ManageEngine
EventLog Analyzer

EventLog Analyzer
User Guide

CONTENTS

1. What is in this guide . . . **1**

2. Introduction . . . **2**

2.1. Overview . . . 2

2.2. Release Notes . . . 4

3. Setup the Product . . . **5**

3.1. What's in this section . . . 5

3.2. System Requirements . . . 6

3.3. Prerequisites . . . 12

3.4. Install and Uninstall . . . 31

3.5. Start and Shutdown . . . 33

3.6. Connect to Server . . . 38

3.7. Backing up database . . . 39

3.8. Increasing Product Memory . . . 40

3.9. License Details . . . 41

3.10. Get Started . . . 44

3.11. Service Account Permission . . . 46

4. Add Log Sources . . . **53**

4.1. What's in this section . . . 53

4.2. Adding Windows Devices . . . 54

4.3. Adding Syslog Devices . . . 58

4.4. Adding CEF devices . . . 63

4.5. Adding Other Devices . . . 64

4.6. Adding IBM iseries(AS400) devices . . . 65

4.7. Adding VMware(Exsi) devices . . . 69

4.8. Adding vCenter . . . 70

4.9. Adding Application Sources . . . **71**

4.9.1. Adding SQL servers . . . 71

4.9.2. Adding IIS Server . . . 77

4.9.3. Configuring an IIS site . . . 80

4.9.4. Adding MySQL Server . . . 84

4.9.5. Adding Oracle Server . . . 87

4.9.6. Adding Print Servers . . . 91

4.9.7. Adding Syslog source as Application . . . 92

4.9.8. Adding Sysmon Application . . . 94

4.9.9. Adding Terminal Servers . . . 96

4.9.10. Adding ManageEngine Applications . . . 97

4.9.11. Import Application Logs . . . 105

4.10. Adding AWS EC2 Windows instance . . . 124

4.11. Configuring Syslog Service . . . **128**

4.11.1. On a UNIX device . . . 128

4.11.2. On a Mac OS device . . . 132

4.11.3. On a HP-UX/Solaris/AIX device . . . 133
4.11.4. On a VMware . . . 134
4.11.5. On Arista Switches . . . 135
4.11.6. On Cisco Switches . . . 136
4.11.7. On HP Switches . . . 137
4.11.8. On Cisco devices . . . 138
4.11.9. On Cisco Firepower devices . . . 139
4.11.10. On Sonicwall devices . . . 140
4.11.11. On Juniper devices . . . 141
4.11.12. On PaloAlto devices . . . 142
4.11.13. On Fortinet devices . . . 144
4.11.14. On CheckPoint devices . . . 146
4.11.15. On NetScreen devices . . . 147
4.11.16. On Watchguard devices . . . 148
4.11.17. On Sophos devices . . . 149
4.11.18. On Cyberoam devices . . . 150
4.11.19. On Barracuda devices . . . 151
4.11.20. On Barracuda Web Application Firewall . . . 153
4.11.21. On Barracuda Email Security Gateway . . . 154
4.11.22. On Huawei Firewall devices . . . 155
4.11.23. On Malwarebytes devices . . . 156
4.11.24. On Meraki devices . . . 157
4.11.25. On FireEye devices . . . 158
4.11.26. On pfSense devices . . . 159
4.11.27. On Symantec DLP devices . . . 160
4.11.28. On Symantec Endpoint Protection devices . . . 161
4.11.29. On H3C devices . . . 162
4.11.30. On StormShield devices . . . 163
4.11.31. On F5 devices . . . 164
4.11.32. On Trend Micro - Deep Security . . . 166
4.11.33. On Forcepoint devices . . . 168
4.11.34. On Dell devices . . . 169
4.11.35. On Esxi 7 devices . . . 170
4.11.36. On Sangfor devices . . . 171
4.11.37. On Topsec devices . . . 173
4.11.38. On Stackato devices . . . 174
4.11.39. On Scaler NSS devices . . . 175
5. User Interface . . . 176
5.1. Tabs . . . 176
5.2. Dashboard Views . . . 182
5.3. Customize Dashboard Views . . . 190
5.4. Log Receiver . . . 200
5.5. Global Search . . . 203
6. EventLog Analyzer Reports . . . 205

6.1. Reports - Overview . . . 205
6.2. Configuring out-of-the-box reports . . . 207
6.3. Managing Predefined Reports . . . 209
6.4. Managing Report Views . . . 211
6.5. Create Custom Reports . . . 215
6.6. Schedule Reports . . . 223
6.7. Mark report as favourite . . . 225
6.8. Available Reports . . . 227
6.8.1. Reports for Networking Devices . . . 227
6.8.2. Reports for Windows Environment . . . 228
6.8.3. Reports for Unix Environment . . . 235
6.8.4. Reports for Applications . . . 243
6.8.5. Reports for vCenter . . . 264
6.8.6. Reports for H3C Devices . . . 266
6.8.7. Reports for Arista Devices . . . 268
6.8.8. Reports for StormShield . . . 270
6.8.9. Reports for HP Switches . . . 272
6.8.10. Reports for Barracuda Devices . . . 277
6.8.11. Reports for CheckPoint Devices . . . 282
6.8.12. Reports for Cisco Firepower Devices . . . 286
6.8.13. Reports for Fortinet Devices . . . 291
6.8.14. Reports for Huawei Devices . . . 295
6.8.15. Reports for Juniper Devices . . . 299
6.8.16. Reports for Malwarebytes Devices . . . 303
6.8.17. Reports for Meraki Devices . . . 306
6.8.18. Reports for NetScreen Devices . . . 310
6.8.19. Reports for PaloAlto Devices . . . 314
6.8.20. Reports for pfSense Devices . . . 318
6.8.21. Reports for SonicWall Devices . . . 322
6.8.22. Reports for Sophos Devices . . . 326
6.8.23. Reports for WatchGuard Devices . . . 330
6.8.24. Reports for F5 Devices . . . 334
6.8.25. Reports for IBM AS/400 devices . . . 339
6.8.26. Reports for Sangfor devices . . . 343
6.8.27. Reports for Topsec devices . . . 344
7. Threat Intelligence Data Analytics . . . 345
7.1. Overview . . . 345
7.2. FireEye Threat Solutions . . . 346
7.3. Symantec Endpoint Solutions . . . 349
7.4. Symantec DLP Applications . . . 352
7.5. Malwarebytes Solutions . . . 355
7.6. CEF format . . . 358
7.7. Configuring McAfee solutions for analysis . . . 360
8. Vulnerability Data Analytics . . . 362

8.1. Overview . . . 362
8.2. Vulnerability reports . . . 365
9. Real-time Event Correlation . . . 371
9.1. Understanding Correlation . . . 371
9.2. Correlation Reports . . . 375
9.3. Last Ten Incidents Overview . . . 380
9.4. Activity Reports . . . 381
9.5. Creating Custom Correlation Rules . . . 386
9.6. Managing Correlation Rules . . . 397
10. Compliance . . . 398
10.1. Compliance Reports . . . 398
10.2. Risk Posture . . . 401
10.2.1. Overview . . . 401
10.2.2. SQL Server . . . 404
11. Search Logs . . . 427
11.1. Overview . . . 427
11.2. How to Search Logs . . . 432
11.3. How to Extract New Fields . . . 440
11.4. How to Tag Fields . . . 447
12. Threat investigation . . . 452
12.1. Incident workbench . . . 452
12.1.1. Overview . . . 452
12.1.2. Access . . . 454
12.1.3. User Analytics . . . 458
12.1.4. Process Analytics . . . 463
12.1.5. Advanced Threat Analytics . . . 467
12.1.6. Incident Building . . . 472
12.2. Device Summary . . . 476
13. Alerts . . . 485
13.1. Overview . . . 485
13.2. Create Alert Profile . . . 488
13.3. View Log Alerts . . . 496
13.4. Alert Notification & Remediation . . . 505
13.5. Ticketing Tools Integration . . . 511
13.6. Manage alert Profiles . . . 531
13.7. Bulk Deleting/Updating Alerts . . . 537
14. Incident Management . . . 541
14.1. Create and assign workflow profiles . . . 541
14.2. Incident Workflow Management . . . 550
15. Framework Integration . . . 570
15.1. MITRE ATT&CK TTP(S) Framework Integration . . . 570
16. Configurations . . . 572
16.1. What's in this section . . . 572
16.2. Device Management . . . 573

16.3. Applications . . . 581
16.4. Database Audit . . . 582
16.5. File Integrity Monitoring . . . 583
16.6. Manage security applications . . . 591
16.7. Adding custom threat sources . . . 593
16.8. Advanced Threat Analytics . . . 601
16.8.1. Overview . . . 601
16.8.2. Log360 Cloud Threat Analytics . . . 605
16.8.3. VirusTotal . . . 612
16.8.4. Constella Intelligence . . . 619
16.9. Threat Whitelisting . . . 623
16.10. Threat Import . . . 628
16.11. Switching threat stores . . . 629
16.12. Manage Vulnerability Data . . . 631
16.13. Device Group Management . . . 633
16.14. VM Management . . . 636
16.15. Log Forwarder . . . 639
16.16. Manage Cloud Sources . . . 643
17. Admin Settings . . . 655
17.1. Admin Settings . . . 655
17.2. Privacy Settings . . . 656
17.3. Agent Administration . . . 658
17.3.1. Agent Administration . . . 658
17.3.2. Agent Settings . . . 673
17.4. Archive . . . 674
17.5. Technicians and Roles . . . 696
17.6. Logon Settings . . . 702
17.7. Security hardening . . . 722
17.8. Reset Account Settings . . . 724
17.9. Domains and Workgroups . . . 726
17.10. Working Hour Settings . . . 733
17.11. Product Settings . . . 734
17.12. API Settings . . . 739
17.12.1. API Settings . . . 739
17.12.2. Get log sources . . . 742
17.12.3. Get log fields . . . 744
17.12.4. Get log types . . . 746
17.12.5. Synchronous search . . . 748
17.12.6. Asynchronous search . . . 753
17.12.7. Jobs endpoint . . . 755
17.12.8. Jobs Result endpoint . . . 759
17.12.9. Get alert profiles . . . 762
17.12.10. Synchronous alerts . . . 764
17.12.11. Asynchronous alerts . . . 769

17.13. Retention Settings . . . 772
17.14. Log Collection Filter . . . 774
17.15. Log Collection Alerts . . . 777
17.16. Report Profiles . . . 778
17.17. Custom Log Parser . . . 779
17.18. Tags . . . 788
17.19. Profiles . . . 789
17.20. Database settings . . . 791
17.20.1. Database auto backup . . . 791
17.20.2. Database migration . . . 794
18. System Settings . . . 799
18.1. System Settings . . . 799
18.2. Notification Settings . . . 800
18.3. Manage Account TFA . . . 811
18.4. Install EventLog Analyzer as a service . . . 813
18.5. Connection Settings . . . 814
18.6. Re-branding . . . 819
18.7. System Diagnostics . . . 821
18.7.1. System Info . . . 821
18.7.2. System Utilization . . . 825
18.7.3. Database Access . . . 829
18.7.4. System Resource Calculator . . . 830
18.7.5. Log Level Settings . . . 835
18.8. Port Management . . . 836
19. Help, Questions, and Tips . . . 843
19.1. Troubleshooting Tips . . . 843
19.2. Frequently Asked Questions . . . 887
19.3. EventLog Analyzer Help . . . 897
20. Additional Utilities . . . 898
20.1. Additional Utilities . . . 898
20.2. Data Migration . . . 899
20.3. Working with HTTPS . . . 906
20.4. Configure MS SQL Database . . . 908
20.5. Migrate data from PostgreSQL to MS SQL database . . . 913
20.6. Migrate data from MySQL to MS SQL database . . . 917
20.7. Move Database to Different Directory in the Same Server . . . 921
20.8. Move Installation to Another Machine . . . 923
20.9. Configurations after changing the EventLog Analyzer server Hostname/IP address . . . 928
20.10. Move Installation to Different Directory in the Same Server . . . 938
20.11. Configuring NAT Settings . . . 943
20.12. Disk monitoring for search nodes . . . 945
20.13. SSL/TLS Settings for Elasticsearch . . . 949
20.14. Configuring DNS servers . . . 953
21. Distributed Edition . . . 954

21.1. Introduction to Distributed Edition . . . 954
21.2. Prerequisites for converting EventLog Analyzer standalone to distributed edition . . . 955
21.3. Converting standalone installation to Admin Server . . . 957
21.4. Converting standalone installation to Managed Server . . . 958
21.5. Manage Server Settings . . . 959
21.6. Setting up auto upgrade . . . 963
21.7. Auto-upgrade guidelines . . . 965
21.8. Frequently Asked Questions . . . 967
21.9. Centralized log archival . . . 971
22. Search Engine - Elasticsearch . . . 973
22.1. Data Upgrade . . . 973
23. Technical Support . . . 977
23.1. Technical Support . . . 977
23.2. Create SIF offline . . . 978
23.3. Contact Support . . . 981

1. What is in this guide?

This document allows you to make the best use of EventLog Analyzer. Explore the solution's capability to:

- Collect log data from sources across the network infrastructure including servers, applications, network devices, and more.
- Analyze log data to extract meaningful information in the form of reports, dashboards, and alerts.
- Monitor user behavior, identify network anomalies, system downtime, and policy violations.
- Detect internal and external security threats.
- Generate predefined reports to meet the requirements of regulatory compliance mandates such as PCI DSS, HIPAA, FISMA, SOX, GLBA, SOX, ISO 27001, and more.

Are you new to EventLog Analyzer?

A quick glance of the topics discussed below should be good enough to let you be able to deploy, configure, and generate reports using EventLog Analyzer.

- How to add devices and applications, and get logs into EventLog Analyzer?
- What are the reports available?
- How to generate custom rerports?
- How to search logs for specific information?
- How to extract additional fields from the logs?
- How to generate and send alert notifications?
- How to customize the web client?

2.1. Overview

EventLog Analyzer is a web-based, real-time, log monitoring and compliance management solution for Security Information and Event Management (SIEM) that improves network security and helps you comply with the IT audit requirements. Using an agent less architecture, EventLog Analyzer can collect, analyze, search, report on, and archive logs received from systems (Windows, Linux/UNIX), network devices (routers, switches, firewalls, and IDS/IP), applications (Oracle, SQL and Apache). It provides important insights into user activities, policy violations, network anomalies, system downtime, and internal threats. It can be used by network administrators and IT managers to perform audits for regulations such as SOX, HIPAA, PCI DSS, GLBA, etc.

You can use EventLog Analyzer to:

- Monitor activities of servers, workstations, devices, and applications spread across geographies.
- Monitor user activities like logons/logoffs and objects accessed.
- Generate reports for security events of interest.
- Generate compliance reports for PCI DSS, HIPAA, FISMA, SOX, GLBA and other regulatory mandates.
- Perform log forensics by swiftly searching the log database and save the search results as reports.
- Configure automatic e-mail or SMS alerts for indicators of compromise, such as network anomalies or compliance threshold violations.
- Execute workflows upon alert generation to respond to security threats automatically.
- Secure and tamper-proof archival of log data for forensic analysis and compliance audits.

Get log data from devices and applications

ManageEngine EventLog Analyzer collects, analyzes, searches, reports on, and archives event logs from distributed Windows devices; syslogs from Linux/UNIX devices, routers, switches and other syslog devices; and application logs from IIS web/FTP servers, print servers, MS SQL and Oracle database servers, DHCP Windows/Linux servers, and more.

- For real-time Windows event log collection, DCOM, WMI, and RPC have to be enabled in the remote windows machine for the logs to be collected by EventLog Analyzer.
- For real-time syslog collection ensure that the syslog listener ports in EventLog Analyzer are configured to listen to the port where the syslog or syslog-ng service is running on that particular (Cisco device, UNIX, HP-UX, Solaris or IBM AIX) machine.
- For application logs, EventLog Analyzer can be scheduled to import logs (HTTP or FTP) periodically from the application devices. You can also import and analyze the older logs from Windows and Linux machines.

Search log data and extract new fields to extend search

EventLog Analyzer provides a powerful log search engine for all types of logs. Universal log search is made possible with the help of the field extraction procedure, which allows you to define/extract new fields from your log data, in addition to the set of default fields that EventLog Analyzer automatically parses and indexes. Once new fields have been extracted, EventLog Analyzer automatically parses and indexes them from the new logs that are subsequently received; this drastically improves your search performance and helps EventLog Analyzer handle any kind of log format.

Generate IT audit reports to assess network security and comply with IT regulations

EventLog Analyzer provides a set of canned reports addressing important aspects of internal security. The software has the flexibility to create custom reports to address your IT department's complex requirements. Over and above the set of canned reports for SOX, HIPAA, GLBA, FISMA and PCI DSS, EventLog Analyzer also allows you to create customized reports for other compliance requirements.With this software you can schedule periodic report generation and distribute them to various users in different formats.

Real-time event correlation, instant alert notification and quick remediation

EventLog Analyzer comes with a robust event correlation and alerting moduleThe software can correlate events occurring across systems and applications and generate alerts. You can get instant notification via email and SMS. You can also execute workflows upon the generation of alerts to take quick remedial action.

2.2. Release Notes

This section contains a summary of the updates in EventLog Analyzer version 12.5.3 (Build 12531).

12.5.3 Build 12531 - Standalone Edition

Issue Fixes:

- An issue that occurred during credential synchronization, when domain credentials from ADAudit Plus were synced to EventLog Analyzer, has been fixed.
- An error that occurred when deleting a device or technician in EventLog Analyzer, while using MS SQL as EventLog Analyzer's backend database, has been fixed.
- An issue during bulk device synchronization between EventLog Analyzer and Log360, that occurred when the Convert host call API threshold limit exceeded 200 per minute has been rectified by increasing the limit to 1500 per minute.
- An issue in the CSV export of Alerts, where Add/Remove Columns changes were not reflected in the exported file, has been resolved.
- Fields such as backup file location, backup file size, and backup time taken, which are available for MS SQL reports, are now made available for Search and Custom Alert Criteria Builder.
- An erroneous message, 'Mail server not configured,' that appeared despite the successful configuration of the SMTP API, has been fixed.
- An issue involving the download of a corrupted Compliance zip file during file export has been fixed.
- An issue in rendering the error message for mandatory fields in integrated ServiceDesk Plus has been fixed.

Enhancement:

- EventLog Analyzer's integration with ServiceDesk Plus now enables you to create tickets using custom templates.

Distributed Edition

Issue Fixes:

- An issue where the Compliance Overview data for AS admin technicians was not available has been resolved.

> **Note:** The updates for the **Distributed Edition** are the same as that of the Standalone edition.

Setup the Product

3.1. Setup EventLog Analyzer

- Download the product
- Check the installation requirements
- Install the product
- Ensure the prerequisites are met
- Run the product
- Connect to the EventLog Analyzer Server
- Backup the EventLog Analyzer database
- Check the EventLog Analyzer editions available
- Buy the product

3.2. System Requirements

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	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

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.

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 is higher than what a single node can handle, it is recommended to implement **distributed setup**.
- 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

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 discovery	Available	N/A
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 better performance. Off-heap memory is maintained by the operating system and will free up when necessary.

Additional Elasticsearch Node Recommendations:

Hardware	Minimum	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*

3.3. Prerequisites

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/8400 (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
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
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 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/8400 (configurable)	EventLog Analyzer Server	EventLog Analyzer Agent Machine	**Environment Permission:** • 8400 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/8400 (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	
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	
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
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
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	
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 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	
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 Device	EventLog Analyzer Server	RPC	**UserGroups:** • Distributed COM Users **User Permissions:**
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	

TEST PROCESS	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	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 Device	EventLog Analyzer Server	-	-

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.

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.
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
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/StandaloneManagedServer-UserGuide/IncidentManagement/incident-workflow.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/StandaloneManagedServer-UserGuide/IncidentManagement/incident-workflow.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/StandaloneManagedServer-UserGuide/IncidentManagement/incident-workflow.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/StandaloneManagedServer-UserGuide/IncidentManagement/incident-workflow.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/StandaloneManagedServer-UserGuide/IncidentManagement/incident-workflow.html#fortigateCredentials

7. Distributed communication Setup

Distributed

PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
HTTP/8400 (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 8400. • The port can be customized by the user.
HTTP/8400 (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 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.
<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.
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/

3.4. How to Install and 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,

```
> chmod +x ManageEngine_EventLogAnalyzer.bin
```

- 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 8400. 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.

```
> ./Change\ ManageEngine\ EventlogAnalyzer\ Installation
```

3. You will be asked to confirm your choice, after which EventLog Analyzer is uninstalled.

3.5. How to Start and Shutdown 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
Top level directories like /opt/, /home , /, and others	Root User: Yes Other User: Yes	**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 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:8400

- The 8400 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:

```
> /bin$ ./configureAsService.sh -i
```

- Once the software is installed as a service, execute the command given below to start Linux Service:

```
> /etc/init.d/eventloganalyzer start
```

- Check the status of the EventLog Analyzer service by executing the following command (sample output given below):

```
> /etc/init.d/eventloganalyzer status
  ManageEngine EventLog Analyzer 11.0 is running (<Process ID>).
```

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

```
> /etc/init.d/eventloganalyzer stop
```

Stopping ManageEngine EventLog Analyzer <version number>...

Stopped ManageEngine EventLog Analyzer <version number>

- Check the status of the service again:

```
> /etc/init.d/eventloganalyzer status
```

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**'.

3.6. Access EventLog Analyzer Server

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>:8400 (where <devicename> is the name of the machine in which EventLog Analyzer is running, and 8400 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.

3.7. How do I backup my database?

Below are the procedures for backing up data from PostgreSQL, MySQL and MS SQL databases.

> **Note:** Before starting the backup process, **stop EventLog Analyzer service.**

Database backup procedures for PostgreSQL:

Take a backup of the existing EventLog Analyzer PostgreSQL database by creating a ZIP file of the contents available in <EventLog Analyzer Home>\pgsql directory and save it as pgsql_backup.zip in **<EventLog Analyzer Home>** directory.

Database backup procedure for MySQL:

Take a backup of existing EventLog Analyzer MySQL database by creating a ZIP file of the contents available in <EventLog Analyzer Home>\mysql directory and save it as **mysql_backup.zip** in **<EventLog Analyzer Home>** directory.

Database backup procedure for MS SQL:

- Find the current location of the data and log file for the database eventlog by using the following commands:

```
> use eventlog
  go
  sp_helpfile
  go
```

- Detach the database using the following commands:

```
> use master
  go
  sp_detach_db 'eventlog'
  go
```

- Backup the data file and 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**.
- Re-attach the database and point to the old location by using the following commands:

```
> use master
  go
  sp_attach_db 'eventlog' , '<MSSQL Home>/data/eventlog.mdf' , <MSSQL
  Home>/data/eventlog_log.LDF
  go
```

3.8. Increasing Product Memory

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.

3.9. 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 edition, license model and number of devices. The editions are **Standalone/Premium,** and **Distributed**. The license models are, **Perpetual (Standard)** and **Annual Subscription Model (ASM)**.

EventLog Analyzer comes in two editions: Standalone and Distributed. The solution is licensed based on the number of Windows Workstations, Windows Servers, and Syslog devices along with add-ons such as Application Auditing for IIS and SQL servers , Linux File Server Auditing and Advanced Threat Analytics.

Available Editions

Standalone Edition

If your company is a Small or Medium Business (SMB), the network is in a single geographical location, and the number of devices and/or applications to be monitored is less than 1000, the Standalone edition is suitable for your company. Also, the log reception rate should be well within 20,000 logs/second. If your log rate increases, then you can easily switch over to Distributed Edition to handle the capacity.

Distributed Edition

If your company is a Large Business or Managed Security Service Provider (MSSP), and the network is spread across multiple geographical locations, the Distributed edition is suitable for your company. You can monitor 50 to virtually unlimited number of hosts/applications with this edition.

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.

Advantages of ManageEngine Licensing

- Simple cost-conscious, need-based licensing, depending on the number of devices/applications to be monitored.
- The Distributed license is applied on the Admin server and there will be no restriction on the number of Managed servers deployed.

How to choose the license

- Assess your network and decide upon Standalone or Distributed.
- Choose Perpetual model for a license with no expiry and choose Annual Subscription Model for low entry cost.
- Decide upon the number of devices/ applications to be monitored.

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:

- For the distributed edition, login to your admin server and add the license file by following the same procedure. The license will then be synced with the managed servers.
- 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 Premium or Distributed
- Number of days remaining for the license to expire
- Maximum number of devices that you are allowed to manage

3.10. Get Started

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

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.

3.11. Account privileges required for Event Log Collection

- 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.

4.1. Adding Devices

Add a device in the user interface using any one of the following menu options:

- **Home** tab > **Manage Devices** > **Devices** > **+Device**
- **+Add** tab > **Device**
- **Settings** tab > **Configurations** > **Device Management** > **+Add Device(s)**

Adding Device Groups

You can group your devices into a particular **Device Group**. The default device groups available are **Windows Group, Unix Group** and **Default Group** (which contains all the devices). To add a new host group, click on the **Add** link beside **Device Groups** field in **Device group management** page**.** You can manage the device groups in the Device Group Management page.

4.2. Adding Windows devices

In all Windows devices, ensure that WMI, DCOM are enabled, and logging is enabled for the respective modules/objects. To forward the Windows event logs in syslog format, use a third party utility like SNARE. To add a domain or to update a domain or workgroup, refer to the Domains and Workgroups page.

Note: Installation of Windows agent application is mandatory to collect Windows eventlogs for EventLog Analyzer deployed on Linux operating systems.

To add Windows devices

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.

To add workgroup(s):

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.

Windows

Windows custom log collection

EventLog Analyzer now allows you to customize log collection according to the time. You can choose to collect logs from the past based on hours, days, weeks and even months.

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**.

4.3. Adding Syslog Devices

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.

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.

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.

4.4. Adding Common Event Format (CEF) Devices

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.**

4.5. Adding Other Devices

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.

4.6. Adding IBM iSeries (AS/400) devices

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. iIn 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:

```
> CRTJRNRCV JRNRCV(JRNLIB/AUDRCV0001) + THRESHOLD(100000) AUT(*EXCLUDE) +
  TEXT('Auditing Journal Receiver')
```

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:

```
> CCRTJRN JRN(QSYS/QAUDJRN)+
  JRNRCV(JRNLIB/AUDRCV0001)+
  MNGRCV(*SYSTEM) DLTRCV(*NO)+
  AUT(*EXCLUDE) TEXT('Auditing Journal')
```

- 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:

```
> CHGSECAUD QAUDCTL(*ALL) QAUDLVL(*ALL)
```

- 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.

4.7. Adding VMware (ESXi) devices

1. In the Manage Devices window, navigate to the **Other Devices** tab and click on **+Add Device(s)**.
2. Select the **Device Type** as ESXi and add the VMware device as a Unix device as per the steps given here.
3. Configure the syslog daemon in the VMware device as per the steps mentioned here.

4.8. Adding vCenter

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.

4.9.1. Adding SQL server

EventLogAnalyzer supports the following SQL auditings:

- DDL/DML Monitoring
- Advanced Auditing
- Column Integrity Monitoring

Supported SQL Server Versions:

- **SQL Server 2012 and above :** Full support
- **SQL Server 2008 :**
  - **Enterprise and Datacenter editions :** Full support
  - **Other editions :** Partial Support(Only Advanced auditing and Column Integrity Monitoring available)

Steps to create a SQL Server Audit Object manually

Carry out the following steps to create a SQL Server Audit Object manually:

1. Navigate to **Object Explorer** in the MSSQL Server Management Studio.
2. In the Object Explorer, expand the **Security node**.
3. Right-click the **Audits** folder and select the **New Audit** option. It will open a **Create New Audit** page.
4. Define the **Audit Name** field with a suitable name for the Audit Object.
5. Choose the Application log type in the **Audit Destination** field.
6. Accept the other default settings and save the new audit specifications.

Steps to add a SQL Server

1. Navigate to **Settings > Log Source Configuration > Database Audit**.

2. In the **Database Management** page, click **+ Add SQL Server Instance**. The SQL server instances are automatically

discovered and listed out.

3. Select the SQL Server instance(s) you wish to monitor and click **Next**. You will be taken to the **Credential Configuration** page and prompted to enter valid credentials.
4. If you wish to use the default credentials, select the check-box (default credentials could be the device or domain or logged on credentials). Alternatively, you can enter a username and password in the credentials field and click **Save**.

If the SQL Server instance you wish to add for monitoring is not discovered automatically, click

+ Add Manually and you will be prompted to enter details for Windows Server configuration and SQL Server instance configuration.

Steps to add a SQL Server instance manually

Windows server configuration

- Select the Windows server and enter valid credentials. Alternatively, you can use the default credentials.
- **SQL Server instance configuration**
- Enter the instance name, port number, and credentials in the given fields
- Enable or disable **Advanced Auditing**.

> **Note:** Enabling advanced auditing will create an audit policy and disabling advanced auditing will remove the audit policy on the selected SQL Server instance.

- Select the **instance authentication method** (Windows or SQL authentication) from the available dropdown menu.

> **Note:** Windows Authentication is recommended for Advanced Auditing.

- Click **Add**.

Viewing added SQL Server instances

EventLog Analyzer lists all the SQL Server instances being monitored. From this list, you can enable, disable, or delete SQL Server instances.

What are the different types of SQL auditing performed by EventLog Analyzer?

In EventLog Analyzer UI, go to **Settings tab** → **Database Audit** page → **SQLServer Audit Logs** to view the status of each mode.

Case 1: DDL/DML Monitoring

1. When **Advanced Auditing** is enabled for an instance in EventLog Analyzer, a server-level audit specification is created in the SQL Server instance for the following audit action types:
    1. SCHEMA_OBJECT_ACCESS_GROUP
    2. DATABASE_ROLE_MEMBER_CHANGE_GROUP
    3. SERVER_ROLE_MEMBER_CHANGE_GROUP
    4. FAILED_LOGIN_GROUP
    5. SUCCESSFUL_LOGIN_GROUP
    6. DATABASE_CHANGE_GROUP
    7. DATABASE_OBJECT_CHANGE_GROUP
    8. DATABASE_PRINCIPAL_CHANGE_GROUP
    9. SCHEMA_OBJECT_CHANGE_GROUP
    10. SERVER_PRINCIPAL_CHANGE_GROUP
    11. LOGIN_CHANGE_PASSWORD_GROUP
    12. SERVER_STATE_CHANGE_GROUP
2. The **Application** type events collected for the corresponding Windows device are used for this mode of auditing.
3. The following report groups (**Reports** tab → **Applications** → **SQLServer Audit Logs**) are populated with this mode of auditing:
    1. SQL Server Events
    2. SQLServer Trend Report
    3. DDL Auditing Report
    4. DML Auditing Report

5. Auditing Account Management
6. Auditing Server Report
7. Attack Reports
8. Additional Security Reports

> Note: **Advanced Auditing** needs to be enabled for server-level audit specification to be created. It can be disabled later. The required logs will be fetched even if Advanced Auditing has been disabled.

Case 2: Database Auditing

1. When **Advanced Auditing** is enabled for an instance in EventLog Analyzer, queries are executed every night at 11PM to collect events in this auditing mode.
2. Following reports (**Reports** tab → **Applications** → **SQLServer Audit Logs** → **Advanced Auditing Reports**) are populated with this mode of auditing:
    1. Last Login Time Report
    2. Delete Operations Report
    3. Logins Information Report
    4. Most Used Tables
    5. Table Update Report
    6. Index Information Report
    7. Server Information Report
    8. Waits Information Report
    9. Blocked Processes Report
    10. Schema Change History
    11. Object Change History
    12. Connected Applications Report
    13. Security Changes Report
    14. Permissions Information Report
    15. Last Backup of Database
    16. Last DBCC Activity

> Note: The queries to fetch logs will succeed only if **Advanced Auditing** is enabled.

Case 3: Column Integrity Monitoring

1. When **Column Integrity Monitoring** is configured, **EventLog Analyzer** creates a **trigger** in the SQL Server instance which automatically writes an event in **Event viewer** when the monitored column of the given table is modified (i.e. an UPDATE query is executed).

2. The **Column Integrity Monitoring** report provides information on the changes in a monitored column including who changed the value, at what time the value was changed, and the database table in which the value was changed. Additionally, the old and new values are shown.
3. Data types such as text, ntext, and images will not be monitored.
4. Columns to be monitored must be chosen carefully, as triggers are used to monitor changes and is a performance intensive operation.
5. Following reports (**Reports** tab → **Applications** → **SQLServer Audit Logs** → **Advanced Auditing Reports**) are populated with this mode of auditing:
    1. Column Modified Reports

> **Note**: To enable Column monitoring, the following prerequisite to be met
>
> 1. **Advanced Auditing should** be **enabled** to **create Trigger** in the SQL server. it can be **disabled** later, once the **trigger** is **created**.
> 2. The trigger that has to be created is of type "**AFTER TRIGGER**" , hence a **primary key** must be present in the table for the **trigger** to be **fired**.

Case 4: Events Collected

When advanced auditing is enabled, the following event id's will be enabled in the SQL server for the following reports.

DBCC Information Reports - 211, 427, 610, 8440, 9100, 15612, 15615, 2509, 2510, 2514, 17557

Host Activity Reports - 18100

Integrity Reports - 806, 825

Permission Denied Reports - 229, 300, 230, 262, 916, 5011

Violation Reports - 17308, 17311

> **Note:**
>
> - The minimum permission required for SQL server auditing is given in this link.

4.9.2. Adding an IIS server

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.

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.

4.9.3. Configuring an IIS site for non-admin users

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**

4.9.4. Adding MySQL Server

To add a MySQL server for monitoring:

- Navigate to **Settings > Log Source Configuration > Database Audit**.
- Click on the **+Add Instance** button.

- Enter the name of the device or click on the + icon to choose from the list of discovered MySQL servers.
- Enter the port number of the MySQL server.

Note: If the name of the MySQL server is manually entered, the port number has to be filled. For the MySQL servers selected from the list of discovered servers, the port number will be filled in automatically.

- Select the appropriate protocol to be used from the drop down.

- Enter the file path of the general and error logs.
- Click on Verify & Save to save the changes made

Advanced Settings

To make changes to the time zone and file encoding, click on the Advanced button and choose the relevant option from the drop downs provided.

Prerequisites to Discover MySQL Servers

Discovering MySQL servers in UNIX or Linux devices:

The MySQL server configuration file is found using the **mysqld process.**

- The Secure Shell protocol is used to access the mysqld process to get the configuration file path.
- The SFTP protocol is used to read configuration file.

Discovering MySQL servers in Windows devices:

The MySQL server configuration file is found using the mysqld.exe process.

- WMI API is used to access mysqld.exe process to get the configuration file path.
- SMB protocol is used to read the configuration file.

In addition, the configuration file parameters are explored in the order:
--defaults-extra-file
--defaults-file

If the MySQL configuration file is not found with the mysqld or mysqld.exe process, then the following occurs:

UNIX or Linux: The configuration file location defaults to the location

- /etc/my.cnf
- /etc/mysql/my.cnf.

Windows: The configuration file location defaults to the following locations

- C:/Windows/my.ini
- C:/Windows/my.cnf
- C:/my.ini
- C:/my.cnf

From the command line parameters and the configuration file, the MySQL server **General log path** and **Error log path** are discovered.

Credentials for discovery:

For Windows devices, credentials for discovery is picked in the following order:

1. Domain/workgroup credential if a device is under a domain or a workgroup.
2. Device credential, if it is provided in the "Manage Devices" page.
3. Logon credential.

For Linux devices, the credentials used while configuring auto log forward will be used for MySQL discovery.

> **Note:** In Linux installations, MySQL server discovery on Windows devices is not possible.

4.9.5. Adding Oracle Server

- Navigate to **Settings > Log Source Configuration > Database Audit**.
- Next, select the **Oracle** tab.
- Click on **+ Add oracle server** if no oracle servers are configured.
- 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 Unix, check the **Add as Syslog device** box. If the device type is Windows, enter **Username > Password > Verify Credentials** and click on **Select**.
- Based on your selected device type, choose between **Windows** and **Unix** platform options. If you have configured the log sources manually, the platforms will be automatically updated.
- Click on **Add** to add the log source.

Oracle Server Configuration

- Oracle server - Windows platform
- Oracle server - Linux platform

Reference: http://download.oracle.com/docs/cd/B28359_01/network.111/b28531/auditing.htm#CEGBIIJD

For Oracle server installed in Windows platform

- Connect to SQL *Plus using the sqlplus command.
- Execute the command given below to check whether the audit_trail is set to OS or not.

```
> Show parameter AUDIT_TRAIL;
```

- Change audit parameters using the below command:

```
> Show parameter AUDIT_TRAIL;ALTER SYSTEM SET AUDIT_TRAIL=OS SCOPE=SPFILE;
```

- Restart the Oracle server to let the changes take effect.
- To disable AUDIT_TRAIL

```
> ALTER SYSTEM SET audit_trail = NONE SCOPE=SPFILE ;
```

For Oracle Server installed in Unix platform

- Execute the command given below to check whether the audit_trail is set to OS or not.

```
> Show parameter AUDIT_TRAIL;
```

- Change audit parameters using the below command:

```
> ALTER SYSTEM SET AUDIT_TRAIL=OS SCOPE=SPFILE;
```

To enable Oracle syslog auditing, follow the procedure given below:

1. Manually add and set the **AUDIT_SYSLOG_LEVEL** parameter in the initialization parameter file, initsid.ora.

   The **AUDIT_SYSLOG_LEVEL** parameter is set to specify a facility and priority in the format AUDIT_SYSLOG_LEVEL=facility.priority.

   facility: Describes the part of the operating system that is logging the message. Accepted values are user, local0–local7, syslog, daemon, kern, mail, auth, lpr, news, uucp, and cron.

   The local0–local7 values are predefined tags that enable you to sort the syslog message into categories. These categories can be log files or other destinations that the syslog utility can access. To find more information about these types of tags, refer to the syslog utility MAN page.

   priority: Defines the severity of the message. Accepted values are notice, info, debug, warning, err, crit, alert, and emerg.

   The syslog daemon compares the value assigned to the facility argument of the **AUDIT_SYSLOG_LEVEL** parameter with the **syslog.conf** file to determine where to log information.

   For example,the following statement identifies the facility as local1 with a priority level of warning:

   AUDIT_SYSLOG_LEVEL=local1.warning

   See Oracle Database Reference for more information about AUDIT_SYSLOG_LEVEL.

2. Log in to the machine that contains the syslog configuration file, /etc/syslog.conf, with the superuser (root) privilege.
3. Add the audit file destination to the syslog configuration file **/etc/syslog.conf.**

   For example: assuming you had set the AUDIT_SYSLOG_LEVEL to local1.warning, enter the following:

```
> local1.warning /var/log/audit.log
```

This setting logs all warning messages to the **/var/log/audit.log** file.

4. Restart the syslog logger:

```
> $/etc/rc.d/init.d/syslog restart
```

Now, all audit records will be captured in the file /var/log/audit.log through the syslog daemon.

5. Restart the Oracle server so that the changes take effect.

> **Note**: When logged in as SYSDBA/SYSOPER, Oracle database provides limited information on database activity monitoring. Hence, to get the complete audit trail activities of Oracle database, we suggest that you log in as a user with privilege other than SYSDBA/SYSOPER.

Auditing statements

DDL

You can audit DDL activities of a selected user in the database.

- To enable auditing of all privileges of users:

```
> AUDIT ALL PRIVILEGES by user_name; (or)
  AUDIT CREATE TABLE by user_name;
```

- To enable auditing of specific privileges:

```
> AUDIT CREATE TABLE by user_name;
```

Add your required auditing option near "CREATE TABLE".

- Restart the Oracle server to let the changes take effect.

> **Note**: To check the audit options that are enabled under any user, execute the statement given below.
>
> ```
> > SELECT user_name, audit_option, success, failure FROM DBA_STMT_AUDIT_OPTS;
> ```

DML

This auditing enables you to audit specific statements on a particular object. It always applies to all users of the database.

```
> AUDIT SELECT, INSERT, UPDATE, DELETE on table_name
```

You can also add your required auditing option(s) here.

- The following statement specifies default auditing options for objects that might be created in the future:

```
> AUDIT SELECT, INSERT, UPDATE, DELETE on DEFAULT;
```

- Restart the Oracle server to let the changes take effect.

Note: To check the audit options that are enabled under any object, simply execute the below statement.

```
> SELECT OWNER, OBJECT_NAME, OBJECT_TYPE, INS, UPD, DEL FROM
  DBA_OBJ_AUDIT_OPTS;
```

To disable audit option, use NOAUDIT instead of AUDIT in same statement.

Details about the audit options are available here.

4.9.6. Adding Print Servers

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

4.9.7. Adding a Syslog Application

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.

4.9.8. Adding Sysmon Application

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**.

4.9.9. Adding Terminal Servers

- 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.

4.9.10. Adding ManageEngine Applications

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.

Data Enrichment Configuration for ManageEngine Endpoint Central

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

Configuring ManageEngine Endpoint Central 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.

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.

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.

4.9.11. Import Log Files

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

- 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.

```
> log_line_prefix = '%m [%p] '
```

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
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.

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:

```
> db2audit configure datapath "C:\IBM\DB2\DataPath" archivepath "C:\IBM\DB2\ArchivePath"
```

Note: Replace the given paths with the paths of your choice for data path and archive path respectively.

- Run the following command:

```
> db2audit configure scope all status both error type normal
```

Note: Replace the given parameters with the parameters of your choice.

- Run the following command:

```
> db2audit start
```

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:

```
> db2 connect to your_database
```

Note: Replace your_database with the database name of your choice.

- Run the following command to create an audit policy for the database:

```
> db2 create audit policy policy_name categories all status both error type audit
```

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:

```
> db2 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:

```
> db2 audit database using policypolicy_name
```

Note: Replace policy_name with the name of the audit policy that you created.

- Run the following command to commit:

```
> db2 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:

```
> db2audit archive databaseyour_database
```

Note: Replace your_database with the name of the database.

- Run the following command to archive active instance logs:

```
> db2audit archive
```

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:

```
> db2audit extract file C:/IBM/DB2/instancelog.txt from files
  db2audit.instance.log.0.20060418235612
```

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:

```
> db2audit extract file C:/IBM/DB2/databaselog.txt from files
  db2audit.db.your_database.log.0.20060418235612
```

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.

```
> db2 get dbm cfg | findstr DIAGPATH
```

or

```
> db2 get dbm cfg | grep DIAGPATH
```

or

```
> db2 get dbm cfg
```

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.

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:

```
> %h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\"
```

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:

```
> %h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\" %{ms}T %I
```

%{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.

```
> LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\" %{ms}T %I"
  modified
```

2. The label can be used to reference the new format string as the customLog directive.

> **CustomLog logs/access.log modified**

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:

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

Installation procedure

Ensure that EventLog Analyzer server can access EC2 Windows instance.

Welcome screen with copyright protection message appears.

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 8400).

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.

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

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.

4.11.1. Configuring the Syslog Service on a UNIX devices

Steps to configure log forwarding manually

Note: Please take a note of the default port numbers used for the different protocols.

Default port number & protocol used

1. 513 & 514 UDP
2. 514 TCP
3. 513 TLS

To find the Syslog service used, use the below command

```
> ps aux | grep syslog
```

As a result, this will return the current running Syslog service.

Follow the steps below to configure log forwarding to EventLog Analyzer server based on the Syslog Service used.

1. Add the required entries in the configuration file based on protocol. Restart the syslog daemon service to apply the changes
   - **syslogd**
     - File path: /etc/syslog.conf
     - UDP:

       ```
       > *.*<space/tab>@<eventloganalyzer_server_name>:<port_no>
       ```

   - **rsyslogd**
     - File path: /etc/rsyslog.conf
     - UDP:

       ```
       > *.*<space/tab>@<eventloganalyzer_server_name>:<port_no>
       ```

     - TCP:

       ```
       > *.*<space/tab>@@<eventloganalyzer_server_name>:<port_no>
       ```

     - TLS:

       Note: Please check the prerequisites before appending the entries mentioned

       ```
       > $DefaultNetstreamDriverCAFile <CACertificate>
         $ActionSendStreamDriver gtls
         $ActionSendStreamDriverMode 1
         $ActionSendStreamDriverAuthMode x509/name
         $ActionSendStreamDriverPermittedPeer <commonname>
         *.*<space/tab>@@<eventloganalyzer_server_name>:<port_no>
       ```

   - **syslog-ng**
     - File path: /etc/syslog-ng/syslog-ng.conf
     - <source_name> can be found from existing configuration of source with system(); and internal(); calls in the syslog-ng.conf file

       For ex: Here the <source_name> should be "**s_src**"

       source s_src {

       system();

       internal();

       };
     - UDP:

```
>
destination d_eventloganalyzer { network(<eventloganalyzer_server_name> port(<port>) transport("udp")); };
log { source(<source_name>); destination(d_eventloganalyzer); };
```

- TCP:

```
>
destination d_eventloganalyzer { network(<eventloganalyzer_server_name> port(<port>) transport("tcp")); };
log { source(<source_name>); destination(d_eventloganalyzer); };
```

- TLS:

Note: Please check the prerequisites before appending the entries mentioned

```
>
destination d_eventloganalyzer { network(<eventloganalyzer_server_name> port(<port>) transport("tls") tls(key-file("/path/to/private.key") cert-file("/path/to/certificate.crt") ca-dir("/path/to/ca/directo
log { source(<source_name>); destination(d_eventloganalyzer); };
```

2. Save the configuration and **restart** the Syslog daemon using the below command

```
> service <syslog/rsyslog/syslog-ng> restart
```

or

```
> systemctl restart <syslog/rsyslog/syslog-ng>
```

Note:
The above configuration will only enable forwarding the machine logs to the EventLog Analyzer server.

To configure auto log forwarding from EventLogAnalyzer server using sudo or non sudo user, refer here.

Prerequisites:

- Enable HTTPS and configure a valid certificate in server.xml. Click here to know how to configure a valid SSL certificate.
- Only pfx format is supported for storing certificate, if you use keystore format, please convert it to pfx.

Using self-signed certificates:

- After applying a self-signed certificate, a file named **ca.crt** will be created in the location **<EventLogAnalyzer_Home>/Certificates**.
- Use this file as the root certificate while configuring log forwarding in clients.

Using other certificates:

- For configuring log forwarding, get the root certificate from the certificate vendor.

Note:

1. If you want to use a different port other than the default ports as specified above, please specify it in the port management settings.
2. The CommonName should be the same value as given in the certificate file.

Forwarding application/audit logs to the EventLog Analyzer Server

If any particular applications' logs or audit logs needs to be forwarded, then the following configurations needs to be done in Linux devices under **rsyslog.conf** (or) **syslog.conf**

1. Under the MODULES section, check whether the "$ModLoad imfile" is included. (This module "imfile" converts any input text file into a syslog message,which can then be forwarded to the EventLog Analyzer Server.)
2. The following directives contain the details of the external log file:
   $InputFileName **<Monitored_File_Absolute_Path>**
   $InputFileStateFile **<State_Filename>**
   $InputFileSeverity **<Severity >**
   $InputFileFacility **<Facility >**
   $InputRunFileMonitor
3. To forward the logs we must provide this line: **<Facility>.<Severity> @Host-Ip:Port**

Example:

$InputFileName /var/log/sample.log

$InputFileStateFile sample

$InputFileSeverity info

$InputFileFacility local6

local6.info @eventloganalyzer-Server:514

Here **/var/log/sample.log** is the external file to be forwarded.

> **Note:**
> 1. These instructions can be applied to all Linux devices.
> 2. Please use a unique **<State_Filename>** for different **<Monitored_File_Absolute_Path>**.
> 3. When forwarding audit logs, sometimes default policies in Red Hat systems with Security enhancement (SElinux) won't allow the audit logs to be read. Refer troubleshooting tips.

Syntax for Installing Packages:

- For CentOS/RHEL:

```
> yum install <package_name>
```

- For Ubuntu:

```
> apt-get install <package_name>
```

- For other Linux distros kindly refer the official website for package installation.

> **Important Note:** The below privileges are specific to an individual user.

Auto Log Forwarding Privileges for Sudo and Non-Sudo User:

Granting privileges to the rsyslog.conf [or] syslog.conf file.

```
> setfacl -m u:<username>:rw /etc/rsyslog.conf [or] /etc/syslog.conf
```

Example:

syslog.conf: setfacl -m u:**testuser**:rw /etc/syslog.conf

rsyslog.conf: setfacl -m u:**testuser**:rw /etc/rsyslog.conf

Please follow the instructions below to give restart privilege for the syslog/rsyslog service for non-sudo user:

- Use the root user for configuring the privileges.
- **Please execute the below command:**

```
> visudo -f /etc/sudoers.d/<username>
```

- **Add the below line to the sudoers file:**

```
> <username> ALL=NOPASSWD: /usr/sbin/service <syslog/rsyslog> restart
```

  Example:
  - visudo -f /etc/sudoers.d/testuser
  - testuser ALL=NOPASSWD: /usr/sbin/service rsyslog restart

- **To verify, follow the below command**

```
> cat /etc/sudoers.d/<username>
```

Example: cat /etc/sudoers.d/testuser

Expected Output: testuser ALL=NOPASSWD: /usr/sbin/service rsyslog restart

Note: The acl package must be installed. Before that the filesystem is mounted with the acl support. For more details, kindly refer the official documentation [ref].

4.11.2. Configuring the Syslog Service on a Mac OS devices

1. Login as root user and edit the **syslog.conf** file in the **/etc** directory.
2. Append ***.*<tab>@<server_IP>** at the end, where **<server_IP>** is the IP Address of the machine on which EventLog Analyzer is running.

   > **Note**: Ensure that the EventLog Analyzer server IP address is reachable from the MAC OS device.

3. Save the file and exit the editor.
4. Execute the below commands to restart the syslog device:

$ sudo launchctl unload /System/Library/LaunchDaemons/com.apple.syslogd.plist

$ sudo launchctl load /System/Library/LaunchDaemons/com.apple.syslogd.plist

> **Note**: TLS option is not available for Syslog.

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

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**

4.11.4. Configuring the Syslog Service on VMware

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:

- On ESXi devices, you can use the vSphere Client or the vSphere CLI command vicfg-syslog to configure the following options:
  1. **Log file path**: Specifies a datastore path to the file where syslogd logs all messages.
  2. **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.
  3. **Remote port**: Specifies the port used by the remote host to receive syslog messages.
- **Configuration using vSphere CLI command**: For more information on vicfg-syslog, refer the vSphere Command-Line Interface Installation and Reference Guide.
- **Configuration using vSphere Client**:
  1. In the vSphere Client inventory, click on the host.
  2. Click the **Configuration** tab.
  3. Click **Advanced Settings** under **Software**.
  4. Select **Syslog** in the tree control.
  5. 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.
  6. 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.
  7. 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.
  8. Click **OK**.

4.11.5. Configuring the Syslog Service on Arista Switches

1. Login to the Arista Switch
2. Go to the **config** mode.
3. Configure the Switch as below to send the logs to the Eventlog Analyzer Server
    - Arista# **config terminal**
    - Arista(config)# **logging host < Eventlog_Server_Ip > < port_number > protocol [tcp/udp]**
    - Arista(config)# **logging trap information**
    - Arista(config)# **copy running-config startup-config**

To configure command executed logs:

- Arista (config)# **aaa accounting commands all console start-stop logging**
- Arista (config)# **aaa accounting commands all default start-stop logging**
- Arista (config)# **aaa accounting exec console start-stop logging**
- Arista (config)# **aaa accounting exec default start-stop logging**
- Arista (config)# **copy running-config startup-config**

To configure logon logs:

- Arista (config)# **aaa authentication policy on-success log**
- Arista (config)# **aaa authentication policy on-failure log**
- Arista (config)# **copy running-config startup-config**

4.11.6. Configuring the Syslog Service on Cisco Switches

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:

   ```
   > Catalyst6500(config)# logging facility local7
     Catalyst6500(config)# logging trap notifications
   ```

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.

4.11.7. Configuring the Syslog Service on HP Switches

1. Login to the switch.
2. Enter the following commands.

   HpSwitch# **configure terminal**

   HpSwitch(config)# **logging severity debug**

   HpSwitch(config)# **logging <ELA IP_ADDRESS>**

4.11.8. Configuring the Syslog Service on Cisco devices

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

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**

4.11.9. Configuring the Syslog Service on Cisco Firepower devices

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.

4.11.10. Configuring the Syslog Service on SonicWall devices

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.

4.11.11. Configuring the Syslog Service on Juniper devices

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

4.11.12. Configuring the Syslog Service on PaloAlto devices

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"

4.11.13. Configuring the Syslog Service on Fortinet devices

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**:

```
> config system syslog
  edit "syslog server name"
  set ip "EventLog Analyzer IP Address"
  set port 514
  next
  end
```

3. Use the following CLI commands to send Fortinet logs to the Eventlog Analyzer server.

```
> config system locallog syslogd setting
  set severity debug
  set facility local7
  set status enable
  set syslog-name <syslog server name set in above step>
  end
```

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.

4.11.14. Configuring the Syslog Service on Check Point devices

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**.

4.11.15. Configuring the Syslog Service on NetScreen devices

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:

Execute the following commands:

```
> Netscreen > set syslog config <ip address> facilitates local0 local0
  Netscreen > set syslog config <ip address> port 514
  Netscreen > set syslog config <ip address> log all
  Netscreen > set syslog enable
```

4.11.16. Configuring the Syslog Service on WatchGuard devices

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**

4.11.17. Configuring the Syslog Service on Sophos devices

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.

4.11.18. Configuring the Syslog Service on Cyberoam devices

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

Enabling Cyberoam Syslog:

1. Login to Cyberoam as administrator.
2. Navigate to **Logs & Reports > Configuration > Syslog Server > 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: < Cyberoam Standard Format >
4. Click on **Save**
5. Navigate to **Logs & Reports > Configuration > Log Settings>** select the logs that has to be sent to the EventLog Analyzer Server.

4.11.19. Configuring the Syslog Service on Barracuda devices

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**.

4.11.20. Configuring the Syslog Service on Barracuda Web Application Firewall

The Barracuda web application can be configured by following these steps:

1. Navigate to **ADVANCED > Export Logs** > **Add Export Log Server**
2. In the **Add Export Log Server**, enter the following details, and click **OK**
    - Name: Enter a name for the EventLog Analyzer Server
    - IP Address or Hostname: Enter the IP address or the hostname of the EventLog Analyzer server
    - Port: Enter the port associated with the IP address of the EventLog Analyzer server (513,514)
    - Log Timestamp and Hostname: Enable to send log with date and time of the event

4.11.21. Configuring the Syslog Service on Barracuda Email Security Gateway

The Barracuda email security gateway application can be configured by following these steps:

1. To configure the email Syslog, using the Barracuda Email Security Gateway Web interface, navigate to the **ADVANCED > Advanced Networking**
2. Enter the IP address of the EventLog Analyzer server to which syslog data related to mail flow should be sent.
3. Specify the protocol TCP or UDP, and also port (513,514) over which syslog data should be transmitted.

4.11.22. Configuring the Syslog Service on Huawei Firewall devices

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.

4.11.23. Configuring the Syslog Service on Malwarebytes devices

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.

4.11.24. Configuring the Syslog Service on Meraki devices

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.**

4.11.25. Configuring the Syslog Service on FireEye devices

1. Login to the FireEye device as an **administrato**r.
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.**

4.11.26. Configuring the Syslog Service on pfSense devices

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**.

4.11.27. Configuring the Syslog Service on Symantec DLP devices

1. Locate and open the c**onfig\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.

4.11.28. Configuring the Syslog Service on Symantec Endpoint Protection devices

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**.

4.11.29. Configuring the Syslog Service on H3C devices

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.

4.11.30. Configuration the Syslog service on Stormshield firewall

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**.

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

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.
     - 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**.

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

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:
     1. Hostname <EventLog Analyzer IP>
     2. UDP port <default 514>
     3. Syslog Format <CEF>
     4. 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:
     1. Hostname <EventLog Analyzer IP>
     2. UDP port <default 514>
     3. Syslog Format <CEF>
     4. 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**

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**.

4.11.33. Adding Forcepoint devices to EventLog Analyzer

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 to

   Configuration > 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 to

   Configuration > 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.

4.11.34. Adding Dell switches to EventLog Analyzer

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.

4.11.35. Configuring the Syslog Service on the Esxi 7

1. Enable the firewall rule to allow syslog
2. Execute the command lines below one by one:
    - loghost='udp://<eventloganalyzer_server_name>:<port_no>'
    - esxcli system auditrecords remote enable
    - esxcli system syslog reload

Note: In order to confirm that the configuration was successful,

- Open **\etc\Vmsyslog.conf** and check the loghost parameter

4.11.36. Configuring the Syslog Service on Sangfor devices

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

1. Access the NGAF Web Interface.

   Open a web browser and navigate to the NGAF's management IP address. Login using your administrator credentials.

2. Navigate to System > Logging Options
3. Check all Syslog checkboxes under Log Location for the type of logs to be forwarded.

4. 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.
5. Click OK to apply changes.

For NGAF version 6.4 and below:

1. Access the NGAF Web Interface.

   Open a web browser and navigate to the NGAF's management IP address. Login using your administrator credentials.

2. Navigate to System > Logging Options > Syslog
3. Check **Enable Syslog** checkbox.

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

5. 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.

   Open a web browser and navigate to the IAM's management IP address. Login using your administrator credentials

2. Navigate to System > General> Advanced > Syslog Server.

3. Check the **Enable Syslog Server** checkbox.
4. 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
5. Click Commit to apply changes.

4.11.37. Configuring the Syslog Service on Topsec devices

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

4.11.38. Enabling Stackato Logging

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.

4.11.39. Configuring Zscaler NSS

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.

5.1. User Interface Tabs

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

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.

5.2. Dashboard Views

EventLog Analyzer has a near real-time dashboard that presents security related data in the form of graphs and charts. The dashboard helps you discern anomalies quickly, investigate threats and attack patterns, and get insights from log trends. This dashboard is customizable.

Dashboard tabs:

The EventLog Analyzer dashboard comes with the following default subtabs:

- Events Overview
- Network Overview
- Security Overview

Each tab consists of numerous widgets.

Events Overview

This tab presents an overview of various security events monitored by EventLog Analyzer. The widgets in this dashboard provide insights on the various critical events generated in the network during 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 EventLog Analyzer during the given time frame.	
Windows Events	This widget presents the total number of Windows-based events collected by EventLog Analyzer during the chosen time frame. In addition to that, the pie chart splits the windows events in to 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 during 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	

The Events Overview tab also has the following widgets:

Widget Name	Function	Widget image
Logs Trend	This widget presents a time-based log count trend of all events/logs ingested into EventLog Analyzer. 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.	
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 EventLog Analyzer by generating graphical reports. The widgets in this dashboard provide insights on the various critical events generated in the network during 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 EventLog Analyzer during 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 during the specified time period.	
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 during the specified time period.	
Network Devices	This widget provides a total count of network devices that are added for monitoring.	

The Network Overview tab also has the following widgets:

Widget Name	Function	Widget image
Traffic Trend	This widget presents a 3D graph that shows a time based trend of allowed traffic and blocked traffic. The X-axis represents the time range. It will be based on the calendar range you choose. If the calendar range is less than 24 hours, then this will show hourly ranges. If it is less than 1 hour, it will show 1 minute ranges. If it is less than 30 days, it will show 1 day ranges. If it is more than 30 days, it will show 1 month ranges. The Y-axis represents the Event Count.	
Top Network Devices Based On Traffic	This widget displays the top 10 network devices based on the log count. Each row is further split into allowed traffic and blocked traffic.	
Top 5 Denied Connections by Source	This widget displays the top 5 sources for which connections were denied.	
Recent Interface Status Changes	This widget shows the recent interface status for each interface in each network device. The red downwards arrow indicates that the interface is down. The green upwards arrow indicates that the interface is up.	
Top Websites Accessed	This widget categorizes the top 10 websites accessed based on the number of times the site was accessed.	
Top VPN Logons by User	This widget lists the top 10 users based on VPN logons.	

Security Overview

This tab provides an overview of the key security events monitored by EventLog Analyzer. The widgets in this dashboard provide insights on the various critical events generated in the network during 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 EventLog Analyzer's correlation engine.	
Threats Detected	This widget presents the total number of threats detected during the chosen time frame from the Threat Sources (such as Symantec, McAfee, Malwarebytes etc) added in the EventLog Analyzer.	
Vulnerabilities	This widget displays the total number of vulnerabilities detected by the vulnerability scanner(s) whose data are being imported into EventLog Analyzer.	
IDS/IPS	This widget presents the total count of IDS/IPS events during the chosen time frame.	
Threats detected by Advanced Threat Analytics	This widget displays the count of threats detected by "Advanced Threat Analytics" feature in EventLog Analyzer.	

The Security Overview tab also has the following widgets:

Widget Name	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 3D 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.	

In addition to the above, predefined templates are also available for dedicated monitoring of Cisco, IIS and SQL Server Devices.

5.3. Customizing Dashboard Views

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.

To edit dashboard profiles, click here.

To customize the dashboard according to your preferences, the following options are available to you:

Adding a new tab to the dashboard

To add a new tab to the dashboard,

- In EventLog Analyzer's dashboard, click the icon on the top-right corner and select **Add Tab**.

- In the pop-up box that appears, you can see the following:
  1. Three default tabs: Events Overview, Network Overview, and Security Overview
  2. Three predefined templates: Cisco Overview, IIS Overview, and SQL Server Overview
  3. Add Custom Tab option
- Click **Add Custom Tab**. Enter a name for the tab in the given field and click **Add**.
- Navigate to the new tab in your dashboard and click **Add Widget** to start adding widgets of your choice.

> If you want to add an existing report as a widget, click here to know how.

Adding a new widget to a tab

To add a new widget,

- In EventLog Analyzer's dashboard, navigate to the tab to which you want to add a new widget and click the icon on the top-right corner.
- Click **Add Widget**. In the pop-up box that appears, select the widget, widget type, chart type, chart color, and enter a display name for the widget.

- Once you've entered all the details, click **Add**.

> You also have the option of **pinning a report as a new widget**. To know how, click here.

Deleting and reordering tabs in the dashboard

To delete tabs from the dashboard,

- In EventLog Analyzer's dashboard, click the icon on the top-right corner and click **Manage Tabs.**

- In the **Manage Tab** dialog box that appears, click the icon corresponding to that tab that you want to delete.
- In the pop-up confirmation box, click **Yes** to complete the deletion of the tab

To edit the order of tabs in the dashboard,

- In EventLog Analyzer's dashboard, click the icon on the top-right corner and click **Manage Tabs.**
- Click the icon and drag and drop the tabs in the order of your choice.

Reordering and resizing widgets

To reorder the widgets in a tab,

- In EventLog Analyzer's dashboard, navigate to the tab whose widgets you want to reorder, click the icon on the top-right corner and click **Reorder Widgets.**
- Click and drag the widgets wherever you want to place them.
- You can also resize widgets by dragging them from their bottom-right corner and adjusting their sizes as required.
- Click on the Save button present on the top-right corner.

Editing and deleting widgets

To edit a widget in a tab,

- In EventLog Analyzer's dashboard, click the icon corresponding to the widget that you want to edit.
- Select **Edit Widget**. Update the necessary information and click **Update**.

To delete a widget from a tab,

- In EventLog Analyzer's dashboard, click the icon corresponding to the widget that you want to delete.
- Select **Delete Widget** and click **Yes** in the pop-up box that appears.

Viewing the dashboard in full screen mode

To view the dashboard in full screen,

- In EventLog Analyzer's dashboard, click the icon on the top-right corner.

- In the full screen view, you can view a slideshow of the tabs by clicking the play icon located at the top of the screen.
- You can switch to different tabs by clicking on the drop-down button located at the top of the screen.
- You can also remove a particular tab from the slideshow by clicking the toggle button next to the name of the tab in the drop-down list.
- You can also switch to dark mode by clicking the toggle button at the top-right corner of the screen.
- To go back to the normal viewing mode, click the icon.

Viewing a widget in full screen mode

To view a widget in full screen, in EventLog Analyzer's dashboard, click the icon on the top-right corner of the widget you want to view.

Refreshing the dashboard and widgets

To refresh the dashboard, in EventLog Analyzer's dashboard, click the icon on the top-right corner of the screen.

To refresh a particular widget, in EventLog Analyzer's dashboard, click the icon on the top-right corner of the widget.

Changing refresh interval

To change the time interval for the automatic refreshing of the dashboard,

- In EventLog Analyzer's dashboard, click the icon on the top-right corner and click **Refresh Interval**.
- In the pop-up box that appears, select the refresh interval—Never, 30 Secs, 1 Min, 5 Mins, 10 Mins, and 1 Hr.

> **Note**: If you choose **Never** for the refresh interval, the dashboard will never be refreshed automatically. You will have to refresh it manually.

Check out our video for a step by step demonstration of customizing the EventLog Analyzer dashboard here.

Configuring the Embed Dashboard

The Embed Dashboard enhances data sharing by enabling the creation of external share links for specific tabs or widgets. This allows precise and targeted data access within a dashboard, facilitating focused collaboration and streamlined decision-making across various platforms. The Embedded Dashboard feature allows users to create an External Share Link for a particular tab or a specific widget within the dashboard.

To embed a widget,

In EventLog Analyzer dashboard, click the ⋮ icon corresponding to the widget that you want to embed.

- Click on the **Embed Widget** option.
- Provide a unique **Link Name**.
- Choose the desired **Time Range** from the drop-down menu.
- Provide the Refresh Time (to be set between 60-1440 minutes) and **Set Expiry** (to be within 1-365 days) from the options provided in the drop-down menu.

The embed widget link is now successfully created.

NOTE:

- The embed widget will be automatically refreshed at the specified interval.
- The generated external share link is only valid till the expiry date.

To manage embed links,

In the EventLog Analyzer dashboard, click the icon on the top-right corner and select **Manage Embed Links**.

- This will display a table containing all the Active Dashboard Links.

- To edit a specific link, locate the desired entry and click the **Edit** option associated with it.

- A window will appear allowing you to modify the properties of the chosen link. Make the necessary changes.

- Once finished, click **Save** to confirm the updated properties for the Active Dashboard Link.

5.4. Log Receiver

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)

Fig 1 EventLog Analyzer- Log Receiver

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.

Fig 2 Syslog Viewer Tab

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)

Fig 3 Server Tab

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

5.5. Global Search

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.

6.1. EventLog Analyzer 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.

6.2. Setting up Windows Event Log Reports

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. These reports 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 learn how 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 **Audit policies** 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 on the left 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\Channels\Microsoft-Windows-AppLocker/EXE and DLL**, and create an expandable string value with name **File**. Use the copied log path 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 be collected. > auditpol.exe /set /subcategory:"MPSSVC rule-level policy change,Filtering Platform policy change" /success:enable /failure:enable > auditpol.exe /set /subcategory:"IPsec Main Mode,IPsec Quick Mode,IPsec Extended Mode" /success:enable /failure:enable > auditpol.exe /set /subcategory:"IPsec Driver,Other system events" /success:enable /failure:enable > auditpol.exe /set /subcategory:"Filtering Platform packet drop,Filtering Platform packet drop" /success:enable /failure:enable
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** registry key namec as **HotPlugSecureOpen** and set value as **1**.

Registry changes		Enable **Audit Registry**, under **Advanced Audit Policy Configuration > Object Access**.	Set SACL for the registry key by right-clicking on the required registry and navigating to **Permission > Advance > Auditing in Registry Editor**.
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 Configuration Repor**
Print service	• Microsoft-Windows-PrintService/Operational • Microsoft-Windows-PrintService/Admin	No modification required.	
Terminal	• Microsoft-Windows-TerminalServices-Gateway/Operational	No modification required.	

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

6.3. Manage Predefined Reports

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.

EventLog Analyzer
Dashboard
Reports
Compliance
Search
Correlation
Alerts
Settings
LogMe
Support
IIS W3C Web Server

6.4. Manage Report Views

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.

6.5. Custom Reports

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.

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.

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.

EventLog Analyzer
Dashboard
Reports
Compliance
Search
Correlation
Alerts
Settings
LogMe
Support
Custom Reports
Multi report
Export As
Schedule Reports
Select Device
Period
Report Name
Count
Action
All Events
Success Events
All Events
User Logoffs
SU Logoffs
Logons
Failed logons
SSH logons
View Report

6.6. Schedule Reports

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.

6.7. Adding reports to the Favorites section

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.

6.8.1. List of Network Device Event Reports

Apart from servers, applications and workstations, enterprise networks also consists of various perimeter networking devices such as routers and switches. It is important to monitor these devices to gain visibility into who is entering and leaving your network.

For instance, a misconfigured router, switch, or firewall can lead to the entry of malicious traffic. Monitoring network activity along with the changes in perimeter network devices can spot and help seal such loopholes.

EventLog Analyzer helps you collect, analyze, and conduct forensic investigation on perimeter devices' log data.

This solution offers built-in support for different types of networking and security devices such as routers, switches, intrusion detection and prevention systems, and firewalls.

Some important report categories are mentioned below.

Router Logon Reports

These reports provide insights into events such as successful logons, failed logons, VPN logons, etc.

Router Configuration Reports

These reports ensure that all the changes made to your network's configuration are authorized and don't create any loopholes in your network security.

Router/Switch System Events

The reports in this category provide critical insights into the key events taking place in your routers and switches such as the commands executed, the fan status, the system temperature, etc.

Router Traffic Errors

Keep track of router transmission errors such as occurrences of too many fragments, fragment overlap, or invalid fragment length.

IDS/IPS Activity

The reports in this category help you to understand what type of attacks your network is susceptible to, which network devices need to be secured further, how to decide which malicious traffic sources to target, and more.

Firewall Threats

These reports give detailed information on possible security threats to the network.

Firewall Traffic Reports

These reports provide insights into the allowed and denied traffic with details on the source, destination, port, and protocol.

Firewall Logon Reports

With these reports, you can monitor the successful and failed firewall logons.

6.8.2. List of Windows Event Reports

EventLog Analyzer offers a range of reports for the Windows environment that can aid in granular monitoring and auditing of events. It also contains reports on attacks common to Windows devices. The moment an a suspicious event is detected, an alert notification will be sent via email or SMS. The following are the report groups for Windows devices.

Windows Event Reports

Windows Firewall Auditing

Reports on the common attacks that can be detected by monitoring events in the Windows Firewall will be listed here.

- **Spoof Attack** - A malicious entity poses as a legitimate user to compromise a system.
- **Internet Protocol half-scan attack** - The attacker attempts to scan for open ports by requesting ACK packets to launch an attack.
- **Flood Attack** - This is a DDoS attack where the attacker initiates multiple connections without finalizing any connection.
- **Ping of Death Attack** - A DDoS attack where malicious actors try to disrupt a server by sending abnormally large packets.
- **SYN Attack** - An attacker attempts to flood all the open ports of a server at the same time to launch an attack.

Threat Detection

This section contains reports on some common threats to the Windows environment which can aid in the detection, analysis, and forensic investigation of vulnerabilities. The attacks in this category are primarily focused on weakening the defenses of a system. Conducting a deeper analysis of the threats captured in these reports can help prevent an attack at a later stage.

- **DoS Attack Subsided** - Possible denial of service attack that have ended.
- **DoS Attack Entered Defensive Mode** - This report is generated when the Windows Filtering Platform has discovered a potential DoS attack and entered into a defensive mode.
- **DoS Attacks** - This report captures information on the denial of service attacks in a system where legitimate users will be deprived of a service due to a high volume of malicious traffic.
- **Downgrade Attacks** - This report captures instances of Downgrade Attacks. In this attack, advanced security features of a system will be downgraded to adopt older legacy security features thereby making it vulnerable to attacks.
- **Replay Attack** - This report captures instance of legitimate data or requests that are captured and replayed by an attacker to bypass authentication or for other malicious purposes.
- **Defender Malware Detection** - Instances of malware detection in Windows defender will be listed in this report.
- **Defender Real Time Protection Detection** - This report contains information on anti-virus data from Windows Defender.
- **Terminal Server Attacks** - This report captures data on attacks to the terminal. server that enables multiple clients in a network to communicate.
- **Terminal Server Exceeds Maximum Logon Attempts** - Information of multiple failed logon attempts in the terminal server will be available here.
- **IP Conflicts** - If more than more than one host is assigned the same IP address, an IP conflict that inhibits communication between hosts will occur.The information on such IP conflicts in a network will be listed here.

- **User Account Locked Out Error** - Instances of user account lockouts will be listed here. This report will aid in the investigation of the probable cause leading up to the account lockout.

Application Whitelisting

Reports on whitelisted and blocked EXE, DLL, and MSI files or automated scripts are listed here.

- **EXE or DLL File Allowed to Run** - This event is generated when certain apps blocked by the organization are allowed to run.
- **EXE or DLL Files Not Allowed to Run due to Enforced rules** -This event is generated when certain apps are not allowed to run due to enforced rules.
- **EXE or DLL File Not Allowed to Run** - This event is generated when certain apps blocked by the organization is not run.
- **MSI or Script File Allowed to Run** -This event is generated when certain scripts or MSI files blocked by the organization are allowed to run.
- **MSI or Script Files Not Allowed to Run due to Enforced rules** - This event is generated when certain scripts or MSI files are blocked due to enforced rules.
- **MSI or Script File Not Allowed to Run** - This event is generated when MSI files or automated scripts blocked by the organization are not allowed to run in a system.
- **Software Restricted to Access Program** - Any software that is restricted from making changes to systems or files.

Domain Events

Reports on crucial Active Directory events will be listed here. Monitoring these critical changes is essential to ensure that the security features in Active Directory have not been compromised or downgraded.

- **Special groups assigned to new logon** - This report captures instances of logons to special groups designated by the administrators.
- **SID History added to account** - If a user is migrated to a new domain, the security identifier history will be added to the new domain. This report essentially helps in tracking users across domains by recording instances where SID history has been added to an account.
- **Failed SID History addition** - Instances of failed additions of SID history to a user account will be listed here.
- **Kerberos policy changes** - This report will contain a history of policy changes made to the Kerberos authentication protocol in a network. Monitoring these policy changes is essential to ensure that authentication standards in a network are not downgraded.
- **Special groups logon table modifications** - This report captures all instances of modifications to special groups.

Application Crashes

This report group helps monitor issues related to performance of applications installed in Windows devices.

- **Application Errors** - This report captures instances of errors in the loading of applications installed in Windows devices.
- **Application Hanged** - This report captures instances of applications hanging in Windows devices.
- **Windows Error Reporting** - This report will have information on the frequently occurring errors in Windows devices.
- **Blue Screen Error (BSOD)** - This report contains instances of blue screen errors in Windows devices.

- **System Errors** - This report contains reports of the system errors in Windows devices.
- **EMET Logs** - Information from Microsoft Enhanced Mitigation Experience Toolkit will be available in this report.
- **Windows File Protection** - This report captures instances of attempts to replace critical Windows system files.

Threat Detection From Antivirus

EventLog Analyzer can collect log data from antivirus solutions such as Kaspersky, Sophos, and McAfee. The reports in this category give an overview of all the threats detected by these solutions.

- Threats Detections by ESET Endpoint Antivirus
- Threats Detections by Kaspersky
- Threats Detection by Microsoft Antimalware
- Threats Detection by Sophos Anti-Virus
- Threats Detection by Norton Anti Virus
- Infected files detected by Symantec Endpoint Protection
- Threat Detections by McAfee
- Defender Malware Detection
- Defender Real Time Protection Detection

Registry Changes

This report group helps in monitoring the Windows registry changes, and records attempts to modify it.

- **Registry Accessed** - A record of all attempts to access the Windows registry.
- **Failed Registry Access** - This report has a record of failed attempts to access the Windows registry.
- **Registry Created** - This report will contain a record of all newly created registry keys.
- **Failed registry Creations** - This report will contain a record of all failed attempts to create registry keys.
- **Registry Value Modified** - This report captures the changes made to Registry values.
- **Failed Registry Modifications** - This report captures all failed attempts to modify Registry values.
- **Registry Deleted** - A record of deleted Registry keys will be available in this report.
- **Failed Registry Deletions** - A record of failed attempts to delete Registry values will be available in this report.
- **Registry Permission Changes** - All instances of a change in Registry Permissions will be listed here.
- **Top Users on Registry** - A list of users who access the Registry the most will be listed here. This report can help flag suspicious users.

Removable Disk Auditing

This report group gives an overview of removable disk activity in Windows devices. This also includes instances of USB or removable disks that have been plugged in and removed even if no files are copied.

- USB Plugged In
- USB Plugged Out
- Removable Disk Reads
- Removable Disk Failed Reads
- Removable Disk Creates
- Removable Disk Failed Creates

- Removable Disk Modifications
- Removable Disk Failed Modifications
- Removable Disk Deletes
- Removable Disk Failed Deletes
- Device Based Removable Disk Changes
- Top Successful Users on Removable Disk Auditing
- Top Failed Users on Removable Disk Auditing
- Removable Disk Changes Trend

Windows Startup Events

This report group provides an overview of Windows System Events such as start-up, shut-downs, and restarts.

- Windows Startups
- Windows Shutdowns
- Windows Restarts
- Unexpected Shutdown
- System Uptime
- Windows Startup and Windows ShutDown

Service Audit

These reports help you track all the services installed in your Windows devices.

- New Service Installed
- Service Started
- Service Stopped
- Service Failed

Program Inventory

These reports provide information on software, services, or updates that happen in your Windows environment.

- Software Installed
- Software Updated
- Failed software installations
- Failed software installations due to privilege mismatches
- Software Uninstalled
- Windows Updates - Installed
- Windows update process failed
- Failed hot patching
- Update Packages Installed
- Non valid Windows license
- Failed Windows license activations
- Non activated windows products
- New kernel filter driver installed

Wireless Network Reports

These reports help you closely monitor your wireless network events.

- Wireless Network Authentication
- Wired Network Authentication
- Wired Network Connected
- Wired Network Disconnected
- Wireless Network Connected
- Wireless Network Disconnected

Eventlog Reports

These reports help you track the status of your event logging service in Windows devices.

- Audit Events Dropped
- Error in EventLog Service
- Event log automatic backup
- Security Log Full

Eventlog Reports

These reports capture instances of the logging service shut down to prevent recording logs of any change including malicious or inadvertent activity.

- Event Logging Service Shutdown
- Security Logs Cleared
- Event Logs Cleared

System Events

These reports can help you monitor some critical system events in your Windows infrastructure.

- Windows Time Change
- Windows Updates Installed
- AD Backup Error
- GPO Queries Failed
- Invalid Windows license
- Non activated Windows licenses
- Active Directory database corruptions
- Bad disk block
- Failed loadings of Kernel driver
- Code Integrity Check
- Invalid image hash file
- Invalid page hash image file
- Hard disk failures
- System Restored

Windows Event

This report group gives the overall trends in Windows reports based on all recorded events, important events, and user based events.

- All Events
- Important Events
- User Based Report

Trend Report

This report group gives an overview of the trends detected in the logs collected from Windows devices. This report group helps identify the events that are generated the most and the frequency of those events.

- Weekly Report
- Hourly Report

Windows Severity Reports

This report group gives an overview of the success, failure, information, and warning events in Windows devices.

- Success Events
- Information Events
- Failure Events
- Warning Events
- Error Events

Windows Backup and Restore

This report group gives an overview of all the backup and restoration events in Windows devices.

- Failed Windows backup
- Successful Windows backup
- Failed Windows restores
- Successful Windows restores
- System Restored

Windows Firewall Auditing

The Windows Firewall Auditing report group helps in auditing critical changes in Windows Firewall such as the addition, deletion, or modification of Firewall rules and settings.

- Rule Added
- Rule Modified
- Rule Deleted
- Settings Restored
- Settings Changed
- Group Policy Changes

Network Policy Server

This report group helps in the monitoring of the Network Policy server in Windows devices.

- Access granted to users
- Access denied to users
- Discarded requests for users
- Discarded accounting requests for users
- Locked users due to repeated logon failures
- NPS Unlocked user accounts

Data Theft Detection

This report group helps mitigate data theft with reports to monitor printer activity, removable disks, and databases.

- Printer Document Theft
- Removable Media Data Theft
- Shared Network Data Theft
- SQL Server Data Theft by Backups
- SQL Server Data Theft by Reads
- Oracle Data Theft by Reads
- Windows FTP Data Thefts
- Unix FTP Data Thefts

6.8.3. Unix Event Reports

EventLog Analyzer has a wide range of out-of-the-box reports and alert profiles for Unix devices. With these you can audit system events such as package installs and updates, track important events such as low disk space, and more. You can also audit critical events based on device, alert type, or severity. Apart from critical events, you can also track other events on your Unix systems such as cron jobs, session connections and disconnections, deactivated services, and more.

Unix Logon Reports

A record of different logon types specific to Unix devices such as SU, SSH, and FTP logons will be available here. In addition, the top logon reports classify these logons based on users, devices, remote devices, and method of logon. The logon trend report gives real-time insights on the general trend detected in Unix logons. This can help detect sharp deviations in general trend which could be indicative of malicious activity.

- User Logons
- SU Logons
- SSH Logons
- FTP or SFTP Logons
- Logons Overview
- Top logons based on users
- Top logons based on devices
- Top logons based on remote devices
- Top Unix Logon Method
- Logon Trend

Unix Logoff Reports

A record of different logoffs specific to Unix devices such as SU, SSH, FTP, and user logoffs will be available here. The Logoffs overview report gives real-time insights on the general trend.

- User Logoffs
- SU Logoffs
- SSH Logoffs
- FTP or SFTP Logoffs
- Logoffs Overview

Unix Failed Logon Reports

This report group can help in the monitoring of failed logons in any Unix device. The top failed reports based on users, devices, and remote devices will help identify an unusual number of logon failures which could be indicative of an attack. In addition, devices with repeated logon failures will be listed separately.

- User Failed Logons
- SU Failed Logons
- SSH Failed Logons
- FTP or SFTP Failed Logons

- Failed Logons Overview
- Top failed logons based on users
- Top failed logons based on devices
- Top Failed logons based on remote devices
- Top failed logon methods
- Failed Logon Trend
- Repeated authentication failures
- Invalid user login attempts
- Unsuccessful logon failures with long password
- Repeated login failures based on remote devices
- Repeated authentication failures based on remote devices

Unix User Account Management

This report group can help monitor critical changes to user accounts, groups, and passwords such as creations, deletions, modification of groups, user accounts, and passwords.

- Added user accounts
- Deleted user accounts
- Renamed user accounts
- Groups added
- Groups deleted
- Groups renamed
- Password Changes
- Failed password changes
- Failed user additions
- Top Unix Account Management Events

Unix Removable Disk Auditing

These reports can help track removable disk activity in Unix devices.

- USB Plugged In
- USB Plugged Out

SUDO Commands

The reports in this group can help ensure that security privileges of the super user are not misused.

- SUDO command executions
- Failed SUDO command executions
- Top SUDO command executions
- Top Failed SUDO command executions

Trend report

The reports in this group give an overview of the trend in activity in Unix devices.

- Weekly Report
- Hourly Report

Unix Mail Server Reports

These reports help in monitoring Unix mail servers. The 'Top' reports give the usage statistics of Unix mail servers. Reports to monitor mailbox usage, general trends, mail deliveries and the execution of commands are also available in this report group.

- Mails Sent Overview
- Mails Received Overview
- Top mails sent based on senders
- Top mails sent based on remote device
- Top mails received from remote devices
- Top Sender Domain
- Top Recipient Domain
- Trend report on mails sent
- Trend report on mails received
- Top mails rejected based on sender
- Top receivers who rejected the mails
- Top mail rejection errors
- Top Rejected Domains
- Mails rejected Overview
- Mailbox Unavailable
- Insufficient Storage
- Bad Sequence of Commands
- Bad Email Address
- Non existent email address on remote side
- Top Mail Errors
- Top mail errors based on senders
- Failed Mail Deliveries

Unix Threats

The reports in this group and their corresponding alert profiles help discover and mitigate some of the threats common to Unix devices.

- Reverse Lookup Errors
- Bad DeviceConfig Errors
- Bad ISP Errors
- Invalid connection remote device
- Denial of Service Attack

Unix NFS Events

These reports help monitor the storage of file in remote systems using the Network File Share (NFS) protocol.

- Successful NFS mounts
- Refused NFS Mounts
- Denied NFS mounts based on users
- Top Successful NFS mounts based on remote device
- Top Refused NFS mounts based on remote devices

Unix Other Events

This report group contains reports to monitor Unix events such as timed out or denied connections, failed updates, name and address mismatch errors for devices, and more. This group also contains reports to monitor cron jobs or the scheduling of commands to be executed later.

- Cron Jobs
- Cron Edit
- Cron Job Started
- Cron Job Terminated
- Connection aborted by a software
- Receive identification string
- Session Connected
- Session Disconnected
- Deactivated services
- Unsupported Protocol Version
- Timeout While Logging
- Failed Updates
- Device Name Mismatch Error
- Device Address Mismatch Error
- Top cron jobs based on users

Unix FTP Server Reports

This report group has a range of reports to monitor the usage of the File Transfer Protocol (FTP) in Unix devices. Monitoring this protocol is crucial for data security.

- File downloads
- File Uploads
- Data transfer stall timeouts
- Login Timeouts
- Session idle timeouts
- No transfer timeouts
- Connection timeouts
- FTP Reports Overview
- Top FTP operations based on user
- Top FTP operations based on remote device

Unix System Events

Crucial Unix system events such as Yum installs, stopping and restarting of the Syslog service, system shutdowns, and low disk space can be monitored with these reports.

- Syslog service stopped
- Syslog service restarted
- Low Diskspace
- System Shutdown
- Yum installs
- Yum updates
- Yum Uninstalls

Unix Severity Reports

This report group classifies and presents Unix events in eight different levels of severity. This classification can help prioritize events and alerts.

- Emergency Events
- Alert Events
- Critical Events
- Error Events
- Warning Events
- Notice Events
- Information Events
- Debug Events

Unix Critical Reports

This report group helps analyze critical events further based on the level, event, device, and also the general trends.

- Criticality level of events
- Critical reports based on event
- Critical events based on device
- Critical events based on remote device
- Critical events Trend
- Critical events Overview

VMWare Logons/Logoff

This report group helps in the monitoring of logons/logoffs of the virtual machines installed in Unix devices. The reports in this group categorize the events based on the type, status, and the number of events.

- User Logons
- SU Logons
- SSH Logons
- SFTP Logons
- Logons Overview

- Top logons based on user
- Top logons based on remote devices
- Failed Logon
- Failed SU Logon
- Failed SSH Logon
- Failed FTP or SFTP Logon
- Failed Logon Overview
- Top failed logons based on users
- Top failed logon based on remote devices
- User Logoff
- SU Logoff
- SSH Logoff
- SFTP Logoff
- Logoff Overview

VMWare System Events

The reports in this group deal with monitoring system events in the virtual machines installed in Unix devices. Creation and modification of user accounts, logging activity, disk space availability, and password changes can be tracked with these reports.

- User Account Added
- User Account Deleted
- User Account Renamed
- Group Added
- Group Deleted
- Groups Renamed
- Password Changes
- Password Change Failed
- User Addition Failed
- Syslog Service Stopped
- Syslog Service Restarted
- Low Diskspace
- System Shutdown

VMWare Server Events

Critical events specific to VMs such as creation, deletion, and the modification of VMs and guest logins can be monitored with these reports.

- Guest Login on VM
- VM Created
- VM Deleted
- VM State Changes

- Top VM Changes
- VM Events Overview

AS400 Reports

This report group contains reports to monitor changes in AS400 devices. All critical system changes, logon events, hardware errors, configuration changes and more can be tracked with this report.

- Logons
- Failed Logons
- Logoff
- Failed Authorization
- Authority changes
- User Profile changes
- Objects deleted
- Job changes
- Ownership changes
- Logon failure due to invalid passwords
- System value changes report
- Successful Job Start
- Successful Job End
- Job Logs
- Device Configuration
- System time changes
- Subsystem varied off workstation
- ASP storage threshold reached
- ASP storage limit exceeded
- Disk Unit Errors
- Expired system IDs report
- Unable to write audit record
- Disabled user profiles due to maximum number of sign-on attempts
- Report on weak battery
- Report on battery failures
- System password bypass period ended
- Storage directory threshold reached
- Report on serious storage conditions
- Report on battery cache expiry
- Report on i5 grace period expiry
- Temporary IO Processor errors
- System Processor Failure
- Hardware Errors
- Top logons based on users

- Top failed logons based on users
- Top jobs based on users

6.8.4. Reports for Applications

EventLog Analyzer has multiple report groups to track critical activity in Terminal servers, IIS Web Servers, SQL servers, and printers. The moment a suspicious event is detected, an alert notification will be sent via email or SMS. The following are the report groups available for applications.

Terminal Server Gateway Logons

These reports help in the monitoring of successful and failed connections in terminal servers. You can also track access to your critical resources using these reports.

- Successful user disconnections from the resource
- Successful user disconnections from the resource by administrators
- Successful user connections to the resource
- Failed user connections to the resource
- Successful connection authorizations
- Failed connection authorizations
- Successful resource authorizations
- Failed resource authorizations

Terminal Server Gateway Communications

These reports help in the monitoring of session activity in Terminal Servers.

- Top Byte transferred
- Top Byte received
- Top Session Duration
- Top activities based on events

Terminal Server Gateway Top Reports

These reports help determine which gateways, clients, and resources in your terminal servers have the highest usage.

- Top Gateway Users
- Top Clients
- Top Resources

DHCP Windows Based Server Reports

These reports help monitor all critical activities in your DHCP Windows based servers such as lease granted, denied, or released, DNS updates, and critical requests. Since DHCP server auditing reports can track client-server exchanges that occur when IP addresses are allotted, these reports can be essential in detecting suspicious network activity.

- Lease renewed by client
- Lease denied
- Lease Granted
- Lease Released
- Lease Expired

- Lease Deleted
- IP Found To Use in Network
- Pool Exhausted
- DNS Update Request
- DNS Update failed
- DNS update successful
- Unreachable domain
- BOOTP Lease Report
- Authorization succeeded
- Authorization failed
- Server found in domain
- Network failure
- DHCP Logging started
- DHCP Logging stopped
- DHCP logging paused due to low disk
- Critical Events Report
- Error Reports
- Warning Reports
- Top Clients
- Top Mac Address
- DHCP Reports Overview

DHCP Linux Based Server Reports

Each step in the exchange of client-server messages in DHCP Linux based servers can be viewed using these reports. With these you can get information on the most active IP addresses, MAC addresses, gateways, and operations with the top N reports.

The DHCP Linux overview report will summarize all DHCP log events.

- Discovers
- Offers
- Requests
- Acknowledges
- Releases
- Negative Acknowledges
- Abandoning IP
- Information Report
- DHCP Linux Overview
- Top Operation
- Top IP Address
- Top MAC Address
- Top Gateway

IIS FTP Server Reports

The IIS FTP Server reports can help you track user logons and logoffs, check what data is being shared, and also identify trends in the overall file sharing activity.

- Logons
- Failed Logons
- Login attempts
- File downloads
- File uploads
- Disconnects
- File Transfer Aborts
- File Deletions
- Make Directories
- Remove Directories
- Rename Operations
- List Directory Contents
- Password Changes
- Bad Sequence of Commands
- Successful Commands
- Command Syntax Errors
- Transfer Incomplete due to insufficient space
- Security Data Exchange
- Top File Types Downloaded
- Top File Types Uploaded
- Top Users
- Top Clients
- Top Methods
- Top Status
- FTP Reports Overview

IIS Web Server Error Reports

With these reports, you can detect the problems users might be facing on your website and closely track all error alerts.

- HTTP Status Success
- Failed User Authentication
- HTTP Bad Request
- HTTP Payment Required
- Site Access Denied
- Password Change
- HTTP Request URI Too Large
- HTTP Request Entity Too Large
- HTTP Expectation Failed

- HTTP Unsupported Media Type
- HTTP Locked Error
- HTTP Bad Gateway
- IP Address Rejected
- Read Access_Forbidden
- Write Access_Forbidden
- Service Unavailable
- Gateway Timeout
- UNC Authorization Failed
- Denied direct request to Global.asa
- IO Operation Aborted
- Web Server Restart
- Web Server Busy
- Information Reports
- Success Reports
- Redirection Reports
- Client Error Reports
- Server Error Reports

IIS Web Server Attack Reports

These reports can help you detect some of the most common and dangerous web server attacks instantly, including SQL injection attacks or denial of service attacks.

- SQL Injection reports
- Cross site scripting reports
- Malicious URL Requests
- Malicious File Executions
- cmd.exe and root.exe file executions
- xp_cmdshell executions
- Admin Resource Accesses
- Denied Directory listing
- DoS Attacks
- Directory Traversal
- Spam Mail Header

Apache Web Server Error Reports

This report group can help you track several common HTTP error codes. It also has consolidated reports for both client errors and server errors. These reports help you identify which errors are occurring most frequently in your Apache web servers.

- HTTP Status Success
- HTTP Bad Gateway

- HTTP Internal Server Error
- HTTP Gateway Timeout
- HTTP Request URI Too Large
- HTTP Unsupported Media Type
- HTTP Request Entity Too Large
- HTTP Forbidden
- HTTP Server Not Found
- HTTP Request Timeout
- HTTP Bad Request
- HTTP Unauthorized
- Information Reports
- Success Reports
- Redirection Reports
- Client Error Reports
- Server Error Reports

Apache Web Server Top Reports

These top reports can help you discover the most frequently occurring errors and rectify them. With these, you can also identify the most popular pages in your website and see who's accessing your site most often to get insights on user behavior.

- Top Visitors
- Top Users
- Top URL
- Top Browsers
- Top Errors
- Top Referrers
- Apache Server Trend
- Apache Reports Overview

Apache Web Server Attack Reports

These reports can help you detect some of the most common and dangerous attacks in Apache web servers such as SQL injection attacks or cross-site scripting errors.

- SQL Injection reports
- Cross site scripting reports
- Directory Traversal
- Malicious URL Request

SQL Server Advanced Auditing Reports

These reports assist database administrators in monitoring and tracking operational issues, unauthorized access to confidential data, and user permissions. Specifically, the **Logins Information Report** provides details on changes to login information, such as password alterations or updates to user and user group logins.

- Column Modified Report
- Last Login Time Report
- Logins Information Report
- Most Used Tables
- Table Update Report
- Index Information Report
- Server Information Report
- Waits Information
- List Of Blocked Processes
- Schema Change History
- Object Change History
- List Of Connected Applications
- Security Changes Report
- List Of Permissions
- Last Backup of Database
- Last DBCC Activity report

SQL Server DDL Auditing Reports

These reports help in monitoring and tracking structural changes within the database, including alterations to tables, views, procedures, triggers, schema, and other elements.

- Databases Created
- Databases Dropped
- Databases Altered
- Tables Created
- Tables Dropped
- Tables Altered
- Views Created
- Views Dropped
- Views Altered
- Stored Procedures Created
- Stored Procedures Dropped
- Stored Procedures Altered
- Index Created
- Index Dropped
- Index Altered
- Triggers Created
- Triggers Dropped
- Triggers Altered
- Schemas Created
- Schemas Altered

- Schemas Dropped
- DDL Events Summary

SQL Server DML Auditing Reports

The reports in this group can help you figure out when functional queries are executed, who executed them, and from where. You can also track activities such as data being viewed, updated, deleted, or new entries being added to your confidential data.

- Selected Tables
- Inserted Tables
- Updated Tables
- Deleted Tables
- Execute Command
- Receive Command
- Check reference command executed
- Jobs Added
- Jobs Updated
- Jobs Deleted
- DML Events Summary

SQL Server Logon/Logout Events

This report group provides comprehensive insights into SQL Server logon and logout activities. These reports are helpful for monitoring user activity, detecting security threats, optimizing resource usage, and ensuring compliance with access policies.

- Trusted Logons
- Non-Trusted Logons
- Top logons based on user
- Top logons based on remote devices
- Logons Trend
- Logout Accounts

SQL Server Failed Logon Events

This report group monitor failed logon attempts in SQL Server, identifying top failure logons by users and remote devices while tracking trends over time. It helps quickly detect security breaches and authentication issues for effective mitigation.

- Failed Logons
- Top failure logons based on users
- Top Failure Logons based on Remote Devices
- Failed Logons Trend

SQL Server Startup Shutdown events

This report group provides insights into SQL Server's startup and shutdown events. It helps administrators monitor server activity, assess performance, and ensure smooth server operations.

- Server Startups
- Server shutdowns
- Status Reports

Server Principal Changes

These reports can help you track create, update, and delete changes made to server principals.

- Login Created
- Login Dropped
- Login Altered
- Logins Enabled
- Logins Disabled
- Server roles Created
- Server roles Dropped
- Server roles Altered
- Credential Created
- Credential Dropped
- Credential Altered

SQL Server Database Principal Changes

These reports can help you track changes made to any Database Principals, Applications, and Database Roles.

- User Created
- User Dropped
- User Altered
- DataBase Role Created
- DataBase Role Dropped
- DataBase Role Altered
- Application Role Created
- Application Role Dropped
- Application Role Altered

SQL Server Password Changes

These reports help audit various methods of password changes within SQL Server.

- All Password Changes
- Own Password Changes
- Own Password Changes Failed
- Password Changes
- Password Changes Failed

- Password Reset
- Password Reset Failed
- Own password resets
- Own Password Reset Failed
- Logins Unlocked

SQL Server Audit Changes

These reports help audit the changes made to the Server audit or database audit configurations.

- Server Audits Created
- Server Audits Dropped
- Server audits Altered
- Server Audit Specifications Created
- Server Audit Specifications Dropped
- Server Audit Specifications Altered
- Database Audit Specifications Created
- Database Audit Specifications Dropped
- Database Audit Specifications Altered
- Audit Sessions Changed
- Audit Shutdown on Failure

SQL Server Backup and Restore Events

These reports offer insights into SQL Server backup and restore events. It enables administrators to effectively manage data protection, monitor backup activities, and ensure database reliability and recoverability.

- Database backup report
- Database Restore
- Database Backup Failed
- Transaction log backup report
- All Objects Backup Report

SQL Server Auditing Account Management

These reports can help you track changes made to any account with respect to the users, logons and logoffs, and passwords. You can also track the creation, deletion, or modification of privileged accounts to ensure that unauthorized privilege escalations don't take place. In addition, you can audit logon and logoff activities, and learn the reasons behind logon failures and instantly know when the password of a critical account gets changed, and more.

- User Created
- User Dropped
- User Altered
- Login Created
- Login Dropped
- Login Altered

- Database Role Created
- Database Role Dropped
- Database Role Altered
- Application Role Created
- Application Role Dropped
- Application Role Altered
- Credential Created
- Credential Dropped
- Credential Altered
- Own Password Changes
- Failed Own password changes
- Password changes
- Password changes Failed
- Password resets
- Password resets Failed
- Own password resets
- Failed Own password resets
- Unlocked accounts
- Enabled users
- Disabled users

SQL Server Auditing Server Reports

These reports help audit MS SQL Server activities such as startups, shutdowns, logons, logon failures, database backup, restoration, audit, audit specifications, administrator authorities, and a lot more.

- Database backup report
- Database restoration report
- Transaction log backup report
- Admin authority changes report
- Permission changes report
- Owner Changes report
- Created server roles
- Dropped server roles
- Altered server roles
- Created Server Audits
- Dropped Server Audits
- Altered server audits
- Created Server Audit Specifications
- Dropped Server Audit Specifications
- Altered Server Audit Specifications
- Created Database Audit Specifications

- Dropped Database Audit Specifications
- Altered Database Audit Specifications
- Changed Audit Sessions
- Shutdown and Failure Audits
- Trace Audit C2 On
- Trace Audit C2 Off
- Started Trace Audits
- Stopped Trace Audits
- Server Startups
- Server shutdowns
- Logons
- Failure logons
- Logout Accounts
- Top logons based on user
- Top logons based on remote devices
- Top failure logons based on users
- Top failure logons based on remote devices
- Logons Trend
- Failed Logons Trend
- Event Trend report

SQL Server Security Reports

This report group gives detailed information on SQL injection and denial of service attacks to help you conduct detailed forensic analysis on how the attack happened.

You can also track account lockouts, privilege abuses, and unauthorized copying of sensitive data with these reports.

- Privilege Abuse
- Unauthorized Copies of Sensitive Data#
- Account Lockouts
- SQL Injection
- Denial of Service
- Additional Security Events

SQL Server System Events

This report group monitors critical system events in SQL Server, including processes killed by the host, access violations, and insufficient resource events. It helps administrators identify and address system issues promptly for optimal server performance and stability.

- Processes Killed by Host
- Access Violation
- Insufficient Resources Events

SQL Server DBCC Information Reports

These reports help you track the execution of DBCC commands in your SQL servers.

- DBCC Check Catalog required
- DBCC Check DB required
- DBCC failure events

SQL Server Host Activity Reports

This report help you track host activity in your SQL servers.

- Killed processes by hosts

SQL Server Integrity Reports

These reports ensure data integrity by consolidating SQL server error notifications, helping to detect any tampering with data.

- Check Database Integrity
- Check Catalog Integrity
- Check Table Integrity
- DBCC Error Events
- Integrity check Failure

SQL Server Authority Changes

With these reports, you can track changes in role membership, permissions, and ownership, ensuring data integrity and security.

- Role Members Added
- Dropped Role Members
- Permissions Changed
- Ownership Changed

SQL Server Trace Changes

This report group offers a comprehensive overview of trace activity within SQL Server environments. They help in monitoring system activity and ensuring compliance with auditing standards.

- Trace Audit C2 On
- Trace Audit C2 Off
- Started Trace Audits
- Stopped Trace Audits

SQL Server Permissions Denied Reports

The SQL server permissions denied reports can help you track unauthorized access attempts on critical data.

- Object permission denied
- Column permission denied
- Database permission denied

- Alter DB permission denied

SQL Server Violation Reports

SQL server violation report can give you details on the access violations which could be indicative of an attack or data theft.

- Access violation

SNMP Trap Type Reports

These report can help you consolidate the information from SNMP traps and help you manage your network better.

- Cold Start
- Warm Start
- Link Down
- Link Up
- Authentication Failure
- EGP Neighbor Loss
- Enterprise Specific

SNMP Severity Reports

These reports can help you track the error and information events to ensure that critical issues are brought to your notice.

- Error Events
- Information Events

Oracle Auditing Reports

These reports provide insights into Oracle database access, command execution, critical task performance, and more, including who did what, when, and from where.

- Created Databases
- Dropped Databases
- Altered Databases
- Created clusters
- Dropped clusters
- Altered Clusters
- Created Tables
- Dropped Tables
- Altered Tables
- Selected Tables
- Inserted Tables
- Updated Tables
- Deleted Tables
- Created functions

- Dropped functions
- Altered functions
- Created Schemas
- Created procedures
- Dropped procedures
- Altered procedures
- Executed procedures
- Created triggers
- Dropped triggers
- Altered Triggers

Oracle Auditing Account Management

These reports can help track the creation, modification, and deletion of user accounts and roles. With these reports, you can also monitor who accessed a user account or role, from where, and when the event occurred.

- Created profiles
- Dropped profiles
- Altered profiles
- Users created
- Dropped users
- Altered users
- Roles created
- Dropped roles
- Altered roles
- Granted roles
- Revoked roles
- System Grant
- System Revoke

Oracle Auditing Server Reports

These reports give insights on Oracle database access to monitor all user activity within the database. These reports help you audit user logons, remote logons, and user logoffs.

- Connect Events
- Server Startup
- Server Shutdown
- Logons
- Failed Logons
- Top logons based on users
- Top logons based on remote devices
- Top failed logons based on users
- Top failed logons based on remote devices

- Logon Trend
- Failed logon trend
- Oracle Events Trend

Oracle Security Reports

These reports help you detect attacks on Oracle databases such as SQL injections and Denial of Service attacks. With these you can also track expired passwords and account lockout to ensure that legitimate uses have uninterrupted access to resources.

- SQL Injection report
- Account Lockouts
- Expired Passwords
- Denial of Service Reports

MySQL Logon Events

These reports will help you track logons in your MySQL database to ensure that there is not unauthorized access to your MySQL database.

- Logon Success
- Logon Failures

MySQL General Statements

These reports help you track DDL and DML statements to make sure that there is no unauthorized modification or access to sensitive data.

- DDL Statements
- DML Statements
- Transactional and Locking Statements
- Utility Statements
- Replication Statements

MySQL Database Administrative Statements

These reports can help you track database administrative statements including account management and resource group management statements in MySQL servers.

- Account Management Statements
- Resource Group Management Statements
- Table Maintenance Statements
- Component and Plugin Statements
- Other Administrative Statements
- Set Statements
- Show Statements

MySQL Server Events

This report helps you track startup and shutdown events in your MySQL server.

- Server Startup/Shutdown Events

Printer Auditing

The printer auditing reports help you keep track of the documents that get printed within your network. These reports can also help you identify which documents get printed the most and by whom. This can help ensure that sensitive information is not indiscriminately printed which can increase the risk of data theft.

- Documents Printed
- Deleted documents
- Timed out documents
- Moved Documents
- Resumed Documents
- Paused documents
- Corrupted documents
- Documents' priority changes
- Insufficient Privilege to Print Documents
- Top printed documents based on users
- Top printed documents
- Printer Activity trend
- Failed Printer Activity Trend

Sysmon Process Auditing Reports

- Process Created
- Process Terminated
- Remote Thread Creation
- Process Access
- Pipe Created
- Pipe Connected

Sysmon Registry Auditing Reports

- Registry Object Renamed
- Registry Value Set
- Registry Key Created
- Registry Key Deleted
- Registry Value Created
- Registry Value Deleted

Sysmon File Auditing Reports

- File Created
- File Stream Creation
- File Time Change

- Raw Access Read

Sysmon Library and Drivers Reports

- Drivers Loaded
- Image Loaded

Sysmon Network Auditing Reports

- Network Connection
- DNS Query

Sysmon WMI Auditing Reports

- WMI Filter Events
- WMI Event Consumer Activity
- WMI Consumer to Filter Activity

Sysmon Configuration Reports

- Service State Change
- Config Modification

ADSelfService Plus Product Activity Report

- All Activity

ADSelfService Plus Debug Reports

- Instances Created
- Services Created
- Server Started
- Successful Logins
- Failed Logins

ADSelfService Plus Web Access Reports

- HTTP Status Success
- HTTP Bad Gateway
- HTTP Internal Server Error
- HTTP Gateway Timeout
- HTTP Request URI Too Large
- HTTP Unsupported Media Type
- HTTP Request Entity Too Large
- HTTP Forbidden
- HTTP Server Not Found
- HTTP Request Timeout
- HTTP Bad Request
- HTTP Unauthorized

- Information Reports
- Success Reports
- Redirection Reports
- Responses over time
- Client Error Reports
- Server Error Reports

ADManager Plus Product Activity Report

- All Activity
- User Activity

ADManager Plus Debug Reports

- Instances Created
- Services Created
- Server Started
- Successful Logins
- Failed Logins

ADManager Plus Web Access Reports

- HTTP Status Success
- HTTP Bad Gateway
- HTTP Internal Server Error
- HTTP Gateway Timeout
- HTTP Request URI Too Large
- HTTP Unsupported Media Type
- HTTP Request Entity Too Large
- HTTP Forbidden
- HTTP Server Not Found
- HTTP Request Timeout
- HTTP Bad Request
- HTTP Unauthorized
- Information Reports
- Success Reports
- Redirection Reports
- Responses over time
- Client Error Reports
- Server Error Reports

ADAudit Plus Product Activity Report

All Activity

ADAudit Plus Debug Reports

- Instances Created
- Services Created
- Server Started
- Successful Logins
- Failed Logins

ADAudit Plus Web Access Reports:

- HTTP Status Success
- HTTP Bad Gateway
- HTTP Internal Server Error
- HTTP Gateway Timeout
- HTTP Request URI Too Large
- HTTP Unsupported Media Type
- HTTP Request Entity Too Large
- HTTP Forbidden
- HTTP Server Not Found
- HTTP Request Timeout
- HTTP Bad Request
- HTTP Unauthorized
- Information Reports
- Success Reports
- Redirection Reports
- Responses over time
- Client Error Reports
- Server Error Reports

Endpoint Central SOM Management

- Computer Modifications
- Domain Changes
- IP Scope Changes
- Replication Policy Events
- Agent Updates

Endpoint Central Remote Activity

- Remote Control Activities
- Remote Shutdown Actions

Endpoint Central Patch Management

- Successful Patch Events
- Policy Deployment Events

Endpoint Central Device Control Management

- Whitelist Events
- Temporary Access Events
- Policy Events
- File Extension Group Events
- Policy Deployment Events

Endpoint Central Inventory Management

- Inventory Scanning Changes
- License Modifications

Endpoint Central BitLocker Reports

- Recovery Key Audit Events
- Policy Events
- Policy Deployment Events

Endpoint Central User Management

- Successful Logons
- Password Policy Modifications
- User Account Modifications
- Role Changes
- Other User Activities

ITOM Solutions Product Activity Report

- All Activity

ITOM Solutions Debug Reports

- Instances Created
- Services Created
- Server Started
- Successful Logins
- Failed Logins

ITOM Solutions Web Access Reports:

- HTTP Status Success
- HTTP Bad Gateway
- HTTP Internal Server Error
- HTTP Gateway Timeout
- HTTP Request URI Too Large
- HTTP Unsupported Media Type
- HTTP Request Entity Too Large
- HTTP Forbidden
- HTTP Server Not Found

- HTTP Request Timeout
- HTTP Bad Request
- HTTP Unauthorized
- Information Reports
- Success Reports
- Responses over time
- Client Error Reports
- Server Error Reports

ServiceDesk Plus Reports

ServiceDesk Plus Product Activity Report:

- All Activity

ServiceDesk Plus Debug Reports:

- Instances Created
- Services Created
- Server Started
- Successful Logins
- Failed Logins

ServiceDesk Plus Web Access Reports:

- HTTP Status Success
- HTTP Bad Gateway
- HTTP Internal Server Error
- HTTP Gateway Timeout
- HTTP Request URI Too Large
- HTTP Unsupported Media Type
- HTTP Request Entity Too Large
- HTTP Forbidden
- HTTP Server Not Found
- HTTP Request Timeout
- HTTP Bad Request
- HTTP Unauthorized
- Information Reports
- Success Reports
- Redirection Reports
- Responses over time
- Client Error Reports
- Server Error Reports

6.8.5. List of reports for vCenter Monitoring

Cluster changes

- Cluster created
- Cluster destroyed
- Cluster renamed
- Cluster reconfigured

Datacenter changes

- Datacenter created
- Datacenter deleted
- Datacenter renamed

Datastore changes

- Datastore created
- Datastore destroyed
- Datastore renamed
- Datastore file copied
- Datastore file moved
- Datastore file deleted

Folder changes

- Folder created
- Folder deleted
- Folder renamed
- Inventory objects moved into a folder

Permission changes

- Permission created
- Permission removed
- Permission updated

Resource pool changes

- Resource pool created
- Resource pool destroyed
- Resource pool moved
- Resource pool reconfigured

Role changes

- Role added
- Role removed

- Role updated

VM changes

- VM created
- VM deployed
- VM removed
- VM renamed
- VM reconfigured
- VM power state changes

Device changes

- Device added
- Device added failure
- Device IP changed
- Device shutdown
- Device removed
- Device connection overview
- Device powered down to standby

EventLog Analyzer also provides predefined alert criteria for all the above mentioned vCenter events. Setting up vCenter alert profile is same as setting up a predefined alert profile, except that you need to choose '**vCenter**' type in alert criteria.

6.8.6. Reports for H3C Devices

H3C Events Reports

- All Events
- Important Events

Firewall Allowed Traffic

- Allowed Traffic
- Top Traffic based on source
- Top Top Traffic based on destination
- Allowed Traffic Trend

Firewall Denied Connections

- Denied Traffic
- Top Denied Connections based on Source
- Top Denied Connections based on Destination
- Denied Connections Trend

Logon Reports

- Successful Logons
- Successful Logon Trend

Failed Logon Reports

- Failed Logons
- Failed Logons attempts
- Failed Logons Trend

Firewall Rules Management Reports

- Rules Added
- Rules Deleted
- Rules Modified

DHCP Reports

- Allocated IP address
- Conflicting IP Address
- Lease Extend IP Address

Interface Status Reports

- Interface Up
- Interface Down

Firewall IDS/IPS Reports

- All Attacks
- Attacks Trend

VPN Logon Reports

- Successful VPN Logons
- VPN Logout
- Successful VPN Logons Trend

Failed VPN Logon Reports

- Failed VPN Logons attempts
- Failed VPN Logons Trend

Firewall Security Reports

- Web Filtering
- Anti-virus reports

System Events

- Configuration Changes
- Clock Update
- System Reboot
- Fan Failure
- Memory Status
- CPU Status
- Temperature Status
- High Availability Status

Severity Reports

- Emergency Events
- Alert Events
- Critical Events
- Error Events
- Warning Events
- Notice Events
- Information Events
- Debug Events

6.8.7. Reports for Arista Devices

Arista Events

- All Events
- Important Events

Logon Reports

- Successful Logon
- Top Source
- Top Users
- Logoff Events
- Top Source
- Top Users
- Successful Logons Trend

Failed Logon Reports

- Failed Logons
- Top Source
- Top Users
- Failed Logons Trend

Allowed Traffic

- Allowed Traffic
- Top Source
- Top Destination
- Top Protocol
- Top Port
- Allowed Traffic Trend

Denied Connections

- Denied Connections
- Top Source
- Top Destination
- Top Protocol
- Top Port
- Denied Connections Trend

Interface Status

- Interface Up
- Interface Down

System Events

- Configuration Changes
- Configuration Errors
- System Reboot
- Clock Update
- Command Executed
- Fan Status
- Power Status
- Temperature Status
- Package Status

Severity Reports

- Emergency Events
- Alert Events
- Critical Events
- Error Events
- Warning Events
- Notice Events
- Information Events
- Debug Events

6.8.8. StormShield Reports

StormShield Events

- All Events
- Important Events

Logon Reports

- Successful Logon
- Failed Logons
- Logon Overview

Traffic Reports

- Allowed Traffic
- Denied Connections
- Traffic Overview

Firewall Rule Management

- Rule Added
- Rule Modified
- Rule Deleted

Firewall User Management

- Admin Added
- Admin Modified
- Admin Deleted

System Event

- Clock Updated
- System Shutdown
- System Reboot

IDS/IPS Reports

- Attack Overview

Severity Report

- Emergency Events
- Alert Events
- Critical Events
- Error Events
- Warning Events
- Notice Events

- Information Events
- Debug Events

6.8.9. HP Switches Reports

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

- **HP Events:** Provides information on all events on HP devices.
- **Successful and Failed Logons:** Provides information on all successful and failed logons based on source and users, including trend reports.
- **Interface Events:** Provides information on all interface and trunk status events.
- **Configuration Reports:** Provides information on both successful and failed commands and insights on ACL error and VLAN status.
- **System Events:** Provides information on configuration changes, clock update, system update and reboot, power, and license status.
- **Device Severity Reports:** Provides information on all emergency, alerts, critical, error, warning, and notice events.

HP Switches reports dashboard

- Go to the Reports section. Navigate to Network Devices and select HP from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity, Device, and Message.

- Use logical operators as required to create the filter criteria.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- The graphs can be viewed in different formats.

- The left panel lists all the available out-of-box reports for HP. Select the report you want to view.

- To quickly export the report, click **Export as** and choose the format. Once done, you can download the report.

- Click **Scheduled Reports** to have this report exported and emailed periodically.

- Click **More** for further customization options.

1. **Set as Default,** to set this report as the default for HP reports.
2. **Add to Favorites,** to mark this report as favorite.
3. **Pin to dashboard,** to pin this report to the main dashboard in the **Home** page.

6.8.10. Barracuda reports

EventLog Analyzer supports Barracuda Firewall and provides out-of-box reports for:

- **Barracuda Events:** Information on all events on Barracuda devices
- **Firewall Allowed and Denied Traffic:** Insights on traffic based on source, destination, protocol and port, also provides a report on traffic trends.
- **Firewall Website Traffic:** Traffic reports based on source, destination, and website traffic trend reports
- **Successful and Failed Logons:** Source and User based reports, trends reports
- **Firewall Rule Management:** Information on rules added, deleted or modified
- **Firewall Accounts Management:** Reports on administrators, users and groups added, deleted or modified.
- **Firewall IDS/IPS Events:** Insights on attacks based on source and destination IP address, critical and possible attacks with a report on attack trends
- **Firewall Security:** Antivirus reports and anti-spam reports.
- **Email Security:** Information on scanned, sent and received emails.
- **System Events:** Reports on service, power and memory status, clock update, system shutdown and reboot.
- **Device Severity:** Information on all emergency, alerts, critical, error, warning, and notice events

Barracuda reports dashboard

- Go to the Reports section. Navigate to Network Devices and select Barracuda from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity and Device and Message.

- Use logical operators as required to create the filter criteria.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- The graphs can be viewed in different formats.

- To quickly export the report in view, click **Export as** and choose the format. Once done, you can download the report.

- Click **Scheduled Reports** to have this report exported and emailed periodically.

- Click **More** for further customization options.
  1. **Set as Default,** to set this report as the default for Barracuda reports.
  2. **Add to Favorites,** to mark this report as favorite.
  3. **Pin to dashboard,** to pin this report to the main dashboard in the **Home** page.

EventLog Analyzer
Dashboard
Reports
Compliance
Search
Correlation
Alerts
Settings
Logfile
Support
Barracuda
All Events
Chart
Summary
Emergency
Alert
Critical
Error
Warning
Notice
Information
Debug

6.8.11. CheckPoint reports

EventLog Analyzer supports CheckPoint Firewall and provides out-of-box reports for:

- **CheckPoint Events:** Information on all events on CheckPoint devices.
- **Firewall Allowed and Denied Traffic:** Insights on traffic based on source, destination, protocol and port, also provides a report on traffic trends.
- **Successful and Failed Logons:** Insights on successful and failed logons categorized based on the user, the source, and the general trend.
- **Firewall Accounts Management:** Reports on user and user group added or deleted.
- **Configuration:** Reports on configuration changes, interface status and executed commands.
- **Firewall IDS/IPS Events:** Insights on attacks based on source and destination IP address and attack trends.
- **System Events:** Reports on system shutdowns and clock updates.
- **Device Severity:** Emergency, alerts, critical, error, warning, and notice events.

CheckPoint reports dashboard

- Go to the Reports section. Navigate to Network Devices and select CheckPoint from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity and Device and Message.

- Use logical operators as required to create the filter criteria.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- The graphs can be viewed in different formats.

- To quickly export the report in view, click **Export as** and choose the format. Once done, you can download the report.

- Click **Scheduled Reports** to have this report exported and emailed periodically.

- Click **More** for further customization options.
  1. **Set as Default,** to set this report as the default for CheckPoint reports.
  2. **Add to Favorites,** to mark this report as favorite.
  3. **Pin to dashboard,** to pin this report to the main dashboard in the **Home** page.

6.8.12. FirePower reports

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

- **FirePower Events:** Information on all events on FirePower devices
- **Firewall Allowed and Denied Traffic:** Insights on traffic based on source, destination, protocol and port, and traffic trends.
- **Firewall Website Traffic:** Traffic reports based on source, destination, and website traffic trend reports
- **Firewall IDS/IPS Events:** Insights on attacks based on source and destination IP address, also provides a report on attack trends
- **Device Severity Reports:** Emergency, alerts, critical, error, warning, and notice, information, and debug events

FirePower reports dashboard

- Go to the Reports section. Navigate to Network Devices and select FirePower from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity, Device, and Message.

- Use logical operators as required to create the filter criteria.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- The graphs can be viewed in multiple formats. To switch to a different graph format, click the drop down button.

- This panel lists all the available out-of-box reports for FirePower. Select the report you want to view.

- To export the report in view, click Export as and choose the format. Once done, you can download the report.

- Click **Scheduled Reports** to have this report automatically generated, exported, and emailed to the specified users in the desired format, at the specified times.

- Click **More** for further customization options.

  1. **Set as Default**, to set this report as the default for FirePower reports.
  2. **Add to Favorites**, to mark this report as favorite.
  3. **Pin to dashboard**, to pin this report to the main dashboard in the **Home** page.

6.8.13. Reports for Fortinet Devices

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

- **Fortinet Events:** These reports provide valuable information on all events including important events such as logons, failed logons, possible attacks, users added/deleted etc., on Fortinet devices.
- **Firewall Allowed and Denied Traffic:** The reports in this category provide insights on traffic based on the source, destination, protocol and port, and traffic trends.
- **Successful and Failed Logons:** These reports provide information on source, user-based, and trends reports.
- **Firewall IDS/IPS Events:** The reports in this category provide insights on possible attacks, and attacks based on the source and destination IP address. They also provide reports on attack trends.
- **Firewall Security Events:** These reports provide valuable information on applications, email and web filters. They also provide reports on antivirus and DLP.
- **Firewall Accounts Management:** This category provides reports on administrators and users added, deleted, or modified.
- **Firewall Policy Management:** The reports in this category provide useful information on policies added, deleted, or modified.
- **Successful and Failed VPN Logon Reports:** These reports provide insights on VPN logons and logouts based on success, failure, remote devices, users and trends.
- **System Events:** These reports provide valuable information on configuration changes, license expiration, power restores and failures, system shutdowns and reboots, and failed commands.
- **Device Severity Reports:** The reports in this category provide insights into emergency, alerts, critical, error, warning, notice, information, and debug events.
- **VPN IP Assigned Reports:** These reports provide information on private IP assigned, IP assigned users, remote IP and VPN IP assigned.

Managing Fortinet reports dashboard

- Go to the Reports section. Navigate to Network Devices and select Fortinet from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity and Device and Message.

- Use logical operators as required to create the filter criteria.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- The graphs can be viewed in different formats.

- The **All Events** panel lists all the available out-of-the-box reports for Fortinet. Select the report you want to view.

- To export the report being viewed, click **Export as** and choose the format. Once done, you can download the report.

- Click **Scheduled Reports** to have this report exported and emailed periodically.

- Click More for further customization options.
  1. **Set as Default**, to set this report as the default for Fortinet reports.
  2. **Add to Favorites**, to mark this report as favorite.
  3. **Pin to dashboard**, to pin this report to the main dashboard in the **Home** page.

6.8.14. Reports for Huawei Devices

EventLog Analyzer supports Huawei firewall devices and provides out-of-the-box reports for the following categories of events:

- **Huawei Events:** These reports provide valuable information on all events, including important events such as logons, failed logons, policies added/deleted, users added/deleted etc., on Huawei devices.
- **Successful and Failed Logons:** These reports provide information on source and user-based reports, and trend reports.
- **Firewall Allowed and Denied Traffic:** The reports in this category provide insights on traffic based on the source, destination, protocol and port, and traffic trends.
- **Firewall Accounts Management:** This category provides reports on users and groups added, deleted or modified.
- **Firewall Policy Management:** This category of reports provides valuable information on policies added, deleted, modified, enabled or disabled.
- **Firewall IDS/IPS events:** This category of reports provide useful insights on attacks based on the source and destination IP address. They also provide reports on attack trends.
- **Firewall Security Events:** These reports provide information on application, email and web filters. They also provide reports on antivirus and DLP.
- **Successful and Failed VPN Logon Reports:** This category of reports provide insights into VPN logons and logouts based on source, users and trend reports.
- **System Events:** This category provides reports on power status, command executed, CPU status, clock update, interface status, temperature status, and fan status.
- **Device Severity Reports**: The reports in this category provide insights into emergency, alerts, critical, error, warning, notice, information, and debug events.

Managing Huawei reports dashboard

- Go to the Reports section. Navigate to Network Devices and select Huawei from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity and Device and Message.

- Use logical operators as required to create the filter criteria.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- The graphs can be viewed in different formats.

- The **All Events** panel lists all the available out-of-the-box reports for Huawei. Select the report you want to view.

- To export the report being viewed, click **Export as** and choose the format. Once done, you can download the report.

- Click **Scheduled Reports** to have this report exported and emailed periodically.

- Click **More** for further customization options.
  1. **Set as Default**, to set this report as the default for Huawei reports.
  2. **Add to Favorites**, to mark this report as favorite.
  3. **Pin to dashboard**, to pin this report to the main dashboard in the **Home** page.

6.8.15. Reports for Juniper Devices

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

- **Juniper Events:** These reports provide valuable information on all events including important events such as logons, failed logons, possible attacks, configuration errors, interface up/down, etc., for Juniper devices.
- **Successful and Failed Logons:** These reports provide insights on source and user-based reports, trends reports. They also provide information on firewall, web, and CLI logons.
- **Configuration Reports:** The reports in this category provide information on interface settings, commands executed, and configuration errors.
- **Firewall Allowed and Denied Traffic:** This category of reports provides valuable insights on traffic based on the source, destination, protocol and port, and traffic trends.
- **Firewall IDS/IPS Events:** These reports provide insights on possible, critical, top attacks; attacks based on source, destination IP address, and severity; and attack trends.
- **Application Tracking Reports:** The reports in this category provide useful information on applications accessed based on username and reports on applications started and stopped.
- **System Events:** These reports provide information on process and fan status, and system reboots.
- **Device Severity Reports:** The reports in this category provide insights on emergency, alerts, critical, error, warning, notice, information, and debug events.

Managing Juniper reports dashboard

- Go to the Reports section. Navigate to Network Devices and select FirePower from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity, Device, and Message.

- Use logical operators as required to create the filter criteria.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- The graphs can be viewed in different formats.

- The **left** panel lists all the available out-of-the-box reports for Juniper. Select the report you want to view.

- To quickly export the report being viewed, click **Export as** and choose the format. Once done, you can download the report.

- Click **Scheduled Reports** to have this report exported and emailed periodically.

- Click **More** for further customization options.
  1. **Set as Default**, to set this report as the default for Juniper reports.
  2. **Add to Favorites**, to mark this report as favorite.
  3. **Pin to dashboard**, to pin this report to the main dashboard in the **Home** page.

6.8.16. Reports for Malwarebytes devices

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

Malwarebytes Events: The reports in this category provide valuable information on detected threats and exploits based on source and users. Additionally, granular reports on blocked, allowed exploits, quarantined threats, and websites blocked based on source and users are available.

Managing Malwarebytes reports dashboard

- Go to the **Reports** section and click on the **Threats** option in the drop down menu. Select Malwarebytes from the displayed list of vendors.

- You can set filter criteria for events based on object type, action value, action, object scanned, risk name, username and source IP. Use logical operators as required.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- The graphs can be viewed in different formats.

- In the left panel, under **Malwarebytes Reports, you can view** all the available threat reports for Malwarebytes. Select the report you want to view.

- To quickly export the report being viewed, click **Export as** and choose a format. Once done, you can download

the report.

- Click **Scheduled Reports** to have this report exported and emailed periodically.

- Click **More** for further customization options.
  1. **Set as Default**, to set this report as the default for Malwarebytes reports.
  2. **Add to Favorites**, to mark this report as favorite.
  3. **Pin to dashboard**, to pin this report to the main dashboard in the **Home** page.

6.8.17. Reports for Meraki Devices

EventLog Analyzer supports analysis of Meraki Firewall log format and provides out-of-the-box reports for the following categories of events:

- **Meraki Events:** The reports in this category provide information on all events including important events such as allowed traffic, denied connections, possible attacks etc., on Meraki devices.
- **Firewall Allowed and Denied Traffic:** This category of reports provide valuable insights on traffic based on the source, destination, protocol, port, and traffic trends.
- **Logon Reports:** These reports provide valuable information on user logons and its trends.
- **Firewall Website Traffic:** This category provides reports on traffic based on the source, destination IP address, website, and traffic trends.
- **Firewall IDS/IPS Events:** The reports in this category provide insights on possible attacks, and top attacks based on source and destination IP address. They also provide reports on attack trends.
- **Firewall Security Events:** This category provides reports on web filtering.
- **Successful and Failed VPN Logon Reports:** These reports give you valuable insights on VPN logouts and logons based on remote devices, users and trend reports.
- **Device Severity Reports:** The reports in this category provide insights on , alerts, critical, error, warning, notice, information and debug events.

Managing Meraki reports dashboard

- Go to the Reports section. Navigate to Network Devices and select Meraki from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity and Device and Message.

- Use logical operators as required to create the filter criteria.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- The graphs can be viewed in different formats.

- The **All Events** panel lists all the available out-of-the-box reports for Meraki. Select the report you want to view.

- To quickly export the report being viewed, click Export as and choose the format. Once done, you can download the report.

- Click **Scheduled Reports** to have this report exported and emailed periodically.

- Click **More** for further customization options.
  1. **Set as Default**, to set this report as the default for Meraki reports.
  2. **Add to Favorites**, to mark this report as favorite.
  3. **Pin to dashboard**, to pin this report to the main dashboard in the **Home** page.

6.8.18. NetScreen reports

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

- **NetScreen events**: Detailed information on all events on NetScreen devices.
- **Firewall Allowed and Denied Traffic**: Provides insights on traffic based on source, destination, protocol and port, also provides a report on traffic trends.
- **Firewall Website Traffic**: Traffic reports based on source, destination, and website traffic trend.
- **Successful and Failed Logons**: Provides source and user based reports, trend reports.
- **Firewall Accounts Management**: Provides reports on administrator added, deleted or modified.
- **Firewall Policy Management**: Provides information on policies added, deleted, or modified.
- **Firewall IDS/IPS Events**: Provides insights on attacks based on source and destination IP address, also provides a report on attack trends.
- **System Events**: Provides reports on configuration changes, clock update, system status, start and stop of services.
- **Failed VPN Logon Reports**: Monitors the VPN activities from pfSense logs and offers out-of-the-box reports for failed VPN logons.
- **Device Severity Reports**: Provides reports on emergency, alerts, critical, error, warning, and notice events.

NetScreen Reports Dashboard

- Go to the Reports section. Navigate to Network Devices and select NetScreen from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity and Device and Message.

- Use logical operators as required to create the filter criteria.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- To export a report, click **Export as** and choose the format. The solution allows you to export the reports in PDF and CSV formats.

- To generate and redistribute the reports over email at periodic time intervals, you can use the **Schedule Reports** option.

- The **More** link at the top right corner provides you the below customization options:
  1. **Set as Default**: Allows you to set the selected report as the default report.

2. **Add to Favorites**: Marks the selected report as favorite.

3. **Pin to dashboard**: Pins the selected report to the dashboard in the **Home** page.

6.8.19. Palo Alto reports

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

- **Palo Alto Events**: Provides information on all the events associated with Palo Alto devices.
- **Firewall Allowed and Denied Traffic**: Provides insights on traffic based on source, destination, protocol and port, and also generates a report on traffic trends.
- **Firewall Website Traffic**: Provides traffic reports based on source, destination, and website traffic trend.
- **Successful and Failed Logons**: Provides source and user based reports, trend reports.
- **Firewall Accounts Management**: Provides reports on administrator added, deleted or modified.
- **Firewall Policy Management**: Provides information on policies added, deleted, or modified.
- **Firewall IDS/IPS Events**: Provides insights on attacks based on source and destination IP address, also provides a report on attack trends.
- **System Events**: Provides reports on configuration changes, clock update, system status, start and stop of services, features and license status.
- **Failed VPN Logon Reports**: Monitors the VPN activities from Palo Alto logs and offers out-of-the-box reports for failed VPN logons.
- **Device Severity Reports**: Provides reports on emergency, alerts, critical, error, warning, and notice events.

Palo Alto Reports Dashboard

- Go to the Reports section. Navigate to Network Devices and select PaloAlto from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity, Device and Message.

- Use logical operators as required to create the filter criteria.

- If you want to generate the reports for a specific time **period**, select the Period calendar option from the top right corner, specify the time period and then click **Apply**.

- The **All Events** panel lists all the available out-of-the-box reports for PaloAlto. Select the report you want to view.

- To export a report, click **Export as** and choose the format. The solution allows you to export the reports in PDF and CSV formats.

- To generate and redistribute the reports over email at periodic time intervals, you can use the **Schedule**

Reports option.

- The **More** link at the top right corner provides you the below customization options:
  1. **Set as Default**: Allows you to set the selected report as the default report.
  2. **Add to Favorites**: Marks the selected report as favorite.
  3. **Pin to dashboard**: Pins the selected report to the dashboard in the **Home** page.

6.8.20. pfSense reports

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

- **pfSense Events**: Provides information on all events on pfSense devices.
- **Firewall Allowed and Denied Traffic**: Provides insights on traffic based on source, destination, protocol and port, and also generates a report on traffic trends.
- **Firewall Website Traffic**: Provides traffic reports based on source, destination, and website traffic trend.
- **Successful and Failed Logons**: Provides source and user based reports, trend reports.
- **Firewall Accounts Management**: Provides reports on administrator added, deleted or modified.
- **Firewall Policy Management**: Provides information on policies added, deleted, or modified.
- **Firewall IDS/IPS Events**: Provides insights on attacks based on source and destination IP address, also provides a report on attack trends.
- **System Events**: Provides reports on configuration changes, clock update, system status, start and stop of services, features and license status.
- **Failed VPN Logon Reports**: Monitors the VPN activities from pfSense logs and offers out-of-the-box reports for failed VPN logons.
- **Device Severity Reports**: Provides reports on emergency, alerts, critical, error, warning, and notice events.

pfSense Reports Dashboard

- Go to the Reports section. Navigate to Network Devices and select pfSense from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity and Device and Message.

- Use logical operators as required to create the filter criteria.

- If you want to generate the reports for a specific time **period**, select the Period calendar option from the top right corner, specify the time period and then click **Apply**.

- The **All Events** panel lists all the available out-of-the-box reports for pfSense. Select the report you want to view.

- To export a report, click **Export as** and choose the format. The solution allows you to export the reports in PDF and CSV formats.

- To generate and redistribute the reports over email at periodic time intervals, you can use the Schedule Reports option.

- The **More** link at the top right corner provides you the below customization options:
  1. **Set as Default**: Allows you to set the selected report as the default report.
  2. **Add to Favorites**: Marks the selected report as favorite.
  3. **Pin to dashboard**: Pins the selected report to the dashboard in the **Home** page.

6.8.21. SonicWall reports

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

- **SonicWall Events**: Provides information on all events on SonicWall devices.
- **Firewall Allowed and Denied Traffic**: Provides insights on traffic based on source, destination, protocol and port, and also generates a report on traffic trends.
- **Firewall Website Traffic**: Provides traffic reports based on source, destination, and website traffic trend.
- **Successful and Failed Logons**: Provides source and user based reports, trend reports.
- **Firewall Accounts Management**: Provides reports on administrator added, deleted or modified.
- **Firewall Policy Management**: Provides information on policies added, deleted, or modified.
- **Firewall IDS/IPS Events**: Provides insights on attacks based on source and destination IP address, also provides a report on attack trends.
- **System Events**: Provides reports on configuration changes, clock update, system status, start and stop of services, features and license status.
- **Failed VPN Logon Reports**: Monitors the VPN activities from SonicWall logs and offers out-of-the-box reports for failed VPN logons.
- **Device Severity Reports**: Provides reports on emergency, alerts, critical, error, warning, and notice events.

SonicWall Reports Dashboard

- Go to the Reports section. Navigate to Network Devices and select SonicWall from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity and Device and Message.

- Use logical operators as required to create the filter criteria.

- If you want to generate the reports for a specific time **period**, select the Period calendar option from the top right corner, specify the time period and then click **Apply**.

- To export a report, click **Export as** and choose the format. The solution allows you to export the reports in PDF and CSV formats.

- To generate and redistribute the reports over email at periodic time intervals, you can use the **Schedule Reports** option.

- The **More** link at the top right corner provides you the below customization options:
  1. **Set as Default**: Allows you to set the selected report as the default report.
  2. **Add to Favorites**: Marks the selected report as favorite.
  3. **Pin to dashboard**: Pins the selected report to the dashboard in the **Home** page.

6.8.22. Sophos reports

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

- **Sophos Events**: Provides information on all the events associated with Sophos devices.
- **Firewall Allowed and Denied Traffic**: Provides insights on traffic based on source, destination, protocol and port, and also generates a report on traffic trends.
- **Firewall Website Traffic**: Provides traffic reports based on source, destination, and website traffic trend.
- **Successful and Failed Logons**: Provides source and user based reports, trend reports.
- **Firewall Accounts Management**: Provides reports on administrator added, deleted or modified.
- **Firewall Policy Management**: Provides information on policies added, deleted, or modified.
- **Firewall IDS/IPS Events**: Provides insights on attacks based on source and destination IP address, also provides a report on attack trends.
- **System Events**: Provides reports on configuration changes, clock update, system status, start and stop of services, features and license status.
- **Failed VPN Logon Reports**: Monitors the VPN activities from Sophos logs and offers out-of-the-box reports for failed VPN logons.
- **Device Severity Reports**: Provides reports on emergency, alerts, critical, error, warning, and notice events.

Sophos Reports Dashboard

- Go to the Reports section. Navigate to Network Devices and select Sophos from the displayed list of devices.

- You can set filter criteria for events based on Source, Severity and Device and Message.

- Use logical operators as required to create the filter criteria.

- Select the **Period** for which you want the data to be displayed and click **Apply**.

- To export a report, click **Export as** and choose the format. The solution allows you to export the reports in PDF and CSV formats.

- To generate and redistribute the reports over email at periodic time intervals, you can use the **Schedule Reports** option.

- The **More** link at the top right corner provides you the below customization options:
  1. **Set as Default**: Allows you to set the selected report as the default report.

2. **Add to Favorites**: Marks the selected report as favorite.

3. **Pin to dashboard**: Pins the selected report to the dashboard in the **Home** page.

6.8.23. WatchGuard reports

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

1. **WatchGuard Events**: The reports in this category provides Information on all events on WatchGuard devices.
2. **Firewall Allowed and Denied Traffic**: The reports in these categories provide information on traffic based on source, destination, protocol and port. It also, provides information on traffic trends.
3. **Firewall Website Traffic**: This category has traffic reports based on source, destination, and website traffic trend reports.
4. **Successful and Failed Logons**: The reports in these categories provide information on successful and failed logins based on source and user. It also provides insights on logon trends.
5. **Firewall Accounts Management**: The reports in this category provides information on added, deleted, or modified firewall administrator accounts.
6. **Firewall Policy Management**: These reports provide information on added, deleted, or modified firewall policies.
7. **Firewall IDS/IPS Events**: The reports in this category provide information on attacks based on source and destination IP address. It also provides insights on attack trends.
8. **System Events**: These reports provide information on configuration changes, clock updates, system status, start and stop of services, features, and license status.
9. **Failed VPN Logon Reports**: These reports provide information on the VPN activities from WatchGuard logs and offers out-of-the-box reports for failed VPN logons.
10. **Device Severity Reports**: The reports in this category provide information on emergency, alerts, critical, error, warning, and notice events.

WatchGuard reports dashboard

1. Go to the Reports section. Navigate to Network Devices and select WatchGaurd from the displayed list of devices.

2. You can set filter criteria for events based on Source, Severity and Device and Message.

3. Use logical operators as required to create the filter criteria.

4. Select the **Period** for which you want the data to be displayed and click **Apply**.

5. The graphs can be viewed in different formats.

6. To quickly export the report in view, click **Export as** and choose the format. You can then download the report.

7. Click **Scheduled Reports** to have this report exported and emailed periodically.

8. Click **More** for further customization options.

    1. **Set as Default**, to set this report as the default for WatchGuard reports.
    2. **Add to Favorites**, to mark this report as favorite.
    3. **Pin to dashboard**, to pin this report to the main dashboard in the **Home** page.

6.8.24. F5 reports

EventLog Analyzer audits F5 devices and provides out-of-the-box reports for the following categories of events:

1. **F5 Events**: The reports in this group contains information on all events logged by F5 devices.
2. **Logon Reports**: These reports provide information on successful firewall logons and logoffs, and also gives insights into logon trends.
3. **Failed Logon Reports**: The reports in this category provide information on failed firewall logons and insights into failed logon trends.
4. **LTM Health Monitoring**: The reports in this category let you track recent changes made to monitor status, node status, pool status, pool member status, and virtual server status.
5. **Connection Monitoring**: These reports let you view all CMI events and monitor connection limits.
6. **Interface Events**: The reports in this category let you monitor interface events such as Interface Up, Interface Down, Interface error, and VLAN events.
7. **Firewall Allowed Traffic**: The reports in this category provide information on all connections allowed through the firewall, and firewall trends.
8. **Firewall Denied Traffic**: These reports provide information on all denied connections and insights on trends in firewall traffic.
9. **Firewall Policy Changes**: These reports let you track all policy changes.
10. **Firewall IDS/IPS Reports**: The reports in this category let you monitor attacks and attack trends.
11. **System Events**: The reports in this category provide information on configuration changes and errors, reports on license, policy, and memory status. Monitor status of hardware such as chassis module, temperature, fan, and sensor. Reports on hardware errors.
12. **Application Security Reports**: These reports provide an overview of application security, information on requests allowed and blocked, and trends reports.
13. **Device Severity Reports**: These reports provide information on emergency, alert, critical and error events.

F5 reports dashboard

1. Go to the Reports section. Navigate to Network Devices and select F5 from the displayed list of devices.

2. You can set filter criteria for events based on Source, Severity and Device and Message.

3. Use logical operators as required to create the filter criteria.

4. Select the Period for which you want the data to be displayed and click Apply.

5. The panel on left lists all the available out-of-the-box reports for F5. Select the report you want to view.

6. To quickly export the report in view, click **Export as** and choose the format. You can then download the report.

7. Click **Scheduled Reports** to have this report exported and emailed periodically.

8. Click More for further customization options.

    1. **Set as Defaul**t, to set this report as the default for WatchGuard reports.
    2. **Add to Favorites**, to mark this report as favorite.
    3. **Pin to dashboard**, to pin this report to the main dashboard in the **Home** page.

6.8.25. IBM AS/400 reports

EventLog Analyzer supports IBM iSeries (AS/400) devices and provides out-of-the-box reports on:

1. **Journal logons and logoffs**: The reports in this category provide information on all journal logons and logoffs.
2. **User activity**: These reports offer insights into user profile changes, authority changes, logons and logoffs, objects deleted, ownership changes, disabled user profiles due to maximum number of sign-on attempts.
3. **Logon failures**: The reports in this category provide information on failed logons and authorization, and logon failure due to invalid passwords.
4. **System events**: These reports provide information on system value changes and time changes, expired system IDs, password bypass period, and information on subsystem varied off workstation.
5. **Job logs**: These reports provide information on top jobs based on users, successful job start and end, and changes made to jobs.
6. **Storage events**: These reports provide information on breach of ASP storage threshold, storage directory threshold, and reports on serious storage conditions.
7. **Battery condition**: These reports provide information on battery cache expiry, weak battery and battery failures.
8. Reports on i5 grace period expiry
9. **Configuration and hardware**: These reports provide information on device configuration, hardware errors, disk unit errors, temporary IO Processor errors, and system processor failure.

IBM reports dashboard

1. Go to the Reports section. Navigate to Servers and Workstation and select IBM AS/400 from the displayed list of devices.

2. The panel on the left lists all the available out-of-box reports for IBM AS/400. Select the report you want to view.

3. You can set filter criteria for events based on Source, Severity and Device and Message.

4. Use logical operators as required to create the filter criteria.

5. To view the security events of specific time period, select the **period** from the Period calendar option on the top right corner and click **Apply**.

6. To quickly export the report in view, click **Export as** and choose the format. You can then download the report.

7. Click **Scheduled Reports** to have this report exported and emailed periodically.

8. Click **More** for further customization options.
    1. **Set as Default**, to set this report as the default for IBM AS/400 reports.
    2. **Add to Favorites**, to mark this report as favorite.
    3. **Pin to dashboard**, to pin this report to the main dashboard in the **Home** page.

6.8.26. 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.

6.8.27. 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.

7.1. Threat Data Analytics

The EventLog Analyzer ingests contextual threat data from threat intelligence solutions such as FireEye, Symantec, and Malwarebytes. The data from these solutions are analyzed and presented to you in the form of reports that highlights critical events such as infections, possible malware and web infections, and so on.

Supported threat intelligence solutions and other similar sources:

- FireEye Threat Solutions
- Symantec Endpoint Solutions
- Symantec DLP Applications
- Malwarebytes Solutions
- CEF format
- Trend Micro
- McAfee Solutions

EventLog Analyzer can automatically analyze data from the above solution and gives you insights on commonly found severities, source and destination IP addresses, and the most targeted ports in the form of security analytical reports.

These reports can also be exported in the PDF, CSV, and HTML formats. Report generation can also be automated using the Schedule report option. These are the solutions that EventLog Analyzer supports.

7.2. FireEye Threat Solutions

EventLog Analyzer can process log data from FireEye and present the data in the form of graphical reports. For the solution to start collecting log data from FireEye, it has to be added as a threat source.

Steps to add a FireEye threat source:

To add a FireEye device as a threat source, the syslog service has to be configured on the FireEye device.

1. Login to the FireEye device as an administrator.
    - Navigate to **Settings > Notifications**, select rsyslog and the **Event type**.
2. Click **Add Rsyslog Server**.
3. 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).
4. Click on **Save**.

Once the device is added in EventLog Analyzer, it should then be listed as a threat source. This can be done in a few simple steps.

1. In the EventLog Analyzer console, navigate to **Settings > Log Source Configurations > Applications > Security Applications > Add Security Applications**
2. Select Add-on type as **FireEye**
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**.

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.

The reports provide information on:

- Domain matches
- Malware infections
- Callbacks
- Malware objects

- Web infections

EventLog Analyzer also provides reports that give information on the top:

- Severities
- Source IPs of infections
- Target IPs
- Target ports
- Malware
- Active sensors

7.3. Symantec Endpoint Solutions

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

Adding a Symantec Endpoint Solutions device as a threat source:

To add a Symnatec Endpoint Solutions device as a threat source, the syslog service has to be configured.

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 values.
8. Click on **OK**.

1. In the EventLog Analyzer console, navigate to **Settings > Log Source Configurations > Applications > Security Applications > Add Security Applications**
2. Select Add-on type as **Symantec**
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**.

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.

The reports provide information on:

- Security risks
- Virus detected
- Port cans
- Installation of commercial applications
- Threat activities

- HIPS activities

EventLog Analyzer also provides reports on the top:

- Affected devices
- Source devices
- Risks
- Problems

7.4. Symantec DLP Application

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

Adding a Symantec DLP Application device as a threat source:

To add a Symnatec DLP Application device as a threat source, the syslog service has to be configured.

1. Locate and open the config\Manager.properties file. The file path is as follows
    - Windows - **\SymantecDLP\Protect\config directory**
    - Linux - **/opt/SymantecDLP/Protect/config directory**
2. Uncomment the **systemevent.syslog.host= line** and specify the **EventLog Analyzer server IP address** as follows:

    systemevent.syslog.host=xxx.xx.xx.xxx
3. 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
4. After making the above mentioned changes, save and close the properties file.

1. In the EventLog Analyzer console, navigate to **Settings > Log Source Configurations > Applications > Security Applications > Add Security Applications**
2. Select Add-on type as **Symantec DLP**
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**.

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.

The reports provide information on the top:

- Senders
- Recipients
- Targets
- Protocols
- Data Owners

- Severities

Additionally, a Symantec DLP overview report is also provided.

7.5. Malwarebytes Reports

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

Adding Malwarebytes as a threat source:

To add a Malwarebytes as a threat source, the syslog service has to be configured.

1. Log into the **Management** console of the Malwarebytes device.
2. Navigate 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 the 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 on **OK** to 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 **Malwarebytes**
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**.

The available reports are:

- Detected Threats
- Quarantined Threats
- Allowed Threats
- Top Threats based on source
- Top Threats based on user

- Top Threats Types
- Top Websites blocked based on source
- Detected Exploits
- Blocked Exploits
- Allowed Exploits
- Top Exploits based on source
- Top Exploits based on user
- Top Exploits types
- Malicious Websites Blocked
- Top Websites Blocked

7.6. CEF format Reports

EventLog Analyzer collects log data in the CEF format and presents it in the form of graphical reportsFor the solution to start collecting this log data, the device has to be added as a threat source.

Adding a device with logs in the CEF format as a threat source:

To add the application that uses CEF as a threat source, the syslog service has to be configured.

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.

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 **CEF format**
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**.

The available reports are:

- CEF Format Overview
- Very High Severity Events
- High Severity Events
- Medium Severity Events
- Low Severity Events
- Top Events Based On Event Class ID
- Top Events Based On Event Name

7.7. Configuring McAfee Solutions

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

8.1. Vulnerability Data Analytics

EventLog Analyzer can process log data from vulnerability scanners such as Nessus, Qualys, OpenVAS, and NMAP. The data ingested from vulnerability scanners can be incorporated into the correlation engine to discover complex attack patterns. The solution generates out-of-the-box reports and predefined alert criteria that help in identifying and prioritizing vulnerabilities in your network. The report groups available are:

- Top Vulnerability Reports
- Reports on Nessus vulnerability data
- Reports on Nessus Compliance
- Reports on Qualys vulnerability data
- Reports on NMAP vulnerability data
- Reports on OpenVas vulnerability data
- Reports on Nexpose vulnerability data

EventLog Analyzer also has predefined alert criteria corresponding to the above categories. Setting up an alert profile for vulnerability scanners is similar to a predefined alert profile. The only difference is that you need to choose Vulnerability as the type from the predefined list and then choose the appropriate alert condition.

Exporting data from vulnerability scanners

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.

Nexpose

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.

Nessus

1. Select a scan under Scans Tab.
2. In the upper-right corner, click **Export**
3. From the drop-down box, select Nessus.

NMAP

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**.

OpenVas

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.

Qualys

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**.

8.2. Vulnerability Reports

EventLog Analyzer has over 50 out-of-the-box reports for analyzing log data from vulnerability scanners such as Nessus, Qualys, OpenVAS, and NMAP. The reports are essential for discovering and remediating network vulnerabilities.

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, vCenter, 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

Reports on Qualys vulnerability data

The information on potential vulnerabilities in a network including service vulnerabilities and potential vulnerabilities gathered from Qualys will be provided in these reports. This information is also presented in the graphical format for improved insights.

Available reports:

- **Information gathered from vulnerabilities** - Information that can be gathered from detected vulnerabilities such as CVSS scores and the severity level will be available in this report.
- **Services vulnerabilities** - Service vulnerabilities like open TCP and UDP services will be listed in this report.
- **Potential vulnerabilities** - Vulnerabilities that could be exploited by an attacker will be listed in this report.
- **Confirmed vulnerabilities** - Vulnerabilities that are above a CVSS base score of 5 will be listed in this report.
- **Severe vulnerabilities** - Vulnerabilities with the severity level 'Urgent'will be listed in this report.
- **Open TCP Ports** - Open TCP ports in the network will be displayed in this report.
- **Open UDP Ports** - Open UDP ports in the network will be displayed in this report.
- **Qualys Reports Overview** - An overview of all important events in Qualys reports will be displayed here.

Reports on NMAP vulnerability data

EventLog Analyzer can collect vulnerability data from open source, vulnerability scanning platforms such as NMAP. These reports can help you discover open ports in your network sorted according to device, service, or protocol.

Available reports:

- **Top Vulnerable Service** - From NMAP data, the services in the system most prone to be exploited will be available here.
- **Top Vulnerable OS** - From NMAP data, the services in the operating systems most prone to be exploited will be available here.
- **Top Open Ports** - A list of all the open ports in the system will be available here.
- **Open Ports** - A list of all the open ports in the system will be available here.
- **Top Vulnerable Devices** - A list of the most vulnerable devices, according the the NMAP data will be available here.
- **Top Vulnerable protocol** - The most vulnerable protocols used in the system will be available in this report.
- **Top Vulnerable ports** - A list of the most vulnerable ports according to the NMAP data will be available here.

Reports on OpenVas vulnerability data

EventLog Analyzer collects data from OpenVas and helps you classify the reports based on the threat level as high, medium, or low.

- **Top Vulnerabilities High Threat** - Vulnerabilities that pose the highest risk of attacks will be listed here.
- **Top Vulnerabilities Medium Threat** - Vulnerabilities that pose a moderate risk of attacks will be listed here.
- **Top Vulnerabilities Low Threat** - Vulnerabilities that do not pose a high risk of attacks will be listed here.

Data from OpenVas is also segregated based on severity, CVS score, and group.

- **Top CVS Score by Count** - This report identifies the most frequent vulnerabilities categorized based on the CVS score.
- **Top Vulnerable Group** - This report lists the most vulnerable workgroups in your network based on the
- **Top Vulnerabilities** - This report lists the most common vulnerabilities in the network.

Reports on Nexpose vulnerability data

EventLog Analyzer collects data from Nexpose and categorizes the vulnerability information based on the level of severity.

Available reports:

- **Critical threats** - Vulnerabilities that pose the highest risk of attacks will be listed here.
- **High threats** - Vulnerabilities that pose a considerably high risk of attacks will be listed here.
- **Medium threats** - Vulnerabilities that pose a moderate risk of attack will be listed here.
- **Low threats** - Vulnerabilities that do not pose a high risk of attacks will be listed here.
- **Vulnerability trend** - The general trend that can be inferred based on the vulnerabilities in your network will be listed here.

9.1. Understanding correlation

What is correlation?

Correlation is the process of identifying a sequence of multiple events, across one or more devices, which are all related, and form a single large incident. The main reason correlation is so useful is because, in many cases, the individual events may not seem suspicious on their own, but when taken in relation to the other events, a larger picture emerges which points to a potential security incident.

For instance, the two events "employee logs on to Device A" and "employee logs on to Device B" seem perfectly normal.

However, "**same employee** logs on to two **different devices** (Device A and Device B) at almost the **same time**" may indicate a possible account sharing incident.

What is a correlation rule?

A correlation rule is a pattern or a template used to relate multiple logs and identify a security incident. The rule specifies a series of events that make up a larger incident, the time window between events, and specific conditions if any. The following illustrates the various parameters that can be specified in a correlation rule:

- **Correlation rule:** A correlation rule is an ordered sequence of network actions.
- **Actions:** An action corresponds to a network log. It contains several fields with unique values such as username, device name, and so on.
- **Time window between actions:** Each action has to follow the previous action within a specified time window.
- **Threshold for an action (optional):** A single action may have to occur several times continuously for a specific rule to hold true. A threshold can be specified for the minimum number of repetitions that need to be observed within the specified time window.
- **Filters for an action (optional):** Conditions can be imposed on the fields within each action, with the use of filters.

For more information on constructing a correlation rule using these parameters, see Constructing custom correlation rules.

Example:

Correlation Rule:Brute force

A brute force attack occurs when an attacker tries to gain access to a device in your network, by trying several logon credentials until one succeeds. It is characterized by several failed logons on a device, followed by a successful logon:

General pattern: Failed logon -> Failed logon -> Failed logon -> (...) -> Successful logon (all within a few minutes, to the same device)

Specific pattern: At least 10 failed logons to a single device within 2 minutes -> (within the next 1 minute) -> Successful logon to the same device

The rule can thus be configured as below:

Action 1: Failed logon - an employee fails to log on to a network device.

- **Threshold:** This action should occur a minimum of 10 times within 2 minutes.
- **Filters:** The device name should be the same for all occurrences of Action 1.

Time window between Action 1 & Action 2: 1 minute

Action 2: Successful logon - an employee logs on to a network device.

- **Threshold:** None.
- **Filters:** The device name should be the same as the device name from Action 1.

Comparison between correlation rules and alert profiles

- A correlation rule specifies one or more events, occurring on one or more devices. An alert profile can only specify a single event, from a single device type.
- A correlation rule provides more power than an alert profile in defining a scenario. As a correlation rule can include more than one event, it allows you to specify the ordering of the events, time windows between events, and make use of various conditions.
- Threshold limits can be specified in **both** correlation rules and alert profiles. However, while a correlation rule can check that a specific field's value is the same throughout all repetitions of an action, an alert profile cannot.

Best practices for correlation

- Correlation is a memory intensive process. If you enable the correlation engine, be sure to enable/create rules only for your most important business use cases.
- Before creating a new rule, ensure that the same rule cannot be created as an alert profile instead. Please configure your use case as an alert profile instead of a correlation rule, if your answer is "yes" to all items in the below checklist:
    - Your use case consists of only one action.
    - You only need to specify the devices to which the use case is applicable, and don't need to check for a specific value for other fields (like username).

    - In case you specify a threshold value for the action, you don't need to check for a constant field value for any field (username, device name, etc.).
- Periodically review the logic for your correlation rules. If any rule is generating too many false positives, you can adjust the rule parameters to reduce them.

To know more about correlation, check out the following pages:

1. Managing correlation rules
2. Session activity
3. Viewing last 10 incidents
4. Creating custom correlation rules

Some examples

Correlation Rule : Excessive application crashes (Windows)

A series of application crashes on a device over a short time-frame may point to a faulty device. Further, this check should not be applied to a specific device named "Device-1234" as it is used for application crash testing purposes and may generate too many false positives.

General action flow: Application crash -> Application crash -> (...) -> Application crash (all within few hours on a single device, not applicable to Device-1234)

Specific action flow: At least 5 application crashes on a single device within 180 minutes (except for Device-1234)

The rule can thus be configured as below:

Action 1: Application crash - an application crashes on a Windows device.

- **Threshold:** This action should occur a minimum of 5 times within 180 minutes.
- **Filters:**
    - The device name should be the same for all occurrences of Action 1.
    - The device name should not equal Device-1234.

Correlation Rule: Possible ransomware activities (Windows)

A ransomware attack typically progresses with a newly started process modifying several files on a network devices (in order to encrypt them). It can be identified with a process being started, shortly followed by multiple file modifications.

General action flow: Process started -> File modified -> File modified -> (...) -> File modified (all within a few minutes, on the same device)

Specific action flow: Process started -> (within the next 5 minutes) -> At least 15 file modifications on the same device, by the same process

The rule can thus be configured as below:

Action 1: Windows Process started - a process is started on Windows.

- **Threshold:** None.
- **Filters:** None

Time window between Action 1 & Action 2: 5 minutes

Action 2: File modified - a file is modified on a Windows device.

- **Threshold:** 15 times within 30 minutes.
- **Filters:**
  - The device name should be the same for all occurrences of Action 2.
  - The process name should be the same for all occurrences of Action 2.
  - The device name should be the same as the device name from Action 1.
  - The process name should be the same as the process name from Action 1.

9.2. Generating Incident Timeline Reports in Correlation

With EventLog Analyzer's correlation reports, you can understand complex incidents happening across your network and get a clear picture of the sequence in which they unfold.

Three types of reports are available:

- Incidents overview report
- Incident reports
- Timeline view

You can also perform several reporting actions, empowering you to gain maximum value from your log data. To know more about what correlation is, how correlation rules are structured, and more, see understanding correlation.

Incidents overview report

The incidents overview report provides a summary of the various incident types encountered. Each incident type corresponds to a correlation rule. For each incident type, you can view the total count of correlated incidents.

To view the incidents overview report,

- Click on the **Correlation** tab.
- Select **Recent Incidents** from the left menu.

Incident reports

An incident report provides the details of the various occurrences of a specific incident type (or correlation rule). It displays the count of correlated events over time.

To view the report for a specific rule, go to the Correlation tab, navigate to the rule name on the left menu, and click on it. You can also go to the incident report from the incidents overview report by clicking on the corresponding entry in the graphical or tabular parts of the report.

- Click on the **Correlation** tab.
- Select the desired rule name from the left pane.
- You can also view the incident report for a particular incident by selecting the corresponding entry from the table.

Timeline view

The timeline view provides the history of correlated actions for each occurrence of an incident. It is a sequential list of logs that led to the triggering of a particular rule.

- To get an Event timeline for each incident on the table, click on **Event Timeline** corresponding to the specific incident.

- To view the details of each log, click on the **Details** next to each event.

Incident report actions

The following actions can be performed on the incident reports:

1. Export reports

   You can export incident reports in either PDF or CSV format.

   - To export a report, navigate to the required report, and click on the **Export as** option.
   - Select the format in which you would like to export the report from the drop down list.
   - The status of all previous and ongoing exports can be viewed by clicking on the **Report export history icon** next to the **Export as** option.

2. Schedule reports

   An incident report schedule allows you to generate incident reports at regular periods, and optionally receive them via email.

   - To view the list of existing schedules for a specific report, navigate to the required incident report and click on **Schedule Report**.
   - You can enable/disable or edit the schedules by clicking on the respective icons. To create a new schedule, click on **Add Schedule**.

Specify the following details for the schedule:

- **Schedule name**: A name for the new schedule.
- **Schedule frequency**: The frequency to generate the report (only once/hourly/daily/weekly/monthly)
- **Run schedule at**: The day/time within the chosen period at which the report must be generated.
- **Export time range**: The time range for which the report data must be exported..
- **Report format**: Reports can be generated in either PDF or CSV formats.
- **Email address**: The email address to which the report needs to be sent to.
- **Email subject line**: The subject of the email to be sent.
- Click on **Save**.

You can choose what information must be displayed in your incident report by adding or removing the required fields as columns in the report.

- To select the fields, click on the column selector icon on the top right cornerof the required report.

- Select the fields to be displayed in the report by choosing the respective checkboxes under each action.

You can also specify the below options for each field by clicking on the edit icon next to the required field.

- **Display name**: This is the name of the field as displayed in the report. This is useful if you would like to display the same field (e.g. username) from more than one action. You can distinguish between similar fields by changing their display names. For instance, 'Failed logon username' and 'Successful logon username'.
- **Show value of**: When you have specified a threshold value for the action and it occurs more than once, you can choose to display the field value from either the first, last or all occurrences of the action. Once you have specified the required information to be displayed, click **Save**.

9.3. View Last 10 Incidents

EventLog Analyzer's correlation engine allows you quick access to the last 10 correlation incidents that happened on the network. To view the last 10 correlation events:

Click **Last 10 incidents** in the **Rules Overview** or **Rule Report** window.

The **Incidents Overview** window provides you with the list of 10 previous correlation incidents, in raw log format.

Users can toggle between the **List** and **Grid** report views.

9.4. Activity Monitoring

EventLog Analyzer processes log data across your network and provides reports on session activity of your network devices and users. You can access these reports by clicking on **Activity Monitoring** under the **Correlation** tab.

Activity Monitoring Rules

You can either use the predefined rules in EventLog analyzer to generate reports on session activity or you can build your own rules with individual actions.

Predefined activity rules

- Navigate to **Correlation > Manage Rules > Activity Rules**.
- Select the predefined rules which you wish to use, click the **enable** icon, and confirm the same.

Custom activity rules

To open the activity rule builder, navigate to **Correlation** > **Manage Rules > Activity Rules > Create Activity Rule.**

1. Select the individual actions that make up the rule, from the categorized list of actions on the left of the screen.
    - You can also search for actions using the search bar on top of the list.
    - You can drag and drop the actions to rearrange their order, or delete the action by clicking on the delete icon on its right.
    - To detect repetition of the same action within a particular time interval, tick the Threshold limit check box and enter the number of occurrences and time interval.
2. For each action, specify the time interval within which it is to be followed by the next action, under the **Followed by within** label. You can specify the time interval in seconds or minutes by using the provided dropdown.
3. To configure advanced options for any of the selected actions, click **Filters** on the top right corner of the action.
4. The first rule starts the session and the last rule ends the session. The duration of the session is the time-interval between the first and the last rule.

Advanced options

Each action in a activity rule corresponds to a log. Logs contain various fields, and each field has a specific value. With advanced options (found under **Filters** on the right of the action), you can provide filter criteria for each field of the log/action and specify a threshold limit on the minimum number of repetitions of the action.

1. You can select a filter field from the dropdown list provided. The fields provided in the dropdown may vary based on the action selected.
2. You can select the comparison type as **equals**, **not equals**, **contains**, **starts with**, **ends with**, **link to**, or **is constant**, from the dropdown provided.

> Note: When you provide more than one value for an **equals** comparison, the set of values provided are treated as a list of possible values and the action is accepted if any one value from the list is true. The same holds true for the **contains, starts with,** and **ends with** comparisons.

When you provide more than one **not equals** comparison, the set of values provided need to hold true for the action to be accepted.

Link to

The **link to** comparison type is used to check the value of the selected field against the value of a field in another action (belonging to the same rule or the primary action of the other rule). For instance, if the field **Device type** of Action 1 is linked to Action 2's **Device type** value, then Action 1 would get triggered only if the value of both the linked fields are the same.

When you choose **link to**, the icon appears at the end of the filter. Clicking on the icon will present a new tab.

> Note: At least one field of the starting rule should be linked to a field in the ending rule.

Click the check box corresponding to the field of the second action against which you want to compare the value of the previous action. Click OK to complete linking the two actions.

Is constant

The **is constant** option is used to treat the specific field as constant. By selecting this option, a set of repeated actions are accepted by the rule only if this field's value remains constant throughout all the iterations. For instance, if the **Target User** field is kept as constant, then the action gets triggered only when the value of this field remains constant in all the iterations. The action doesn't get triggered if the event is generated with different values.

Activity Monitoring Reports

EventLog Analyzer's Activity Monitoring Reports provide information on Windows, Unix and VPN Sessions. The reports provide details such as Device name, Username, Start Time, End Time, Status, and Duration.

EventLog Analyzer provides the following reports for activity monitoring:

- Interactive Sessions, Remote Interactive Sessions, and PMP Sessions for Windows machines.
- Unix Session Reports to provide you all details about all the Unix sessions.
- VPN Session reports such as Cisco VPN Sessions, Fortinet VPN Sessions, Sonicwall VPN Sessions, Huawei VPN Sessions, H3C VPN Sessions, Meraki VPN Sessions, PaloAlto VPN sessions, and WatchGuard VPN sessions for the respective VPN devices.
- Custom reports are also displayed under the activity monitoring section, if any.

The calendar widget allows you to select the time period for which you want to review the session activity for the selected devices/users. You can also schedule an activity monitoring report. The activity monitoring report can be exported in the PDF and CSV formats, by clicking **Export as**.

To know more details of a particular session, you can click on **View History**. This tab displays all the details as given below:

This page contains the **Configure Fields** and **Advanced View** tabs. The Configure Fields tab allows you to view similar logs generated in a session by extracting logs that have the same field value (Domain, Device Name, Logon ID, and Username). You can choose the field by which you want to retrieve logs by clicking on the desired options from the drop-down box. By clicking on the Advanced View tab, you can drill down and view the raw logs of that session.

Viewing Activity Monitoring Reports

EventLog Analyzer allows you to view the Activity Monitoring Reports for Windows, Unix, and VPN Sessions based on users and devices in the form of **User-Based View** and **Device-Based View**, in addition to the default view.

In the User-based view, you can analyze the weekly login and logout activities of a particular user. You can hover your mouse pointer over a generated user-based report in the table to find the **Weekly Login View** tab. Clicking on this tab displays a timeline graph for every day of the week in which you can view a particular user's active session duration, login time, and logout time for any given day. This view also provides the number of hours the user was active per day and for the entire week. The Weekly Login View report is available only for all system-generated reports.

9.5. Creating Correlation custom rules with the Correlation Rule Builder

EventLog Analyzer comes equipped with a custom correlation rule builder, which allows you to form custom rules easily by combining various network actions, and specifying the threshold limits and filter criteria as per expected attack patterns in your organization. This enables you to create a highly flexible and powerful rule set that suits your specific organizational environment.

To open the correlation rule builder, click on the Correlation tab of the product. Click on Manage Rules on the top right of the tab and select +Create Correlation Rule on the top right. Creating a custom rule involves:

To know more about what correlation is, how correlation rules are structured, and more, see Understanding correlation.

To create correlation rules, select one or more actions from the following groups:

- General Events
- MITRE ATT&CK TTP(S)
- Custom Actions

Building a new rule

To build a new rule, follow the below steps:

1. Select the individual actions that make up the rule, from the categorized list of actions on the left of the screen.
    - You can also search for actions using the search bar on top of the list.
    - You can drag and drop the actions to rearrange their order, or delete the action by clicking on the delete icon ( ) on its right.
    - To detect repetition of the same action within a particular time interval, tick the Threshold limit check box and enter the number of occurrences and time interval.
2. For each action, specify the time interval within which it is to be followed by the next action, under the '**Followed by within**' label. You can specify the time interval in seconds or minutes by using the provided dropdown.
3. To configure advanced options for any of the selected actions, click **Filters** on the top right corner of the action.

Advanced options

Each action in a correlation rule corresponds to a log. Logs contain various fields, and each field has a specific value. With advanced options (found under **Filters** on the right of the action), you can provide filter criteria for each field of the log/action, specify a threshold limit on the minimum number of repetitions of the action, and also bunch the filter criteria into groups, which can be used to create rules for complex scenarios.

1. You can select a filter field from the dropdown list provided. It is to be noted that the filters provided in the dropdown may vary based on the action selected.

2. From the dropdown list provided, you can select the comparison type as one among the following: **equals, contains, starts with, ends with, less than, greater than, between, is malicious, not equals, not contains, not starts with, not ends with, not between, link to, is constant, or is variable**.

> **Note**: When you provide more than one value for an **equals** comparison, the set of values provided are treated as a list of possible values and the action is accepted if any one value from the list is true. The same holds true for the **contains, starts with, ends with, less than**, greater than, and **between** comparisons.

When you provide more than one **not equals** comparison, the set of values provided need to hold true for the action to be accepted. The same holds true for the **not contains, not starts with, not ends with**, and **not between** comparisons.

Less than, greater than, between, and **not between** conditions are applicable only for IP, port number, and privilege fields.

Port range is between 0 and 65535.

Privilege range is between 1 and 15.

Link to

The **link to** comparison type is used to check the value of the selected field against the value of a field in another action (belonging to the same rule). For instance, if the field **Device type** of Action 1 is linked to Action 2's **Device type** value, then Action 1 would get triggered only if the value of both the linked fields are the same.

When you choose link to, the icon appears at the end of the filter. Clicking on the icon will present a new tab.

Click the check box corresponding to the field of the second action against which you want to compare the value of the previous action. Click **OK** to complete linking the two actions.

> **Note**: Using the link to condition, you cannot link a field to another one having the is variable condition.

Is constant

The **is constant** condition is used to treat the specific field as constant. When you select this condition, this action

will get triggered when the field's value remains constant in all the iterations. For instance, if the **is variable** condition is applied for the 'Target User' field in an action, the action would get triggered when the value of this field is the same in all iterations. The action doesn't get triggered if events get generated with different values for that field.

Is variable

The '**is variable**' condition is used to treat a field as a variable. When you select this condition, this action will get triggered when the field's value keeps changing each time it is checked. For instance, if the **is variable** condition is applied for the 'Target User' field in an action, the action would get triggered when the value of the field is different in each iteration.

> **Note**: A field having the is variable condition cannot be linked to another one using the link to condition.

Is malicious

The '**is malicious**' condition is available only for IP address fields. It can be used to check if the detected IP address is present in the predefined list of malicious IP addresses that the product has stored in the internal database.

3. Values which are to be compared against the selected field can be provided directly in the textbox. Specify the value to be checked for, in the corresponding textbox.

1. To add another filter to the same log/action, click the icon on the right side of the value textbox. The new filter gets added on the next line.
   - You can choose if the two filters are to be logically ANDed or ORed with the previous one, by selecting **AND** or **OR** from the dropdown list present on the left side of the second filter.
   - You can delete a filter by clicking on the icon on its right.

2. Filters can be collected together by creating groups. This would help to create correlation rules for complex scenarios. To create a new group, click **+Add group** on the bottom right corner of a log/action.
    - Select the criteria for the filter in the new group. You can also add more filters to the new group.
    - You can delete a group by clicking the Remove group icon on the top right of the group.
3. You can choose if two groups are to be logically ANDed or ORed, by selecting **AND** or **OR** from the dropdown list present between the two groups.

Using vulnerability and misconfiguration comparators:

These comparators are available only after successful integration with Endpoint Central 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).

Note: To utilize the vulnerability and misconfiguration comparators, please configure data enrichment for ManageEngine Endpoint Central. Click here to know how.

Threshold limit filter

A threshold limit filter for an action allows you to specify the minimum number of times the action has to occur (within the time window specified for the action to follow from the previous action), for the rule to be triggered. To set a threshold limit, click on the **Filters** link on the right of the action, and select the **Threshold Limit** checkbox. In the text box provided, specify the minimum number of occurrences.

> **Note**: If the action is the first action in the rule, then you should also provide a time window within which the repetitions have to be observed (as it is the first action and there is no preceding action or time window).

Specifying rule configurations

Along with the rule definition, you can also provide some descriptive information to finish configuring the rule:

- **Rule name**: A unique name for the rule.
- **Rule description**: A short explanation describing the attack pattern that the rule checks for.

Click **Save** to save these rule configurations.

Once you have built the rule pattern and specified the configurations, click **Create** so that the rule gets saved and EventLog Analyzer can start correlating logs to check for this rule pattern.

You can now choose what report will be displayed by clicking on the check box. The selected report will be displayed or

hidden from the Correlation Custom Rules Screen.

Create Custom Action

- To create a Custom Action, click on Manage Custom Actions.
- The manage custom actions popup will open. In the top right corner, click on the "create new action" button.

- The Create Custom Action popup will open.
- Enter the name for the action, action description (if required).
- Choose from the drop downs provided to set the criteria for the action.
- Click on Create.

MITRE Correlation Actions

You can now create correlation rules utilizing the available correlation actions for Mitre ATT&CK TTP(s).

Click here to know more about MITRE ATT&CK TTP(s).

Best practices to be followed while creating correlation rules

Correlation reports are crucial for enhancing an organization's security posture since they provide insight into potential security issues. They also help you identify patterns of malicious activity, and facilitate timely response actions. Here are some best practices for creating correlation rules..

- Make sure that you only enable the rules that the organization requires.
- Depending on the logs obtained, each rule may operate differently in each organization. So, make sure to enable the rules in batches, and then watch the behavior of that particular set of rules in that batch and identify the rules that are actually required. Depending on the requirement, the rules can be fine-tuned to reduce false positives.
- Multi-event correlation rules are typically set up by adding various conditions (action, threshold, advanced operators) into them. The number of logs that match each correlation condition determines the amount of resources required. The larger the matched data set, the more resources required, resulting in increased memory utilization. Ensure the criteria you specify is constrained to reduce the dataset used for analysis; this will limit the memory usage.
- Make sure to monitor the memory utilized by each correlation rule. By determining the memory utilization of each rule, the rules can be fine-tuned for improved efficiency.The correlation memory usage can be monitored by navigating to Settings -> System Diagnostics -> System Info -> View report in correlation information.

Correlation use cases

1. Spearphishing:

An attacker targets an individual by delivering malicious Excel files pretending to be a legitimate file via email. When the victim opens the file, it will run a macro and launche a malicious process capable of doing destructive activities.

- **Event sequence:** Excel document spawning a process and large number of file deletions by the same process.
- **Threshold:** 100 file deletions within 30 minutes.

2. Port scanning attack:

Attackers perform port scanning attacks to identify the weak points in a network.

- **Event Sequence:** A large number of traffic events to multiple ports from the same IP are identified within a short span of time.
- **Threshold:** 1000 different ports within 5 mins.

3. Password spraying attack:

An attacker attempts to access multiple accounts using a few commonly used passwords rather than trying different passwords against a single account.

- **Event Sequence:** Large number of login failed events across multiple devices attempted from the same device within a short span of time.
- **Threshold:** 100 events from the same IP.

4. Impossible travel:

A security alert is triggered when a user's account is accessed from two geographically distant locations within a timeframe that is shorter than the possible time frame between those locations. This condition implies that it's highly unlikely (or impossible) for the same user to have made both access attempts, indicating a potential security breach or account compromise.

- **Event Sequence:** Login attempts made to an account in the same device from different countries within a specified time frame, i.e., the username and device name would be the same but the country would be different.
- **Threshold:** 10 events within 10 mins.

5. Data exfiltration to malicious IP address:

A malicious program exfiltrates data to a malicious IP address which is identifiedby threat analytics.

- **Event sequence:** More than 100 network connections identified as malicious within 5 mins.
- **Threshold:** 100 times within 5 mins.

9.6. Manage Correlation Rules

You can manage all your correlation rules from the **Manage Rules** page, which you can access by clicking the **Manage Rules** button on the top right of the **Correlation** tab. The **Manage Rules** page provides you with a tabular list of all correlation rules:

You can use the search bar ( ) on the top of the table to search for a specific rule. You can use the dropdown on the top right of the table to select the number of rules to be displayed per page.

Rule actions

You can perform a several managerial actions on the rules, by clicking on the respective icons, as described below:

- **Enable/disable rule** (/): The icon implies that a rule is currently enabled, and the icon implies that it is disabled. You can toggle between enabling/disabling the rule by clicking on these icons. When a rule is disabled, EventLog Analyzer does not check for the pattern and does not report on the rule.
- **Update rule** ( ): You can modify the rule definition and configurations by selecting this icon, which takes you to the correlation rule builder page. You can modify all details except for the rule name.
- **Delete rule** ( ): You can delete any of the custom rules created by clicking on this icon. Predefined rules cannot be deleted.
- **Enable/disable notification** ( ): You can enable or disable notifications/alerts for the correlation rules by using this option. You can view and manage correlation alerts under the **Alerts** tab of the product:
    - View correlation alerts, assign owners and track their status under **Correlation Alert Profiles**.
    - You can update notification settings for each correlation alert profile on the **Manage Alert Profile** page.

You can also enable or disable a group of rules by selecting the rules and clicking on the enable or disable icon on the top of the table. You can enable or disable all rules by using the **More Options** dropdown.

10.1. Compliance Reports

Organizations must maintain audit reports to demonstrate compliance. EventLog Analyzer provides predefined audit reports for IT regulations such as FISMA, PDPA, CCPA and CPRA, PCI DSS 4.0, SOX, HIPAA, GLBA, POPIA, GPG13, Cyber Essentials, ISO 27001:2013, ISO 27001:2022, ISLP, NRC RG 5.71, GDPR, FERPA, NERC, CoCo, CMMC, NIST CSF, QCF, TISAX, SAMA, ECC, PDPL, CJDN, UAE-NESA, SOC 2 and LGPD. The predefined audit reports are automatically generated and can only be disabled, not deleted.

Configuring custom compliance reports

EventLog Analyzer allows you to create custom compliance reports for IT regulations that aren't supported out-of-the-box or to meet internal organizational policies.

1. Navigating to the **Compliance** tab of EventLog Analyzer and the option to **Manage compliance** can be accessed from the top right corner.
2. Click on the **+Create New Compliance** button.
3. In the **Add Compliance** page, enter a name for the compliance mandate in the **Compliance Name** field.
4. Click on the **Description** link to enter a brief description about the compliance mandate.
5. In the **Source Selection** box, click on the required device tab.
6. Select the devices for which you want to generate reports by clicking on the + icon present in the **Select Devices** field.
7. Select the reports to be generated for this compliance mandate from the list of reports displayed.
8. Click **Save**.

Editing and deleting compliance regulations

You can edit and delete compliance regulations by navigating to the **Compliance tab → Manage Compliance** page and clicking on the edit and delete icons present against the compliance mandates. You can use the **Show/Hide** toggle button to show or hide the compliance regulations in the left pane of the Compliance tab.

Compliance can also be edited through the respective compliance widgets.

Scheduling compliance reports

You can schedule and send compliance reports to your mail IDs by following the below steps:

1. Navigate to the **Compliance tab → Schedule Compliance → +Create New Scheduler** page.
2. Enter a name for the scheduler in the **Scheduler Name** field.
3. Select the compliance for which you want to schedule reports from the drop-down menu.
4. In the **Schedule Frequency** field, select the frequency and the date and time at which the reports have to be scheduled.
5. You can generate the report for a specific time frame by selecting an option from the **Report For** drop-down menu.
6. Select the format of the report from the **Report Format** drop-down menu.
7. Select the type of report you want to generate: **Only Summary** or **Summary and Details**.
8. Enter the mail IDs to which the report has to be sent in the **Email ID** field. Use a comma (,) to separate multiple mail IDs.
9. Enter a subject line for the mail in the **Subject** field.
10. Click **Save**.

Editing and deleting compliance schedulers

You can edit and delete compliance schedulers by navigating to the **Compliance tab → Schedule Compliance** page and clicking on the edit and delete icons present against the compliance mandates. You can also enable/disable schedulers by clicking on the icon present under the **Actions** tab.

10.2.1. Risk Posture

A company's overall capacity to identify and respond to risks is referred to as its risk posture. It entails inspecting every aspect of a company's network and identifying potential vulnerabilities. All users, network elements, and any information that may be stored but is at risk of being hacked are included. It also involves examining current security practices and software to assess how well they can fend off attacks.

Edit Compliance

- Go to **Manage Compliance**.
- Select the required risk posture source.
- Click **Edit** to edit parameters of the rules with the possible values to get your personalized scores. (By default, the recommended values from the Microsoft/CIS standards will be present).
- There is an option to edit risk posture source configurations from the risk posture widget as well.

Run Analysis Schedules:

- You can get the fresh analysis results by clicking the Run Now link at the top left corner of the Risk Posture.
- The frequency can be set by clicking the **Schedule** button next to the Run Now Link.
- By default, the schedule will run once per day. It also allows you to change the frequency of analysis.
- Click the **Schedule** button to see the time when the next analysis is scheduled to run.
- You can also see the time when the last analysis has been completed.
- There is also an option to run analysis from the compliance widget.

Rule Status and its definitions

Low/No Risk

This status informs that the selected source's configurations have met the Recommended / User set compliance value as per their norms.

High Risk

This status informs that the selected source's configurations have not met the Recommended / User set compliance value as per their norms.

Unable to Verify

This status informs that the EventLog Analyzer server was unable to fetch the required data needed for analyzing the specific rule. It can be due to the following reasons.

Troubleshooting steps

SQL Server

Possible reasons for the status "Unable to verify" are as follows:

1. SQL Server down
2. Insufficient server details/user credentials

SQL Server down

The analysis requires SQL Server to be up and running. If the SQL server is down, the analysis cannot be completed.

Troubleshooting Steps:

- Make sure the selected SQL server(s) is up and running.

Insufficient server details/user credentials:

The selected SQL server(s) configuration details and credentials should be up to date and valid. Outdated or wrong details will cause analysis to fail. The configured user should have sysadmin role in the selected SQL server for all the rules to succeed.

Troubleshooting Steps:

- Update credentials and server details in **Settings → Log Source Configuration → Database Audit**.
- Update Advanced Auditing credentials in **Settings → Log Source Configuration → Database Audit → Advanced Auditing**.
- Refer here for more details.

Possible Reasons for "No SQL Server(s) Configured" in edit compliance are as follows:

1. No SQL server(s) is configured.
2. Advanced Auditing not enabled for the SQL server.

No SQL server(s) is configured

To configure MSSQL DB, please refer here.

Advanced Auditing not enabled for the SQL server

To enable Advanced Auditing, please refer here.

10.2.2. SQL Server

Data is a critical asset of every organization, and poorly-secured databases are often the reason for security breaches. SQL Server is designed to be a secure database platform, however, using the default settings leaves security gaps in the system. SQL Server has many security features you should configure individually to improve security. This page details SQL server security best practices and essential security considerations for protecting your databases from malicious attacks.

The major predefined rules in risk posture are

1. Ad Hoc Distributed Queries

Description:

Ensure '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 'Ad Hoc Distributed Queries', 0; RECONFIGURE;
> GO
> EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;

2. CLR Assembly Functions

Description:

Ensure '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 '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 '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 '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 '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 server. 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'

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 '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 '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 '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 malicious CLR 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 '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 in 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, change the TCP Port field from 1433 to a non-standard port or leave the TCP Port field empty and set the TCP Dynamic Ports value to 0 to enable dynamic port assignment and then click OK.
- In the console pane, click SQL Server Services.
- In the details pane, right-click SQL Server (<InstanceName>) and then click Restart, to stop and restart SQL Server.

> **Note**: The connection settings of any application that uses port number to communicate with 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:

- Shutdown 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 '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 SQL Browser service to discover SQL Server instance will not be able to discover the instance automatically if 'Hide Instance' is enabled. Either the 'Hide Instance' should be temporarily disabled or port number should be used to connect to 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 different user while altering the 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 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.

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 SQL Server connection need to be reconfigured 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 '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: 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. 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 role.

Best Practice:

No extraneous permission must be given to public role and should be removed if given and delegated to user defined role if needed.

Recommendation:

Add the extraneous permissions found in the results to the specific logins to user-defined server roles which 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 role, '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 very 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 may it be BUILTIN or user defined, they 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 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
  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 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 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. 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 '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'

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 '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 '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:

```
> 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 Errorlog. 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 Errorlog 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

Description:

Ensure 'SQL Server Audit' is set to capture both 'failed' and 'successful logins'

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 just 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 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 prior to 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;
```

34. 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 database must use 'AES_128' or higher as encryption algorithm.

Recommendation:

Refer Microsoft learn for learning about Altering symmetric key.

If required, use 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 to use at least a 2048-bit encryption algorithm for asymmetric keys. The RSA_2048 encryption algorithm for asymmetric keys in SQL Server is the highest bitlevel 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:

Refer Microsoft learn for learning about Altering asymmetric key.

If required, use following T-SQL command to drop asymmetric keys:

```
> USE <database_name>
  GO
  DROP ASYMMETRIC KEY <key_name>;
```

11.1. Log Search in EventLog Analyzer

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"

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.

11.2. Saving search and exporting search results

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.

11.3. Custom Log Parser

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 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**.

11.4. Tagging tool

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.

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.

12.1.1. Overview

- 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:

- 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.

12.1.2. Access

Please refer the Overview page to learn about Incident Workbench. This page details on how to access the workbench in EventLog Analyzer.

Invoking Incident Workbench from different dashboards of EventLog Analyzer:

- From Reports

- From Log Search

- From Alerts

- From Compliance dashboard

- 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.

12.1.3. User analytics

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. 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 Risk Score Trend, Peak Risk Score and the Cards Based Peak Risk Score for insider threat and data exfiltration. Click on the Calendar icon and set the required period.

Other than the risk score analysis, the following messages will be displayed for the specific cases:

- UEBA not purchased

- Baseline creation is in progress as the model is training

- The particular user has no anomalies

EventLog Analyzer
Search
Incident Workbench
User Risk Analysis
User Activity Overview
User Details
No Anomaly

User Activity Overview

Note: User activity overview does not require UEBA

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: User details doesn't require UEBA

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.

12.1.4. Process analytics in Incident Workbench

The Process Analytics section of the Incident Workbench showcases process spawning with the parent child relationships and the process event details.

Note:

1. 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

1. Device Name: The device in which the process is active for the selected period.
2. 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. 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. The Process being analyzed currently will be highlighted in orange and the rest of the linked processes will be in a different color.
5. 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.

12.1.5. Advanced Threat Analytics

Note:

1. 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 accesed once the add-on 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, you can use your API 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.

12.1.6. Incident building

This page explains about building incidents using the instances of the Incident Workbench. Check the Access page to learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer

> **Note:** 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.

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.

12.2. Device Summary

The Device Summary is EventLog Analyzer's analytical console to view the overall device summary events and contextual data. Users can find the machine summary and event summary for the selected period, top active users, file monitoring events, device severity events, and alerts summary.

Access:

Users can access the Device Summary from multiple dashboards of EventLog Analyzer such as Reports, Log Source, Alerts, Incidents and others.

From Log Source

From Reports

From Incident dashboard

Analysis

Other than the device summary, based on the configurations, users can also access activity overview for the configured web servers, databases, endpoint security solutions, and vulnerability scanners.

SQL Overview

IIS Overview

FireEye Overview

OpenVas Overview

1. Device list dropdown - Click on the dropdown option and select from the list of devices to analyze.

2. Click on the arrows to proceed to the previous device or next device.
3. Click on specific users in the **Top 5 Currently Active Users section** to view the **Interactive Sessions History** with domain details, session details, and events history.

Click on **Details** in the Interactive Sessions History popup to view the individual **Event Details** containing Event ID, Process Name, Domain details and Access Rights

EventLog Analyzer
ELA-W2019-SQL
Device Overview
Machine Summary
Important Events
Severity Events
Top 5 Currently Active Users
Event Details
Security ID : Information
Domain : ZOHOCORP
Task Category : Special Logon
Device Type : Windows
Logon ID : 0x3424228
Event ID : 234324
Process Name : 34Sennew
Domain : eventloganalyzer.com
Group ID : 8683
Access Rights : SeSecurityPrivilge
SeTakeOwnershipPrivilage
SeLoadDriverPrivilage
SeBackupPrivilage
SeRestorePrivilage
Close

13.1. Event Alerts

EventLog Analyzer keeps you informed about security events of interest with its alerting feature. The solution audit logs identifies indicators of compromise (IoCs) and notifies you via SMS or email as required.

The alerts are categorized on three severity levels: Attention, Trouble, and Critical. The severity level indicates the degree of importance associated with the alert. This helps you prioritize alerts and remediate them quickly.

EventLog Analyzer offers a powerful real-time event response system with which you can generate:

- Security event alerts including those for imported logs
- Compliance-specific event alerts.
- File integrity monitoring alerts for critical changes occurring in sensitive files/folders.

Predefined and custom alert profiles

EventLog Analyzer provides 1000+predefined alerting criteria that address a wide range of security use cases. You can also customize alert profiles based on your needs. With additional parameters such as the threshold and time range, you can specify the precise criteria for the alert to be triggered. This helps you be informed about any critical event that might affect your organization's security.

Remediation through alerts

You can also manage a security incident within the EventLog Analyzer console or by raising tickets in an external ticketing tool like ServiceDesk Plus, ServiceNow, Jira Service Desk, Zendesk, Kayako, and BMC Remedy Service Desk. This ensures accountability and helps build an effective event response system.

You can also designate a workflow for a triggered alert to automatically initiate responses such as disabling the affected Active Directory user account, shutting down a system, and killing a process.

The list of all alerts triggered can be viewed under the Alerts tab.

13.2. How to create an alert profile

EventLog Analyzer provides predefined alert profiles and the ability to define customized criteria for specific requirements.

Creating Alert Profiles

To create an alert profile, click on **+Add** in the top right corner of the navigation bar. You can also add an alert profile by clicking on the "Add Profile" button in the Manage Profile page.

Here's what you can do to create an an alert profile:

1. Enter a unique name for the alert profile.

2. Assign a criticality to the alerts generated using this profile. Choose from **Critical, Trouble** and **Attention**.
3. Click on the icon to select device(s) and/or device groups(s) which should generate this alert.
4. Click on the icon to define the alert criteria.
5. The Alert criteria can be chosen from the following categories:
   - Predefined Alerts - choose from a vast collection of predefined alert criteria. This saves time and you can set up an alert profile with minimum effort.
   - Compliance Alerts - Contains a list of pre-defined alert criteria to help you comply with all the IT regulations.
   - Custom Alerts - customize your own alert conditions based on log message, type, and more. This option is useful to set alerts for imported logs.
6. You can customize your alert message by adding information such as User Account Name and more.

7. Clicking on **+Add** near the Alert Format Message section will open another pop-up. There you can set the variables by clicking on the drop down and enter the required message format in the space provided.

8. You can use the **Advanced Configuration** to tweak the alert trigger conditions in order to reduce alert noise. The Advanced Configuration has 2 fields:

Threshold

You can set the threshold for alerts based on the number of occurrences of an event within a specific time frame. There are 2 threshold modes: Manual and Smart.

- Using the **Manual Threshold** mode, you will have to manually assess and set the values for the number of events and the time interval in minutes.

- Using the **Smart Threshold** mode, you will only have to enter the time interval. EventLog Analyzer will analyze the usual occurrence of events based on ML algorithms and automatically determine the number of events that will be ideal for reducing false positive triggers.

Time Range

You can use **Time Range** to configure working hours.

9. Under **Alert Notifications**, you can configure the **Notification Settings** and the **Workflow** for the alert profile.

Notification Settings

- Select the preferred time during which the notification has to be sent.

- Choose the preferred medium for receiving notifications. You can either choose **Email Notification** or **SMS Notification** or both. You can find the steps to configure the mail server and SMS server here.

Workflow

- Check the **Enable Workflow** box to select the required workflow, or to add a new workflow for the alert profile.

10. Click **Save Profile**.

Predefined Alerts

Select **Predefined Alert** under **Define Criteria**:

- Select the log type and then choose the desired category.
- Among the reports, select the desired report by clicking on the radio button next to it.
- Append new criteria to predefined alert by clicking **+ Add Criteria**.
- You can use the **Advanced settings** to tweak the alert trigger conditions in order to reduce alert noise. Here you can set the threshold (number of occurrences of an event within a specific time frame) and time range (working hours) for the alert profile.

You can then specify the notification type for the alert profile.

Compliance Alerts

Compliance alerts contain sets of pre-defined compliance related alerting criteria to notify you of any violation of IT regulations. EventLog Analyzer provides granular audit reports to help you comply with compliance regulations such as PCI DSS, SOX, HIPAA, GLBA, PDPA, NIST, CCPA, GDPR, ISO 27001:2013, and more. The compliance alerts detects anomalies such as policy changes, privilege escalations, sensitive file access and modification events, and unauthorized logons to help you mitigate internal and external threats.

You can then specify the notification type for the alert profile created.

Custom Alerts

- You can define 'n' number of criteria and group them with **AND/OR** operations.
- To define alert criteria, choose desired attributes from the predefined list.
- Specify the values for the attributes. Select the comparator and then provide the value for the attributes.
- With drag and drop, you can group and ungroup the alert criteria.

Generating Alerts for Imported Logs

With EventLog Analyzer's **Advanced Custom Alert** option, you can generate alerts for custom extracted fields for Oracle, Microsoft SQL, print Servers, IIS, and other imported application logs.

To generate alert for specific custom extracted field of imported log, choose the log type and select the imported log for which you need to trigger alerts. Specify the custom field and its value, upon the occurrence of which the alert has to be triggered. EventLog Analyzer will automatically populate all the custom extracted fields for the selected log type and you choose the field of your choice from the list and then specify the value for the selected custom field.

> **Note**: To add multiple custom extracted fields, make use of + option.

You can then specify the notification type for the alert profile created.

Using vulnerability and misconfiguration comparators:

- **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).

Note: To utilize the vulnerability and misconfiguration comparators, please configure data enrichment for ManageEngine Endpoint Central. Click here to know how.

Default Alert Profiles

EventLog Analyzer has prebuilt alert profiles that are enabled by default. To make it easier for users, newly added devices will also get added automatically to the corresponding alert profile(s) based on the device types selected in the alert profile. For example, firewalls will be automatically added to alert profiles based on network devices.

You can edit, enable, disable, and delete the default alert profiles.

> **Note**: When you edit a default custom alert profile, auto-addition will be stopped. For example, if you manually add devices to an alert profile, devices will not be automatically added to that alert profile from then on.

13.3. Active Alerts

The **Alerts** tab lists details of all alerts triggered (if you have not set up any alert profiles, the tab directs you to do so). You can view the timestamp of the alert, the device which triggered it, the severity, the status of the alert, and the message.

Filtering Alert Profiles

- Click on the filter icon at the top-left corner of the table.

- The **Filter Alerts** pop-up opens. Here, you can select the appropriate filter options based on the various Alert Parameters and Alert Criteria-Based Fields available.

- You can also select one or more filter options to customize your alerts view.

Creating Alert Views

EventLog Analyzer categorizes the alerts as views Active alerts, Critical alerts, Trouble alerts, Critical alerts, Attention alerts, and All alerts. You can select the required view from the **Select view** drop-down menu.

You can also create custom views for alerts by configuring a filter for the alert and clicking Apply. Click the **Save As View** link to enter a name for the view and click **Save**.

The custom views can only be viewed by the respective users who created the views. Hover your mouse pointer over the created view in the Select View drop-down menu to edit and delete the created views.

Alert Configurations

You can access the following options from the top right corner of the Alerts page:

- The Export As drop-down menu allows you to export alert messages in the CSV and PDF formats.

- The +Add Alert Profile link allows you to add a new alert profile.

Click the settings icon on the top right corner of the page to view the following options:

- **Workflow**: This option allows you to assign workflows to alert profiles to execute a logical action in your network when an adversity is detected.
- **Ticketing tool Integration**: This option allows you to configure an external help desk software (ServiceDesk Plus, ServiceNow, Jira Service Desk, Zendesk, Kayako, and BMC Remedy Service Desk) to forward the alerts to.

Whitelisting Threats

Click on the check boxes to select the required alerts. Once the alerts are selected, the options Assign, Status, Delete, and More will appear. You can assign the alert to an administrator, change the status, or delete the alerts by choosing the appropriate options.

Clicking on **More** will give you the option to **Whitelist the Source**. In case an alert is raised by Advanced Threat Analytics and you are convinced that the source is not malicious, you can whitelist it by choosing the option here.

Information on the alert

Hovering over the alert gives additional information such as what triggered the alert, the domain, the device involved and more.

Alert Format Message

Clicking on an alert opens a pop-up titled Alert Format Message.

Details such as SL Event ID, Logon Type and more can be obtained by clicking on **More Details**.

Workflow status

In case a workflow is configured for the alert, the status of the workflow can be viewed in the Alert Format Message pop-up.

Click the status of the workflow for more information. Once clicked, a pop-up will open.

Threshold alerts

For Threshold based alerts, you can now view each instance by clicking on the alert. There will be a section called **Threshold**.

Clicking on the threshold number will give you a pop-up with more details.

Add / Remove Columns

Cloumns can be added or removed by clicking on the Add / Remove option in the top right corner. You have the option to choose and rearrange the columns as needed. A minimum of 3 and maximum of 7 can be selected.

> **Note**: The default columns cannot be removed and rearranged. The default columns are Time, Notes, and Alert Format message.

Clicking on this will give you a pop-up. Choose the required options by clicking on the checkboxes.

Advanced Threat Analytics Alerts

These alerts are raised when malicious domains, URLs, and IPs intrude into your network. Clicking on this alert will give you a reputation score, the number of times it had appeared on a threat list and more.

EventLog Analyzer
Advanced Threat Analytics

13.4. Alert Notification & Remediation

EventLog Analyzer provides you with two alert notification mechanisms

Further, you can also remediate the alert condition by creating incident workflows.

Settings to notify alert by Email

Enter the details required for sending alert notification via email.

1. Enable the **Email Notification** check box under the **Notification Settings** tab to enable email notifications.
2. Choose **Send Notification**: Choose the desired frequency for receiving **alert notifications**. This will notify you whenever an alert has been triggered, based on the frequency you set.
   - **All Alerts**: An alert notification will be generated for each alert created.
   - **Once a day**: An alert notification will be generated only once daily.
   - **Once a week**: An alert notification will be generated weekly once.
   - **Once a month**: An alert notification will be generated monthly once.
   - **Custom**: You can also tailor the notification schedule by predetermining the exact number of days, hours and minutes between each notification.

3. Specify the **receiver's email address** and for multiple emails, separate the addresses with commas (,).
4. Add a **subject line** for the email notification. You can also append the alert argument(s) to the subject line. Select the arguments from the list available under Macros.
5. The **default mail content** is shown above, you can modify this and also add arguments from the Macros list. Click **Save Profile**.

> **Note**: The email content of **correlation alerts** can be customized to include the **rule name, correlated time**, and the **action**. Furthermore, you can select and **add specific fields of the action** by choosing them from the list that appears when the action is clicked. Please refer to the image below.

6. If the mail server is not configured in EventLog Analyzer, you will be prompted to when **Notify by Email** option is selected.

Settings to notify alert by SMS

Enter the details required for sending alert notification using SMS.

1. Enable the **SMS Notification** check box under **Notification Settings** tab checkbox to enable SMS notifications.
2. Enter the recipient's number.
3. You can customize the SMS content by clicking **Add More Fields** next to **SMS Message** field.

If SMS settings is not configured in EventLog Analyzer, you will be prompted to set it when **Notify by SMS** option is selected.

> **Note**: Notification using Run Program can now be configured with Incident Management Workflows.

Assigning Workflows to Security Incidents

You can associate incident workflows with the security alerts configured in the product. This way, when a security alert is triggered, the corresponding workflow automatically starts executing, and you can view its status on the **Manage Workflows** page.

To assign a workflow to a new security alert:

- Navigate to **Alerts → +Add Alert Profile**, or

- Click on **+Add → Alerts**

And configure your alert as given above.

To assign a workflow to an existing alert:

Navigate to **Alerts → Alert Configurations → Manage Alert Profiles →** Select the update

OnDemand Workflows

Users can run workflows and view their statuses directly from the **Alerts** console.

To run a workflow for an alert,

- Select an **Alert** and click **the Run Workflow** button under **Workflow Status**.

- Select a workflow from the drop down menu and click **Run**.

- You can select **Associate to Alert Profile** to assign a workflow to the alert profile on the dashboard directly.

You can check the status of the workflow by clicking **Workflow History**.

You can also run multiple workflows for a single alert.

13.5. Ticketing Tool Integration

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, add, edit, and delete 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 **Data Center** in drop-down list. Click **API Registration URL** to generate **Client ID** and **Client Secret ID**.

2. Once the Zoho API Console is opened, click **GET STARTED**.

3. Select the **Server-based Applications** tile.

4. To create a new client, enter the required details. Enter the redirect URL as given in the EventLog Analyzer console and click **Create**.

5. Copy the generated **Client ID** and **Client Secret ID**.

6. Back in the ELA console, paste the **Client ID** and **Client Secret ID** in the corresponding fields.

7. 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.
8. 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.

9. Click **Accept** for API approval.

10. Click the **Verify** button in ELA console. The ticketing tool will now be configured successfully.

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.

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.

For ServiceNow

> **Note**: Only users who have been granted permissions to execute create, read, write, and delete operations on the incident table 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.

For JIRA Service Desk On-Demand

> **Note**: Only users with permissions to create, delete, and edit issues 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.

For Zendesk

> **Note**: Only users with Admin/Agent privilege can proceed with the configuration.

Configuring Zendesk with OneAuth authentication:

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. The value that appears corresponding to Unique Identifier needs to be saved in a separate document. This would be needed while configuring Zendesk in EventLog Analyzer.
6. 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.
7. 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 **Login Name** and **Password** of a valid account in the ticketing tool.
- 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.

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.

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.

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.

For ManageEngine ServiceDesk Plus

> **Note**: Only users with permissions to view, add, edit, and delete 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.
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.

For ManageEngine ServiceDesk Plus MSP

> **Note**: Only users with permissions to view, add, edit, and delete 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. Enter the **Subject** and the **Message** for the alert. You can choose them from the predefined list available under **Macros** or type your own.
6. Click the **Test and Save** button.

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.

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.

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.

13.6. Manage Profiles

With EventLog Analyzer, you can centrally view and manage the configured alert profiles.

- In the **Manage Profiles** tab, you can add, enable, disable, export, and import alert profiles.

- Here, you can also filter a specific category of alert profile by selecting the required option from the drop-down.

Import Alert Profiles

Alert profiles can be imported or exported by clicking on the Import option. Once you select an option, you will get the message below.

Select the file from which you wish to import the alert profiles by clicking on **Browse**.

In case an imported alert profile is similar to an existing alert profile, you will get the message below. To overwrite an existing profile with an imported profile, select the required profile and click on **Import**.

What are Sigma rules?

Sigma is a text-based format for describing security events in log data, which simplifies security threat detection.

EventLog Analyzer allows you to import these rules in the **Alerts** tab.

From **Alerts**:

- Navigate to the **Alerts** tab, and select **Manage Profiles**. Choose the **Import** option.

- EventLog Analyzer supports importing Sigma rules from YML files.

- During the import process, you will have the option to map fields and the log type associated with the Sigma rule. Click **Save**.

- Click **Save** to finalize the import process. EventLog Analyzer will store the imported Sigma rule profile along with its defined criteria.

Note: False positives mentioned in the Sigma rule file are not included in the criteria. Users have to manually add those criteria after importing the Sigma rule file.

Export alert profiles

To export alert profiles, select the required alert profiles and click on Export.

Note: Default alert profiles cannot be exported.

Filtering alert profiles

To filter alert profiles based on the number of alerts raised, click on the number of alerts under the No. of Alerts column.

Showing and select the required category.

To configure notifications for the alert:

To configure notifications for the alert, click on **configure**. You will be directed to the edit alerts page. You could set the notification type there.

Delete Alert profiles

To delete an alert profile, select an alert profile and click on the delete option. A pop-up like the one shown below will appear. Click on yes to proceed.

13.7. How to delete/update alerts in bulk:

1. Navigate to the Alerts tab of EventLog Analyzer.
2. Select the dropdown icon near check box in the table, click **Select All**.

3. Choose the delete option to remove specific alerts, or select the status option to change the status of alerts.

4. After selecting, confirm the action by clicking **Yes**.

5. Below are a few more ways to bulk delete or update alerts.

   - By using filters:

   - By using widgets or select view:

Verify request status with notifications:

In the notification tab, users can verify the status of their pending and active bulk modification requests.

Modification records:

To verify the success or failure rates of the requests and get more details about the modification requests, go to **Settings > Technicians & Roles > User audit**.

Note: Bulk modification queue will be paused when alerts unarchive process is running and resumes automatically once the process is complete.

14.1. Incident management

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, and Critical incidents 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.

14.2. Incident workflow management

You can mitigate security incidents in your network before they result in a breach by automating response workflows when alerts are triggered. EventLog Analyzer allows you to create workflows to automatically perform actions such as disabling USB ports, shutting down systems, and changing firewall rules when security incidents are detected.

Steps to create a workflow

1. In EventLog Analyzer, click on the **Alerts** tab.
2. Click on the **More tools** icon present at the top-right corner of the page.
3. Click on **Workflow** to open the Manage Workflow page and click on the **+Create Workflow** button.
4. Enter a name for the workflow in the **Workflow Name** field.
5. Click on the **Description** link next to the Workflow Name field to enter an appropriate description for the workflow.
6. Create a workflow by dragging and dropping the workflow blocks from the left pane into the space provided. Ensure that these blocks are logically arranged to execute an event in your infrastructure.

   EventLog Analyzer contains multiple workflow blocks to help you configure workflows to perform the required actions. The logic blocks are categorized under different sections.

   The list of workflow blocks and the details to be specified while configuring workflows using them are given below:

Logic blocks	Details to be specified
Logic actions	
Decision Allows you to branch the workflow based on the status of the previous action.	
Time Delay Allows you to introduce a time delay in the execution of the workflow.	The time delay in minutes.
Network actions	
Ping Device Allows you to ping a device within your network to check connectivity	• The name of the device to be pinged. • Number of echo request messages to be sent. • Size of the packet to be sent. • Timeout for the action. • Number of action retries within the specified time.

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.
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.
Linux actions	
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.
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.
Active Directory actions	
Disable User Allows you to disable a user's account.	The name of the user account you want to disable.
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.
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.
ADManager Plus actions	
Workflow 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 workflow. • 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 workflow. • 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 workflow. • 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 workflow. • The username of the user account you want to add to the group. • The name of the group you want to add the user.

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 workflow. • 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 workflow • 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 workflow. • 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 workflow. • 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.

Delete Computer Allows you to delete a computer account	• The name of the block. • The action to be performed(here, Delete Computer). • A brief description for this block to record its purpose in the workflow. • 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 workflow. • The device name of the computer account you want to enable.
Endpoint Central actions	
Workflow Blocks	**Details to be specified**
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.

Note: To utilize the Endpoint Central actions, please configure data enrichment for ManageEngine Endpoint Central. Click here to know how.

7. You can enter a brief description for each logic block to record its purpose in the workflow. This makes it easier for you to understand and edit the workflow later.

8. Click on the **Save** button to create the workflow.

To edit an existing workflow you can click on the edit icon present against the workflow name in the Manage Workflow page.

NOTE:
List of devices supported:

- All types of Windows operating system.
- Linux operating systems :
  - Ubuntu
  - Debian
  - Fedora
  - CentOS
  - Red Hat Enterprise Linuc (RHEL)
  - Arch Linux
  - SUSE Linux Enterprise Server (SLES)
  - openSUSE
  - Gentoo OS

Managing workflows

You can view and edit existing workflows in EventLog Analyzer by navigating to the **Alerts** tab and clicking on **Workflow** from the **More tools** icon. The Manage Workflows page displays the list of workflows, their descriptions, the number of alert profiles associated with each workflow, and their histories. You can enable or disable, delete, edit, and copy the workflows by clicking on the respective icons.

Updating workflow credentials

You can automate workflows on Windows, Linux, and Cisco devices for which you have administrative privileges. You have to update credentials of these devices in EventLog

Analyzer for seamless execution of the workflows.

To automate workflows in Windows devices:

If the Windows devices have already been added to EventLog Analyzer, workflows can be executed by using the devices credentials or the domain credentials of the devices. So, you need not manually update credentials for Windows devices.

To automate workflows in Linux devices

You can configure a set of common credentials for executing workflows in all Linux devices by following the steps given below:

- Click on the **Workflow Credentials** link present in the Manage Workflow page.
- Select credential type as Linux Devices.
- Enter the username, password, and port number.
- Click on **Update** to store and use these credentials to execute workflows in all Linux devices.

To automate workflows in Cisco devices

You must configure the REST API agent in the Cisco firewall to execute workflows 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 workflows in all Cisco devices using EventLog Analyzer by following the steps given below:

- Click on the **Workflow Credentials** link present in the Manage Workflow page.
- Select credential type as Cisco Devices.
- Enter the username and password.
- Click on **Update** to store and use these credentials to execute workflows in 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:

- Navigate to **Settings → Configuration → Manage Devices → Syslog Devices**.
- Hover your mouse pointer near the device on which you want to execute workflows and click on the edit icon.

- In the Update Device pop-up menu, click on **Advanced**.
- Select the **Configure REST API Credentials** check box.
- Enter a username and password.
- Click on **Verify Credential** to send a REST API call to the Cisco device to verify if the credentials are valid.
- Click on **Update** to store and use the specified credentials for executing workflows.

To automate workflows in Fortigate devices

In order to generate an API token to execute workflows in Fortigate devices, you need to create a new REST API Admin using the steps given below:

Step-1: Create Administrator profile

- Navigate to **System** from the sections listed on the left in the dashboard.
- Click on the **Admin Profiles** under the **System** section.
- Click the **Create** icon to start creating a new admin profile.
- You will see the **New Admin Profile** window open up.
- Enter an appropriate name for your admin profile.
- Select access control permissions for different functionalities between **None, Read, Read/Write** or **Custom.**
- Select **Read/Write** for both Policy and Address options under Firewall Option.
- Click **OK** to create your new admin profile

Step-2: Create a REST API Admin and generate an API key

- Navigate to **System** from the sections listed on the left in the dashboard.
- Select **Administrators** under **System** section.
- Click on the **Create New** icon.
- Select **REST API Admin** option.
- You will see the **New REST API Admin** window open up.
- Enter an appropriate username for your REST API admin profile.
- Select your previously created **Administrator Profile** from the drop down menu.
- Click on **OK** to confirm your New **REST API Admin.**

- Once you are done with this process, the system will automatically generate a new API key, which will be displayed only once.
- 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 workflows in all Fortigate devices using EventLog Analyzer by following the steps given below:

- Click on the **Workflow Credentials** present on the top-right corner of the Manage Workflow page.
- Select credential type as Fortigate Devices.
- Enter the generated API key along with the Username in the workflow credentials page.
- Click on **Update** to store and use these credentials to execute workflows in all Fortigate devices.

To automate workflows in PaloAlto devices

To execute workflows successfully, API access should be enabled by following the steps given here. 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 workflows in all PaloAlto devices by following the steps given below:

- Click on **Workflow Credentials** on the top-right corner of the Manage Workflow page.
- Select credential type as PaloAlto Devices.
- Enter the created administrator Username/Password.

- Click on **Update** to store and use these credentials to execute workflows in all PaloAlto devices.

To automate workflows in SophosXG devices

You must configure the encrypted password to execute workflows of SophosXG devices to to execute workflows in them. First, generate the encrypted password using the steps given in the links below:

Step 1: Create an Administrator Profile.

Step 2: Create an Administrator.

Step 3: Allow API Access.

Step 4: Generate Encrypted password.

After generating the encrypted password, you can configure a set of common credentials for executing workflows in all SophosXG devices by following the steps given below:

- Click on the **Workflow Credentials** present on the top-right corner of the Manage Workflow page.
- Select credential type as SophosXG Devices.
- Enter the encrypted password along with the Username in the workflow credentials page.
- Click on **Update** to store and use these credentials to execute workflows in all SophosXG devices.

To automate workflows in Barracuda CloudGen devices

In order to execute workflows in Barracuda CloudGen devices, you need to create an X-API Token using the steps given below:

Step 1: Enable the REST API for HTTPS.

Step 2: Create an Administrator Profile for REST API authentication.

Step 3: Create an X-API Token for authentication.

After finishing the process, you can configure a set of common credentials for executing workflows in all Barracuda CloudGen devices by following the steps given below:

- Click on the **Workflow Credentials** present on the top-right corner of the Manage Workflow page.
- Select credential type as Barracuda CloudGen Devices
- Enter the generated Access Token along with the Username in the workflow credentials page.
- Click on **Update** to store and use these credentials to execute workflows in all Barracuda CloudGen devices.

Automating workflows in ADManager Plus

ADManager Plus , an IGA solution with hybrid AD management, reporting, and automation capabilities, must be integrated with EventLog Analyzer for the successful execution of response workflows. The list of actions that can be added to the workflow are called workflow 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 EventLog Analyzer to execute actions via ADManager Plus. Here are the steps:

1. Click on **Workflow Credentials** at the top-right corner of the Manage Workflow page.
2. Select credential type as **ADManager Plus**
3. Fill in the required details about the Host, Protocol, Port and Auth Token.

4. Click on **Update**, to integrate ADManager Plus with EventLog Analyzer.

5. If the **SOAR Workflow** in ADManager Plus is not enabled, integration failure will occur.

6. After a successful integration, the user can begin constructing the workflow.

Additionally, the user will not be able to construct workflows following an unsuccessful integration.

Note:

- Event Log Analyzer version above 12430 and ADManager Plus version above 7224 are required for this integration.
- Integration must also be enabled for EventLog Analyzer in the ADManager Plus integration configuration page.
- One help desk technician (HDT) license can only be used to perform a maximum of 50 actions per day. To perform more actions, ensure you have additional HDT licenses purchased in ADManager Plus.
- The default admin account will not be considered as a HDT account.

Enabling tight integration for EventLog Analyzer in ADManager Plus

To perform Workflow actions from Eventlog Analyzer, tight integration must be enabled from within ADManager Plus. Here are the steps to do this:

1. In ADManager Plus, click on the **Admin** tab.
2. Click on **Integrations** under System Settings.
3. Select EventLog Analyzer under Log Forwarding.

4. Enable **SOAR workflow** by checking the **Allow LOG360 SIEM to execute AD Management actions** box.
5. Click the **Test Connection** and **Save** button.
6. This will enable SOAR workflow in ADManager Plus to execute workflow actions from EventLog Analyzer.

Automating workflows in SNMP TRAP

To automate all SNMP Trap workflows using EventLog Analyzer, you can configure a common credential by following these steps:

- Navigate to the Manage Workflow page and click on the **Workflow Credentials** link.
- Choose **SNMP Trap** as the credential type.
- Enter the **SNMP credential**.

- Click Add/**Update** to save. This credential will now be used to execute all **SNMP Trap** workflows.

Note: Refer to the port management page for details on how to update credentials.

15.1. Integrating and using the MITRE ATT&CK framework with EventLog Analyzer

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

16.1. Configurations

Carry out the necessary configurations required for EventLog Analyzer functioning. You can carry out the following configurations:

- Manage Devices
- Manage Device Groups
- Applications
- Database Audit
- File Integrity Monitoring
- Threat Management
- Threat whitelisting
- Threat Import
- Switching threat stores
- Manage Threat Source
- VM Management
- Manage Vulnerability Data
- Log Forwarder
- Manage Cloud Sources

16.2. Device Management

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?

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.**

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.**

16.3. Applications

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.

Viewing all other monitored servers

EventLog Analyzer lists all the other servers being monitored under **Other application sources** tab. You can view details of the device associated with the application, application type, as well as an option to view the relevant reports.

16.4. Database Audit

This module lets you manage the database servers being monitored by EventLog Analyzer. Applications such as SQL Servers, MySQL Servers and Oracle Servers can be added, deleted, and viewed.

16.5. File Integrity Monitoring (FIM)

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, both Windows server and Windows file server license are required for monitoring.

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 (see how)
  - 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 8400) is reachable from the agent machine.

  To verify if a port is reachable, you can use the below commands:

  ```
  > echo > /dev/tcp/[Server Machine HostName/IP]/[Server Port] && echo "Port is Reachable"
  ```

  Example: echo > /dev/tcp/ubuntu/8400 && echo "Port is Reachable"

  (or)

  ```
  > telnet [Server Machine HostName/IP] [Server Port]
  ```

  Example: telnet ubuntu 8400
- 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:**

```
> visudo -f /etc/sudoers.d/<username>
```

- **Add the below line to the sudoers file:**

```
> <username> ALL=NOPASSWD:
  /opt/ManageEngine/EventLogAnalyzer_Agent/bin/AgentManager *
```

Example:

1. visudo -f /etc/sudoers.d/testuser
2. 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:

```
> mkdir /opt/ManageEngine/
```

Granting privileges to the directory:

```
> setfacl -m u:<username>:rwx /opt/ManageEngine/
```

For CentOS/RHEL v8 and later/Ubuntu/openSUSE/Debian/Fedora:

```
> setfacl -m u:<username>:wx /etc/audit/ /etc/audit/plugins.d/
```

For CentOS/RHEL v6 to v7.9:

```
> setfacl -m u:<username>:wx /etc/audisp/ /etc/audisp/plugins.d/
```

Granting privilege to the audit.rules:

```
> setfacl -m u:<username>:r /etc/audit/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
  a. Certain file types.
  b. Certain sub-locations within the main location.
  c. 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**.

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
  a. Certain file types.
  b. Certain sub-locations within the main location.
  c. 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.

EventLog Analyzer
Home
Reports
Compliance
Search
Correlation
Alerts
Settings
Log Me
Support
Manage File Integrity Monitoring Templates
Configuration
Manage Devices
Import Log Data
Manage Application Sources
Manage File Integrity Monitoring
Manage Threat Source
Manage Vulnerability Data
Manage Device Groups
Manage FIM Templates
Manage vCenter
Log Forwarder
Admin Settings
System Settings
Windows
Linux
Template Name
Locations
Associated Devices
Windows.Update
Temp
SysWOW64
System32
ProgramFiles
Drivers
Dlls

16.6. Manage Security Applications

> 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.

16.7. Threat Management

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.

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

16.8.1. Advanced Threat Analytics

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, 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. 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 accesed 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
   - Investigation: The Threat Analytics information can be accessed through the External Threat report and the Incident Workbench for investigations.
   - 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 reduces 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

EventLog Analyzer

EventLog Analyzer

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.

16.8.2. Log360 Cloud Threat Analytics

- Configuration
- Analysis

Configuration

1. Get the Access Key
   - Navigate to https://log360feeds.manageengine.com/
   - Copy the **Advanced Threat Analytics Feed Server** access key.

> **Note**: For users who do not have a feeds account, please create an account to sign in and obtain the Threat Analytics Feed Server access key.

2. Add the Access Key in EventLog Analyzer and Configure
   - In EventLog Analyzer, navigate to **Settings → Threat Management → Advanced Threat Analytics→ Log360 Cloud Threat Analytics → Integrate**

   - Paste the Access Key in the **Access Key** box

- The scheduler will be enabled automatically. To change the frequency in which the feeds are populated, click the edit button next to Interval.

Note: We recommend whitelisting the URLs "https://log360feeds.manageengine.com/" and "https://log360cloud.manageengine.com/" to establish a connection to Threat Server without being blocked by the firewall.

Analysis

The Log360 Cloud Threat Analytics is available in the Incident Workbench. Learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer.

Select any IP, URL, or Domain to analyze in the Workbench. You can access the following data:

- Info

  This section contains the Reputation Score of the Threat Source on a scale of 0-100.

  > **Note:** The risk factor is inversely proprtional to the Reputation Score.

  You can also view the Reputation Score Trend chart, Status of the Threat Source(whether it's actively part of the threat list), Category, Number of occurences on threat list, and when the source has been released from the threat list.

- Geo info

  The Geo Info contains location mapping details of the Threat Source such as city, state, region and the Whois information of the domain.

- Related Indicators

  This section contains the risk profile of the related indicators of IPs, URLs and Domains.

  Here are the related indicators:

  IP:

  - hosted_urls
  - asn
  - hosted_files
  - hosted_apps

  URL/ Domain:

  - virtuallyhosted
  - sub_domains
  - hosted_files
  - hosted_apps
  - hosting_ips

- common_registrant

Threat Evidences

This section contains eveidences produced by the security vendor for different attacks attempted from the threat source.

16.8.3. VirusTotal

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.

Configuration

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 Workbech. Learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer.

Select any IP, URL, or Domain to analyze in the Workbench. You can access the following data:

- VirusTotal Info

  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 info of the Threat Source are also available.

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 Info

  This section contains the Whois information 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 is the past and current IP resolutions for a particular domain.

16.8.4. Constella Intelligence

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.

- 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

16.9. Threat Whitelisting

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.

16.10. Threat Import

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 **dae.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 **dae.threat.import.schedule.enable** property key from **<dir>\EventLog Analyzer\conf\EventLogAnalyzer\threat folder\threatstore.properties** file back to "false".
- If the **dae.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 FileImportTask.

16.11. Switching threat stores

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**.

16.12. Manage Vulnerability Data

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.

16.13. Device Group Management

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

16.14. VM Management

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.

How to delete a vCenter server?

To delete a vCenter server, select the vCenter you want to delete and click the **Delete** icon.

16.15. Log Forwarder

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.

16.16. Amazon Web Services (AWS)

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
    - **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

- Open the login page of Salesforce and copy the Login URL.

  For instance, https://testingtech-ap48.my.salesforce.com
- Paste the URL in the Login URL field in the format,

  https://login.testingtech-ap48.my.salesforce.com.

Note: Ensure that '**login**.' is added after **https://** in the Salesforce login URL.

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.

17.1. Admin Settings

The Admin Settings helps you to configure the Eventlog Analyzer and to tweak it's functioning as required.

You may carry out the following operations using the admin settings tab:

- Agent Administration
- Archive Settings
- Technicians and Roles
- Logon Settings
- Security Hardening
- Reset Account Settings
- Domain and Accounts
- Log Collection Filter
- Working Hour Settings
- Product Settings
- API Settings
- Retention Settings
- Log Collection Alerts
- Report Profiles
- Custom Log Parser
- Tags
- Profiles

17.2. Privacy 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**.

17.3.1. Agent Administration

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):

- Open **Group Policy Management**.
- In the left pane, right-click the **Group Policy Objects** container and select **New**.

- Give the GPO a suitable name and click **OK**.

Step 2: Configuring script settings

- Right-click the newly created GPO and click **Edit**.

- 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**.
- For Windows Server 2008 and later, navigate to **Computer Configuration → Policies → Windows Settings → Scripts (Startup/Shutdown) → Startup**.

- Right-click **Startup** and in the dialog box that appears, click **Add**.

- In the Add Script dialog box, click **Browse** and select InstallEventLogAgent.vbs from the shared location.

- In the **Script Parameters** field, enter the following parameters:

> /MSIPATH:"< share path of msi file>" /SERVERNAME:" <ELA server name>" /SERVERIPADDRESS:" <IP address of server>" /SERVERPORT: "<port occupied by server>" /SERVERPROTOCOL:" <protocol (http/https)>"

> **Note**: Ensure that the Agent MSI files in the shared folder are the latest version. You can find the latest version in the following path: <Installation directory>:\EventLog Analyzer\lib\native.

Example:
/MSIPATH:"\\192.168.1.5\elaagent\EventLogAgent.msi" /SERVERNAME:"DC01" /SERVERIPADDRESS:"192.168.1.5" /SERVERPORT:"8400" /SERVERPROTOCOL:"http"

- Click **OK** to return to the Startup Properties dialog box.
- Click **Apply** and then **OK**.

Step 3: Configuring Administrative Template Settings

- In the left pane of the Group Policy Management Editor, navigate to **Computer Configuration → Administrator Templates → System**.
- Under **System**, select **Scripts**.
- In the right pane of the GPO Editor, double-click **Run logon scripts synchronously** and enable it.
- Click **Apply** and then **OK**.

- Similarly, enable **Maximum wait time for Group Policy scripts**.
- Then, navigate to **Logon** under **System**.
- In the right pane, double-click **Always wait for the network at startup and logon** and enable it.
- Click **Apply** and then **OK**.

- Then, navigate to **Group Policy** under **System**.

- In the right pane, double-click **Group Policy slow link detection** and enable it.
- 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.

- On the left pane of the Group Policy Management Editor, right-click the GPO you are working on and select **Properties**.
- Navigate to the **Security** tab and unselect the **Apply Group Policy permissions for Authenticated Users**.
- Click **Add** and in the dialog box that appears, click **Object Types**.

- 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**.

- Enter the name of the desired computer(s) and/or group(s) and click **Check Names**.
- Select the desired computer(s) and/or group(s) and click **OK** to return to the properties dialog box.

- 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

- Click **Apply** and then **OK**.
- Right-click on the **Domain** and click on "**Link an Existing GPO...**" option

- Now select the **GPO** you are working on and Click **OK**.

- 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 Eventlogagent.msi in a network-shared folder.
- In the device(s) on which the agent needs to be installed, execute the following command:

```
> msiexec.exe /i "EventLogAgent.msi" /qn /norestart /L*v "Agent_Install.log" SERVERNAME=
  <eventlog_server_name> SERVERIPADDRESS=<eventlog_server_ip> SERVERPORT=
  <eventlog_server_port> SERVERPROTOCOL=<eventlog_server_protocol>
  ENABLESILENT=yes ALLUSERS=1
```

Example:

msiexec.exe /i "EventLogAgent.msi" /qn /norestart /L*v "Agent_Install.log" SERVERNAME="me-eventlog" SERVERIPADDRESS="10.51.241.163" SERVERPORT="8400" SERVERPROTOCOL="http" ENABLESILENT=yes ALLUSERS=1

> **Note:** Values assigned to SERVERNAME, SERVERIPADDRESS, SERVERPORT, and SERVERPROTOCOL should be in double quotes.

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.

```
> msiexec.exe /i "EventLogAgent.msi" /qn /norestart /L*v "Agent_Install.log" SERVERNAME=
<eventlog_server_name> SERVERIPADDRESS=<eventlog_server_ip> SERVERPORT=
<eventlog_server_port> SERVERPROTOCOL=<eventlog_server_protocol>
ENABLESILENT=yes ALLUSERS=1
```

Example:

msiexec.exe /i "EventLogAgent.msi" /qn /norestart /L*v "Agent_Install.log" SERVERNAME="me-eventlog" SERVERIPADDRESS="10.51.241.163" SERVERPORT="8400" 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

```
> <eventlog_server>:<eventlog_server_port>/event/downloadMsi.nms?platform=windows
```

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 8400 for HTTP)

For example: localhost:8400/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:

```
> eval "wget http://<eventlog_server>:<eventlog_server_port>/downloadMsi.nms?platform=agentInstaller -O AgentInstaller && sh AgentInstaller http://<eventlog_server>:<eventlog_server_port> lesssecure"
```

HTTPS Command:

```
> eval "wget --no-check-certificate https://<eventlog_server>:<eventlog_server_port>/downloadMsi.nms?platform=agentInstaller -O AgentInstaller && sh AgentInstaller https://<eventlog_server>:<eventlog_server_port> secured"
```

Example:

Sudo User:

```
> sudo -s eval "wget http://ubuntu:8400/downloadMsi.nms?platform=agentInstaller -O
  AgentInstaller && sh AgentInstaller http://ubuntu:8400 lesssecure"
```

Non-Sudo User:

```
> eval "wget http://ubuntu:8400/downloadMsi.nms?platform=agentInstaller -O AgentInstaller &&
  sh AgentInstaller http://ubuntu:8400 lesssecure"
```

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**.

17.3.2. Agent Settings

The Agent Settings page offers options for setting the maximum size limit (GB) for the collection of logs in the agent's data directory, when the server is unreachable. This ensures critical logs are securely stored in the agent and can be sent once the connection is restored. This prevents data loss arising from server communication gaps.

Configuration	Default Value	Description
Maximum size of data directory, when agent is unable to send data to server	0	When an agent is disconnected from the network, it collects and stores logs up to a configured limit. These logs are then uploaded when the connection is restored, ensuring data integrity for roaming devices.

Steps for configuration:

1. **Settings > Agent Administration > Agent Settings**.
2. Change the data size to the required value.
3. Click **Save**.

17.4. Archive

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:
    a. **Verified** - Archived logs are intact.
    b. **Archive file is missing** - When the flat file is not found during the compression/zipping process.
    c. **Archive file not found** - When an archived file is not available in the location where it was originally stored in the DB.

d. **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".

e. **Archive file available** - When the archive integrity check is disabled, both the verified and tampered files will carry this status.

f. **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.

g. **Access Denied** - When the remote location can't be accessed where the archives are stored

h. **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:**

a. **Loaded** - The archived files are already loaded to the database. Click View to view the file

b. **Data already available** - If the archive file is in Elastic Search database

c. **Data partially available** - If some of the archive data is in ElasticSearch database

d. **Not Loaded** - If the archive file is not in ElasticSearch database.

e. **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.

EventLog Analyzer
Archived Logs

EventLog Analyzer
Dashboard
Reports
Compliance
Search
Correlation
Alerts
Settings
Logfile
Support
Edit archive policy
Back
Log Source Configuration
Admin Settings
Enable archiving
Policy name
Default Config
Retain Archive Logs For
Forever
Archive Log Type
Raw Logs
Archive Zip Location
Local
Note
Click here to change log index location
It is recommended that this location is kept locally for optimal performance
File File Encryption
Disable
Temp File Location
Verify
Logs Retention Period
Days
Advanced
File Creation Interval
Zip Creation Interval
Zip Now
Archive Timestamping
Enable Archive Integrity Check
Enable
Save
Cancel
1
2
3
4
5
5a
6
7
8
8a
8b
8c
8d

EventLog Analyzer
Edit archive policy

EventLog Analyzer
Edit archive policy

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.
   a. **Local** - To store archives in a local location, choose **local** from the dropdown and enter the storage location
   b. **Shared** - To store archives in a shared location, select 'Shared' from the dropdown menu and enter the storage location.
      i. 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.
      ii. Ensure that the remote machine is available and it has sufficient read and write permissions for the share.
   c. **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**"
      i. **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

      ii. **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

iii. **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

iv. **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:

i. AWS console → Services → All Services → Key Management Service → Create key.

Permissions:

i. To list the configured kms keys for your cloud account , provide "kms:ListKeys" policy permission to your IAM user.

ii. 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:
   a. 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.

   b. 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.

   c. Enable **Archive Timestamping** if required. By default, it is disabled.
   d. 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
- **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.

17.5. Technicians and Roles

EventLog Analyzer supports authorization and authentication at a local level and is compatible with third-party applications like Active Directory and RADIUS server. It allows adding users in three realms (user groups) viz., **Admin**, **Operator**, and **Guest**. The Admin realm has the highest order of privilege in the EventLog Analyzer server and UI. The Operator has limited privileges that enables access to perform create and delete operation on the allotted resources. The Guest has read-only privilege on the allotted security resources (device groups).

How to add a new EventLog Analyzer technician?

To add new users, use the following menu option:

- **Settings** tab > **Technicians and Roles** > **Add Technician**

You can either add a user from AD or add a local technician in EventLog Analyzer.

To add a local technician, click on the **Add local technician** link.

1. Enter a name for the technician in the Technician Name field.
2. Enter a new password and confirm it in the respective fields.
3. Enter the email address of the technician in the **Email** field.
4. In the **Roles** drop-down box, choose the role(s) you want to assign to the technician. You can assign more than one role to the technician and permissions of all the selected roles will be assigned to the technician.
5. Assign device group(s) to provide segmented view to the user and limit the privilege on security resources. Select the device group(s) checkbox(es) and click **OK**.
6. Complete the add user operation using the **Add** button.

How to manage (delete, assign role to, assign group to) EventLog Analyzer technicians?

In the **Manage Technician** screen, all the users of EventLog Analyzer are listed along with user's login name, delegated roles, the domain in the network to which the users belong to, and the link to view their audit details. You can delete, enable or disable users and re-assign roles and device groups for technicians.

1. To monitor the users of EventLog Analyzer, click on the **User Audit** icon. This will give you the report of all EventLog Analyzer user activity. You can view the user audit data for the required username, type of user(administrator, operator, guest), resource and action. The report can be extracted into PDF/CSV format.
2. Delete, enable or disable users by selecting the users and clicking on the respective icons.
3. Click on the **edit** icon to update the technician details such as the roles assigned, device groups, email and password.

How to import users from Active Directory into EventLog Analyzer?

- **Settings** tab > **Admin Settings**: **Technicians and Roles** > **Add Technician** EventLog Analyzer will automatically discover and display Active Directory users from the selected domain. You have two options - basic and advanced.
- **Basic Options**: The AD users are displayed along with their **Login Name** and **Organizational Unit**. Select the user(s) by clicking on the respective checkbox(es) and click on the **Next** button. You can easily search for a device using the search option or by filtering based on the OU using OU Filter.

1. In the **Roles** drop-down box, choose the role(s) you want to assign to the technician. You can assign more than one role to the technician and permissions of all the selected roles will be assigned to the technician.
2. Assign device group(s) to provide segmented view to the user and limit the privilege on security resources. Select the device group(s) checkbox(es) and click **OK**.
3. Click on the **Add** button.

- **Advanced Options**: By clicking to the **switch to advanced options link**, you can add users based on their **Domain Groups** and **Domain OUs**. The domain groups/OUs will be automatically discovered and displayed for the selected domain. Select the Domain Groups or Domain OUs by clicking on the respective checkbox(es) and click on the **Next** button. **Configure Schedule**: To synchronize users in Active Directory with the users in EventLog Analyzer, you can configure a schedule for periodically importing users from domain groups and OUs.

1. Enter a name for the schedule.
2. Specify the interval (in days) for running the scheduled automatic import.
3. Click on the **Save** button or the **Save and Run Now** button if you wish the run the scheduled import right away.

Note: To create a Domain Technician (A domain technician is the one created from the users of Active Directory), the domain must first be added to the Admin Server. A domain added to a Managed Server cannot be used for creating an Admin Server AD Domain Technician.

Creating custom user roles

EventLog Analyzer allows you to create custom user roles in addition to the default Admin, Operator, and Guest roles. Custom user roles enable you to have multiple user groups depending on the level of control and access that users need in EventLog Analyzer. Custom user roles help you adopt the principle of least privilege (POLP) while adding users and assigning roles to them.

Steps to create a Custom User Role

1. In EventLog Analyzer, navigate to **Settings → Admin Settings → Technicians and Roles**.
2. Click on the **Manage Roles** button.
3. To create a new role, click on **+Add New Role**.
4. In the Add New Role page, enter an appropriate role name in the **Role Name** field.
5. Click on the **Description** link next to the Role Name field to enter a description for the role you want to create.

6. You will see multiple tabs such as **Home, Reports, Compliance, Correlation, Alerts, Settings**, and **Others**. You can click on the checkbox provided for each of these tabs to allow the role to have all the permissions associated with the selected tabs. You can also navigate to each of these tabs individually and select the required permissions.
   - Under the **Home tab**, you can see two sections: **Dashboard** and **View the Log Sources**. In the **Dashboard** section, you can allow users to **view**, and **create and manage** the dashboard. In the **View the Log Source** section, you can assign permissions to view device, application, and file integrity monitoring logs. You can also click on the checkboxes next to the Dashboard and View the Log Sources section to select all the

options present under them.

- Under the **Reports** tab, you can specify if the user can view, schedule, and create reports by selecting the appropriate checkboxes. You can select all permissions associated with the Reports section by choosing **General**.
- Similarly, under the **Compliance** tab, you can choose if the user can view, create, and schedule compliance reports. You can click on the General checkbox if you want the user to have all permissions related to the Compliance tab.
- Under the **Search** tab, you can choose if you want to allow the user to perform search operations on the collected logs.
- Under the **Correlation** tab, you can find the **Correlation** and **Activity Monitoring** sections. In the Correlation section, you can choose if you want the role to view correlation reports, schedule them, and create and manage correlation rules and custom correlation actions. In the Activity Monitoring section, you can choose if the role can view and schedule activity monitoring reports, and create and manage activity monitoring rules.
- Under the **Alerts** tab, you can find three sections: **Alerts, Incident Workflows**, and **Ticketing Tools**. In the Alerts section, you can specify if you want the role to view generated alerts, and manage alert profiles and alert assigning rules by clicking on the appropriate checkbox. In the Incident Workflows section, you can select if the role can manage incident workflows. In the Ticketing Tools section, you can allow the role to configure ticketing tools.
- Under the **Settings** tab, you can find three tabs on the left pane: **Log Source Configuration, Admin Settings, and System Settings**. The Log Source Configuration tab contains multiple sections -- in which you can choose if you want the user to have permissions to configure and manage devices, applications, databases, virtual machines, and the File Integrity Monitoring component. In the Admin tab, you can choose whether the user can configure and manage domains, workgroups, and agents. In the System Settings tab, you can specify the permissions for managing general and system settings.

- Under the **Others** section, you can specify if the user can view product support related information, supported log sources, and notifications.

7. After choosing all the required permissions, click on Create to **create** the custom user role.

Viewing the created Custom User Role

In EventLog Analyzer, you can view all the default and custom user Roles by navigating to **Settings → Admin Settings → Technician and Roles → Manage Roles**. The role names, descriptions, and the number of technicians associated with each role will be displayed in a table. The **Actions** column of the table contains **Click to Copy, Edit**, and **Delete** icons to enable you to perform the required management actions. The Click to Copy option allows you to copy the permissions associated with an existing role to a new role -- which you can later edit as per your needs.

17.6. Logon Settings

Learn how to configure the following logon settings.

- **General**: Learn how to configure CAPTCHA and block users after a certain number of invalid login attempts.
- **Password policy:** Learn how to customize password policy for all technicians logging into EventLog Analyzer.
- **Two-factor Authentication**: Learn how to enable two-factor authentication for users logging into EventLog Analyzer.
- **Smartcard Authentication**: Learn how to configure EventLog Analyzer to authenticate users through smart cards, bypassing other first-factor authentication methods.
- **External Authentication**: Learn how to configure EventLog Analyzer to authenticate users through Active Directory and RADIUS server.
- **Allow/restrict IPs**: Learn how to allow or restrict access to EventLog Analyzer based on the users' IP address.

General

Under the **General** tab of **Logon Settings**, you can configure the following.

- CAPTCHA Settings
- Block User Settings

CAPTCHA Settings

CAPTCHA stands for **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part. Login CAPTCHA serves as a security measure against bot-based brute force attacks. Enabling this setting will display a CAPTCHA image on the login page. End-users must enter the characters shown in the CAPTCHA image to log into the EventLog Analyzer web portal.

You can configure whether to show CAPTCHA always or after a certain number of invalid login attempts. Apart from the CAPTCHA image, you can also enable Audio CAPTCHA.

Steps to enable CAPTCHA:

- Log into EventLog Analyzer as an administrator.
- In the **Settings** tab, navigate to **Admin Settings** > **Logon Settings** > **General**.
- Tick the **Enable CAPTCHA on login page** checkbox.
- Select **Always show CAPTCHA** if you want users to go through CAPTCHA verification every time they login.
- Select **Show CAPTCHA after invalid login attempts** if you want only those users who failed at login to go through the CAPTCHA verification process.
- Enter the number of invalid login attempts after which the CAPTCHA verification should appear.
- Enter the threshold (in minutes) to reset the invalid login attempts. After the specified duration, the invalid login attempts will be reset.
- Select **Enable Audio CAPTCHA** to assist visually impaired users.
- Note: 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.
- Click **Save Settings**.

Block User Settings

Using this option you can block users from accessing EventLog Analyzer after a certain number of invalid login attempts for a defined duration. A blocked user cannot log into EventLog Analyzer until the threshold for reset is reached.

Steps to block users:

- Log into EventLog Analyzer as an administrator.
- In the **Settings** tab, navigate to **Admin Settings** > **Logon Settings** > **General**.
- Select the **Block user after invalid login attempts** checkbox.
- Set the number of invalid login attempts after which users should be blocked and the number of minutes the user should be blocked by entering the appropriate values in the given fields.
- Set the threshold (in minutes) to reset the invalid login attempts. After the specified duration, the user will be allowed to attempt login.
- Click **Save Settings**.

Password Policy

Password Policy

To strengthen logon security, EventLog Analyzer allows the administrator to customize password policy for all technicians.

To configure password policy,

- Login to EventLog Analyzer as an administrator.
- Navigate to **Settings → Admin Settings → Logon Settings.**
- Click on the **Password Policy** tab.

The administrator can configure the following parameters:

1. **Minimum password length** - This parameter indicates the minimum number of characters the password must contain.
2. **Enforce password change after 'n' days** - This parameter indicates the number of days after which the password will automatically expire. If this parameter has been enabled, a notification alert will be triggered in the notification center 3 days before the password expires.

After the password expires, the following page will be displayed to the user on their subsequent login so that they can create a new password.

3. **Enforce password change for new users at their first login** - This parameter makes it mandatory for new users to change their password when they login for the first time. If this parameter has been enabled, when new users try to login, they will be redirected to the following page to set up a new password.

4. **Restrict reuse of password** - While changing the password, users cannot reuse the last 'n' passwords they had used previously. For example, if the administrator has configured the value as 3, users will not be able to re-use their last 3 passwords as their new password.

   After configuring the parameters, click **Save Settings** to save the updates.

Two-Factor Authentication

To strengthen logon security, EventLog Analyzer supports two-factor authentication (TFA).

If TFA is enabled, EventLog Analyzer will require its users to authenticate using one of the following authentication mechanisms in addition to Active Directory or RADIUS authentication.

- Email Verification
- SMS Verification
- Google Authenticator
- RSA SecurID
- Duo Security

Note: As a preventive measure against lockout, it has been made possible for an administrator to skip two-factor authentication during logon.

Setting up Two-factor Authentication

To enable two-factor configuration,

- Login to EventLog Analyzer as an administrator.
- Move to the **Settings** tab and click **Admin Settings** > **Logon Settings.**
- Switch the Two-factor Authentication toggle button to the Enabled position.

- Click on the authentication mechanism of your choice and enter the necessary details.

Note: If multiple authentication options are enabled, the user will be asked to choose one at the time of logging in.

Email Verification

When email verification is enabled, EventLog Analyzer sends a verification code to the configured email address. That verification code would need to be entered to successfully login.

To configure email verification as the second authentication mechanism,

- Click the **Enable Email Verification** check box to enable it.
- Enter the subject and body of the email containing the verification code.
- Set the priority of the mail according to your requirement.
- Click the **Macros** button at the bottom to include them in the email.
- Click **Save** to save the email verification settings.

SMS Verification

When SMS verification is enabled, EventLog Analyzer sends a verification code via SMS to the configured mobile number. That verification code would need to be entered to successfully login.

To configure SMS verification as the second authentication mechanism,

- Click the **Enable SMS Verification** check box to enable it.
- Enter the body of the message containing the verification code.
- Click the **Macros** button at the bottom to include them in the SMS.
- Click **Save** to save the email verification settings.

Google Authenticator

When verification via Google Authenticator is enabled, a six-digit security code will be generated in the Google Authenticator application in the configured mobile. This code would need to be entered to successfully login.

To configure Google Authenticator as the second authentication mechanism,

- Click the **Enable Google Authenticator** button.
- Enroll for two-factor authentication using the Google Authenticator application. For setting up Google Authenticator, go to Google Authenticator setup.

> **Note**: Ensure that the client time and device (mobile) time are syncronized.

RSA SecurID

When verification via RSA SecurID is enabled, the security codes generated by the RSA SecurID mobile app, hardware tokens, or tokens received via mail or SMS would need to be entered to successfully log in.

To configure RSA SecurID as the second authentication mechanism,

- Login to your RSA admin console.
- Navigate to **Access** >**Authentication Agents** and click **Add New**.
- Add the EventLog Analyzer server as an authentication agent and click **Save**.
- Navigate to **Access** > **Authentication Agents** and click **Generate Configuration File**.
- Download AM_Config.zip (Authentication Manager config) and extract sdconf.rec from the ZIP file.
- In the EventLog Analyzer two-factor authentication menu, select the **Enable RSA SecurID** check box.
- Click **Browse** and select the sdconf.rec file.
- Click **Save** to save the configuration.

Duo Security

If your organization uses Duo Security for two-factor authentication, it can be integrated with Eventlog Analyzer to secure logins. Users can approve or deny the Eventlog Analyzer 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 in Eventlog Analyzer: Web v2 SDK and Web v4 SDK.

Web v2 SDK uses a traditional Duo prompt which will be displayed in an iframe in Eventlog Analyzer, whereas Web v4 SDK uses Duo's OIDC-based universal prompt with a redesigned UI that redirects users to Duo for authentication.

> Duo Security has phased out Web v2 SDK, so it is recommended to switch to Web v4 SDK, which features the new Universal Prompt.

Prerequisites

- 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.

- Please follow these steps in the Duo Admin Panel to migrate from Web v2 SDK, which uses the traditional prompt, to Web v4 SDK, which employs the new Universal Prompt.

Web v4 SDK configuration steps

> **Note**: It is required to have a secure connection to set up the Web v4 SDK authentication. Please make sure that you have enabled HTTPS connection.

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 **Protect an Application**.

3. Search for Web SDK and click **Protect**.

4. Copy the **Client ID, Client secret**, and **API hostname** values.

5. In Eventlog Analyzer, navigate to **Admin > Logon Settings > Two-Factor Authentication > Duo Security**.
6. Check the **Enable Duo Security** box and select **Web v4 SDK** for **Integration Type**.

7. Paste the Client ID, Client secret, and API hostname obtained from the Duo Admin Panel in the respective fields.
8. Enter the same username pattern used in Duo Security in the **Username Pattern** field.
9. Click **Save**.

Steps to migrate to the new Universal Prompt

1. In the Duo Admin Panel, select the **Web SDK** application, which was previously configured for Eventlog Analyzer, 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 Eventlog Analyzer.

3. In Eventlog Analyzer, navigate to **Admin > Logon Settings > Two-Factor Authentication > Duo Security**.
4. Click **Web v4 SDK** and paste the Integration key, Secret key, and API hostname values in the **Client ID, Client Secret**, and **API Host name** fields respectively.
5. Once the Web v4 SDK is configured in Eventlog Analyzer 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.

6. Select **Show new Universal Prompt** to activate the universal prompt for Eventlog Analyzer.

Backup Verification Codes

As a backup mechanism against user lockout because of two-factor authentication failure, EventLog Analyzer has backup verification codes. Each user can generate a set of backup verification codes, which will have five, and use one code each time they are unable to login by authenticating using the configured mechanism.

To allow users to login using backup verification codes, enable the **Backup Verification Code** check box.

To generate backup verification codes, go to Two-factor Authentication in My Account.

Managing Enrolled Users

As an admin, you can view the authentication method users have enrolled for and also remove users' enrollment for two-factor authentication. To manage enrolled users,

- In the **Settings** tab, navigate to **Admin Settings** > **Logon Settings**.
- Click **Enrolled Users** at the bottom of the authentication mechanisms list to view the list of users enrolled for two-factor authentication and the authentication method they have chosen.

- To remove a user, select the user and click the delete icon.

Managing Account Two-factor Authentication

To manage the two-factor authentication settings of the logged in account, check Manage Account TFA.

Smart card Authentication

If you have a smart card authentication system enabled in your environment, you can configure EventLog Analyzer to authenticate users through it, bypassing other first-factor authentication methods.

This feature provides an additional authentication option for EventLog Analyzer login by enabling the use of smart cards/PKI/certificates to grant access to the tool. Smart card authentication strengthens the security further because getting access to EventLog Analyzer shall then require the user to possess the smart card and know the personal identification number (PIN) as well.

Steps to configure smart card authentication settings:

- Login to EventLog Analyzer as an administrator.
- SSL port must be enabled for configuring smart card authentication settings. To check your SSL port settings, select the **Settings** tab and navigate to **System Settings** > **Connection Settings** > **General Settings**. If not enabled already, select the checkbox against **Enable SSL [HTTPS]**, and specify the port number in the field. Click **Save**.
- In the **Settings** tab, navigate to **Admin Settings** > **Logon Settings** > **Smart Card Authentication**.
- Click the **+Add a New Smartcard** button at the top-right corner of the screen.
- In the **Import CA Root Certification** field, click **Browse** and import the required Certification Authority root certification file from your computer.
- In the **Mapping Attribute in Certificate** field, specify the certificate attribute for mapping.
- The user details need to be mapped between the smart card certificate and the EventLog Analyzer database. This denotes that the attribute in the smart card certificate that uniquely identifies the user should match with the corresponding value in the EventLog Analyzer user database. This mapping involves specifying which attribute in the certificate should be taken up for comparison with which attribute in EventLog Analyzer user store.
- EventLog Analyzer provides 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 if any other attribute is used to uniquely identify the user in your environment, contact EventLog Analyzer support to add that attribute.
- In the **Mapping Attribute in AD** field, specify the LDAP 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 EventLog Analyzer user store, e.g., sAMAccountName. During authentication, EventLog Analyzer reads the value corresponding to the certificate attribute that you specified in Mapping Attribute in Certificate and compares it with the specified LDAP attribute in Mapping Attribute in AD.
- In the **Linked Domains** field, select the appropriate domains from the drop-down menu.
- Click **Save.**

Note: Only internal CA certificates are supported. Third-party certificates are not supported.

After you have added a smart card for authentication, you can perform any of the following functions:

- Edit a configured smart card
- Enable/Disable a smart card
- Delete a configured smart card

Edit a configured smart card

To edit a configured smart card, follow the steps given below:

- In the **Settings** tab, navigate to **Admin Settings** > **Logon Settings** > **Smart Card Authentication**.
- Click the **Edit** icon located in the **Action** column of the particular smart card.
- Modify the settings you wish to change.
- Click **Save**.

Enable/Disable a smart card

To enable/disable a configured smart card, follow the steps given below:

- In the **Settings** tab, navigate to **Admin Settings** > **Logon Settings** > **Smart Card Authentication**.
- To enable/disable a configured smart card, click on the **Enable/Disable** icon located in the **Action** column of the particular smart card.

Delete a configured smart card

To delete a configured smart card, follow the steps given below:

- In the **Settings** tab, navigate to **Admin Settings** > **Logon Settings** > **Smart Card Authentication**.
- Click the corresponding **Delete** icon corresponding to the smart card which you wish to delete.
- Click **Yes** to confirm the deletion.

Enabling external authentication

Technicians can logon to EventLog Analyzer with their Active Directory and RADIUS server credentials.

Steps to enable Active Directory authentication in EventLog Analyzer

- Navigate to **Settings → Admin Settings → Logon Settings.**
- Click on the **External Authentication** tab.
- Under the **Active Directory** section, you will see the **Enable Active Directory Authentication** button.
- Click on the button to enable all the users imported from Active Directory to logon to EventLog Analyzer using their domain credentials.

Steps to enable RADIUS server authentication in EventLog Analyzer

- Navigate to **Settings → Admin Settings → Logon Settings**.
- Click on the **External Authentication** tab.
- Click on the **RADIUS server** section.
- Select the **Enable RADIUS server Authentication** check box.
- Enter the **RADIUS server IP** and the **Authentication port** number.
- Choose the authentication protocol from the **Protocol** drop-down menu.
- Enter the RADIUS shared secret password in the **RADIUS server secret** field.
- Specify the maximum number of authentication attempts that can be made from the **Automatic Retries** drop-down menu.
- Click on **Save** to enable the users to logon to EventLog Analyzer by authenticating with the configured RADIUS server.

Allow/restrict IP addresses

One way to secure EventLog Analyzer 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.

Controlling access to the product

1. Navigate to **Settings → Admin Settings → Logon Settings**.
2. Click the **Allow/Restrict IPs** tab.
3. Tick the **Enable Allow/Restrict IPs** Checkbox to enable IP restriction.

4. In the textbox that appears, select either **Allowed IPs** or **Restricted IPs** option.
5. **Enter the IP addresses** as per your requirement.
   - **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.
6. Refer to the Appendix for more information.

7. Finally, click **Save** to save the settings.
8. If you have changed the 3rd party reverse **proxy settings** of EventLog Analyzer for which you are enabling IP-based restriction, then:
   - **Add the following line to the server.xml file** (default location: <InstallationDirectory>/conf/server.xml).

9. <Valve className="org.apache.catalina.valves.RemoteIpValve" internalProxies="192\.168\.0\.10|192\.168\.0\.11" trustedProxies="172\.168\.0\.10|176\.168\.0\.11" />
    a. Edit the values of **internalProxies** and **trustedProxies** as per your environment.
    b. Enter IP address while specifying the values for internalProxies and trustedProxies, and use the vertical bar (|) character to enter multiple values.
    c. Restart for the changes to take effect.
    d. Repeat these steps for the integrated components as well.

Controlling access to APIs and product URLs

1. Navigate to **Settings → Admin Settings → Logon Settings**.
2. Click the **Allow/Restrict IPs** tab.
3. Tick the **Enable Allow/Restrict IPs** Checkbox to enable IP restriction.

4. In the textbox that appears, check the **Enable API/URL Access for Selected IPs** box.

5. Enter the **API/Product URLs** in the box provided.
6. 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:8400/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 (*).

7. **Enter the IP addresses** as per your requirement. Click [] icon if you want to allow access to multiple IP address ranges.
8. Finally, click **Save** to save the settings.
9. If any changes are made to 3rd party reverse proxy for EventLog Analyzer, or any of its integrated components, then:
   - Add the following line to the **server.xml file** (default location: <InstallationDirectory>/conf/server.xml).
10. <Valve className="org.apache.catalina.valves.RemoteIpValve"
    internalProxies="192\.168\.0\.10|192\.168\.0\.11"
    trustedProxies="172\.168\.0\.10|176\.168\.0\.11" />

a. Edit the values of **internalProxies** and **trustedProxies** as per your environment.

b. Enter IP address while specifying the values for internalProxies and trustedProxies, and use the vertical bar (|) character to enter multiple values.

c. Restart EventLog Analyzer for the changes to take effect.

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:

- **Disable/enable IP-based restriction**: Use the Checkbox under the Allow/Restrict IPs to enable or disable IP-based restriction.
- **Edit IP-based restriction settings**: Use the Allowed/Restricted IP Range textbox to add, delete, or edit the IP ranges and individual IP addresses.

Appendix

- **Use * as 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.* denies access to all addresses for that subnet.
- You can also enter **hostname** instead of IP addresses.
- You can allow or restrict only IPv4 addresses. **IPv6** is **not supported**.
- The IP addresses corresponding to the following servers cannot be restricted in EventLog Analyzer.
  - Remote Integrated Child/Parent Components server
  - Admin server
  - Managed server
- The implementation of IP restriction for forward proxy is not supported.
- After initially configuring IP Restriction or Reverse Proxy in the parent product, you need to manually restart EventLog Analyzer.
- If EventLog Analyzer is installed remotely and the Reverse Proxy is configured in the parent product, add the parent product server's IP as an internal proxy in EventLog Analyzer. Following this, manually restart EventLog Analyzer.

17.7. Security hardening

EventLog Analyzer provides numerous security settings to strengthen account security. The **Security Hardening** feature enables you to configure and manage all these settings in one place.

The dashboard lists the available security settings with a corresponding security score that is calculated based on the importance of the enabled configuration(s).

To manage individual settings, click the option against the target security setting and make the required changes. Once the process is complete, the option will have a green tick next to it, as shown in the image above.

A description for each setting is provided below:

1. **Enforce HTTPS*** - Enabling this setting helps establish a secure connection between the web browsers used to access EventLog Analyzer and the EventLog Analyzer server.
2. **Change Default Admin Password*** - Change the default admin password within 30 days of signing up. Choose a unique password that fits the application's complexity requirement.
3. **Enforce Two Factor Authentication*** - Add a second layer of security and prevent unauthorized access to EventLog Analyzer.
4. **Enable CAPTCHA** - Include CAPTCHA as a security measure in the login process to secure the account from brute force attacks. You can choose whether to show CAPTCHA always or only after a certain number of invalid login attempts.
5. **Block Invalid Login Attempts** - Block a particular user from accessing the account after a specific number of failed login attempts.
6. **Automatic update for critical security fixes** - Automatically install updates for highly critical security issues.

* - The highlighted settings are mandatory for EventLog Analyzer. The others are enabled by default in the application. You can turn them off manually to match your preference.

To ensure that you don't miss configuring any important security settings, EventLog Analyzer 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%.

Note: The security settings alerts will also be included under the License tab and will be emailed to you along with product downtime and start-up emails.

17.8. Reset Account Settings

1. Reset admin password

Carry out the steps below to reset the admin password of your EventLog Analyzer account.

For Windows -

- Navigate to **<EventLog Analyzer>/troubleshooting** folder.
- Execute the **resetPwd.bat** file.
- The admin password will be reset to the default password - **admin**.

For Linux -

- Open a terminal.
- Navigate to the **<EventLog Analyzer>/troubleshooting** folder.
- Execute the **resetPwd.sh** file to reset the admin password to the default password.
- You can access the account by using **admin** as the password.

2. Unblock admin account

Several unsuccessful attempts might lead to the blocking of the **default admin account** to ensure security. The account will be restored automatically in a while. To unblock the account immediately, follow the steps specific to the environment.

For Windows -

- Navigate to **<EventLog Analyzer>/bin/adsf** folder.
- Find and run the **unblockAccount.bat** file to complete the process.

For Linux -

- Open a terminal.
- Go to the **<EventLog Analyzer>/bin/adsf** folder.
- Execute the **unblockAccount.sh** file to unblock the account.

3. Reset the TFA enrollment

The steps to reset the TFA settings dedicated for two-factor authentication are as follows. This procedure can only be carried out for the **default admin** account.

For Windows -

- Go to the **<EventLog Analyzer>/bin/adsf** folder.
- Execute the **resetAdminTFAEnrollment.bat** file.
- Login to the EventLog Analyzer application and register for the two-factor authentication to match your preference.

For Linux -

- Open a terminal.

- Navigate to the **<EventLog Analyzer>/bin/adsf** folder.
- Execute the **resetAdminTFAEnrollment.sh** file to reset the existing TFA settings.
- Open EventLog Analyzer as the default admin and re-enroll for TFA.

17.9. Domain and 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.

17.10. Working Hour Settings

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.

17.11. Product Settings

EventLog Analyzer offers numerous customization capabilities, including limits for emails and SMSs, alert email formats, correlation permissions, and notification settings. The Product Settings tab has two sections, each having certain customization options:

Product Configurations

To configure settings such as views per page, number of rows displayed in reports, and so on in EventLog Analyzer, navigate to **Settings > Admin Settings > General > Product Settings > Product Configurations**.

A description of each of the settings is given below:

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: 5, 10, 20, 25, 50, 75, 100, 250, and 500.
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.
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.

Alert Email Format	HTML	Select whether the alert emails are sent in HTML or plaintext format.
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.
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**.
Export Limit	20000	Set the maximum number of records to be included in an exported report.
Rows in Top N Reports	10	Set the number of rows to be displayed for reports under the Top N Reports section.
Compliance Report Record Limit	500	Set the maximum number of records to be included in a Scheduled Compliance Report.
Report Time Out	25 mins	Set the maximum time allowed to generate a report.
Attach Report As	ZIP Report	Select the report format to be attached in email. The available options are: PDF/CSV Report and ZIP Report.
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**.
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.

After making the necessary changes, click **Save**.

Product Notifications

To configure the scenarios for which you want to receive notifications from EventLog Analyzer, navigate to **Settings > Admin Settings > General > Product Settings > Product Notifications**.

The different scenarios for which you have the option of enabling or disabling alerts have been listed below:

Configurations	Description
License Expiry	You will be notified that your EventLog Analyzer 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.
EventLog Analyzer Down	You will be notified when the EventLog Analyzer service crashes or stops.
EventLog Analyzer Upgrade	You will be notified when EventLog Analyzer has been successfully upgraded.
Unprocessed Log Files	When EventLog Analyzer 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 EventLog Analyzer is able to process logs. You can set a limit on the number of files which get filled with unprocessed logs. You will be notified once the limit is exceeded. In a new installation of EventLog Analyzer, default value for Unprocessed Log Files is 100.
Low Disk Space	You will be notified when the free space available in the disk on which EventLog Analyzer 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 which will get triggered.
Log Collector Failure	You will be notified when EventLog Analyzer's log collector is unable to collect logs. You can configure the subject of the email which will get triggered.
Archive integrity	You will be notified when the archive files are deleted or tampered via an email notification.

Note: In a new installation of EventLog Analyzer, notifications will be turned on by default for License Expiry, EventLog Analyzer Down, EventLog Analyzer Upgrade, and Unprocessed Log Files.

- After configuring the necessary notification settings, select if those notification emails need to be sent to all EventLog Analyzer Admins or only to specific email addresses -- which you can enter in the corresponding text box.
- Then, click **Save** to complete configuration.

Security Patch Updates

Whenever critical vulnerabilities are discovered in EventLog Analyzer, a security patch update is pushed to help mitigate any security threats. The Security Patch Update option has to be enabled for automatic download of security patches, whenever available.

Prerequisites:

- Internet connection should be available
- Zoho creator website should be whitelisted as the patches will download from here.

Enabling Security Patch Update in EventLog Analyzer:

In the EventLog Analyzer console, go to **Settings > Product Settings > Enable Security Patch Update > Save**.

17.12.1. Eventlog Analyzer REST APIs

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.
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.

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.

Generated Authtoken
AuthToken
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

17.12.2. Get log sources API

The API returns the list of log sources available in EventLog Analyzer.

Request URL

GET http://hostname:8400/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

Sample request

```
> curl --location --request GET 'http://localhost:8400/RestAPI/v1/meta/log_sources' \ -H "Accept: application/json" -H "Authorization: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx " --data-raw '{ "from": 0, "to": 10 }'
```

Sample response:

```
> { "devices": [ { "name": "tsi2k16adc", "ip_address": "202.0.112.248", "host_id": 3, "group": "WindowsGroup" }, { "name": "rog", "ip_address": "172.23.64.1", "host_id": 301, "group": "Windows Workstation" } ] }
```

Example usage using Postman (Third party tool)

17.12.3. Get log fields API

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:8400/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

Sample request

```
> curl --location --request GET 'http://localhost:8400/RestAPI/v1/meta/log_fields' \ -H "Accept: application/json" -H "Authorization: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx "
```

Sample response:

```
> { "fields": [ { "description": "Severity", "id": "SEVERITY" }, { "description": "Facility", "id": "FACILITY" }, { "description": "Source", "id": "SOURCE" }, { "description": "Event Name", "id": "IENAME" }, { "description": "Username", "id": "USERNAME" } ] }
```

Example usage using Postman (Third party tool)

17.12.4. Get log types API

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:8400/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

Sample request

```
> curl --location --request GET 'http://localhost:8400/RestAPI/v1/meta/log_types' \ -H "Accept: application/json" -H "Authorization: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx "
```

Sample response:

```
> { "log_types": [ { "description": "Windows", "id": "Windows" }, { "description": "Unix", "id": "Unix" }, { "description": "Hypervisor/ESXi", "id": "Hypervisor" }, { "description": "Cisco Device", "id": "Cisco Device" } ] }
```

Example eusag using Postman (Third party tool)

17.12.5. Synchronous Search API

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:8400/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
groups	all	No	JSONArray	List of device groups to search
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

Sample request

```
> curl --location --request POST 'http://localhost:8400/RestAPI/v1/search' \ -H "Accept: application/json" -H "Authorization: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx " --data-raw '{ "query": "EVENTID = 16384 AND USERNAME = mhtoc", "hosts": [1, 2, 601], "groups": [3], "from": 1643480792000, "to": 1643480479500 }'
```

Sample response:

```
> { "cursor": "DnF1ZXJ5VGhlbkZldGNoFwAAAAAAAARoFlloajVvRlN5UlQ2RGVTWlhPS2V1WHcAA",
  "hits": { "hits": [{ "COMMON_SEVERITY": "INFORMATION", "IS_THROWAWAY": true, "HOSTNAME":
  "lix", "APPID": 2, "FORMATID": 302, "RAWLOG": "roy.sulivan
  /event/emberAPI/ELANotificationActions \"https://eventlog.loin64; x64; rv:71.0)
  Gecko/20100101 Firefox/71.0\"", "TIME": "1643531422443", "IMPORTED_TIME": 1643531420365,
  "HOSTID": 601, "IPAddress2": "10.128.156.152" }, { "COMMON_SEVERITY": "INFORMATION",
  "IS_THROWAWAY": true, "HOSTNAME": "lix", "APPID": 2, "FORMATID": 302, "RAWLOG": "roy.sulivan
  /event/emberAPI/ELANotificationActions \"https://eventlog.l 15 142 200 \"Mozilla/5.0 (Windows
  NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0\"", "TIME": "1643531422446",
  "IPAddress1": "10.128.156.152", "HOSTID": 601, "IPAddress2": "10.128.156.152" }],
  "hits_count_in_current_page": 3 } }
```

ii) Search request with cursor

Sample request

```
> curl --location --request POST 'http://localhost:8400/RestAPI/v1/search' \ -H "Accept:
  application/json" -H "Authorization: Bearer
  mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx " --data-raw '{ "cursor":
  "DnF1ZXJ5VGhlbkZldGNoFwAAAAAAAARoFlloajVvRlN5UlQ2RGVTWlhPS2V1WHcAA" }'
```

Sample response:

```
> { "hits": { "hits": [{ "COMMON_SEVERITY": "INFORMATION", "IS_THROWAWAY": true, "HOSTNAME":
  "lix", "APPID": 2, "FORMATID": 302, "RAWLOG": "roy.sulivan
  /event/emberAPI/ELANotificationActions \"https://eventlog.loin64; x64; rv:71.0)
  Gecko/20100101 Firefox/71.0\"", "TIME": "1643531422443", "IMPORTED_TIME": 1643531420365,
  "HOSTID": 601, "IPAddress2": "10.128.156.152" }, { "COMMON_SEVERITY": "INFORMATION",
  "IS_THROWAWAY": true, "HOSTNAME": "lix", "APPID": 2, "FORMATID": 302, "RAWLOG": "roy.sulivan
  /event/emberAPI/ELANotificationActions \"https://eventlog.l 15 142 200 \"Mozilla/5.0 (Windows
  NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0\"", "TIME": "1643531422446",
  "IPAddress1": "10.128.156.152", "HOSTID": 601, "IPAddress2": "10.128.156.152" }],
  "hits_count_in_current_page": 3 } }
```

iii) Invalid Search query

Sample request

```
> curl --location --request POST 'http://localhost:8400/RestAPI/v1/search' \ -H "Accept:
  application/json" -H "Authorization: Bearer
  mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx " --data-raw '{ "query": "EVENTID :=
  16384 AND USERNAME <> mhtoc", "hosts": [1, 2, 601], "groups": [3], "from": 1643480792000,
  "to": 1643480479500 }'
```

Sample response

> { "ERROR": "SR007", "ERROR_DESCRIPTION": "QUERY NOT VALID", "ERRORS" : { "context": "Failed to build query", "cause": { "reason": "Encountered \" \":\" \": \"\" at line 1, column 159.\r\nWas expecting one of:\r\n ...\r\n \"+\" ...\r\n \"-\" ...\r\n ...\r\n \"(\" ...\r\n \"*\" ...\r\n ...\r\n ...\r\n ...\r\n ...\r\n \"[\" ...\r\n \"{\" ...\r\n ...\r\n ...\r\n ", "type": "ParseException" } } }

Example usage using Postman (Third party tool)

i) Search request with query

ii) Search request with cursor

iii) Invalid query

17.12.6. Asynchronous Search API

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:8400/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
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

Sample request

```
> curl --location --request POST 'http://localhost:8400/RestAPI/v1/search/async' \ -H "Accept: application/json" -H "Authorization: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx " --data-raw '{ "query": "EVENTID = 16384 AND USERNAME = mhtoc", "hosts": [1, 2, 601], "groups": [3], "from": 1643480792000, "to": 1643480479500 }'
```

Sample response:

```
> { "message": "Request submitted", "request_id": "AX6qKwX7hJby8kAkaqDG", "status": 200 }
```

Example usage using Postman (Third party tool)

17.12.7. Jobs API

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:8400/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 • **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:8400/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

Sample request

```
> curl --location --request DELETE 'http://localhost:8400/RestAPI/v1/jobs?
  request_id=AYVTeCb0wPH5eWuO5jkC' \ -H "Accept: application/json" -H "Authorization: Bearer
  mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx "
```

Sample response:

```
> { "message": "deleted hits for for request_id [AX6qJeaDhJby8kAkaqDE]" }
```

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

17.12.8. Results API

The API allows you fetch the results for the async search/alerts task.

Request URL

GET http://localhost:8400/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

Sample request

```
> curl --location --request GET 'http://localhost:8400/RestAPI/v1/jobs/results?
  request_id=AYVTeCb0wPH5eWuO5jkC' \ -H "Accept: application/json" -H "Authorization: Bearer
  mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx "
```

Sample response:

> { "next_page": 5, "results": { "hits": [{ "COMMON_SEVERITY": "INFORMATION", "IS_THROWAWAY": true, "HOSTNAME": "lix", "APPID": 2, "FORMATID": 302, "RAWLOG": "roy.sulivan /event/emberAPI/ELANotificationActions \"https://eventlog.lo [16/Jun/2020:21:13:21 +0530] 15 142 200 \"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0\"", "TIME": "1643531422443", "IMPORTED_TIME": 1643531420365, "Url": "https://eventlog.logme.cn/event/index2.do?url=collectorSettings&tab=system&sel=1\"", "IPAddress1": "10.128.156.152", "HOSTID": 601, "IPAddress2": "10.128.156.152" }, { "COMMON_SEVERITY": "INFORMATION", "IS_THROWAWAY": true, "HOSTNAME": "lix", "APPID": 2, "FORMATID": 302, "RAWLOG": "roy.sulivan /event/emberAPI/ELANotificationActions \"https://eventlog.logme.cn/event/index2.do?url=collectorSettings&tab=system&sel=1\" 10.128.156.152 10.128.156.152 POST [16/Jun/2020:21:13:27 +0530] 15 142 200 \"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0\"", "TIME": "1643531422446", "IMPORTED_TIME": 1643531420365, "Url": "https://eventlog.logme.cn/event/index2.do?url=collectorSettings&tab=system&sel=1\"", "IPAddress1": "10.128.156.152", "HOSTID": 601, "IPAddress2": "10.128.156.152" }], "hits_count_in_current_page": 2 }, "status": 200 }

Example usage using Postman (Third party tool)

i) Get results of async search

ii) Get particular page of results of async search

17.12.9. Get alert profiles API

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:8400/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
Profile Based Alerts	JSON Array of profile based alerts
Correlation Alert Profiles	JSON Array of correlation alert profiles

Example usage using cURL

Sample request

```
> curl --location --request POST 'http://localhost:8400/RestAPI/v1/meta/alert_profiles' \ -H "Accept: application/json" -H "Authorization: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx "
```

Sample response:


```
> { "Number of Records": 4, "Profile Based Alerts": [ { "Alert Id": 1001, "Alert profile name": "Alert Profile 1", "Type": "Predefined", "Status": "enabled", "Severity": "critical", "Notifications": ["SMS"] }, { "Alert Id": 1003, "Alert Profile Name": "Alert Profile 2", "Type": "Custom", "Status": "enabled", "Severity": "critical", "Notifications": ["Email"] }], "Correlation Alert Profiles": [ { "Alert profile name": "Rule 1", "Alert Id": 1234, "Type": "Correlation", "Status": "enabled", "Severity": "critical", "Notifications": [] }, { "Alert profile name": "Rule 2", "Alert Id": 1235, "Type": "Correlation Profile", "Status": "enabled", "Severity": "critical", "Notifications": [] } ... ] }
```


Example usage using Postman (Third party tool)

17.12.10. Synchronous Alerts API

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:8400/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
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

Sample request

```
> curl --location --request POST 'http://localhost:8400/RestAPI/v1/alerts' \ -H "Accept: application/json" -H "Authorization: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx " --data-raw '{ "query": "EVENTID = 16384 AND USERNAME = mhtoc", "alert_profiles": [1, 2, 601], "severity": ["CRITICAL"], "status": ["OPEN"], "from": 1643480792000, "to": 1643480479500 }'
```

Sample response:

```
> { "cursor": "DnF1ZXJ5VGhlbkZldGNoFwAAAAAAAARoFlloajVvRlN5UlQ2RGVTWlhPS2V1WHcAA",
  "hits": { "hits": [{ "COMMON_SEVERITY": "INFORMATION", "IS_THROWAWAY": true, "HOSTNAME":
  "lix", "APPID": 2, "FORMATID": 302, "RAWLOG": "roy.sulivan
  /event/emberAPI/ELANotificationActions \"https://eventlog.loin64; x64; rv:71.0)
  Gecko/20100101 Firefox/71.0\"", "TIME": "1643531422443", "IMPORTED_TIME": 1643531420365,
  "HOSTID": 601, "IPAddress2": "10.128.156.152", "Alert Profile": "Alert profile 1" }, {
  "COMMON_SEVERITY": "INFORMATION", "IS_THROWAWAY": true, "HOSTNAME": "lix", "APPID": 2,
  "FORMATID": 302, "RAWLOG": "roy.sulivan /event/emberAPI/ELANotificationActions
  \"https://eventlog.l 15 142 200 \"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0)
  Gecko/20100101 Firefox/71.0\"", "TIME": "1643531422446", "IPAddress1": "10.128.156.152",
  "HOSTID": 601, "IPAddress2": "10.128.156.152", "Alert Profile": "Alert profile 1" }],
  "hits_count_in_current_page": 3 } }
```

ii) Search request with cursor

Sample request

```
> curl --location --request POST 'http://localhost:8400/RestAPI/v1/alerts' \ -H "Accept:
  application/json" -H "Authorization: Bearer
  mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx " --data-raw '{ "cursor":
  "DnF1ZXJ5VGhlbkZldGNoFwAAAAAAAARoFlloajVvRlN5UlQ2RGVTWlhPS2V1WHcAA" }'
```

Sample response:

```
> { "hits": { "hits": [{ "COMMON_SEVERITY": "INFORMATION", "IS_THROWAWAY": true, "HOSTNAME":
  "lix", "APPID": 2, "FORMATID": 302, "RAWLOG": "roy.sulivan
  /event/emberAPI/ELANotificationActions \"https://eventlog.loin64; x64; rv:71.0)
  Gecko/20100101 Firefox/71.0\"", "TIME": "1643531422443", "IMPORTED_TIME": 1643531420365,
  "HOSTID": 601, "IPAddress2": "10.128.156.152", "Alert Profile": "Alert profile 1" }, {
  "COMMON_SEVERITY": "INFORMATION", "IS_THROWAWAY": true, "HOSTNAME": "lix", "APPID": 2,
  "FORMATID": 302, "RAWLOG": "roy.sulivan /event/emberAPI/ELANotificationActions
  \"https://eventlog.l 15 142 200 \"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0)
  Gecko/20100101 Firefox/71.0\"", "TIME": "1643531422446", "IPAddress1": "10.128.156.152",
  "HOSTID": 601, "IPAddress2": "10.128.156.152", "Alert Profile": "Alert profile 1" }],
  "hits_count_in_current_page": 3 } }
```

iii) Invalid Search query

Sample request

```
> curl --location --request POST 'http://localhost:8400/RestAPI/v1/alerts' \ -H "Accept:
  application/json" -H "Authorization: Bearer
  mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx " --data-raw '{ "query": "EVENTID :=
  16384 AND USERNAME <> mhtoc", "alert_profiles": [1, 2, 601], "severity": ["CRITICAL"], "status":
  ["OPEN"], "from": 1643480792000, "to": 1643480479500 }'
```

Sample response

> { "ERROR": "SR007", "ERROR_DESCRIPTION": "QUERY NOT VALID", "ERRORS" : { "context": "Failed to build query", "cause": { "reason": "Encountered \" \":\" \": \"\" at line 1, column 159.\r\nWas expecting one of:\r\n ...\r\n \"+\" ...\r\n \"-\" ...\r\n ...\r\n \"(\" ...\r\n \"*\" ...\r\n ...\r\n ...\r\n ...\r\n ...\r\n \"[\" ...\r\n \"{\" ...\r\n ...\r\n ", "type": "ParseException" } } }

Example usage using Postman (Third party tool)

i) Search request with query

ii) Search request with cursor

iii) Invalid query

17.12.11. Asynchronous Alerts API

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:8400/RestAPI/v1/alerts/async

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

Copyright © 2020, ZOHO Corp. All Rights Reserved.

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 hits_count_in_current_page: Hits count in current alert hit response

Example usage using cURL

i) Search request with query

Sample request

```
> curl --location --request POST 'http://localhost:8400/RestAPI/v1/alerts/async' \ -H "Accept: application/json" -H "Authorization: Bearer mdrkoda0odmtmznloc00ndziltg0mgutmwzkztljmjvmzwmx " --data-raw '{ "query": "EVENTID = 16384 AND USERNAME = mhtoc", "alert_profiles": [1, 2, 601], "severity": ["CRITICAL"], "status": ["OPEN"], "from": 1643480792000, "to": 1643480479500 }'
```

Sample response:

> { "message": "Request submitted", "request_id": "AX6qKwX7hJby8kAkaqDG", "status": 200 }

Example usage using Postman (Third party tool)

17.13. Retention Settings

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**.

17.14. Log Collection Filter

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.

17.15. Log Collection Failure Alerts

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.

17.16. Report Profiles

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.

17.17. Custom log parsing

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.

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.

- 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.

- 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.

17.18. Tags

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.

17.19. Profiles

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**.

17.20.1. Database auto backup

EventLog Analyzer 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 database restores

- Bundled PostgreSQL to Bundled PostgreSQL
- External PostgreSQL to External PostgreSQL
- MS SQL to MS SQL
- MySQL support has not been introduced yet

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 logical or 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. Create a folder named <product_home>/pgsql/data. <product_home> refers to the home directory of EventLog Analyzer 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 Settings → Database Settings → Database Backup.
2. Choose EventLog Analyzer 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 **Backup Storage Path**. You can either choose a local folder or shared folder to store the backups.
5. If the shared folder you've chosen needs permission to store the backups, then select the check against the **Authentication Required** box, and enter the necessary credentials.
6. Set a retention period for the backup files from the **Maintain Backup Files** drop-down.
7. Click **Save**.

Other settings

1. To disable auto backup for EventLog Analyzer click the icon located in the **Actions** column of the auto backup configuration table.
2. To get the status of the latest backup, click the icon.
3. To edit the backup schedule for a particular component, click on the icon located in the action column of the component.
4. Use the **Backup Now** option to initiate a backup instantly.
5. 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

1. If you've installed a new version of MS SQL server and want to configure it in EevntLog Analyzer in place of the old MS SQL server, you can do so by using the backup you've taken using EventLog Analyzer. Just note that, in addition to the backup you've taken using EventLog Analyzer, you need to copy the files in <MS_SQL_Old_Version>/**Backup** to <MS_SQL_New_Version>/**backup**.

MSSQL Backup

Automatic backups cannot be deleted directly from EventLog Analyzer since they are stored on the MSSQL server path. To manage backup files, adjustments must be made within the MSSQL application settings.

Troubleshooting tips

1. 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.

17.20.2. Database migration

Using this option you can change the built-in database server (PostgreSQL) of EventLog Analyzer 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.
- MySQL to Postgres migration:
  - If you need an external backup for Postgres during the migration from MySQL to Postgres, please contact our support team for assistance.
- 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.

Prerequisites for MSSQL migration

- Copy the bcp.exe and bcp.rll files from the installed SQL server directory and paste them in the EventLog Analyzer bin folder (<EventLog Analyzer_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**
- For migration to MS SQL, please install the corresponding SQL Native Client in the EventLog Analyzer machine as per the MS SQL server version.

SQL Server version	Command Line Utilities (cmdlnutils)	Files to be download for CmdLnUtils	Native Client (ncli)	File to be download for Native client	ODBC Driver (odbc)	File to be downloaded for ODBC Driver
2008	https://www.microsoft.com/en-in/download/details.aspx?id=44272	SqlCmdLnUtils.msi	https://www.microsoft.com/en-in/download/details.aspx?id=44272	sqlncli.msi	Not Needed	Not Needed
2012	64 bit: http://go.microsoft.com/fwlink/?LinkID=239650&clcid=0x409 32 bit: http://go.microsoft.com/fwlink/?LinkID=239649&clcid=0x409 Ref: https://www.microsoft.com/en-us/download/details.aspx?id=29065	The previous column contains the download link.	https://www.microsoft.com/en-in/download/details.aspx?id=50402	sqlncli.msi	Not Needed	Not Needed
2014	https://www.microsoft.com/en-US/download/details.aspx?id=53164	MsSqlCmdLnUtils.msi	Not Needed	Not Needed	https://www.microsoft.com/en-in/download/details.aspx?id=36434	msodbcsql.msi
2016	https://www.microsoft.com/en-us/download/details.aspx?id=56833	MsSqlCmdLnUtils.msi	Not Needed	Not Needed	https://www.microsoft.com/en-us/download/details.aspx?id=56833	msodbcsql.msi
2017	https://www.microsoft.com/en-us/download/details.aspx?id=56833	MsSqlCmdLnUtils.msi	Not Needed	Not Needed	https://www.microsoft.com/en-us/download/details.aspx?id=56833	msodbcsql.msi
2017	https://www.microsoft.com/en-us/download/details.aspx?id=53591	MsSqlCmdLnUtils.msi	Not Needed	Not Needed	https://www.microsoft.com/en-us/download/details.aspx?id=53339	msodbcsql.msi
2019	64 bit: https://go.microsoft.com/fwlink/?linkid=2230791 32 bit: https://go.microsoft.com/fwlink/?linkid=2231320	MsSqlCmdLnUtils.msi	Not Needed	Not Needed	64 bit: https://go.microsoft.com/fwlink/?linkid=2223304 32 bit: https://go.microsoft.com/fwlink/?linkid=2223303	msodbcsql.msi
2022	https://www.microsoft.com/en-us/download/details.aspx?id=53591	MsSqlCmdLnUtils.msi	Not Needed	Not Needed	64 bit: https://go.microsoft.com/fwlink/?linkid=2249006 32 bit: https://go.microsoft.com/fwlink/?linkid=2249005	msodbcsql.msi

Note - MS SQL server version 2022 is also supported by EventLog Analyzer.

- If firewall is enabled in the MS SQL Server machine, the TCP and UDP ports must be opened.
- 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

```
# 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.

```
# - 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. Create a folder named <product_home>/pgsql/data. <product_home> refers to the home directory of EventLog Analyzer 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 EventLog Analyzer before proceeding with the steps (Important)

1. Open the Command Prompt and navigate to <EventLog Analyzer home\bin> (Here, EventLog Analyzer home is the location where EventLog Analyzer is installed).
2. Stop EventLog Analyzer by running **shutdown.bat**.
3. Run the **tools/ChangeDBServer.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.

7. 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.

8. 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 EventLog Analyzer.

9. If the MS SQL server you wish to migrate to has **Force encryption** enabled, check the box next to **SSL connection**.
10. Click **Test Connection** and wait for the connection to be established.
11. Once **Test Connection** has been established successfully, click **Configure DB** to initiate migration.

12. Click the **OK** button to initiate the migration process. During the migration, you have the option to cancel if necessary.

18.1. System Settings

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

18.2. Notification Settings

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:8400/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.

- 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:8400/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**.
- 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) 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.

Notification Settings

Mail Settings | SMS Settings

SMS Provider	SMS Service Provider
Service Type	SMPP
* SMPP Server/Port	
* Username	
* Password	
Advanced Settings	
SMPP Timeout	5 Mins
SMPP Source Address	
ESME System Type	
ESME Bind Type	Bind Transmitter
Source Address TON	Unknown
Source Address NPI	Unknown
Destination Address TON	Unknown
Destination Address NPI	Unknown

Save Settings | Cancel | Send Test Message

18.3. Manage Account TFA

To strengthen logon security, EventLog Analyzer supports two-factor authentication.

To manage the two-factor authentication settings of the logged in user account, click the profile icon on the top right corner and select **My Account**.

You get a screen with three tabs: Personalize, Two-factor Authentication, and Change Password.

Personalize

In this tab, you change the email ID of your account and the language of the product.

Two-factor Authentication

In this tab, you can change the two-factor authentication settings of your account. For that, you would first need to authenticate using the existing two-factor authentication mechanism.

From this tab, you can also manage trusted browsers and manage backup authentication codes.

To manage your trusted browsers, click **Manage Trusted Browsers**.

To view the already-generated backup verification codes or to generate new ones, click **Manage Backup Verification Codes**.

In the pop-up box that appears, you can see a list of backup verification codes. If all of the previously generated codes have been used up, you can generate a new set by clicking **Generate New Codes**. Once new codes have been generated, it is advisable to back them up by downloading the list, printing it, or emailing it.

Change Password

In this tab, you can change the password of your account.

18.4. Install EventLog Analyzer as a service

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.

18.5. Configure Connection Settings

The connection settings for EventLog Analyzer can be modified in the following page:

- **Settings** tab > **System Settings** > **Connection Settings**
- The **Connection Settings** page appears as follows:

- Enter the following details:
  1. **Application Port Number:** Specify the http port through which EventLog Analyzer connects to the web client.
  2. **SSL Port Number:** Specify the SSL port for a secure http connection. EventLog Analyzer also provides a tool to generate a CSR file for SSL certification here.

     > **Note:** The http and https port numbers should be different from each other.

  3. **Keystore Password:** If you require the keystore password to be encrypted, enable this option and provide the required password.
  4. **Session Expiry Time:** Mention the maximum duration for which a session of EventLog Analyzer can stay idle, following which it expires.

Advanced Settings

5. **TLS**: Configure the required TLS protocol to bound with Eventlog Analyzer Server
6. **Ciphers**: Select the respective cipher suites compatible with the Above selected TLS version

   The list of default ciphers supported in ELA 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

7. **Bind address**: Select the IP address to which the Eventlog Analyzer web port and its underlying listners should be bound with.
8. **Application Access URL**: Specify the DNS host name using which Eventlog Analyzer Network communication would take place between agents

- Click on "**Save**" to save the settings.
- Restart EventLog Analyzer for the settings to take effect.

SSL Certification Tool

Steps to apply SSL certificate and enable HTTPS

Let's see how to generate and apply a SSL certificate for Eventlog Analyzer

- Navigate to **Settings** tab > **System Settings > Connection 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.

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**:

1. If your CA has sent you a ZIP file, then select ZIP Upload, and upload the file.
2. 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**:
  1. If your CA has sent you just one certificate file (PFX or PEM format), then select Individual Certificates, and upload the file.
  2. 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:**
  1. 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 EventLog Analyzer.

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 **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.

    1. Click **Download CSR** or manually get it by going to the **<Install_dir>\Certificates** folder.
    2. 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.

Proxy Settings

- Navigate to **Settings > System Settings > Connection Settings > Proxy Settings.**

- In Proxy Settings, select the **Enable Proxy Server** check box.
- Configure the server by entering Server Name/Port, Username and Password in provided fields.
- Click on **Save Settings** to save the configured proxy server.

18.6. Re-branding

EventLog Analyzer gives you the ability to customize logos, images, and links in the product to suit the needs of the MSSPs (Managed Security Service Providers).

How to rebrand the EventLog Analyzer client?

Use the following menu option.

- **Settings** tab > **System Settings > Rebranding**

Customize Images

Replace the default images with your company/enterprise images

Client Logs & Images	Where it is used	Image Size & Thumbnail	New Image
Product Logo	Login Page	289*59 pixels	
Top Band Image	Client Header	232*47 pixels	
PDF Cover Image	PDF Cover Page	612*820 pixels	
Server Status Image	Tray Icon (Windows)	400*60 pixels	

Customize Strings/Links

Replace the default strings/links with your company/enterprise strings/links

Client Logs & Images	Where it is used	Existing String/Link	New String/Link
Company Name	Login Page	ZOHO Corp.	
Brand Name	Login Page	ManageEngine	
Company Website	Login Page	www.zohocorp.com	
Product Website	Login Page	www.eventloganalyzer.com	
Support Email	Login Page	eventlog-support@manageengine.com	
Sales Email	About Popup	sales@manageengine.com	
Toll Free	Support Page	+1 844 649 7766	

Click **Update** to update the customized images/logos and strings/texts.

Note:

- You can customize ZohoCorp/ManageEngine image/links as per your requirement.
- Customization takes effect only for the changed image/links, else default images/links are retained.
- Size of new image should be of same size as the default image.
- Images with the following file extensions are only permitted: **.jpg, .jpeg** and **.png**

18.7.1. System Info

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.
- 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.

EventLog Analyzer
Settings
System Diagnostics
Configuration
Admin Settings
System Settings
Notification Settings
Connection Settings
Re-branding
System Diagnostics
Listener Ports
System Info
System Utilization
System Resources Calculator
Log Level settings
JVM Information
System Information
Active Features Information
Generate Troubleshooting Data
Auto
Manual
Email
Ticket-Id
Comments
Cancel

EventLog Analyzer
Settings
Configuration
Admin Settings
System Settings
Notification Settings
Connection Settings
Re-branding
System Diagnostics
Listener Ports
System Diagnostics
System Info
System Utilization
System Resources Calculator
Log Level settings
JVM Information
System Information
Active Features Information
Generate Troubleshooting Data
General Build Information
Agent Logs
Thread dump
Completed

18.7.2. System Utilization

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 "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:
    1. Database retention period
    2. 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:
    1. (ELA-HOME)/ES/CachedRecord -> Number of entries
    2. (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

18.7.3. Database Access

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.

18.7.4. System Resource Calculator

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.

When the Log flow exceeds the high flow threshold, i.e., 3000 Windows EPS, the distributed setup recommendation will be shown.

EventLog Analyzer
Settings
System Diagnostics
Configuration
Admin Settings
System Settings
Notification Settings
Connection Settings
Re-branding
System Diagnostics
Listener Ports
System Info
System Utilization
System Resources Calculator
Log Level settings
Distributed Setup Recommendation
Log Flow
Windows Event
Syslogs
Other Logs
Searchable Log
Index Retention Period
Zip Index after
Archived Log
Archive Retention Period
Available
Recommended
CPU Cores
RAM
Archived Disk Space
Index Disk Space

EventLog Analyzer
Distributed Setup Split-Up
Hardware
Low Flow
Normal Flow
High Flow
Processor cores
RAM
IOPS
Disk Space
Network card capacity
CPU Architecture
OK

18.7.5. Log Level Settings

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.

18.8. Port Management

EventLog Analyzer lets you manage UDP/TCP ports to listen for syslogs and SNMP traps from devices through this dashboard.

Note that

- For each protocol, you can add up to a maximum of six ports.
- For collecting Syslog data, you can use the same port for multiple protocols.
- You can also disable the existing default ports and instead can add additional listening ports.

Syslog Ports

1. Go to **Settings > System Settings > Listener Ports.**

2. Click **Add Syslog Port** button
3. In the pop-up box that appears, enter the appropriate port number.
4. Select its corresponding protocol.

5. Click **Add.**

6. To disable a Syslog port, click corresponding to the port you want to disable.

7. To enable a Syslog port, click corresponding to the port you want to enable.

8. Click corresponding to the port you want to delete.

TCP and TLS protocols cannot share the same port number.Syslog Ports.

SNMP Traps Port Management

To edit the port using which EventLog Analyzer listens to SNMP traps,

1. Click corresponding to the SNMP trap port.

2. In the pop-up box that appears, enter the desired port number.
3. Click Update.

4. To enable/disable the SNMP trap port, click / corresponding to it.

5. To update credentials for SNMP Trap, click on the credentials button mentioned below.

6. Click on the **Add Credential** to add a new SNMP credential.

7. Enter the name for SNMP Credential.
8. Select the required **Credential level**.

9. Enter the desired **port number**. This port will only be used by the workflow and syslog device discovery modules.
10. The SNMP V1/V2C will use **community string** for SNMP Trap and Discovery.

11. When you select security level of **SNMP V3**, additional fields will be required.

12. Enter the **Engine ID**. This will be used for trap collection and sending traps in workflows.
13. Select SNMPV3 Credential's **Authentication Level**.
14. Enter the **Authentication Phrase** for SNMPv3 Credential.
15. Select SNMPV3 Credential's **Privacy Level**.
16. Enter **Privacy Phrase** for SNMPv3 Credential.

Note:

1. By default, EventLog Analyzer listens to port 162 (UDP) for SNMP traps.
2. When a device not added to EventLog Analyzer 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.
3. 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.

19.1. EventLog Analyzer - Troubleshooting Tips

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.

```
> rem %JAVA% %JAVA_OPTS% -cp "%CLASS_PATH%" com.adventnet.mfw.Starter
  %SAFE_START% -c default -b <ip-address>
```

to

```
> %JAVA% %JAVA_OPTS% -cp "%CLASS_PATH%" com.adventnet.mfw.Starter
  %SAFE_START% -c default -b <ip-address>
```

```
> %JAVA% %JAVA_OPTS% -cp "%CLASS_PATH%" com.adventnet.mfw.Starter
  %SAFE_START%
```

to

```
> rem %JAVA% %JAVA_OPTS% -cp "%CLASS_PATH%" com.adventnet.mfw.Starter
  %SAFE_START%
```

- 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.

```
> rem set JAVA_OPTS=-Djava.library.path=..lib;..libnative -DpdfReport=false -Duser.country=US -Duser.language=en -DminDiskSpace=5 -Xms128m -Xmx512m -Dspecific.bind.address=<ip-address>
```

to

```
> set JAVA_OPTS=-Djava.library.path=..lib;..libnative -DpdfReport=false -Duser.country=US -Duser.language=en -DminDiskSpace=5 -Xms128m -Xmx512m -Dspecific.bind.address=<ip-address>
```

```
> set JAVA_OPTS=-Djava.library.path=..lib;..libnative -DpdfReport=false -Duser.country=US -Duser.language=en -DminDiskSpace=5 -Xms256m -Xmx1024m
```

to

```
> rem set JAVA_OPTS=-Djava.library.path=..lib;..libnative -DpdfReport=false -Duser.country=US -Duser.language=en -DminDiskSpace=5 -Xms256m -Xmx1024m
```

- 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.

```
> url=jdbc:postgresql://localdevice:33336/eventlog?stringtype=unspecified

  to

  url=jdbc:postgresql://<binding IP address>:33336/eventlog?stringtype=unspecified
```

- 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.

> #----------
> # CONNECTIONS AND AUTHENTICATION
> #----------
>
> # - Connection Settings -
>
> **#listen_addresses = 'localdevice'** # what IP address(es) to listen on;
>
> # comma-separated list of addresses;
>
> # defaults to 'localdevice'; use '*' for all
>
> # (change requires restart)
>
> to
>
> #----------
> # CONNECTIONS AND AUTHENTICATION
> #----------
>
> # - Connection Settings -
>
> **listen_addresses = <binding IP address>** # what IP address(es) to listen on;
>
> # comma-separated list of addresses;
>
> # defaults to 'localdevice'; use '*' for all
>
> # (change requires restart)

- 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.xxx**to 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="8400" 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="8400" 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

```
> sudo yum install fontconfig dejavu-sans-fonts dejavu-serif-fonts
```

- Case 2 : Ubuntu/Debian

```
> sudo apt install fonts-dejavu fontconfig
```

- Case 3 : SLES

```
> sudo zypper install dejavu-fonts fontconfig
```

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 8400 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 8400. 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:

1. In Add or Remove Programs, click **Add/Remove Windows Components**.
2. In the Windows Components Wizard, select **Management and Monitoring Tools**, then click **Details**.
3. In the Management and Monitoring Tools dialog box, select **WMI Windows Installer Provider** and then click **OK**.
4. 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.

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:

1. 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.
2. Export the certificate as a binary DER file from your browser.
3. 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.
4. For IE, **Internet Options > Content > Certificates > Personal > Export**
5. For Chrome, **Settings > Show Advanced Settings > Manage Certificates**
6. 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.

```
> keytool -import -alias ticketingtool -keystore <Eventlog Analzyer
  Home>/jre/lib/security/cacerts -file path-to-certificate-file
```

7. 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:

1. Go to the ticketing tool instance and try logging in to your account.
2. Enter the valid credentials and complete the captcha verification.
3. 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:

1. Login to your JIRA On-Premise account.
2. In the top right corner, select **Administration** and go to **System > General Configuration > Edit Settings**.
3. 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.
4. 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.

Check whether event logs are collected in dashboard for the particular host
Yes
Check the folders specified are correct in the FIM profile. (make sure that the folders are comma separated)
No
Check whether agent is running in agent administration page
No
Try restating the service
Yes
Check whether the agent can be connected to ELA server. By connecting to ELA client in the agent machine's browser
No
Check the firewall for errors
Yes
Try the following troubleshooting, if username is enabled for a particular folder
No
Contact EventLog Analyzer's customer support
Yes
Check any domain policies are overriding object access policies in the agent
No
Yes
computer configuration -> security settings -> advanced audit policy configuration -> audit policies -> object access
enable the following,
audit file share
audit file system
audit handle manipulation
audit detailed file share
audit other object access events
No
No
Yes
Check if SACL is enabled for the monitored folder
folder properties -> security -> advanced -> auditing
If there are no entries, please add a new entry for everyone to enabling the following permissions
Permission ->
(Permissions has to be set on two principals "folders" and "subfolders and files")
traverse folder/execute file
create files/write data
create folders/append data
write attributes
write extended attributes
delete subfolders and files
delete read permissions (only for folders)
change permissions
take ownership
No
Yes
Check the eventviewer security log size and the time difference between first log and last log.
If the time difference is less than 10, increase the security log file size.
No

Note: The following GUI is for the SACL entry in folder properties.

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.

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>

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.

1. **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.
2. **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:

```
> active = yes
  direction = out
  path = builtin_syslog
  type = builtin
  args = LOG_INFO
  format = string
```

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.

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.

```
> setfacl -R -m u:<username>:rwx /opt/ManageEngine/temp
```

- Setting Privileges for the agent folder.

```
> setfacl -R -m u:<username>:rwx /opt/ManageEngine/EventLogAnalyzer_Agent
```

For CentOS/RHEL v8 and later/Ubuntu/openSUSE/Debian/Fedora:

```
> setfacl -m u:<username>:w /etc/audit/plugins.d/elafim.conf
```

For CentOS/RHEL v6 to v7.9:

```
> setfacl -m u:<username>:w /etc/audisp/plugins.d/elafim.conf
```

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"

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:

```
> auditctl -s
```

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)

  ```
  > grep -rniw -e '-e' /etc/audit/
  ```

  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.

  ```
  > auditctl -s
  ```

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:

1. Click on the update icon next to the device name.
2. Select the appropriate device type.
3. Provide any other required information for the selected device type.
4. 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

Scanning of the Windows workstation failed due to one of the following reasons:

1. The login name and password provided for scanning is invalid in the workstation. **Solution:** Check if the login name and password are entered correctly.
2. 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:

   1. Select **Start > Run.**
   2. Type dcomcnfg in the text box and click **OK.**
   3. Select the **Default Properties** tab.
   4. Select the **Enable Distributed COM** in this machine checkbox.
   5. Click **OK.**

   To enable DCOM on Windows XP devices:

   Select **Start > Run**

1. Type dcomcnfg in the text box and click **OK**
2. Click on **Component Services > Computers > My Computer**
3. Right-click and select **Properties**
4. Select the **Default Properties** tab
5. Select the **Enable Distributed COM in this machine** checkbox
6. Click **OK**

3. 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:

```
> net use \<RemoteComputerName>C$ /u:<DomainNameUserName> "<password>"
  net use \<RemoteComputerName>ADMIN$ /u:<DomainNameUserName> "<password>"
```

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:

1. Disable the default Firewall in the Windows XP machine:

   Select **Start > Run**

   Type Firewall.cpl and click **OK**

   In the **General** tab, click **Off**

   Click **OK**

2. If the firewall cannot be disabled, launch Remote Administration for administrators on the remote machine by executing the following command:

```
> netsh firewall set service RemoteAdmin
```

After scanning, you can disable Remote Administration using the following command:

```
> netsh firewall set service RemoteAdmin disable
```

Error Code 0x80040154

1. 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.

2. 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:

1. Select **Start > Run**
2. Type Services.msc and click **OK**
3. In the Services window that opens, select **Windows Management Instrumentation** service.
4. 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 occured 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:

1. Ping the server.
2. For TCP, you can try the command telnet <ela_server_name> <port_no> where 514 is the default TCP port.
3. **tcpdump**

```
> tcpdump -n dst <ela_server_name> and dst port <port_no>
```

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.

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.

1. Force restart agent
2. Stopping agent
3. Updating device IP and credentials
4. Adding, deleting, enabling or disabling Device/LogCollection Filter/FIM
5. Updating FIM template
6. 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.

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.

```
SERVER_NAME=192.168.208.123
SERVER_IPADDRESS=192.168.208.123
SERVER_DBTYPE=postgres
PUBLICKEYSERVER=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg
Lx6CKAx64+ZICi8SqMOVvd6Ny2tORrJhxKeMLcMu55+htUFAqPIAF+
test@elau18-test:/opt/ManageEngine/EventLogAnalyzer_Ag
```

- Finally, restart the EventLog Analyzer agent to establish connection with the new server.

Performance

For troubleshooting, please follow the steps below:

1. Check if other applications are blocking the CPU cycle for EventLog Analyzer.
2. If a virtual machine is used, check for over provisioning or if snapshots are affecting the performance.
3. 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.

SMS Settings

Troubleshooting SSLHandshakeException in SMS Server Settings.

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.
> 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 EventLog Analyzer.

- Open a command prompt and change to the \jre\bin folder. For example: C:\ManageEngine\EventLogAnalyzer\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 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:

1. Review the firewall settings and look for any rules that might block the access.
2. If you find any blocking rules, create a new rule that allows the traffic to the Log360Cloud feeds server.
3. 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:

1. 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.
2. Try to resolve the domain name using a command line tool such as **nslookup** or **dig** to confirm that the DNS resolution is failing.
3. Check if there are any firewalls or security settings that may be blocking DNS traffic.
4. 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:

1. Login to https://log360feeds.manageengine.com/
2. Click on Regenerate Key.
3. 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.

1. Download Java SE TZUpdater from the official Oracle site. link "https://www.oracle.com/java/technologies/javase-tzupdater-downloads.html"
2. Take back up of <Eventlog Analyzer_HOME>\jre
3. After downloading, extract and copy the file tzupdater.jar to <EventLog Analyzer HOME>\jre\bin
4. Stop EventLog Analyzer Service.
5. Open Command Prompt as Administrator, navigate to <EventLog Analyzer HOME>\jre\bin.
6. 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

   ```
   > java -jar tzupdater.jar -l https://data.iana.org/time-zones/releases/tzdata2023c.tar.gz
   ```

   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

   ```
   > java -jar tzupdater.jar -l file:"C:/ManageEngine/EventLog/jre/tzdata2023c.tar.gz"
   ```

7. 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

1. 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
2. Make sure that both read and write permissions are enabled for the service account running EventLog Analyzer.
3. 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.

19.2. EventLog Analyzer - Frequently Asked Questions

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?

This depends on the platform on which EventLog Analyzer is installed. If installed on a Windows machine, EventLog Analyzer can collect event logs or syslogs from Windows and Unix devices, Cisco Switches and Routers, and other syslog devices . If installed on a Unix machine, EventLog Analyzer can collect syslogs only from Unix devices, Cisco Switches and Routers, and other syslog devices.

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?

No. EventLog Analyzer cannot work if DCOM is disabled on remote systems. You need to have DCOM enabled in remote windows servers for the logs to get collected and shown in EventLog Analyzer.

How to monitor Windows Events in EventLog Analyzer Linux Installation?

To monitor Windows Events in ELA Linux installation, you need to convert Windows Event messages into Syslog messages. To convert the message you have to use a separate tool.

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 Devices → Add Device(s)	Available	N/A	Manually enter device name and associate them with Agents.
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.	Download and 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	
7	MSSQL Discovery	ELA UI → Settings → Database Audit → Mssql Servers	Available	Not Available.	We can collect logs from MSSQL in 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:

1. Processor - Pentium 4 - 1.5GHz
2. RAM - 2GB
3. Disk Space - 5GB
4. Operating System - Windows 7, 2000, XP, 2003, Linux Ubuntu 8.0/9.0
5. 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?

EventLog Analyzer can be started as a root user, but all file permissions will be changed, and later you cannot start the server as another user.

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?

The archiving feature in EventLog Analyzer automatically stores all logs received in zipped flat files. You can configure archiving settings to suit the needs of your enterprise. Apart from that, if you need to backup the database, which contains processed data from event logs, you can run the database backup utility, **BackupDB.bat/.sh** present in the <EventLog Analyzer Home>/troubleshooting directory.

How to take database backup?

PostgreSQL database - For Build 8010 onwards

To take a backup of the existing EventLog Analyzer PostgreSQL database, ensure that the EventLog Analyzer server or service is stopped and create a ZIP file of the contents of <EventLog Analyzer Home>/pgsql directory and save it.

MSSQL database

Steps to take backup of MSSQL database:

Find the current location of the data file and log file for the database eventlog by using the following commands:

```
> use eventlog
  go
  sp_helpfile
  go
```

Detach the database by using the following commands:

```
> use master
  go
  sp_detach_db 'eventlog'
  go
```

Backup the data file and log file from the current location (<MSSQL Home>data**eventlog.mdf** and <MSSQL Home>data**attention-grabbing**) by zipping and saving the files.

MySQL database - For Build 8000 or earlier

To take a backup of the existing EventLog Analyzer MySQL database, ensure that the EventLog Analyzer server or service is stopped and create a ZIP file of the contents of <EventLog Analyzer Home>/mysql directory and save it.

How to configure EventLog Analyzer as service in Windows, after installation?

Normally, EventLog Analyzer is installed as a service.

Normally, the EventLog Analyzer is installed as a service. If you have installed it as an application and not as a service, you can configure it as a service any time later. The procedure to configure as service, start and stop the service is given below.

To configure EventLog Analyzer as a service after installation:

1. Stop the EventLog Analyzer application.
2. Execute the following command in the command prompt window in the <EventLog Analyzer Home>bin directory.

```
> service. bat -i
```

1. Start the EventLog Analyzer service.

How to configure EventLog Analyzer as service in Linux, after installation?

Normally, the EventLog Analyzer is installed as a service. If you have installed as an application and not as a service, you can configure it as a service any time later. The procedure to configure as service, start and stop the service is given below.

To configure EventLog Analyzer as a service after installation:

1. Stop the EventLog Analyzer application.
2. Execute the following command:

```
> sh configureAsService.sh -i
```

1. Start the EventLog Analyzer service.

Usage of EventLog Analyzer service command

```
> <EventLog Analyzer Home>/bin # /etc/init.d/eventloganalyzer

  Usage: /etc/init.d/eventloganalyzer { console | start | stop | restart | status | dump }
```

Configuration

How do I add devices to EventLog Analyzer so that it can start collecting event logs?

For Windows devices, enter the device name and the authentication details, and then add the device. For Unix devices, enter the device name and the port number of the syslog service, and then add the device. (Ensure that the syslog service is running, and that it is using the same port number specified here.)

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 the below steps to move an existing EventLog Analyzer server to a new machine/server.

PostgreSQL database - For Build 8010 onwards

1. Stop the existing EventLog Analyzer server/service

2. Ensure that the process '**java.exe**', '**postgres.exe**' and '**SysEvtCol.exe**' are not running/present in the task manager, kill these processes manually if some of them are still running

3. As a precautionary measure, copy the following complete folders (including the files and sub-folders) to another drive or to a mapped network drive. This will help us to restore to the settings and data in-case of any issue with the new machine installation.

    1. The folder, **pgsql** located under <EventLog Analyzer Home> directory

    2. The folder, **Archive** located under <EventLog Analyzer Home>archive directory

    3. The folder, **Indexes** located uncer <Eventlog Analyzer Home>server/default directory

4. Please download and install in the new machine/server the latest build of Eventlog Analyzer from the following link: https://www.manageengine.com/products/eventlog/download.html

5. Do not start the newly installed EventLog Analyzer server/service.

6. In the newly installed EventLog Analyzer machine/server, rename the folder **pgsql** located under <EventLog Analyzer Home> as **old_pgsql**.

7. Copy the **pgsql** folder (including the files and sub-folders), which is located under <EventLog Analyzer Home> , from the old machine/server to the newly installed Eventlog Analyzer machine/server.
   Note: Kindly take extra care that the EventLog Analyzer is not running on both the systems while performing this operation.

8. Start the EventLog Analyzer on the new machine and check whether the data and configurations are intact.

MSSQL database

1. Stop Eventlog Analyzer server/service.

2. Download and install the latest build of Eventlog Analyzer in the new server using the following link: https://www.manageengine.com/products/eventlog/download.html

3. Once you install the application in the new machine, kindly make sure that you do not start the application or shutdown the Eventlog Analyzer if started.

4. Please configure the MSSQL server credentials of the earlier Eventlog Analyzer server installation as explained in the **Configuring MSSQL Database** topic.

5. Start the Eventlog Analyzer server/service on the new machine and check whether the data and the configurations are intact.

6. In-case of any issues while performing the above steps, please do not continue any further and contact eventlog-support@manageengine.com to assist you better.

MySQL database - For Build 8000 or earlier

1. Stop the existing EventLog Analyzer server/service

2. Ensure that the process '**java.exe**', '**mysqld-nt.exe**' and '**SysEvtCol.exe**' are not running/present in the task manager, kill these processes manually if some of them are still running

3. As a precautionary measure, copy the following complete folders (including the files and sub-folders) to another drive or to a mapped network drive. This will help us to restore to the settings and data in-case of any issue with the new machine installation.

    1. The folder, **MySQL** located under <EventLog Analyzer Home> directory

    2. The folder, **Archive** located under <EventLog Analyzer Home>archive directory

    3. The folder, **Indexes** located uncer <Eventlog Analyzer Home>server/default directory

    if MySQL password is set in the old server

    1. **startDB.bat** and **configureODBC.vbs** located under <Eventlog Analyzer Home>bin directory.

    2. **myodbc3.dll** and **myodbc3s.dll** located under <Eventlog Analyzer Home>lib directory.

    3. **mysql-ds.xml** located under <Eventlog Analyzer Home>server/default/deploy directory

4. Please download and install in the new machine/server the latest build of Eventlog Analyzer from the following link: https://www.manageengine.com/products/eventlog/download.html

5. Do not start the newly installed EventLog Analyzer server/service.

6. In the newly installed EventLog Analyzer machine/server, rename the folder **MySQL** located under <EventLog Analyzer Home> as **OldMySQL**.

7. Copy the **MySQL** folder (including the files and sub-folders), which is located under <EventLog Analyzer Home> , from the old machine/server to the newly installed Eventlog Analyzer machine/server.
   Note: Kindly take extra care that the EventLog Analyzer is not running on both the systems while performing this operation.

8. Start the EventLog Analyzer on the new machine and check whether the data and configurations are intact.

How long can I store data in the EventLog Analyzer database?

The **DB Storage Options** box in the Settings tab lets you configure the number of days after which the database will be purged. The default value is set at **32 days**. This means that after 32 days, only the top values in each report are stored in the database, and the rest are discarded.

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

19.3. EventLog Analyzer Help

EventLog Analyzer gives you a wide range of options to contact the Technical Support team in case you run into any problem.

License

The License page displays the existing license details such as the type of license, the number of days to expire, and the number of device(s), and/or application(s) currently monitored. There is a link to upgrade the EventLog Analyzer license. You can enter the name of the new license file in the text box provided, or use the Browse button to select the license file, and apply it using the Upgradebutton.

Support

Support page displays all the information regarding the support channels available to solve any of the product issues.

About

The About page displays the knowledge information, about the product, such as the build version, build number, service pack applied if any, database used, build date, type, installation language, support and sales email IDs.

User Guide

The User guide (this document) displays contextual help information for the particular product screen selected.

Feedback

At any time, you can click the **Feedback** link in the bottom right, to send any issues or comments to the EventLog Analyzer Technical Support team.

20.1. EventLog Analyzer - Additional Utilities

EventLog Analyzer gives you a wide range of options to contact the Technical Support team in case you run into any problem.

- Working with SSL
- Configure MSSQL database
- Migrate data from PostgreSQL to MSSQL database
- Migrate ELA Data from MySQL to MSSQL Database
- Move ELA Database to Different Directory in the Same Server
- Move ELA Installation to Different Server
- Move Installation to Different Directory in the Same Server
- Configuring NAT Settings

20.2. Data Migration

Migrate Elasticsearch Data

Pre-requisites

	Service account permissions		Storage
	Local system account	**Service user account**	
Local drives	Should have sufficient read and write permissions.	Should have sufficient read and write permissions.	Sufficient disk space should be provided.
Network drives	Local system account cannot be used.	• The network path should be accessible from the EventLog Analyzer machine using the service user account. • Should have sufficient read and write permissions for that service user account. • There should be no interruption in connectivity to the network share.	

System requirements

	Network latency	Network speed	Disk IOPS
Local drive	<10ms	-	Refer to System Requirements
Remote storage	<10ms	> 20Mbps	Refer to System Requirements

- For optimal performance, 10ms or lower latency is recommended, and it should not exceed 100ms.
- 50% of the server's RAM should be kept free for off-heap utilization of Elasticsearch for optimal performance.

Overview of Elasticsearch (ES) data paths

ES directories

- ES\repo folder contains temporary files for ES archives
- ES\data folder contains data
- ES\archive folder contains ES archives
- ES\repo, ES\data and ES\archive should never point to the same folder

Examples:

For remote network path use the following format:

- **path.data : ["//remote machine name/shared folder/data"]**
- **path.repo : ["//remote machine name/shared folder/repo"]**

For Windows local storage, use the following format:

- **path.data : ["C:\\ManageEngine\\EventLog Analyzer\\ES\\data"]**
- **path.repo : ["C:\\ManageEngine\\EventLog Analyzer\\ES\\repo"]**

For Linux local storage, use the following format:

- **path.data : ["/opt/ManageEngine/EventLog Analyzer/ES/data"]**
- **path.repo : ["/opt/ManageEngine/EventLog Analyzer/ES/repo"]**

Steps to migrate Elasticsearch data to a new location

Case 1: EventLog Analyzer is integrated with Log360 and is installed with Log360 installer (Bundled)

In this case, EventLog Analyzer uses a common Elasticsearch that is shared with the other modules.

> Note: Here, only one Elasticsearch will be in use and it can be located in **Log360 Admin > Administrator > Search Engine Management**. By clicking on **Details**, we can see that it is running from **<ManageEngine>\elasticsearch\ES folder**. (Refer to Figure 1)

Figure 1: Details of the Elasticsearch node running location

Here are the steps to migrate data for EventLog Analyzer bundled with Log360:

1. Shutdown EventLog Analyzer and Log360.
2. Shutdown common ES.
   - Open Command Prompt as the Administrator in **<ManageEngine>\elasticsearch\ES\bin**
   - **Run stopES.bat**
3. Copy the data directory from **<ManageEngine>\elasticsearch\ES\data** to the new location.
4. Navigate to **<ManageEngine>\elasticsearch\ES\config\elasticsearch.yml**, and update **path.data** to include the new data location. (Refer to Figure 2)
5. Update **path.repo** in **<ManageEngine>\elasticsearch\ES\config\elasticsearch.yml** to the new repository location (parallel to the new data path).
6. Start the Log360 application along with its EventLog Analyzer module.

```
1  cluster.name: LOG360-CLUSTER
2  indices.query.bool.max_clause_count: 10240
3  indices.fielddata.cache.size: 50%
4  node.master: true
5  node.data: true
6  path.logs: D:\5426\Log360\...\elasticsearch\ES\logs
7  path.data:
8  - E:\ManageEngine\elasticsearch\ES\data
9  path.repo: E:\ManageEngine\EventLog Analyzer\ES\repo
10 script.inline: true
11 script.stored: true
12 indices.store.throttle.max_bytes_per_sec: 100mb
13 discovery.zen.minimum_master_nodes: 1
14 bootstrap.system_call_filter: false
15 cluster.indices.tombstones.size: 0
16 searchguard.disabled: false
17 searchguard.ssl.transport.pemcert_filepath: certificates/localnode.pem
18 searchguard.ssl.transport.pemkey_filepath: certificates/localnode.key
19 searchguard.ssl.transport.pemtrustedcas_filepath: certificates/root_ca.pem
20 searchguard.ssl.transport.enforce_hostname_verification: "false"
21 searchguard.ssl.transport.resolve_hostname: "false"
22 searchguard.ssl.http.enabled: false
23 http.enabled: false
24 searchguard.ssl.http.pemcert_filepath: certificates/localnode.pem
25 searchguard.ssl.http.pemkey_filepath: certificates/localnode.key
26 searchguard.ssl.http.pemtrustedcas_filepath: certificates/root_ca.pem
27 searchguard.nodes_dn:
28 - CN=NODE_CERTIFICATE.node, OU=none, O=none, L=none, ST=US, C=US
29 searchguard.authcz.admin_dn:
30 - CN=ADMIN, OU=none, O=none, L=none, ST=US, C=US
31 cluster.routing.allocation.node_initial_primaries_recoveries: 20
32 node.attr.admp: true
33 node.attr.hostname: yaswant-15509
34 transport.tcp.port: 9322
35 node.attr.csp: true
36 node.attr.dsp: true
37 node.attr.log360web: true
38 network.bind_host: 0.0.0.0
39 node.attr.log360: true
40 node.attr.ela: true
41 node.attr.o365: true
42 node.attr.erp: true
43 network.publish_host: 192.168.0.102
44 node.attr.adag: true
45 node.attr.location: D:\5426\Log360\...\elasticsearch\ES
46 node.name: int_yaswant-15509
```

Figure 2: Update path.data and path.repo to new location

Case 2: EventLog Analyzer as a standalone setup (Not integrated with Log360)

> **Note**: In this case, Elasticsearch will be running from <ManageEngine>\EventLog Analyzer\ES.

Here are the steps to migrate data for standalone EventLog Analyzer:

1. Shutdown EventLog Analyzer.
2. Copy the data directory from **<ManageEngine>\EventLog Analyzer\ES\data** to the new location.
3. Create a folder with the name archive (parallel to the new data directory).
4. Move the files from **<ManageEngine>\<EventLog Analyzer>\ES\archive** folder to the new folder named archive.
5. Navigate to **<ManageEngine>\<EventLog Analyzer>\ES\config\elasticsearch.yml**, and update **path.data** to include the new data location. (Refer to Figure 2)
6. Update **path.repo** in **<ManageEngine>\<EventLog Analyzer>\ES\config\elasticsearch.yml** to the new repository location (parallel to the new data path).
7. Start EventLog Analyzer.

Case 3: EventLog Analyzer is manually integrated into Log360

Note: In this case, EventLog Analyzer will be using its existing Elasticsearch (Local ES) and common ES (after integration with Log360). Since two Elasticsearch instances are in use, the same can be found in Log360 Admin > Administrator > Search Engine Management. By clicking on Details, we can see the running locations of both ES instances. (Refer to Figure 3)

Figure 3: Details of the running location Elasticsearch nodes

Here are the steps to migrate data for EventLog Analyzer integrated with Log360:

1. Shutdown EventLog Analyzer and Log360.
2. Shutdown common ES.
   - Open Command Prompt as the Administrator in <ManageEngine>\elasticsearch\ES\bin
   - Run stopES.bat

There are two running Elasticsearch nodes for which we need to migrate data:

A. Migrating common ES data

1. Copy the data directory from **<ManageEngine>\elasticsearch\ES\data** to the new location.
2. Navigate to **<ManageEngine>\elasticsearch\ES\config\elasticsearch.yml**, and update **path.data** to include the new location. (Refer to Figure 2)
3. Update **path.repo** in **<ManageEngine>\elasticsearch\ES\config\elasticsearch.yml** to include the new repository location (parallel to **path.data**).

B. Migrating local ES data

Note: The path here should be different from the one given for common ES.

1. Copy the data directory from **<ManageEngine>\EventLog Analyzer\ES\data** to the new location.
2. Navigate to **<ManageEngine>\<Eventlog>\ES\config\elasticsearch.yml**, update **path.data** to include the new location. (Refer to Figure 2)
3. Update **path.repo** in **<ManageEngine>\<Eventlog home>\ES\config\elasticsearch.yml** to the same repository location as that of common ES.
4. Create a folder with the name archive (parallel to the new data directory).
5. Move the files from **<ManageEngine>\<Eventlog>\ES\data** to the new location.

6. Move the files from **<ManageEngine>\<Eventlog>\ES\archive** folder to the new folder named archive.
7. Start Log360 and EventLog Analyzer.

Migrate Archive Data

Pre-requisites

	Service account permissions		Storage
	Local system account	Service user account	
Local drives	Should have sufficient read and write permissions.	Should have sufficient read and write permissions.	Sufficient disk space should be provided according to the archives size already present.Refer to the System requirements and Tuning Guide document for disk space.Exact disk space for the archives to be stored once migrated can be calculated only with the log flow.
Network drives	Local system account cannot be used.	1. The network path should be accessible from the EventLog Analyzer machine using the service user account.2. Should have sufficient read and write permissions for that service user account.3. No interruption in connectivity to the network share.	
S3 Bucket	Refer to the document for configuration and pre-requisites.		

System requirements

	Network latency	Network speed	Disk IOPS
Local drive	-	-	Refer to the System Requirements
Remote storage \ S3 bucket	< 2ms	> 20Mbps	Refer to the System Requirements

Note: The values mentioned above are approximate and can vary depending on the size and flow of the logs.

Steps to migrate the old archive data

Note: This is applicable for EventLog Analyzer build greater than 12330.

Steps to change the location of the archives in the database

Here are steps to change the location of the archives in the database:

1. If the newly created archives should be stored in the new location

   Go to **Settings > Admin Settings > Data Storage > Archives > Settings**

   Update the zip location to the new location. If it is required to be stored in the old location, then this step can be skipped. (Refer to Figure 1)

Figure 1: Update archive location

2. Manually move the old archives from the old location to the new location.
3. Now the location has to be updated in the database for each archive. (Refer to Figure 2)

   Go to **Settings > Admin Settings > Data Storage > Archives > More** in the top right corner Update path.

Figure 2: Archive data - Update paths

4. Select the old archive location in the dropdown and enter the new location where the archives are moved.
5. Once all the archive locations are updated, click on the Refresh icon in the top right corner to update the status of

the archives. (Refer to Figure 3)

Figure 3: Update status of archives

20.3. Working with HTTPS

Configuring Secure Communication - HTTPS

The HTTPS protocol provides several features that enable secure transmission of web traffic. These features include data encryption, server authentication, and message integrity. You can enable secure communication between the web clients and the EventLog Analyzer server using HTTPS.

To configure HTTPS using the HTTPS configuration tool, refer to the connection settings page.

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 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.

20.4. Configuring the MS SQL database for EventLog Analyzer

This page describes the various steps involved in configuring the MS SQL database in EventLog Analyzer.

How to find the build number?

> **Note:**
> This procedure to configure MS SQL will clear all existing data.
>
> 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.

Here's how you can configure and run the EventLog Analyzer with MS SQL as the database.

1. 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=2249006

32bit link: https://go.microsoft.com/fwlink/?linkid=2249005

After installing the required Native client/ODBC Driver, you can check if you've got the right version of bcp.exe+bcp.rll files or the right version of the Native client/ODBC Driver by going to <EventLog Analyzer Home>\bin folder, opening the command prompt with admin rights and executing the following command:-

bcp.exe -v

If you get an error, either your bcp files are wrong or your Native Client/ODBC Driver version in the EventLog Analyzer machine is incorrect.

2. Invoke the <EventLog Analyzer Home>\tools\changeDBServer.bat, to configure MS SQL server credentials like Server Name, Port, User Name and Password.
3. **The Database Setup Wizard** will appear.
4. In the wizard screen, choose the **Server Type** as SQL Server. Enter the **Host Name** and **the port** of the SQL Server. Select the instance from the available SQL Server Instances.
5. **Tips:**

- Ensure that the server browser service is enabled as it provides information about the SQL Server instances.
- Ensure that TCP/IP are enabled under protocols in the SQL Server Configuration Manager.

6. Select the authentication type using the "**Connect Using:**" options.
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

- To use **SQL Windows Authentication**, enter the **Domain Name, Username,** and **Password**.

SQL Server Authentication

For SQL Server Authentication, enter the **User Name** and **Password**.

EventLog Analyzer - DB Configurati...
Server Type
MSSQL Server
Host Name
GIRI-12835
Port
1433
Select Server Instances
GIRI-12835;MSSQLSERVER;1433
Database Name
eventlog
ELA
Authentication
Windows
SQL Server
Username
sa
Password
SSL connection
Migrate Existing Data
Configure DB
Test Connection
Cancel

Note: The product functions even if the table compression is enabled.

S. no.	Start-up Type	Required Permission(s) for Login	Comments
1	(First start)	• Server Roles page: 1. public 2. dbcreator • User Mapping page ('Database role membership' for 'eventlog' DB):- 1. db_datareader 2. db_datawriter 3. db_ddladmin 4. db_backupoperator • Control privilege on the created certificate, execute following queries:-	• 'public' is the default minimum permission • 'dbcreator' is required to create 'eventlog' database, else you'll get "CREATE DATABASE permission denied in database 'master' " error message
2	Warm Start	GRANT CONTROL ON SYMMETRIC KEY::[##MS_DatabaseMasterKey##] TO [user]; -- if not provided, user will not know if a master key exists in DB GRANT CONTROL ON SYMMETRIC KEY::[ZOHO_SYMM_KEY] TO [user]; GRANT CONTROL ON CERTIFICATE::[ZOHO_CERT] TO [user];	• 'db_backupoperator' is required only if the user wishes to back-up the 'eventlog' database

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.

If you are already using the EventLog Analyzer with PGSQL or MySQL and you want to change the database to MS SQL, please refer the Migrating EventLog Analyzer Data from PGSQL to MS SQL Database page or Migrating EventLog Analyzer Data from MySQL to MS SQL Database page respectively and follow the procedure given there.

20.5. Migrate EventLog Analyzer Data from PGSQL to MS SQL Database

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. Stop the **EventLog Analyzer Server/Service.**
2. Invoke the **<EventLog Analyzer Home>/tools/backUpDatabase.bat** in command prompt 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 **'backup_eventlog_<Build_Number>_database_MM_DD_YY_hh_mm.data'**.
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.

20.6. Migrate EventLog Analyzer Data from MySQL to MS SQL Database

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.

20.7. Moving the EventLog Analyzer MSSQL Database to a Different Directory in the Same Server

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:

```
> use eventlog
  go
  sp_helpfile
  go
```

4. Detach the database by entering the following commands:

```
> use master
  go
  sp_detach_db 'eventlog'
  go
```

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:

```
> use master
  go
  sp_attach_db 'eventlog' , '<New Location>eventlog.mdf' , '<New
  Location>eventlog_log.ldf'
  go
```

7. Verify the changed location by using the following commands:

```
> use eventlog
  go
  sp_helpfile
  go
```

8. Start the **Eventlog Analyzer Server/Service**.

20.8. Moving the EventLog Analyzer Installation to Another Machine

If you're planning to migrate EventLog Analyzer to a different server, possible data loss could be a major concern. This document will provide the steps to migrate your EventLog Analyzer installation to a different server without the loss of any data.

1. Stop the EventLog Analyzer server. (Start → Run → Type services.msc and press OK → Stop the service **ManageEngine EventLog Analyzer**)

   > **Note:** For a Linux service, Execute the commands given below to stop the Linux service (sample outputs are given):
   >
   > - Stop the service
   > **/etc/init.d/eventloganalyzer stop**
   > Stopping ManageEngine EventLog Analyzer <version number>...
   > Stopped ManageEngine EventLog Analyzer <version number>

2. Ensure that the processes java.exe, postgres.exe, and SysEvtCol.exe are not running in the task manager.

   > **Note:** For Linux, Ensure that the processes java, postgres, and SysEvtCol are not running.

3. Copy the entire **<EventLog Analyzer Home>** directory to the new server. It is strongly recommended that the new location is on the same path as the previous one.

Integration with Log360:

Case 1: If only EventLog Analyzer is being moved:

1. If EventLog Analyzer is integrated with Log360, and only EventLog Analyzer is being moved, then integration with Log360 needs to be removed first. You can integrate EventLog Analyzer with Log360 again after moving it to a different server).
2. After EventLog Analyzer is moved, if new path is not the same as the previous path, **path.data & path.repo** in **<EventLog Analyzer Home>\ES\config\elasticsearch.yml** needs to be updated accordingly.

```
elasticsearch.yml - Notepad
File  Edit  Format  View  Help
# ---- sample paths for index location ---
# for windows os,
# path.data : ["C:\\ManageEngine\\EventLog Analyzer\\ES\\data"]
# path.data : ["D:\\NewIndexStorage\\data"]
# for linux os,
# path.data : ["/opt/ManageEngine/EventLog Analyzer/ES/data"]
# path.data : ["/NewIndexStorage/data"]
# path.data : ["//remote machine name/shared folder/data"] //for shared locations
# NOTE:
# parent path should be a valid folder, since adjacent folders will be used for archives and others

cluster.name: LOG360-CLUSTER
indices.query.bool.max_clause_count: 10240
indices.fielddata.cache.size: 50%
node.master: true
node.data: true
path.logs: D:\ManageEngine\EventLog Analyzer\ES\logs
path.data:
- D:\ManageEngine\EventLog Analyzer\ES\data
path.repo: D:\ManageEngine\EventLog Analyzer\ES\repo
script.inline: true
script.stored: true
indices.store.throttle.max_bytes_per_sec: 100mb
discovery.zen.minimum_master_nodes: 1
bootstrap.system_call_filter: false
cluster.indices.tombstones.size: 0
searchguard.disabled: false
searchguard.ssl.transport.pemcert_filepath: certificates/localnode.pem
searchguard.ssl.transport.pemkey_filepath: certificates/localnode.key
searchguard.ssl.transport.pemtrustedcas_filepath: certificates/root_ca.pem
searchguard.ssl.transport.enforce_hostname_verification: "false"
searchguard.ssl.transport.resolve_hostname: "false"
searchguard.ssl.http.enabled: false
http.enabled: false
searchguard.ssl.http.pemcert_filepath: certificates/localnode.pem
```

3. Open the command prompt with administrator privileges. Navigate to **<EventLog Analyzer Home>\bin** and execute **initPgsql.bat** to set the permissions for the database.

> **Note:** For Linux, **initPgsql.sh** has to be executed.

4. Since the service has not been installed in the new server, we have to install it manually. Open the Command Prompt with administrator privileges. Navigate to **<EventLog Analyzer Home >\bin** and execute the following command to install the EventLog Analyzer service.

```
> service.bat -i
```

> **Note:** For Linux, the service installation command is:
>
> **sh configureAsService.sh -i**
>
> Click here to know more.

To install Log360 service please go to <Log360 Home >\bin and execute

> execute InstallNTService.bat

5. The service will now be installed. Try starting the service and open EventLog Analyzer with your browser to log in.
6. EventLog Analyzer archive path has to be modified. **Settings → Admin Settings → Manage Archives → Settings → Archive Location**.

   Previously archived files cannot be loaded. The migration is now complete.

Case 2: If EventLog Analyzer and Log360 are being moved:

1. If EventLog Analyzer is integrated with Log360, and both Log360 & EventLog Analyzer are being moved, the integration needn't be removed. However, you would need to move the following,
   - **<ManageEngine Home>\EventLog Analyzer** folder
   - **<ManageEngine Home>\ElasticSearch**
   - **<ManageEngine Home>\Log360**
2. After Log360 & elasticsearch folders are moved along with EventLog Analyzer, if new path is not the same as the previous path, **path.data** & **path.repo** in **<ManageEngine Home>\elasticsearch\ES\config\elasticsearch.yml** needs to be updated. **path.data** in **<EventLog Analyzer Home>\ES\config\elasticsearch.yml** needs to be updated as well.

```
elasticsearch.yml - Notepad
File  Edit  Format  View  Help
# ---- sample paths for index location ---
# for windows os,
# path.data : ["C:\\ManageEngine\\EventLog Analyzer\\ES\\data"]
# path.data : ["D:\\NewIndexStorage\\data"]
# for linux os,
# path.data : ["/opt/ManageEngine/EventLog Analyzer/ES/data"]
# path.data : ["/NewIndexStorage/data"]
# path.data : ["//remote machine name/shared folder/data"] //for shared locations
# NOTE:
# parent path should be a valid folder, since adjacent folders will be used for archives and others

cluster.name: LOG360-CLUSTER
indices.query.bool.max_clause_count: 10240
indices.fielddata.cache.size: 50%
node.master: true
node.data: true
path.logs: D:\ManageEngine\EventLog Analyzer\ES\logs
path.data:
- D:\ManageEngine\EventLog Analyzer\ES\data
path.repo: D:\ManageEngine\EventLog Analyzer\ES\repo
script.inline: true
script.stored: true
indices.store.throttle.max_bytes_per_sec: 100mb
discovery.zen.minimum_master_nodes: 1
bootstrap.system_call_filter: false
cluster.indices.tombstones.size: 0
searchguard.disabled: false
searchguard.ssl.transport.pemcert_filepath: certificates/localnode.pem
searchguard.ssl.transport.pemkey_filepath: certificates/localnode.key
searchguard.ssl.transport.pemtrustedcas_filepath: certificates/root_ca.pem
searchguard.ssl.transport.enforce_hostname_verification: "false"
searchguard.ssl.transport.resolve_hostname: "false"
searchguard.ssl.http.enabled: false
http.enabled: false
searchguard.ssl.http.pemcert_filepath: certificates/localnode.pem
```

3. Open the command prompt with administrator privileges. Navigate to **<EventLog Analyzer Home>\bin** and execute **initPgsql.bat** to set the permissions for the database.

Note: For Linux, **initPgsql.sh** has to be executed.

4. Since the service has not been installed in the new server, we have to install it manually. Open the Command Prompt with administrator privileges. Navigate to **<EventLog Analyzer Home >\bin** and execute the following command to install the EventLog Analyzer service.

```
> service.bat -i
```

Note: For Linux, the service installation command is:

sh configureAsService.sh -i

Click here to know more.

5. The service will now be installed. Try starting the service and open EventLog Analyzer with your browser to log in.
6. EventLog Analyzer archive path has to be modified. **Settings → Admin Settings → Manage Archives → Settings → Archive Location**.

   Previously archived files cannot be loaded. The migration is now complete.

If EventLog Analyzer is not integrated with Log360:

1. If EventLog Analyzer is not integrated with Log360 and if the new path is not the same as the previous path, then **path.data and path.repo** in **<EventLog Analyzer Home>\ES\config\elasticsearch.yml** need to be updated.
2. Open the command prompt with administrator privileges. Navigate to **<EventLog Analyzer Home>\bin** and execute **initPgsql.bat** to set the permissions for the database.

   Note: For Linux, **initPgsql.sh** has to be executed.

3. Since the service has not been installed in the new server, we have to install it manually. Open the Command Prompt with administrator privileges. Navigate to **<EventLog Analyzer Home >\bin** and execute the following command to install the EventLog Analyzer service.

   ```
   > service.bat -i
   ```

   Note: For Linux, the service installation command is:

   sh configureAsService.sh -i

   Click here to know more.

4. The service will now be installed. Try starting the service and open EventLog Analyzer with your browser to log in.
5. EventLog Analyzer archive path has to be modified. **Settings → Admin Settings → Manage Archives → Settings → Archive Location**.

   Previously archived files cannot be loaded. The migration is now complete.

Note:

- If you have enabled log forwarding from any Linux, Unix, router, switch, firewall, or syslog devices to EventLog Analyzer, you would need to re-point them to the new server.
- If an agent has been configured for any device, check if it has been modified appropriately.
- Do not delete the previous installation until you ensure the migration is successful. Verify the migration by checking the log collection after 30 minutes.

If you are using MS SQL server as your database and if it is running on a remote computer, download and install the SQL Native Client/ODBC Driver that is appropriate for the SQL Server version in the new Event Log Analyzer machine.

More information on SQL Native Client/ODBC Driver is available here.

20.9. Configurations after changing the EventLog Analyzer server Hostname/IP address

This document provides the configurations to check after changing EventLog Analyzer server hostname or IP address.

Configuration for Standalone Edition

- If you have enabled log forwarding from any Linux, Unix, router, switch, firewall, or syslog devices to EventLog Analyzer, you would need to re-point them to the new server.
- If an agent has been configured for any device, check if it has been modified appropriately.
- Do not delete the previous installation until you ensure the migration is successful. Verify the migration by checking the log collection after 30 minutes.

> **Note**: To configure log forwarding through the product, please refer here.

Configuring Standalone edition-Integration with Log360

> **Note**: Ensure that all the components are set up and running before proceeding with the steps given below. Also, check whether you have the appropriate versions of the components with respect to the Log360 version you are currently running.

> **Note**: If you integrate EventLog Analyzer with Log360, change the IP or host name and protocol & port in **Admin** -> **Log360 Integration** -> **EventLog Analyzer Integration**.

1. Go to **Admin → Log360 integration**. You will be presented with eight tabs, each representing a component of Log360.
2. Click on the EventLog Analyzer tab .
3. Enter the name or IP address and the port number of the server on which that particular component is running.
4. Select the connection **Protocol** from the drop-down menu.
5. Click **Integrate Now**.

Repeat the above 3 steps for other components under the respective tabs.

Bulk agent administration:

Follow the below steps to update the EventLog Analyzer server new IP address in all the agents using Group Policy Object (GPO).

Step 1

1. Open the Group Policy Management Console (gpmc.msc) on a domain controller.

2. Right Click on the Domain and Click 'New Organization Unit'.
3. Enter OU name and click OK. Add all agent machines which need to update the EventLog Analyzer server IP address to it.

Step 2

1. Right click on the created OU and Click 'create new GPO and link it here'.
2. Enter GPO name and click **OK**.
3. Right Click the created GPO and click **edit**.
4. Navigate to Computer Configuration > Preferences > Windows Settings > Registry.
5. Right-click on the Registry node and select New > Registry Item.

Step 3

1. Configure the registry key values (IP Address) that you want to update and save.
2. After completing, check the settings page of GPO and make sure the values are correct.

Step 4

1. Update the GPO by Right clicking on the OU and clicking 'group policy update...'
2. Click **Yes**.
3. It will take 10min to reflect in all the Domain computers.

1
Force Group Policy update
You have chosen to force a Group Policy update on all computers within SCCM Servers and all subcontainers. If you choose 'Yes' below, User and Computer policy settings will be updated on:
1 Computer
Are you sure you want to update policy for these computers?
2
Yes
No
Help
3

Configurations for Distributed Edition

Prerequisites for configuring distributed edition

1. Reachability: Check whether both the admin server and managed server are up and open bidirectionally.
2. Connectivity: Check whether the admin server console can be accessed in the managed server machine and the managed server console in the admin server machine.
3. Product Build: Check whether the admin server build and all managed server builds are the same.
4. Navigate to <EventLog Analyzer Installation Directory> Enterprise.txt : Check whether Enterprise.txt values are correctly present as mentioned below.

adminserver.webserver.port = admin server running port.

adminserver.webserver.protocol = admin server running protocol.

webserver.protocol = managed server running port.

server.startidrange = managed server using startid.

isCentralArchiveEnabled = set true if Customer using Centralized Archives.

CollectorIP = managed server IP address/ hostname

adminserver.hostname = admin server name.

webserver.port = managed server running port.

DisablePPMCheck = Set false to auto upgrade managed server when Admin Server is upgraded, else set true for Manual upgrade.

Configurations for Managed Server

Registration/Connection

Go to the Database Console and Query as below to find the managed server details - hostname, startid, port, protocol, SSL enabled status in Admin Server : Select * from Collectors

The CollectorIP value in the managed server enterprise file and the hostname column in the admin server collectors table need to be the same.

If not same, edit correct details in managed server enterprise.txt and restart the managed server or update in Admin Server's Manage Server Settings page.

Change in IP and hostname on managed server

If there are any changes in port and protocol, alter that changes in **Enterprise.txt** file in EventLog Analyzer managed server. Restart the EventLog Analyzer managed server and change managed server details in "Edit user logon details" in admin server.

Migrating Managed Server to another machine

1. Follow the stand-alone steps
2. When successfully copied, finalize the IP and port for this Managed Server
3. Open enterprise.txt in Managed Server and update/add the entry:

   CollectorIP=<hostName/IP> and also update the webserver.port entry to match with the new one
4. Also open the Admin Server UI collector Settings page and edit the Managed Server that is being moved and update the IP, Port and all the other details that is changed now.
5. Restart the Admin Server.
6. Now, start the Managed Server.

If Centralized Archiving is enabled:In Admin Server, change the Admin Server Hostname/IP in SSH Server Settings located on Settings -> Admin Settings -> Archives -> Settings

Integration with Log360

> **Note**: Make sure that all the components are set up and running before proceeding with the steps given below. Also, check whether you have the appropriate versions of the components with respect to the Log360 version you are currently running.

1. Go to **Admin → Log360 integration**. You will be presented with eight tabs, each representing a component of Log360.
2. Click on any one of the tabs (say EventLog Analyzer).
3. Enter the name or IP address and the port number of the server on which that particular component is running.
4. Select the connection **Protocol** from the drop down menu.
5. Click **Integrate Now**.
6. Repeat the above 3 steps for other components as well under the respective tabs.

Configurations for Admin Server:

Registration/Connection

Query to find the managed server details - hostname, startid, port, protocol, SSL enabled status in Admin Server : Select * from Collectors

The CollectorIP value in the managed server enterprise file and the hostname column in the admin server collectors table need to be the same.

If not same, edit correct details in managed server enterprise.txt and restart the managed server or update in Admin Server Manage Server Settings page.

Change in IP and hostname in admin server

If any changes in port and protocol alter that changes in Enterprise.txt file of all EventLog Analyzer managed server and restart the all EventLog Analyzer managed server.

Migrating Admin Server to another machine

1. Follow the stand-alone steps
2. When successfully copied, finalize the IP and port for this Admin Server
3. Changes in Enterprise.txt file of all EventLog Analyzer managed server adminserver.hostname and adminserver.webserver.port entry to match with an new one
4. Restart the all EventLog Analyzer managed server.
5. Run RegisterWithAdminServer.bat in managed server located on <ELA_HOME>/troubleshooting folder the commend prompt as administrator privilege it need to be success.

If Centralized Archiving is enabled

In Admin Server, change the Admin Server Hostname/IP in SSH Server Settings located on Settings -> Admin Settings -> Archives -> Settings.

Integration with Log360

> **Note**: Make sure that all the components are set up and running before proceeding with the steps given below. Also, check whether you have the appropriate versions of the components with respect to the Log360 version you are currently running.

> **Note**: If you integrate the admin server with Log360, change the IP or host name and protocol & port in **Admin** -> **Log360 Integration** -> **EventLog Analyzer Integration**.

1. Go to **Admin → Log360 integration**. You will be presented with eight tabs, each representing a component of Log360.
2. Click on any one of the tabs (say EventLog Analyzer).
3. Enter the name or IP address and the port number of the server on which that particular component is running.
4. Select the connection **Protocol** from the drop down menu.
5. Click **Integrate Now**.
6. Repeat the above 3 steps for other components as well under the respective tabs.

20.10. Moving EventLog Analyzer installation to a Different Directory in the Same Server

If you are planning to migrate EventLog Analyzer to a different directory in the same server, possible data loss could be a major concern. This document will provide the steps to migrate your EventLog Analyzer installation to a different directory in the same server without the loss of any data.

1. Stop the EventLog Analyzer server. (Start → Run → Type services.msc and press OK → Stop the service **ManageEngine EventLog Analyzer**)

   > **Note:** For a Linux service, Execute the commands given below to stop the Linux service (sample outputs are given):
   >
   > - Stop the service
   > **/etc/init.d/eventloganalyzer stop**
   > Stopping ManageEngine EventLog Analyzer <version number>...
   > Stopped ManageEngine EventLog Analyzer <version number>

2. Ensure that the processes java.exe, postgres.exe, and SysEvtCol.exe are not running in the task manager.

   > **Note:** For Linux, Ensure that the processes java, postgres, and SysEvtCol are not running.

3. Copy the entire **<EventLog Analyzer Home>** directory to the new server. It is strongly recommended that the new location is on the same path as the previous one.

Integration with Log360:

Case 1: If only EventLog Analyzer is being moved:

1. If EventLog Analyzer is integrated with Log360, and only EventLog Analyzer is being moved, then integration with Log360 needs to be removed first. You can integrate EventLog Analyzer with Log360 again after moving it to a different directory.
2. After EventLog Analyzer is moved, if new path is not the same as the previous path, **path.data & path.repo** in **<EventLog Analyzer Home>\ES\config\elasticsearch.yml** needs to be updated accordingly.

```
elasticsearch.yml - Notepad
File  Edit  Format  View  Help
# ---- sample paths for index location ---
# for windows os,
# path.data : ["C:\\ManageEngine\\EventLog Analyzer\\ES\\data"]
# path.data : ["D:\\NewIndexStorage\\data"]
# for linux os,
# path.data : ["/opt/ManageEngine/EventLog Analyzer/ES/data"]
# path.data : ["/NewIndexStorage/data"]
# path.data : ["//remote machine name/shared folder/data"] //for shared locations
# NOTE:
# parent path should be a valid folder, since adjacent folders will be used for archives and others

cluster.name: LOG360-CLUSTER
indices.query.bool.max_clause_count: 10240
indices.fielddata.cache.size: 50%
node.master: true
node.data: true
path.logs: D:\ManageEngine\EventLog Analyzer\ES\logs
path.data:
- D:\ManageEngine\EventLog Analyzer\ES\data
path.repo: D:\ManageEngine\EventLog Analyzer\ES\repo
script.inline: true
script.stored: true
indices.store.throttle.max_bytes_per_sec: 100mb
discovery.zen.minimum_master_nodes: 1
bootstrap.system_call_filter: false
cluster.indices.tombstones.size: 0
searchguard.disabled: false
searchguard.ssl.transport.pemcert_filepath: certificates/localnode.pem
searchguard.ssl.transport.pemkey_filepath: certificates/localnode.key
searchguard.ssl.transport.pemtrustedcas_filepath: certificates/root_ca.pem
searchguard.ssl.transport.enforce_hostname_verification: "false"
searchguard.ssl.transport.resolve_hostname: "false"
searchguard.ssl.http.enabled: false
http.enabled: false
searchguard.ssl.http.pemcert_filepath: certificates/localnode.pem
```

3. Open the command prompt with administrator privileges. Navigate to **<EventLog Analyzer Home>\bin** and execute **initPgsql.bat** to set the permissions for the database.

> **Note:** For Linux, **initPgsql.sh** has to be executed.

4. Since the service has not been installed in the new server, we have to install it manually. Open the Command Prompt with administrator privileges. Navigate to **<EventLog Analyzer Home >\bin** and execute the following command to install the EventLog Analyzer service.

```
> service.bat -i
```

> **Note:** For Linux, the service installation command is:
>
> **sh configureAsService.sh -i**
>
> Click here to know more.

5. The service will now be installed. Try starting the service and open EventLog Analyzer with your browser to log in.
6. EventLog Analyzer archive path has to be modified. **Settings → Admin Settings → Manage Archives → Settings → Archive Location**.

Previously archived files cannot be loaded. The migration is now complete.

Case 2: If EventLog Analyzer and Log360 are being moved:

1. If EventLog Analyzer is integrated with Log360, and both Log360 & EventLog Analyzer are being moved, the integration needn't be removed. However, you would need to move the **<ManageEngine Home>\elasticsearch** folder (log360 & elasticsearch to same parent directory as EventLog Analyzer).
2. After Log360 & elasticsearch folders are moved along with EventLog Analyzer, if new path is not the same as the previous path, **path.data** & **path.repo** in **<ManageEngine Home>\elasticsearch\ES\config\elasticsearch.yml** needs to be updated. **path.data** in **<EventLog Analyzer Home>\ES\config\elasticsearch.yml** needs to be updated as well.

```
elasticsearch.yml - Notepad
File  Edit  Format  View  Help
# ---- sample paths for index location ---
# for windows os,
# path.data : ["C:\\ManageEngine\\EventLog Analyzer\\ES\\data"]
# path.data : ["D:\\NewIndexStorage\\data"]
# for linux os,
# path.data : ["/opt/ManageEngine/EventLog Analyzer/ES/data"]
# path.data : ["/NewIndexStorage/data"]
# path.data : ["//remote machine name/shared folder/data"] //for shared locations
# NOTE:
# parent path should be a valid folder, since adjacent folders will be used for archives and others

cluster.name: LOG360-CLUSTER
indices.query.bool.max_clause_count: 10240
indices.fielddata.cache.size: 50%
node.master: true
node.data: true
path.logs: D:\ManageEngine\EventLog Analyzer\ES\logs
path.data:
- D:\ManageEngine\EventLog Analyzer\ES\data
path.repo: D:\ManageEngine\EventLog Analyzer\ES\repo
script.inline: true
script.stored: true
indices.store.throttle.max_bytes_per_sec: 100mb
discovery.zen.minimum_master_nodes: 1
bootstrap.system_call_filter: false
cluster.indices.tombstones.size: 0
searchguard.disabled: false
searchguard.ssl.transport.pemcert_filepath: certificates/localnode.pem
searchguard.ssl.transport.pemkey_filepath: certificates/localnode.key
searchguard.ssl.transport.pemtrustedcas_filepath: certificates/root_ca.pem
searchguard.ssl.transport.enforce_hostname_verification: "false"
searchguard.ssl.transport.resolve_hostname: "false"
searchguard.ssl.http.enabled: false
http.enabled: false
searchguard.ssl.http.pemcert_filepath: certificates/localnode.pem
```

3. Open the command prompt with administrator privileges. Navigate to **<EventLog Analyzer Home>\bin** and execute **initPgsql.bat** to set the permissions for the database.

> **Note:** For Linux, **initPgsql.sh** has to be executed.

4. Since the service has not been installed in the new server, we have to install it manually. Open the Command Prompt with administrator privileges. Navigate to **<EventLog Analyzer Home >\bin** and execute the following command to install the EventLog Analyzer service.

```
> service.bat -i
```

> **Note:** For Linux, the service installation command is:
>
> **sh configureAsService.sh -i**
>
> Click here to know more.

5. The service will now be installed. Try starting the service and open EventLog Analyzer with your browser to log in.
6. EventLog Analyzer archive path has to be modified. **Settings → Admin Settings → Manage Archives → Settings → Archive Location**.

   Previously archived files cannot be loaded. The migration is now complete.

If EventLog Analyzer is not integrated with Log360:

1. If EventLog Analyzer is not integrated with Log360 and if the new path is not the same as the previous path, then **path.data and path.repo** in **<EventLog Analyzer Home>\ES\config\elasticsearch.yml** need to be updated.
2. Open the command prompt with administrator privileges. Navigate to **<EventLog Analyzer Home>\bin** and execute **initPgsql.bat** to set the permissions for the database.

   Note: For Linux, **initPgsql.sh** has to be executed.

3. Since the service has not been installed in the new server, we have to install it manually. Open the Command Prompt with administrator privileges. Navigate to **<EventLog Analyzer Home >\bin** and execute the following command to install the EventLog Analyzer service.

```
> service.bat -i
```

   Note: For Linux, the service installation command is:

   sh configureAsService.sh -i

   Click here to know more.

4. The service will now be installed. Try starting the service and open EventLog Analyzer with your browser to log in.
5. EventLog Analyzer archive path has to be modified. **Settings → Admin Settings → Manage Archives → Settings → Archive Location**.

   Previously archived files cannot be loaded. The migration is now complete.

Note:

- If you have enabled log forwarding from any Linux, Unix, router, switch, firewall, or syslog devices to EventLog Analyzer, you would need to re-point them to the new server.
- If an agent has been configured for any device, check if it has been modified appropriately.
- Do not delete the previous installation until you ensure the migration is successful. Verify the migration by checking the log collection after 30 minutes.

If you are using MS SQL server as your database and if it is running on a remote computer, download and install the SQL Native Client/ODBC Driver that is appropriate for the SQL Server version in the new Event Log Analyzer machine.

More information on SQL Native Client/ODBC Driver is available here.

20.11. Configuring NAT Settings

If you want EventLog Analyzer server to be reachable via public IP address, you can configure the NAT settings in such a way that all the requests that are sent to the public IP address get redirected to the EventLog Analyzer server.

- **For devices within the LAN**

  If you use the same DNS name for both public and private IP, then all internal requests within the LAN will be directed through the internal DNS to reach the private IP without getting routed through the public IP.

- **For devices in the Internet**

  Devices from the internet use the DNS name to reach the public IP address from where it gets directed to the private IP address.

Log collection for windows internet devices:

This can be achieved through agent-based log collection by specifying the public IP address and port.

Steps for applying/changing the IP & Port details on the agent registry

1. If you are installing the agent for the first time, please follow the steps given here.
2. Kindly follow the steps given below to update the IP/Port details in the registry if you have already installed or are running the EventLog Analyzer agent.

   Steps to update the IP/Port in registry:

   - Open the registry using regedit.exe in command prompt
   - Navigate to "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ZOHO Corp\EventLogAnalyzer\ServerInfo"
   - Update the ServerIPAddress and ServerPort

20.12. Disk Monitoring for Search Nodes in EventlogAnalyzer

All the live and searchable logs processed by EventLog Analyzer are stored in ElasticSearch, an open-source search engine referred to as Search Node or ES. The processing of logs and preparation for search is called indexing. All the indexed data are stored in ElasticSearch data search.

Locating data folder for Elasticsearch

- In a standalone build, the data is stored by default in <EventlogAnalyzer>\ES\data folder. This can be updated in the <EventlogAnalyzer>\ES\config\elasticsearch.yml file.
- If EventLog Analyzer is installed with Log360, the data can be found in the <ManageEngine>\elasticsearch\ES\data folder. This can be updated in the <ManageEngine>\elasticsearch\ES\config\elasticsearch.yml file.
- If the standalone EventLog Analyzer is integrated with Log360 manually, then the data is distributed between <EventlogAnalyzer>\ES\data folder and <ManageEngine>\elasticsearch\ES\data folder.
- EventLog Analyzer's search data can also be distributed on multiple machines with the help of Log360's Search Engine Management. SEM creates a cluster of ElasticSearch which distributes the data and the search load using multiple machines.

EventLog Analyzer monitors the data folder(s) of ElasticSearch for free disk space and will automatically stop indexing if the drive where ES's data is stored has only 5GB of disk space left. When indexing is stopped, all the new processed data will be stored in <EventlogAnalyzer>\ES\CachedRecord folder. These cached logs will automatically be processed when the indexing restarts.

- If any of the nodes are full, a mail will be sent with **Disk full on search nodes** as the subject line.
- Once in 6 hours, a mail will be sent with the list of all the nodes that are still full.
- If the indexing stops, the user will receive a mail with **Indexing stopped in EventLog Analyzer** as the subject line. The user will also receive a notification on the EventLog Analyzer dashboard.

1. Indexing will not start until the disk space is increased on the data drive of ES. EventLog Analyzer will automatically attempt to carry out the indexing process every 10 minutes. You can quickstart the process with the **Restart Indexer** option.

2. Disk space should be cleared up or increased before restarting the indexer.

3. If disk space is sufficient now, the indexing process will restart.

4. If the disk monitor finds that the disk has not been cleared up, indexing will not restart.

5. A list of all the full search nodes will be displayed under the bell notification icon present in the EventLog Analyzer console.

Note: It is recommended that you have at least 20% free disk space on all the search node data drives to avoid non-indexing when there's an increase in the flow of logs or any other process uses up disk space on the server.

20.13. SSL/TLS Settings for Elasticsearch

If required we can limit the permitted ciphers & TLS protocols used by Elasticsearch.

All these changes have to be done in elasticsearch.yml configuration file.

Locating and updating the configuration file

- In case of a standalone build of EventLog Analyzer (i.e running without Log360) the change needs to be done in <EventlogAnalyzer>\ES\config\elasticsearch.yml. After making the change, restart EventLog Analyzer.
- If EventLog Analyzer was installed or integrated with Log360, then the change needs to be done in both \config\elasticsearch.yml, and <EventlogAnalyzer>\ES\config\elasticsearch.yml. After making the change, run stopES.bat from <ManageEngine>\elasticsearch\ES\bin using a admin command prompt. After this, restart Log360 and EventLog Analyzer.

TLS Ciphers & Protocols settings

- **searchguard.ssl.transport.enabled_protocols**
    - List of enabled TLS protocols, supported protocols with current JVM are

      > TLSv1.1, TLSv1.2

- searchguard.ssl.transport.enabled_ciphers
    - List of enabled TLS cipher suites, supported ciphers with current JVM (1.8.0_282) are

TLS_AES_128_GCM_SHA256,
TLS_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
TLS_EMPTY_RENEGOTIATION_INFO_SCSV

For example if we want to enable only **TLSv1.2** protocol & **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**, **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** ciphers.

We can add one of the following entries at the bottom of the elasticsearch.yml file

```
searchguard.ssl.transport.enabled_protocols: ["TLSv1.2"]
searchguard.ssl.transport.enabled_ciphers: ["TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"]
```

or

```
searchguard.ssl.transport.enabled_protocols:
- TLSv1.2
searchguard.ssl.transport.enabled_ciphers:
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
```

or

elasticsearch.yml

```yaml
# ==== sample paths for index location ===
# for windows os,
# path.data : ["C:\\ManageEngine\\EventLog Analyzer\\ES\\data"]
# path.data : ["D:\\NewIndexStorage\\data"]
# for linux os,
# path.data : ["/opt/ManageEngine/EventLog Analyzer/ES/data"]
# path.data : ["/NewIndexStorage/data"]
# path.data : ["//remote machine name/shared folder/data"] //for shared locations
# NOTE:
# parent path should be a valid folder, since adjacent folders will be used for archives and others

cluster.name: LOG360-CLUSTER
indices.query.bool.max_clause_count: 10240
indices.fielddata.cache.size: 50%
node.master: true
node.data: true
path.logs: E:\ME2\12270_ELA_HEAD3\EventLog Analyzer\ES\logs
path.data:
- E:\ME2\12270_ELA_HEAD3\EventLog Analyzer\ES\data
path.repo: E:\ME2\12270_ELA_HEAD3\EventLog Analyzer\ES\repo
script.inline: true
script.stored: true
indices.store.throttle.max_bytes_per_sec: 100mb
discovery.zen.minimum_master_nodes: 1
bootstrap.system_call_filter: false
cluster.indices.tombstones.size: 0
searchguard.disabled: false
searchguard.ssl.transport.pemcert_filepath: certificates/localnode.pem
searchguard.ssl.transport.pemkey_filepath: certificates/localnode.key
searchguard.ssl.transport.pemtrustedcas_filepath: certificates/root_ca.pem
searchguard.ssl.transport.enforce_hostname_verification: "false"
searchguard.ssl.transport.resolve_hostname: "false"
searchguard.ssl.http.enabled: false
http.enabled: false
searchguard.ssl.http.pemcert_filepath: certificates/localnode.pem
searchguard.ssl.http.pemkey_filepath: certificates/localnode.key
searchguard.ssl.http.pemtrustedcas_filepath: certificates/root_ca.pem
searchguard.nodes_dn:
- CN=NODE_CERTIFICATE.node, OU=none, O=none, L=none, ST=US, C=US
searchguard.authcz.admin_dn:
- CN=ADMIN, OU=none, O=none, L=none, ST=US, C=US
cluster.routing.allocation.node_initial_primaries_recoveries: 20
network.bind_host: 0.0.0.0
node.attr.hostname: roy-22120
node.attr.ela: true
transport.tcp.port: 9300
network.publish_host: 172.24.241.43
node.attr.location: E:\ME2\12270_ELA_HEAD3\EventLog Analyzer\ES
node.name: ela_master_roy-22120

searchguard.ssl.transport.enabled_protocols:
- TLSv1.2
searchguard.ssl.transport.enabled_ciphers:
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
```

20.14. Configuring DNS servers

Maintaining an accurate and up-to-date DNS setup is critical for the proper execution of EventLog Analyzer capabilities. A well-managed DNS system ensures that all devices can communicate effectively, preventing disruptions such as:

1. RPC Server Unavailability
2. Device addition Issues
3. Failed logons

Follow these best practices for Proper DNS Configuration

- Verify that each device in a Domain has a unique hostname.
- Establish forward and reverse DNS lookup zones.
- Make sure that DNS servers are properly configured and accessible for all the devices.
- Consider enabling Dynamic DNS (DDNS) to automatically update DNS records as the IP addresses change.
- Regularly monitor DNS servers and zones for any anomalies.
- Perform routine maintenance tasks such as zone cleanup, DNS database optimization, DNS Cache Clean up and DNS server software updates.

Appendix:

Forward DNS lookup and reverse DNS lookup are two types of queries used in the Domain Name System (DNS) to resolve domain names to IP addresses and vice versa.

1. **DNS Forward Lookup - Translation of Domain Names to IP Addresses:**

   Translates human-readable domain names (e.g., www.domain.org) into machine-readable IP addresses (e.g., 192.0.2.1) that computers use to locate resources on the internet.

2. **DNS Reverse Lookup - Translation of IP Addresses to Domain Names:**

   Translates IP addresses(e.g., 192.0.2.1) back into domain names(e.g., www.domain.org), allowing users to identify the domain associated with a particular IP address.

DNS Cache(Stored Locally) - Temporary Storage of DNS Records:

DNS cache temporarily stores recently resolved domain name-to-IP address mappings, reducing the time required to resolve frequently accessed domain names by caching the results of previous lookups and DNS caches are stored locally, to clear DNS caches we can use the command *ipconfig /flushdns*

21.1. EventLog Analyzer distributed edition

What is the EventLog Analyzer distributed edition?

The distributed edition of EventLog Analyzer allows enterprises to monitor their network deployments across geographical locations. This edition encompasses one admin server and one or more managed servers. While the managed servers that are installed at the different locations collect and process the local network's security data, the admin server acts as the central console for viewing all the managed servers.

Here are a few highlights of the EventLog Analyzer distributed edition:

- Centralizes log management
- Supports multiple devices across different geographical locations
- Ensures secured communication between the components.
- Exclusive segmented and secured view for various customers of the MSSP.

Note: To install the distributed edition of EventLog Analyzer, you need to install the standard edition across your organization's network and then convert the installations into an admin or a managed server. You can refer to the steps given here.

21.2. Prerequisites for EventLog Analyzer distributed edition

Prerequisites for converting to distributed edition

Here are a few of the prerequisites which need to be taken care of before converting a standalone setup to the distributed edition:

1. Ensure there is communication between the admin server and the managed servers bidirectional accessibility or via VPN and optimal functionality by opening the port in the firewall.
2. EventLog Analyzer requires 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 EventLog Analyzer.
   - **8400 (Web server port)**- This is the default web server port used by EventLog Analyzer. This port is used for connecting to EventLog Analyzer using a web browser. You can change this port during installation.

By default, the managed and admin server communicate using HTTP (port number 8400). 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.

Best practices to deploy the admin and managed server

1. It is always recommended to convert the new EventLog Analyzer server as admin server to prevent data loss. You can follow the steps given here to convert the standard edition of EventLog Analyzer into an admin server.
2. For managed server, in case, you already have an existing EventLog Analyzer server, you can convert it into a managed server by following the steps here. The data in this case will remain on the same server and will not get lost/formatted unlike in the admin server.
3. Both the admin server and the managed server should be in the same build. If they are not in the same build, follow the steps mentioned here to download and apply the latest service packs.

> - If both the admin and managed servers are not in the same build, it can lead to sync issues.
> - One admin server is designed to manage up to 50 managed servers.

Licensing details of distributed edition

EventLog Analyzer's Distributed Edition license will be applied to the admin server. The number of devices and applications for which the license has been purchased can be utilized amongst the registered managed servers. You can keep adding the devices and applications in various managed servers until the purchased device licenses are exhausted. You can view the number of devices and applications managed by each managed server in the **Managed Server Settings** page of the admin server.

When the number of devices and applications managed by all the managed servers exceeds the number of licenses purchased, a warning message appears in the admin server. To resolve this warning, you can:

- Purchase the license to manage the additional devices and applications

Copyright © 2020, ZOHO Corp. All Rights Reserved.

- Check the number of devices and applications managed by each managed server in the Managed Server Settings page of the admin server. Go to the individual managed server and manually manage the devices. Make sure that the number of devices and applications are within the license limit.
- Go to the individual managed server and manually manage the devices. Make sure that the number of devices and applications are within the license limit.

21.3. Convert EventLog Analyzer standard edition to an admin server

Note: You need to back up the data of the standard edition to prevent data loss.

Converting the standard edition of EventLog Analyzer into an admin server will result in the deletion of data present in the standard edition. You can follow the steps given below to convert the standard edition of EventLog Analyzer into an admin server:

- Shut down EventLog Analyzer.
- Open the command prompt with administrative privilege and execute the **ConvertToAdminServer.bat/sh** file located in <EventLog Analyzer Home>/troubleshooting.
- 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.
- If you want to configure a proxy server, enter **y** for the next query and enter the proxy server details.
- You will see a success message if EventLog Analyzer has been converted from the standalone edition into an admin server of the distributed edition.
- To change the database for the admin server using the **changeDBServer.bat** file, first ensure that the product is fully started. Then, stop the product before running the **changeDBServer.bat** file.

21.4. Converting EventLog Analyzer standard edition to a managed server

You can convert your standalone EventLog Analyzer installation (Standard Edition) into a Managed Server installation of distributed edition by following the below steps:

1. Shut down EventLog Analyzer installation.
2. Backup the database.
3. Execute the **ConvertToManagedServer.bat/sh** file located in <EventLog Analyzer Home>/troubleshooting with administrative privilege.
4. Enter **y** and press the **Enter** key to continue.
5. Enter the details such as the name or the IP address, web port, and web server protocol of the managed server and the admin server.
6. If you want to configure a proxy server, enter **y** for the next query and then enter the proxy server details such as the proxy server name, port number, username, and password.
7. You will see a success message if EventLog Analyzer has been converted from the standalone installation into a managed server installation of the distributed edition.
8. Open the admin server console to which you've linked this managed server and navigate to **Settings > Configurations > Managed Server Settings** to ensure that the converted server is listed.

If your managed server is unable to reach the admin server, please ensure the following:

- The admin server to which you want to link the new managed server is accessible on the given port using the mentioned protocol.
- If the admin server is using a proxy server, check whether the provided proxy server details are correct.

21.5. Manage Server Settings

Introduction to Manage Server Settings

In the Admin Server, the configuration for all Managed Servers is conducted on the "Manage Server Settings" page located on the **Settings tab > Log Source Configurations > Manage Server Settings**. Default Admin credentials are used for data collection from Managed Servers, and in case there are any changes in login details, they can be managed through the "Edit User Login Details" option.

The Manage Server Settings offers the following information and options:

- The total number of devices associated with the Managed Server, including disabled ones.
- Last synced time, adjusted based on the specified time zone.
- Display name with a hyperlink reference to the Managed Server.
- Sync Now: Initiates a restart of data collection, syncing the managed server immediately.
- Auto-upgrade managed server: Enables automatic upgrades for the managed server.
- Upgrade now: When the Auto upgrade option is disabled, Individual upgrade for the managed server.

Editing user login details

The scope of the Admin Server user interface i.e dashboard, reports, and other features, will be determined directly by the credentials of technician that associated with the specified Managed Server. To update the credentials for the managed server, click on the Edit icon.

1. Display name: Enter the name for the Managed Server to be displayed on the UI.
2. Server name: Enter the Managed Server name with its port.
3. Protocols: The protocol to be used for communication (HTTP & HTTPs).
4. User Name and Password: Credentials used by the admin server for logging into the managed server.

Note:

- When the Managed Server protocol is changed, ensure corresponding changes in the Manage Server Settings of the Admin Server.
- You may use different Techincian credentials with admin privileges.

Deleting managed server

Deleting the managed server will result in the deletion of all its associated data from the Admin Server, leading to disruption in synchronization. This action should be carried out before deleting the managed server on the local machine.

Sync now

The Sync now option initiates data collection, causing the data in the managed server to synchronize immediately with the admin server and update the status.

Following are the different data collection status types.

Success Status:

- Data Collection Successful - Sync succeeded.
- Scheduled for data collection - Sync scheduled when adding a new managed server.

In-Process Status:

- Delete action is triggered. Please refresh after some time - Deleting request call sent to the managed server.
- Requested action triggered. Please refresh after some time - Data request sent to the managed server.

Warning Status:

- Build number mismatch between admin and this distributed server. managed server needs an upgrade - The Admin server is in higher version.
- Build number mismatch between Admin and this distributed server. managed server running a higher version - Managed Server is at a higher version.
- Unable to upgrade managed server from Admin server. Please try to update manually - Auto Upgrade fails to upgrade the manager server with build less than 12216.
- Unable to contact remote machine - Managed Server is not reachable.

Failed Status:

- Deletion failed - Managed Server deletion failed.
- Error occurred during sync. Please contact support - Sync failed.
- Unable to upgrade managed server. Please contact support. - Auto upgrade failed.
- Exception during data collection - Failed to store/fetch data.
- Error during reset in collector server - Sync schedule was not restarted.
- The service pack required to upgrade the managed server is unavailable. Please contact support - The latest patch does not exist in the Admin Server.

During the data collection cycle:

- Licenses will sync to all managed servers.
- Auto-upgrade will be triggered in case of build mismatches between the servers if the "Auto Upgrade managed server" toggle is enabled.

Auto-Upgrade

When the " Auto-Upgrade Managed servers " toggle is enabled, the admin server will automatically upgrade the managed servers once the PPM is applied to the admin server.

Upgrade now

When the " Auto-Upgrade Managed Servers " toggle is disabled, the Upgrade now option will be shown across each managed server; if clicked, it will individually upgrade the selected managed server.

21.6. Auto-upgrading the distributed setup

To upgrade the distributed setup of EventLog Analyzer, carry out the steps given below.

1. Apply the service pack only to the admin server.
2. The admin server will auto-upgrade the reporting managed servers, and the managed servers will automatically update the agents in use.
3. The **Auto-Upgrade Managed Servers** toggle will be enabled by default. Disabling the toggle will disable auto-upgrade of all managed servers by the admin server.
4. If the option is disabled, each managed server can be upgraded manually by clicking the **Upgrade now** option against each managed server.

Resolving upgrade failures

When the Admin server is upgraded through a service pack, all its managed servers will be automatically upgraded by default. A backup storage space check is conducted on the managed 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. If the managed server does not have sufficient backup storage space, a resolve button is shown. Using the Resolve option, users can skip or retry backup.

Here are possible reasons for upgrade failure

Upgrade failure due to insufficient space for backup in Managed server.

1. PostgreSQL
    - No space for database backup.
    - No space for config files and database backup.
2. MS SQL

- No space for config files backup.
- No space for database files backup.
- No space for config files and database backup.

The resolve option allows you to perform two actions in case of upgrade failure.

Continue without backup: Choosing this option will skip backup and proceed with the upgrade (not recommended). Please make sure to take a backup of the managed server and upgrade.

Retry backup and upgrade: Retries upgrade by taking backup first.

> **Note**: EventLog Analyzer does not support auto backup for MySQL database. We suggest taking a backup manually before the upgrade.

Other possible reasons for upgrade failure include runtime errors, such as failure to compress the files, and read and write errors.

21.7. Distributed edition upgrade best practices

This guide explains how users can upgrade the EventLog Analyzer Distributed Edition. In order to access the latest features and enhancements, users are required to upgrade to the latest version.

Steps to upgrade the EventLog Analyzer Distributed edition

The managed servers should be synchronized and registered with the admin server, facilitating a proper connectivity between them. This ensures a seamless auto upgrade without any issues. Before upgrading, you need to backup both the Managed and Admin servers. This is essential in the event of an upgrade failure, ensuring a swift recovery.

Here are the steps for upgrading:

A) Taking a manual backup of Admin Server

1. Shutdown the EventLog Analyzer Admin server.
2. Copy the following folders/files as backup
    - <Home>/Conf
    - <Home>/adsdata
    - <Home>/lib/AdventNetLicense.xml
3. Database backup

Please follow the same steps as for Standalone server.

B) Taking a manual backup of Managed Server

1. Shutdown the EventLog Analyzer Managed server(s).
2. Copy the following folders/files as backup
    - <Home>/Conf
    - <Home>/adsdata
    - <Home>/lib/AdventNetLicense.xml
3. Database backup

Please follow the same steps as for Standalone server.

C) Prerequisites before performing the upgrade:

1. Ensure all the managed servers are in sync and registered with admin server. This is required in order to achieve a smooth auto upgrade without encountering any issues.
2. During the upgrade within the same storage drive of EventLog Analyzer, a backup is executed. Hence, it is important to ensure that there is sufficient space available for backup.
3. Take snapshot or folder backup of all the servers. In the event of an upgrade failure, these backups can be utilized for restoration.

D) Performing the upgrade on the Admin Server:

Apply the latest service pack in the PPM on the Admin Server. Please check the instructions to apply service pack.

E) Upgrading Managed Servers:

Upon completion of the Admin Server upgrade, the subsequent step involves upgrading the managed servers.

There are two ways to achieve this: Case - I) Auto upgrading all managed servers through the Admin Server, and Case - II) Manually upgrading managed servers.

Case - I: Auto upgrading all managed servers through the Admin Server

When the Admin server is upgraded through a service pack, all its managed servers will be automatically upgraded by default.

Here are the steps for auto upgrading the managed servers:

- Shutdown admin server and all the managed servers.
- Take snapshot or folder backup of all the servers.(Either folder backup or snapshot)
- Apply PPM in the admin server.
- Start the admin server.
- After ensuring that the admin server is up and running, start all the managed servers one by one.
- Wait for the admin server to upgrade all the managed servers before applying the next PPM on the admin server.

Case - II: Manually upgrading managed servers

In this case, the managed servers will be upgraded individually. During this process, a space check is conducted on the managed 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 managed servers as mentioned in **Step B**.

Here are the steps to manually upgrade each managed server

- Shutdown admin server and all the managed servers.
- Take snapshot or folder backup of all the servers.
- Add **DisablePPMCheck=true** in enterprise.txt of all the managed servers.
- Upgrade the managed server one by one using updatemanager.bat
- After upgrading all the managed servers, apply PPM on the admin server.
- Start the admin server.

After ensuring that admin server is up and running, start all the managed servers one by one.

21.8. Frequently Asked Questions - EventLog Analyzer Distributed Edition

General

Why should you go for the distributed edition of EventLog Analyzer?

If your organization has multiple network devices, servers, applications, and databases spread across geographical locations, using the distributed edition of EventLog Analyzer will help you unify all your logs and gain actionable insights from a single console. The distributed edition is also useful for Managed Security Service Providers (MSSPs).

What are managed and admin servers?

The distributed setup of EventLog Analyzer consists of one admin server and one or more managed servers. The managed servers can be installed at different geographical locations and must be connected to the admin server. The admin server centralizes log management across all the managed servers. You can view and manage all the managed servers from the admin server console.

How many managed servers can a single admin server manage?

One admin server is designed to manage up to 50 managed servers.

Can I convert the existing standalone edition of EventLog Analyzer to the distributed edition?

Yes, you can. You need to install a new admin server and convert the existing installation to Managed Server. Please refer to the steps given here. Ensure that the build number of your existing EventLog Analyzer installation is 6000 or above.

While converting the standard edition to an admin server, I'm prompted to specify the proxy server details. Why should I configure it?

Configuring the proxy server is optional. You need to configure the proxy server details during admin server conversion for the admin server needs to pass through a proxy server to contact the managed servers.

I have deleted a managed server from the admin server. How do I add it again?

To add a managed server under the admin server again, follow the steps given below:

1. Register the managed server with the admin server by executing the **registerWithAdminServer.bat/sh** file located in **<EventLog Analyzer Home>/troubleshooting**.
2. Restart the managed server.

Where are the collected logs stored? Is it in the managed server database or in both the managed server and admin server databases?

The logs collected by the managed server are stored only in the managed server database. You can't store the logs in the admin server. However, you can forward the logs to the admin server to archive them.

Secured Communication Mode (HTTPS)

What is the mode of communication between the admin server and the managed server?

By default, the managed and admin server communicate using the **HTTP**. There is also an option to convert the mode of communication to **HTTPS**. To modify the mode of communication, you can refer to the steps given here.

I have changed the managed server communication mode to HTTPS after installation. How to update this change in the admin server?

In the Admin Server, click on **Settings tab > Configurations> Managed Server Settings> Edit** icon of specific managed server. Select the required protocol to configure the web server port details.

Licensing

What are the licensing terms for EventLog Analyzer's distributed edition?

EventLog Analyzer's Distributed Edition license will be applied to the admin server. The number of devices and applications for which the license has been purchased can be utilized among the registered managed servers. You can keep adding the devices and applications in various managed servers till the total number of licenses purchased gets exhausted. You can view the number of devices and applications managed by each managed server in the **Managed Server Settings** page.

If the number of devices and applications managed by all the managed servers exceeds the number of licenses purchased, a warning message appears in the admin server. To resolve this warning, you can:

- Purchase the license to manage the additional devices and applications.
- Check the number of devices and applications managed by each managed server in the Managed Server Settings page of the admin server.
- Go to the individual managed server and manually manage the devices. Make sure that the number of devices and applications are equal to the number of licenses.

Is there an option to apply the license in the managed servers?

There is no option to apply the license in the **managed servers**. The license must be applied to the **admin server** and it will be automatically propagated to all **the managed servers**.

Why do I encounter the "License Restricted" alert even after reconfiguring the managed servers?

The status of devices in the managed server synchronize with the admin server during the data collection cycle, which happens at an interval of 5 minutes. Try to add other devices and applications in the managed server after a few minutes.

21.9. Centralized log file archival

EventLog Analyzer's distributed edition supports centralized archival of event logs received from each host. During log archival configuration in managed servers, if the centralized archival option is enabled, the managed servers will send all their logs to the admin server. The admin server will act as a centralized repository for viewing all the logs in your network.

The steps followed by EventLog Analyzer for log archival in the distributed set up are given below:

1. Logs are zipped at periodic intervals and the file to be archived is transported to the admin server using Secured Shell (SSH).
2. The file will be received by the admin server and a confirmation message for the receipt of the file is sent by the admin server to the respective managed server.
3. Managed server, upon receiving the confirmation message, deletes the archive file.

Note: SSH server will be started on enabling centralized archiving.

Configuring centralized archival in the admin server:

1. In the admin server, select **Configurations > Archive section: Archived Files**.
2. Click **Centralized Archive Settings** in the **Archive Files** screen to configure the centralized archival settings. A **File Archive Settings** screen will pop up.
3. To enable the **Centralized Archive** in the distributed set up, select the **Enable Centralized Archive** check box. On enabling, EventLog Analyzer transfers all the files from managed server to admin server using Secure Copy (SCP). SCP is based on SSH.
4. Enabling the option will also start SSH server with the below configurations:

Setting	Description
Archive Location	Configure the admin server's centralized archive location in this field. The location is set to <EventLog Analyzer Admin Server Home>/archive/**<Individual Managed Server's CollectorID>**/ by default.
Server IP/Name	Configure the IP address of the server on which the SSH is running. It will be admin server by default.
User Name	Configure the user name of the SSH service.
Password	Configure the password of the SSH service.
Port	The default SSH port will be 22. You can configure any other port from 1024 to 65535. You can click on the **Availability** link to check whether the port is free or occupied by some other application.

5. Centralized Archive Settings in EventLog Analyzer:

- **Notification Email Address**: The e-mail IDs mentioned in the field will receive notification emails regarding log archival processes.
- **Archive Retention Period**: Specify how long these archive files should be kept in the server. Once the period elapses, the files will be deleted from the EventLog Analyzer server.
- **Loaded Retention Period**: Specify the period for which the archive files should remain loaded.

Troubleshooting tips:

If the Centralized Archive is enabled, the SSH server will start with the configured values. If the SSH server fails to start, the **Centralized Archive Settings** in EventLog Analyzer will display a **Failed** status.

If the SSH server is not getting started, it could be due to the following reasons:

- The SSH server is not able to bind with the configured IP address. This is more likely to happen with a dual NIC machine. Check and configure the IP address of the correct NIC.
- The archive location configured could be invalid. Configure a valid location to archive the files.

22.1. Data Upgrade

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

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.

23.1. EventLog Analyzer Technical Support

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

23.2. Create an EventLog Analyzer Support Information File (SIF)

In case you face an issue with log collection or any other aspect of EventLog Analyzer, kindly create a SIF and send it to us. The SIF will help us to 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 click the **Support** tab.
2. In the **Support** Window, you can find **Auto** and **Manual** SIF creation options under the **Support Info** section.

3. To automatically create a SIF file, click on **Auto** and select **Create Support Information File**.
4. You will find a new link **Created File** which contains the SIF.
5. Clicking on this link allows you to either directly upload the SIF to ManageEngine's file upload server after providing the required details or download the SIF by clicking on the **Download** link and sending it to eventlog-support@manageengine.com

Procedure to create a SIF when the EventLog Analyzer server or web client is not working (for Build 8010 onwards)

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

Procedure to create SIF when the EventLog Analyzer server or web client is not working (for Build 8000 or earlier)

If you are unable to create a SIF from the EventLog Analyzer UI, you can zip the files under '**log**' folder, which is located in <EventLog Analyzer Home>server/default/log (default path) and upload the ZIP file using the following link:
https://bonitas2.zohocorp.com/#to=eventlog-support@manageengine.com

23.3. Contacting EventLog Analyzer Support

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.
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 **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.