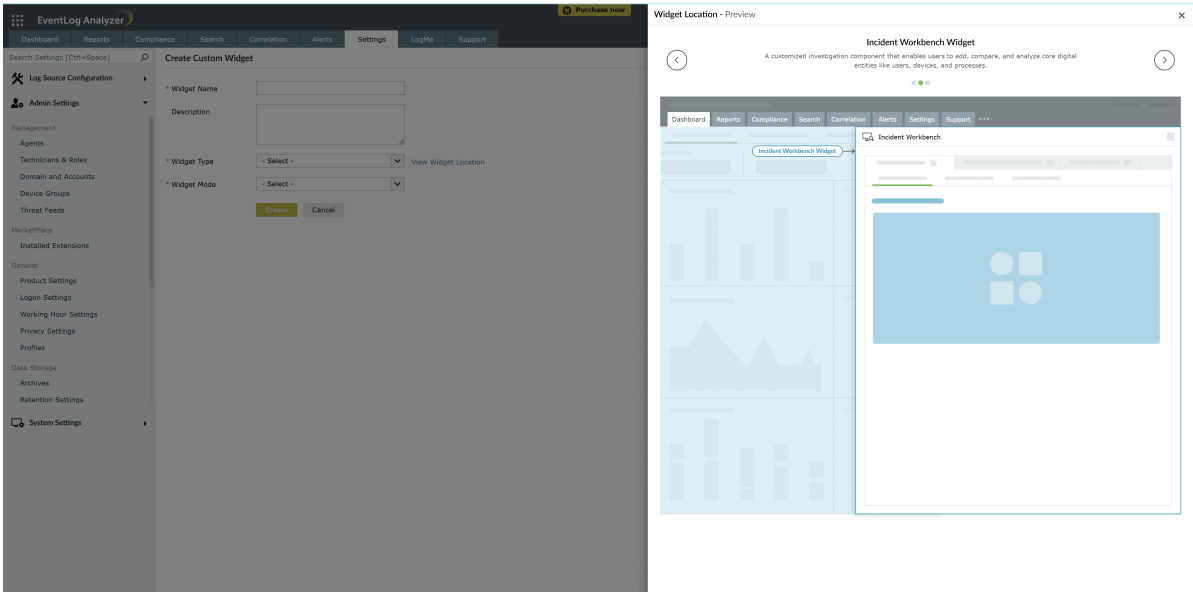


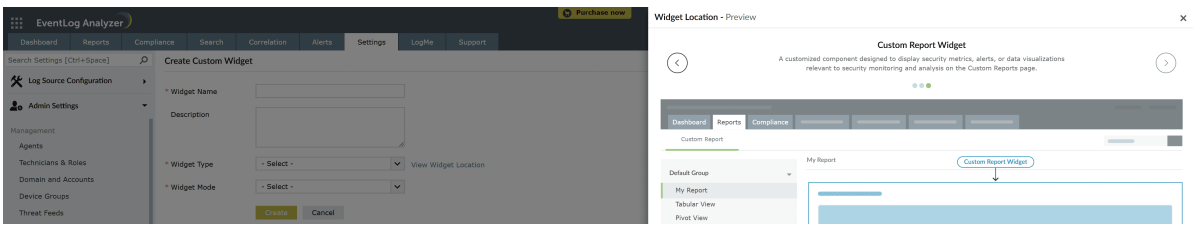
d) Fill Out the Widget Creation Form

In the Create Custom Widget Form:

- Provide the Widget Name and Description.
- Select the Widget Type from the following options:
  - Dashboard Widget
  - Custom Report Widget
  - Incident Workbench Widget
- Choose the View Widget Location to determine where your custom widget will be placed within EventLog Analyzer.









e) Custom Widget Creation Modes in EventLog Analyzer

EventLog Analyzer supports two modes for custom widget creation:

1. Development Mode

- In this mode, you can run and test your custom widget locally before deploying it.
- Start the widget by running:
- Add the URL (ex: https://localhost:5000/app/widget.html) of your widget to the Widget URL input field in EventLog Analyzer.

> Note
>
> - Any changes made to the widget code automatically reflect in EventLog Analyzer (whether in the dashboard or custom report).
> - Development Mode is not available for Incident Workbench Widgets, as field mapping is required in plugin-manifest.json.
> - The custom widget in development mode is visible only to the developer and not to other users.

2. Deployment Mode

In deployment mode, you have two options to add the widget to EventLog Analyzer:

a) Upload ZIP File (ZET Package)

- After developing the custom widget, package it using:
- This creates a ZIP file inside the dist folder of your project.
- Upload this ZIP file to EventLog Analyzer to deploy the widget.

b) External URL Embedding

- Instead of using ZET, you can embed any external URL as a widget inside EventLog Analyzer.
- This option allows seamless integration of third-party dashboards or web apps.

How to Include a Custom Widget in EventLog Analyzer

Custom widgets can be added to the following sections of EventLog Analyzer:

- Dashboard
- Custom Reports
- Incident Workbench

Adding a Custom Widget to the Dashboard

After creating an HTML page for the custom widget, add the following configuration to the plugin-manifest.json file inside the widgets list:
This will ensure that the widget appears on the EventLog Analyzer dashboard.

Adding a Custom Widget to Custom Reports

For adding a custom widget to Custom Reports, add the following configuration to the plugin-manifest.json file inside the widgets list:
This allows the widget to be used as a custom report widget.

Adding a Custom Widget to the Incident Workbench

For including a custom widget in Incident Workbench, use the configuration below:
This ensures the widget is integrated with the Incident Workbench for real-time incident analysis.
Important
Modifying and uploading the name attribute for a custom widget after it has been added will result in the removal of the widget from its mapped module (Dashboard, Reports or Incident Workbench).
Following are the locations allowed in EventLog Analyzer:

- "dashboard"
- "reports"
- "incident-workbench"

Adding a custom widget in Incident Workbench differs from other modules as it requires mapping specific fields to the widget. When adding a widget to the Incident Workbench, you must specify options where the fieldName will be mapped with the custom widget.
Here are some of the important fields.

- HOSTNAME → Device name (source of data/log collection)
- USERNAME → User associated with the data/log
- IPADDRESS → Captured IP in the data/log
- FILENAME → Name of the file in the data/log
- PROCESSNAME → Name of the process in the data/log
- FILEHASH → Hash of the file in the data/log
- EMAIL → User email captured in the data/log
- DOMAINNAME → AD domain name captured in the data/log
- PORT → Port associated with the entity in the data/log
- PROTOCOL → Protocol associated with the entity in the data/log

Passing Log Data to Custom Widgets in Incident Workbench

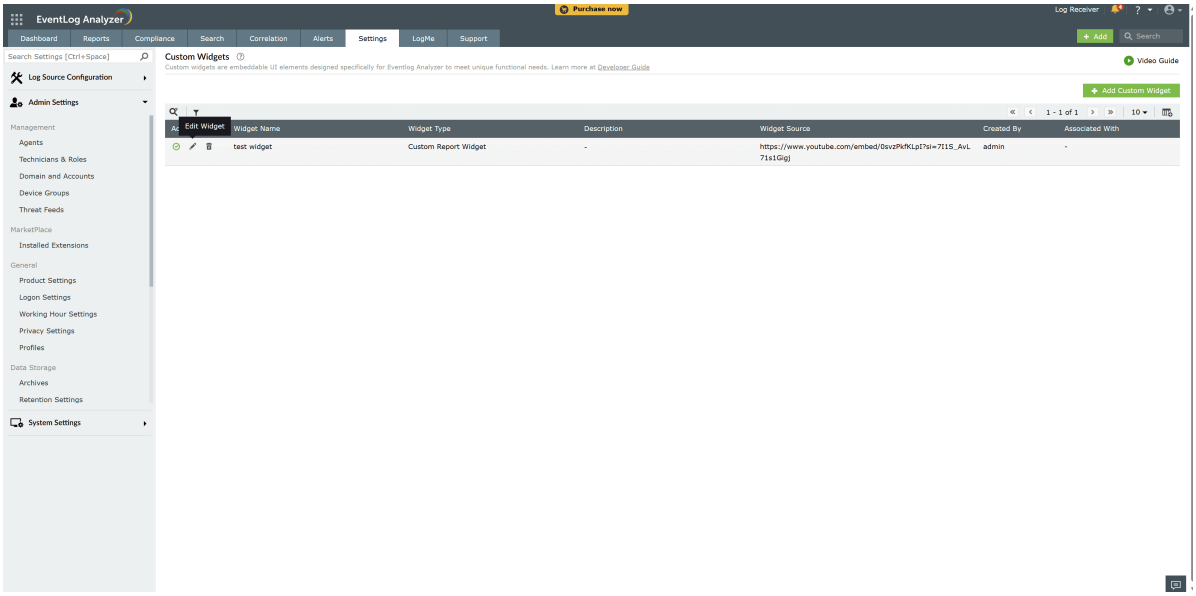
When a field associated with Incident Workbench is clicked, the log data corresponding to that row will be passed from the table data to the Custom Widget.

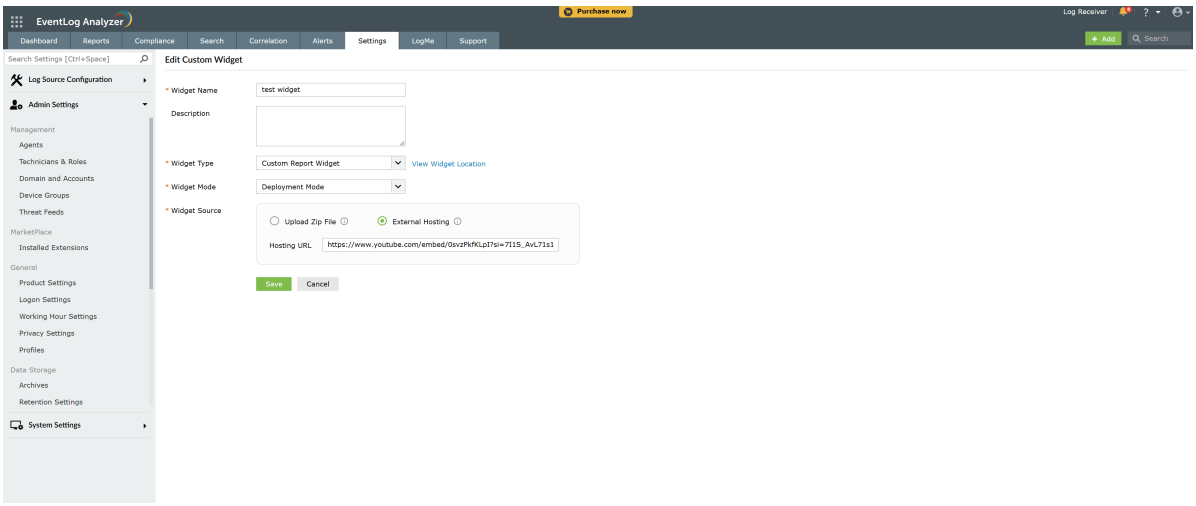
Example Log Data Structure:

```
{
  "logUUID": 430453503444,
  "HOSTNAME": "EVENT-TEST",
  "USERNAME": "admin",
  ...
}
```

How to edit Custom Widgets

1. Go to Settings -> Admin -> Developer Space -> Custom Widgets
2. In the Manage Custom Widgets table, click on edit icon to edit the Custom Widget





When editing a custom widget, certain changes can affect its associations with other modules.

To Retain Associations:

1. The Widget Name must remain the same.
   - For ZIP uploads, the name inside plugin-manifest.json is used.
   - For Development Mode or External Hosting, the Widget Name entered in the form is used.
2. You can safely update the widget URL or ZIP contents as long as the widget name remains unchanged.

> **Note**
>
> The widget name serves as the primary key for maintaining associations.

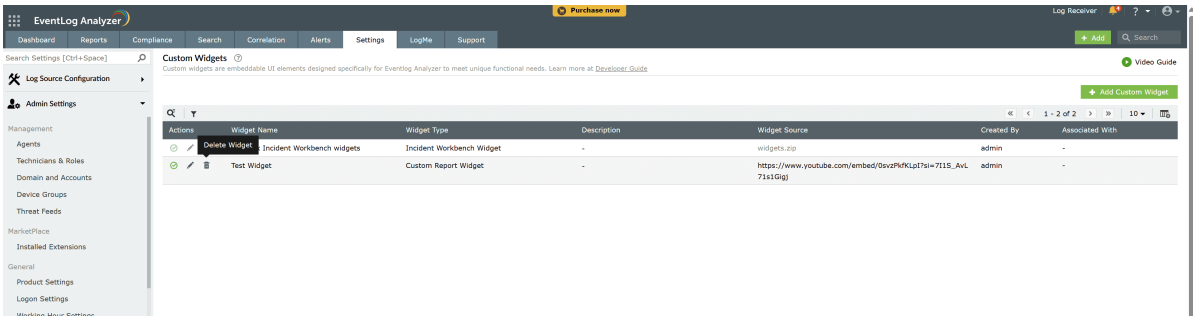
Associations Will Be Removed If:

1. The Widget Type is changed or removed.
2. A new ZIP is uploaded with a different widget name in plugin-manifest.json.
3. The widget source is changed between:
   - ZIP ↔ Development Mode / External Hosting
   - Development Mode / External Hosting ↔ ZIP
     → Only if the widget name (in the form or ZIP) is also changed.

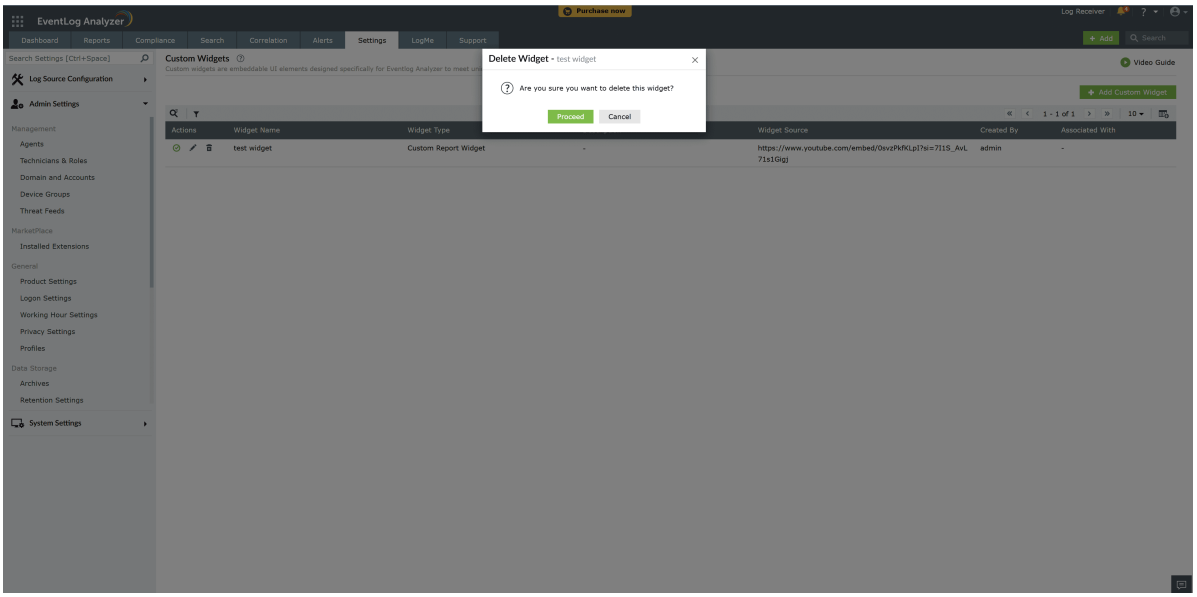
> **Note**
>
> To avoid breaking associations, keep both the Widget Source and Widget Name unchanged when making edits.

How to delete Custom Widgets

1. Navigate to Settings → Admin → Developer Space → Custom Widgets.
2. In the Manage Custom Widgets table, click the delete icon to remove the custom widget.







JS SDK:

JS SDK provides a set of JavaScript functions to integrate EventLog Analyzer functionalities into your custom widget. These APIs enable seamless interaction between your widget and the platform.

Widget usage:

> **Note**
>
> The service name LOGS360CLOUD is used for both EventLog Analyzer and Log360 Cloud.

LOGS360CLOUD.init()

This function acts as a foundational call to establish a connection between the custom widget and the product. Other JS APIs will be defined only when the initialization is completed.
Returns promise

LOGS360CLOUD.get(options)

Fetch the product data, such as meta data, or any input data in the custom widget, from the product server. Note that only Logs360 APIs can be invoked using this function.

LOGS360CLOUD.add(options)

> **Note**
>
> Please ensure that only api/v2 APIs are used.

Add data to the server from the custom widget.Note that only Logs360 APIs can be invoked using this function.

LOGS360CLOUD.showLoader(opts)

The function is used to display a loading indicator on the widget window. This helps improve user experience by visually indicating that a process is in progress, such as data fetching, API calls, or background computations.

LOGS360CLOUD.hideLoder(opts)

The function is used to remove or hide the loading indicator from the widget window. It is typically called after a process, such as data retrieval or API execution, has been completed.

LOGS360CLOUD.showNotification(opts)

The function is used to display a top notification in the widget. This notification can be utilised to inform users about important updates, alerts, or process statuses.

LOGS360CLOUD.HideNotification(opts)

The function is used to hide or remove the top notification from the widget window. This can be useful when you need to manually dismiss a notification before its auto-dismissal time or when clearing notifications based on user interactions.

LOGS360CLOUD.getConnections()

Fetches the details of all successfully installed API applications.

LOGS360CLOUD.invokeUrl()

The function is used to fetch data from integrated third-party applications by making API calls. This function supports multiple configuration options, such as URL, HTTP method, headers, parameters, and payload, allowing seamless interaction with external services.

15.1. Migrate EventLog Analyzer Data from PGSQL to MS SQL Database

Last updated on: September 12, 2025

EventLog Analyzer allows you to migrate the existing EventLog Analyzer data available in the PGSQL database to the MS SQL database.
This procedure is applicable only if you are already using the EventLog Analyzer with PGSQL and you want to change the database to MS SQL.

> Note
>
> Before making changes to the database with the changeDBServer.bat file, it's crucial to ensure that the product is fully operational. Once confirmed, proceed to shut down the product. Once the product has successfully stopped, run the changeDBServer.bat file.

> Note
>
> Re-registering the Managed Server after the database has been changed:
> - When the Managed Server is installed, it is registered with Admin Server as Managed Server with PGSQL.
> - If the database of the Managed Server is changed from PGSQL to MS SQL, the database of the Admin server also needs to be changed from PGSQL to MS SQL.
> - Then, the managed server has to be re-registered with the Admin Server with the help of <EventLog Analyzer Home>/troubleshooting/registerWithAdminServer.bat file (or registerWithAdminServer.sh file)
>
> After changing the database, when the Managed Server is started as a service. There will not be any prompt to re-register. The user has to ensure that the Managed Server is re-registered with the Admin Server.
> If the user is migrating a distributed setup, the user needs to migrate the entire distributed setup to MSSQL. All Managed servers along with the admin server should be migrated to MSSQL.

If you want to configure MS SQL for a fresh installation of the EventLog Analyzer server, please refer to the Configuring MS SQL Database page and follow the procedure given there.
The steps to migrate and run the EventLog Analyzer server with SQL SERVER as the database is given below:

1. Navigate to Settings → Database Settings → Database Backup.
2. Use the Backup Now option to backup the data available in the PGSQL database and wait till the data backup is completed. By default, the backup file will be stored under <EventLog Analyzer Home>/Backup directory with the file name 'ELA_Backup_YYYY_MM_DD_HH_MM_SS.ezip'.

3. From the installed MS SQL SERVER, copy the files bcp.exe and bcp.rll to <EventLog Analyzer Home>/bin folder.

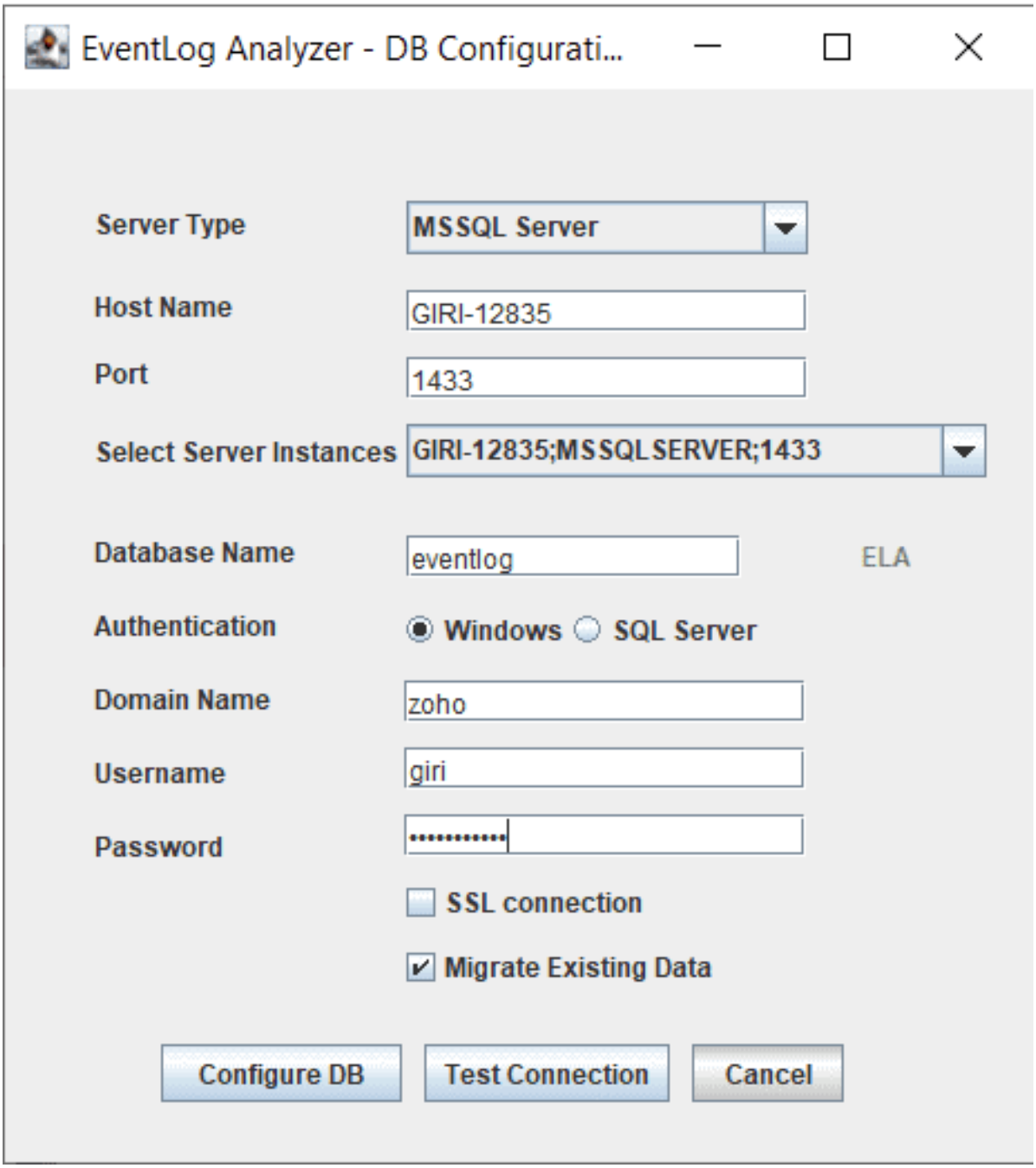
> **Note**
>
> If you are copying the above files from SQL server (Version 2012 and above) and EventLog Analyzer is installed in another machine, please install the SQL native client as per the SQL version and CPU type of the EventLog Analyzer machine.
> For MSSQL version 2012, install the native client and for the remaining versions of MSSQL, install the ODBC driver (links given below).
> MSSQL 2012
> https://www.microsoft.com/en-us/download/confirmation.aspx?id=50402
> MSSQL 2014
> https://www.microsoft.com/en-us/download/details.aspx?id=36434
> MSSQL 2016
> https://www.microsoft.com/en-us/download/details.aspx?id=50420
> MSSQL 2017
> https://www.microsoft.com/en-us/download/details.aspx?id=53339
> MSSQL 2019
> 64bit link: https://go.microsoft.com/fwlink/?linkid=2137027
> 32bit link: https://go.microsoft.com/fwlink/?linkid=2137028
> MSSQL 2022
> 64bit link: https://go.microsoft.com/fwlink/?linkid=2266640
> 32bit link: https://go.microsoft.com/fwlink/?linkid=2266742

4. Invoke the <EventLog Analyzer Home>/tools/changeDBServer.bat in command prompt to configure the MS SQL SERVER credentials like ServerName, Port, User Name and Password.
5. Database Setup Wizard pops-up.
6. In the wizard screen, select Server Type as SQL Server. Available SQL Server Instances are listed in a combo box. Enter the Device Name and Port of the SQL Server from the instances.
7. Select the authentication type using the "Connect Using:" option.
8. The options are:
   - Windows Authentication
   - SQL Server Authentication

> **Note**
>
> Ensure that both EventLog Analyzer Server and MS SQL Server are in the same domain and logged in with the same Domain Administrator credentials.

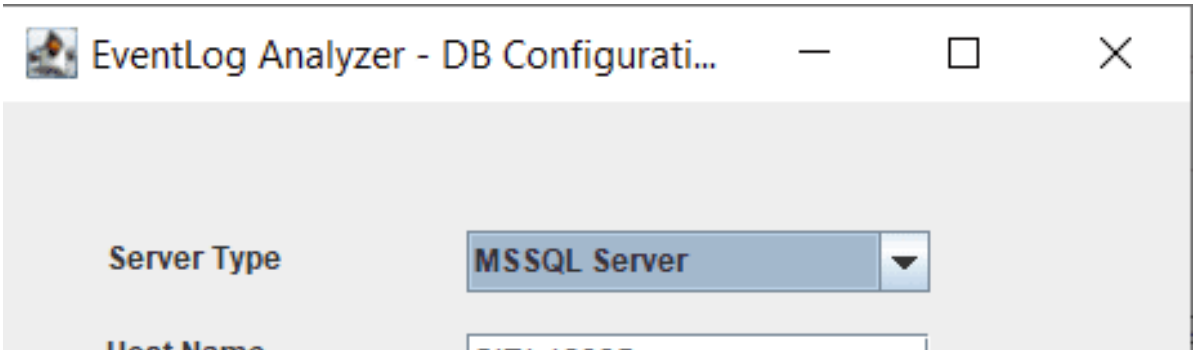
Windows Authentication

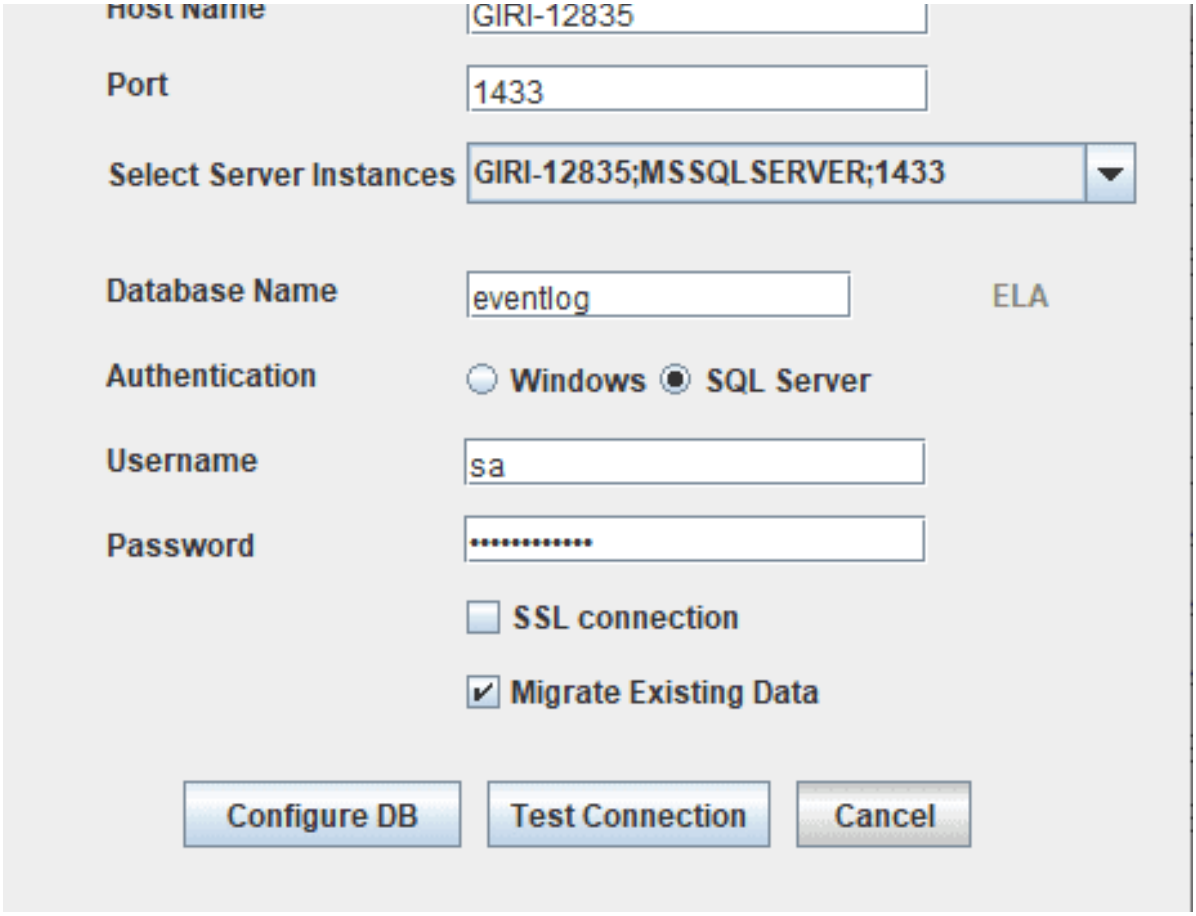
For EventLog Analyzer version 8.0 (Build 8010) onwards,



SQL Server Authentication

For SQL Server Authentication, enter the User Name and Password.





9. Click the Test Connection button to verify the correctness of the credentials. If the test fails, recheck and enter the correct credentials.
10. Click the Configure DB button to save the SQL Server configuration. Note that configuring the settings of the SQL Server database may take a few minutes.
11. The product will start automatically after the configuration is complete.

15.2. Moving the EventLog Analyzer MSSQL Database to a Different Directory in the Same Server

Last updated on: September 12, 2025

This procedure is applicable for EventLog Analyzer version 8.0 (Build 8010) onwards.

How to find the build number?

In the EventLog Analyzer web client, click "?" on the top right corner of the screen and click on About. You will find the build number mentioned below the build version.
This is the build number of the currently installed EventLog Analyzer.



Moving the EventLog Analyzer MS SQL database

1. Stop the EventLog Analyzer Server/Service.
2. Login to SQL Server database with system administrator permissions.
3. Find the current location of the data file and log file for the database named 'eventlog' by using the following commands:
4. Detach the database by entering the following commands:
5. Copy the data file and the log file from the current location (<MSSQL Home>\DATA\eventlog.mdf and <MSSQL Home>\DATA\eventlog_log.ldf) to the new location (<New location>\eventlog.mdf and <New Location>\eventlog_log.ldf).
6. Re-attach the database and point to the new location by using the following commands:
7. Verify the changed location by using the following commands:
8. Start the Eventlog Analyzer Server/Service.

15.3. Migrate EventLog Analyzer Data from MySQL to MS SQL Database

Last updated on: September 12, 2025

EventLog Analyzer allows you to migrate the existing EventLog Analyzer data available in MySQL database to MS SQL database.
This procedure is applicable only if you are already using EventLog Analyzer with MySQL and you want to change the database to MS SQL.

> Note
>
> Before making changes to the database with the changeDBServer.bat file, it's crucial to ensure that the product is fully operational. Once confirmed, proceed to shut down the product. Once the product has successfully stopped, run the changeDBServer.bat file.

> Note
>
> Re-registering the Managed Server after the database has been changed:
> - When the Managed Server is installed, it is registered with Admin Server as Managed Server with MySQL.
> - If the database of the Managed Server is changed from MySQL to MS SQL, the database of the Admin server also needs to be changed from MySQL to MS SQL.
> - Then, the managed server has to be re-registered with Admin Server with the help of <EventLog Analyzer Home>/troubleshooting/registerWithAdminServer.bat file (or registerWithAdminServer.sh file)
>
> After changing the database, when the Managed Server is started as a service, there will not be any prompt to re-register. The user has to ensure that the Managed Server is re-registered with the Admin Server.
> If the user is migrating a distributed setup, the user needs to migrate the entire distributed setup to MSSQL. All Managed servers along with the admin server should be migrated to MSSQL.

If you want to configure MS SQL for a fresh installation of EventLog Analyzer server, please refer the Configuring MS SQL Database page and follow the procedure given there.
The steps to migrate and run the EventLog Analyzer server with SQL SERVER as the database is given below:

1. Stop the EventLog Analyzer Server/Service.
2. From the installed MS SQL SERVER, copy the files bcp.exe and bcp.rll to <EventLog Analyzer Home>/bin folder.

Note

If you are copying the above file from SQL server (Version 2012 and above) and EventLog Analyzer is installed in another machine, please install the SQL native client as per the SQL version and CPU type of the EventLog Analyzer machine.
For MSSQL version 2012, install the native client and for the remaining versions of MSSQL, install the ODBC driver (links given below).
MSSQL 2012
https://www.microsoft.com/en-us/download/confirmation.aspx?id=50402
MSSQL 2014
https://www.microsoft.com/en-us/download/details.aspx?id=36434
MSSQL 2016
https://www.microsoft.com/en-us/download/details.aspx?id=50420
MSSQL 2017
https://www.microsoft.com/en-us/download/details.aspx?id=53339
MSSQL 2019
64bit link: https://go.microsoft.com/fwlink/?linkid=2137027
32bit link: https://go.microsoft.com/fwlink/?linkid=2137028
MSSQL 2022
64bit link: https://go.microsoft.com/fwlink/?linkid=2249006
32bit link: https://go.microsoft.com/fwlink/?linkid=2249005

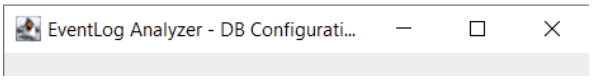
3. Invoke the <EventLog Analyzer Home>/tools/changeDBServer.bat in command prompt to configure the MS SQL SERVER credentials like ServerName, Port, User Name and Password.
4. Database Setup Wizard pops-up.
5. In the wizard screen, select Server Type as SQL Server. Available SQL Server Instances are listed in a combo box. Enter the Device Name and Port of the SQL Server from the instances.
6. Select the authentication type using the "Connect Using:" option.
7. The options are:
   - Windows Authentication
   - SQL Server Authentication

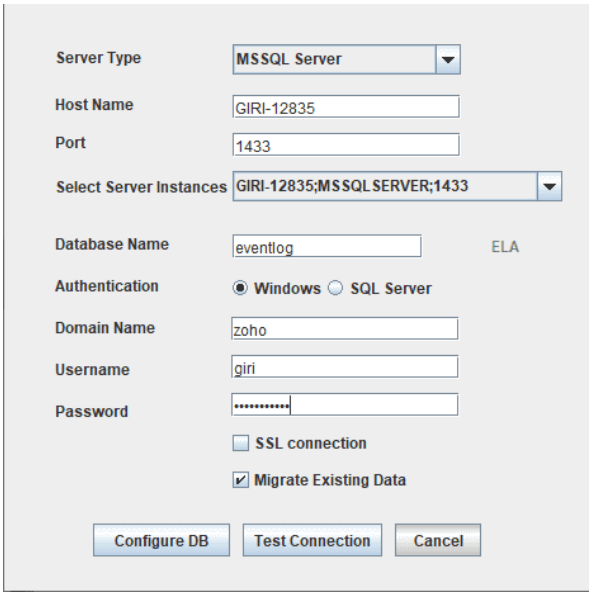
Note

Ensure that both EventLog Analyzer Server and MS SQL Server are in the same domain and logged in with the same Domain Administrator credentials.

Windows Authentication

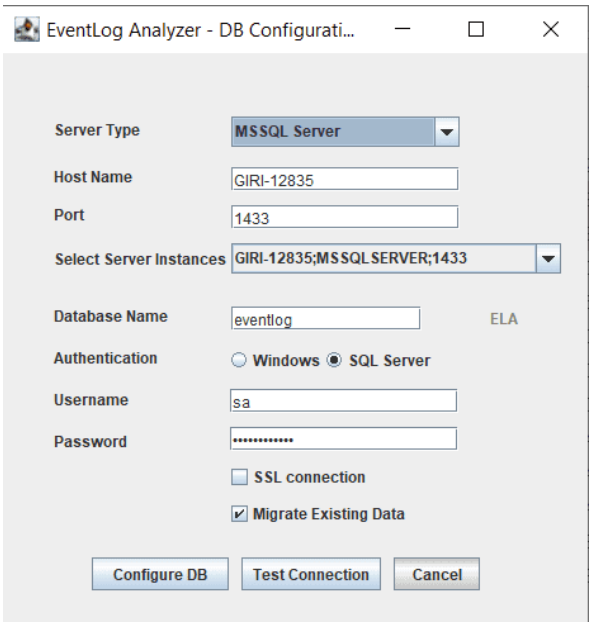
For EventLog Analyzer version 8.0 (Build 8010) onwards,





SQL Server Authentication

For SQL Server Authentication, enter the User Name and Password.



8. Click the Test Connection button to verify the correctness of the credentials. If the test fails, recheck and enter the correct credentials.
9. Click the Configure DB button to save the SQL Server configuration. Note that configuring the settings of the SQL Server database may take a few minutes.
10. The product will start automatically after the configuration is complete.

15.4. Migrating inbuilt Postgres(PG) SQL to a common PGSQL database (DB)

Last updated on: September 12, 2025

In this page

Overview

Steps to migrate bundled DB

Managing DB IP changes

Overview

This section explains how to migrate the bundled DB to a common DB, configure access, and manage changes in the DB IP.

Steps to migrate bundled DB

1. Stop Log360

> NOTE
>
> Stopping Log360 is not required to create the service. However, the bundled DB must be stopped before you can start the service.

- Run Command Prompt as Admin.
- Place the migration script migrateBundledDBAsExternal.bat inside: <LOG360_HOME> \bin
- Navigate to the bin directory and execute the migration command: migrateBundledDBAsExternal.bat <IP/HOST_NAME>
- Add the following entries in the common DB host's pgsql\data\pg_hba.conf file to allow client connections:

```
host    all     all             0.0.0.0/0               md5
```

Figure 1: Accessing the services application

- Start the PostgreSQL service: ManageEngineLog360Postgres

> NOTE
>
> Allow inbound/outbound rules in the postgres machine for client machines to access the DB.
> Ensure Log360 server is started at least once before migration to initialize the database.

Handling DB IP changes

If the common DB IP changes, you must unregister and re-register the PostgreSQL service with the new IP. Two methods are available:

- Manual method
- Using the batch file

Manual method

1. Stop the running service.
2. Run the following command as Administrator to unregister the service: .\pg_ctl unregister -N "ManageEngineLog360Postgres"
3. Update the new IP in the database_params.conf
4. Re-register the service with the new IP: pg_ctl register -N "ManageEngineLog360Postgres" -D "path to pgsql\data" -o "-p 33335 -h ip/hostname"
5. Update the new IP in the database_params.conf file of both server and processors.
6. Start the service.

Using the batch file

You can use reregisterDB.bat file to automatically execute the unregister and re-register commands.

> NOTE
>
> The batch file is located in <Log360_HOME>\bin

Syntax:

1. reregisterDB.bat <new_ip>
   - <new_ip> is mandatory, specifies the new IP address of the common database. The script re-registers the default service ManageEngineLog360Postgres.
2. reregisterDB.bat <new_ip> <service_name>
   - <service_name> refers to the PostgreSQL service name. The script re-registers the specified service.

Read also

This page explained how to migrate the inbuilt PostgreSQL to a common PostgreSQL database in Log360.

15.5. Scalability migration guide

Last updated on: September 12, 2025

In this page

Overview

Steps to switch to scalable architecture

Overview

This section explains how to migrate from the existing High Availability (HA) setup to the new scalable architecture.
In the HA setup, two servers are configured:

- Primary server
- Secondary/Standby server

During migration, only the primary server will be retained, and the secondary server will be decommissioned.

Steps to switch to scalable architecture

Follow the steps below to switch to the scalable architecture.

- Stop the server
- Update wrapper.conf on the primary server
- Update Elasticsearch configuration
- Decommission the secondary server
- Configure scalable architecture

Stop the service

- Shut down the application service on both the primary and secondary servers.

Update wrapper.conf on the primary server

- Navigate to the configuration file: <Log360_Home>\server\conf\wrapper.conf
- On the primary server, remove the following
  - lines:wrapper.java.additional.x+1=-DremoteIp=<Standby Server IP>
  - wrapper.java.additional.x+2=-DlocalIp=<Primary Server IP>
  - wrapper.java.additional.x+3=-DvirtualIp=<Virtual IP>

> NOTE
>
> The standby server configuration does not require any changes, as it will no longer be used in the

The standby server configuration does not require any changes, as it will no longer be used in the scalability setup.

- Update Elasticsearch configuration
  - Navigate to the configuration file: <Log360_Home>\ES\config\elasticsearch.yml
  - If the following property exists, remove it. If not present, no action is required: node.max_local_storage_nodes: 2
- Decommission the secondary server
  - The secondary (standby) server from the HA setup should now be decommissioned.
  - Only the primary server will continue for migration into the scalability architecture.
- Configure scalable architecture
  - After completing the configuration updates on the primary server, configure the scalable architecture.

Read also

This document explains how to migrate from a High Availability (HA) setup to scalable architecture. For related information, refer to the following articles:

- Configuring and managing Log Processors

16.1. Log360 MSSP Edition Overview

Last updated on: September 12, 2025

In this page

Overview

Key features

Pre-requisites for converting to the MSSP edition

Default communication protocols

Best practices for MSSP server deployment

Converting Standard Edition to MSSP Server

What happens after the conversion?

Overview

This document provides a detailed walkthrough for converting the standalone edition of EventLog Analyzer and Log360 into MSSP edition.
What is MSSP deployment: The MSSP deployment allows centralized management of multiple customer instances deployed in various geographical locations. It supports customer and technician management, secure multi-tenant views, and license allocation. The guide also explains necessary prerequisites, port requirements, and best practices to ensure a successful deployment.

Reference glossary

1. Distributed environment
   - Admin server: Acts as the central server in a distributed environment, coordinating data and configurations across all managed servers.
   - Managed server: Refers to the servers deployed at different locations in a distributed environment, which report to the admin server.
2. MSSP environment
   - MSSP server: Functions as the central server in an MSSP environment, enabling service providers to manage multiple customer servers from one console.
   - Customer server: Refers to the servers deployed at different customer locations in an MSSP environment, which are integrated with the MSSP server.

Key features

- Supports multiple customers across different geographical locations.
- Supports customer management, technician management, and customers' license management.
- Exclusive segmented and secured view for various customers of the MSSP in a single console.

> NOTE
>
> Log360 MSSP edition will have the distributed architecture only for its core component, the log management system -- EventLog Analyzer. Please note that you cannot integrate the identity threat detection and response (ITDR) component -- ADAudit Plus, or the data security component -- DataSecurity Plus, with your MSSP deployment. If you need more assistance on the deployment, contact our technical support team.

Pre-requisites for converting to the MSSP edition

Here are a few of the prerequisites which need to be taken care of before converting a standalone setup to the MSSP edition:

Port requirements

If you want to convert your existing standalone EventLog Analyzer or Log360 to MSSP edition, ensure that the following ports to be free for web server and PostgreSQL communication.

- 33335 (TCP): This is the port used for connecting to the bundled PostgreSQL database in Log360.
- 8095 (Web server port): This is the default web server port used by the solutions EventLog Analyzer and Log360. This port is used for connecting to a web browser. You can change this port during conversion.

Default communication protocols (HTTP/HTTPS)

By default, the customer's server and the MSSP server communicate using HTTP (port number 8095). There is also an option to convert the mode of communication to HTTPS.
Verify port availability to ensure it is unoccupied by concurrent local applications. This is crucial because for the product communication, the customer's server will send a request to port 8095 of the MSSP server and vice versa.

Best practices for MSSP server deployment

- We always recommend the conversion of a new server (EventLog Analyzer and Log360) to MSSP server to avoid data loss. You can follow the steps given here to convert the standalone instance into an MSSP server.
- Both the MSSP server and the customer server should be in the same build. If they are not in the same build, follow the steps mentioned in this page to download and apply the latest service packs.

NOTE

- If both the admin and customer servers are not in the same build number, it can lead to sync issues.
- One MSSP server is designed to manage up to 100 customer servers.

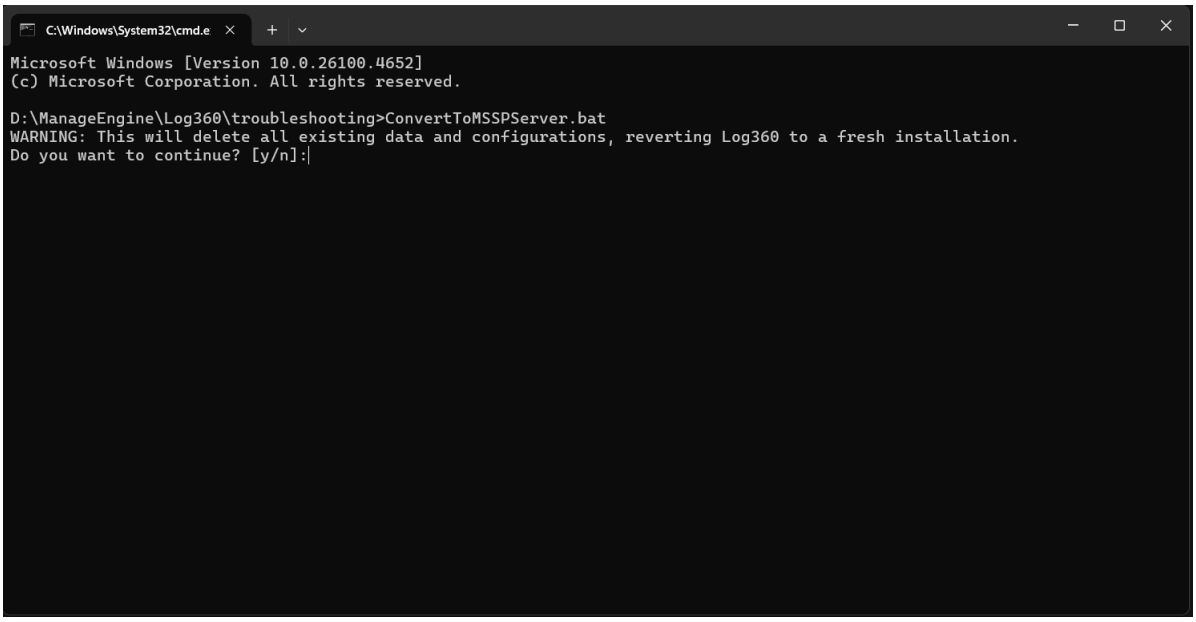
Converting standalone EventLog Analyzer and Log360 instance to MSSP Server

NOTE

Converting the standalone instance into an MSSP server will result in the deletion of data present in the standard edition. You need to back up the existing data if any to prevent data loss.

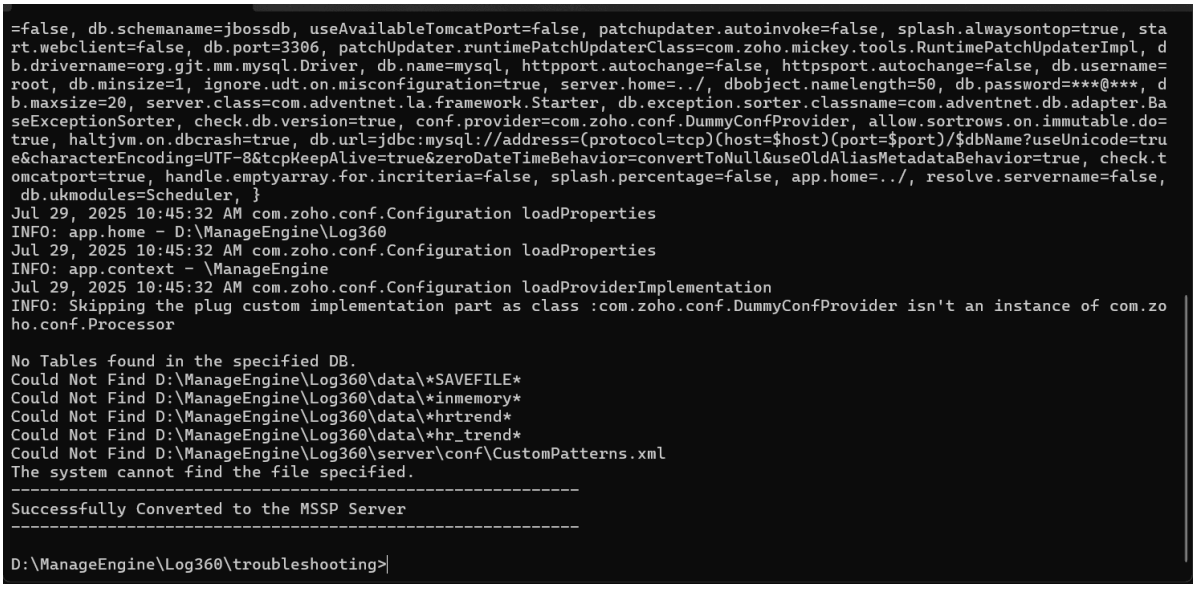
You can follow the steps given below to convert the standard edition of Log360 into an MSSP server:

1. Shut down Log360 or EventLog Analyzer.
2. Open the command prompt with administrative privilege and execute the Convert to MSSPServer.bat/sh file located in <product_home>/troubleshooting/ConvertToMSSPServer.bat/sh.
3. A warning message about the deletion of data of your existing installation will be displayed. Press y and click on the Enter key to continue.



4. If you want to configure a proxy server, enter y for the next query and enter the proxy server details.
5. You will see a success message if the standalone instance has been converted from the standalone edition into an MSSP server.





What happens after the conversion?

After conversion, the Log360 console initiates the application of the pre-existing MSSP-specific configurations and eventually switches to the MSSP version. During the conversion, all the existing Log360 data in the database will be erased and replaced by the MSSP configurations.

After the successful conversion, the functionalities of integration, license management, and more will be enabled in that server thereby acting as the MSSP server.

Read also

This document explained how to set up and convert Log360 to the MSSP edition, including its capabilities, default communication protocols, and post-conversion behavior. For more advanced deployment options and customer-specific configurations, refer to:

- License management
- Technician management
- Reverse proxy
- Auto-upgrade

16.2. Customer management in Log360 MSSP

Last updated on: September 12, 2025

In this page

Overview

Integrating outsourced Log360 instances into Log360 MSSP

Accessing customer management

Customer management

Adding a customer

Editing a customer

Deleting a customer

Manual data sync

Manage customer license (via Customer Management page)

To view the license allocation details

To edit the license allocation details

Monitoring customer server health

Overview

When you are converting your existing standalone instances to MSSP deployment model, you would want to remove multiple instances deployed across various regions and provide a single interface through MSSP deployment model to access them. The Customer Management module in Log360 MSSP allows a seamless onboarding while also providing a centralized interface to access and manage all integrated instances, enabling MSSPs to efficiently oversee customer environments from a single console.

Integrating outsourced Log360 instances into Log360 MSSP

Why is this crucial?

Integrating outsourced Log360 instances into Log360 MSSP is the central element of MSSP in which Log360 is integrated with the MSSP build. The outsourced Log360 instances (customer servers) are Log360 environments deployed on behalf of customers, running in their infrastructure.

> NOTE
>
> Outsourced instances refer to customer instances deployed across different locations.

To centrally manage all the customers from MSSP console, those customer servers need to be integrated with MSSP.

To monitor and maintain outsourced Log360 instances, they have to be integrated into Log360 MSSP. Follow the steps below:

Phase 1: Download and install Log360

> **NOTE**
>
> If you already have Log360 installed and running, you can skip this step and proceed with Phase 2: Integrate Log360.

1. Download Log360 from the Log360 Website.
2. Install Log360 by double-clicking the downloaded EXE files and following the InstallShield wizard.
3. Once the installation is complete, start Log360 by double-clicking the desktop shortcut icons of the respective components.

Phase 2: Integrate Log360

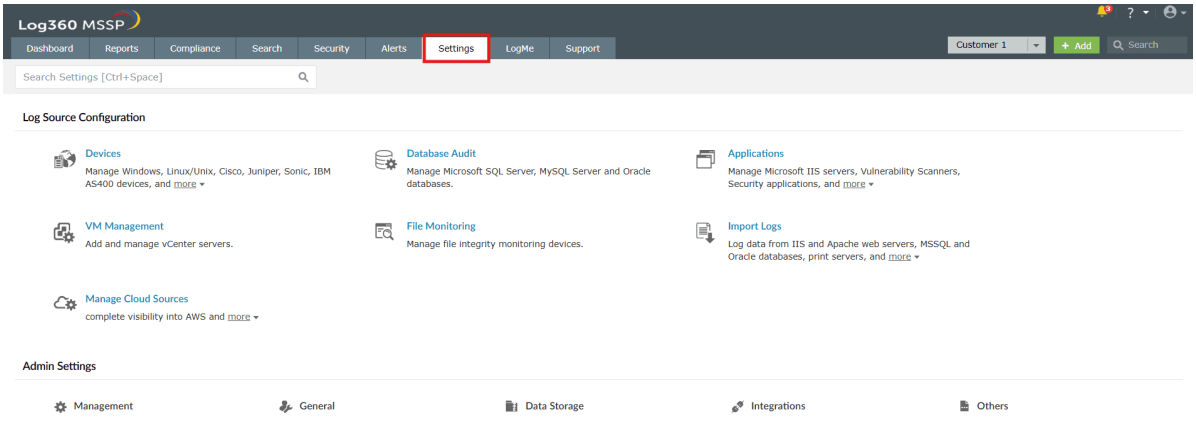
Pre-requisites:

- Make sure that all the customers' product console is set up and running before proceeding with the steps given below.
- Your Log360 MSSP server and your customer server should be in the same version (build).
- Ensure that the connectivity of both Log360 MSSP and customer Log360 are bidirectional.

Accessing customer management

To access the customer management module:

1. Log in to the Log360 MSSP application using the credentials of a Log360 MSSP administrator.
2. Navigate to the Settings tab in the header pane and click on the Customer Management option.



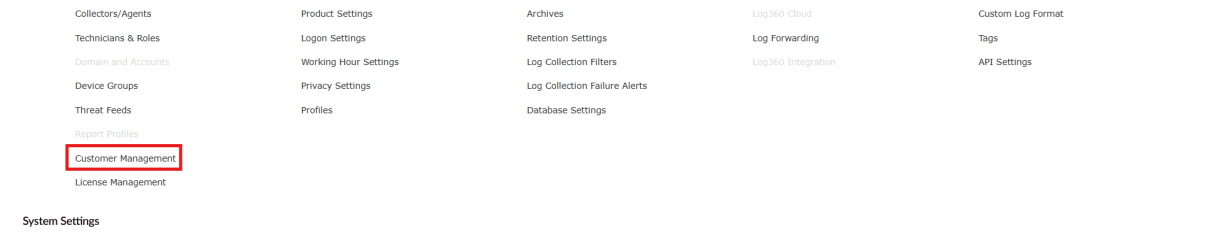


Image 1: Customer Management via Settings tab in Log360 MSSP

3. From this page, you can manage - add, edit, or delete customers.

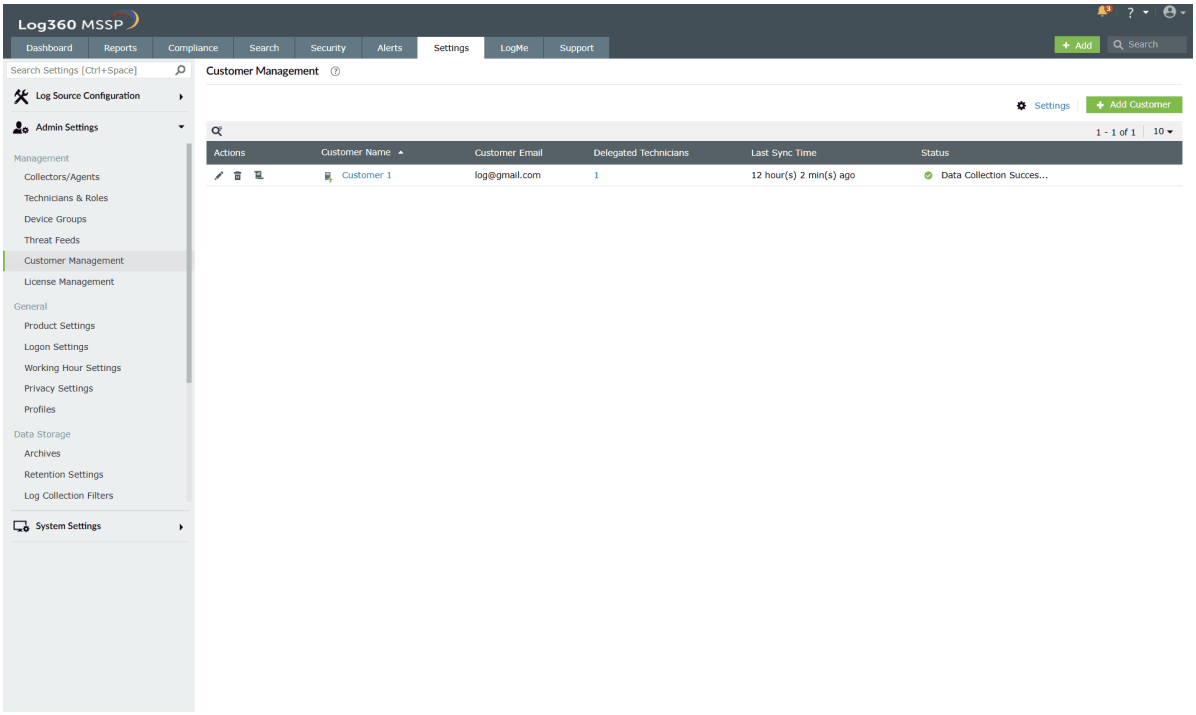


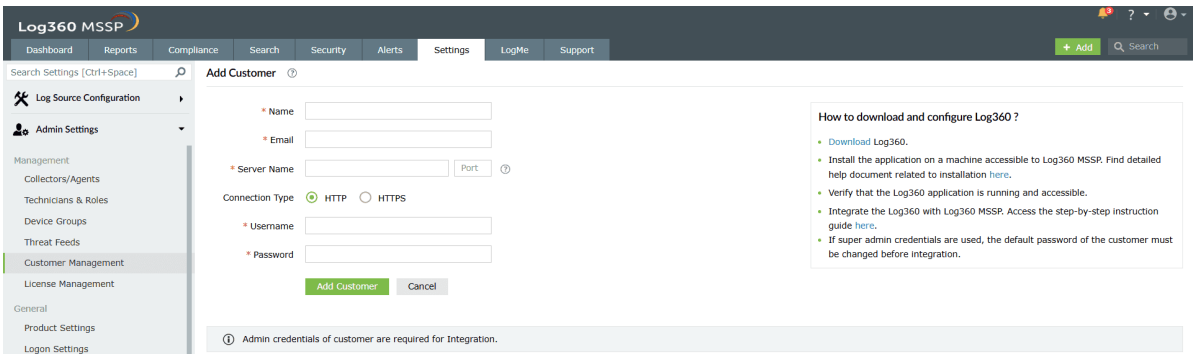
Image 2: Customer Management in Log360 MSSP

Customer management

Adding a customer

To add a customer,

1. Click on the Add Customer link available in the Customer Management page. This opens the Add Customer form.



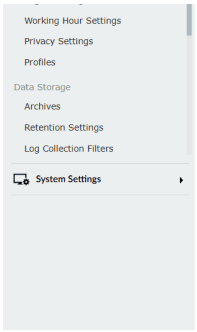


Image 3: Adding a customer in Log360 MSSP

2. Fill in the required fields in the form to add the customer:
   - Enter the Customer Name and a valid Customer mail. The Customer Name needs to be unique and should not exist already.
   - Enter Server Name, Port, and specify the Connection type (HTTP or HTTPS).
   - Enter the Admin Credentials of the respective Log360 Customer.
   - Click Add Customer.
3. Upon successful completion of action, the below pop-up appears, and the respective customer is instantly added.

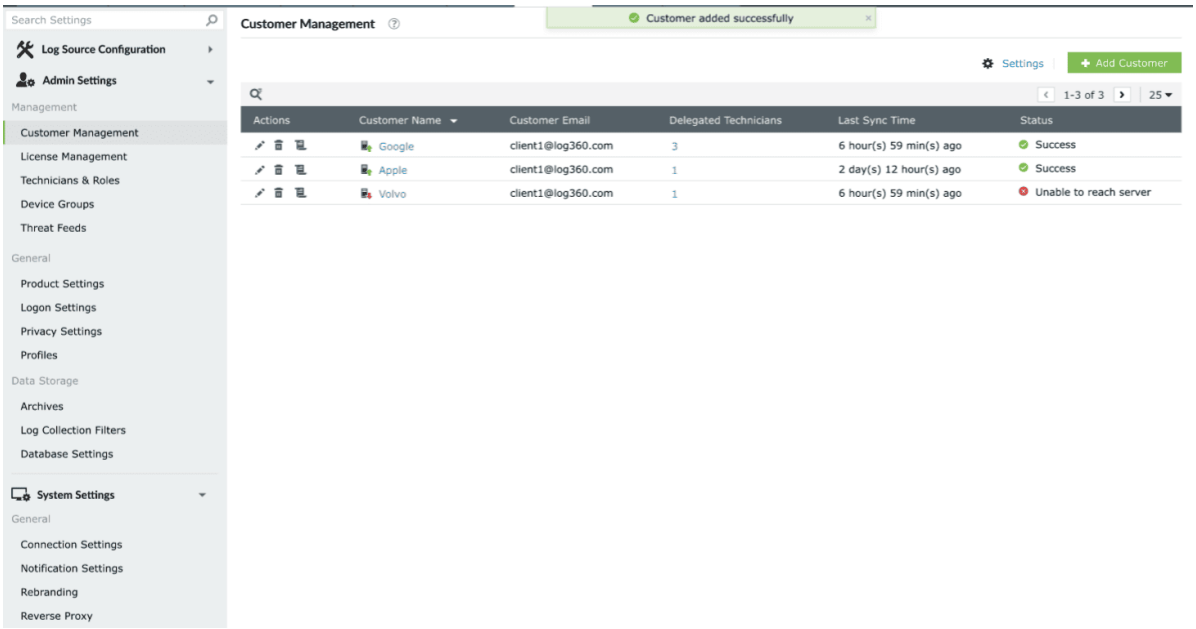
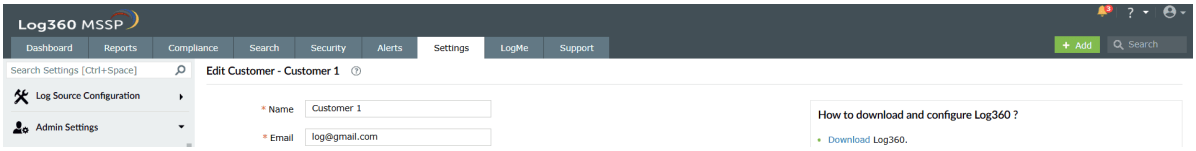


Image 4: Adding a customer in Log360 MSSP

Editing a customer

1. Navigate to the Customer Management page and click on the edit icon beside the customer's name you wish to update. The edit form will open, similar to the Add Customer form.



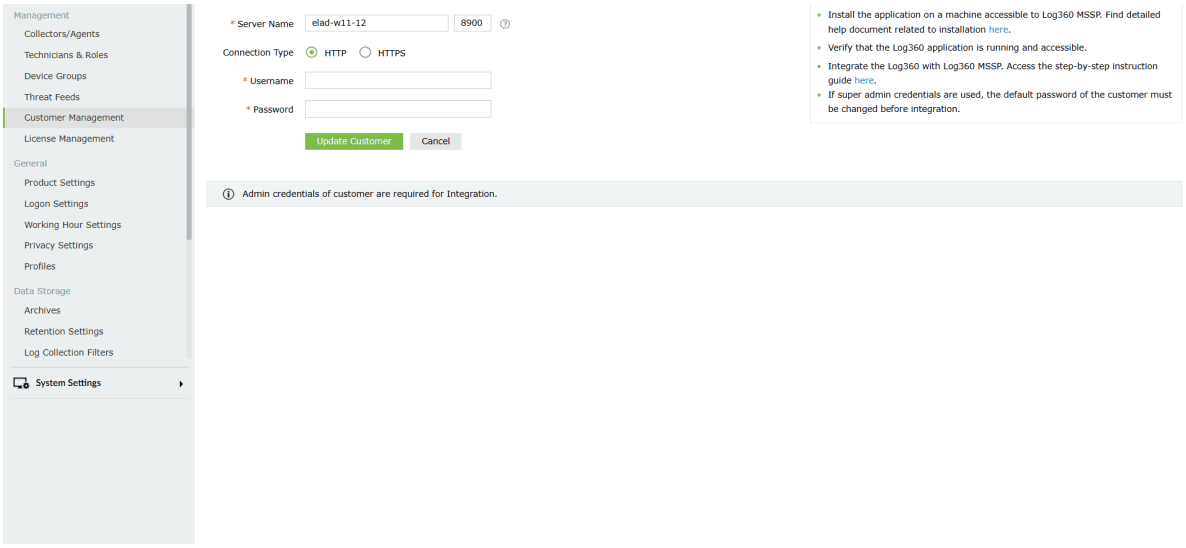


Image 5: Editing a customer in Log360 MSSP

2. Make the necessary changes, enter the Admin Credentials of the respective Log360 Customer, and click on Update Customer.
3. Upon successful completion of action, the below pop-up appears, and the respective customer's details are instantly updated.

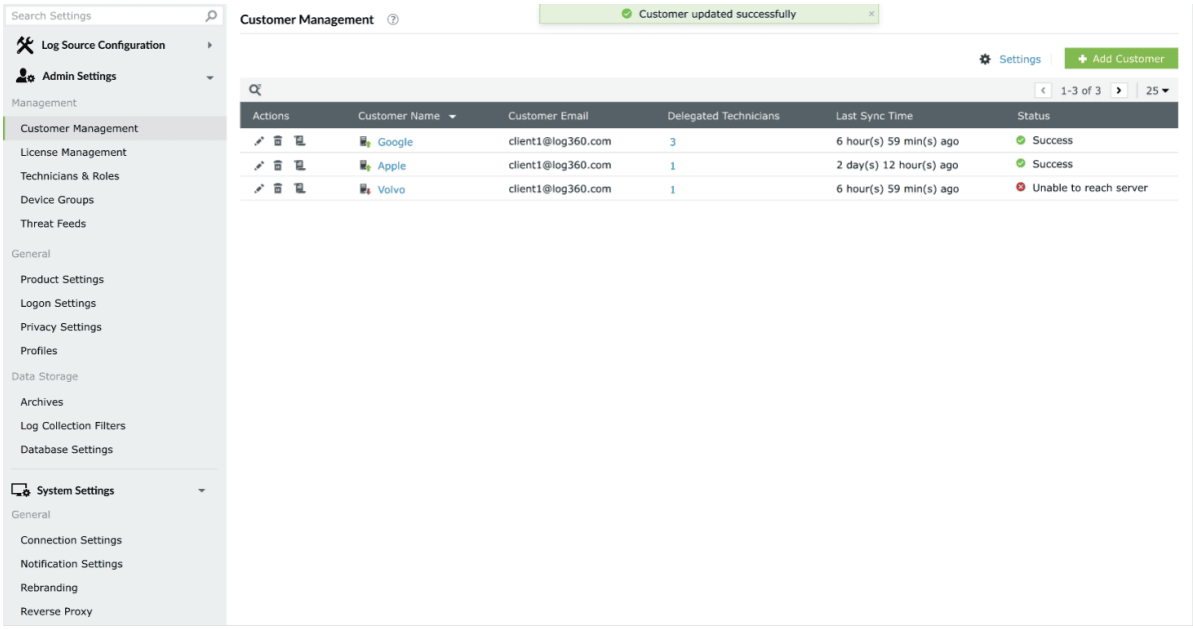
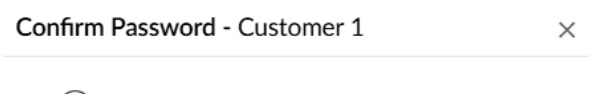


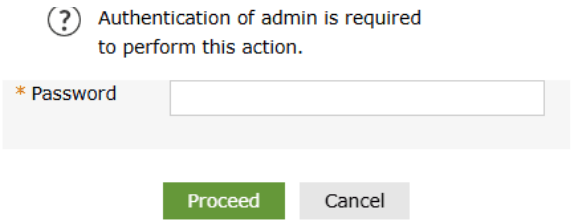
Image 6: Editing a customer in Log360 MSSP

Deleting a customer

Soft delete:

1. Navigate to the Customer Management page and click on the delete icon beside the customer's name you wish to delete. A Confirm Password pop-up appears like shown below.





2. Enter your (the currently logged in admin technician's) Password and click Proceed to confirm.
3. Upon successful completion of action, the below pop-up appears, and the respective customer is instantly deleted.

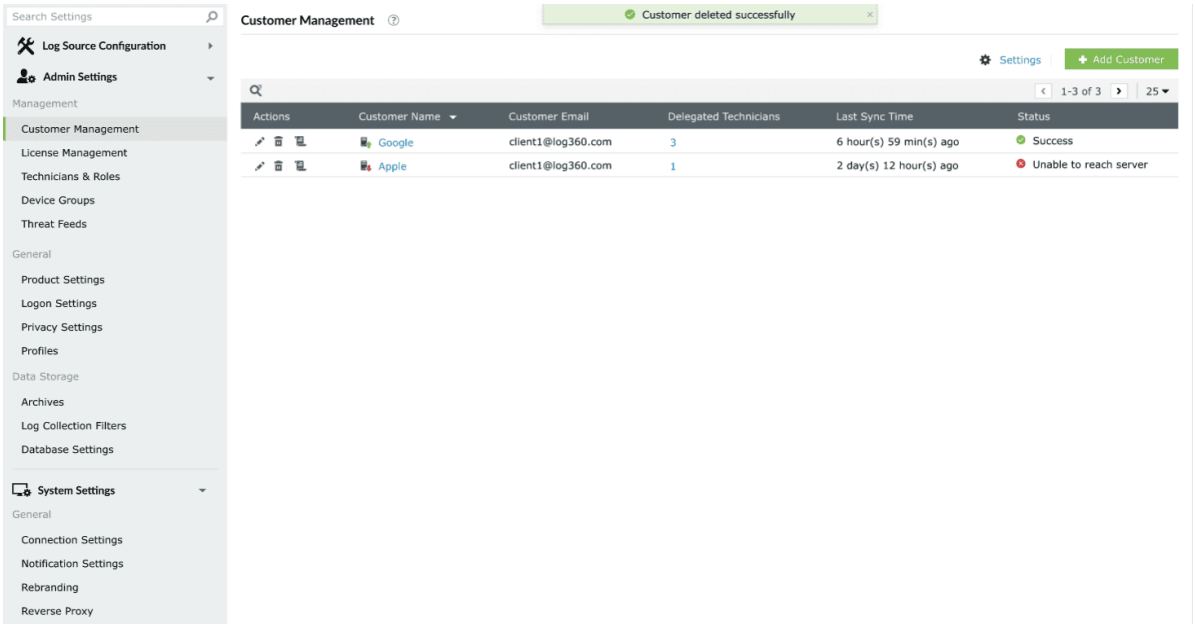


Image 7: Deleting a customer in Log360 MSSP

> NOTE
>
> Make sure that given Log360 customer is up and reachable from Log360 MSSP.

Force delete:

1. In the case of failure in the soft removal of a customer, the product automatically prompts a force delete customer popup. This applies to cases when the customer server is unreachable but the MSSP still needs to delete the customer.
2. Enter the reason for force removal and click on Force Delete.

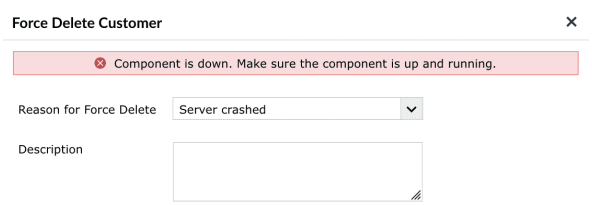




Image 8: Force deleting a customer in Log360 MSSP

> **NOTE**
>
> If a customer is force deleted from Log360 MSSP while the customer is down or disconnected, Log360 MSSP details might not be completely removed from the customer.

Manual data sync

To manually trigger data synchronization between Log360 MSSP and Customer Log360 instance,

1. Hover on the Status column of the desired customer to view the Sync Now button.

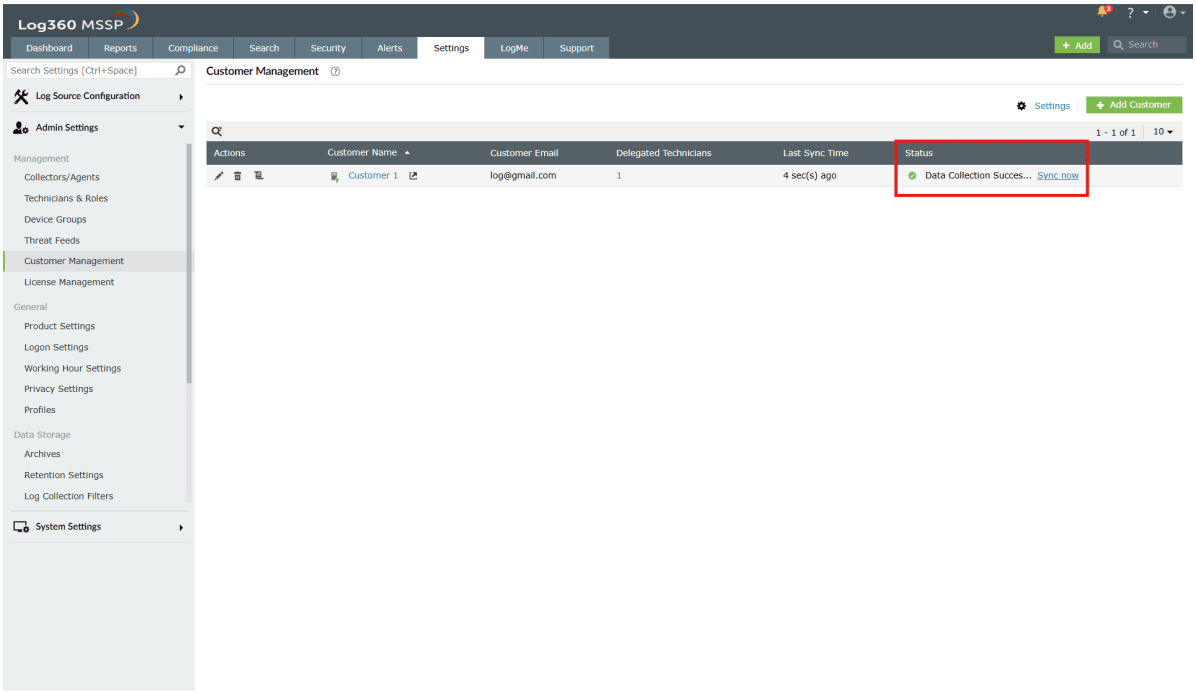
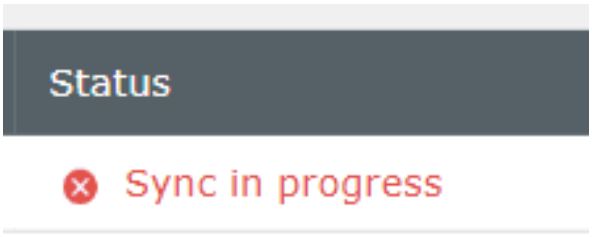
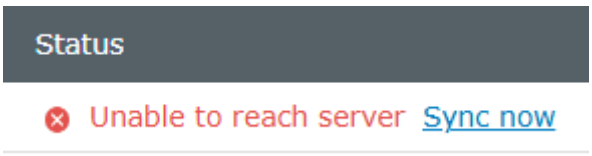


Image 9: Manual data sync in Log360 MSSP

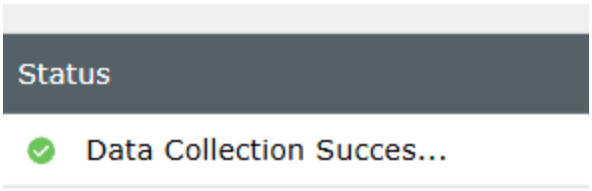
2. Once you click on it the sync process begins and the status will be shown as below.



3. In case the sync fails, the below status is shown.



4. Once the sync is successfully completed, the Data Collection Successful status is displayed as shown below.



Data synchronization between Log360 and Log360 MSSP

Once Customer Log360 has been integrated with Log360 MSSP, the data such as component integration and health details, reverse proxy, technician details, license details and more will automatically be synchronized. This saves time for the administrators, as they no longer have to configure the same settings across every Log360 customer.

Manage customer license (via Customer Management page)

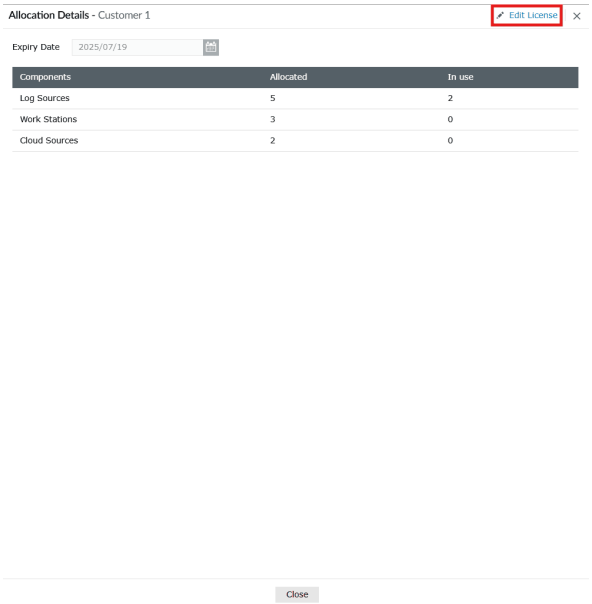
To view the license allocation details:

1. Navigate to the Customer Management page and click on the license icon beside the customer's name. You will be taken to the License Management page with the Allocation Details box open. You can view all the required details pertaining to the license allocation of that customer.

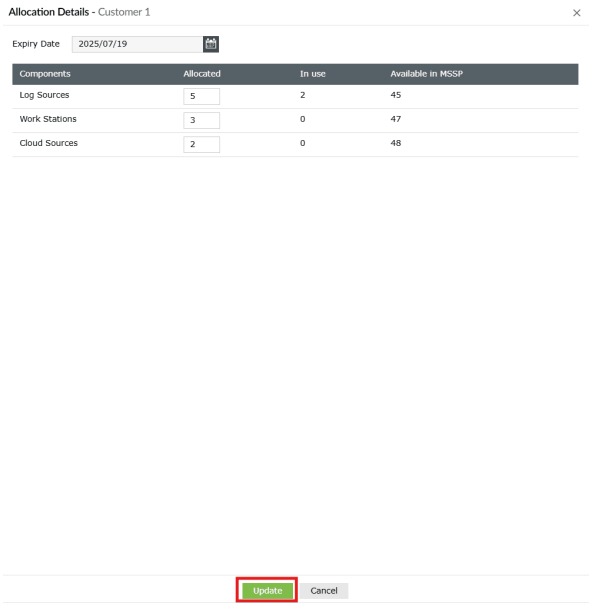


To edit the license allocation details:

1. Upon following the steps to view a customer's license allocation details, the Allocation Details box appears along with the option to edit at the top-right corner of the box. Click on the Edit License button to make changes to an existing customer's allocation details.



2. Make the necessary changes and click on Update.



3. Upon successful completion of the action, the below pop-up appears.



> **NOTE**
>
> Additionally, you can allocate a license to a customer via the License Management page in the product console. To know more, refer to the License Management help document.

Monitoring customer server health

1. There is a server icon located right before the name of the customer.

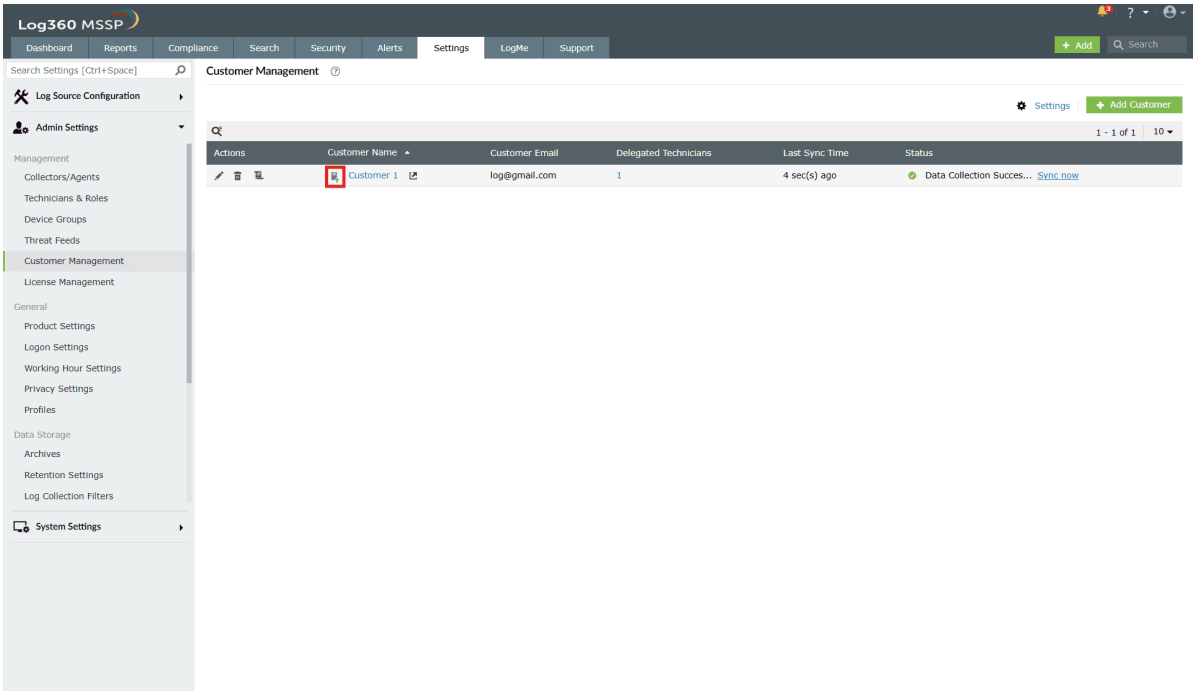
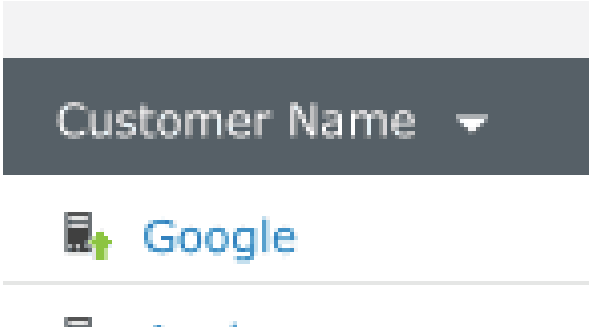
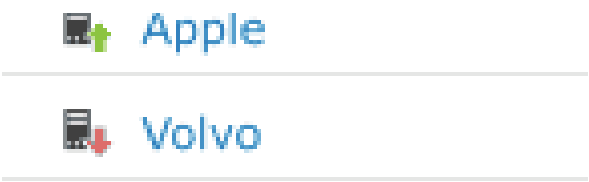


Image 10: Monitoring customer server health in Log360 MSSP

2. As shown below, the server icon near the customer name shows whether the customer server is up or down.
   - The green upward arrow indicates that the server is up and running.
   - The red downward arrow shows that the server is down.





NOTE

In case of a server error, try restarting Log360 and trying again.

Read also

This document covered the complete workflow of integrating and managing customer Log360 instances within Log360 MSSP, from setup to monitoring. For related administrative capabilities, refer to:

- Technician management
- Reverse proxy
- Auto-upgrade

16.3. License management in Log360 MSSP

Last updated on: September 12, 2025

In this page

Overview

Applying for license for MSSP serverApplying a license to customer

Data in the License Management module

Manage existing customer's license

Viewing license allocation details

Edit license allocation details

Overview

Log360 MSSP allows centralized license management of all its customer servers. This document elaborates the steps on applying license to the customer servers and managing those licenses.

Applying for license for MSSP server

1. As the Admin technician in the MSSP, navigate to the Settings tab and click on License Management in the Management section under Admin Settings.

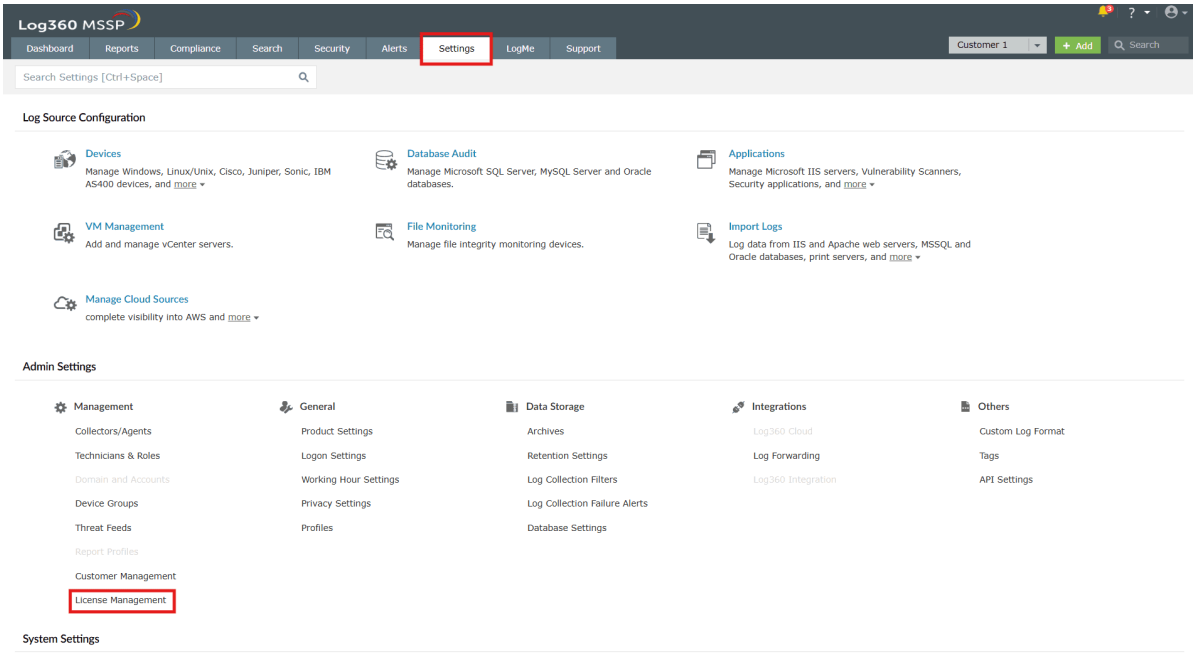


Image 1: License Management settings via the Settings tab in Log360 MSSP

2. The License Management page appears. Click on the drop-down button in the top-right corner as shown below.

below.

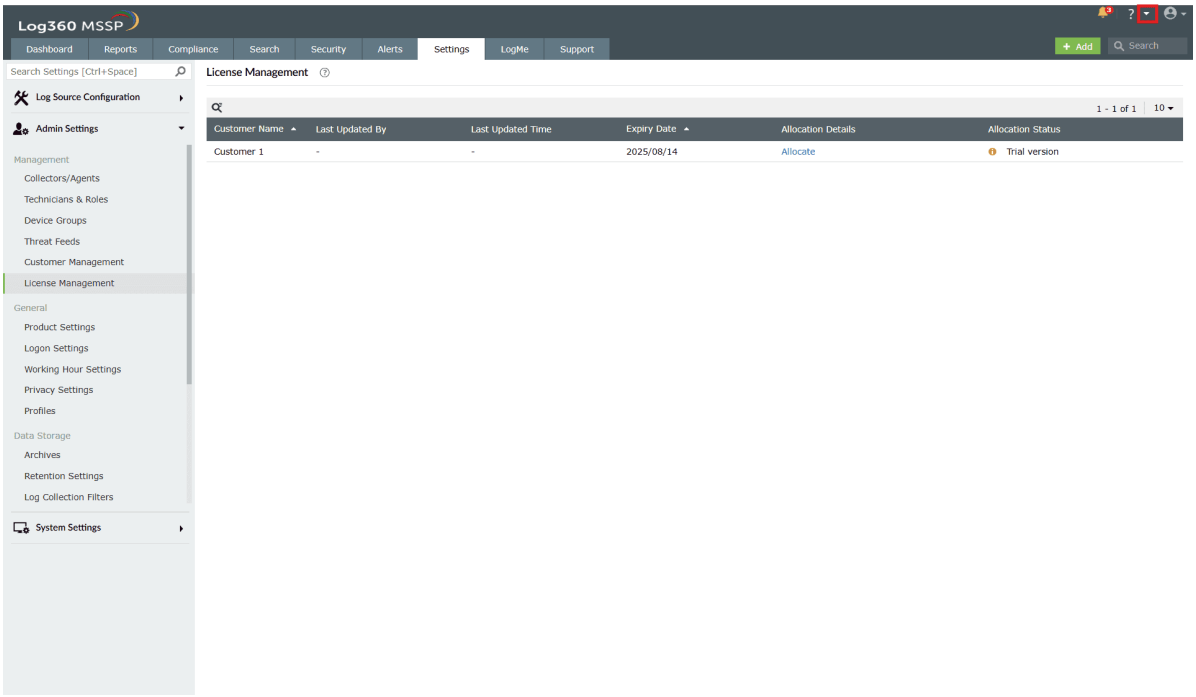
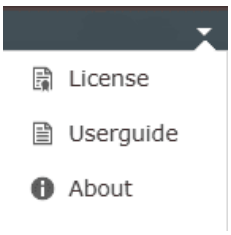
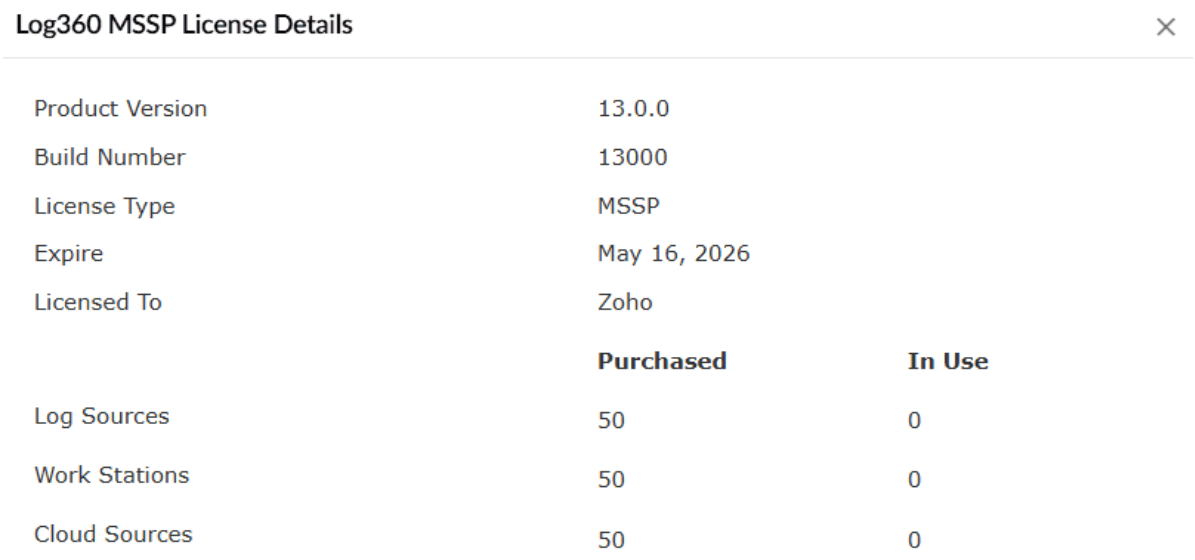


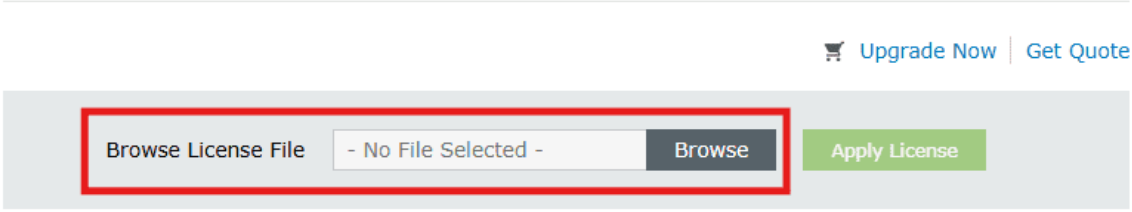
Image 2: License Management in Log360 MSSP

3. Select License from the drop-down list.



4. The Log360 MSSP License Details box appears. Browse the MSSP License File and click on Apply License.





NOTE

- Applying MSSP License is a mandatory step to allocate license to Customers.
- Without applying MSSP License, Customers can be integrated but Resources cannot be allocated.
- Internet connection is a must for License Module to work.

Applying a license to customer

1. As the Admin technician of the MSSP, navigate to the License Management page via the Settings tab and click on Allocate present in the Allocation Details column.

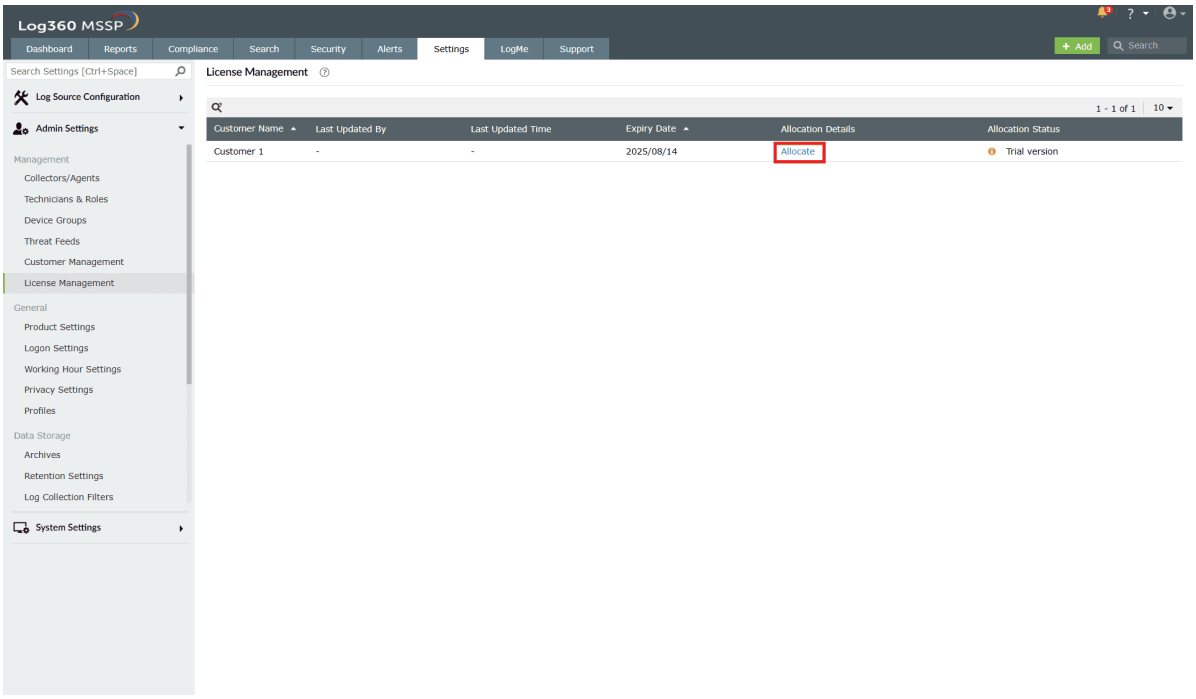
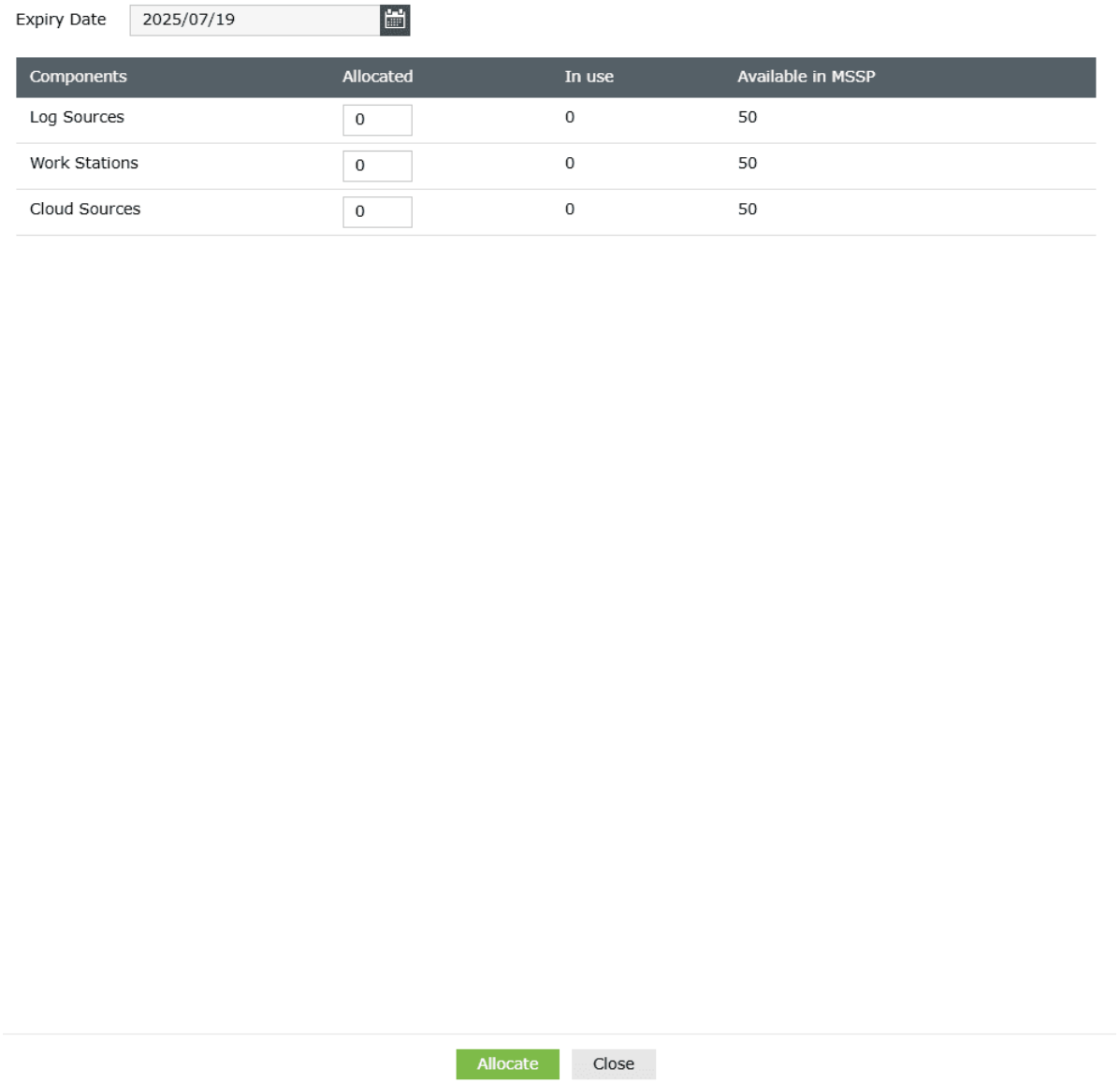


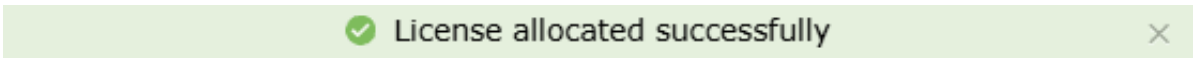
Image 3: License allocation details in Log360 MSSP

2. The Allocation Details box of that particular customer appears.



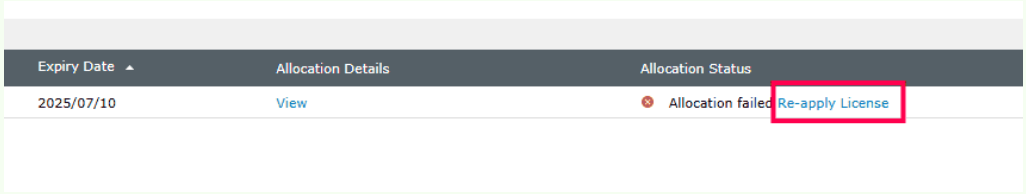


3. When allocating resources to a customer for the first time, the required resources count can be set in the Allocated column and then click on Allocate.
4. Upon successful completion of the action, the Allocation Details box closes and the below pop-up appears.



NOTE

1. Only technicians with the Administrator privilege can apply for a customer license.
2. If allocation fails for a customer, license can be reapplied by clicking the Re-Apply License button.



Re-Apply License button applies the same license again. This can be used when a component was down previously but is now up and running.

Data in the License Management module

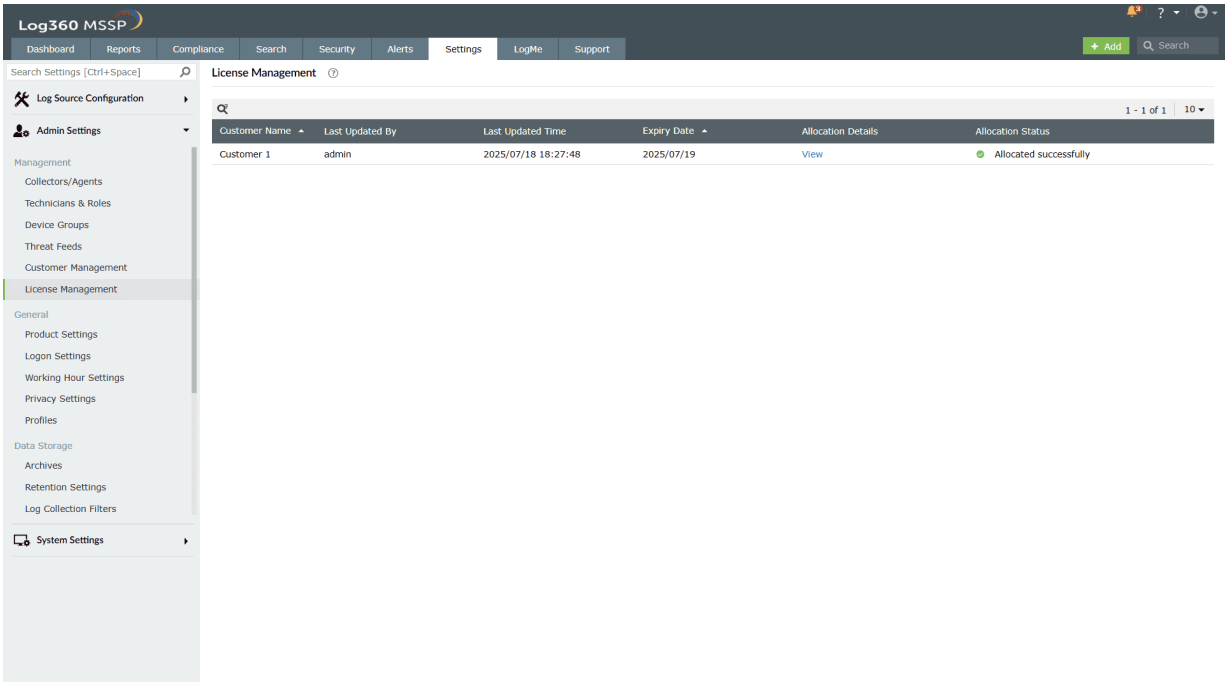


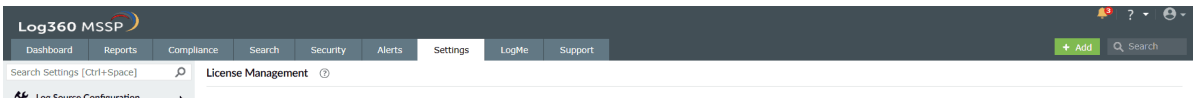
Image 4: License allocation details in Log360 MSSP

1. Customer Name: The name of the customer with an allocated license.
2. Last Updated By: Shows who has made the last change/update for this customer. Additionally, when hovered on the details in the Last Updated By column, the last updated date and time is shown.
3. Last Updated Time: Shows when the last change/update has been made for this customer.
4. Expiry Date: Shows the customer's current license's expiry date.
5. Allocation Details: Provides the option to view (and edit) the allocation details of the customer.
6. Allocation Status: Shows if the license for that customer has been allocated successfully or not.

Manage existing customer's license

Viewing license allocation details

1. In the License Management page, click on the view button under the Allocation Details column as highlighted below.



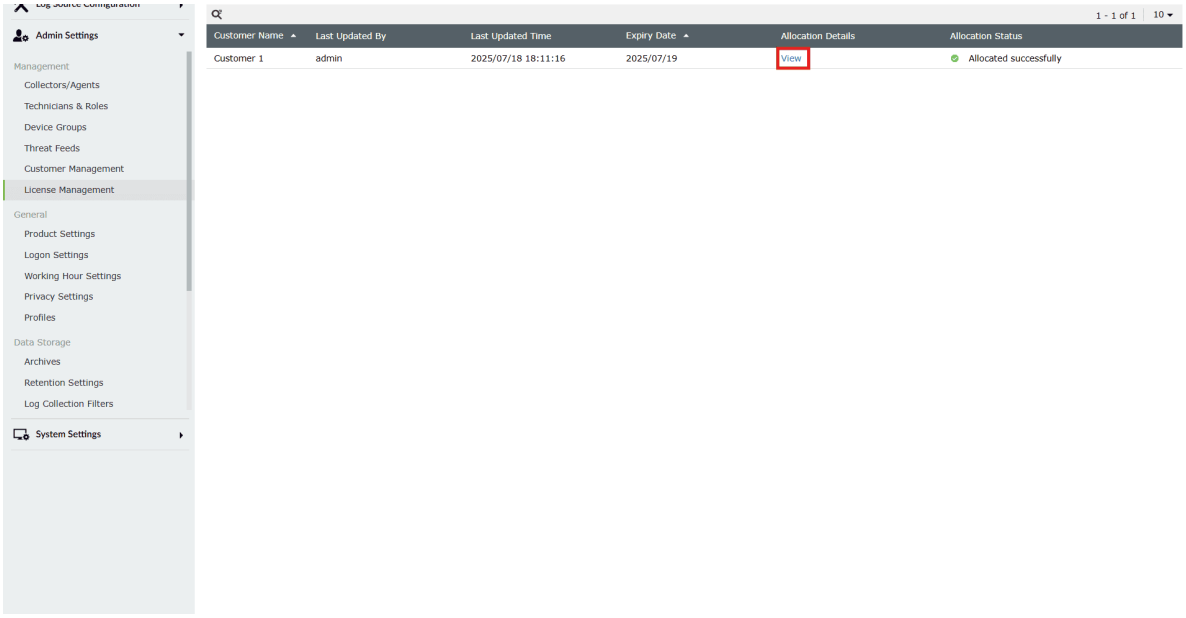
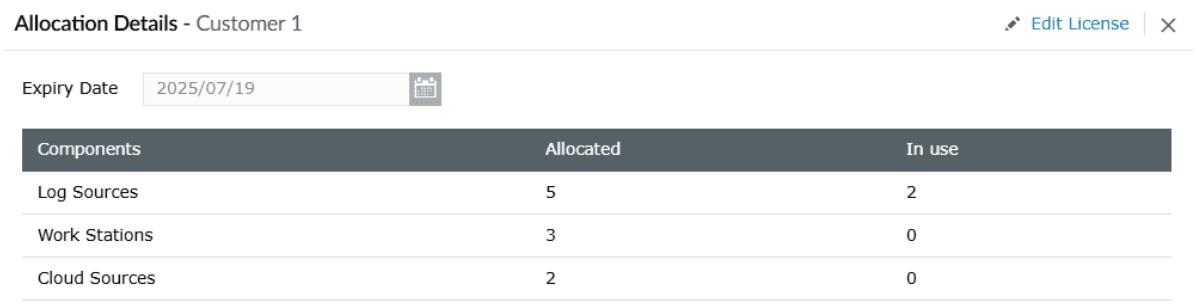


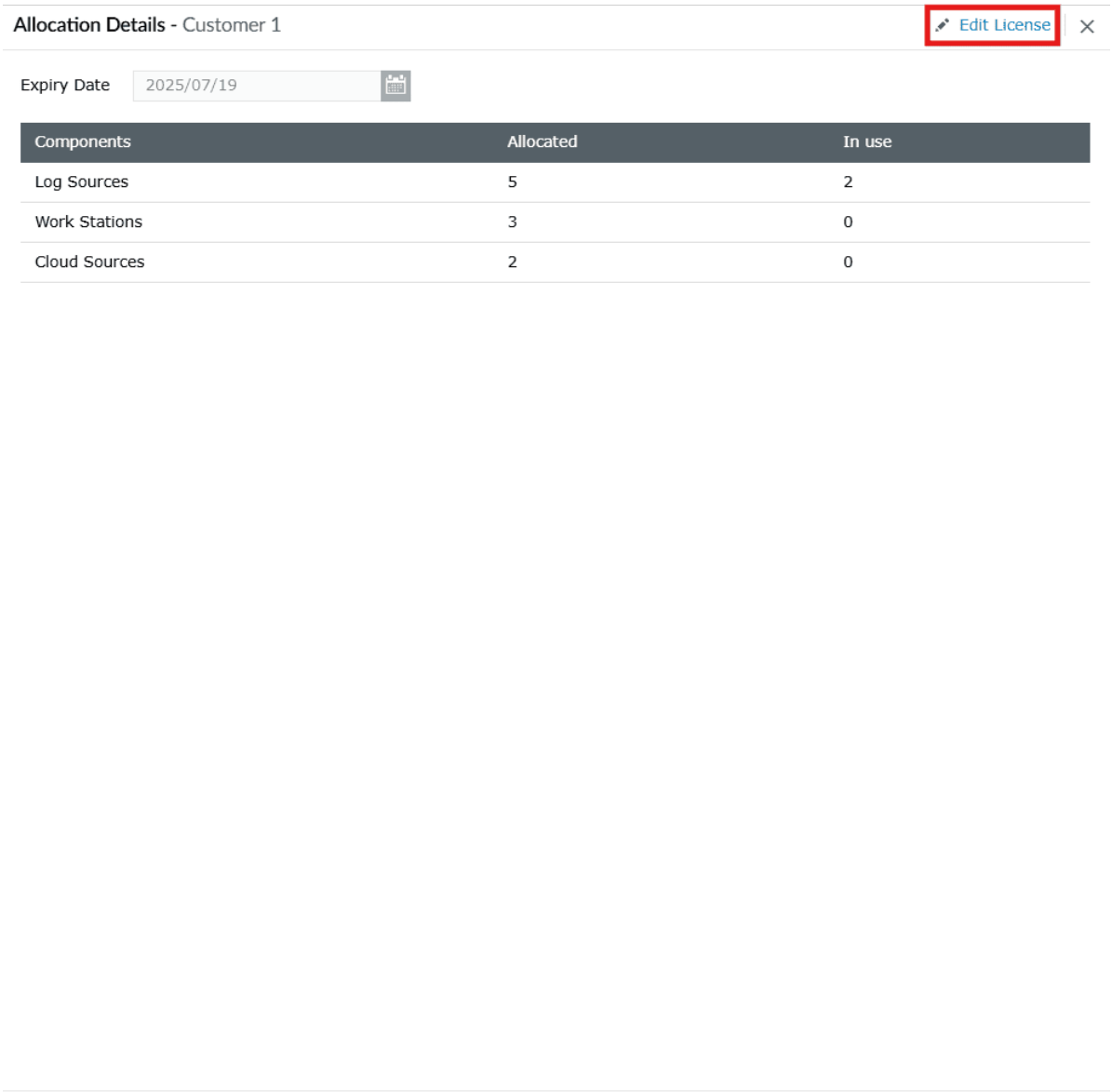
Image 5: Viewing license allocation details in Log360 MSSP

2. The Allocation Details box of that particular customer appears, and you can view all the required details pertaining to the license allocation of that customer.

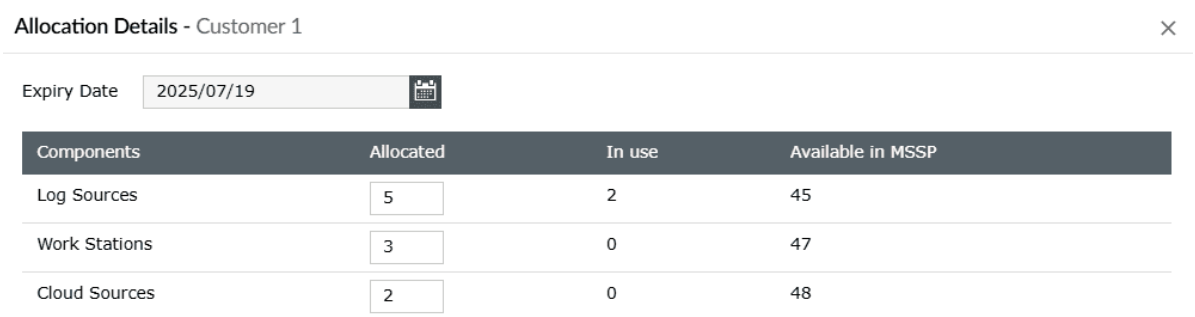


Edit license allocation details

1. Upon following the steps to view a customer's license allocation details, the Allocation Details box appears along with the option to edit on the top-right corner of the box. Click on the Edit License button.

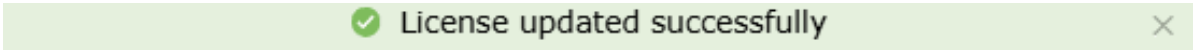


2. Make the necessary changes and click on Update.





3. Upon successful completion of the action, the below pop-up appears.



> NOTE
>
> You can only view and/or edit a customer's license. An option to delete is not provided.

Read also

This document detailed the steps for applying and managing MSSP and customer licenses in Log360. For more features related to centralized administration, refer to:

- Reverse proxy
- Auto-upgrade

16.4. Technician management in Log360 MSSP

Last updated on: September 12, 2025

In this page

Overview

Technician roles and privileges

Managing technicians

Adding a new Log360 MSSP technician

Enable/disable an existing technician

Edit an existing technician

Delete an existing technician

Overview

Log360 MSSP supports authorization and authentication at a local level and is compatible with third-party applications like Active Directory. It allows adding users in three realms (user groups) via., Admin, Operator, and Guest. The Admin user role has the highest order of privilege in both Log360 MSSP and Customer server and UI. The Operator has limited privileges that enables access to perform create and delete operations on the allotted resources. The Guest has read-only privilege on the allotted security resources (device groups).
When a customer gets assigned to a technician, the technician will be synced to that customer. Synced MSSP technician will have "Authentication type" as "Central Authentication" in the customer end. These technicians will be disabled in the customer if the customer instance gets dis-integrated from MSSP instance.Need for efficient technician management
Technician management helps to manage users with specific privileges, which enables them to perform certain actions. Managing technicians helps to assign specific roles and privileges to perform tasks, without granting unnecessary widespread access to critical functions.

> NOTE
>
> If Log360 MSSP technician is delegated with a customer Log360, that technician will be synced from Log360 MSSP to Log360

Technician Roles and Privileges

There are primarily three roles available that can be assigned to various users as listed below:

- Admin
  - Role with the highest privileges.

- Has access to all configurations and operations.

- Operator
  - Role with limited privileges.
  - Can perform management actions (create/edit/delete) on allotted resources .
- Guest
  - Role with least privileges.
  - Has only 'Read only' privilege on allotted resources.

Managing technicians

Adding a new Log360 MSSP technician

You can either add a user from AD or add a local technician in Log360 MSSP

To add a local technician,

1. Navigate to the Settings tab and click on Technicians & Roles in the Management section under Admin Settings.

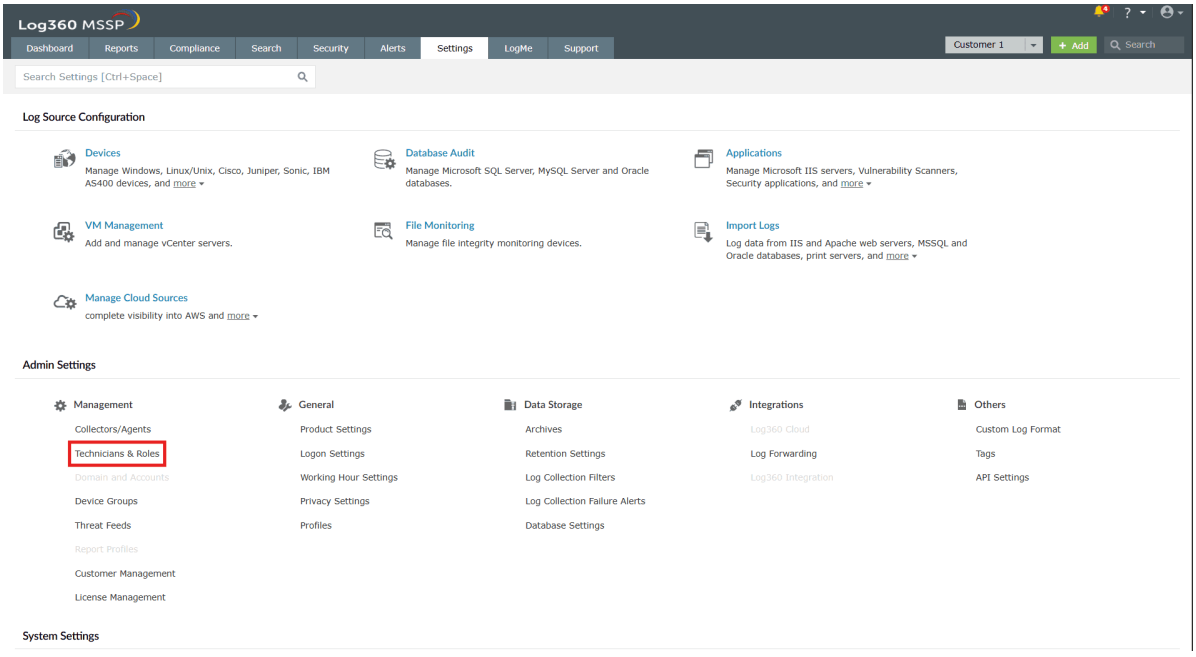
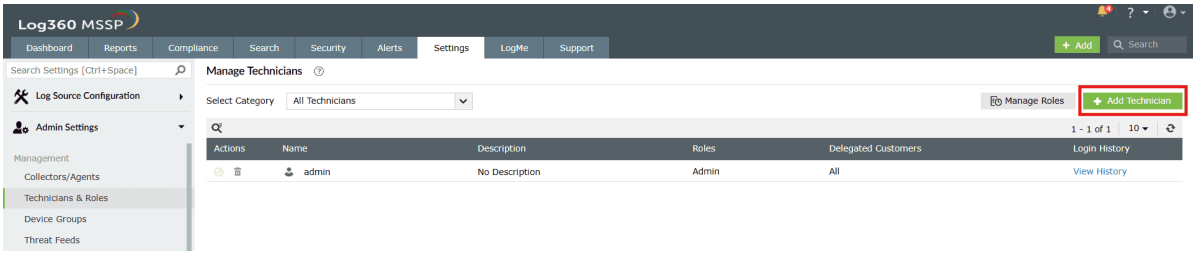


Image 1: Technicians & Roles via the Settings tab in Log360 MSSP

2. Click on the Add Technician button on the top-right corner.



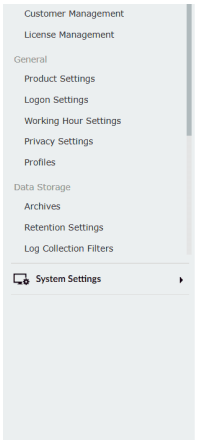


Image 2: Add technicians in Log360 MSSP

3. The Add Technician page expands, providing the necessary fields to be filled to add a technician as shown below.



Image 3: Adding a local technician in Log360 MSSP

4. Fill in the required fields:
   - Authentication type: Choose "Product Authentication"
   - Username: Enter a name for the technician in the Username field. You can additionally add a description by clicking on the Description button.
   - Password and Confirm Password: Enter a new password and confirm it in the respective fields.
   - Email ID: Enter the email address of the respective technician in the provided field.
   - Role: In the drop-down box, choose the role(s) you want to assign to the technician- Admin, Operator, Guest. You can assign more than one role to the technician, and the permissions of all the selected roles will be assigned to the technician.
   - Customers: Assign customer(s) to provide specific access only to that customers for that technician after clicking on the provided drop-down. Selecting All Customers will add provide access to any newly added customers for that technician.

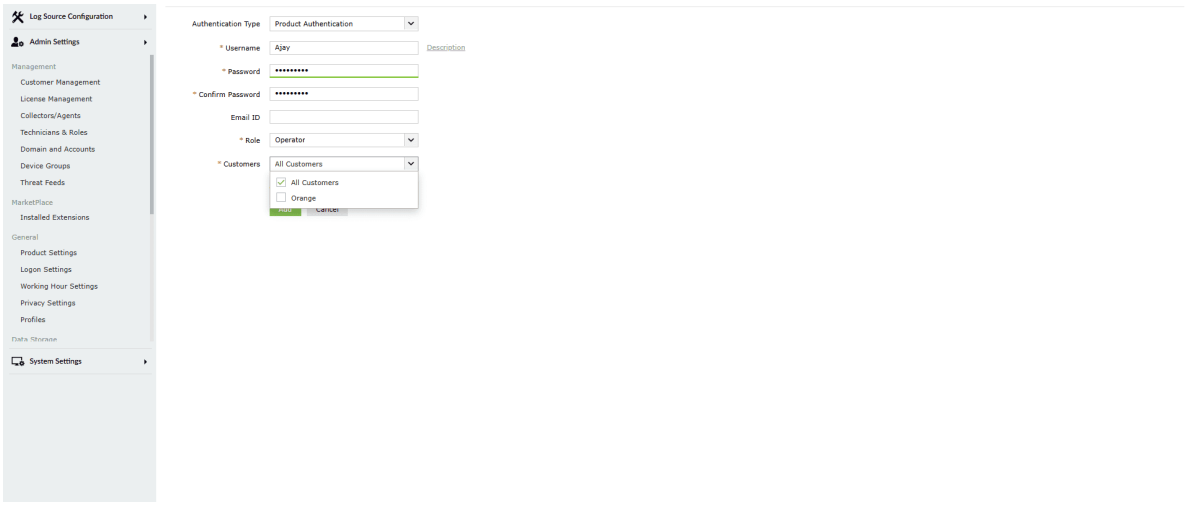


Image 4: Adding a technician in Log360 MSSP

> NOTE
>
> By default, All log source groups will be selected for the technicians.This means the technician will be provided access to all groups that will be added in the future as well.

- Advanced options: You can assign specific log source groups to a user to provide a segmented view to the user and limit the privilege on security resources by toggling the "Delegate Log Source Groups" checkbox under the advanced section

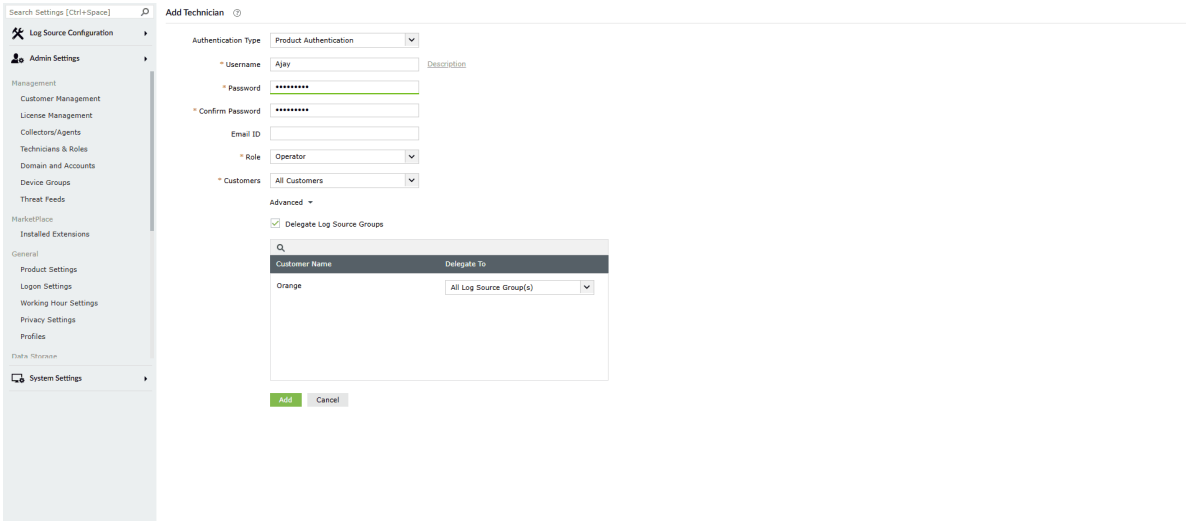
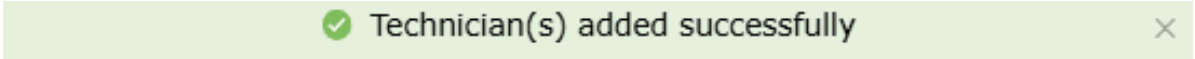


Image 5: Adding technicians in Log360 MSSP

5. After filling all the required fields, click on the Add button.
6. Upon successful completion of the action, the below pop-up appears.



To add an AD technician:

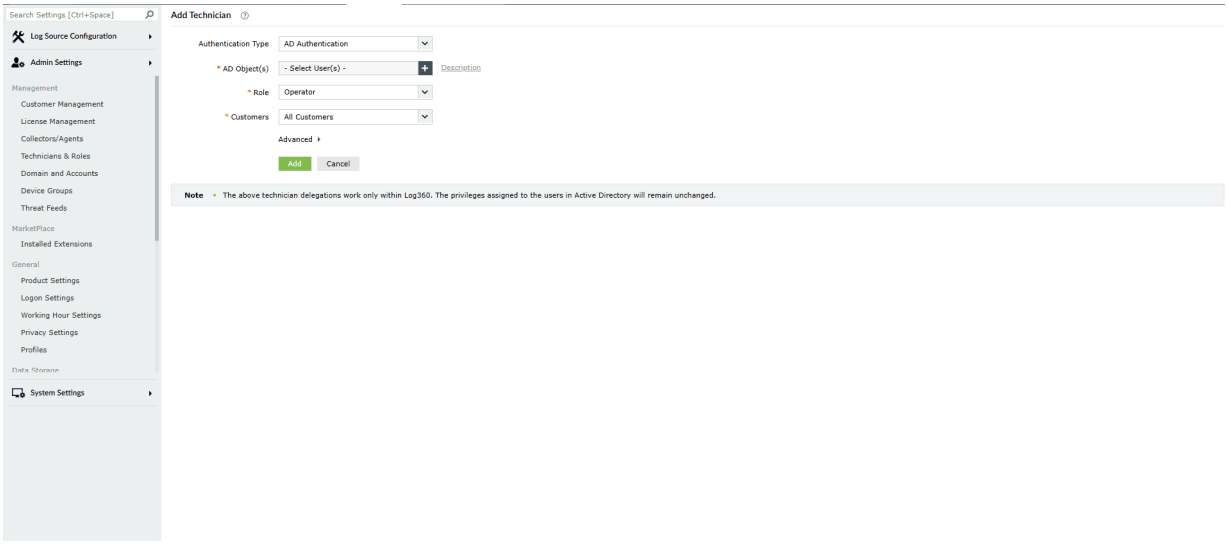
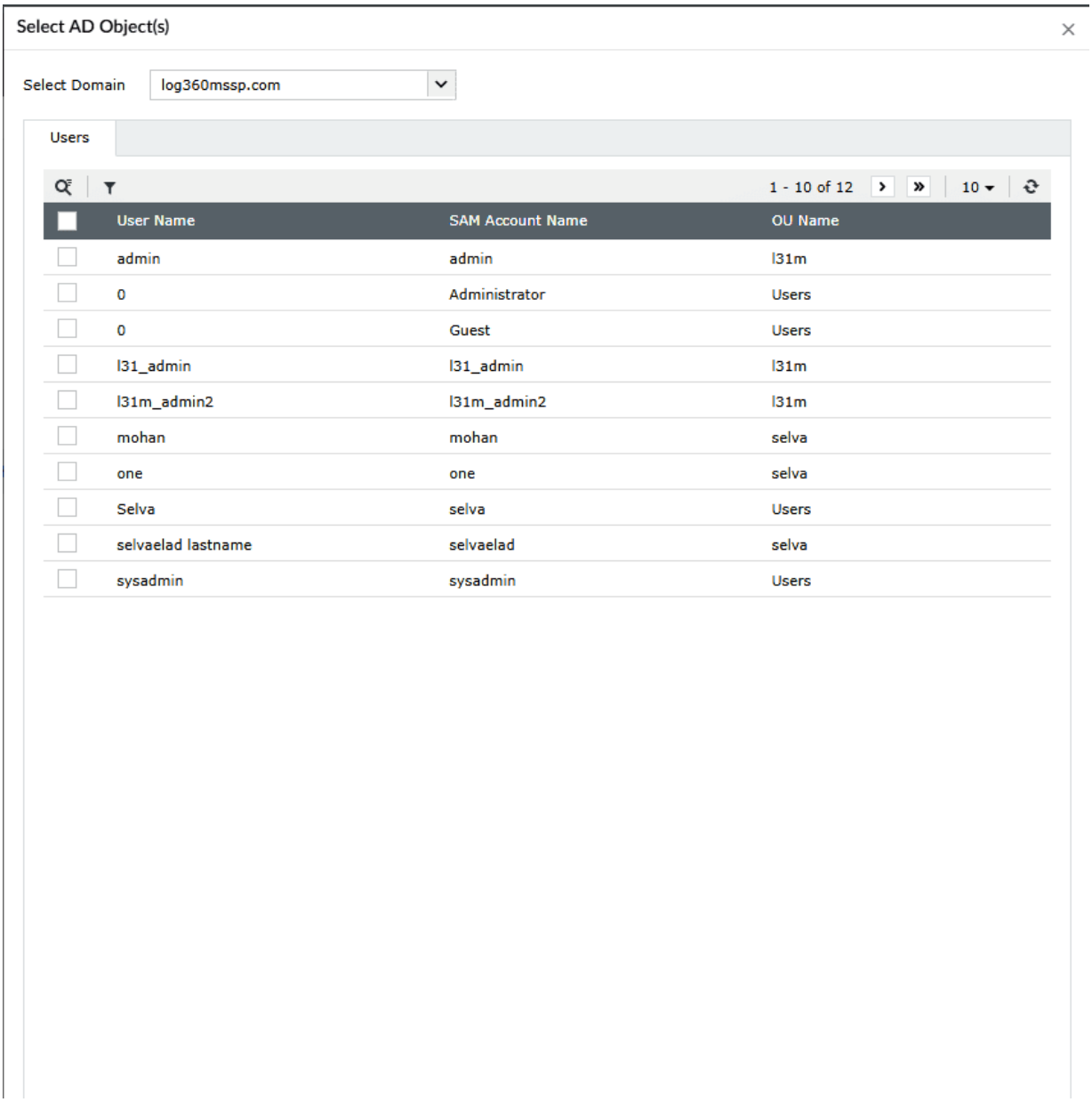


Image 6: Adding a technician



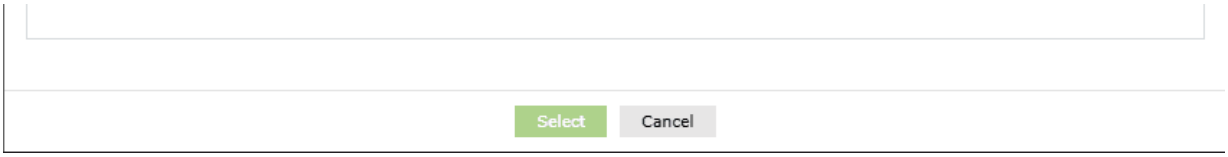


Image 7: Adding a technician

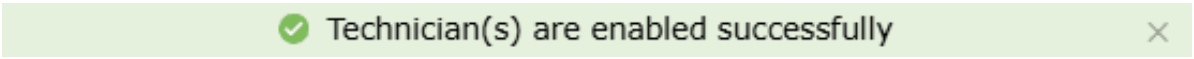
1. Choose Authentication type as "AD Authentication"
2. Click the "+" icon in AD Objects field. MSSP will automatically discover and display Active Directory users from the selected domain.
3. Select one or more users from list displayed and Click "Select".
4. Role: In the drop-down box, choose the role(s) you want to assign to the technician- Admin, Operator, Guest. You can assign more than one role to the technician, and the permissions of all the selected roles will be assigned to the technician.
5. Customers: Assign customer(s) to provide specific access only to that customers for that technician after clicking on the provided drop-down. Selecting All Customers will add provide access to any newly added customers for that technician.

Enable/disable an existing technician

To enable/disable a technician, follow the steps given below.
Navigate to the Technicians & Roles in the Management section under Admin Settings via the Settings tab.

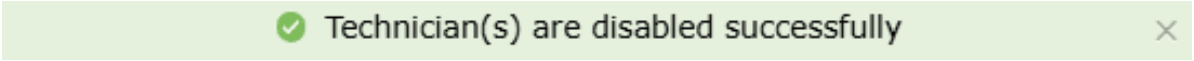
To Enable:

1. Click on the currently disabled icon ⊘ under the Actions column to enable the respective technician.
2. As soon as you perform this action, the icon indicates that the technician is now enabled ✓ and the below pop-up message appears briefly.



To Disable:

1. Click on the currently enabled icon ✓ under the Actions column to disable the respective technician.
2. As soon as you perform this action, the icon indicates that the technician is now disabled ⊘ and the below pop-up message appears briefly.



Edit an existing technician

To edit the information of an existing technician, follow the steps given below.

NOTE

A technician with the role of default admin user cannot be modified.

1. Navigate to the Technicians & Roles in the Management section under Admin Settings via the Settings tab, and click on the edit icon next to the name of the technician that you want to edit as shown below. The icon will appear when the cursor is hovered over the technician name.

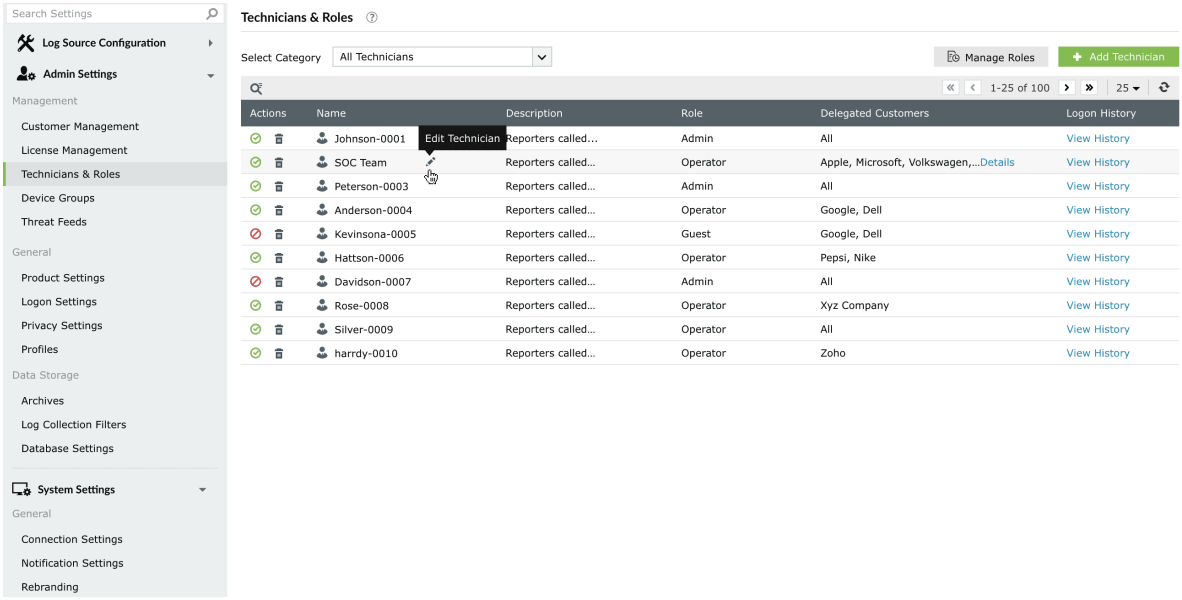


Image 8: Editing technicians in Log360 MSSP

2. Upon clicking on the edit icon, the Edit Technician page appears, similar to the Add Technician page.

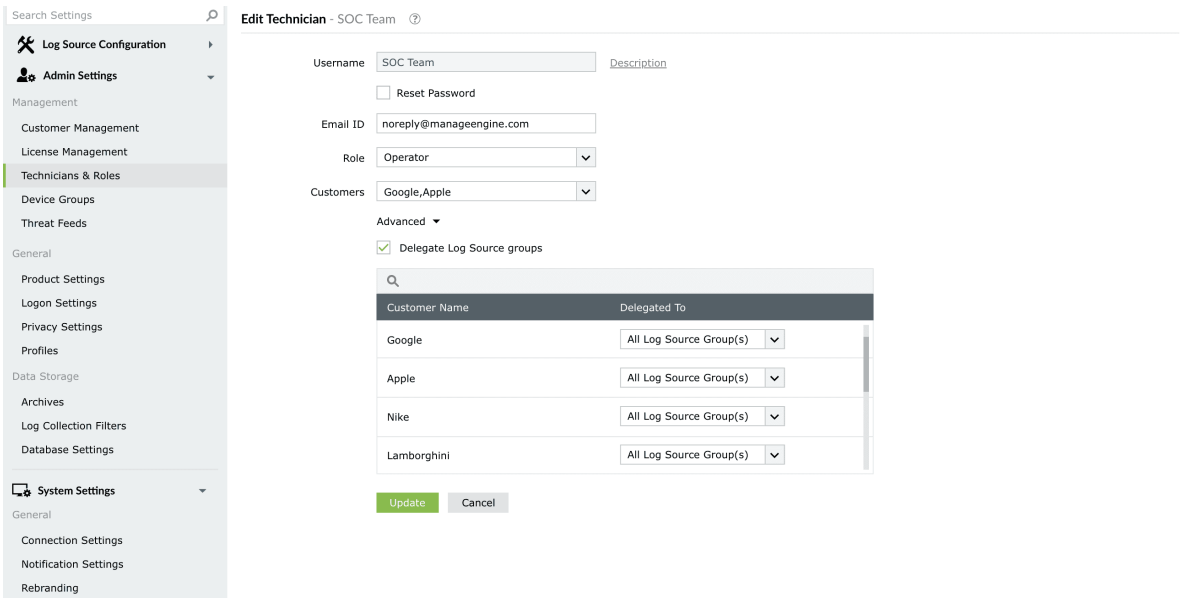
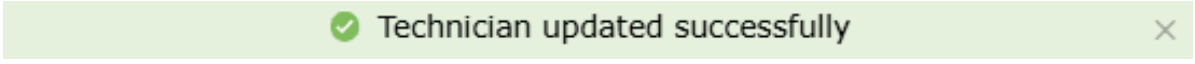


Image 9: Editing technicians in Log360 MSSP

3. Edit the fields as per your requirement and then click on the Update button.
4. Upon successful completion of the action, the below pop-up appears.



Delete an existing technician

To delete an existing technician, follow the steps given below.

1. Navigate to the Technicians & Roles in the Management section under Admin Settings via the Settings tab, and click on the delete icon in the Action column of the respective technician.

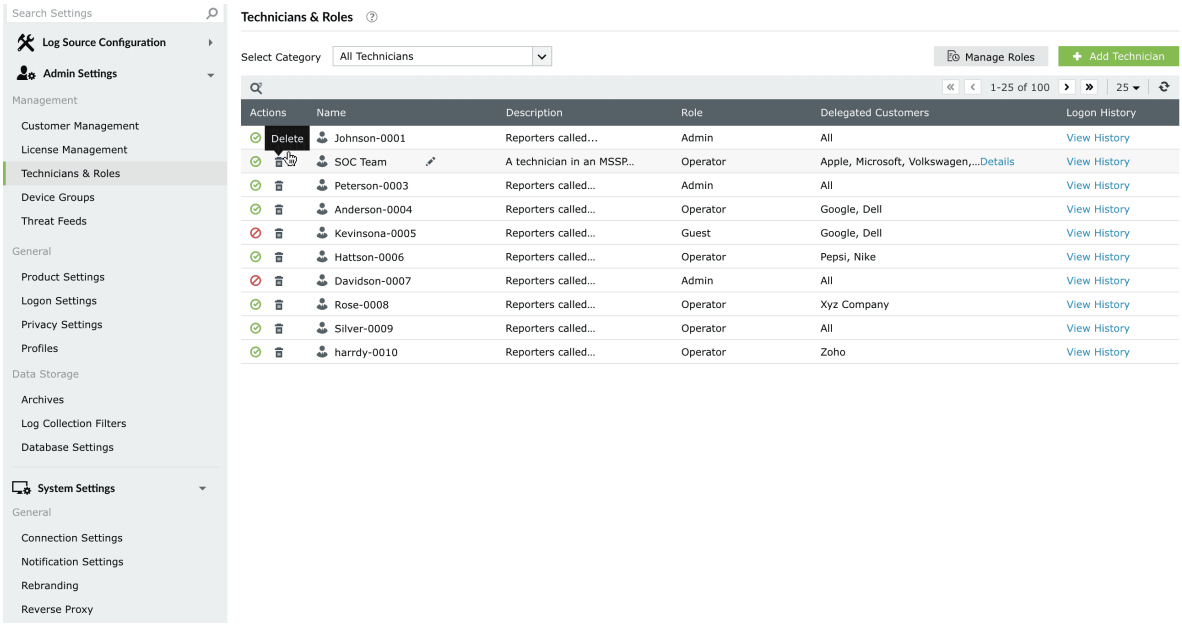


Image 10: Deleting technicians in Log360 MSSP

2. You can also delete a technician for an individual customer by opening the details drop-down in the Delegated Customers column of that specific technician.

> **NOTE**
>
> You cannot delete a technician for an individual customer if you have provided All Customers access for that technician.

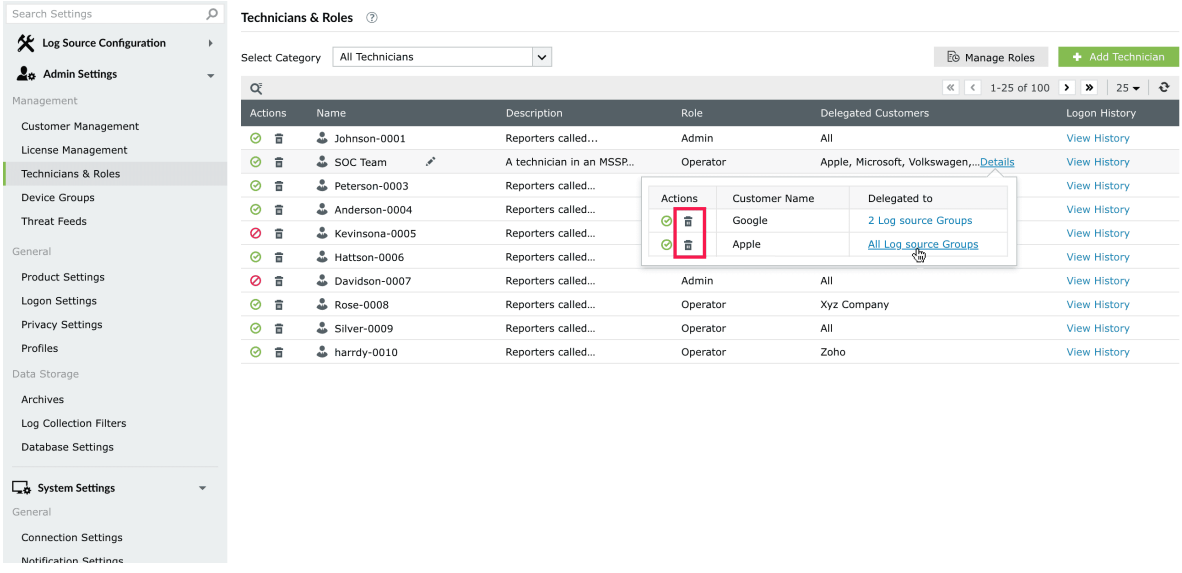
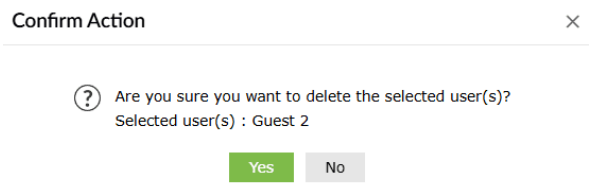


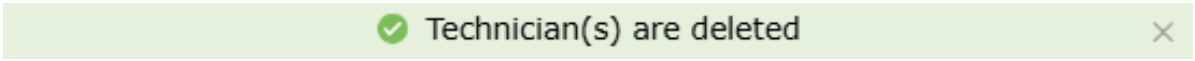


Image 11: Deleting technicians in Log360 MSSP

3. As soon as you click on delete, a Confirm Action pop-up box appears. Click on Yes.



4. Upon successful completion of the action, the below pop-up appears.



Read also

This document covered how to manage technician accounts in Log360 MSSP, including their roles, privileges, and customer-level access. For related multi-tenant administrative tasks, refer to:

- Auto-upgrade
- Log360 MSSP Overview
- Customer management

16.5. Reverse proxy in Log360 MSSP

Last updated on: September 12, 2025

In this page

Overview

Enable/disable reverse proxy

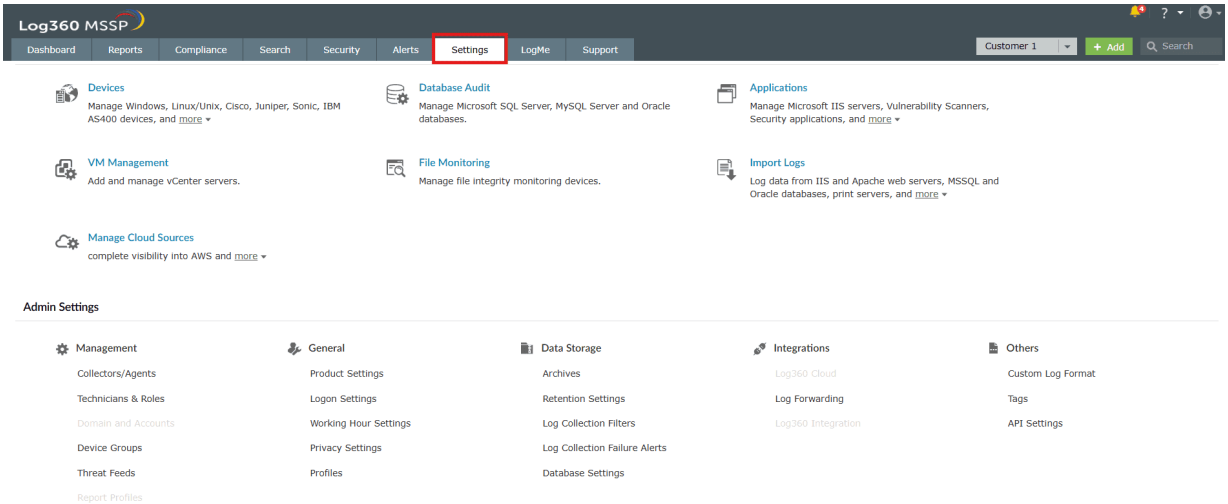
Overview

A reverse proxy is a proxy service that handles requests from customers, forwards them to the necessary servers, and subsequently delivers the servers' responses to the customers without revealing the identity of the servers. Log360 MSSP comes bundled with a reverse proxy server to prevent hackers from finding out, accessing, or exploiting the critical data that it holds.
Whenever a user requests access, the URL is forwarded to the respective servers based on the customers' context path in the URL. The end user will not know the details of the servers from which they are accessing the resources.

> NOTE
>
> 1. Log360 MSSP supports only context-based reverse proxy.
> 2. The hostname of the Log360 MSSP server will serve as the hostname for the customers' servers when reverse proxy is enabled.

Enable/disable reverse proxy

Log into the Log360 MSSP console as an administrator. Navigate to the Settings tab, scroll down, and click on Reverse Proxy listed in General under System Settings.



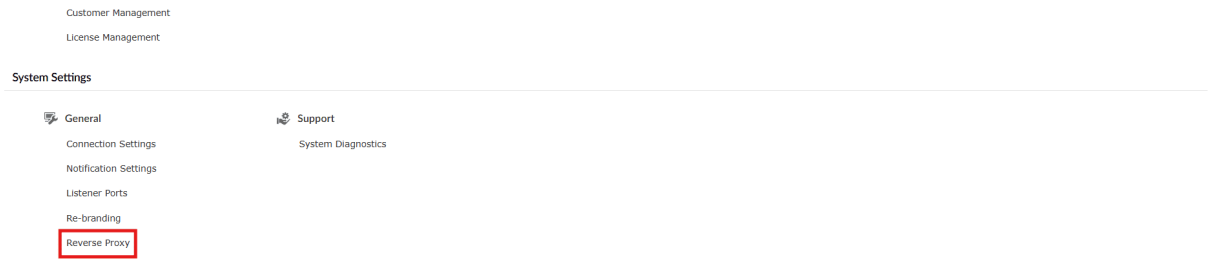


Image 1: Customer management via the Settings tab in Log360 MSSP

To enable reverse proxy:

1. Enable Reverse Proxy by ticking the currently empty checkbox, which is highlighted below.

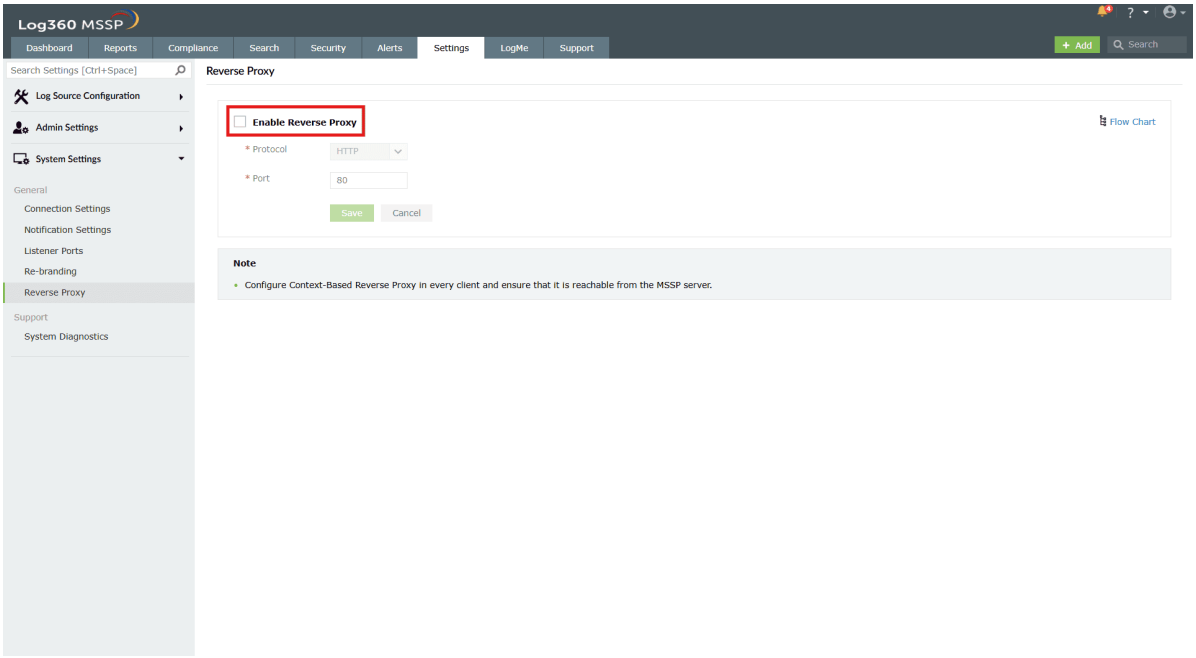
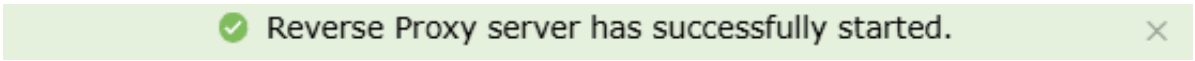


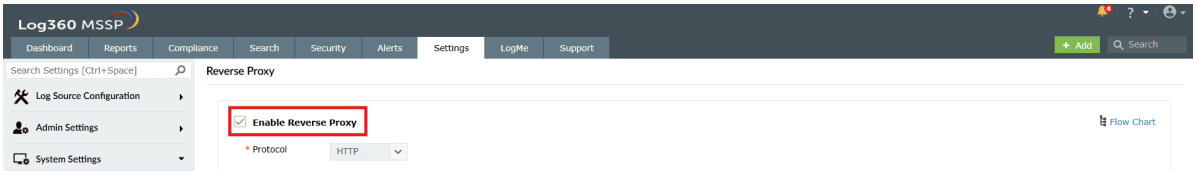
Image 2: Enabling reverse proxy in Log360 MSSP

2. Upon ticking the checkbox, the Port fields become available for editing. Select the required port number. Make sure the port number is not used by other applications.
3. Click on the Save button.
4. Upon successful completion of the action, the below pop-up appears.



To disable reverse proxy:

1. Disable reverse proxy by ticking the currently filled checkbox, which is highlighted below.



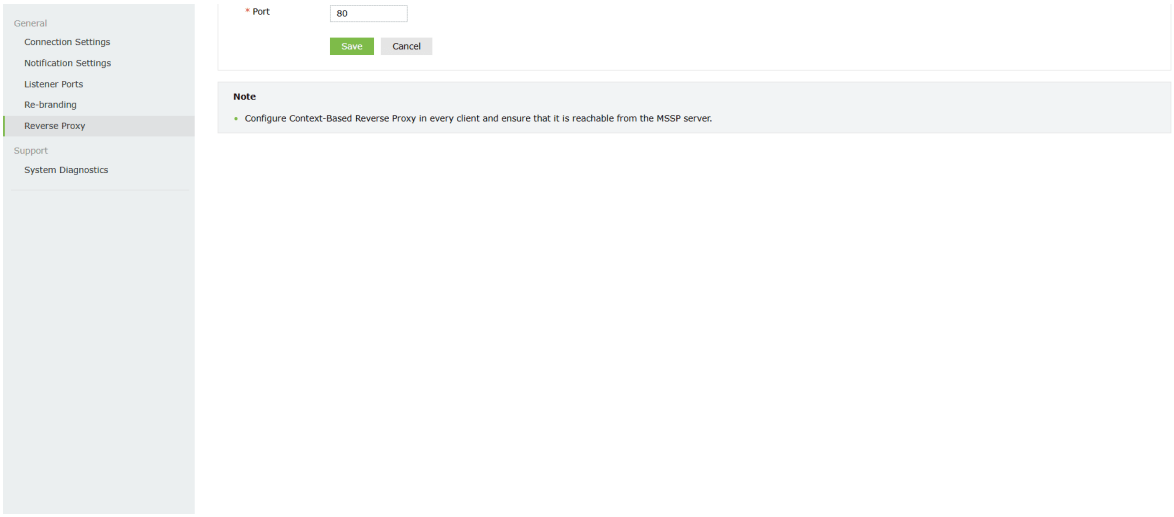


Image 3: Disabling reverse proxy in Log360 MSSP

2. Upon unchecking the checkbox, the Port fields instantly become unavailable for editing, indicating that the reverse proxy has been disabled successfully.

Read also

This document covered how to configure and manage reverse proxy in Log360 MSSP. For more security and integration-related capabilities, refer to:

- Log360 MSSP Overview
- Customer management
- License management
- Technician management

16.6. Auto-upgrade in Log360 MSSP

Last updated on: September 12, 2025

In this page

Overview

Auto-upgrade configuration

MSSP edition upgrade best practices

Overview

The auto-upgrade capability in Log360 MSSP Edition enables seamless version management by automatically applying service packs across all integrated customer servers once the MSSP server is upgraded. This eliminates the need for manual upgrades on individual customer instances. Administrators only need to apply the service pack on the MSSP server, and the rest is taken care of automatically—provided the feature remains enabled under Customer Management settings.

Auto-upgrade configuration

When auto-upgrade is enabled, the MSSP server will automatically distribute service packs to upgrade all Log360 customer servers after completing its own upgrade. This helps to automatically update the customers build to the MSSP build version by applying the service pack only once.
To upgrade the MSSP setup of Log360, carry out the steps given below.

1. Apply the service pack only to the MSSP server.
   Instructions to apply service packs
   Important note
   - Please stop the existing Log360 service and take a copy of the entire Log360 folder or a server snapshot. Please note that backing up Log360 is mandatory so that you can restore the installation to this version in case of upgrade failures. If you are using the MSSP Edition of Log360, back up the MSSP server and all customer servers.
   - Before you proceed with the upgrade process, please ensure the availability of enough disk space on the server where Log360 is installed.
   - If you use a MS SQL database, we strongly recommend you take a snapshot of your database as well.
   - If you've deployed the MSSP Edition of Log360, please apply the service pack only on the MSSP server. The admin server will auto-upgrade all the reporting customer servers, and the managed servers will automatically update the agents if they are in use.
   - In case you apply more than one service pack at a time, please start the Log360 application after each service pack upgrade.

   For Standalone and MSSP Editions of Log360, please update using the following steps.
   Windows

- Stop the Log360 service.
- Open the Command Promptt with administrative privileges.
- Navigate to the <Log360 Home>\bin folder.
- Type these three commands to ensure the proper shutdown of the application: shutdown.bat, stopDB.bat, and stopSEC.bat.

> NOTE
>
> StopDB.bat is only meant for the default database (PostgreSQL). If you use MS SQL, please ignore this command. Kindly execute shutdown.bat and stopSEC.bat.

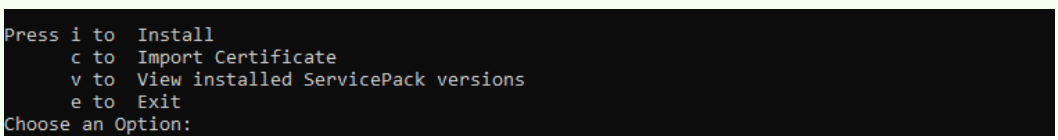
- Execute UpdateManager.bat.
- Click on Browse and select the appropriate PPM file.
- Click on Install. Please wait for it to complete.
- Start the application and check the build number.

Linux

- Take a backup of the server.
- Log360 can be stopped by executing the below command.
  - service log360 stop

    OR
  - systemctl log360 stop
- Followed by executing shutdown.sh, stopDB.sh, stopSEC.sh (To ensure that the product is completely stopped) from the installation directory, i.e. /ManageEngine/Log360/bin folder
- Once the product is stopped, execute sudo UpdateManager.sh (For Linux with GUI) or sudo UpdateManager.sh -c (For CLI-based Linux).
- Now choose i to initiate the PPM installation and specify the path [Eg: /home/ubuntu/**.ppm] in which the PPM files are downloaded
- Once the upgrade is successful, start Log360 using the below command,
  - service log360 start OR
  - systemctl log360 start

To open UpdateManager in console mode
Windows: UpdateManager.bat -c
Linux: ./UpdateManager.sh -c



- To Import Certificate, type c and press enter.
  Now enter the path of the certificate to be imported.

```
In the absence of a Valid certificate for the Patch Installation, it can be
downloaded from
https://www.manageengine.com/certificate/ppmsigner_publickey.crt.

Enter the certificate file to import : D:\Downloads\License\ppmsigner_publickey.crt
The selected certificate already exists in keystore.
```

- To install a PPM file, type i and press enter.
  Now enter the path of the PPM file to be installed and press enter.

```
Press i to  Install
      c to  Import Certificate
      v to  View installed ServicePack versions
      e to  Exit
Choose an Option:i

Enter the patch file to install:D:\Downloads\ManageEngine_EventLog_Analyzer_12_3_0_SP-12_4_0.ppm
```

- To view installed service pack version, type v and press enter.

```
Press i to  Install
      c to  Import Certificate
      v to  View installed ServicePack versions
      e to  Exit
Choose an Option:v

No ServicePack is installed

Do you want to continue ?

Yes(y) No(n)
```

- To exit the console mode, type e and press enter.
- Select the shared certificate by using the Browse button to locate the file.
- Next, select Import to pull in the certificate and proceed with steps mentioned above.

How to import certificate?
Please follow the below steps to import certificate. Download the certificate from one of these links below
Certificate link: https://www.manageengine.com/certificate/ppmsigner_publickey.crt
Updated Certificate link: https://updates.manageengine.com/certificates/latest.crt
For the files ppmsigner_publickey.crt and latest.crt, the SHA256 value is
2baeaee89ad91824b3ceca55499eebeb7a5c02d4b751bddfa2c2149ea2102155
Console mode:

- Run the UpdateManager.bat/sh file with -c as a command line argument.
- After invoking UpdateManager in command line mode, select option c from the list of options provided to import the certificate

Import the certificate.

- Enter the path of the certificate when requested and proceed with the steps mentioned above.

UI mode:

- Execute UpdateManager.bat/sh
- Open the import certificate tool by clicking the Import Certificate button on the top-left corner.
- Select the shared certificate by using the Browse button to locate the file.
- Next, select Import to pull in the certificate and proceed with the steps mentioned above.

Do not interrupt or revert the upgrade process. In case of upgrade failure, please contact Log360 MSSP support team.

The MSSP server will auto-upgrade the reporting customer servers, and the customer servers will automatically update the agents in use.

2. Navigate to the Settings tab in the header pane and click on the Customer Management option.

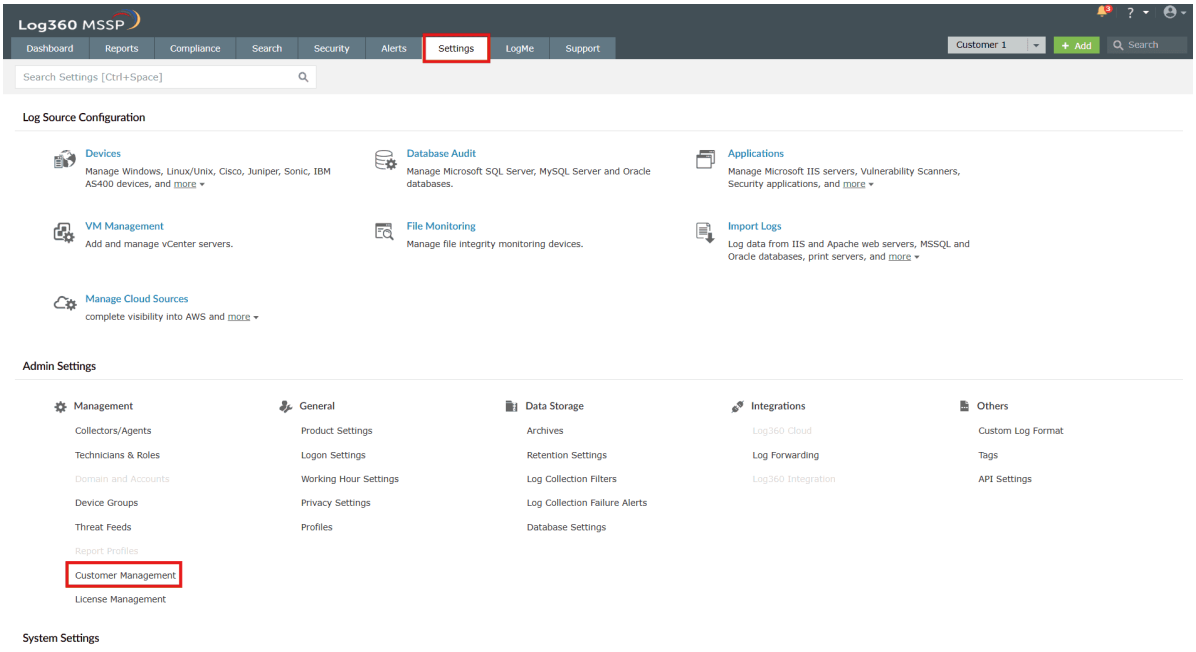
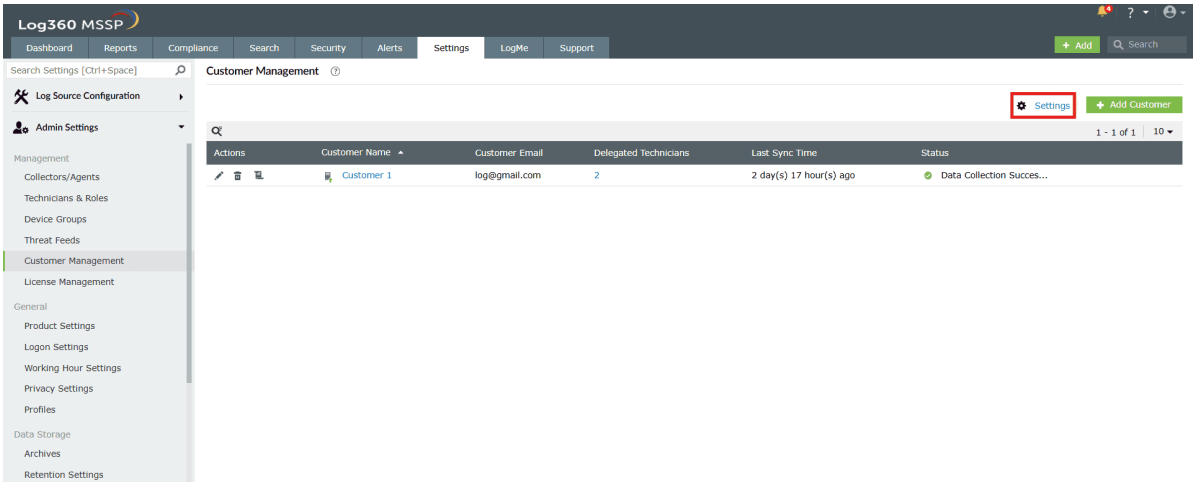


Image 1: Customer management via the Settings tab in Log360 MSSP

3. Click on the Settings link in the Customer Management page.



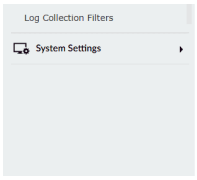


Image 2: Customer management settings in Log360 MSSP

> NOTE
>
> The Auto-Upgrade toggle will be enabled by default. Disabling the toggle will disable auto-upgrade of all customer servers by the MSSP server.

4. Click on the toggle and turn it off in case you wish to disable auto-upgrade. When disabled, Log360 servers must be upgraded individually using the Upgrade Now option in the Status column on the Customer Management module.

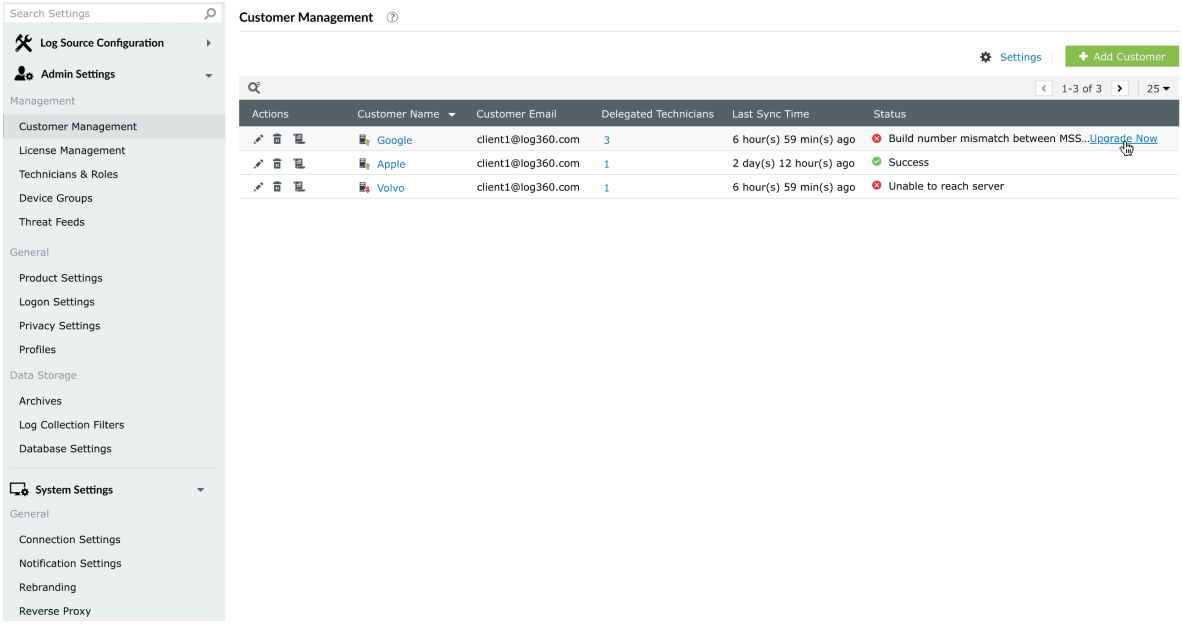


Image 3: Upgrade customer servers in Log360 MSSP

MSSP edition upgrade best practices

This guide explains how you can upgrade the Log360 MSSP Edition. In order to access the latest features and enhancements, users are required to upgrade to the latest version.

Prerequisites

- During the upgrade within the same storage drive of Log360, a backup is executed. Hence, it is important to ensure that there is sufficient space available for backup.
- The customer servers should be synchronized and integrated with the MSSP server, facilitating a proper connectivity between them. This ensures a seamless auto upgrade without any issues.

- Before upgrading, you need to backup both the customer servers and MSSP servers. This is essential in the event of an upgrade failure, ensuring a swift recovery.

Below are the steps for upgrading:

Phase 1: Taking a manual backup of MSSP Server

1. Shutdown the Log360 MSSP server.
2. Copy the following folders/files as backup.
   <Home>/Conf
   <Home>/adsdata
   <Home>/lib/AdventNetLicense.xml
3. Database backup: Take a snapshot of the database for having a database backup.Please follow the same steps as for Standalone server .

Phase 2: Taking a manual backup of Customer Server

1. Shutdown the Log360 customer server(s).
2. Copy the following folders/files as backup
   <Home>/Conf
   <Home>/adsdata
   <Home>/lib/AdventNetLicense.xml
3. Database backup: Take a snapshot of the database for having a database backup. Please follow the same steps as for Standalone server.

Phase 3: Performing the upgrade on the MSSP Server:

Apply the latest service pack in the PPM on the MSSP Server. Please check the instructions to apply service pack.

Phase 4: Upgrading Customer Servers:

Upon completion of the MSSP Server upgrade, the subsequent step involves upgrading the customer servers. There are two ways to achieve this:
Case-1: Auto upgrading all customer servers through the MSSP Server.
Case-2: Manually upgrading customer servers.

Case-1: Auto upgrading all customer servers through the MSSP Server

When the MSSP server is upgraded through a service pack, all its customer servers will be automatically upgraded by default.
Below are the steps for auto upgrading the customer servers:

1. Shutdown the MSSP server and all the customer servers.
2. Take either a snapshot or ensure a folder backup of all the servers.
3. Apply the service pack in the MSSP server.
4. Start the MSSP server.
5. After ensuring that the MSSP server is up and running, start all the customer servers one by one.

6. Wait for the MSSP server to upgrade all the customer servers before applying the next PPM (the service pack) on the MSSP server.

Case-2: Manually upgrading customer servers

In this case, the customer servers will be upgraded individually. During this process, a space check is conducted on the customer servers before applying the service pack.This is to ensure that there is enough storage space to accommodate the backup files of the existing system.
In the event of a backup failure, due to insufficient storage or other reasons, users can choose to skip the backup provided they have manually taken the backup of the customer servers as mentioned in Phase 2.
Below are the steps to manually upgrade each customer server

1. Shutdown the MSSP server and all the customer servers.
2. Take either a snapshot or ensure a folder backup of all the servers.
3. Add DisablePPMCheck=true in enterprise.txt of all the customer servers.
4. Upgrade the customer server one by one using updatemanager.bat
5. After upgrading all the customer servers, apply PPM on the MSSP server.
6. Start the MSSP server.

After ensuring that MSSP server is up and running, start all the customer servers one by one.
Read also
This document explained how customer upgrades and backups are handled in the Log360 MSSP Edition, including the steps to apply service packs, perform pre-upgrade backups, and ensure successful version synchronization across customer servers.

- Overview
- Customer management
- License management
- Technician management

17.1. EventLog Analyzer - Troubleshooting Tips

Last updated on: September 12, 2025

General

Where do I find the log files to send to EventLog Analyzer Support?

For Build 8010 onwards

The log files are located in the <EventLogAnalyzer_Home>logs directory. Typically when you run into a problem, you will be asked to send the serverout.txt file from this directory to EventLog Analyzer Support.

For Build 8000 or earlier

The log files are located in the <EventLogAnalyzer_Home>server/default/log directory. Typically when you run into a problem, you will be asked to send the serverout.txt file from this directory to EventLog Analyzer Support.

I find that EventLog Analyzer keeps crashing or all of a sudden stops collecting logs. What could be the reason?

The inbuilt PostgreSQL/MySQL database of EventLog Analyzer could get corrupted if other processes are accessing these directories at the same time. So exclude ManageEngine installation folder from

- Anti-virus scans
- Automatic backup softwares
- Snapshots in case of VMware installation

Ensure that no snap shots are taken if the product is running on a VM.

How to create SIF (Support Information File) and send it to ManageEngine when you are not able to perform the same from the Web client?

The SIF will help us to analyze the issue you have come across and propose a solution for the same.

If you are unable to create a SIF from the Web client UI,

For Build 8010 onwards

You can zip the files under 'logs' folder, located in C:/ManageEngine/Eventlog/logs (default path) and upload the zip file to the following ftp link: http://bonitas.zohocorp.com/upload/index.jsp?to=eventloganalyzer-support@manageengine.com

For Build 8000 or earlier

You can zip the files under 'log' folder, located in C:/ManageEngineEventlog/server/default/log (default path) and upload the zip file to the following ftp link: http://bonitas.zohocorp.com/upload/index.jsp?to=eventloganalyzer-support@manageengine.com

How to register dll when message files for event sources are unavailable?

To register dll, follow the procedure given in the link below: http://ss64.com/nt/regsvr32.html

How to register/unregister bundled postgres as a service?

Why register/unregister bundled postgres as a service?

Depending on your environment, you may occasionally experience challenges with starting EventLog Analyzer due to a Postgres database startup failure. To avoid this, it is advisable that you register the database first, making it run in the background irrespective of the product's start up or shutdown.

How to register/unregister bundled postgres as a service?

To register bundled postgres as a service:

For Build 12440 onwards

- Execute the following command in the Elevated Command Prompt Window within "<EventLog Analyzer Home>bin" directory.
  register_pgdbservice.bat "<Specify the name of the DB Service to be registered>"
- Stop the EventLog Analyzer service/server and start it after the registered DB service is started.

For Build 12440 or earlier

- Copy register_pgdbservice.bat from "<EventLog Analyzer Home\tools\postgres\bin" and paste it in "<EventLog Analyzer Home\bin" directory
- Execute the following command in the Elevated Command Prompt Window within <EventLog Analyzer Home>bin directory.
  register_pgdbservice.bat "<Specify the name of the DB Service to be registered>"
- Stop the EventLog Analyzer service/server and start it after the registered DB service is started.

Should you no longer wish to be in charge of the database, you may opt to unregister, which will cause the product to start and stop the database, along with its own start and stop.

To unregister the bundled postgres service:

For Build 12440 onwards

- Execute the following command in the Elevated Command Prompt Window within the <EventLog Analyzer Home>bin directory.
  unregister_pgdbservice.bat "<Specify the name of the DB Service to be unregistered>"

For Build 12440 or earlier

- Copy unregister_pgdbservice.bat from "<EventLog Analyzer Home\tools\postgres\bin" and paste it in "<EventLog Analyzer Home\bin"
- Execute the following command in the Elevated Command Prompt Window within the <EventLog

Analyzer Home>bin directory.

unregister_pgdbservice.bat "<Specify the name of the DB Service to be unregistered>"

Installation

EventLog Analyzer displays "Enter a proper ManageEngine license file" during installation

This can happen under two instances:

- Case 1: Your system date is set to a future or past date. In this case, uninstall EventLog Analyzer, reset the system date to the current date and time, and re-install EventLog Analyzer.
- Case 2: You may have provided an incorrect or corrupted license file. Verify that you have applied the license file obtained from ZOHO Corp. If neither is the reason, or you are still getting this error, contact licensing@manageengine.com

Binding EventLog Analyzer server (IP binding) to a specific interface.

For Build 8010 onwards

To bind EventLog Analyzer server to a specific interface, follow the procedure given below:

For Eventlog Analyzer running as application:

- Shutdown EventLog Analyzer
- Open the run.bat file which is under <EventLog Analyzer Home>bin directory and go to "RESTART Command block", uncomment the below RESTART command line and replace <ip-address> with the IP address to which you want to bind the application, comment the existing RESTART command line and save the file.

  to

  to
- Open setcommonenv.bat file which is under <EventLog Analyzer Home>bin directory and go to "JAVA_OPTS Setting command Block", uncomment the below JAVA_OPTS setting command line and replace <ip-address> with the IP address to which you want to bind the application and comment the existing JAVA_OPTS setting command.

  to

  to
- Save the file
- Open the database_param.conf file which is under <EventLog Analyzer Home>conf directory and replace localdevice in url tag with the <binding IP address> to which you want to bind the application and save the file.
- Open the postgresql.conf file which is under <EventLog Analyzer Home>pgsqldata directory and uncomment the line '#listen_addresses = 'localdevice" in the CONNECTIONS AND AUTHENTICATION section and replace the 'localdevice' with the '<binding IP address>' to which you

want to bind the application and save the file.

- Open the pg_hba.conf file which is under <EventLog Analyzer Home>pgsqldata directory and add the line device all all <binding IP address in IPv4 format>/32 trust

  after the line

  device all all 127.0.0.1/32 trust

  and save the file.

  # TYPE DATABASE USER ADDRESS METHOD

  # IPv4 local connections:

  device all all 127.0.0.1/32 trust

  # IPv6 local connections:

  device all all ::1/128 trust

  to

  # TYPE DATABASE USER ADDRESS METHOD

  # IPv4 local connections:

  device all all 127.0.0.1/32 trust

  device all all <binding IP address in IPv4 format>/32 trust

  # IPv6 local connections:

  device all all ::1/128 trust

- Restart EventLog Analyzer

  For Eventlog Analyzer running as service:

  Before proceeding further, stop the EventLog Analyzer service and make sure that 'SysEvtCol.exe','Postgres.exe' and 'java.exe' are not running.

  There are 7 files that must be modified for IP binding.

  Note: data-doc-rid="255l9469213c93f3f4d8cb899c7bf8471fb58">Before editing the files ensure that you have a backup copy of the files.

  Assume xxx.xxx.xxx.xxx is the IP address you wish to bind with EventLog Analyzer.

  File 1)

  <ELA home>\bin\setCommonEnv.bat

- Search for line set JAVA_OPTS=-Djava.library.path=..\lib;..\lib\native -Duser.country=US -Duser.language=en -Xms256m -Xmx1024m
- Append -Dspecific.bind.address= xxx.xxx.xxx.xxxto the line. It will now look as: set JAVA_OPTS=-Djava.library.path=..\lib;..\lib\native -Duser.country=US -Duser.language=en -Xms256m -Xmx1024m -Dspecific.bind.address= xxx.xxx.xxx.xxx

  File 2)

  <ELA home>\bin\runSEC.bat

- Search for line "%SERVER_HOME%\bin\SysEvtCol.exe" -port 513 %syslogPort% -dbhome "%dbhome%" -ELAhome "%serverHome%" -loglevel 2 %RelayIP% %IPadd% %IgnoreHost% %IPadd% %*
- Add -bindip xxx.xxx.xxx.xxx to the line, so that it looks like "%SERVER_HOME%\bin\SysEvtCol.exe" -bindip xxx.xxx.xxx.xxx -port 513 %syslogPort% -dbhome "%dbhome%" -ELAhome "%serverHome%" -loglevel 2 %RelayIP% %IPadd% %IgnoreHost% %IPadd% %*

File 3)

<ELA home>\server\conf\wrapper.conf

- Search for line #wrapper.app.parameter.1=com.adventnet.mfw.Starter
- Remove the # from the line, it should now look like wrapper.app.parameter.1=com.adventnet.mfw.Starter
- The next line from current position should be #wrapper.app.parameter.2=-L../lib/AdventNetDeploymentSystem.jar . Add the following two lines after this line, one after the other.
- wrapper.app.parameter.2=-b xxx.xxx.xxx.xxx
- wrapper.app.parameter.3=-Dspecific.bind.address= xxx.xxx.xxx.xxx
- The block should now look like this :-

wrapper.app.parameter.1=com.adventnet.mfw.Starter

#wrapper.app.parameter.2=-L../lib/AdventNetDeploymentSystem.jar

wrapper.app.parameter.2=-b xxx.xxx.xxx.xxx

wrapper.app.parameter.3=-Dspecific.bind.address= xxx.xxx.xxx.xxx

File 4)

<ELA home>\conf\server.xml

Search for the following block:

<Connector SSLEnabled="false" URIEncoding="UTF-8" acceptCount="100" address="0.0.0.0" clientAuth="false" compressableMimeType="text/html,text/xml" compression="force" compressionMinSize="1024" connectionTimeout="20000" disableUploadTimeout="true" enableLookups="false" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" name="WebServer" noCompressionUserAgents="gozilla, traviata" port="8095" protocol="HTTP/1.1" scheme="http" secure="false"/>

- Replace address="0.0.0.0" with address="xxx.xxx.xxx.xxx"
- It should now look like the following

<Connector SSLEnabled="false" URIEncoding="UTF-8" acceptCount="100" address="xxx.xxx.xxx.xxx" clientAuth="false" compressableMimeType="text/html,text/xml" compression="force" compressionMinSize="1024" connectionTimeout="20000" disableUploadTimeout="true" enableLookups="false" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" name="WebServer" noCompressionUserAgents="gozilla, traviata" port="8095" protocol="HTTP/1.1" scheme="http" secure="false"/>

File 5)

<ELA home>\conf\database_params.conf

- Search for the line url=jdbc:postgresql://127.0.0.1:33335/eventlog?stringtype=unspecified

- Replace the 127.0.0.1 with your xxx.xxx.xxx.xxx, the line should now look like url=jdbc:postgresql://xxx.xxx.xxx.xxx:33335/eventlog?stringtype=unspecified

File 6)

<ELA home>\pgsql\data\postgresql.conf

- Search for the line #listen_addresses = 'localhost'
- Remove the # from the line.
- Replace the 'localhost' with 'xxx.xxx.xxx.xxx', the line should now look like listen_addresses = 'xxx.xxx.xxx.xxx'

File 7)

<ELA home>\pgsql\data\pg_hba.conf

Search for the following block

IPv4 local connections:

host all all 127.0.0.1/32 trust

We need to replicate the host all all 127.0.0.1/32 trust line with the new IP address in place of 127.0.0.1 and add it after that line. For replication, please copy this line itself and paste it in next line and then edit out the IP address.

It should look like this

IPv4 local connections:

host all all 127.0.0.1/32 trust

host all all xxx.xxx.xxx.xxx/32 trust

Start EventLog Analyzer and check <ELA home>\logs\wrapper.log for the current status.

EventLog Analyzer displays "java.lang.Error: Probable fatal error: No fonts found"

ELA employs the Dejavu-seriff font, which is preinstalled on Windows OS, when exporting reports. However, this font is not preinstalled for some Linux distributions. An error occurs in these cases.

In such cases, install the font manually based on the distribution. The command required is listed below:

- Case 1 : RHEL/CentOS
- Case 2 : Ubuntu/Debian
- Case 3 : SLES

Startup and Shut Down

MySQL-related errors on Windows machines

Probable cause: An instance of MySQL is already running on this machine.

Solution: Shut down all instances of MySQL and then start the EventLog Analyzer server.

Probable cause: Port 33335 is not free

Solution: Kill the other application running on port 33335. If you cannot free this port, then change the MySQL port used in EventLog Analyzer.

EventLog Analyzer displays "Port 8095 needed by EventLog Analyzer is being used by another application. Please free the port and restart EventLog Analyzer" when trying to start the server

Probable cause: The default web server port used by EventLog Analyzer is not free.

Solution: Kill the other application running on port 8095. Carry out the following steps.

- Stop the EventLog Analyzer service
- Open wrapper.conf which is available under <EventLog Analyzer Home>server/conf folder.
- Append the below line under # Java Additional Parameters section,
  wrapper.java.additional.21=-Djava.net.preferIPv4Stack=true

  Before adding:

  wrapper.java.additional.20=-Dorg.tanukisoftware.wrapper.WrapperManager.mbean=false

  After adding:

  wrapper.java.additional.20=-Dorg.tanukisoftware.wrapper.WrapperManager.mbean=false
  wrapper.java.additional.21=-Djava.net.preferIPv4Stack=true

- Start EventLog Analyzer service
  If you cannot free this port, then change the web server port used in EventLog Analyzer.

EventLog Analyzer displays "Can't Bind to Port <Port Number>" when logging into the UI.

Probable cause:The syslog listener port of EventLog Analyzer is not free. Solution:

- Check for the process that is occupying the syslog listener port, using netstat -anp -pudp . And if possible, try to free up this port.
- If you have started the server in UNIX machines, please ensure that you start the server as a root user.
- or, configure EventLog Analyzer to listen to a different syslog listener port and ensure that all your configured devices send their syslog to the newly configured syslog listener port of EventLog Analyzer

Start up and shut down batch files not working on Distributed Edition when taking backup.

Probable cause: Path names given incorrectly.

Solution:

- Download the "Automated.zip" and extract the files "startELAservice.bat"and "stopELAservice.bat" to <ELA home>//bin/ folder.
- Create a Windows schedule as per your requirement and ensure that the path should be <ELA Home>//bin folder.

- If you would like to have the files to a different folder, you need to edit the downloaded files and give the absolute path as below: < eg. is the application is installed on e:\ >
- e:\ManageEngine\EventLog\bin\wrapper.exe -p ..\server\conf\wrapper.conf ---> to stop the EventLog Analyzer service.
- e:\ManageEngine\EventLog\bin\wrapper.exe -t ..\server\conf\wrapper.conf ---> to start the EventLog Analyzer service.

Note:The script will work only if the application is started as a service.

EventLog Analyzer displays "Couldn't start elasticsearch at port 9300".

Probable cause: requiretty is not disabled

Solution: To disable requiretty, please replace requiretty with !requiretty in the etc/sudoers file.

Note:Elasticsearch uses multiple thread pools for different types of operations. It is important for new threads to be created whenever necessary. Please make sure that the number of threads that an elasticsearch user can create is at least 4096 by setting ulimit -u 4096 as root before starting Elasticsearch or by adding elasticsearch - nproc 4096 in /etc/security/limits.conf.

Service pack

How to upgrade your service pack if failure is due to lack of permission?

Navigate to <PRODUCT_HOME>\bin and invoke StartDB.bat as administrator. If you see access denied error, Execute setAppPermission.bat and wait for its completion.

Note: EventLog Analyzer directory permissions will be modified on executing the setAppPermission.bat as mentioned in this document here.

Troubleshooting PPM backup and failure cases

Note: Backup will be done only for the instances with PGSQL or MSSQL database. PPM backup feature is not available for MySQL database.

- If the database size exceeds 10GB, the auto-backup won't work and the user will be notified to backup manually before proceeding with the upgrade.
- For PGSQL database, backup will be done only if there is enough free space available in the EventLog Analyzer installed drive. Incase of MSSQL database, the backed up data will be stored in the default backup folder configured for MSSQL. The availability of free space will be checked before backup operation and if enough space is not available, the user will be notified. Users can either clear-up enough space for auto-backup or they can proceed to back up manually.
- For PGSQL database, only two PPM backups will be maintained and older backups will be deleted upon rotation.
- For MSSQL database, backups won't be deleted automatically. Users will have to manually clear them.
- Incase of upgrade failure, the backups can be used to restore the last known working state of the instance.

Please contact support for the restoration process.

Configuration

While adding device for monitoring, the 'Verify Login' action throws RPC server unavailable error

The probable reason and the remedial action is: Probable cause: The device machine RPC (Remote Procedure Call) port is blocked by any other Firewall. Solution: Unblock the RPC ports in the Firewall.

While adding device for monitoring, the 'Verify Login' action throws 'Access Denied' error.

The probable reasons and the remedial actions are:

Probable cause: The device machine is not reachable from EventLog Analyzer machine.

Solution: Check the network connectivity between device machine and EventLog Analyzer machine, by using PING command.

Probable cause: The device machine running a System Firewall and REMOTEADMIN service is disabled.

Solution: Check whether System Firewall is running in the device. If System Firewall is running, execute the following command in the command prompt window of the device machine:
netsh firewall set service type=REMOTEADMIN mode=ENABLE profile=all

When WBEM test is carried out. it fails and shows error message with code 80041010 in Windows Server 2003.

The probable reasons and the remedial actions are:

Probable cause: By default, WMI component is not installed in Windows 2003 Server

Solution: Win32_Product class is not installed by default on Windows Server 2003. To add the class, follow the procedure given below:

- In Add or Remove Programs, click Add/Remove Windows Components.
- In the Windows Components Wizard, select Management and Monitoring Tools, then click Details.
- In the Management and Monitoring Tools dialog box, select WMI Windows Installer Provider and then click OK.
- Click Next.

How to enable Object Access logging in Linux OS?

The probable reasons and the remedial actions are:

Probable cause: The object access log is not enabled in Linux OS

Probable cause: The object access log is not enabled in Linux OS.

Solution: Steps to enable object access in Linux OS, is given below:

In the file /etc/xinted.d/wu-ftpd, edit the server arguments as mentioned below:

server_args = -i -o -L

What are commands to start and stop Syslog Deamon in Solaris 10?

The probable reasons and the remedial actions are:

Probable cause: Unable to start or stop Syslog Daemon in Solaris 10

Solution: In Solaris 10, the commands to stop and start the syslogd daemon are:

svcadm disable svc:/system/system-log:default

svcadm enable svc:/system/system-log:default

In Solaris 10, to restart the syslogd daemon and force it to reread /etc/syslog.conf:

svcadm refresh svc:/system/system-log:default

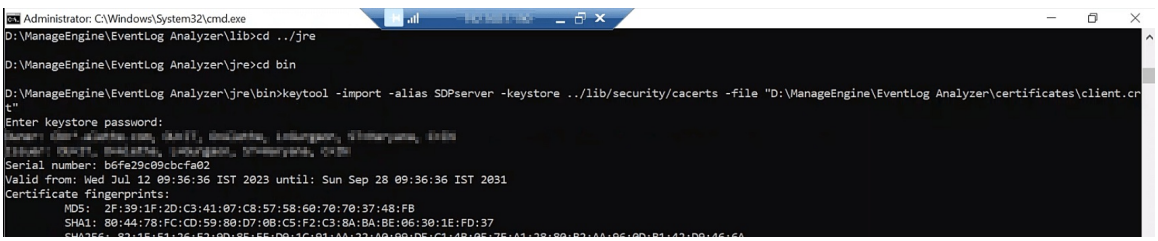
(or)
svcadm -v restart svc:/system/system-log:default

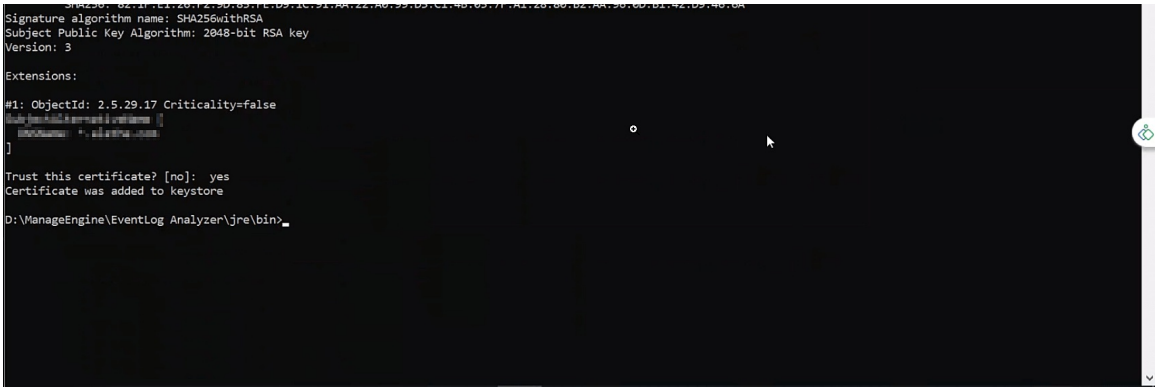
While configuring incident management, I am facing SSL Connection error.

This error can occur if the ticketing tool server's HTTPS certificate is not included in EventLog Analyzer's JRE certificate store. To import the certificate to EventLog Analyzer's JRE certificate store, follow the steps below:

- Place the server's certificate in your browser's certificate store by allowing trust when your browser throws up the error saying that the certificate is not trusted.
- Export the certificate as a binary DER file from your browser.
- For Firefox, you can do this by following the steps below:

- Click the lock symbol next to the URL and click More Information.
- Select the Security tab, click View certificate, and click the Details tab.
- Select the certificate and click Export. Select a location in your local machine and save the certificate.
- For IE, Internet Options > Content > Certificates > Personal > Export
- For Chrome, Settings > Show Advanced Settings > Manage Certificates
- Use the keytool utility to import the certificate into EventLog Analyzer's JRE certificate store. The command should be executed from <Eventlog Analyzer Home>/jre/bin.





- Enter the keystore password. Note that the default password is changeit.

While configuring EventLog Analyzer with JIRA On-Premise, the 'Test and Save' action throws Captcha Verification failed error.

If you are facing problems while configuring EventLog Analyzer with JIRA On-Premise even after entering the valid credentials, please follow the steps below:

- Go to the ticketing tool instance and try logging in to your account.
- Enter the valid credentials and complete the captcha verification.
- You can now try configuring EventLog Analyzer with JIRA On-Premise again. The Test and Save action will complete successfully without any errors.

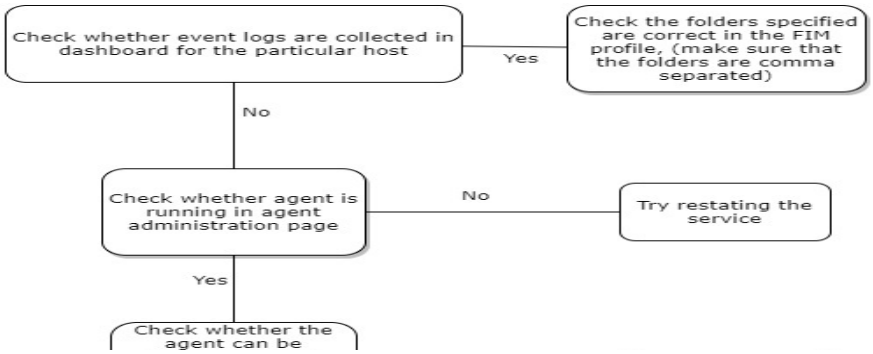
Help link: https://developer.atlassian.com/cloud/jira/software/basic-auth-for-rest-apis/#captcha

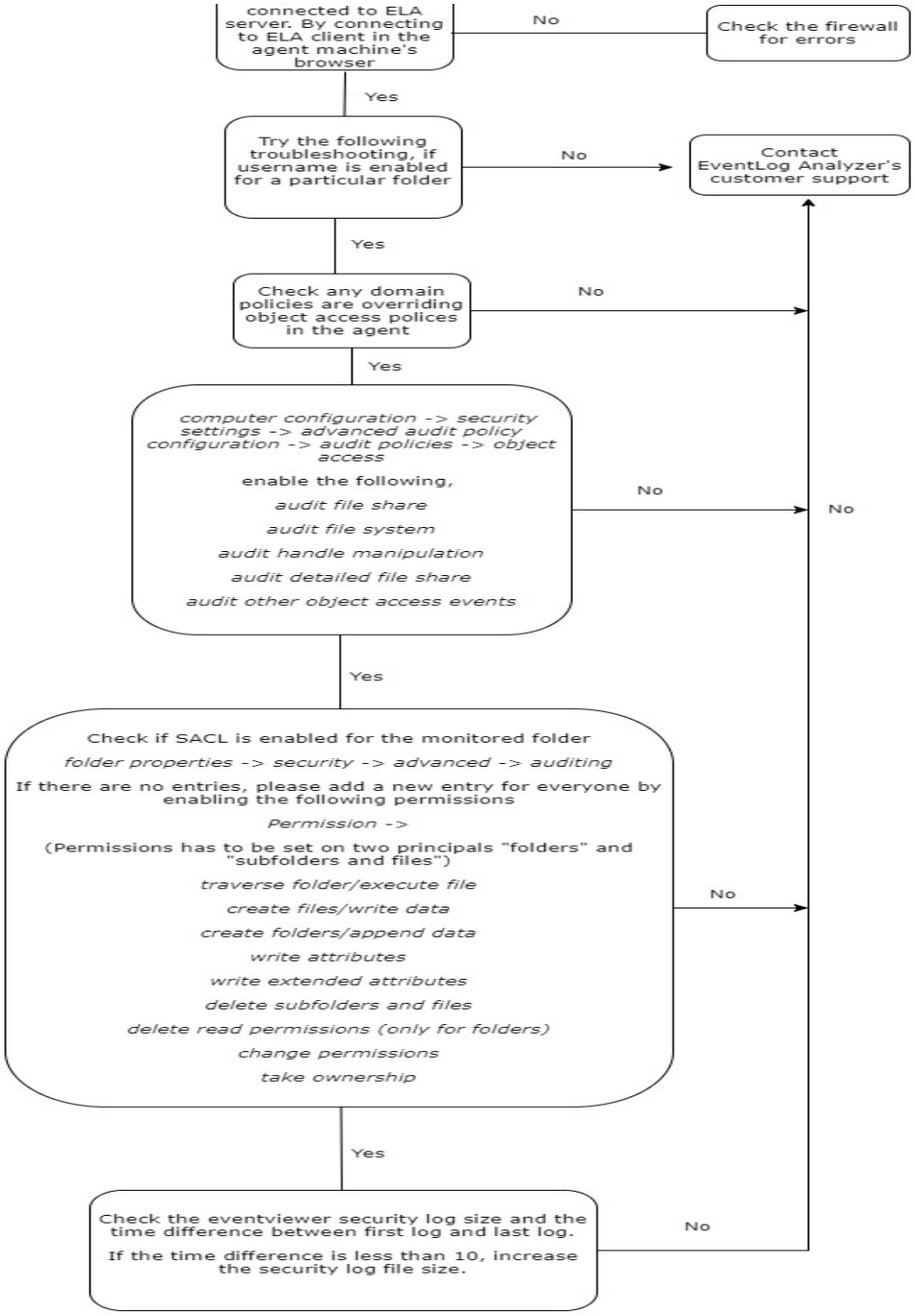
Steps to edit maximum attempts or disable captcha:

- Login to your JIRA On-Premise account.
- In the top right corner, select Administration and go to System > General Configuration > Edit Settings.
- Go to the Maximum Authentication Attempts Allowed field and enter the desired value. When you exceed this limit, you have to login to your JIRA On-Premise account with captcha verification again. Otherwise, you won't be able to configure EventLog Analyzer with JIRA On-Premise even with valid credentials.
- If you leave this field blank, captcha will be disabled. You can attempt to integrate EventLog Analyzer with JIRA On-Premise even after multiple authentication failures.

File Integrity Monitoring (FIM) troubleshooting

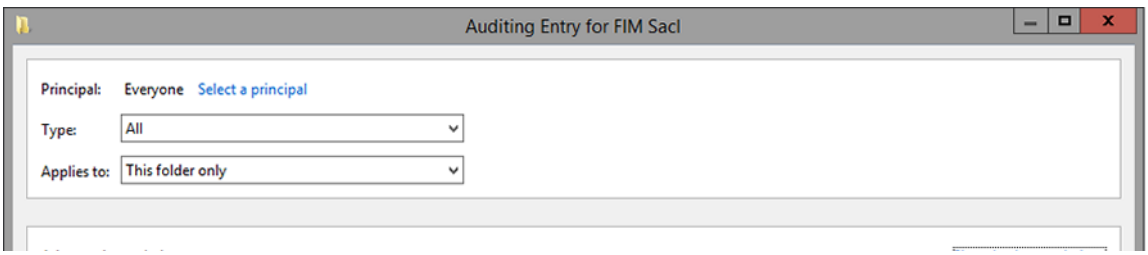
Try the following troubleshooting, if username is enabled for a particular folder.

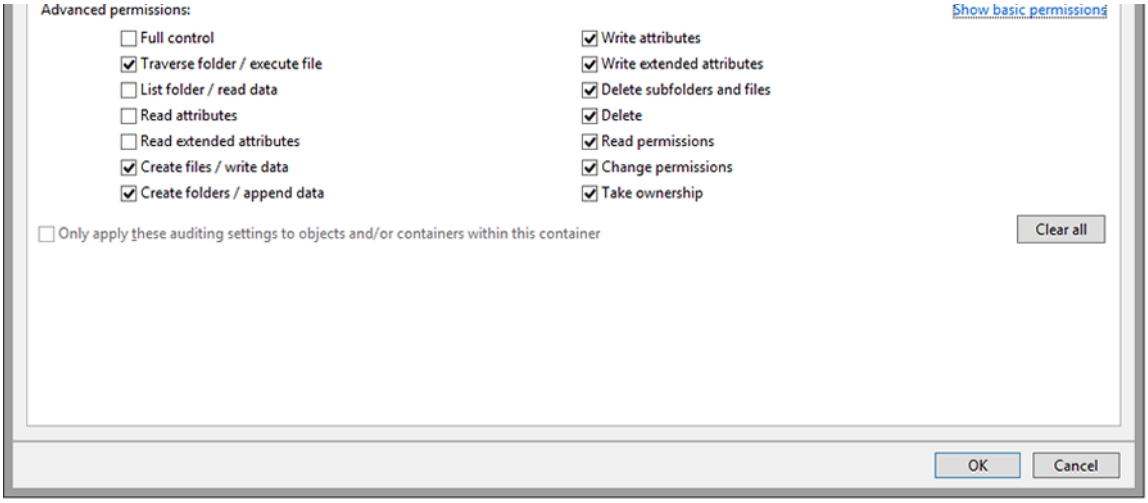




Note

The following GUI is for the SACL entry in folder properties.





Port management error codes

The following are some of the common errors, its causes and the possible solution to resolve the condition. Feel free to contact our support team for any information.

Port already used by some other application

Cause: Cannot use the specified port because it is already used by some other application.

Solution: This can be solved either by changing the port in the specified application or by using a new port.

If you use a new port, make sure to change the ports in the forwarding device either manually or using auto log forwarding configuration.

TLS not configured

Cause: HTTPS not configured to support TLS encrypted logs.

Solution: Configure the server to use either a self-signed certificate or a valid PFX certificate.

For more details visit Connection settings.

PFX not configured

Cause: HTTPS is configured, but the type of certificate is not supported.

Solution 1: If no valid certificate is used, it's recommended to use SelfSignedCertificate.

To find the type of certificate used,

- Open Conf/Server.xml file check for connector tag.
- Check the extention for the attribute keystoreFile.

Solution 2: If valid KeyStore certificate is used, execute the following command in the <EventLog Analyzer home>/jre/bin terminal.

keytool -importkeystore -srckeystore <certificate path> -destkeystore server.pfx -deststoretype PKCS12 -deststorepass <password> -srcalias tomcat -destalias tomcat

For more details visit Connection settings.

External error

Cause: Unknown external issue

Cause: Unknown external issue.

Solution: please contact EventLog Analyzer Technical Support

The event source file(s) configuration throws the "Unable to discover files" error.

Possible remedial actions include:

- Check the credentials of the machine.
- Check the connectivity of the device.
- Ensure that the remote registry service is not disabled.
- The user should have admin privileges.
- The open keys and keys with sub-keys cannot be deleted.

How to change PostgreSQL superuser password

Execute the changeDBPassword.bat/sh file located in <EventLog Analyzer Home>/bin.

Windows:

- changeDBPassword.bat -U postgres -p <old_password> -P <new_password>

Linux:

- changeDBPassword.sh -U postgres -p <old_password> -P <new_password>

Handling duplicated Windows devices

Problem statement:

Some Windows devices appear duplicated due to a user interface issue identified as ELA 12260.

Action taken:

Local collector association:

Duplicated devices with the oldest log collection timestamps will be deleted if they are linked to a local collector.

Remote collector association with shorter last message time:

Duplicated devices with the oldest log collection timestamps will be disabled if:

They are linked to a remote collector.

The difference between the current date and the last message time is less than the retention period.

Remote collector association with longer last message time:

Duplicated devices with the oldest log collection timestamps will be deleted if:

They are associated with a remote collector.

The difference between the current date and the last message time exceeds the retention period.

Profile remapping:

If any of the deleted or disabled devices were previously configured under the following profiles: Application, Import, Alert, Report, Log Collection Filter, Syslog Forwarder, Agent, they will be remapped to ensure continued functionality.

Action required by the customer:

Device reconfiguration:

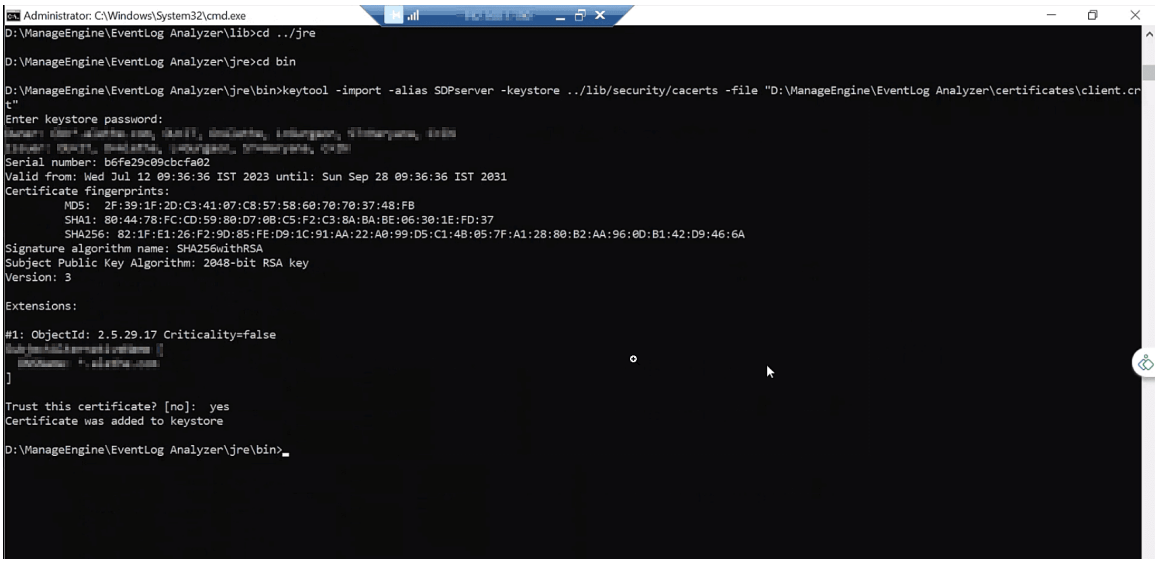
For configurations pertaining to device groups, log collection failure alerts, compliance and custom log parser, please reconfigure the respective device. The erroneous device may have been mistakenly configured due to the UI issue mentioned above.

When forwarding audit logs, sometimes default policies in Red Hat systems with Security enhancement (SElinux) won't allow the audit logs to be read.

- Issue: When SELinux (Security Enhancement) is enabled, some default policies prevent audit logs from Red Hat Linux systems from being read during the forwarding process.
- Solution: The audit logs can be forwarded by adding "active=yes" in etc/audisp/plugins.d/syslog.conf or create the file in etc/audit/plugins.d/syslog.conf for CentOS/RHEL v8 and later with the below entries:
  Note: This will forward the audit logs to the syslog service. Log Forwarding via Syslog Service should be enabled to receive the logs in EventLog Analyzer server.

How to add an organization-wide proxy certificate in EventLog Analyzer?

- Ensure that you have the proxy certificate file available before running the command.
- Use the keytool utility to import the proxy certificate into EventLog Analyzer's JRE certificate store. The command should be executed from <EventLog Analyzer Home>/jre/bin.





- Enter the keystore password. Note that the default password is changeit.

Error statuses in File Integrity Monitoring (FIM).

Permission denied

Causes

- Credentials may be incorrect.
- Credentials with insufficient privileges.
- There might be a temp folder available with insufficient privileges for the user.
- The user does not have privileges for agent folder.

Solutions

- Credentials can be checked by accessing the SSH terminal.
- Credentials with the privilege to start, stop, and restart the audit daemon, and also transfer files to the Linux device are necessary.
- Setting Privilege for temp if available.
- Setting Privileges for the agent folder. For CentOS/RHEL v8 and later/Ubuntu/openSUSE/Debian/Fedora: For CentOS/RHEL v6 to v7.9:

Audit service unavailable

Cause

- The audit daemon service is not present in the selected Linux device.

Solution

- The audit daemon package must be installed along with Audisp.

Access restriction from SELinux

Cause

- SELinux hinders the running of the audit process.

Solutions

- SELinux's presence could be checked using getenforce command.
- Configure SELinux in permissive mode. After changing it to the permissive mode, navigate to Manage Agent page and click on Reinstall to reinstall the agent.

Agent upgrade failure

Causes

- No connectivity with the agent during product upgrade.
- Incorrect credentials.

Solutions

- Manually install the agent by navigating to the Manage Agent page.
- To install agent:

  Windows device: Run the EventLogAgent.msi.

  Linux device: Execute chmod +x EventLogAgent.bin, then run EventLogAgent.bin.

Agent Installation Failed

Causes

- Machine may be in the offline mode.
- Machine may not exist.
- Network path may not be reachable.

Solutions

- To confirm if the device exists, it could be pinged.
- Manually install the agent by navigating to the Manage Agent page.

Agent Installation on Incompatible Platform

Causes

- The agent is installed on a host which has neither a Linux nor a Windows OS.

Solutions

- Supported Linux distributions are CentOS, Debian, Fedora, openSUSE, Red Hat, and Ubuntu.
- Windows versions greater than 5.2 (Windows Server 2003) are supported.

ACL Package is not installed

Cause:

The acl package is not present in the selected Linux device.

Solution:

The acl package must be installed.

Agent could not be connected using SSH

Causes:

- Due to the missing SSH Algorithm.
- Insufficient privileges for the "/opt/ManageEngine"

Insufficient privileges for the "/opt/ManageEngine"

Solutions:

- Ensure that any of the SSH Algorithms are present in the "/etc/ssh/sshd_config" file.
- Setting privilege for the " /opt/ManageEngine "

How to check if Immutable Rule is enabled in auditd?

Execute the following command to verify that the immutable rule is enabled:

If "enabled 2" is present in the configuration, it indicates that the immutable rule is active. This setting will prevent the Linux agent from applying any newly configured audit rules to monitor the locations specified in EventLog Analyzer.

Solution:

- Run the below command to locate the immutable rule (-e 2) and comment out or remove the configuration from the relevant file.
- Reboot the machine to apply the updated configuration.
- To confirm that the immutable rule is no longer active, run the below command and check that "enabled 1" is present in the configuration.

Log Receiver

What should I do if the network capture driver is not available?

Network capture drivers are files that allow EventLog Analyzer to capture and process incoming network logs from various sources. These include files such as npf.sys, Packet.dll, and wpcap.dll. These files must be stored in the Windows System Directories to ensure they are accessible to any application that requires them.

If the network capture driver is unavailable, you should move the files from the EventLog Analyzer installation directory to the Windows System Directories. To do so, follow the steps below.

Steps to move network capture driver files to Windows system directories

- Navigate to <EventLogAnalyzer_Installation_Directory>\bin directory.
- Open command prompt with admin privileges and execute register-driver.exe.
- Check the output in the console to ensure that the files are copied successfully.

In case of failure, proceed with the manual procedure, given below.

Steps to copy network capture driver files manually

- Copy the npf.sys, wpcap.dll and Packet.dll files from <EventLogAnalyzer_Installation_Directory>\lib\native folder.
- Paste the files in the following folders:
- npf.sys to C:\Windows\system32\drivers\
- wpcap.dll, Packet.dll to C:\Windows\system32\

Finally, open and refresh the Log Receiver window in EventLog Analyzer.

Note: These steps are applicable only if EventLog Analyzer is installed on Windows.

Auto Log Forwarding

Permission Denied

Causes:
Insufficient privileges for the rsyslog.conf or syslog.conf file.

Solutions:
Setting privilege for rsyslog.conf or syslog.conf file.

Log Collection and Reporting

I've added a device, but EventLog Analyzer is not collecting event logs from it

Probable cause: The device machine is not reachable from the EventLog Analyzer server machine
Solution: Check if the device machine responds to a ping command. If it does not, then the machine is not reachable. The device machine has to be reachable from the EventLog Analyzer server in order to collect event logs.
Probable cause: You do not have administrative rights on the device machine
Solution: Edit the device's details, and enter the Administrator login credentials of the device machine. Click Verify Login to see if the login was successful.

Error Code 0x251C

Probable cause: The device was added when importing application logs associated with it. In this case, only the specified application logs are collected from the device, and the device type is listed as unknown.

Solution:

- Click on the update icon next to the device name.
- Select the appropriate device type.
- Provide any other required information for the selected device type.
- Click on update.

I get an Access Denied error for a device when I click on "Verify Login" but I have given the correct login credentials

Probable cause: There may be other reasons for the Access Denied error.
Solution: Refer the Cause and Solution for the Error Code you got during Verify login.

Error Code 00x80070005, 5

Scanning of the Windows workstation failed due to one of the following reasons:

- The login name and password provided for scanning is invalid in the workstation. Solution: Check if the login name and password are entered correctly.
- Remote DCOM option is disabled in the remote workstation Solution:
  Check if Remote DCOM is enabled in the remote workstation. If not enabled, then enable the same in the following way:

- Select Start > Run.
- Type dcomcnfg in the text box and click OK.
- Select theDefault Propertiestab.
- Select theEnable Distributed COMin this machine checkbox.
- Click OK.

To enable DCOM on Windows XP devices:

Select Start > Run

- Type dcomcnfg in the text box and clickOK
- Click on Component Services > Computers > My Computer
- Right-click and selectProperties
- Select the Default Propertiestab
- Select theEnable Distributed COM in this machine checkbox
- ClickOK
- User account is invalid in the target machine.

Check if the user account is valid in the target machine by opening a command prompt and executing the following commands:

If these commands show any errors, the provided user account is not valid on the target machine.

Error Code 0x80041003

The user name provided for scanning does not have sufficient access privileges to perform the scanning operation. This user may not belong to the Administrator group for this device machine.

Solution: Move the user to the Administrator Group of the workstation or scan the machine using an administrator (preferably a Domain Administrator) account.

Error Code 0x800706ba

A firewall is configured on the remote computer. Such exceptions mostly occur in Windows XP (SP 2), when the default Windows firewall is enabled.

Solution:

- Disable the default Firewall in the Windows XP machine:
  SelectStart > Run

  Type Firewall.cpl and click OK

  In the General tab, click Off

  Click OK

- If the firewall cannot be disabled, launch Remote Administration for administrators on the remote machine by executing the following command:
  After scanning, you can disable Remote Administration using the following command:

  Error Code 0x80040154

- WMI is not available in the remote windows workstation. This happens in Windows NT. Such error codes might also occur in higher versions of Windows if the WMI Components are not registered properly.
  Solution: Install WMI core in the remote workstation.
- WMI Components are not registered.
  Solution: Register the WMI DLL files by executing the following command in the command prompt:
  winmgmt /RegServer

  Error Code 0x80080005
  There is some internal execution failure in the WMI service (winmgmt.exe) running in the device machine. The last update of the WMI Repository in that workstation could have failed.

  Solution:
  Restart the WMI Service in the remote workstation:

- Select Start > Run
- Type Services.msc and click OK
- In the Services window that opens, select Windows Management Instrumentation service.
- Right-click and select Restart
  Error Code 1722, 1726, 1753, 1825

  Probable cause: The device machine RPC (Remote Procedure Call) port is blocked by another firewall.
  Solution: Unblock the RPC ports in the firewall.

  For any other error codes, refer the MSDN knowledge base.

I have added an Custom alert profile and enabled it. But the alert is not generated in EventLog Analyzer even though the event has occurred in the device machine

Probable cause: The alert criteria have not been defined properly

Solution: Please ensure that the required fields in the Add Alert Profile screen have been given properly.Check if the e-mail address provided is correct. Ensure that the Mail server has been configured correctly.

When I create a Custom Report, I am not getting the report with the configured message in the Message Filter

Probable cause: The message filters have not been defined properly
Solution:When you are entering the string in the Message Filters for matching with the log message, ensure you copy/enter the exact string as shown in the Windows Event Viewer.
e.g., Logon Name:John

MS SQL server for EventLog Analyzer stopped

Probable cause: The transaction logs of MS SQL could be full
Solution: If the EventLog Analyzer MS SQL database transaction logs are full, shrink the same with the procedure given below:

- Stop the Eventlog Analyzer Server/Service (Check the Eventlog Analyzer server machine's Task Manager to ensure that the processes 'SysEvtCol.exe', 'Java.exe' are not running).
- Connect MS SQL client (using Microsoft SQL Server Management Studio) and execute the below query:
  sp_dboption 'eventlog', 'trunc. log on chkpt.', 'true'
  To execute the query, select and highlight the above command and press F5 key.
- After executing the above command, select and highlight the below command and press F5 key to execute it.
  DBCC SHRINKDATABASE (eventlog)
- Note: This process will take some time, based on the EventLog Analyzer database size.
- Start the Eventlog Analyzer.

I successfully configured Oracle device(s), still cannot view the data

If Oracle device is Windows, open Event viewer in that machine and check for Oracle source logs under Application type. If Linux, check the appropriate log file to which you are writing Oracle logs. If the Oracle logs are available in the specified file, still EventLog Analyzer is not collecting the logs, contact EventLog Analyzer Support.

The user name provided for scanning does not have sufficient access privileges to perform the scanning operation. Probably, this user does not belong to the Administrator group for this device machine

The Syslog host is not added automatically to EventLog Analyzer/the Syslog reception has suddenly stopped

Check EventLog Analyzer's live Syslog Viewer for incoming Syslog packets.

If you are able to view the logs, it means that the packets are reaching the machine, but not to EventLog Analyzer. You need to check your Windows firewall or Linux IP tables.

If you are not able to view the logs in the Syslog viewer, then check if the EventLog Analyzer server is reachable. This can be done in the following ways:

- Ping the server.
- For TCP, you can try the command telnet <ela_server_name> <port_no> where 514 is the default TCP port.
- tcpdump
  If reachable, it means there was some issue with the configuration. If not reachable, then you are facing a network issue.

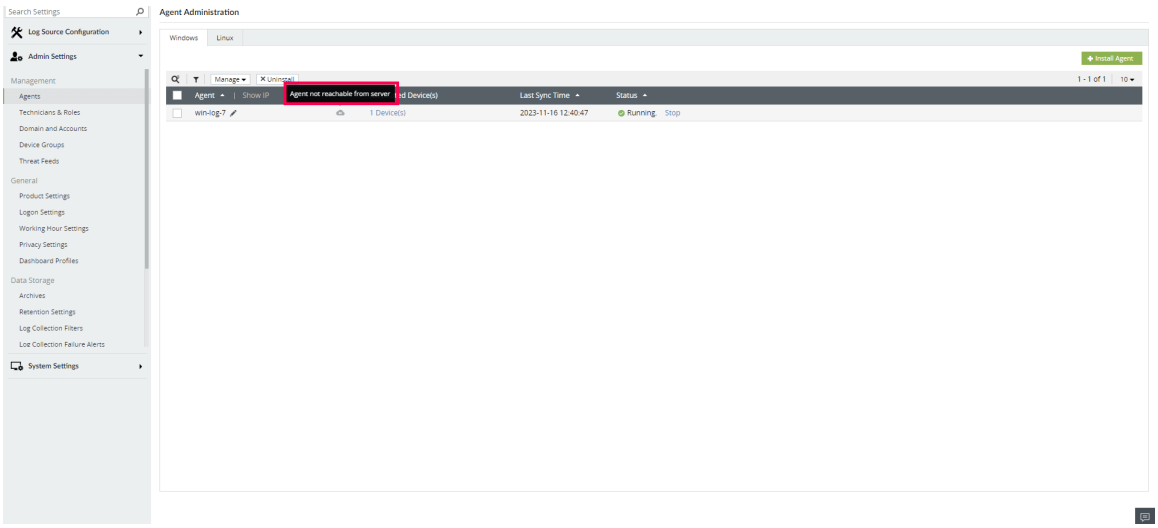
EventLog Analyzer agent management

If you have trouble installing the agent using the EventLog Analyzer console, GPOs or software installation tools, you can try to install the agent manually. Here the the steps for manual agent installation

you can try to install the agent manually. Here are the steps for manual agent installation.

Agents are not reachable from the EventLog Analyzer server

If an agent is installed manually without credentials or if the agent credentials are updated incorrectly, it leads to the "Agent not reachable from server" status (see screenshot below).



In such a state, the following actions performed on the agent will not reflect immediately.

- Force restart agent
- Stopping agent
- Updating device IP and credentials
- Adding, deleting, enabling or disabling Device/LogCollection Filter/FIM
- Updating FIM template
- Updating monitoring interval

> **Note**
>
> This icon does not hinder the log collection process, logs will be collected regardless of the presence of this icon.

Furthermore, actions such as starting and uninstalling the agent must be manually executed, as they cannot be performed through the UI due to invalid credentials.

If the cloud icon, indicating that the agent is unreachable from the server, is to be hidden or if real-time actions are required, please make sure to update the credentials accurately.

Agent not communicating is displayed as the agent status

"Agent not communicating" is the agent status that appears if there has been a prolonged time of no communication between the agent and the server.

In such a state, the following actions should be performed:

- Ensure the EventLog Analyzer server is accessible from the agent device.
- Verify if the latest server details are updated in the registry [Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ZOHO Corp\EventLogAnalyzer\ServerInfo]
- Check if any antivirus or firewall is blocking the communication between the server and agent. If so, provide an exclusion for EventLog Analyzer agent from AntiVirus.
- Ensure the EventLog Analyzer Agent service is running, and start it if necessary.

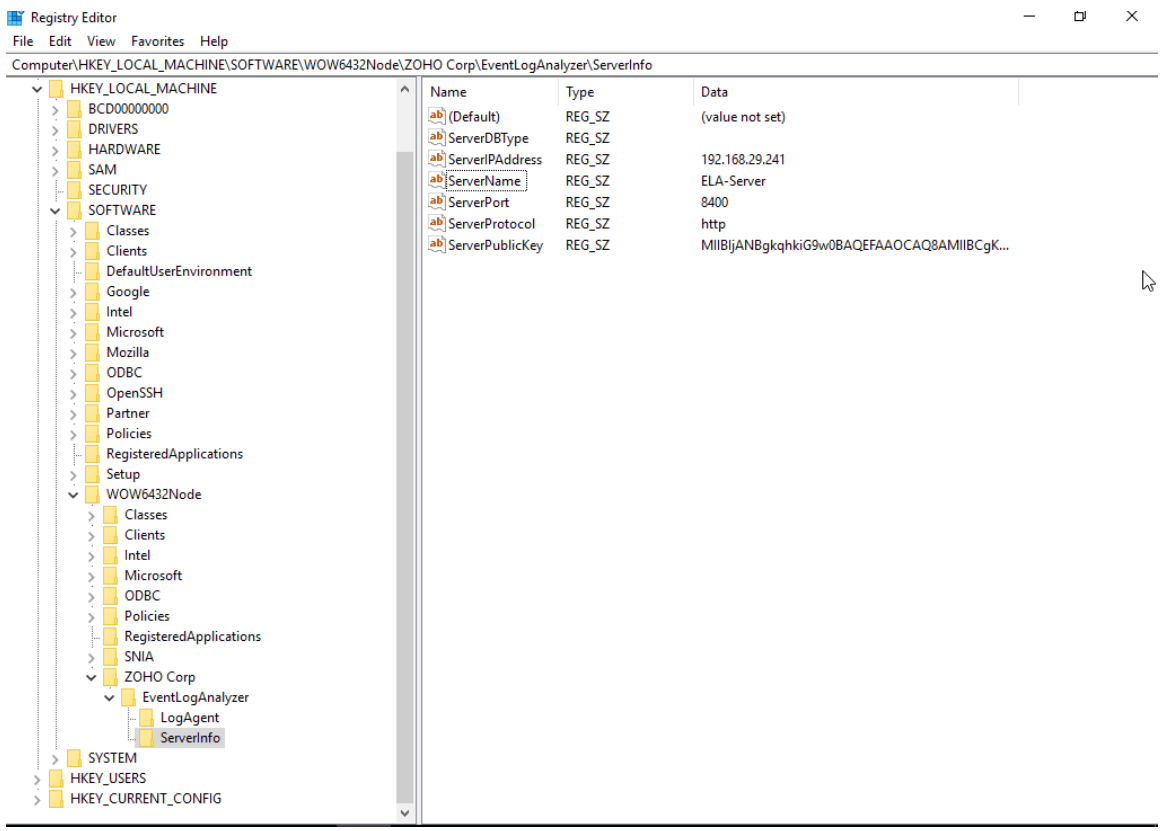
> **Note**
>
> Contact support if the issue persists even after following the above steps.

How to update ServerInfo in an EventLog Analyzer agent after server migration?

Steps to update ServerInfo in an EventLog Analyzer agent after server migration

Windows Agent

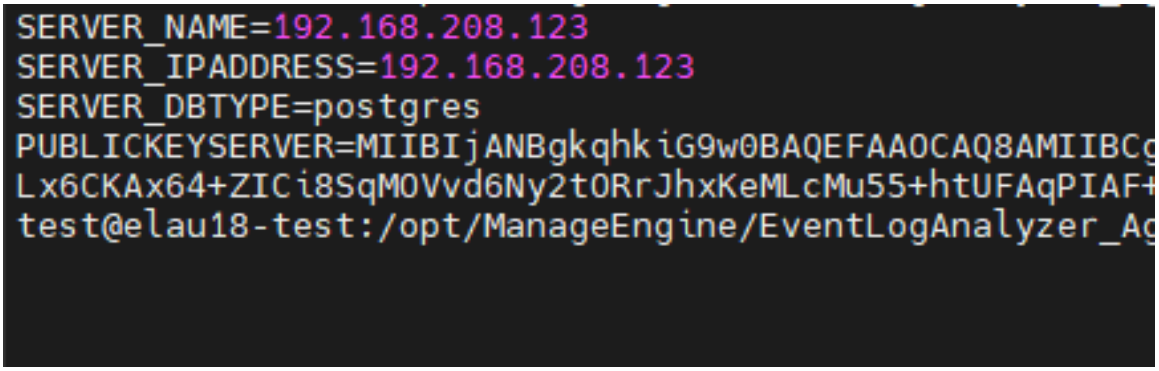
- Open Registry Editor and navigate to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ZOHO Corp\EventLogAnalyzer\



- Select ServerInfo and enter the new SeverIPAddress and ServerName in the corresponding fields.
- Finally, restart the EventLog Analyzer agent to establish connection with the new server.

Linux Agent

- Open the /opt/ManageEngine/EventLogAnalyzer_Agent/conf/serverDetails file.
- Update the new SERVER_NAME and SERVER_IPADDRESS in the corresponding fields.



- Finally, restart the EventLog Analyzer agent to establish connection with the new server.

Performance

For troubleshooting, please follow the steps below:

- Check if other applications are blocking the CPU cycle for EventLog Analyzer.
- If a virtual machine is used, check for over provisioning or if snapshots are affecting the performance.
- If the log flow rate is high, please check our tuning guide.

Error messages while adding STIX/TAXII servers to EventLog Analyzer

While I was trying to add a STIX/TAXII server to EventLog Analyzer, I got the following error messages. What do they mean?

This feature has been disabled for Online Demo!

This error message pops up when the feature you tried to use is not available in the online demo version of EventLog Analyzer. To try out that feature, download the free version of EventLog Analyzer.

Connection failed. Please try configuring proxy server.

This error message can be caused because of different reasons. It might be due to network issues, proxy related issues, bad requests in the network, or if the URL is unable to locate a STIX/TAXII server.

Failed to connect to the URL.

This error message denotes that the URL entered is malformed.

Authorization failed.

This error message signifies that the credentials entered are wrong.

SSL Troubleshooting steps

Certificate name mismatch

Description:

This error occurs when the common name of the SSL Certificate doesn't exactly match the hostname of the server in which the EventLog Analyzer is installed.

Solution:

Please get a new SSL certificate for the current hostname of the server in which EventLog Analyzer is installed.

Invalid Certificate

Description:

This error occurs when the SSL certificate you have configured with EventLog Analyzer is invalid. A certificate can become invalid if it has expired or other reasons.

Solution:

Please configure EvnetLog analyzer to use a valid SSL certificate.

Certificate is not trusted by JVM

Description:

This exception occurs when you configure a SMTP mail server or a web server with SSL in EventLog Analyzer, and the server uses a self-signed certificate. The Java Runtime Environment used in EventLog Analyzer will not trust self-signed certificates unless it is explicitly imported.

Solution:

You need to import the self-signed certificates used by the server in the JRE package used by EventLog Analyzer. Follow the steps given below:

Step 1: Download the certificate

For SMTP servers:

Note:

- To download the certificate used by SMTP server, you must have OpenSSL installed. You can download it from here.
- Open the command prompt and change to the bin folder in the OpenSSL installed location

- Open the command prompt and change to the bin folder in the OpenSSL installed location.
- Now run the following command,
- For example, openssl.exe s_client -connect smtp.gmail.com:587 -starttls smtp > gmailcert.cer

For Web Servers:

- Open the web URL in a browser.
- Click the padlock icon on the address bar.
- Click More Information. This opens the Certificate Viewer window showing the certificate used by that web server.
- Click View Certificate.
- When the Certificate window showing Certificate Information Authority opens, click the Details tab.
- Click Copy to File.
- In the Certificate Export Wizard that opens, click Next.
- Select the format as DRE encoded binary X.509 (.CER) and click Next.
- Enter the path where you wish to save the file and click Finish.

Step 2: Import the certificates in JRE package of EventLog Analyzer.

- Open a command prompt and change to the \jre\bin folder. For example: C:\ManageEngine\EventLogAnalyzer\jre\bin.
- Run the following command,
- For example: Keytool -importcert -alias myprivateroot -keystore ..\lib\security\cacerts -file C:\smtpcert.cer
- Enter changeit when prompted for a password.
- Enter y when prompted Yes or No.
- Close the command prompt and restart EventLog Analyzer.

Threat Intelligence Troubleshooting Tips

IP Geolocation data store corruption

This may happen when the product is shutdowns while the data store is updating and there is no backup available.

Troubleshooting steps:

- This is a rare scenario and it happens only when the product shuts down abruptly during the first ever download of IP geolocation data.
- There is no need for a troubleshoot as EventLog Analyzer will automatically download the data in the next schedule. Please note that the IP geolocation data gets automatically updated daily at 21:00 hours.

IP Geolocation data update failure

This occurs when there is no internet connection on EventLog Analyzer server or if the server is unreachable.

Troubleshooting steps:

- Make sure you have a working internet connection.
- Whitelist the following in your firewall:

- https://creator.zoho.com/
- https://creatorapp.zohopublic.com/

Log360 Cloud threat feed server is unavailable

This may happen when the product is unable to connect to the Log360 Cloud feeds server.

Case 1: Access is Blocked under firewall

Probable cause: The access to Log360 Cloud feeds server may be blocked under the firewall.

Solution:

- Review the firewall settings and look for any rules that might block the access.
- If you find any blocking rules, create a new rule that allows the traffic to the Log360Cloud feeds server.
- Save the new rule and update the firewall with the new settings.

Case 2: Unable to resolve DNS

Probable cause: The machine could not resolve the domain using its DNS resolver.

Solution:

- Check the DNS settings on the machine on which the product is running. Ensure that the DNS server settings are correct and that the machine is able to communicate with the DNS server.
- Try to resolve the domain name using a command line tool such as nslookup or dig to confirm that the DNS resolution is failing.
- Check if there are any firewalls or security settings that may be blocking DNS traffic.
- If using a proxy server resolves the DNS of the host involved, configure the proxy server in the product connection settings.

If none of the above works and the issue persists, contact our Technical Support team.

License file not found

If the license file cannot be accessed in the following page https://licensing.manageengine.com , kindly contact eventlog-support@manageengine.com

Update Access Key(Log360 Cloud Threat Analytics)

This can happen if the access key gets invalidated.

To regenerate the access key, please follow the below steps:

- Login to https://log360feeds.manageengine.com/
- Click on Regenerate Key.
- In the product, go to Settings > Admin Settings > Threat Feeds > Advanced Threat Analytics > Log360

Cloud Threat Analytics and add the new key.

VirusTotal API Quota Limit Exceeded

This happens when you exceed one of your quotas (per minute, per day or per month). Daily quotas are reset every day at 00:00 UTC.

Troubleshooting steps:

- Sign in into VirusTotal Account.
- Find your API quota under Profile → API Key → API Consumption for last 30 days (Check API limit for the day)

Internal Server Error

There may be various reasons for receiving this error.

- The request has been submitted to VirusTotal and there are server-side internal issues.
- The request has been submitted to Log360 Cloud Threat Analytics, and there are server-side internal issues.

Customers are advised to retry in a while, and if the same error is encountered, kindly contact " eventlog-support@manageengine.com "

Default Threat Sync Failure

This occurs when EventLog Analyzer server faces network connectivity issues.

Troubleshooting steps:

Make sure you have a working internet connection.

Whitelist the following in your firewall:

- https://creator.zoho.com/
- https://creatorapp.zohopublic.com/

Time zone

What to do if Daylight Savings Time(DST) is practiced in your region, but the product is not DST updated?

This occurs, when the JRE present in the product is not updated of the changes.

- Download Java SE TZUpdater from the official Oracle site. link "https://www.oracle.com/java/technologies/javase-tzupdater-downloads.html"
- Take back up of <Eventlog Analyzer_HOME>\jre
- After downloading, extract and copy the file tzupdater.jar to <EventLog Analyzer HOME>\jre\bin
- Stop EventLog Analyzer Service.

- Open Command Prompt as Administrator, navigate to <EventLog Analyzer HOME>\jre\bin.
- Execute the following command
  "java -jar tzupdater.jar -l <please select the latest time zone updater link from https://data.iana.org/time-zones/releases/>"
  For example
  Note:
  Incase customer environment is restricted from Online access follow 6.1 and 6.2.

  6.1: please select the latest time zone updater link from https://data.iana.org/time-zones/releases/ and download the latest timezone zip in tar.gz format.

  6.2 Execute the following command "java -jar tzupdater.jar -l file:downloaded_timezone_data_zip.tar.gz"

  For example
- Start EventLog Analyzer Service

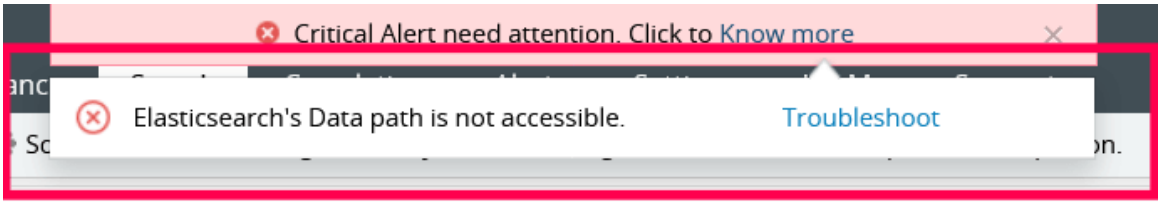
Search Engine - Elasticsearch

Data path not accessible

What is Elasticsearch data path?

Elasticsearch writes the data you index to indices, and data streams to a data directory which is available in elasticsearch.yml. Search and indexing will not work if the data path is not accessible.

If the data path is not accessible to write, the following notification will be shown.



Troubleshooting steps

- Open elasticsearch.yml file,search for path.data and find its value. elasticsearch.yml file can be found in <Installation Dir>/EventLog Analyzer/ES/config/elasticsearch.yml
- Make sure that both read and write permissions are enabled for the service account running EventLog Analyzer.
- If the path is a network location, then ensure connectivity and that the network path is accessible from the machine running EventLog Analyzer. Verify that there are no latency issues between the server and remote data path.

  If there is a need to change the data path of Elasticsearch, kindly follow this guide.

Device Auto Allocation

Failed to disable Auto Allocation.

Issue Description: Failed to disable Auto Allocation.

Possible Causes: Unable to update the database values due to environment issues.

Resolution: Try again after sometime.

Failed to enable Auto Allocation.

Issue Description: Failed to enable Auto Allocation.

Possible Causes: Unable to update the database values due to environment issues.

Resolution: Try again after sometime.

Failed to enable Auto Allocation Policies.

Issue Description: Failed to enable Auto Allocation Policies.

Possible Causes: Unable to update the database values due to environment issues.

Resolution: Try again after sometime.

Failed to disable Auto Allocation Policies.

Issue Description: Failed to disable Auto Allocation Policies.

Possible Causes: Unable to update the database values due to environment issues.

Resolution: Try again after sometime.

Failed to update Auto Allocation Policy.

Issue Description: Failed to update Auto Allocation Policy.

Possible Causes: Unable to update the database values due to environment issues.

Resolution: Try again after sometime.

Failed to update sync settings.

Issue Description: Failed to update Auto Allocation Policy.

Possible Causes:

- Unable to update the database values due to environment issues.
- Unable to communicate with ADAudit Plus.
- ADAudit Plus server may down.

Resolution: Check ADAudit Plus Server status and Communication. If those are correct, Try again after sometime it may be an environment issue.

17.2. EventLog Analyzer - Frequently Asked Questions

Last updated on: September 12, 2025

What is the difference between the Free and Professional Editions?

The Free Edition of EventLog Analyzer is limited to handling event logs from a maximum of five devices, whereas the Professional Edition can handle event logs from an unlimited number of devices. There is no other difference between the two editions, with respect to features or functionality.

Is a trial version of EventLog Analyzer available for evaluation?

Yes, a 30-day free trial version can be downloaded here. At the end of 30 days it automatically becomes a Free Edition, unless a new license is applied.

Does the trial version have any restrictions?

The trial version is a fully functional version of EventLog Analyzer Premium Edition. When the trial period expires, EventLog Analyzer automatically reverts to the Free Edition.

Do I have to reinstall EventLog Analyzer when moving to the paid version?

No, you do not have to reinstall or shut down the server. You just need to enter the new license file in the Upgrade License box.

What devices can EventLog Analyzer collect event logs from?

ManageEngine EventLog Analyzer can collect and analyze logs from a wide range of sources, including Windows and Linux/Unix systems, network devices like Cisco switches and routers, and other syslog-supported devices.

However, the capability depends on the operating system where it is installed:

- On Windows, it can collect event logs from Windows devices and syslogs from Unix systems, network devices, and applications.
- On Linux/Unix, it primarily collects syslogs from Unix systems, network devices, and other syslog-supported sources, but can also collect event logs from Windows machines using agent-based or agentless methods.

How many users can access the application simultaneously?

This depends only on the capacity of the server on which EventLog Analyzer is installed. The EventLog Analyzer license does not limit the number of users accessing the application at any time.

EventLog Analyzer runs in a web browser. Does that mean I can access it from anywhere?

Yes. As long as the web browser can access the server on which EventLog Analyzer is running, you can work with EventLog Analyzer from any location.

How do I buy EventLog Analyzer?

You can buy EventLog Analyzer directly from the ManageEngine Online Store, or from a reseller near your location.

Can EventLog Analyzer work if DCOM is disabled on remote systems?

For EventLog Analyzer to collect logs from remote Windows systems, DCOM must be enabled if you're using agentless log collection. However, if you're using agent-based collection, DCOM is not required.

How to monitor Windows Events in EventLog Analyzer Linux Installation?

You can collect logs from Windows devices in two ways with EventLog Analyzer:

- Convert Windows event logs to syslogs and forward them to EventLog Analyzer.
- Install an agent on the Windows device to directly monitor and collect logs.

What are the differences between ELA installed in Windows and Linux machines?

Most features from windows and linux are identical. Tight integration for windows machines are not available in linux builds, Although there are manual steps available to achieve the missing windows functionality.

#	Feature	UI	Windows Instance	Linux Instance	How to achieve the missing functionality?
1	Domain and workgroup discovery	ELA UI → Settings → Domains and Workgroup	Available	N/A	N/A
2	Device discovery	ELA UI → Settings → Devices → Windows	Available	N/A	Manually enter device name and associate

#	Feature	Devices → Add Device(s) UI	Windows Instance	Linux Instance	them with Agents. achieve the missing functionality?
					Download and
3	Windows devices & Windows Application log collection	ELA UI → Settings → Devices → Windows Devices → Add Device(s)	Agentless, agent-based and snare supported.	Only agent-based and snare supported.	install the agents manually or deploy using GPO/Endpoint Management Tool
4	Auto Push Windows agent	ELA UI → Settings→ Agents → Windows → Install Agent	Available	Not Available	Agents cannot be deployed to windows machines from Linux instances. Download and install the agents manually or deploy using GPO/Endpoint Management Tool
5	IIS Sites Discovery	ELA UI → Settings → Applications → IIS Servers	Available	N/A	We can collect IIS logs by selecting the device and browse the path manually through "Import Logs" feature
6	SQL Server as back-end database	Available	N/A	N/A	
		ELA UI →			We can collect logs from MSSQL in

#	Feature	UI	Available Instance	Not Available.	How to achieve the missing functionality?
7	MSSQL Discovery	Settings → Database Audit → Mssql Servers	Windows Instance	Linux Instance	Windows environments by manually entering the device details in the UI.
8	Mysql Discovery	ELA UI → Settings → Database Audit → MySql Servers	Available for Servers in Linux and Windows Environments	Available for Linux Environments only	We can collect logs from Mysql in Windows environments by manually entering the device details in the UI.
9	Workflow	ELA UI → Alerts → Workflow Audit → Create new workflow	All actions are available	Windows enviroment related actions are not available. Process Actions, Service Actions , Active Directory Actions and windows Actions are not available.	Not available
10	AD User Login	ELA UI → Settings → Technicians & Roles → Add Technician	Available	Not Available	Create and use in-built technicians or integrate with radius login.

Installation

What are the recommended minimum system requirements for EventLog Analyzer?

It is recommended that you install EventLog Analyzer on a machine with the following configuration:

- Processor - 6
- RAM - 16GB
- Disk Space - 1.2 TB
- Operating System - Windows 7, 2000, XP, 2003, Linux Ubuntu 8.0/9.0
- Web Browser - Microsoft Edge, or Mozilla Firefox 1.0

Look up System Requirements to see the minimum configuration required to install and run EventLog Analyzer.

Can I install EventLog Analyzer as a root user?

Yes, you can install EventLog Analyzer as the root user on Linux systems. However, it's generally recommended to use a dedicated user account for better security. Installing as root modifies the installation directory's permissions, which may cause issues if you attempt to start the server using a different user account later.

When I try to access the web client, another web server comes up. How is this possible?

The web server port you have selected during installation is possibly being used by another application. Configure that application to use another port, or change the EventLog Analyzer web server port.

Is a database backup necessary, or does EventLog Analyzer take care of this?

If you need to back up the database, you can do so via Settings > Data Storage > Database Settings. It's also recommended to regularly take snapshots or backups of the EventLog Analyzer installation directory for added data protection.

Please visit this page.

Configuration

How do I add devices to EventLog Analyzer so that it can start collecting event logs?

Please refer to the relevant pages below for detailed steps:

- Windows devices
- Syslog devices
- Application addition

How do I see session information of all users registered to log in to EventLog Analyzer?

The session information for each user can be accessed from the User Management link. Click the View link under Login Details against each user to view the active session information and session history for that user.

How to move EventLog Analyzer to a different machine/server?

Please follow these steps given here to migrate your existing EventLog Analyzer installation to a new machine/server.

How long can I store data in the EventLog Analyzer database?

EventLog Analyzer stores data in two formats: live logs in Elasticsearch and compressed logs in archives.

By default, live logs are retained for 32 days, but this duration can be customized based on your requirements.

For archived logs, retention can also be configured as per your needs; options include indefinite storage, 6 months, 3 months, and more.

How to change the log collection interval for Linux devices?

The log collection interval cannot be changed for Linux devices as EventLog Analyzer keeps listening for logs that come through open ports configured for syslog collection. Therefore, you will not be able to view the 'Change Monitor Interval' icon in the Device Management page for Syslog Devices.

Reporting

Why am I seeing empty graphs?

Graphs are empty if no data is available. If you have started the server for the first time, wait for at least one minute for graphs to be populated.

What are the types of report formats that I can generate?

Reports can be generated in HTML, CSV, and PDF formats. All reports are generally viewed as HTML in the web browser, and then exported to CSV or PDF format. However, reports that are scheduled to run automatically, or be emailed automatically, are generated only as PDF files.

Can't find an answer here? Check out the EventLog Analyzer user forum

18.1. EventLog Analyzer Technical Support

Last updated on: September 12, 2025

EventLog Analyzer offers comprehensive, best-in-class technical assistance and documentation to support deployment and troubleshooting.

Take a look at our resources to find the answers:

- Go through the FAQ
- Look up the troubleshooting tips
- Browse through the EventLog Analyzer forum

Still finding trouble? Get in touch with our technical support team:

- Send an email to eventlog-support@manageengine.com
- Call toll free telephone number (+1 844 649 7766)
- Ask for a meeting (Zoho Meeting) – web conference

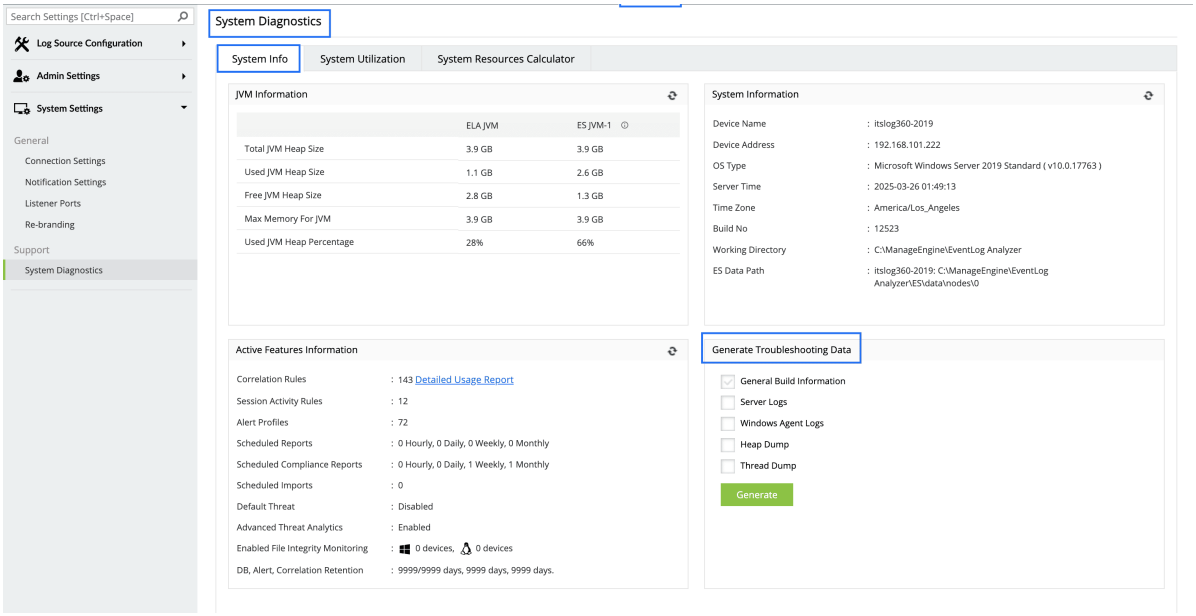
18.2. Create an EventLog Analyzer Support Information File (SIF)

Last updated on: September 12, 2025

In case you face an issue with log collection or any other aspect of EventLog Analyzer, please create a SIF and send it to support@eventloganalyzer.com. The SIF will help us analyze the issue and propose a solution. This article gives you the steps to generate SIF in different scenarios:

Creating SIF automatically

1. Login to the EventLog Analyzer web client and go to Settings -> System Diagnostics -> System Info tab.



2. Under the Generate Troubleshooting Data window, you will see the following log upload options:
   - General Build Information (Selected by default)- Provides general information about the server and product configuration.
   - Server Logs- Compiles logs of the EventLog Analyzer instance, including Elasticsearch logs.
   - Windows Agent Logs- Collects logs from Windows agents managed by this server. Requires access to the agent installed machine and credentials to collect the agent logs automatically.

     > Note: Logs from manually installed agents must be collected manually.

     How to collect agent logs manually?
     - Log in to the agent-installed machine.
     - Navigate to the installation folder of the agent (e.g., C:\Program Files (x86)\EventLogAnalyzer_Agent).
     - Locate the logs folder and compress it.

- Upload the compressed logs to https://bonitas.zohocorp.com/.

- Heap Dump & Thread Dump- Logs are collected by the support team upon request when the server encounters performance issues.

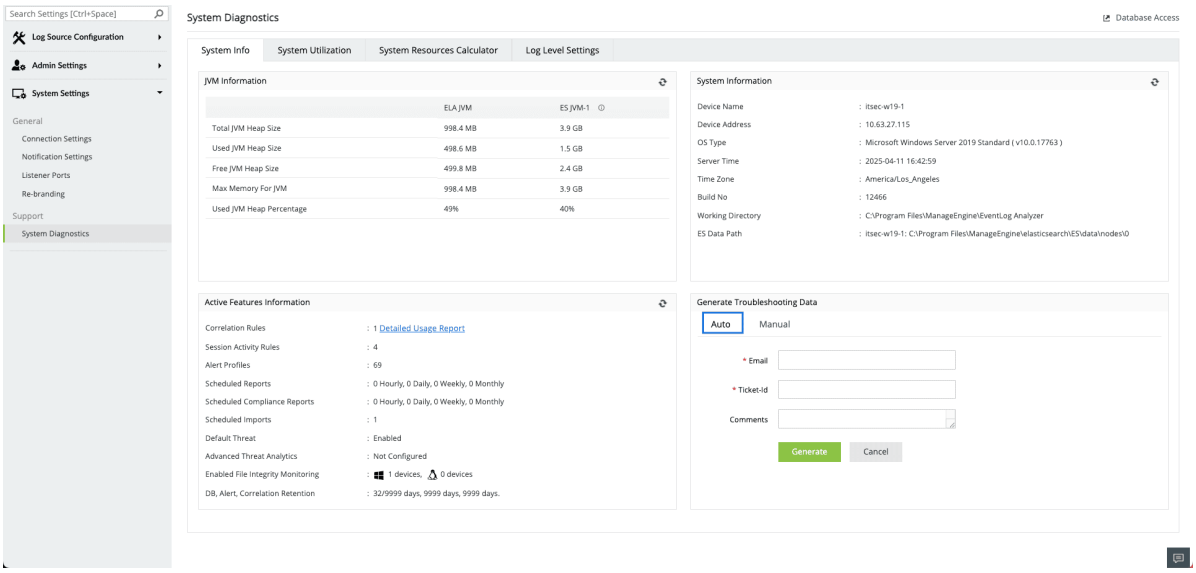
> **Note**
>
> The generated logs will be present under: ManageEngine\EventLog Analyzer\server\support folder in ZIP format.

Steps to upload logs: Auto and Manual SIF creation

After selecting the required logs and clicking 'Generate', you can create a SIF file using either the Auto or Manual upload option.

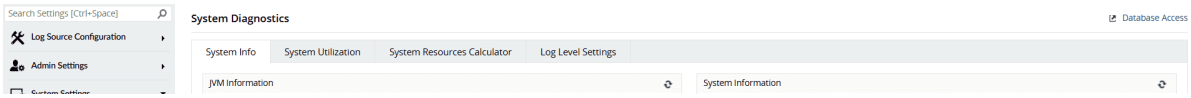
Automated upload process:

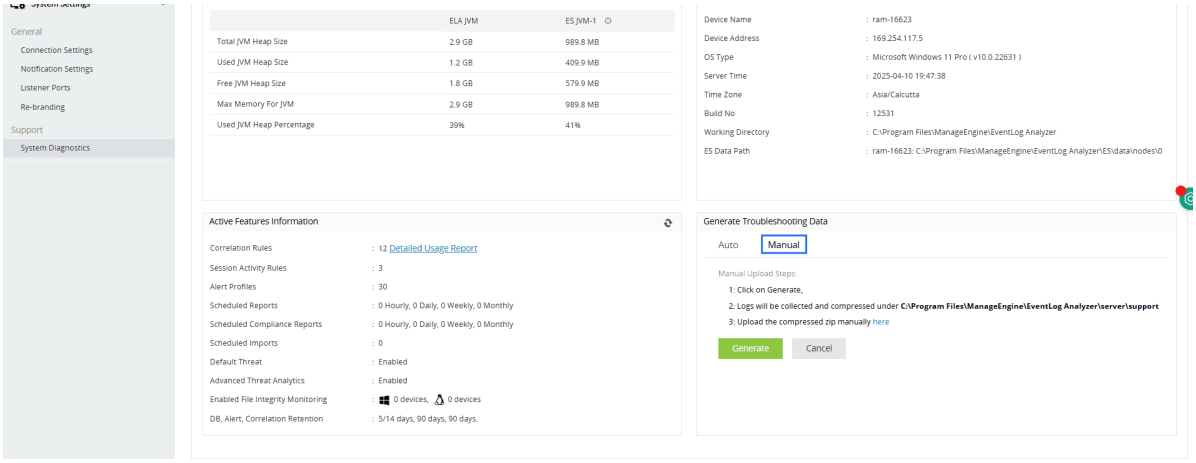
1. Utilize the Auto option to compress and upload logs directly to the support team.
2. Provide the necessary details, such as your email ID and ticket ID (can be left blank if unavailable).
3. Upon uploading, an acknowledgment mail will be sent.



Manual upload process:

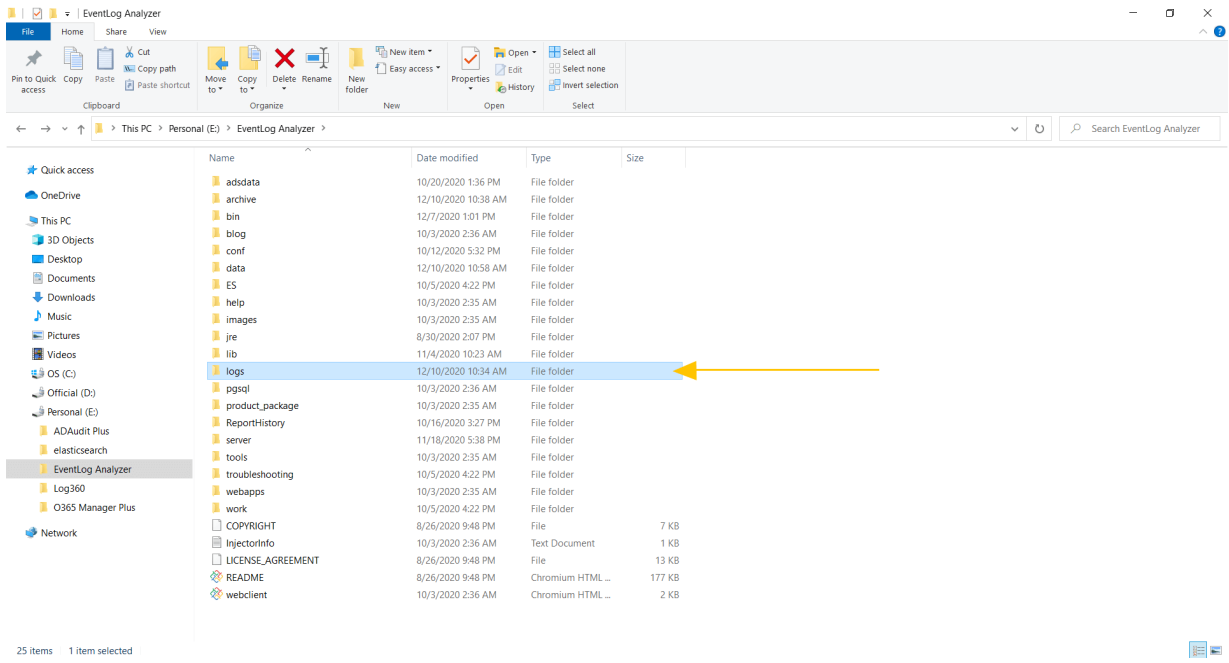
1. Click on Generate.
2. Logs will be collected and compressed under C:\Program Files\ManageEngine\EventLog Analyzer\server\support.
3. Upload the compressed ZIP manually on the bonitas website.





Procedure to create a SIF when the EventLog Analyzer server or web client is not working

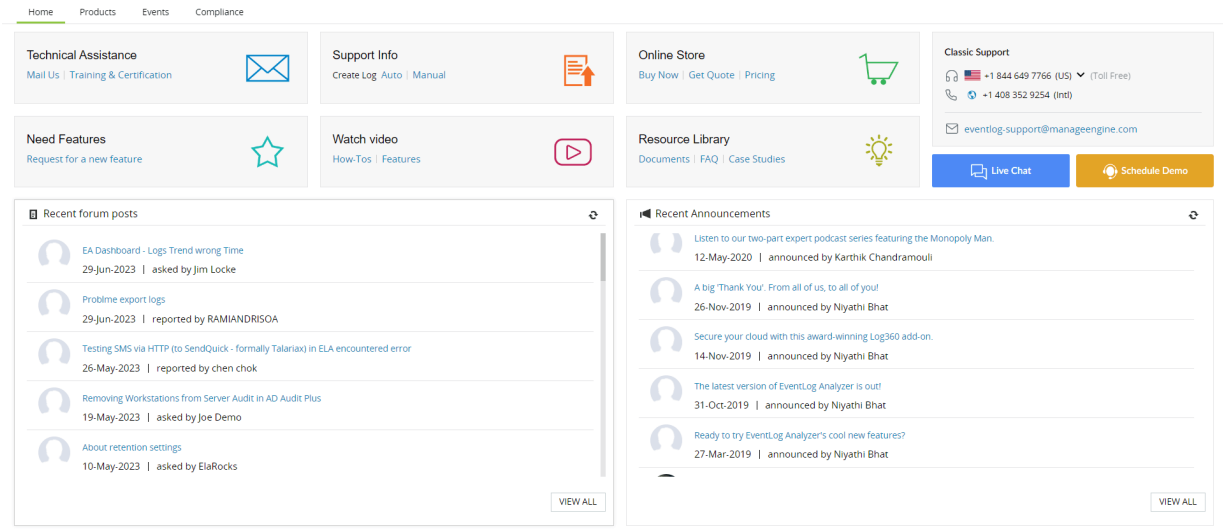
If you are unable to create a SIF from the EventLog Analyzer GUI, you can zip the files under 'logs' folder, which is located in <EventLog Analyzer Home>/logs (default path) and upload the ZIP file using the following link: https://bonitas2.zohocorp.com/#to=eventlog-support@manageengine.com



18.3. Contacting EventLog Analyzer Support

Last updated on: September 12, 2025

EventLog Analyzer provides a wide range of options to contact the support team, make feature requests, ask for a personalized demo, get online training, and more.
To go to the Support page, click the Support tab on the menu bar. The different channels through which you can reach out to us will be listed here. You can also click on the links below to reach our support team.



Request type	Link	Description
Technical Assistance	Mail Us	Click this link or click 'Mail Us' in the Support Page of EventLog Analyzer. Fill in the required fields with a detailed description of the problem that you encountered. Click on Submit.
Technical Assistance	EventLog Analyzer Training	Click this link or click 'Training & Certification' in the Support Page of EventLog Analyzer to take up a course and equip yourself with the knowledge required to work with EventLog Analyzer.
Create Log - Support Information Files		Go to 'Support Info' in the support page of EventLog Analyzer to create a support information file. It can be done automatically if you click the 'Auto' option. To do it manually, click the 'Manual' option. A set of instructions along with an upload link will be presented to you. Note: Click here to know more about Support Information Files.

Request type	Link	Description
Online Store - Get a Price Quote	Price Quote	Click this link or click 'Get Quote' under Online Store in the Support Page of EventLog Analyzer to get a personalized quote that best suits your requirements.
Online Store - Purchasing the product	Buy Now	Click this link or click 'Buy Now'/'Pricing' under Online Store in the Support Page of EventLog Analyzer.
New feature requests	Feature requests	If you'd like to see new features in the upcoming releases of EventLog Analyzer, click this link to give us your suggestions.
Configuration videos	How-To-Videos	Click this link or click 'How-Tos' under Watch Video in the support page of EventLog Analyzer. Under the 'How to' section, there are videos on configuring EventLog Analyzer for different use cases.
Feature videos	Feature-Videos	Click this link or click 'How-Tos' under Watch Video in the support page of EventLog Analyzer. Under the 'Features' section, there are videos on different features of EventLog Analyzer.
Knowledge Base	Documents	Click this link or click 'Documents' under Knowledge Base in the Support Page of the EventLog Analyzer solution to understand how to deploy, configure, and generate reports using EventLog Analyzer.
Knowledge Base FAQ	FAQ	Click this link or click 'FAQ' under Knowledge Base in the support page of EventLog Analyzer to view answers to frequently asked questions.
Knowledge Base Case Studies	Case Studies	Click this link or click 'Case Studies' under Knowledge Base in the support page of EventLog Analyzer. This page has case studies on how EventLog Analyzer has helped customers fulfill their requirements under different circumstances.
Contact our support team		Contact Us: Toll Free Number: US +1 844 649 7766 UK +44 800 028 6590 Australia +1 800 631 268

Request type	Link	Description
		Australia +1 800 631 268 China +86 400 660 8680 International +1 925 9249500 Direct Dialing Number +1 408 352 9254 Mail us at: eventlog-support@manageengine.com
Live Chat with the support team	Live Chat	Click this link or click 'Live Chat' in the Support Page of EventLog Analyzer for a live chat with the support team.
Request a personalized Demo	Schedule Demo	Click this link or click 'Personalized Demo' in the Support Page of EventLog Analyzer to schedule a personalized demo. Note: Personalized demos are available only during the free trial period.
Talk To Us		Click 'Talk To Us' in the Support Page of EventLog Analyzer to directly talk with the Support team. Note: This feature is available only for users with access to premium support.
Free Online Training		Click the 'Events' Tab in the support page of EventLog Analyzer to sign up for upcoming webinars, seminars and workshops. You can also watch videos of completed webinars, seminars and workshops under 'Completed Events' in the Events Tab.
User Forums	EventLog Analyzer User forums	Click this link or click 'View All' under 'Recent Forum Posts' in the Support Page of EventLog Analyzer. In this forum you can post your queries, interact with other EventLog Analyzer users and also get answers from out support team.
Announcements	EventLog Analyzer Announcements	Click this link or click 'View All' under 'Announcements' in the support page of the EventLog Analyzer solution to go to the EventLog Analyzer user forum announcements page for the latest announcements and updates.