ManageEngine
Log360

User Guide

CONTENTS

Chapter 1.1 **Windows Infrastructure**

1.1.1. Overview

📅 Last updated on: September 12, 2025

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

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

1.1.2. Working

Last updated on: September 12, 2025

Agent - Less Log collection

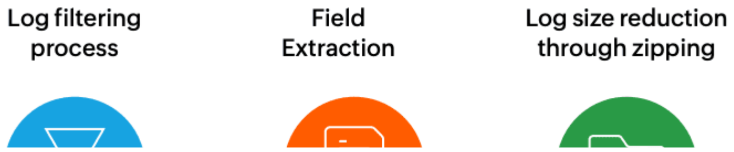
- No agents/client software required for log collection : For event log collection, eventlog analyzer application does not require a separate agent to be installed on each machine from which logs are collected. Rather the agent that collects Windows event log. In this way, eventlog analyzer application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

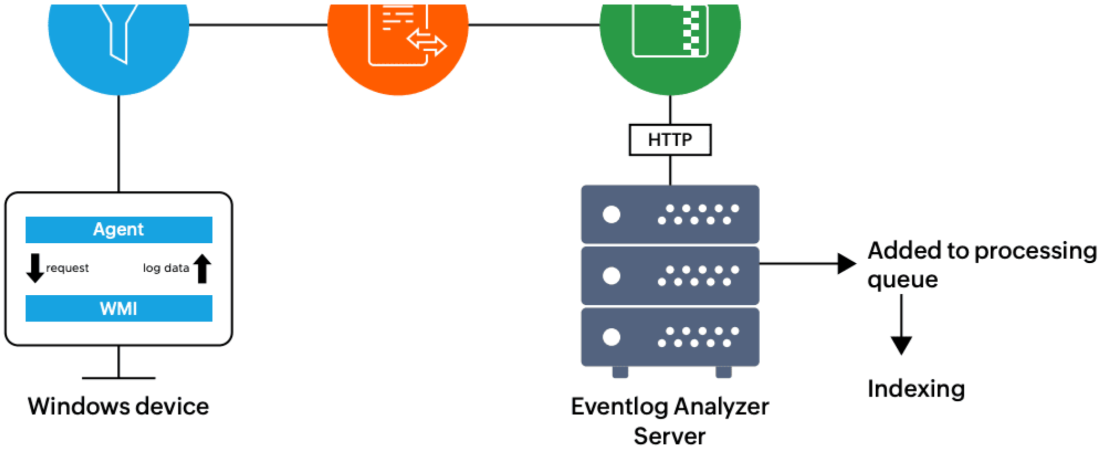
Agent for event log collection

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

Architecture

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





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

1.1.3. Prerequisites

Last updated on: September 12, 2025

Ports required for agentless communication

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

Service account permissions

- Domain Setup
- Workgroup Setup

Domain Setup

For admin users

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

For non-admin users

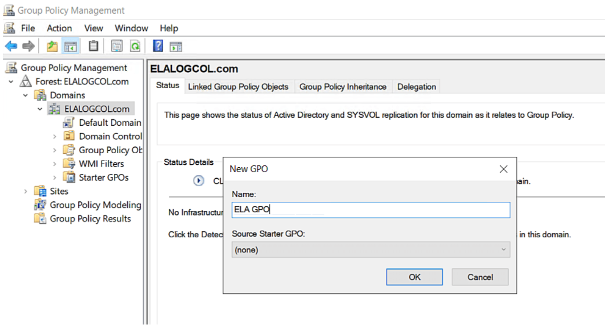
A service account has to be set up with the least privileges to collect logs in a domain setup. To create a service account with least privileges, follow the steps below.

Step 1: Create a new user

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

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

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



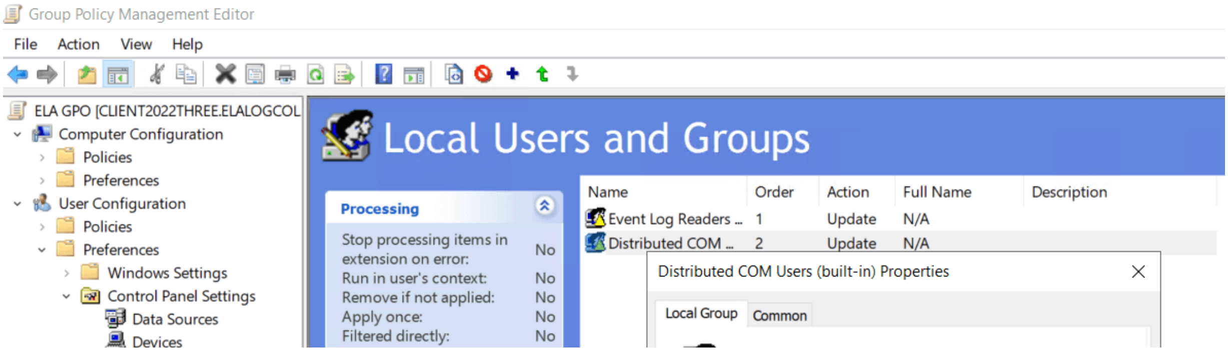
This page shows the status of Active Directory and SYSVOL replication for this domain as it relates to Group Policy.

Name: ELA GPO

Source Starter GPO: (none)

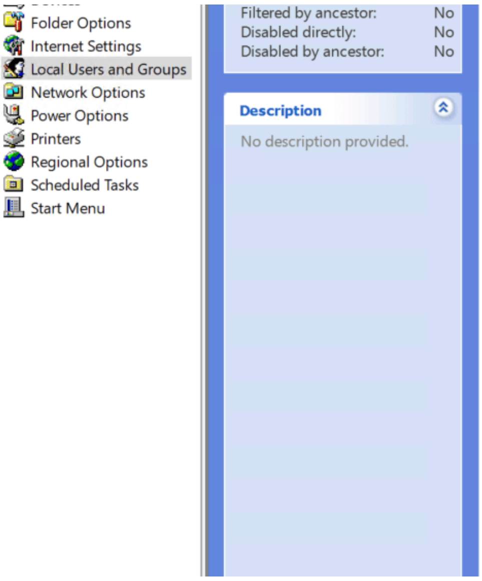
Step 3: Add user to Event Log Readers and Distributed COM user

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.



Name	Order	Action	Full Name	Description
Event Log Readers ...	1	Update	N/A	
Distributed COM ...	2	Update	N/A	

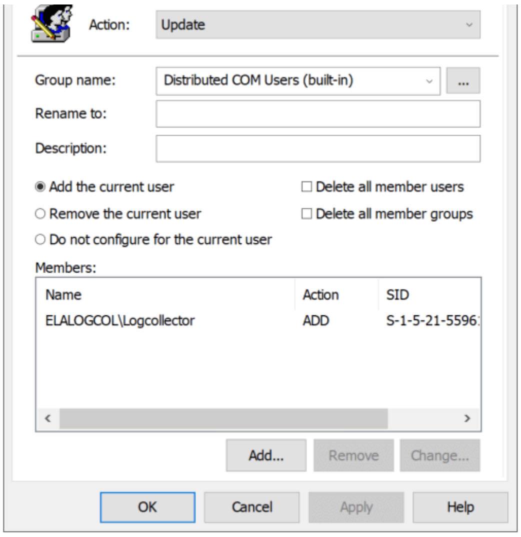
Stop processing items in extension on error: No
Run in user's context: No
Remove if not applied: No
Apply once: No
Filtered directly: No



Filtered by ancestor: No
Disabled directly: No
Disabled by ancestor: No

Description

No description provided.



Action: Update

Group name: Distributed COM Users (built-in)

Rename to:

Description:

● Add the current user
○ Remove the current user
○ Do not configure for the current user

□ Delete all member users
□ Delete all member groups

Members:

Name	Action	SID
ELALOGCOL\Logcollector	ADD	S-1-5-21-5596

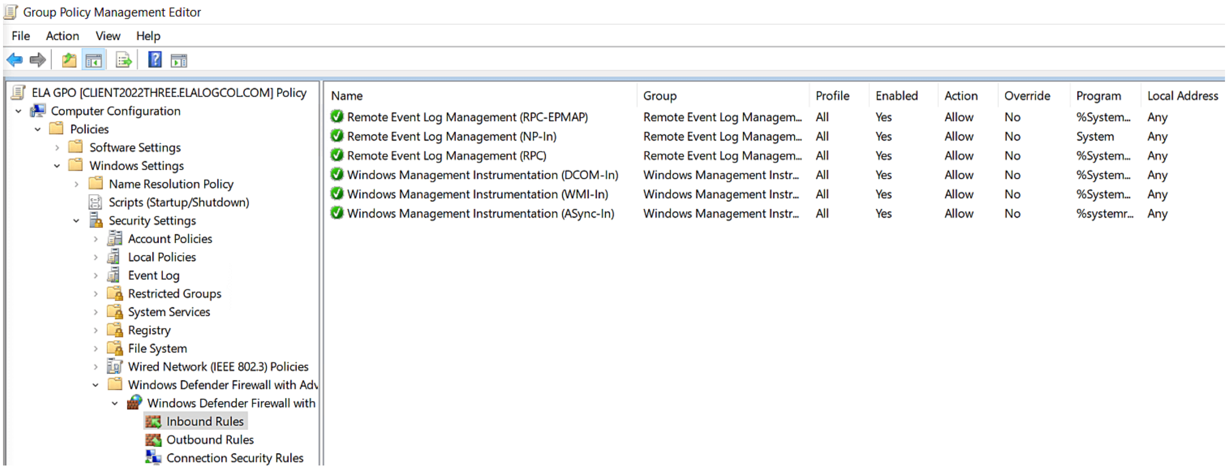
ⓘ Note

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.



Name	Group	Profile	Enabled	Action	Override	Program	Local Address
✓ Remote Event Log Management (RPC-EPMAP)	Remote Event Log Managem...	All	Yes	Allow	No	%System...	Any
✓ Remote Event Log Management (NP-In)	Remote Event Log Managem...	All	Yes	Allow	No	System	Any
✓ Remote Event Log Management (RPC)	Remote Event Log Managem...	All	Yes	Allow	No	%System...	Any
✓ Windows Management Instrumentation (DCOM-In)	Windows Management Instr...	All	Yes	Allow	No	%System...	Any
✓ Windows Management Instrumentation (WMI-In)	Windows Management Instr...	All	Yes	Allow	No	%System...	Any
✓ Windows Management Instrumentation (ASync-In)	Windows Management Instr...	All	Yes	Allow	No	%systemr...	Any

ⓘ 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.

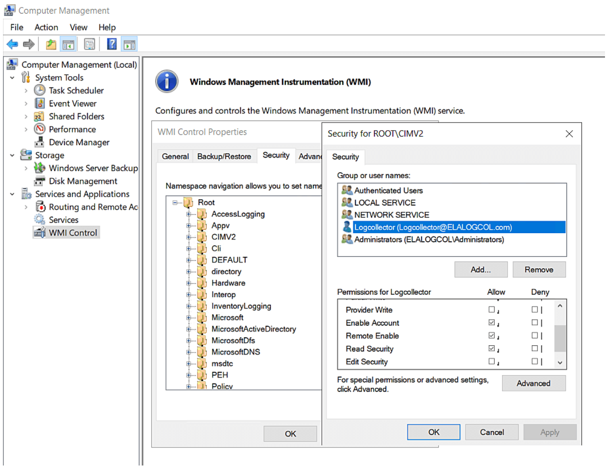
Step 5: Force the group policy

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.



Windows Management Instrumentation (WMI)

Configures and controls the Windows Management Instrumentation (WMI) service.

Namespace navigation allows you to set name

Security for ROOT\CIMV2

Group or user names:

Authenticated Users
LOCAL SERVICE
NETWORK SERVICE
Logcollector (Logcollector@ELALOGCOL.com)
Administrators (ELALOGCOL\Administrators)

Permissions for Logcollector	Allow	Deny
Provider Write	□	□
Enable Account	☑	□
Remote Enable	☑	□
Read Security	☑	□
Edit Security	□	□

For special permissions or advanced settings, click Advanced.

ⓘ 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

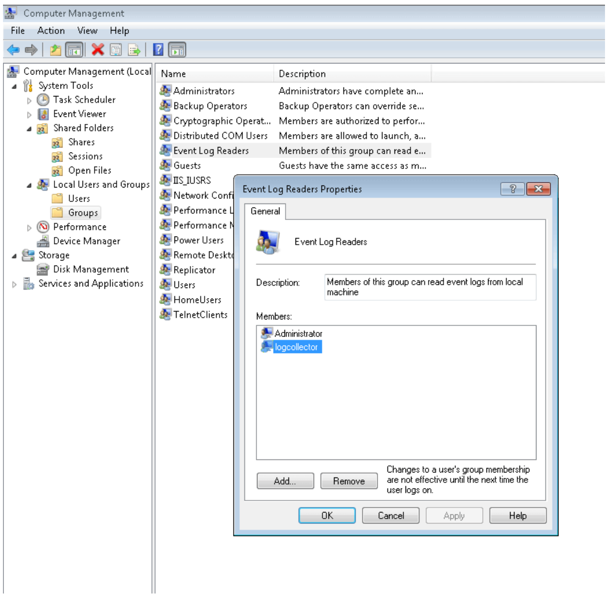
Policies Windows Settings Scripts (Startup/Shutdown) → Startup or the scripts will run every time during startup.

- 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.



Name	Description
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
IIS_IUSRS	
Network Confi	
Performance L	
Performance M	
Power Users	
Remote Deskto	
Replicator	
Users	
HomeUsers	
TelnetClients	

Event Log Readers Properties

General

Event Log Readers

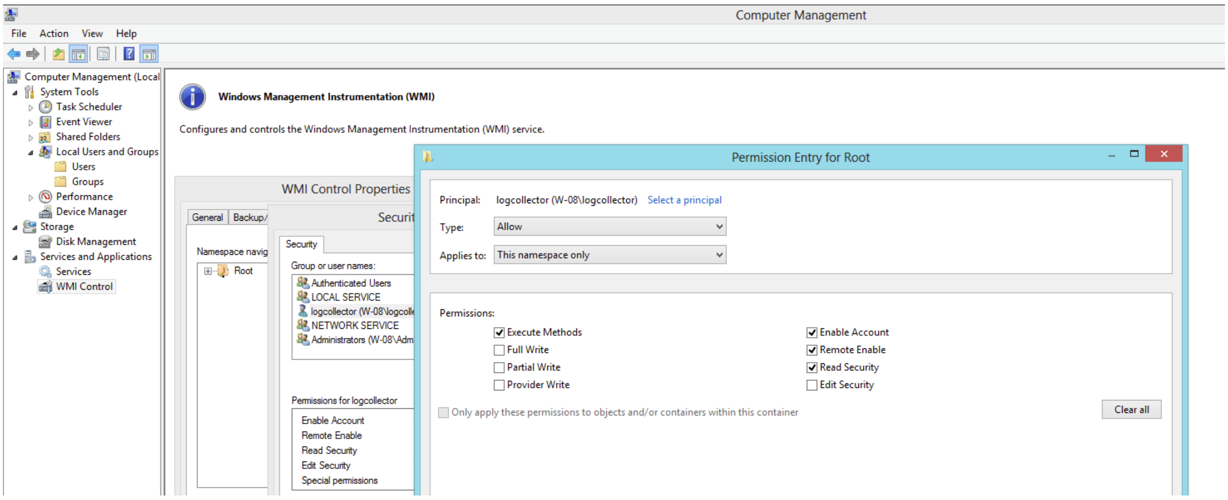
Description: Members of this group can read event logs from local machine

Members:
Administrator
logcollector

Changes to a user's group membership are not effective until the next time the user logs on.

Step 2: Grant necessary WMI permissions:

1. Refer Step 6: Grant necessary WMI permissions.



Windows Management Instrumentation (WMI)

Configures and controls the Windows Management Instrumentation (WMI) service.

WMI Control Properties

Group or user names:
Authenticated Users
LOCAL SERVICE
logcollector (W-08\logcolle
NETWORK SERVICE
Administrators (W-08\Adm

Permissions for logcollector
Enable Account
Remote Enable
Read Security
Edit Security
Special permissions

Permission Entry for Root

Principal: logcollector (W-08\logcollector) Select a principal

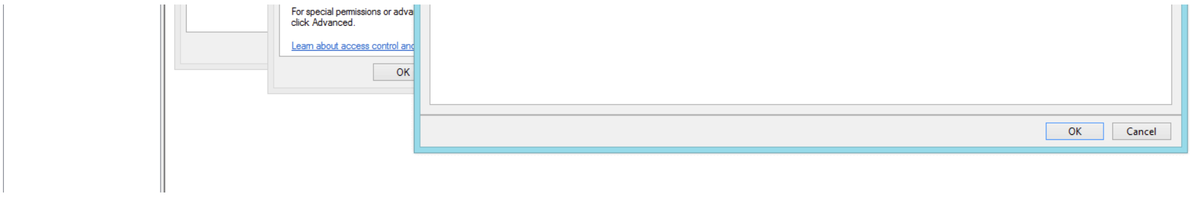
Type: Allow

Applies to: This namespace only

Permissions:

☑ Execute Methods	☑ Enable Account
☐ Full Write	☑ Remote Enable
☐ Partial Write	☑ Read Security
☐ Provider Write	☐ Edit Security

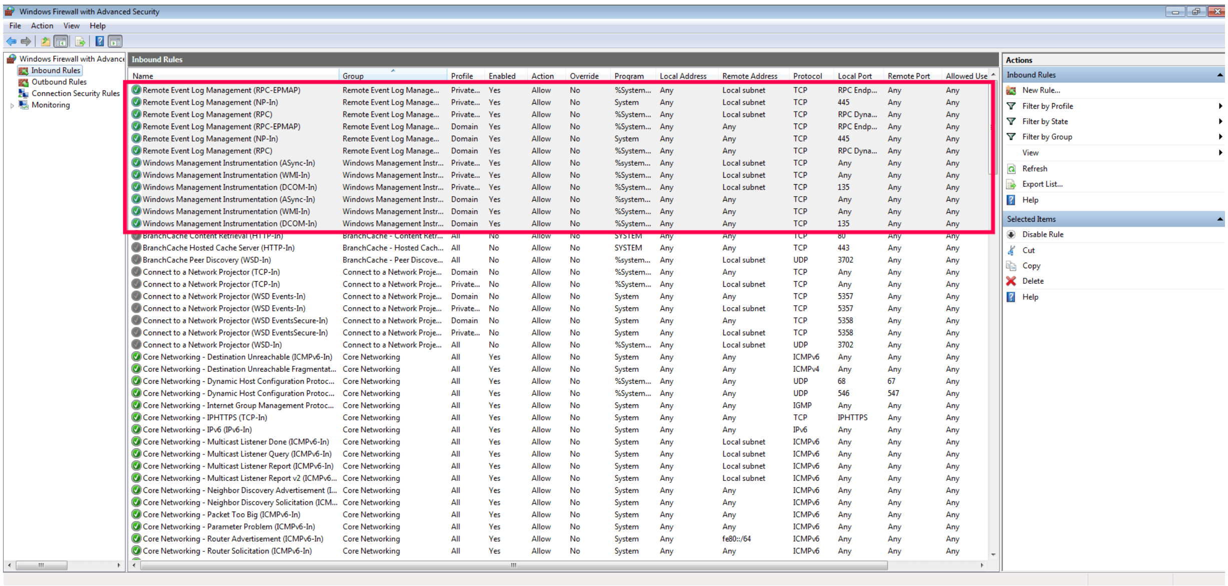
☐ Only apply these permissions to objects and/or containers within this container



For special permissions or adva click Advanced.

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.



Inbound Rules

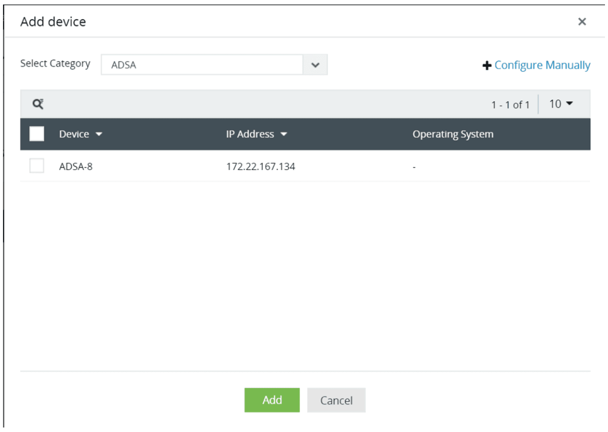
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Allowed Use
Remote Event Log Management (RPC-EPMAP)	Remote Event Log Manage...	Private...	Yes	Allow	No	%System...	Any	Local subnet	TCP	RPC Endp...	Any	Any
Remote Event Log Management (NP-In)	Remote Event Log Manage...	Private...	Yes	Allow	No	System	Any	Local subnet	TCP	445	Any	Any
Remote Event Log Management (RPC)	Remote Event Log Manage...	Private...	Yes	Allow	No	%System...	Any	Local subnet	TCP	RPC Dyna...	Any	Any
Remote Event Log Management (RPC-EPMAP)	Remote Event Log Manage...	Domain	Yes	Allow	No	%System...	Any	Any	TCP	RPC Endp...	Any	Any
Remote Event Log Management (NP-In)	Remote Event Log Manage...	Domain	Yes	Allow	No	System	Any	Any	TCP	445	Any	Any
Remote Event Log Management (RPC)	Remote Event Log Manage...	Domain	Yes	Allow	No	%System...	Any	Any	TCP	RPC Dyna...	Any	Any
Windows Management Instrumentation (ASync-In)	Windows Management Instr...	Private...	Yes	Allow	No	%system...	Any	Local subnet	TCP	Any	Any	Any
Windows Management Instrumentation (WMI-In)	Windows Management Instr...	Private...	Yes	Allow	No	%System...	Any	Local subnet	TCP	Any	Any	Any
Windows Management Instrumentation (DCOM-In)	Windows Management Instr...	Private...	Yes	Allow	No	%System...	Any	Local subnet	TCP	135	Any	Any
Windows Management Instrumentation (ASync-In)	Windows Management Instr...	Domain	Yes	Allow	No	%system...	Any	Any	TCP	Any	Any	Any
Windows Management Instrumentation (WMI-In)	Windows Management Instr...	Domain	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any	Any
Windows Management Instrumentation (DCOM-In)	Windows Management Instr...	Domain	Yes	Allow	No	%System...	Any	Any	TCP	135	Any	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80	Any	Any
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	443	Any	Any
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%system...	Any	Local subnet	UDP	3702	Any	Any
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow	No	%System...	Any	Any	TCP	Any	Any	Any
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow	No	%System...	Any	Local subnet	TCP	Any	Any	Any
Connect to a Network Projector (WSD Events-In)	Connect to a Network Proje...	Domain	No	Allow	No	System	Any	Any	TCP	5357	Any	Any
Connect to a Network Projector (WSD Events-In)	Connect to a Network Proje...	Private...	No	Allow	No	System	Any	Local subnet	TCP	5357	Any	Any
Connect to a Network Projector (WSD EventsSecure-In)	Connect to a Network Proje...	Domain	No	Allow	No	System	Any	Any	TCP	5358	Any	Any
Connect to a Network Projector (WSD EventsSecure-In)	Connect to a Network Proje...	Private...	No	Allow	No	System	Any	Local subnet	TCP	5358	Any	Any
Connect to a Network Projector (WSD-In)	Connect to a Network Proje...	All	No	Allow	No	%System...	Any	Local subnet	UDP	3702	Any	Any
Core Networking - Destination Unreachable (ICMPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Destination Unreachable Fragmentat...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv4	Any	Any	Any
Core Networking - Dynamic Host Configuration Protoc...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67	Any
Core Networking - Dynamic Host Configuration Protoc...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547	Any
Core Networking - Internet Group Management Protoc...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any	Any
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	TCP	IPHTTPS	Any	Any
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6	Any	Any	Any
Core Networking - Multicast Listener Done (ICMPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Query (ICMPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Report (ICMPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Report v2 (ICMPv6...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Neighbor Discovery Advertisement (I...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Neighbor Discovery Solicitation (ICM...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Parameter Problem (ICMPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Router Advertisement (ICMPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	fe80::/64	ICMPv6	Any	Any	Any
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any	Any

1.1.4. Adding windows device

Last updated on: September 12, 2025

Domain

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



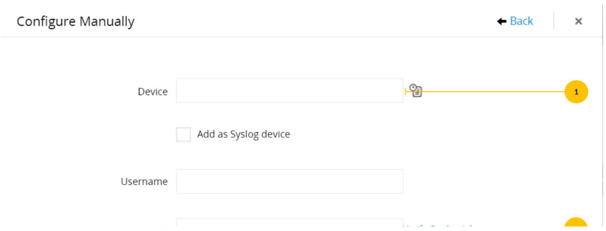
□	Device	IP Address	Operating System
□	ADSA-8	172.22.167.134	-

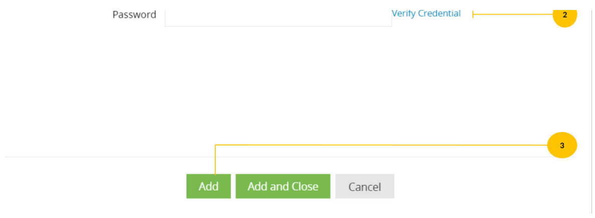
Workgroup

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

Note

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



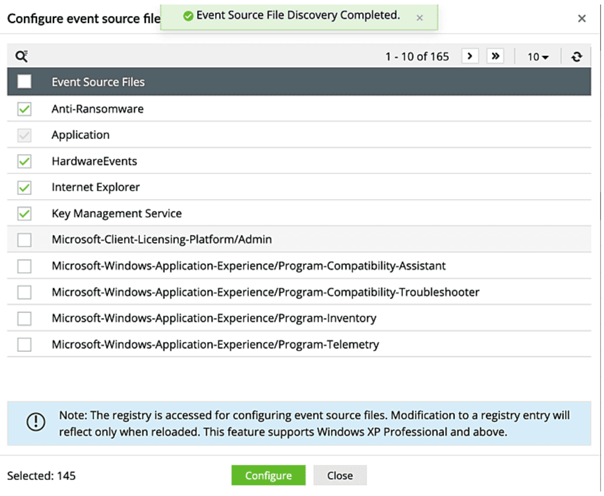


1. Enter the Device name or IP address. You can add the device as a Syslog device by clicking the Add as Syslog device checkbox.
2. Enter the Username and Password with administrator credentials, and click on Verify Credential.
3. Click on the Add button to add the device for monitoring.

How to configure event source files in a device

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

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


Configure event source file

Event Source File Discovery Completed.

1 - 10 of 165

☐	Event Source Files
☑	Anti-Ransomware
☑	Application
☑	HardwareEvents
☑	Internet Explorer
☑	Key Management Service
☐	Microsoft-Client-Licensing-Platform/Admin
☐	Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant
☐	Microsoft-Windows-Application-Experience/Program-Compatibility-Troubleshooter
☐	Microsoft-Windows-Application-Experience/Program-Inventory
☐	Microsoft-Windows-Application-Experience/Program-Telemetry

Note: The registry is accessed for configuring event source files. Modification to a registry entry will reflect only when reloaded. This feature supports Windows XP Professional and above.

Selected: 145

Historic log collection

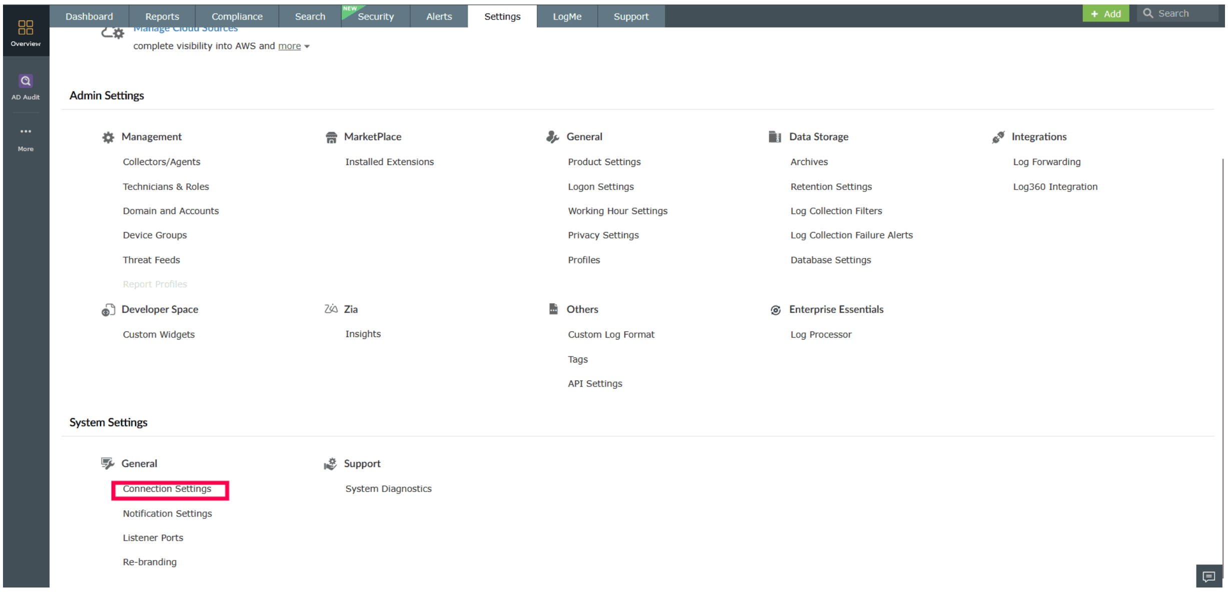
- Navigate to Settings > Configuration > Manage Devices > Add Devices. Select the device, click the icon on the right to enable historic log collection, and click Add.

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

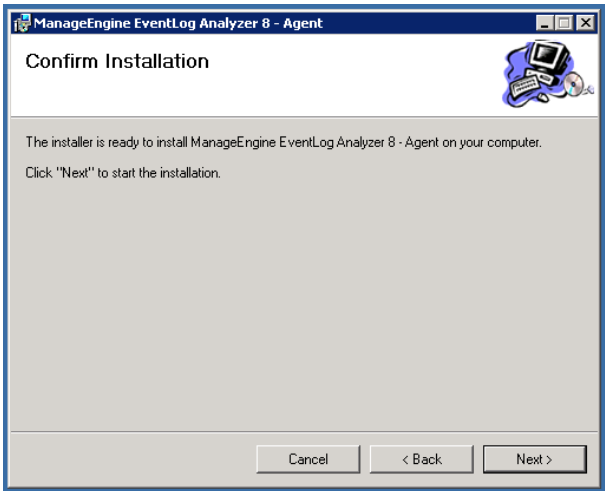
Last updated on: September 12, 2025

Installation procedure

Ensure that EventLog Analyzer server can access EC2 Windows instance.



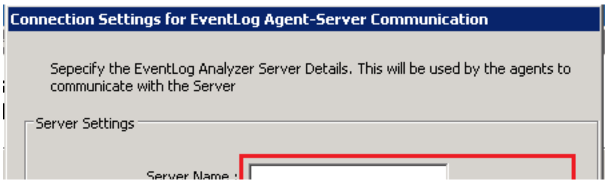
Welcome screen with copyright protection message appears.



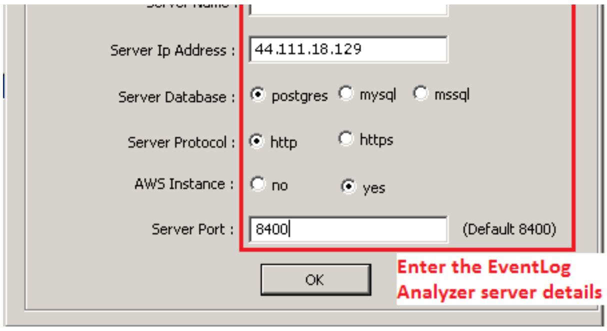
The installer is ready to install ManageEngine EventLog Analyzer 8 - Agent on your computer.

Click "Next" to start the installation.

Confirm the agent installation.



Sepecify the EventLog Analyzer Server Details. This will be used by the agents to communicate with the Server



Server Ip Address : 44.111.18.129

Server Database : ● postgres ○ mysql ○ mssql

Server Protocol : ● http ○ https

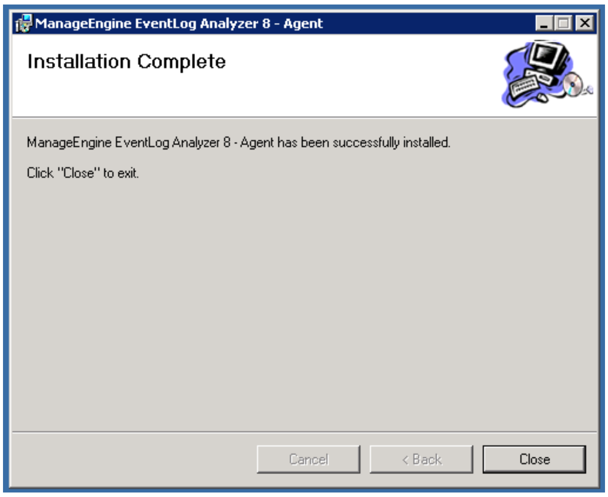
AWS Instance : ○ no ● yes

Server Port : 8400 (Default 8400)

Enter the EventLog Analyzer server details

Confirm the agent installation.

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



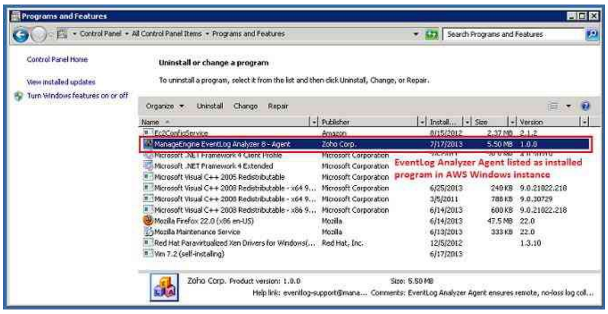
ManageEngine EventLog Analyzer 8 - Agent

Installation Complete

ManageEngine EventLog Analyzer 8 - Agent has been successfully installed.

Click "Close" to exit.

Confirm the agent installation.



Programs and Features
Control Panel ▸ All Control Panel Items ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾
Uninstall
Change
Repair

Uninstall or change a program

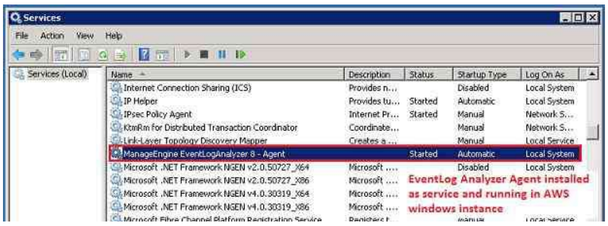
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Install...	Size	Version
Ec2ConfigService	Amazon	8/15/2012	2.37 MB	2.1.2
ManageEngine EventLog Analyzer 8 - Agent	Zoho Corp.	7/17/2013	5.50 MB	1.0.0
Microsoft .NET Framework 4 Client Profile	Microsoft Corporation	[illegible]	[illegible]	[illegible]
Microsoft .NET Framework 4 Extended	Microsoft Corporation			
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation			
Microsoft Visual C++ 2008 Redistributable - x64 9...	Microsoft Corporation	6/25/2013	240 KB	9.0.21022.218
Microsoft Visual C++ 2008 Redistributable - x64 9...	Microsoft Corporation	3/5/2011	788 KB	9.0.30729
Microsoft Visual C++ 2008 Redistributable - x86 9...	Microsoft Corporation	6/14/2013	600 KB	9.0.21022.218
Mozilla Firefox 22.0 (x86 en-US)	Mozilla	6/14/2013	47.5 MB	22.0
Mozilla Maintenance Service	Mozilla	6/13/2013	333 KB	22.0
Red Hat Paravirtualized Xen Drivers for Windows(...	Red Hat, Inc.	12/5/2012		1.3.10
Vim 7.2 (self-installing)		6/17/2013		

EventLog Analyzer Agent listed as installed program in AWS Windows instance

Zoho Corp. Product version: 1.0.0 Size: 5.50 MB
Help link: eventlog-support@mana... Comments: EventLog Analyzer Agent ensures remote, no-loss log coll...

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

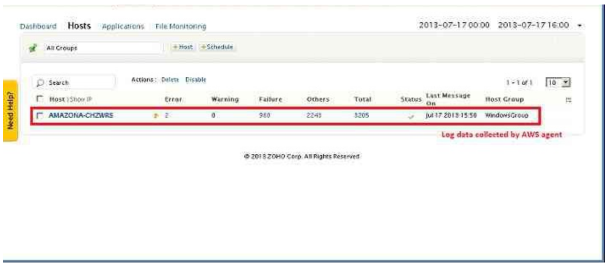


Name	Description	Status	Startup Type	Log On As
Internet Connection Sharing (ICS)	Provides n...		Disabled	Local System
IP Helper	Provides tu...	Started	Automatic	Local System
IPsec Policy Agent	Internet Pr...	Started	Manual	Network S...
KtmRm for Distributed Transaction Coordinator	Coordinate...		Manual	Network S...
Link-Layer Topology Discovery Mapper	Creates a ...		Manual	Local Service
ManageEngine EventLogAnalyzer 8 - Agent		Started	Automatic	Local System
Microsoft .NET Framework NGEN v2.0.50727_X64	Microsoft		Disabled	Local System
Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft			
Microsoft .NET Framework NGEN v4.0.30319_X64	Microsoft			
Microsoft .NET Framework NGEN v4.0.30319_X86	Microsoft			
Microsoft Fibre Channel Platform Registration Service	Registers t...		Manual	Local Service

EventLog Analyzer Agent installed as service and running in AWS windows instance

Microsoft iSCSI Initiator Service	Manages I...	Manual	Local System
Microsoft Software Shadow Copy Provider	Manages s...	Manual	Local System

Check whether the service is running.

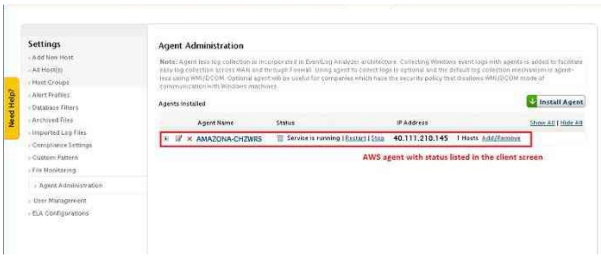


Host | Show IP	Error	Warning	Failure	Others	Total	Status	Last Message On	Host Group
AMAZONA-CHZWRS	2	0	960	2243	3205	✓	Jul 17 2013 15:50	WindowsGroup

Log data collected by AWS agent

© 2013 ZOHO Corp. All Rights Reserved

EC2 server name is resolved from the IP address provided.



Agent Administration

Note: Agent less log collection is incorporated in EventLog Analyzer architecture. Collecting Windows event logs with agents is added to facilitate easy log collection across WAN and through Firewall. Using agent to collect logs is optional and the default log collection mechanism is agent-less using WMI/DCOM. Optional agent will be useful for companies which have the security policy that disallows WMI/DCOM mode of communication with Windows machines.

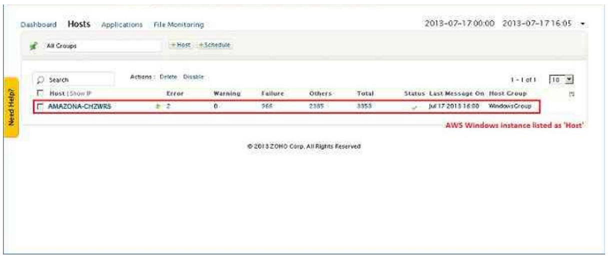
Agents Installed

Agent Name	Status	IP Address	
AMAZONA-CHZWRS	Service is running | Restart | Stop	40.111.210.145	1 Hosts Add/Remove

AWS agent with status listed in the client screen

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.



Host | Show IP	Error	Warning	Failure	Others	Total	Status	Last Message On	Host Group
AMAZONA-CHZWRS	2	0	966	2385	3353	✓	Jul 17 2013 16:00	WindowsGroup

AWS Windows instance listed as 'Host'

© 2013 ZOHO Corp. All Rights Reserved

EC2 server name is resolved from the IP address provided.

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

ⓘ Note

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

1.1.6. Setting up Windows Event Log Reports

Last updated on: September 12, 2025

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

Setting up Windows report generation

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

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

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

Reports	New keys	Audit policies	Other prerequisites
changes		Audit Policy Configuration > Object Access.	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 Cor Reports.
Print service	- Microsoft-Windows-PrintService/Operational - Microsoft-Windows-PrintService/Admin	No modification required.	

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

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

1.2.1. Adding Syslog Devices

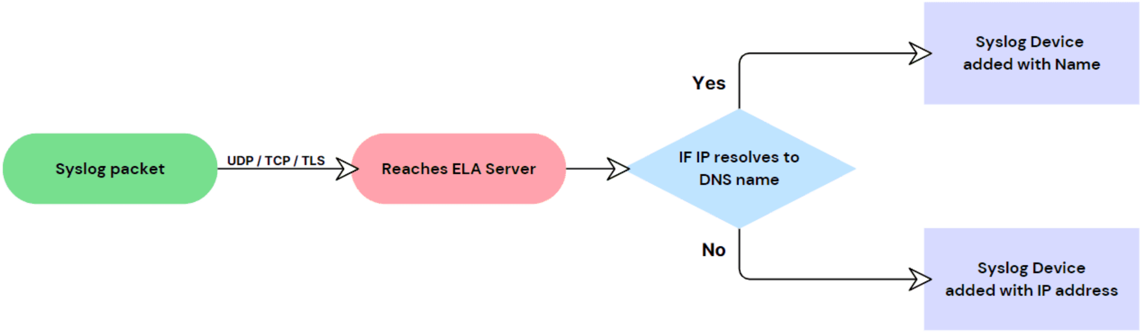
Last updated on: September 12, 2025

Automatic Syslog Device Addition

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

How it works:

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


Syslog packet
UDP / TCP / TLS
Reaches ELA Server
IF IP resolves to DNS name
Yes
Syslog Device added with Name
No
Syslog Device added with IP address

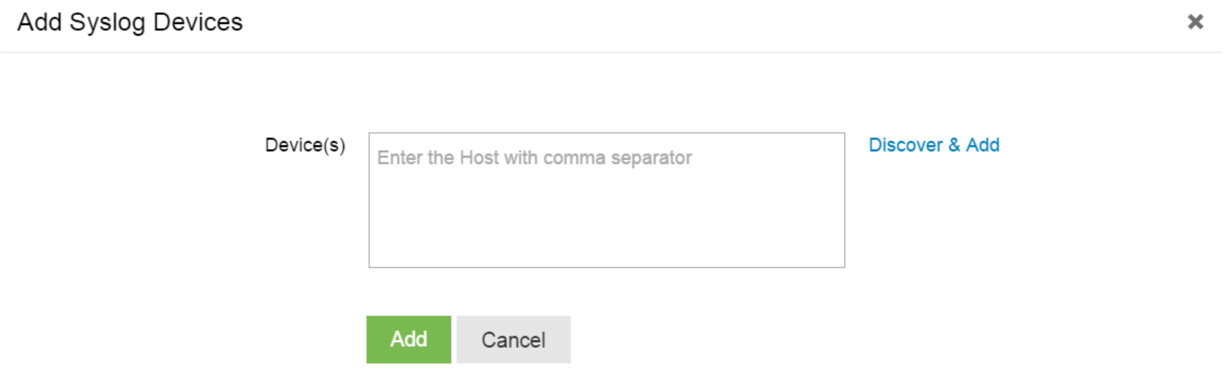
- If resolution is successful : The syslog device will be added with a resolved hostname.
- If resolution is unsuccessful : The syslog device will be added using the IP address.

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.

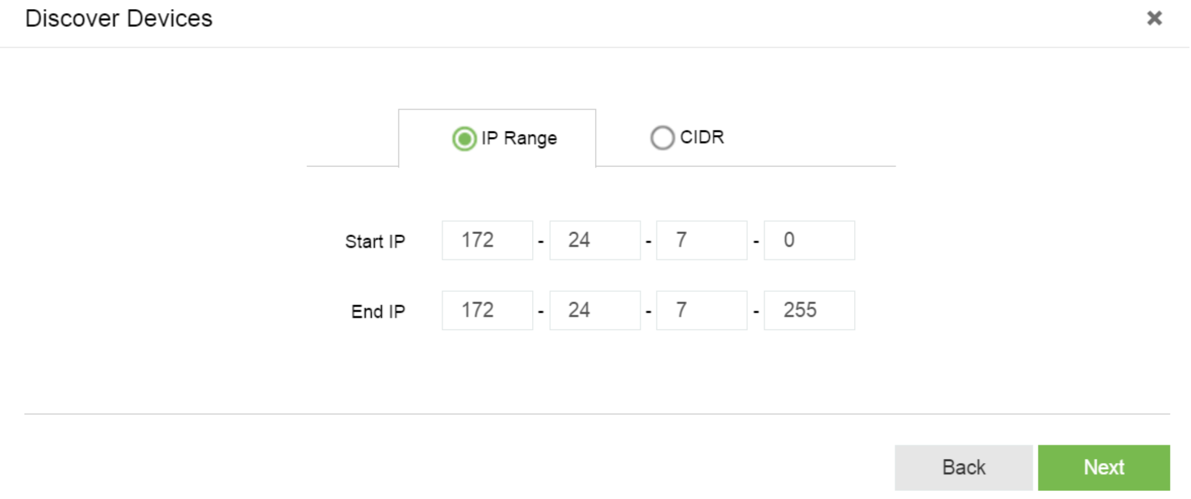
Manual Syslog Device Addition

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:

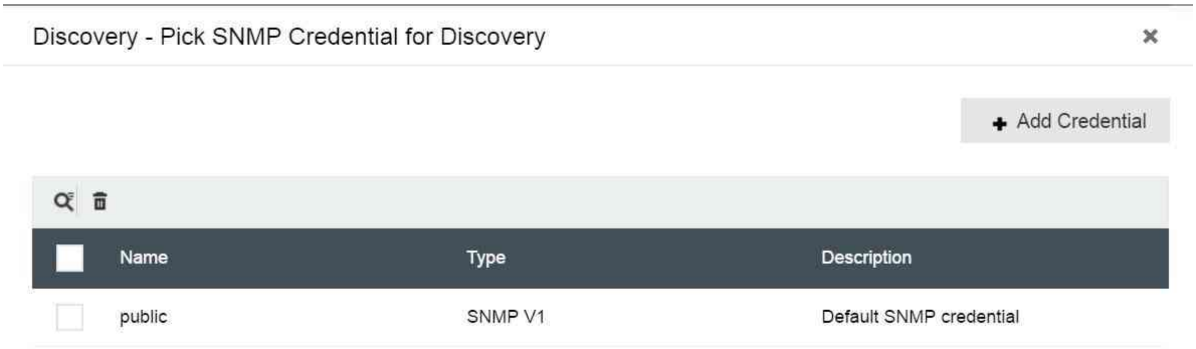
1. Click on the Discover & Add link in the Add Syslog Devices window. You can discover the Syslog devices in your network based on the IP range (Start IP to End IP) or CIDR.



Start IP 172 - 24 - 7 - 0

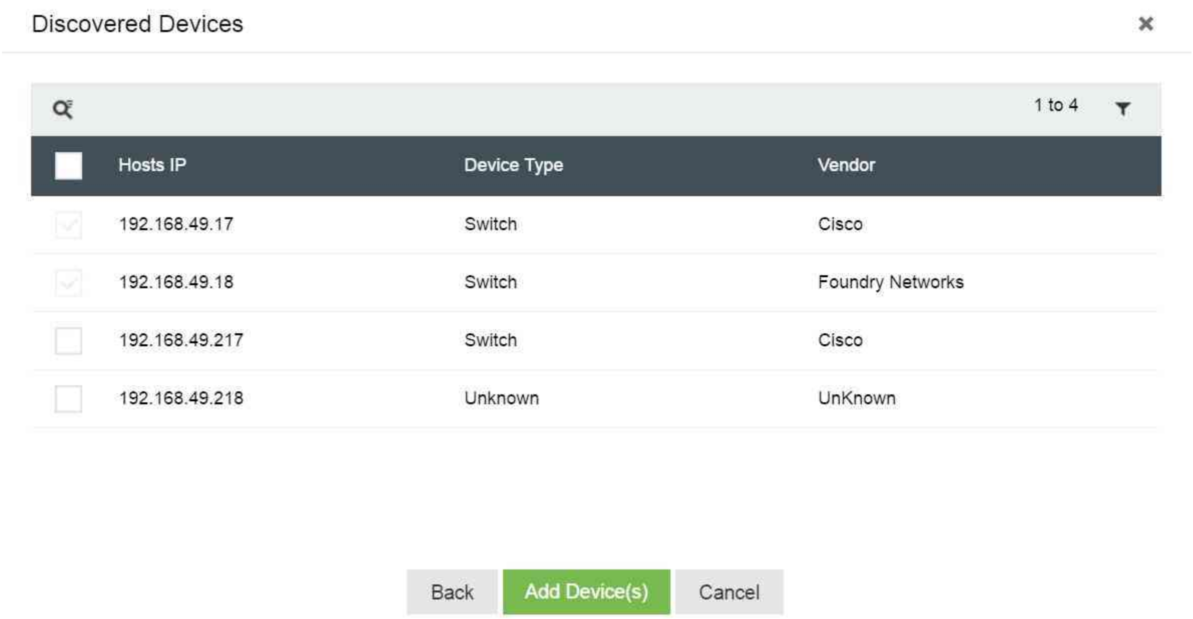
End IP 172 - 24 - 7 - 255

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



□	Name	Type	Description
□	public	SNMP V1	Default SNMP credential

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.



□	Hosts IP	Device Type	Vendor
☑	192.168.49.17	Switch	Cisco
☑	192.168.49.18	Switch	Foundry Networks
□	192.168.49.217	Switch	Cisco
□	192.168.49.218	Unknown	UnKnown

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.

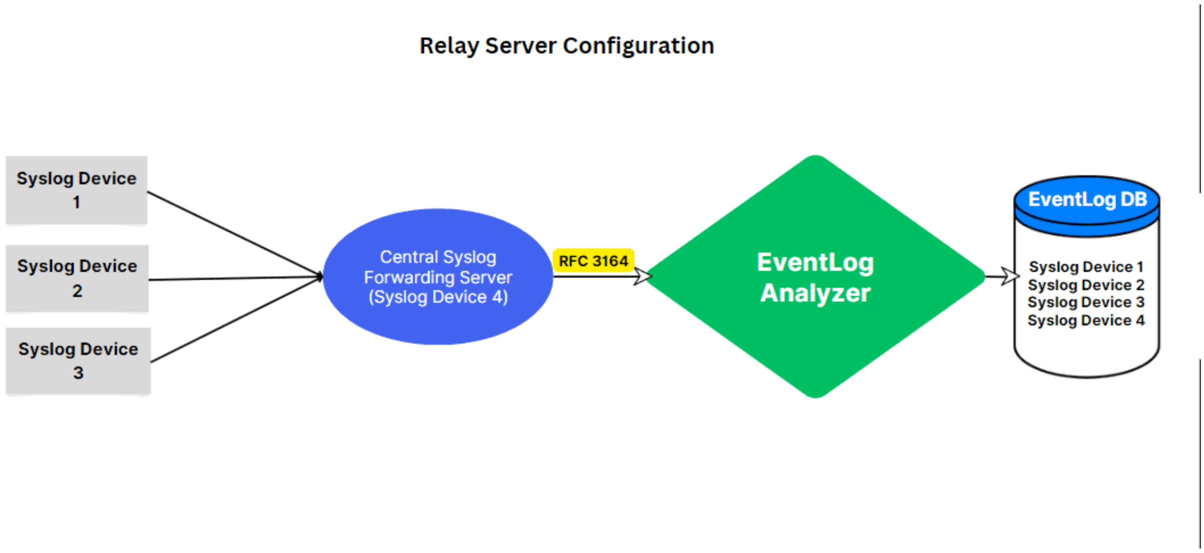
> ⓘ Note
>
> Refer here to configure Auto Log forwarding manually for other devices.

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

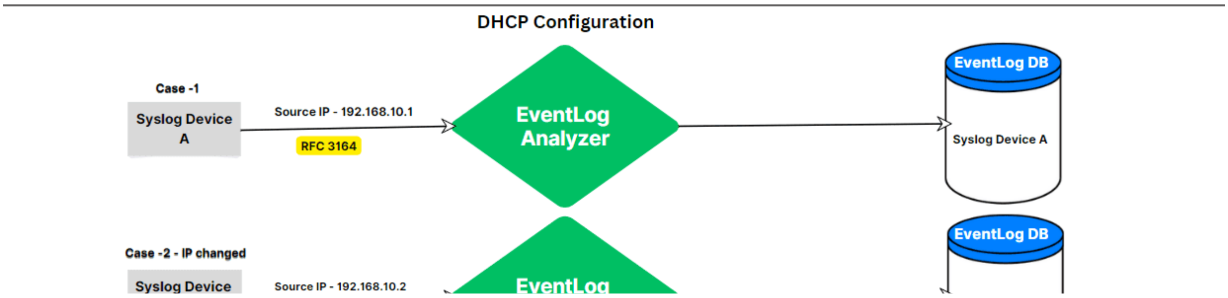
- The hostname (rootmachine) is parsed from the syslog packet and the syslog device is added with the hostname.
- If the hostname is already present in the database, then the logs will be mapped to that device.
- The syslog device can be Unix, Cisco, Fortinet, Palto Alto,etc.

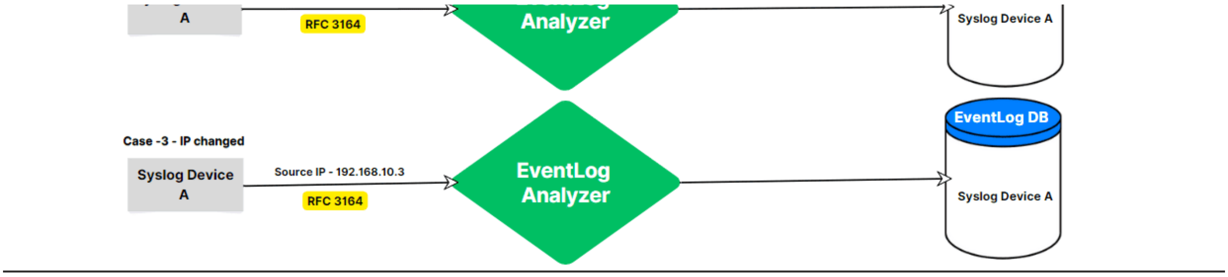
DHCP Configuration

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.

Chapter 1.3

Linux and Unix Systems

1.3.1. Adding Unix devices

Last updated on: September 12, 2025

1.3.2. Adding Mac OS devices

Last updated on: September 12, 2025

Chapter 1.4

Database

1.4.1. Adding SQL server

Last updated on: September 12, 2025

1.4.2. Adding MySQL Server

Last updated on: September 12, 2025

1.4.3. Adding Oracle Server

Last updated on: September 12, 2025

1.5.1. Configuring the Syslog Service on FireEye devices

Last updated on: September 12, 2025

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

1.5.2. Configuring the Syslog Service on Malwarebytes devices

Last updated on: September 12, 2025

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

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

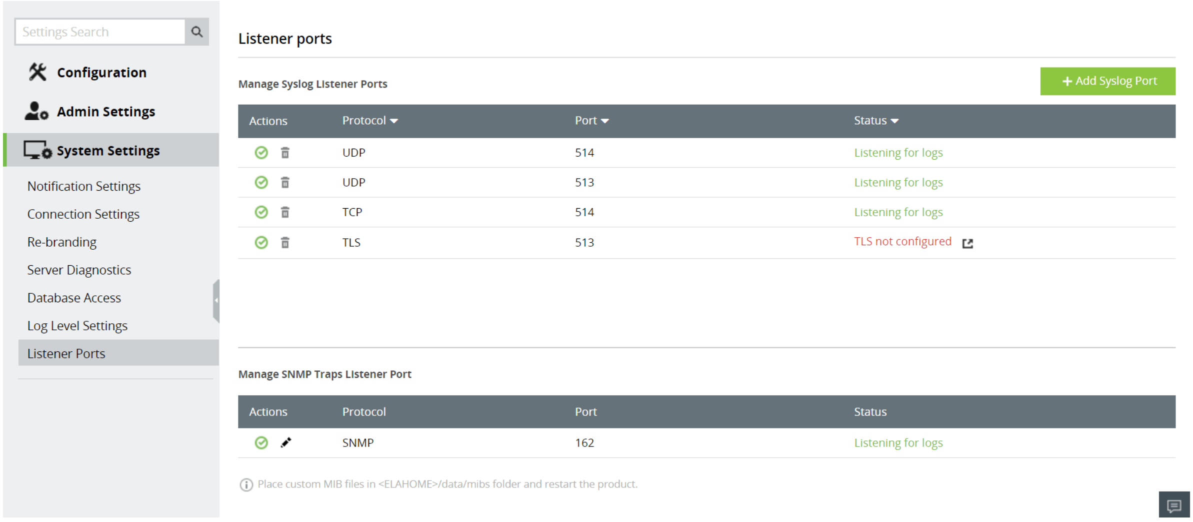
> ⓘ Note
>
> At the moment, only the Malwarebytes Management Console (MBMC) is supported.

1.5.3. Configuring McAfee Solutions

Last updated on: September 12, 2025

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

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



Listener ports

Manage Syslog Listener Ports

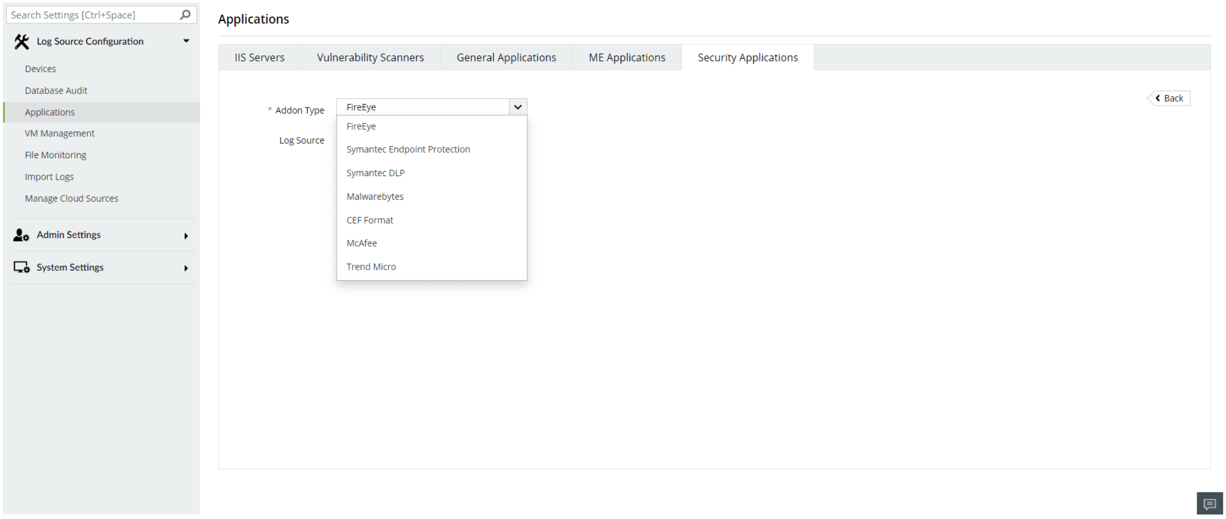
Actions	Protocol	Port	Status
	UDP	514	Listening for logs
	UDP	513	Listening for logs
	TCP	514	Listening for logs
	TLS	513	TLS not configured

Manage SNMP Traps Listener Port

Actions	Protocol	Port	Status
	SNMP	162	Listening for logs

Place custom MIB files in <ELAHOME>/data/mibs folder and restart the product.

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.

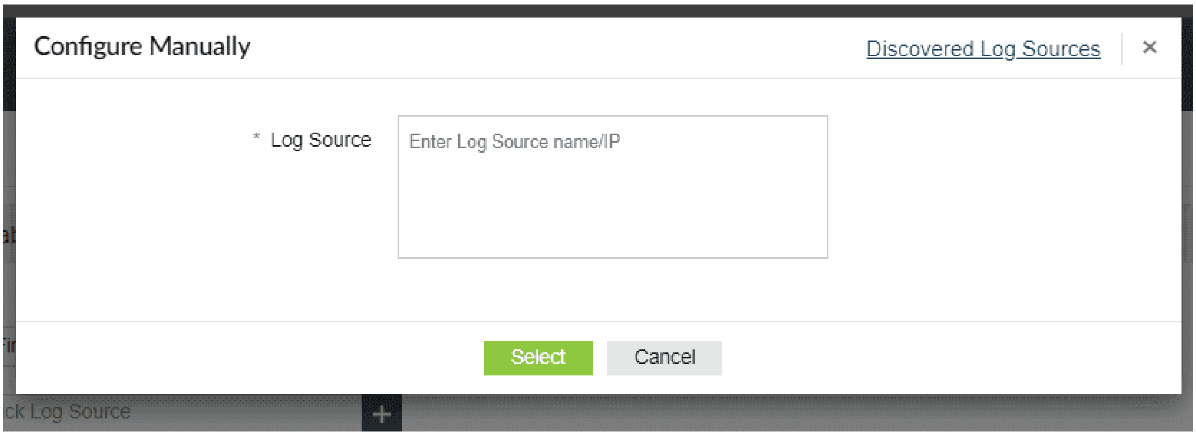


* Addon Type: FireEye

Log Source

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.



Configure Manually

* Log Source: Enter Log Source name/IP

Available reports:

- McAfee Events
- McAfee Threat Reports
- McAfee Virus Reports

1.5.4. Configuring the Syslog Service on Symantec DLP devices

Last updated on: September 12, 2025

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

1.5.5. Configuring the Syslog Service on Symantec Endpoint Protection devices

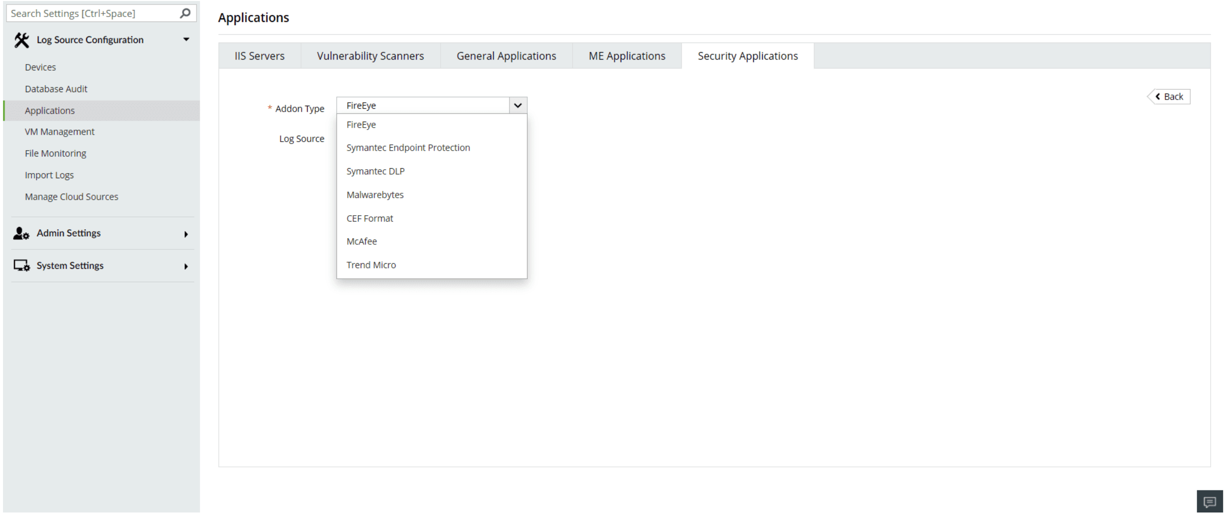
Last updated on: September 12, 2025

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

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

Last updated on: September 12, 2025

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

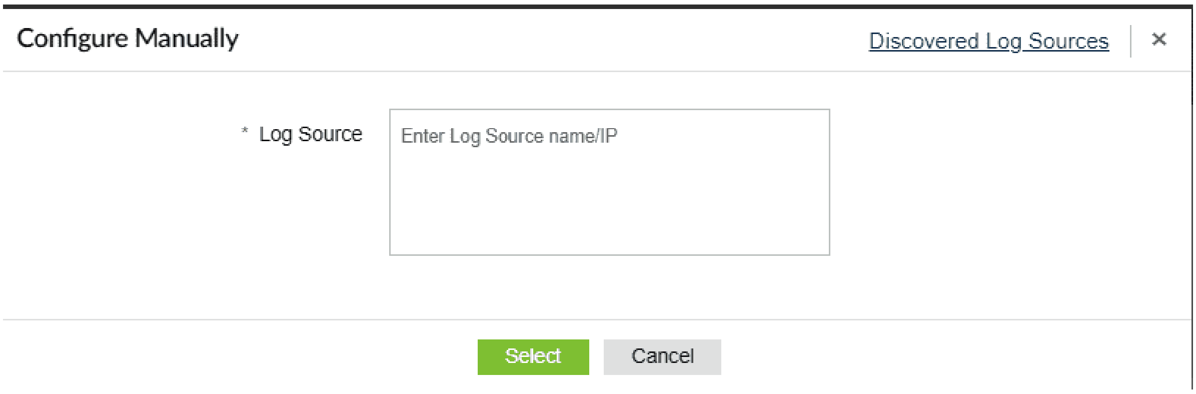


* Addon Type: FireEye

Log Source

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

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



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

Last updated on: September 12, 2025

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

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

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

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

1.6.2. Adding Arista Switches

Last updated on: September 12, 2025

1.6.3. Configuring the Syslog Service on Cisco Switches

Last updated on: September 12, 2025

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

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

1.6.4. Configuring the Syslog Service on Cisco Firepower devices

Last updated on: September 12, 2025

Step 1: Syslog server configuration

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

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

Step 2: Enable external logging for Connection Events

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

Step 3: Enable external logging for Intrusion Events

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

ⓘ Note

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

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

1.6.5. Configuring the Syslog Service on SonicWall devices

Last updated on: September 12, 2025

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

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

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

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

For SonicOS 6.5 and above:

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

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

1.6.6. Configuring the Syslog Service on Juniper devices

Last updated on: September 12, 2025

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

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

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

1.6.7. Configuring the Syslog Service on PaloAlto devices

Last updated on: September 12, 2025

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

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

For version 7.1 and above:

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

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

ⓘ Note

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

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

ⓘ Note

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

1.6.8. Configuring the Syslog Service on Cisco devices

Last updated on: September 12, 2025

1. Login to the Firewall.
2. Go to the config mode;
3. Configure the switch as given below (here, we have used Catalyst 2900) to send the logs to the EventLog Analyzer server:

   ```
   Cisco-ASA# config terminal
   Cisco-ASA (config)# logging host <EventLog _server_IP> [TCP/UDP]/< Port_Number >
   ```

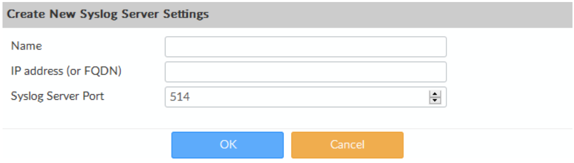
```
Cisco-ASA (config)# logging trap information
Cisco-ASA (config)# logging facility local7
```

1.6.9. Configuring the Syslog Service on Fortinet devices

Last updated on: September 12, 2025

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

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



Create New Syslog Server Settings

Name

IP address (or FQDN)

Syslog Server Port: 514

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

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

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

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

1.6.10. Configuring the Syslog Service on Check Point devices

Last updated on: September 12, 2025

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

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

1.6.11. Configuring the Syslog Service on NetScreen devices

Last updated on: September 12, 2025

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

Enabling Syslog Messages using the NetScreen Device:

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

Enabling Syslog Messages the CLI Console:

1.6.12. Configuring the Syslog Service on WatchGuard devices

Last updated on: September 12, 2025

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

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

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

1.6.13. Configuring the Syslog Service on Sophos devices

Last updated on: September 12, 2025

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

Enabling Sophos-UTM Syslog:

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

Enabling Sophos-XG Syslog:

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

1.6.14. Configuring the Syslog Service on Barracuda devices

Last updated on: September 12, 2025

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

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

4. Disable Log Data Tagging

5. Configure Logdata Streams

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

1.6.15. Configuring the Syslog Service on Huawei Firewall devices

Last updated on: September 12, 2025

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

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

1.6.16. Configuring the Syslog Service on Meraki devices

Last updated on: September 12, 2025

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

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

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

5. Click Save.

1.6.17. Configuring the Syslog Service on pfSense devices

Last updated on: September 12, 2025

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

1.6.18. Configuring the Syslog Service on H3C devices

Last updated on: September 12, 2025

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

1.6.19. Configuration the Syslog service on Stormshield firewall

Last updated on: September 12, 2025

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

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

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

Last updated on: September 12, 2025

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

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

1.6.21. Adding Forcepoint devices to EventLog Analyzer

Last updated on: September 12, 2025

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

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

Forwarding Forcepoint Audit Logs.

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

1.6.22. Adding Dell switches to EventLog Analyzer

Last updated on: September 12, 2025

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

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

Note

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

1.6.23. Configuring the Syslog Service on Topsec devices

Last updated on: September 12, 2025

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

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

Topsec reports

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

Topsec Events:

Provides information on all the events associated with Topsec devices.

Logon Reports

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

Firewall Allowed and Denied Traffic:

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

Firewall IDS/IPS Events:

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

Firewall Policy Management

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

Firewall Account Management

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

Interface Events

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

System Events:

Provides reports on configuration changes and system reboot.

Device Severity Reports:

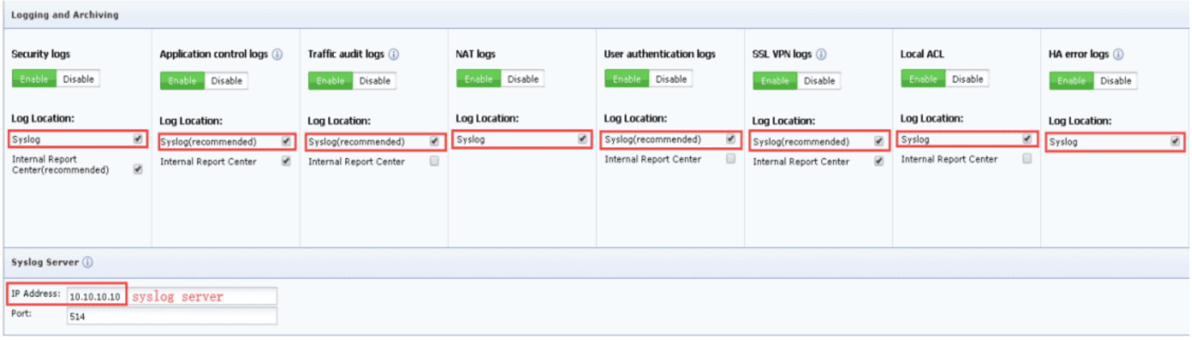
Provides reports on emergency, alerts, critical, error, warning, and notice events.

Configuring the Syslog Service on Sangfor devices

Last updated on: September 12, 2025

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

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



Logging and Archiving

Security logs: Enable
Log Location: Syslog ☑; Internal Report Center(recommended) ☑

Application control logs: Enable
Log Location: Syslog(recommended) ☑; Internal Report Center ☑

Traffic audit logs: Enable
Log Location: Syslog(recommended) ☑; Internal Report Center □

NAT logs: Enable
Log Location: Syslog ☑

User authentication logs: Enable
Log Location: Syslog(recommended) ☑; Internal Report Center □

SSL VPN logs: Enable
Log Location: Syslog(recommended) ☑; Internal Report Center ☑

Local ACL: Enable
Log Location: Syslog ☑; Internal Report Center □

HA error logs: Enable
Log Location: Syslog ☑

Syslog Server

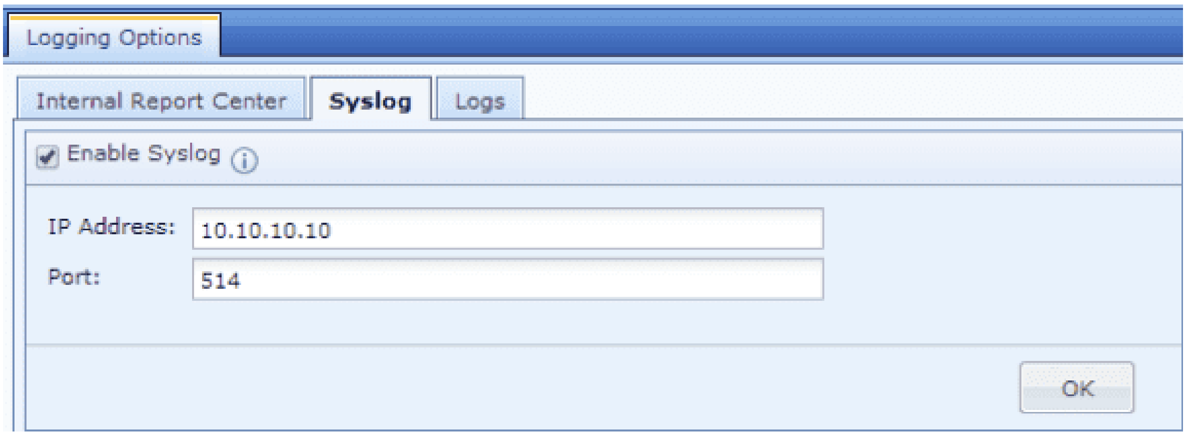
IP Address: 10.10.10.10 syslog server

Port: 514

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

For NGAF version 6.4 and below:

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



☑ Enable Syslog

IP Address: 10.10.10.10

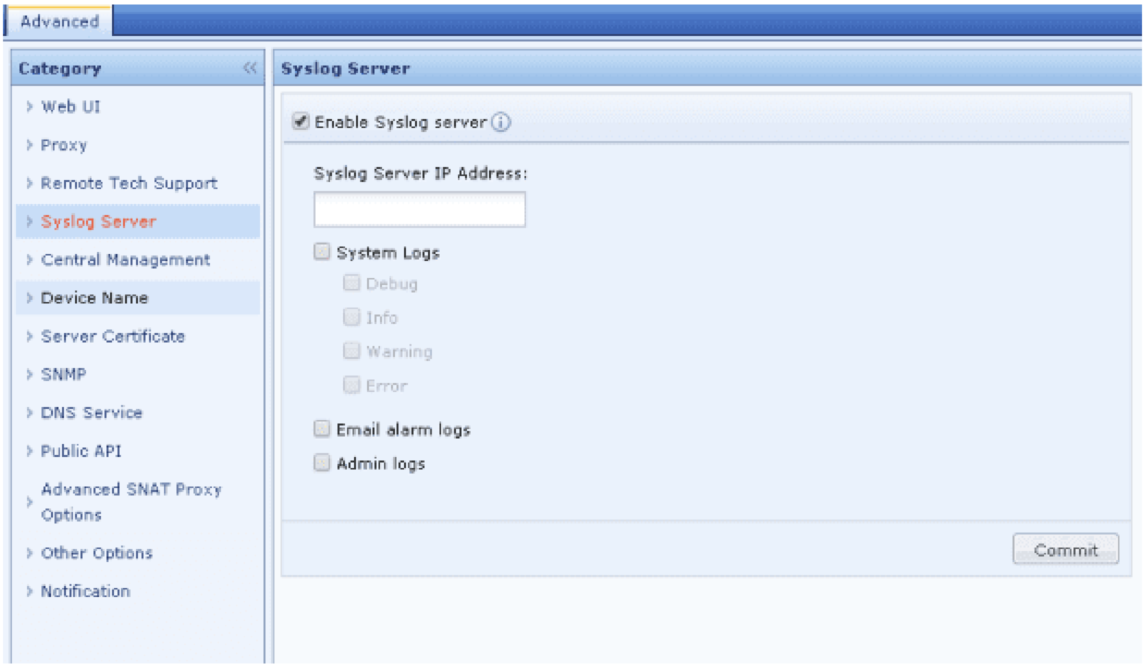
Port: 514

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

2. Click OK to apply changes.

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

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



☑ Enable Syslog server

Syslog Server IP Address:

□ System Logs

□ Debug

□ Info

□ Warning

□ Error

□ Email alarm logs

□ Admin logs

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

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

Sangfor Events:

Provides information on all the events associated with Sangfor devices.

Logon Report

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

Firewall Allowed and Denied Traffic:

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

Firewall IDS/IPS Events:

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

VPN Reports:

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

System Events:

Provides reports on configuration changes.

Device Severity Reports:

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

1.6.25. Enabling Stackato Logging

Last updated on: September 12, 2025

EventLog Analyzer automatically adds and collects your stackato logs upon executing the following command in your tty console:$kato config set logyard drainformats/<Format Name>[<PRI>{{.Text}}]

For UDP based log collection:

$kato drain add ela udp://<ela_server_name>:<udp_port_no> -f systail-ela-local

For TCP based log collection:

$kato drain add ela tcp://<ela_server_name>:<tcp_port_no> -f systail-ela-local

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

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

1.6.26. Configuring Zscaler NSS

Last updated on: September 12, 2025

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

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

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

1.7.1. Adding Common Event Format (CEF) Devices

Last updated on: September 12, 2025

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

To add CEF devices to EventLog Analyzer, click here.

1.7.2. Adding Print Servers

Last updated on: September 12, 2025

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

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

Print Server Configuration

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

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

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

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

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

1.7.3. Adding Terminal Servers

Last updated on: September 12, 2025

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

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

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

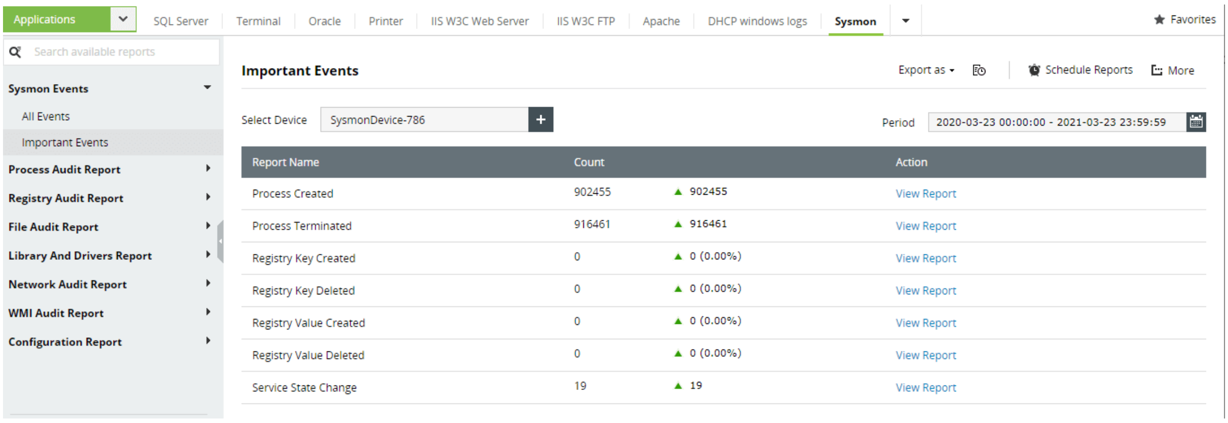
- Open the registry editor 'regedit' of the Terminal Server machine in the Command Line Window.
- Navigate to Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\
- To create a new key, right click on eventlog, click new > key. You can name the key as Microsoft-Windows-TerminalServices-Gateway/Operational.

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

1.7.4. Adding Sysmon Application

Last updated on: September 12, 2025

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



Important Events

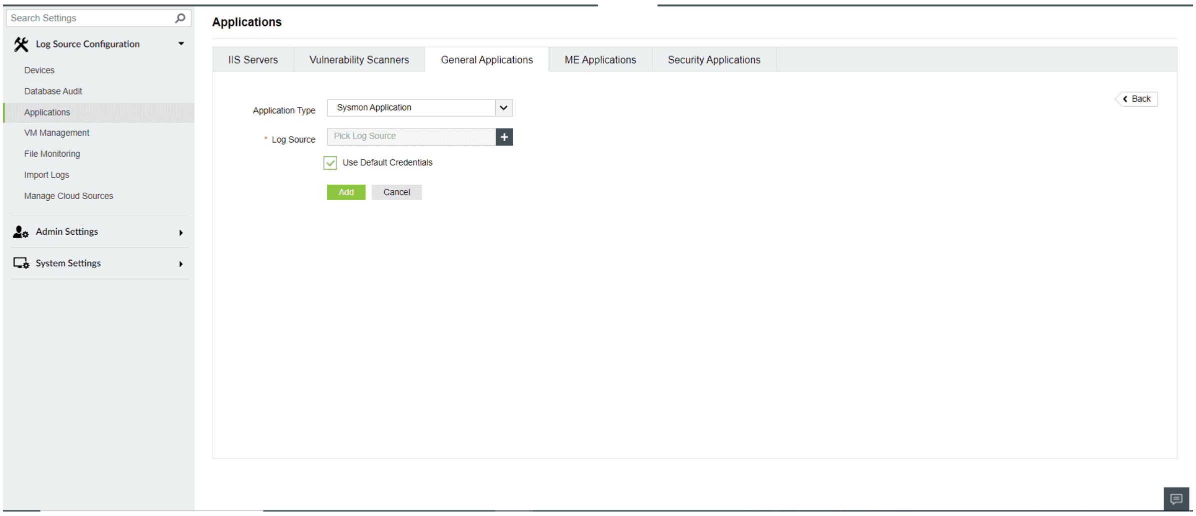
Select Device: SysmonDevice-786

Period: 2020-03-23 00:00:00 - 2021-03-23 23:59:59

Report Name	Count		Action
Process Created	902455	▲ 902455	View Report
Process Terminated	916461	▲ 916461	View Report
Registry Key Created	0	▲ 0 (0.00%)	View Report
Registry Key Deleted	0	▲ 0 (0.00%)	View Report
Registry Value Created	0	▲ 0 (0.00%)	View Report
Registry Value Deleted	0	▲ 0 (0.00%)	View Report
Service State Change	19	▲ 19	View Report

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



Application Type: Sysmon Application

* Log Source: Pick Log Source

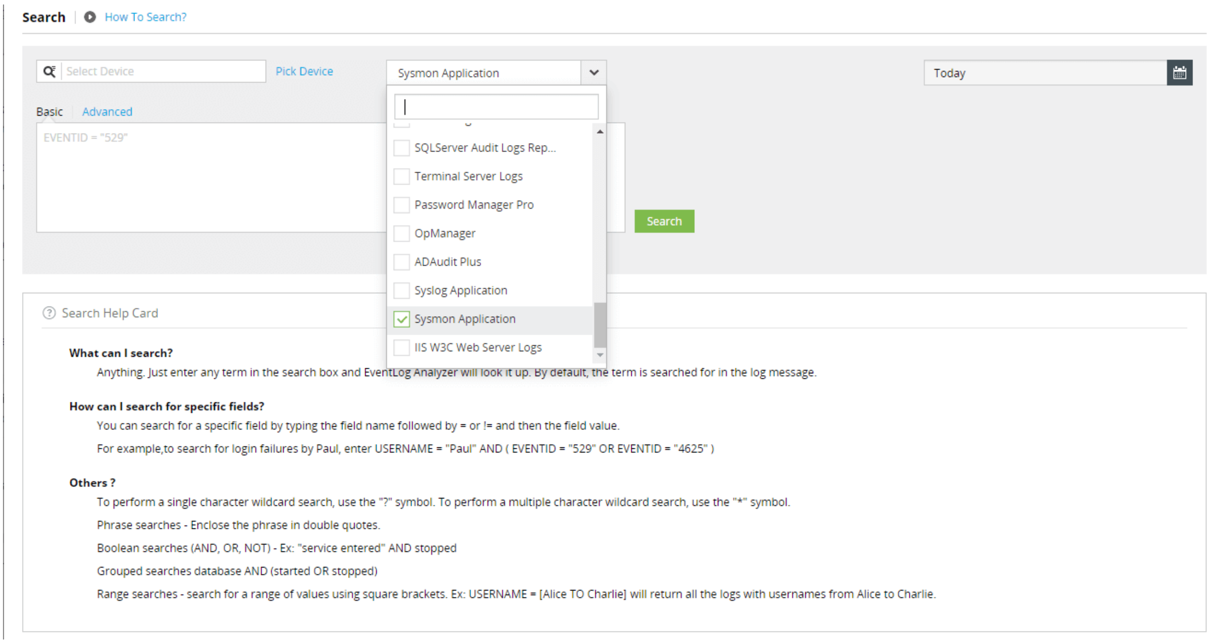
☑ Use Default Credentials

- 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.



What can I search?

Anything. Just enter any term in the search box and EventLog Analyzer will look it up. By default, the term is searched for in the log message.

How can I search for specific fields?

You can search for a specific field by typing the field name followed by = or != and then the field value.

For example,to search for login failures by Paul, enter USERNAME = "Paul" AND (EVENTID = "529" OR EVENTID = "4625")

Others ?

To perform a single character wildcard search, use the "?" symbol. To perform a multiple character wildcard search, use the "*" symbol.

Phrase searches - Enclose the phrase in double quotes.

Boolean searches (AND, OR, NOT) - Ex: "service entered" AND stopped

Grouped searches database AND (started OR stopped)

Range searches - search for a range of values using square brackets. Ex: USERNAME = [Alice TO Charlie] will return all the logs with usernames from Alice to Charlie.

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.

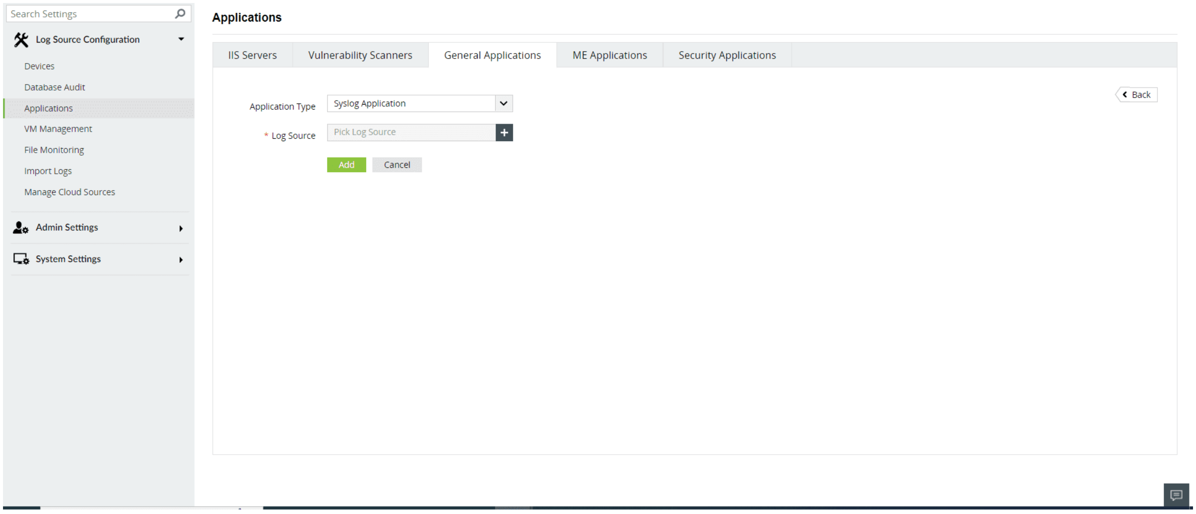
1.7.5. Adding a Syslog Application

Last updated on: September 12, 2025

When should the Syslog Application be used?

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

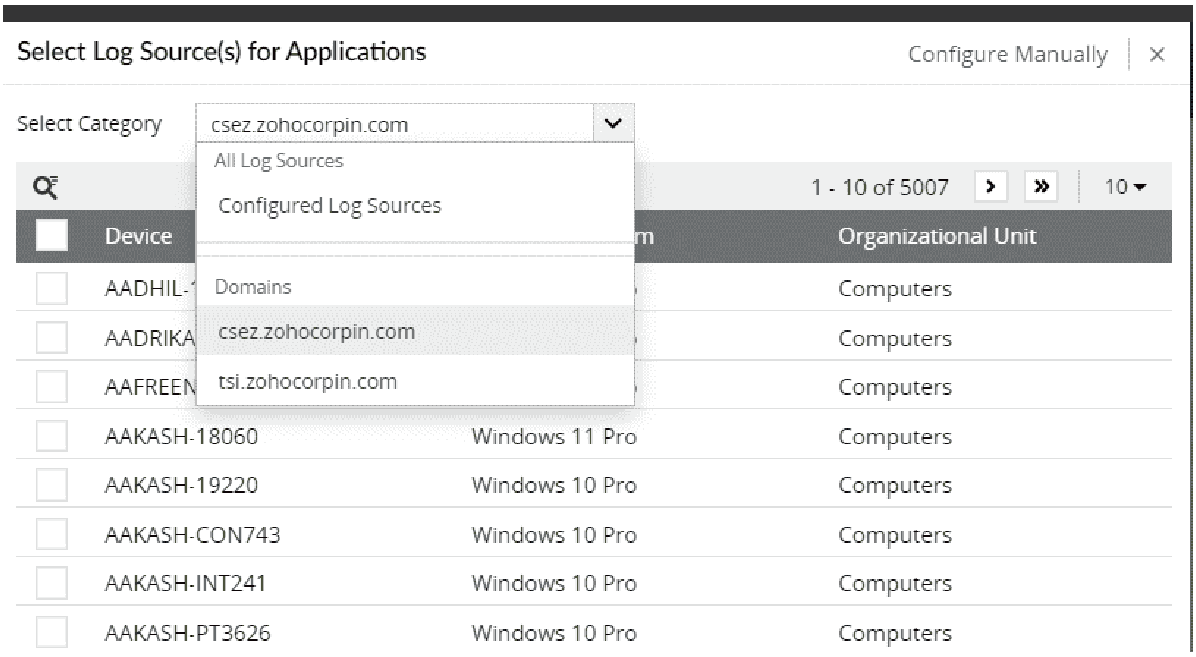
- Navigate to Settings > Log Source Configuration > Applications. You can also click on the +Add button on the top-right corner of the Home page and select Application.
- Click on the General Application -> Add General Applications .
- Choose Syslog Application as Application Type



Application Type: Syslog Application

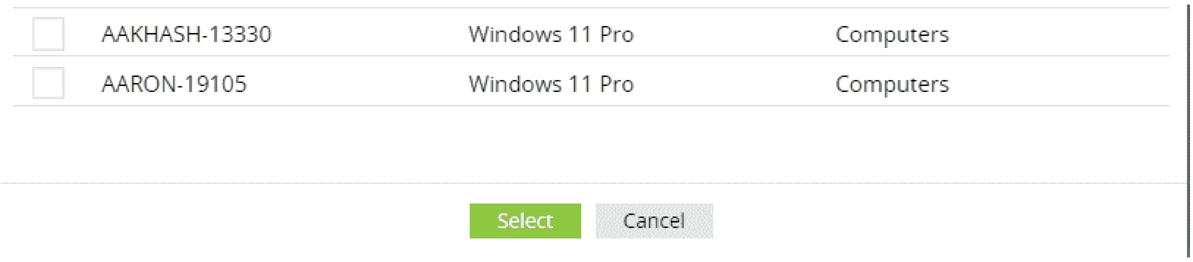
* Log Source: Pick Log Source

- 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.



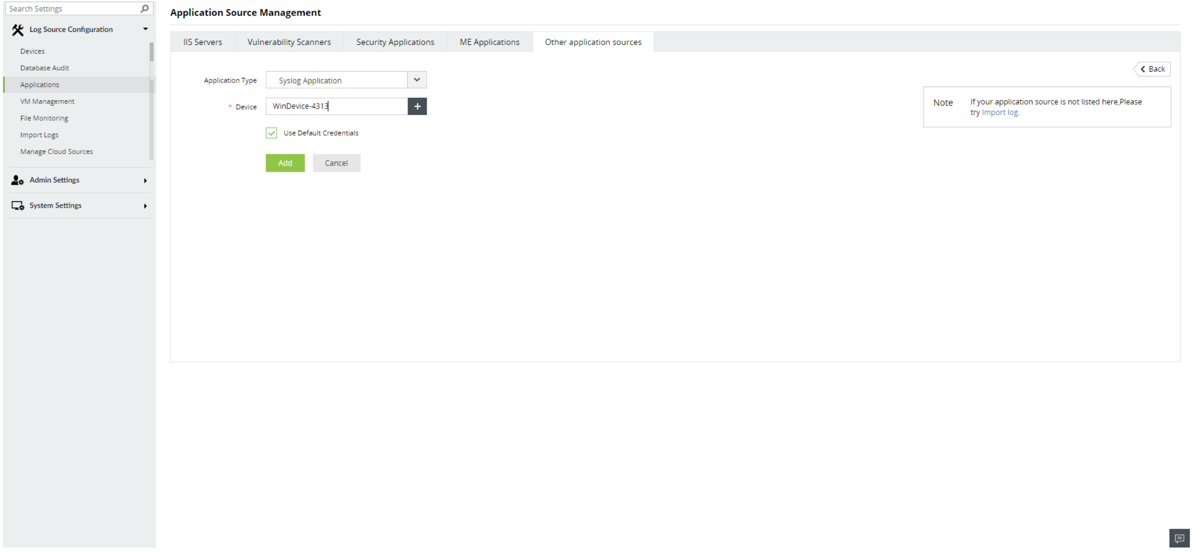
Select Category: csez.zohocorpin.com

□	Device	m	Organizational Unit
□	AADHIL-1		Computers
□	AADRIKA		Computers
□	AAFREEN		Computers
□	AAKASH-18060	Windows 11 Pro	Computers
□	AAKASH-19220	Windows 10 Pro	Computers
□	AAKASH-CON743	Windows 10 Pro	Computers
□	AAKASH-INT241	Windows 10 Pro	Computers
□	AAKASH-PT3626	Windows 10 Pro	Computers



□	AAKHASH-13330	Windows 11 Pro	Computers
□	AARON-19105	Windows 11 Pro	Computers

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



Application Source Management

Application Type: Syslog Application

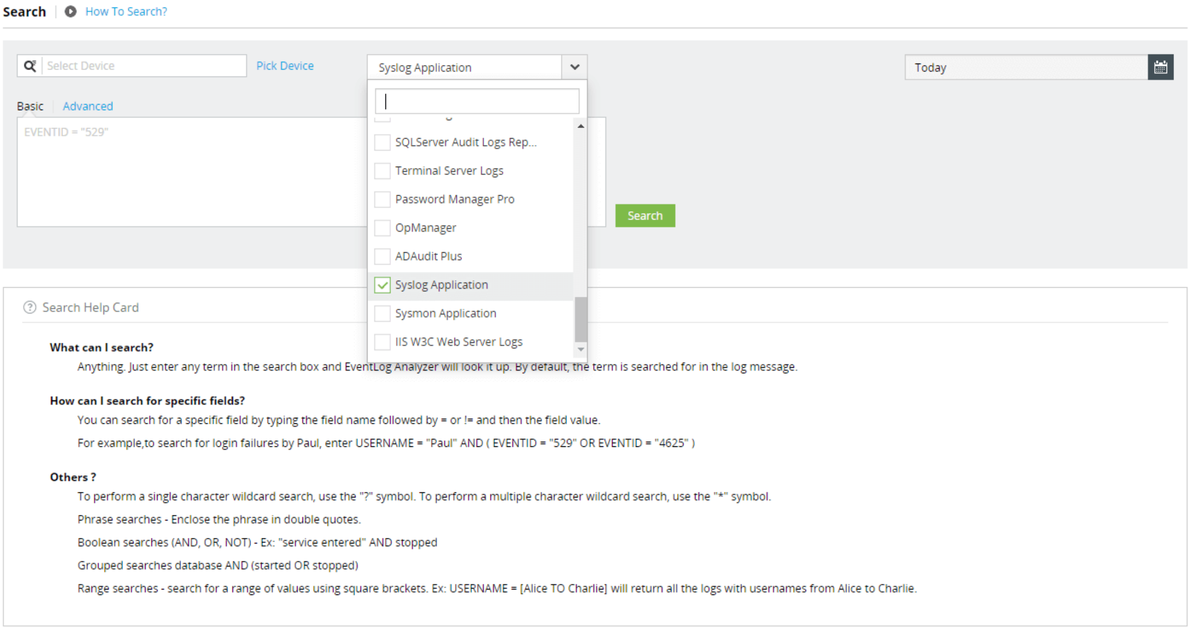
* Device: WinDevice-4313

☑ Use Default Credentials

Note: If your application source is not listed here,Please try Import log.

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.



EVENTID = "529"

☑ Syslog Application

What can I search?

Anything. Just enter any term in the search box and EventLog Analyzer will look it up. By default, the term is searched for in the log message.

How can I search for specific fields?

You can search for a specific field by typing the field name followed by = or != and then the field value.

For example,to search for login failures by Paul, enter USERNAME = "Paul" AND (EVENTID = "529" OR EVENTID = "4625")

Others ?

To perform a single character wildcard search, use the "?" symbol. To perform a multiple character wildcard search, use the "*" symbol.

Phrase searches - Enclose the phrase in double quotes.

Boolean searches (AND, OR, NOT) - Ex: "service entered" AND stopped

Grouped searches database AND (started OR stopped)

Range searches - search for a range of values using square brackets. Ex: USERNAME = [Alice TO Charlie] will return all the logs with usernames from Alice to Charlie.

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

1.8. Adding ManageEngine Applications

Last updated on: September 12, 2025

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

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

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

Steps to configure ManageEngine applications

Import Configuration

Configuring ManageEngine EventLog Analyzer to import ManageEngine Products' Logs.

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

ⓘ Note

Only access logs and debug logs are imported in import configuration
The supported products are:

- ADAudit Plus
- ADSelfServicePlus
- ADManager Plus
- OpManager
- OpManager Plus
- OpManager MSP
- Firewall Analyzer
- Netflow Analyzer
- Network Configuration Manager
- ServiceDesk Plus

Syslog Configuration

Configuring ManageEngine ADAudit Plus

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

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

Logs types description:

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

Configuring ManageEngine ADManager Plus

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

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

Logs types description:

- Access Logs: ADManager plus web server access logs.

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

Configuring ManageEngine ADSelfServicePlus

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

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

Logs types description:

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

Configuring ManageEngine ITOM solution products

Access logs and Debug logs Configuration for ITOM solution products

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

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

Alarms Configuration for ITOM Solution products

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

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

   Profile Type

Select Syslog Profile and enter the following details.

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

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

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

Other important message variables

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

4. Click Next.

Criteria

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

Device Selection

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

Schedule

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

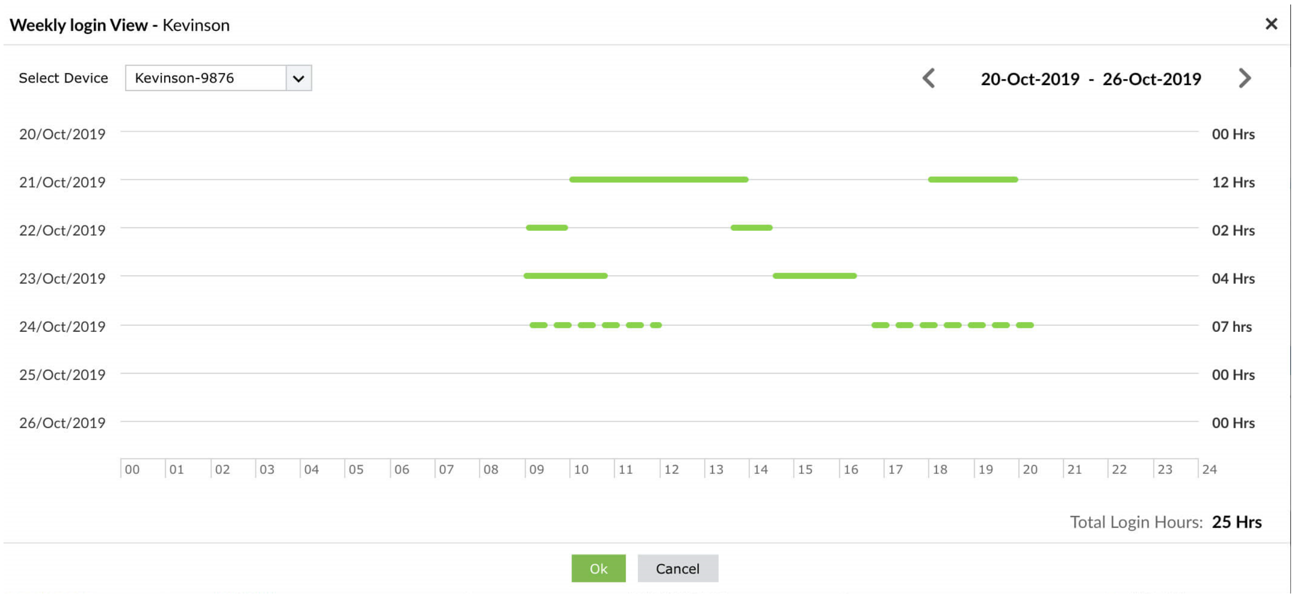
Preview

- Enter a profile name and click Save.

ⓘ Note

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

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



Weekly login View - Kevinson

Select Device: Kevinson-9876

20-Oct-2019 - 26-Oct-2019

20/Oct/2019 00 Hrs
21/Oct/2019 12 Hrs
22/Oct/2019 02 Hrs
23/Oct/2019 04 Hrs
24/Oct/2019 07 hrs
25/Oct/2019 00 Hrs
26/Oct/2019 00 Hrs

Total Login Hours: **25 Hrs**

ⓘ Note

The following products from ManageEngine ITOM Solution Support Alarms Configuration:

- OpManager
- OpManager Plus
- OpManager MSP

Configuring ManageEngine Password Manager Pro

Here are the steps to configure Password Manager Pro.

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

HTTPs Action Log Collection Configuration

Configuring ManageEngine Endpoint Central

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

ⓘ Note

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

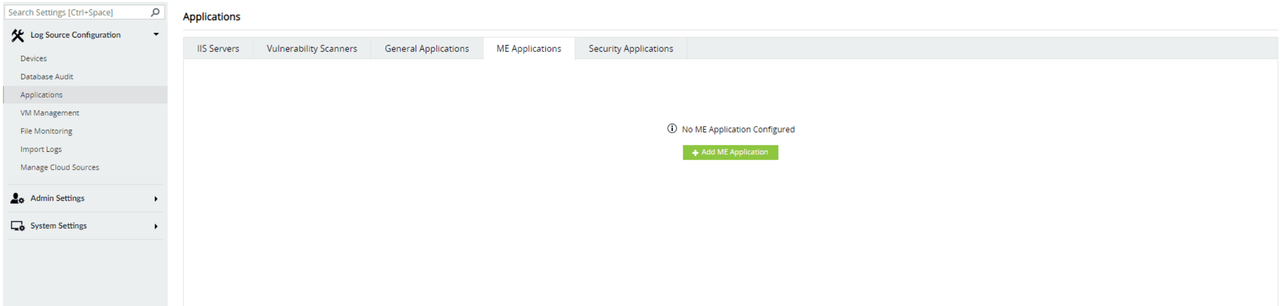
Data Enrichment Configuration for ManageEngine Endpoint Central and Vulnerability Manager Plus

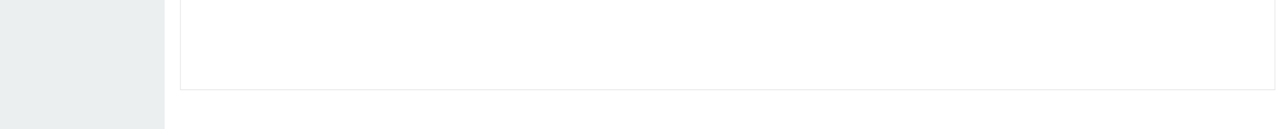
By combining security data points from ManageEngine Endpoint Central or Vulnerability Manager Plus and advanced threat detection in Log360, you can quickly and effectively investigate and respond to security incidents.

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

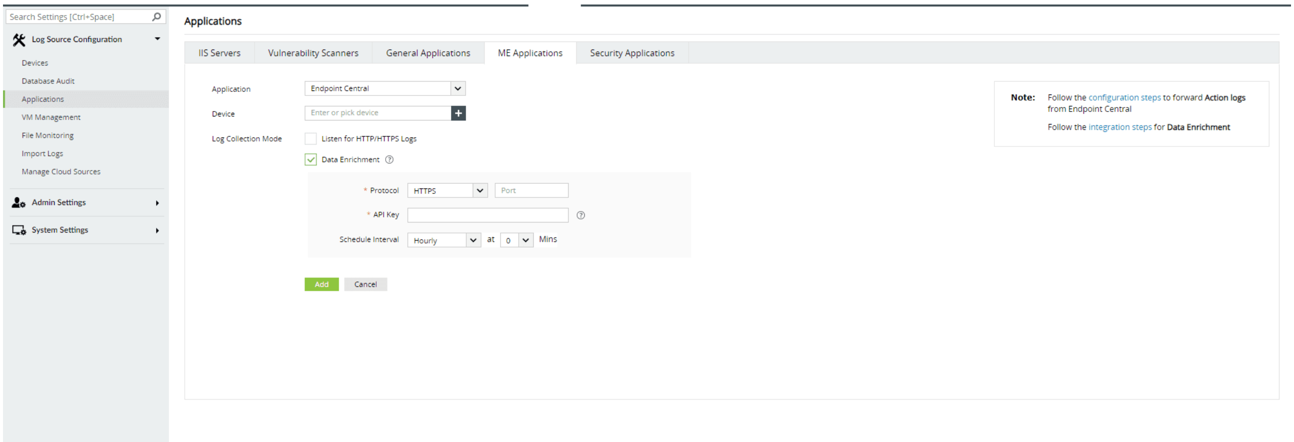
To configure,

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





- Click the Add ME Application button.



Application: Endpoint Central

Device: Enter or pick device

Log Collection Mode: □ Listen for HTTP/HTTPS Logs

☑ Data Enrichment

* Protocol: HTTPS | Port

* API Key:

Schedule Interval: Hourly at 0 Mins

Note: Follow the configuration steps to forward **Action logs** from Endpoint Central

Follow the integration steps for **Data Enrichment**

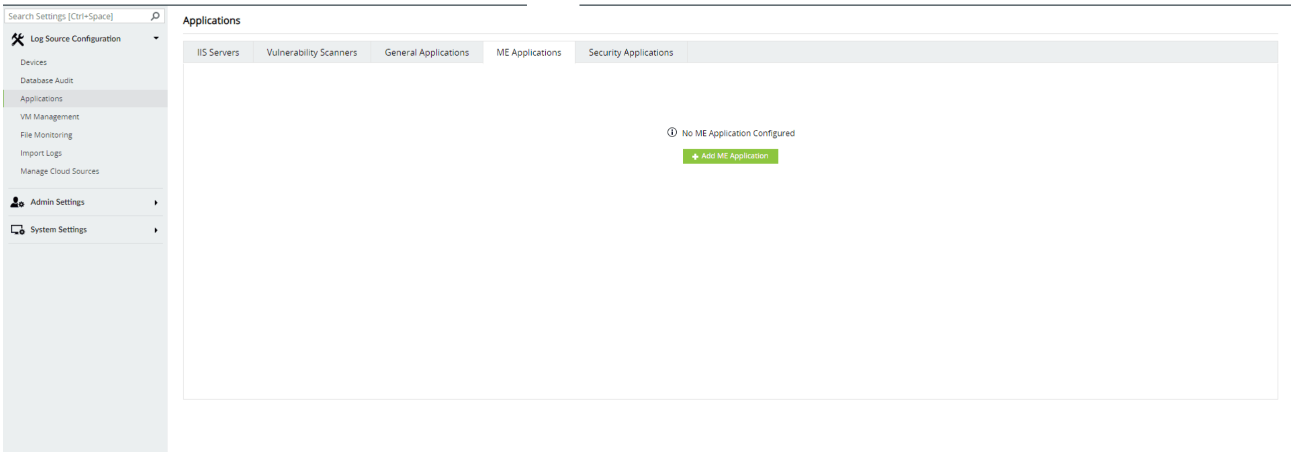
- Select Endpoint Central from the Application drop-down box.
- Enter or pick a device from the Device list. (Note: The device on which the Endpoint Central server runs.)
- Check the Data Enrichment box.
- Configure the following in the Data Enrichment component.
  - Protocol: Select the desired protocol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

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

Configuring ManageEngine Endpoint Central Cloud Version

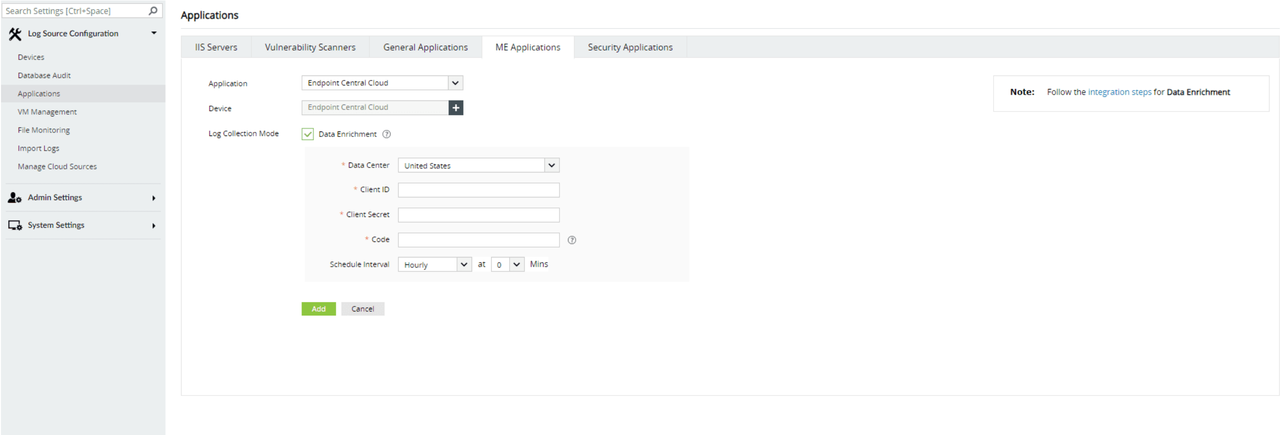
To configure,

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



ⓘ No ME Application Configured

- Click the Add ME Application button.



Application: Endpoint Central Cloud

Device: Endpoint Central Cloud

Log Collection Mode: ☑ Data Enrichment

* Data Center: United States

* Client ID

* Client Secret

* Code

Schedule Interval: Hourly at 0 Mins

Note: Follow the integration steps for Data Enrichment

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

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

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

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

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

Configuring ManageEngine ServiceDesk Plus

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

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

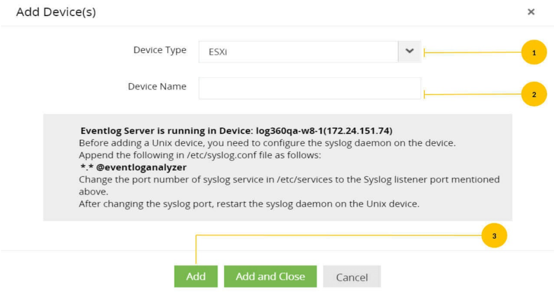
Logs types description:

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

1.9.1. Adding Other Devices

Last updated on: September 12, 2025

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



Device Type: ESXi

Device Name:

Eventlog Server is running in Device: log360qa-w8-1(172.24.151.74)
Before adding a Unix device, you need to configure the syslog daemon on the device.
Append the following in /etc/syslog.conf file as follows:
***.* @eventloganalyzer**
Change the port number of syslog service in /etc/services to the Syslog listener port mentioned above.
After changing the syslog port, restart the syslog daemon on the Unix device.

1. Select the Device Type as ESXi/IBM AS/400.

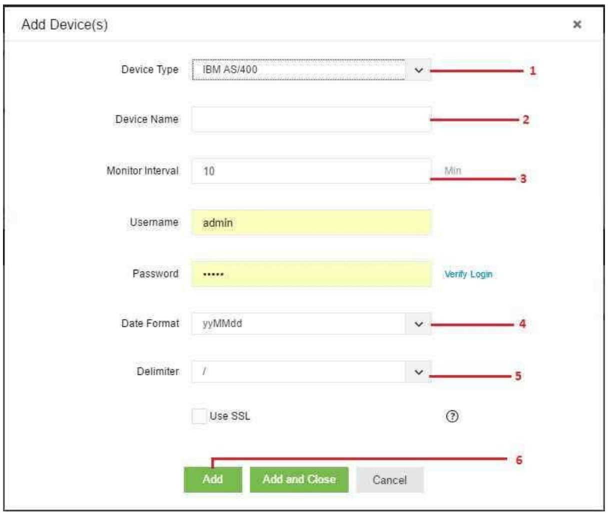
2. Enter the Device Name.

3. Click on the Add button to add the device for monitoring.

1.9.2. Adding IBM iSeries (AS/400) devices

Last updated on: September 12, 2025

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



Add Device(s)

Device Type: IBM AS/400

Device Name:

Monitor Interval: 10 Min

Username: admin

Password: •••••

Date Format: yyMMdd

Delimiter: /

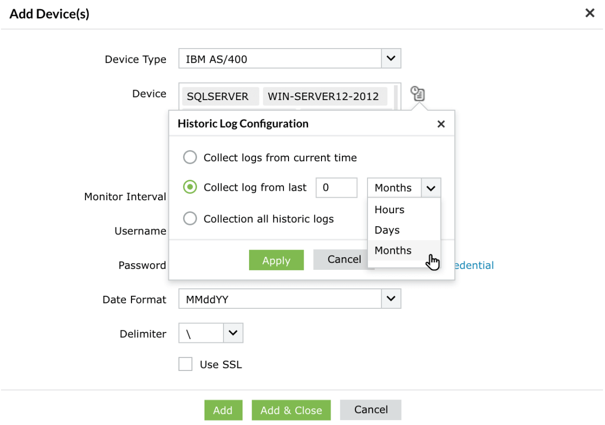
□ Use SSL

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

To import SSL certificate, follow the steps below:

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

IBM AS/400


Add Device(s)

Device Type: IBM AS/400

Device: SQLSERVER WIN-SERVER12-2012

Historic Log Configuration

○ Collect logs from current time

● Collect log from last 0 Months

○ Collection all historic logs

Date Format: MMddYY

Delimiter: \

□ Use SSL

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.

> authority.

Create a journal receiver

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

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

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

Attach the journal receiver to a journal

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

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

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

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

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

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

Once this security auditing set up is completed, EventLog Analyzer will automatically fetch the logs collected in the journal receiver of the AS400/iSeries device that is added for monitoring. If the AS400/iSeries machine is not added to EventLog Analyzer server, add the device to begin collecting its logs.

1.9.3. File Integrity Monitoring (FIM)

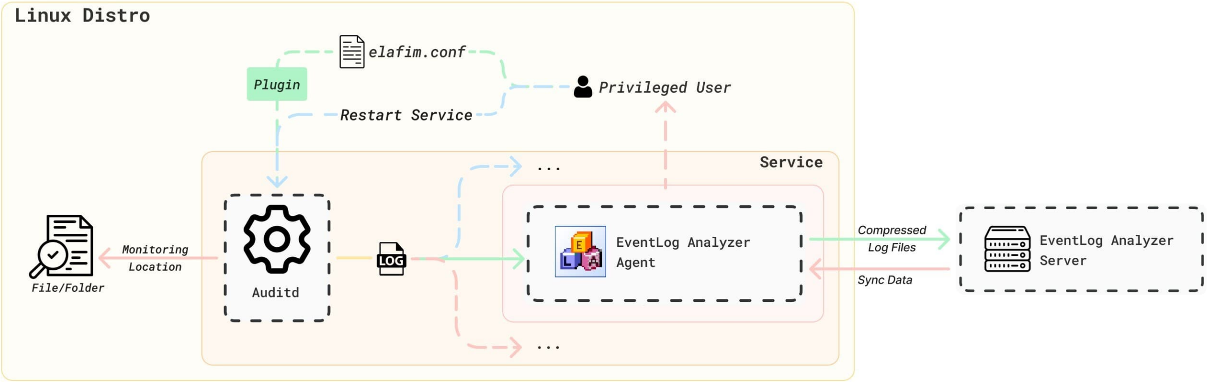
Last updated on: September 12, 2025

File Integrity Monitoring is a feature that helps you monitor all changes (addition/deletion/modification) made to files and folders in Windows and Linux systems.

Important Note

1. It is recommended that FIM be implemented for strictly necessary files and folders so as to avoid disk space issues that may rise due to the high volume of generated logs.
2. In Windows FIM module,
   - If a Windows file server is configured for FIM, both Windows Server and file server licenses are required.
   - If a Windows server is configured for FIM, only a Windows Server license is required.
   - If a Windows workstation is configured for FIM, only a Windows workstation license is required.

Linux FIM Agent Architecture:



To install packages, please find the syntax here.

Prerequisites for File Integrity Monitoring

Windows:

- When you enable File Integrity Monitoring for Windows, certain access policies will be automatically enabled on the file server. If there are overriding GPOs for audit policy in your domain, follow the below procedure to manually enable them

  - In administrator command prompt enter the command, auditpol/get/category:"Object Access"
  - Then proceed to enable the following access policies
    - Audit file share
    - Audit file system
    - Audit handle manipulation
    - Audit detailed file share
    - Audit other object access events.
- SACLs should be enabled for the monitored file/folders. These are automatically enabled by the product. If not, manually update SACLs with the following permissions
  - Execute files/ traverse folder
  - Write data/create files
  - Append data/create folders
  - Write attributes
  - Write extended attributes
  - Delete subfolders and files
  - Delete read permissions
  - Change permissions
  - Take ownership

Linux:

- The following packages should be installed on the agent machine
  - openssh-server [For UI related operations]
  - auditd
  - acl
- Ensure that,
  - SSH Port (default port 22) is reachable from the server.
  - ELA Server Port (default port 8095) is reachable from the agent machine.

  To verify if a port is reachable, you can use the below commands:
  Example: echo > /dev/tcp/ubuntu/8095 && echo "Port is Reachable"
  (or)
  Example: telnet ubuntu 8095
- Also ensure that the:
  - Linux kernel version is 2.6.25 or higher
  - Linux audit framework version is higher than 1.8
- Remove the following rules from /etc/audit/audit.rules file if they are enabled and then reboot the machine.

  - Syscall block rule, "-a never,task", and
  - Immutable rule, "-e 2".
- If you are enabling auditing for SUSE machines, set the following rule:
  - Navigate to /etc/sysconfig/auditd
  - Set AUDITD_DISABLE_CONTEXTS = no
- If Security-Enhanced Linux (SELinux) exists, then it must either be in the permissive mode or disabled:
  - Check SELinux status using the command: getenforce.
  - If the status is 'Enforced', navigate to file/etc/selinux/config and make this edit: SELINUX = permissive.
  - Restart the machine.

> ⓘ Note
>
> The server utilizes the agent credential only for the actions mentioned in the document.
> Configuring FIM for Linux audits the following actions on Linux files:
>
> - Read
> - Write
> - Execute
> - Attribute change

Since auditd requires root or sudo privileges, if the user does not have the privileges, please follow the privileges steps.

Privileges for Installing FIM Agent:

1. Adding AgentManager to the Sudoers file.
2. Create a directory and assign privileges to it.

1. Adding AgentManager to the Sudoers file:
To run AgentManager with sudo privileges for the Non-Sudo User, please follow the below instructions:

- Use the root user for configuring the privileges.
- Please execute the below command:
- Add the below line to the sudoers file:
  Example:
  - visudo -f /etc/sudoers.d/testuser
  - testuser ALL=NOPASSWD: /opt/ManageEngine/EventLogAnalyzer_Agent/bin/AgentManager *

> ⓘ Note

Ensure that AgentManager is added to the sudoers file prior to installation. To verify, follow the below command.

cat /etc/sudoers.d/<username>

Example: cat /etc/sudoers.d/testuser

Expected Output: testuser ALL=NOPASSWD: /opt/ManageEngine/EventLogAnalyzer_Agent/bin/AgentManager *

Reason for adding AgentManager in the Sudoers file:

The following actions require sudo privileges:

- Transfer the ownership of the Agent Directory and elafim.conf file [Under audit [or] audisp directory], to the root user.
- Restarting auditd service may also require root privileges.

2. Create a directory and assign privileges to it

To prevent unauthorized access to directories other than ManageEngine, follow the below commands as the root user for the non-sudo user.

Create a directory:

Granting privileges to the directory:

For CentOS/RHEL v8 and later/Ubuntu/openSUSE/Debian/Fedora:

For CentOS/RHEL v6 to v7.9:

Granting privilege to the audit.rules:

Example: setfacl -m u:testuser:rwx /opt/ManageEngine/

Configuring File Integrity Monitoring

To configure File Integrity Monitoring, go to

- Navigate to Settings > Configurations > Manage File Integrity Monitoring.
- Depending on which device the files and folders that you wish to monitor are located in, click on either the Windows or Linux tab.
- Click Add FIM.
- Pick the device in which the files/folders are located, enter correct credentials, browse and select the files and folders you wish to monitor. Alternatively, you can enter the location of the files/folders.

> ⓘ Note
>
> For Linux devices, in addition to entering the details mentioned above, you will also be prompted to enter the SSH port number.

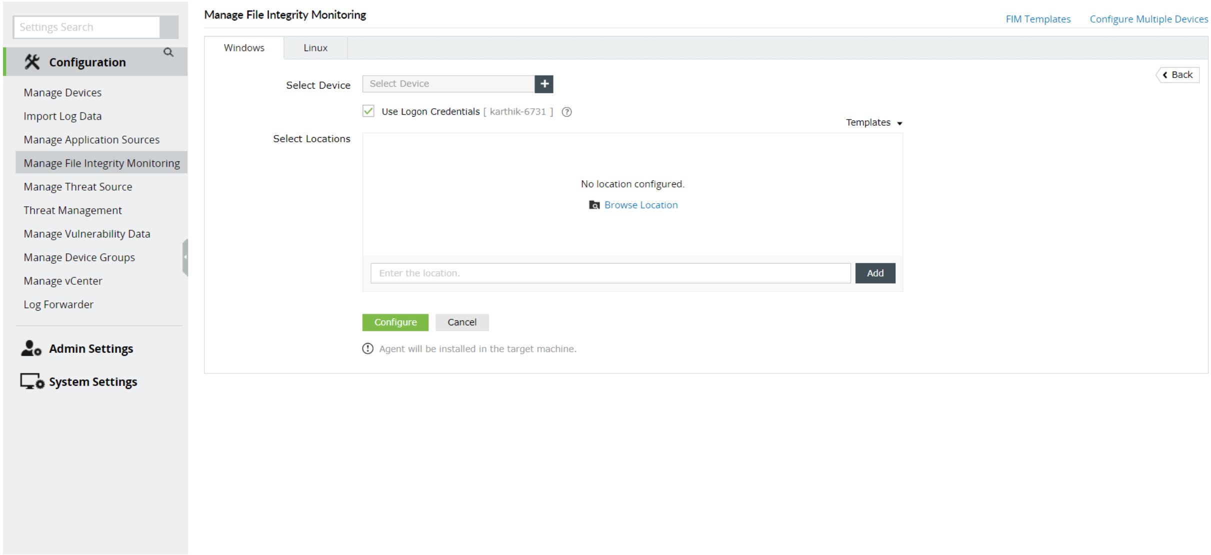
- The Exclude Filter gives you an option to exclude

  - Certain file types.
  - Certain sub-locations within the main location.
  - All sub-locations within the main location.

- If you want to know who has made the change to the file or folder, check the Audit Username checkbox.

> Note
>
> For Linux devices, username is audited by default.

- Click Configure.



Manage File Integrity Monitoring

Select Device: Select Device

☑ Use Logon Credentials [karthik-6731]

Select Locations: No location configured.

Enter the location.

Agent will be installed in the target machine.

Configuring Bulk File Integrity Monitoring

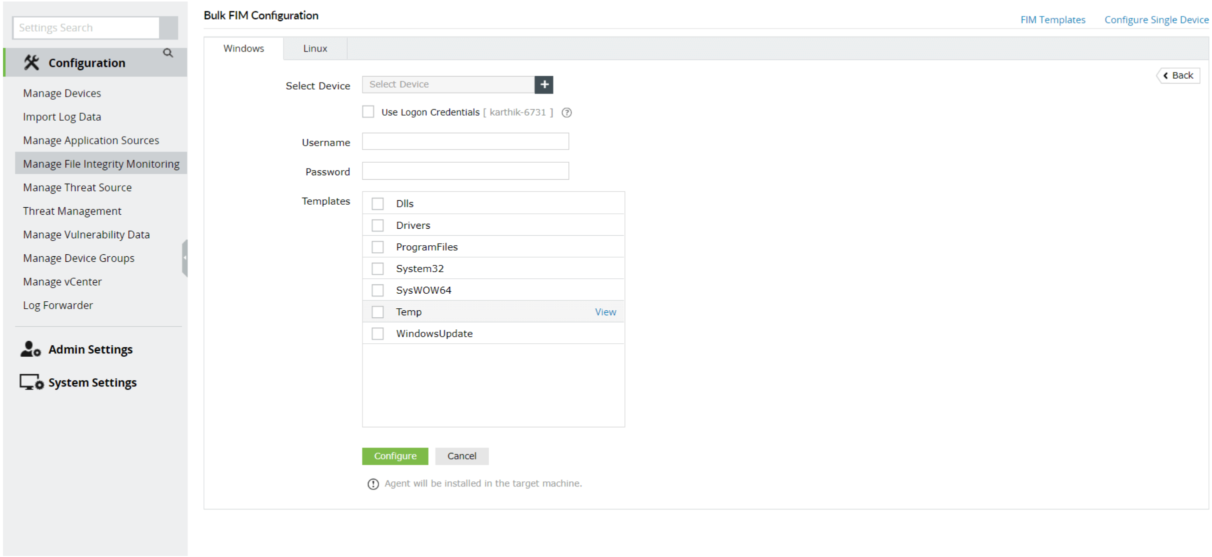
If the same files and folders located in multiple devices need to be added for monitoring, then the Bulk File Integrity Monitoring feature can be used.

- Navigate to Settings > Configurations > Manage File Integrity Monitoring.
- Depending on which device the files and folders that you wish to monitor are located in, click on either the Windows or Linux tab.
- Click Add FIM. Select Configure multiple devices on the top right corner.
- Pick the device in which the files/folders are located, enter correct credentials, and select the file template(s).

> Note
>
> For Linux devices, in addition to entering the details mentioned above, you will also be prompted to enter the SSH port number.

- Click Configure

- Click Configure.



Bulk FIM Configuration

FIM Templates | Configure Single Device

Windows | Linux

Back

Select Device: Select Device +

□ Use Logon Credentials [karthik-6731]

Username:

Password:

Templates:

- □ Dlls
- □ Drivers
- □ ProgramFiles
- □ System32
- □ SysWOW64
- □ Temp View
- □ WindowsUpdate

Configure | Cancel

Agent will be installed in the target machine.

Notes

- If an agent is already installed in the device whose files you want to monitor, file monitoring will automatically be enabled in the agent.
- If no agent is installed in the device for which you want to monitor the files, then an agent will be installed and file monitoring will be enabled in the agent.
- Please note that the volume of logs generated for each change occurring on the folders can affect the performance of the file server. It is a recommended practice to limit file/folder monitoring to the required files/folders.

Manage File Integrity Monitoring (FIM) Templates

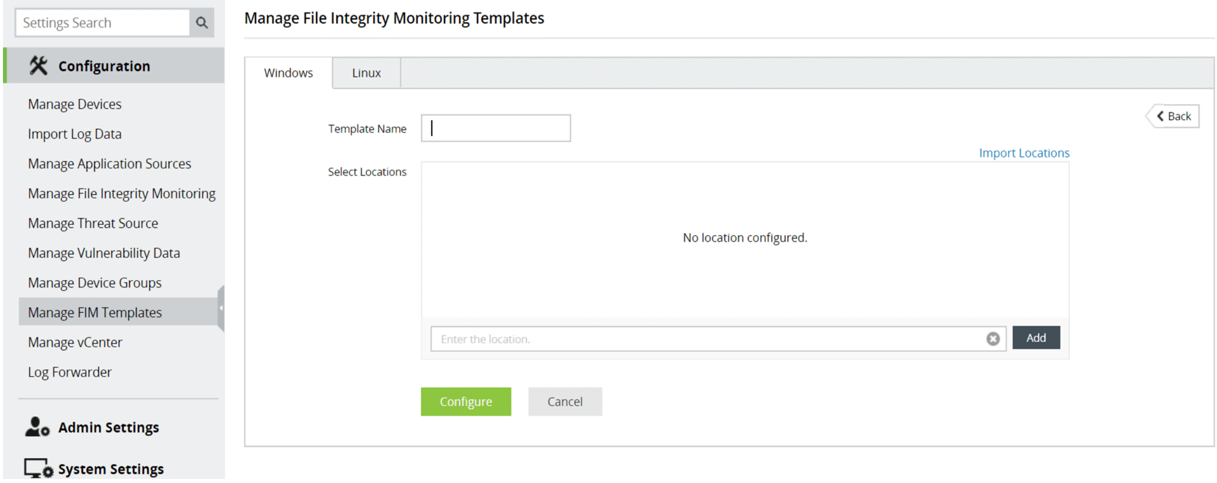
If the same file or folder needs to be monitored in a number of devices, then a template can be created and assigned to these devices. To create a FIM template follow the steps below:

- Navigate to Settings > Configurations > Manage File Integrity Monitoring > FIM Templates.
- Depending on which device the files and folders that you wish to monitor are located in, click on either the Windows or Linux tab.
- Click Add FIM.
- Enter a name for the template and select the locations of the files and folders.

  Alternatively, you can enter the location of the files/folders.
- The Exclude Filter gives you an option to exclude
  - Certain file types.
  - Certain sub-locations within the main location.
  - All sub-locations within the main location

- All sub locations within the main location.

- If you want to know who has made the change to the file or folder, check the Audit Username checkbox.
- Click Configure.



Manage File Integrity Monitoring Templates

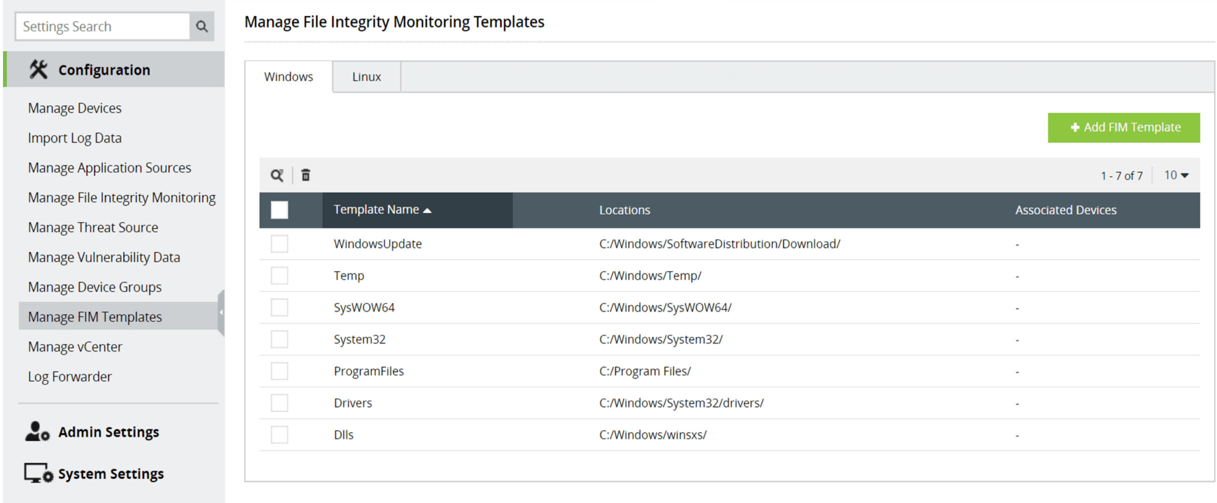
Template Name

Select Locations

No location configured.

Enter the location.

All the created templates are listed in a tabular column with an option to edit / delete them.



Manage File Integrity Monitoring Templates

□	Template Name ▲	Locations	Associated Devices
□	WindowsUpdate	C:/Windows/SoftwareDistribution/Download/	-
□	Temp	C:/Windows/Temp/	-
□	SysWOW64	C:/Windows/SysWOW64/	-
□	System32	C:/Windows/System32/	-
□	ProgramFiles	C:/Program Files/	-
□	Drivers	C:/Windows/System32/drivers/	-
□	Dlls	C:/Windows/winsxs/	-

Import Logs

1.10.1. Import Log Files

Last updated on: September 12, 2025

EventLog Analyzer helps you collect and analyze logs from different sources such as servers, network devices, and applications. The solution provides actionable intelligence that helps security teams stay on top of security threats in the organization.

This solution provides you the capability to import log files. The supported log formats include Windows and syslog device formats, application log formats and archived files log formats.

Windows and syslog device log formats

- Windows Eventlog (EVTX format)
- IBM AS/400
- Linux/Unix Syslog format (RFC 5424 and 2131)

> Note
>
> To import .evt logs (Windows XP and Windows 2003), you will need to convert the .evt to .evtx using the command wevtutil export-log application.evt application.evtx /lf in your EventLog Analyzer installation.

Application log formats

- Apache access logs
- DHCP Linux logs
- DHCP Windows logs
- IBM Maximo logs
- IIS W3C FTP logs
- IIS W3C Web Server logs
- MSSQL Server logs
- MySQL logs
- PostgreSQL Logs
- ADAudit Plus logs
- ADManager Plus logs
- ADSelfService Plus logs
- ITOM solution logs

- ServiceDesk Plus Logs

Archived files log formats

- Cisco archive files
- Syslog archive files
- Windows archive files

Steps to import log files

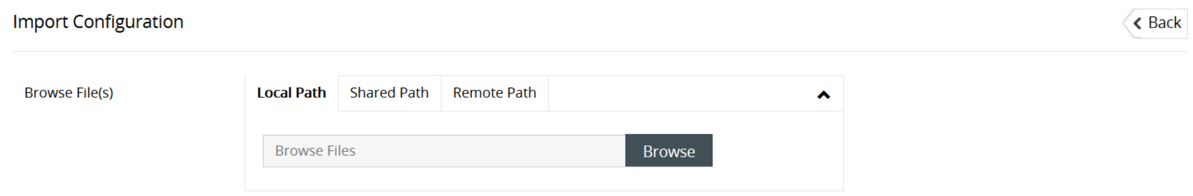
Navigate to the Import Configuration page using any one of the following menu options:

- +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

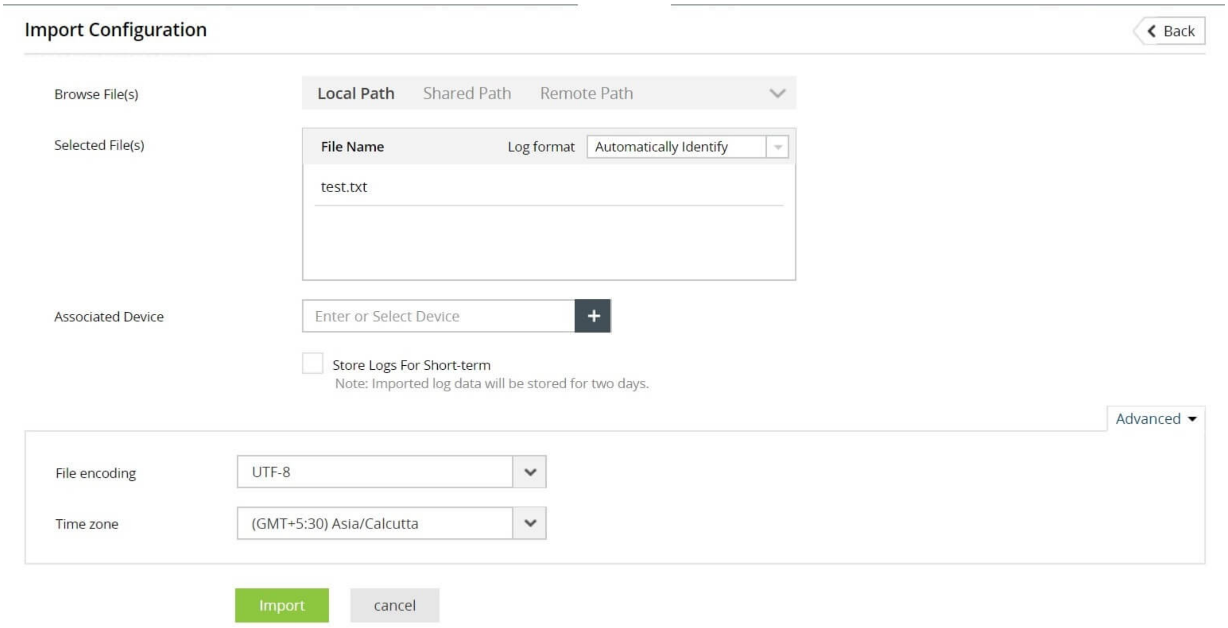
Log import cannot be scheduled to run at regular time intervals

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.



Import Configuration

Browse File(s): Local Path | Shared Path | Remote Path

Selected File(s): File Name — test.txt; Log format: Automatically Identify

Associated Device: Enter or Select Device

□ Store Logs For Short-term
Note: Imported log data will be stored for two days.

File encoding: UTF-8

Time zone: (GMT+5:30) Asia/Calcutta

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.

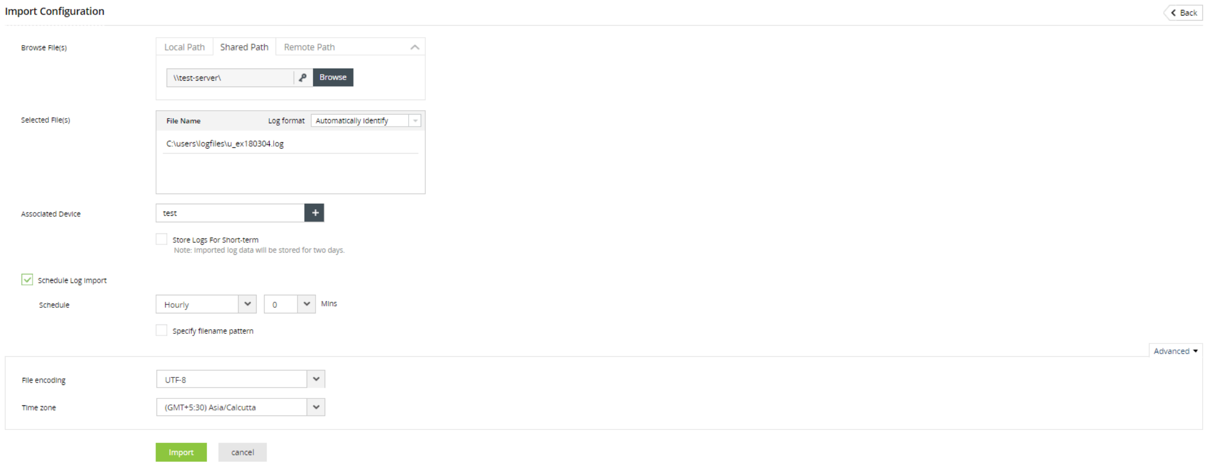
6. If you wish to store the imported logs for 2 days, enable the Store logs for a short term option. By default, the log storage time-period is 32 days.

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.



Browse File(s): Shared Path \\test-server\

Selected File(s): File Name C:\users\logfiles\u_ex180304.log — Log format: Automatically Identify

Associated Device: test

□ Store Logs For Short-term
Note: Imported log data will be stored for two days.

☑ Schedule Log Import

Schedule: Hourly 0 Mins

□ Specify filename pattern

File encoding: UTF-8

Time zone: (GMT+5:30) Asia/Calcutta

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)

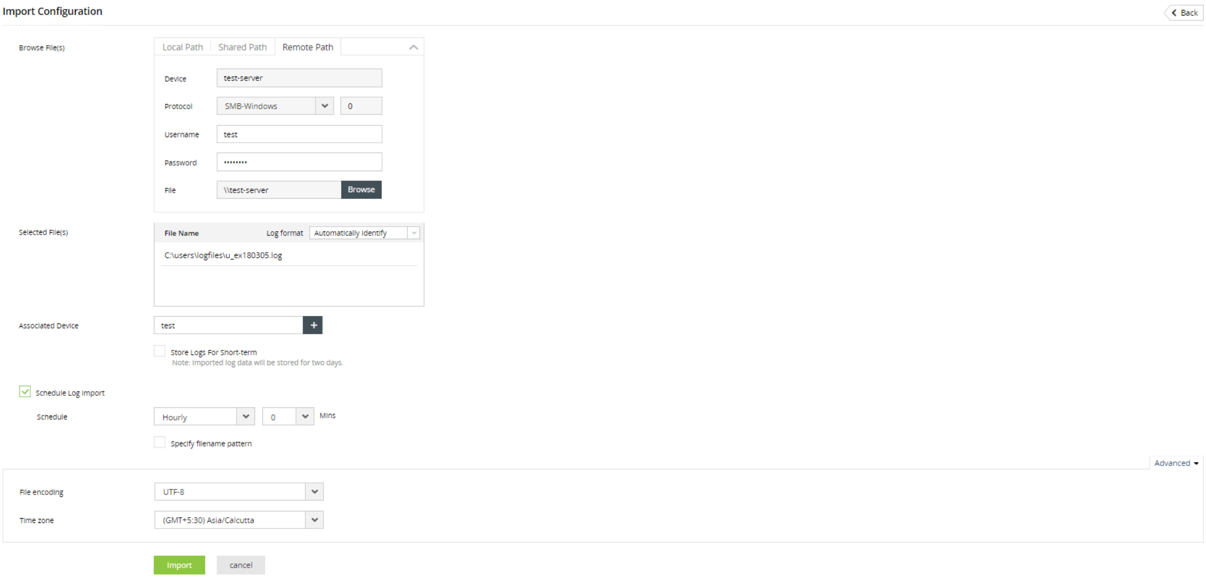
Authentication type: Password

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



Import Configuration

Browse File(s): Local Path | Shared Path | Remote Path

Device: test-server

Protocol: SMB-Windows | 0

Username: test

Password: ••••••••

File: \\test-server | Browse

Selected File(s): File Name | Log format: Automatically Identify

C:\users\logfiles\u_ex180305.log

Associated Device: test | +

□ Store Logs For Short-term
Note: Imported log data will be stored for two days.

☑ Schedule Log Import

Schedule: Hourly | 0 | Mins

□ Specify filename pattern

File encoding: UTF-8

Time zone: (GMT+5:30) Asia/Calcutta

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.

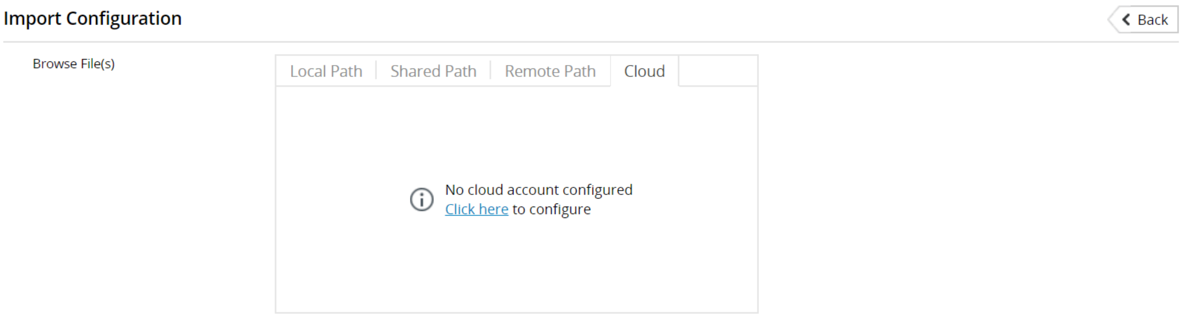
8. The Store Logs for Short-term option will store the imported log data in EventLog Analyzer for a brief period of two days. If the option is left unchecked, the logs will be stored as per your database retention configuration.
9. If you would like to automate a log file import at regular time intervals, 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.

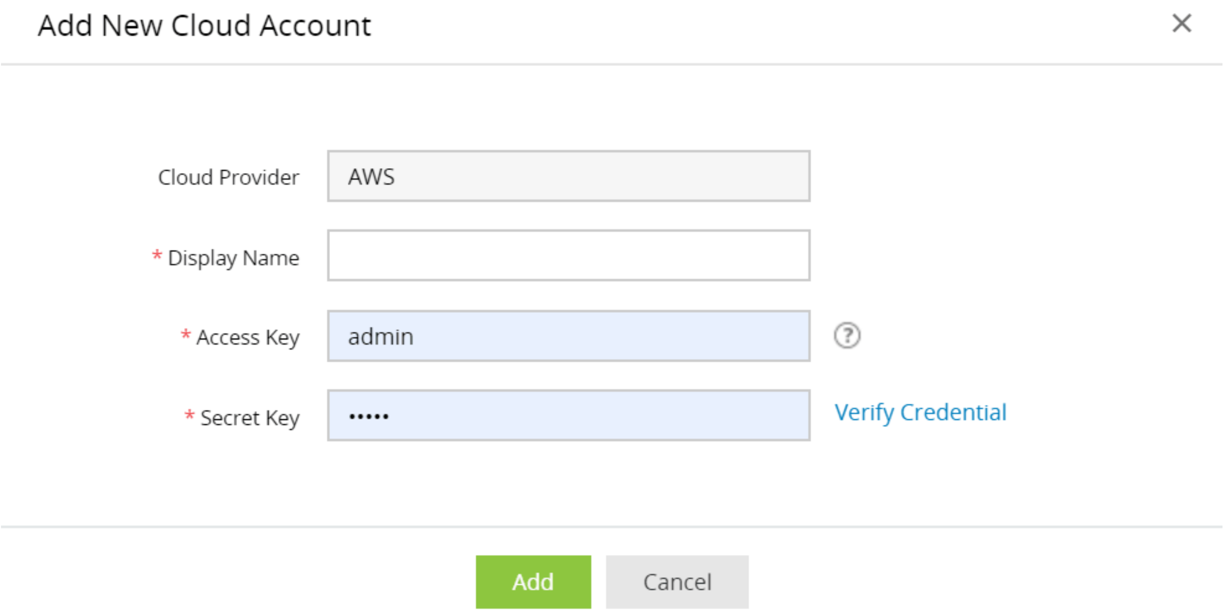


Import Configuration

Browse File(s)

No cloud account configured
Click here to configure

- Enter the Display Name, Access Key, and Secret Key of the AWS account and click Add.



Add New Cloud Account

Cloud Provider: AWS

* Display Name:

* Access Key: admin

* Secret Key: •••••

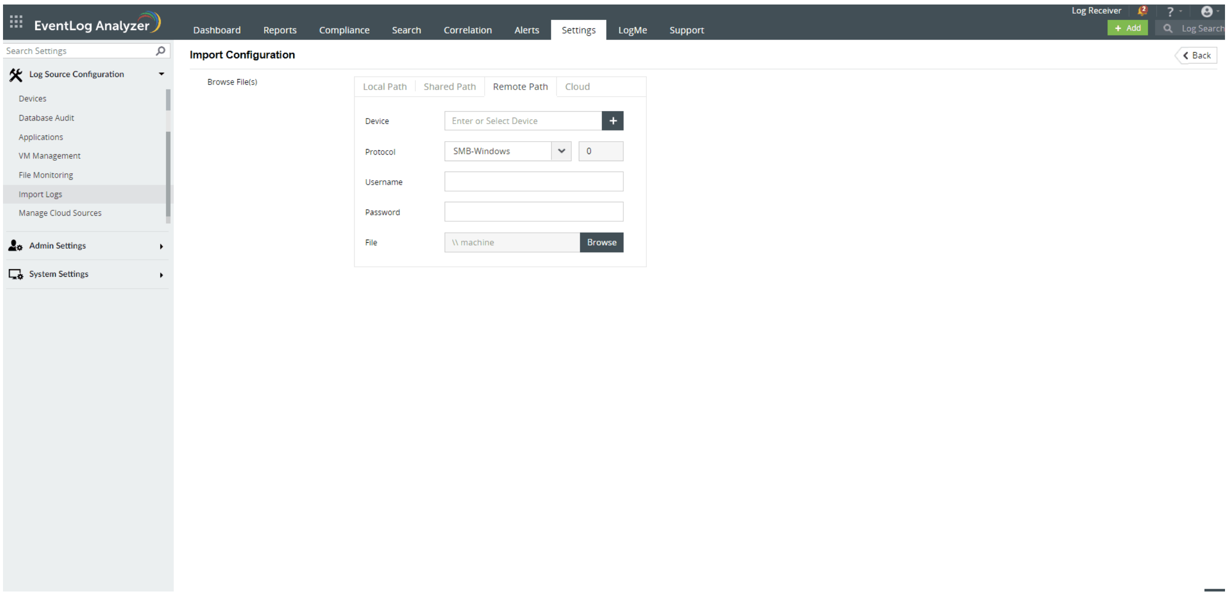
- Once the AWS account gets added, it will be displayed in the drop-down list available in the Cloud tab.

- 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.



Import Configuration

Browse File(s)

Device: Enter or Select Device

Protocol: SMB-Windows 0

Username

Password

File: \\ machine

MySQL Logs

EventLog Analyzer supports only error logs and general logs from MySQL. MySQL logon failures are taken into account from MySQL general query logs.
To enable logging in MySQL,

- Open the my.cnf file (in case of Linux) or my.ini file (in case of Windows) and add the below entries to the file.
- For error logs: log_error=<error-log-file-name>
- For general logs:
  - >= v5.1.29:
    general_log_file=<general-log-file-name>
    general_log=1 (or) ON
  - < v5.1.29:
    log=<log-file-name>
- Restart the MySQL instance for the changes to take effect.

To import MySQL logs in EventLog Analyzer,

- You can import MySQL log files from a local path, a shared path , or a remote path.
- To import MySQL log files, you need to manually choose the log format. Once you've selected the right file, select MySQL Logs from the Log Format drop-down list in the Selected File(s) section.
- Click Import to initiate the log importing process.

PostgreSQL Logs

Log format of PostgreSQL logs is determined by log_line_prefix parameter, set in postgresql.conf file.
The default format of PostgreSQL logs is '%m [%p] ' which logs a time stamp and the process ID.
This format is supported by default in EventLog Analyzer.

Importing additional fields in EventLog Analyzer

If the user wants to add additional fields, log_line_prefix parameter in the postgresql.conf file must be changed. The log_line_prefix parameter must follow the format(key- value pair) given below in the postgresql.conf file.

log_line_prefix format:

log_line_prefix = 'time_stamp=%m or %t process_id=%p application_name=%a database_name=%d connection_from_with_port=%r connection_from=%h session_id=%c transaction_id=%x user_name=%u command_tag=%i sql_state_code=%e session_start_time=%s '

log_line_prefix Parameter	Key	Value
Time stamp with milliseconds or time stamp without milliseconds	time_stamp	%m or %t
Process ID	process_id	%p
Application name	application_name	%a

Parameter	Key	Value
log_line_prefix		
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

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:

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

- Run the following command:

> ⓘ Note
>
> Replace the given parameters with the parameters of your choice.

- Run the following command:

Now the logs will be generated for the DB2 instance in the given data path.

2. Creating an audit policy for database auditing

- Open DB2 Command Line Processor with administrator privilege.
- Run the following command to connect to a database:

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

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

> Note Replace policy_name with the policy name of your choice. Replace the given parameters with the command parameters of your choice. To know more on the allowed command parameters, refer

> source.

- Run the following command to commit:

Now the audit policy has been created.

3. Assigning the audit policy to the database

- Open DB2 Command Line Processor with administrator privilege.
- Run the following command to assign a policy to the database:

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

- Run the following command to commit:

Now the created audit policy is assigned to the database.

4. Archiving the active logs

You can archive the active logs from both instance and database. The logs will be archived to the archive path that you configured in the first step.

- Open DB2 Command Line Processor with administrator privilege.
- Run the following command to archive the active database logs:

> Note Replace your_database with the name of the database.

- Run the following command to archive active instance logs:

Now the logs will be archived to a new file with a timestamp appended to the filename. An example of the filename is given below.

- Instance Log file: db2audit.instance.log.0.20060418235612
- Database Log file: db2audit.db.your_database.log.0.20060418235612

Both files have to be extracted into a human-readable format to be imported into EventLog Analyzer.

5. Extracting the archived logs

- Open DB2 Command Line Processor with administrator privilege.
- Run the following command to extract the archived instance logs:

> Note Replace the instancelog with the filename of your choice. Replace
> db2audit.instance.log.0.20060418235612 with the filename of the archived instance log

> db2audit.instance.log.0.20060418235612 with the filename of the archived instance logs.

- Run the following command to extract archived database logs:

> Note Replace databaselog with the filename of your choice. Replace db2audit.db.your_database.log.0.20060418235612 with the filename of the archived database logs.

Both files will be extracted to the given archive path and can be imported into EventLog Analyzer.

6. Importing the logs to EventLog Analyzer

Now you will have to import the extracted database and instance log files into EventLog Analyzer. Here is a comprehensive guide on how to import log files in EventLog Analyzer.

Diagnostic Logs

EventLog Analyzer also provides a report for diagnostic logs. To generate the diagnostic logs report, follow the given steps.

- Run the following command to find the location of the diagnostic log file.

or or

> Note The path corresponding to Current member resolved DIAGPATH is the path to the diagnostic log file.

- Navigate to the specified path and import the file named db2diag.txt to EventLog Analyzer. Here is a comprehensive guide on how to import log files in EventLog Analyzer.

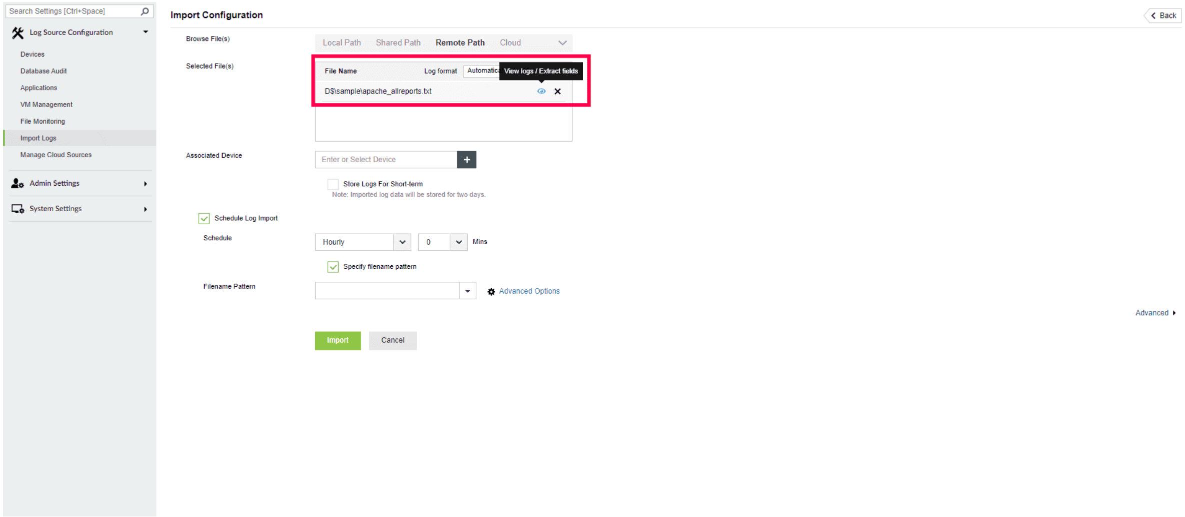
Import Troubleshooting tips

If you are unable to import a log file, ensure the following:

1. The credentials used are valid and have the necessary permissions.
2. The device is reachable.
3. The specified file exists and is accessible.
4. The log file format selected from the drop-down matches the log format of the chosen file.

Field extraction from logs

- Navigate to the Import Configuration page.
- Select the desired file(s) from a local, shared or remote path.
- Under Selected files, click on the eye beside the required file.



Browse File(s): Remote Path

Selected File(s): File Name D$\sample\apache_allreports.txt — Log format Automatic

☐ Store Logs For Short-term

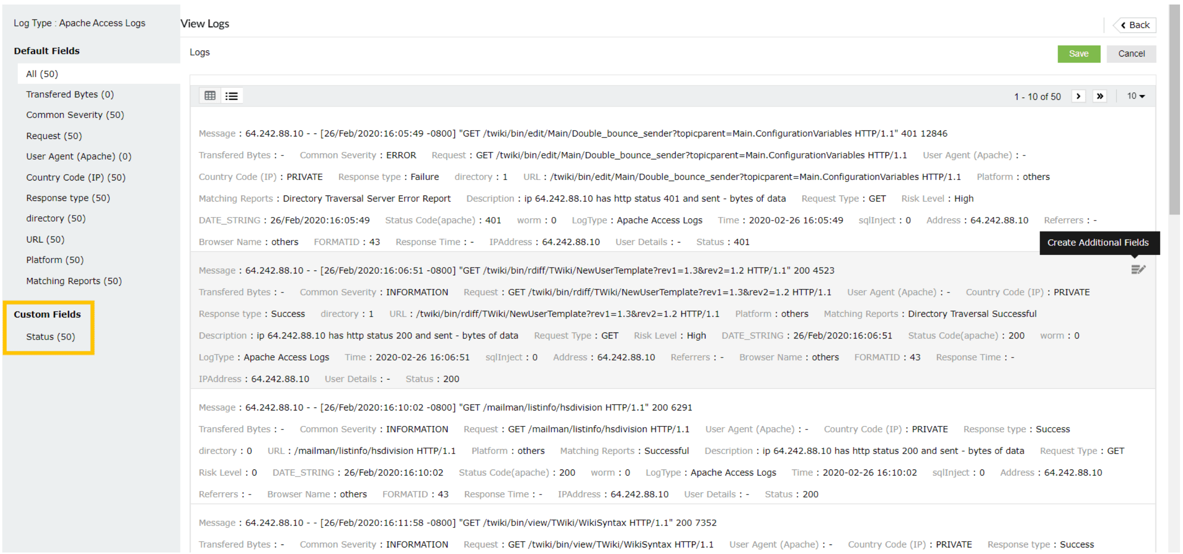
Note: Imported log data will be stored for two days.

☑ Schedule Log Import

Schedule: Hourly 0 Mins

☑ Specify filename pattern

- 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.

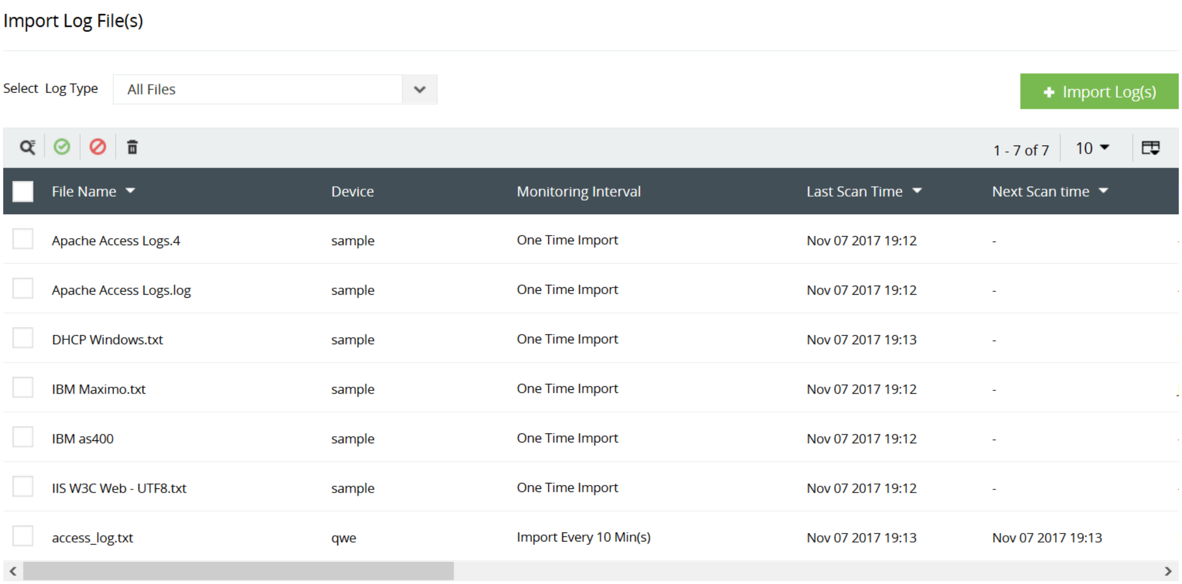


```
Message : 64.242.88.10 - - [26/Feb/2020:16:05:49 -0800] "GET /twiki/bin/edit/Main/Double_bounce_sender?topicparent=Main.ConfigurationVariables HTTP/1.1" 401 12846
Transfered Bytes : -   Common Severity : ERROR   Request : GET /twiki/bin/edit/Main/Double_bounce_sender?topicparent=Main.ConfigurationVariables HTTP/1.1   User Agent (Apache) : -
Country Code (IP) : PRIVATE   Response type : Failure   directory : 1   URL : /twiki/bin/edit/Main/Double_bounce_sender?topicparent=Main.ConfigurationVariables HTTP/1.1   Platform : others
Matching Reports : Directory Traversal Server Error Report   Description : ip 64.242.88.10 has http status 401 and sent - bytes of data   Request Type : GET   Risk Level : High
DATE_STRING : 26/Feb/2020:16:05:49   Status Code(apache) : 401   worm : 0   LogType : Apache Access Logs   Time : 2020-02-26 16:05:49   sqlInject : 0   Address : 64.242.88.10   Referrers : -
Browser Name : others   FORMATID : 43   Response Time : -   IPAddress : 64.242.88.10   User Details : -   Status : 401

Message : 64.242.88.10 - - [26/Feb/2020:16:06:51 -0800] "GET /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2 HTTP/1.1" 200 4523
Transfered Bytes : -   Common Severity : INFORMATION   Request : GET /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2 HTTP/1.1   User Agent (Apache) : -   Country Code (IP) : PRIVATE
Response type : Success   directory : 1   URL : /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.3&rev2=1.2 HTTP/1.1   Platform : others   Matching Reports : Directory Traversal Successful
Description : ip 64.242.88.10 has http status 200 and sent - bytes of data   Request Type : GET   Risk Level : High   DATE_STRING : 26/Feb/2020:16:06:51   Status Code(apache) : 200   worm : 0
LogType : Apache Access Logs   Time : 2020-02-26 16:06:51   sqlInject : 0   Address : 64.242.88.10   Referrers : -   Browser Name : others   FORMATID : 43   Response Time : -
IPAddress : 64.242.88.10   User Details : -   Status : 200

Message : 64.242.88.10 - - [26/Feb/2020:16:10:02 -0800] "GET /mailman/listinfo/hsdivision HTTP/1.1" 200 6291
Transfered Bytes : -   Common Severity : INFORMATION   Request : GET /mailman/listinfo/hsdivision HTTP/1.1   User Agent (Apache) : -   Country Code (IP) : PRIVATE   Response type : Success
directory : 0   URL : /mailman/listinfo/hsdivision HTTP/1.1   Platform : others   Matching Reports : Successful   Description : ip 64.242.88.10 has http status 200 and sent - bytes of data   Request Type : GET
Risk Level : 0   DATE_STRING : 26/Feb/2020:16:10:02   Status Code(apache) : 200   worm : 0   LogType : Apache Access Logs   Time : 2020-02-26 16:10:02   sqlInject : 0   Address : 64.242.88.10
Referrers : -   Browser Name : others   FORMATID : 43   Response Time : -   IPAddress : 64.242.88.10   User Details : -   Status : 200

Message : 64.242.88.10 - - [26/Feb/2020:16:11:58 -0800] "GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200 7352
Transfered Bytes : -   Common Severity : INFORMATION   Request : GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1   User Agent (Apache) : -   Country Code (IP) : PRIVATE   Response type : Success
```

- 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.



Import Log File(s)

Select Log Type: All Files

✚ Import Log(s)

1 - 7 of 7 | 10 ▾

☐	File Name ▾	Device	Monitoring Interval	Last Scan Time ▾	Next Scan time ▾
☐	Apache Access Logs.4	sample	One Time Import	Nov 07 2017 19:12	-
☐	Apache Access Logs.log	sample	One Time Import	Nov 07 2017 19:12	-
☐	DHCP Windows.txt	sample	One Time Import	Nov 07 2017 19:13	-
☐	IBM Maximo.txt	sample	One Time Import	Nov 07 2017 19:12	-
☐	IBM as400	sample	One Time Import	Nov 07 2017 19:12	-
☐	IIS W3C Web - UTF8.txt	sample	One Time Import	Nov 07 2017 19:12	-
☐	access_log.txt	qwe	Import Every 10 Min(s)	Nov 07 2017 19:13	Nov 07 2017 19:13

Apache Overview Dashboard: Parsing Additional fields by modifying the log format

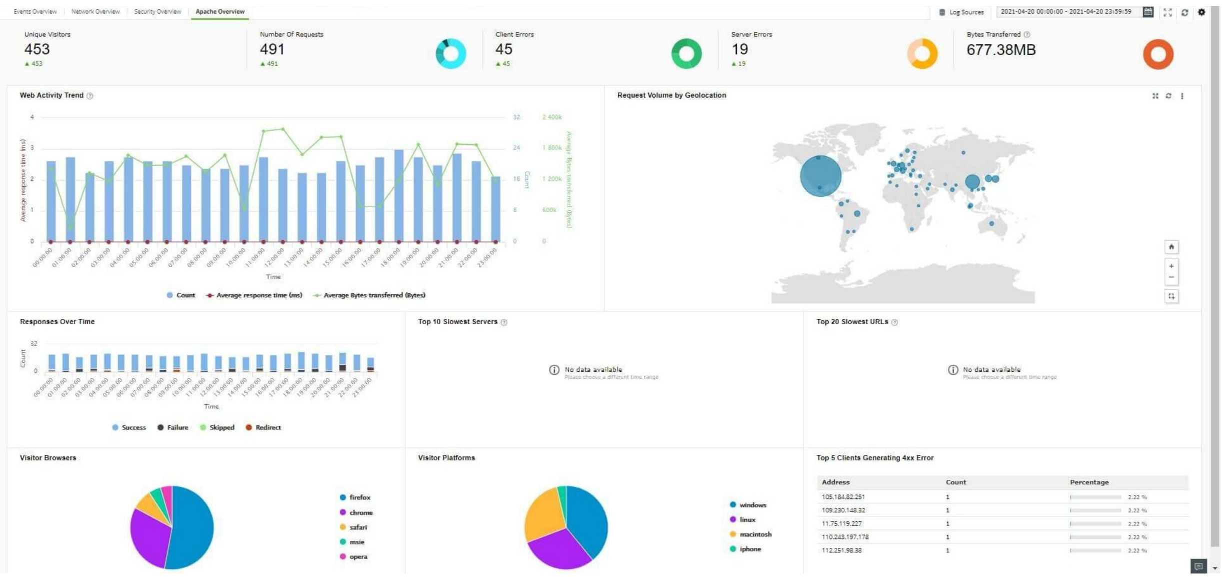
The Combined Log Format is one of the log formats commonly used with Apache logs.

The Combined Log format is:

While importing the log files in the Combined log format, the log files will not include the values for the fields response time and bytes received.

The following widgets in the Apache Overview dashboard can display their values accurately only if the response time and bytes received fields are parsed.

1. Bytes Transferred
2. Top 20 Slowest URLs
3. Web Activity Trend
4. Top 10 Slowest Servers



Unique Visitors 453 ▲ 453

Number Of Requests 491 ▲ 491

Client Errors 45 ▲ 45

Server Errors 19 ▲ 19

Bytes Transferred 677.38MB

Top 10 Slowest Servers: No data available. Please choose a different time range

Top 20 Slowest URLs: No data available. Please choose a different time range

Top 5 Clients Generating 4xx Error

Address	Count	Percentage
105.184.82.251	1	2.22 %
109.230.148.32	1	2.22 %
11.75.119.227	1	2.22 %
110.243.197.178	1	2.22 %
112.251.98.38	1	2.22 %

In order to parse these additional fields, the log format has to be modified. The values for the additional fields can be obtained once the logs are configured with the parameters "%{ms}T" and "%I".
Eventlog Analyzer can parse the modified log format by default.
The modified log format containing the parameters for response time and bytes received is:
%{ms}T - time taken to serve the request (in milliseconds) %I - bytes received, including headers

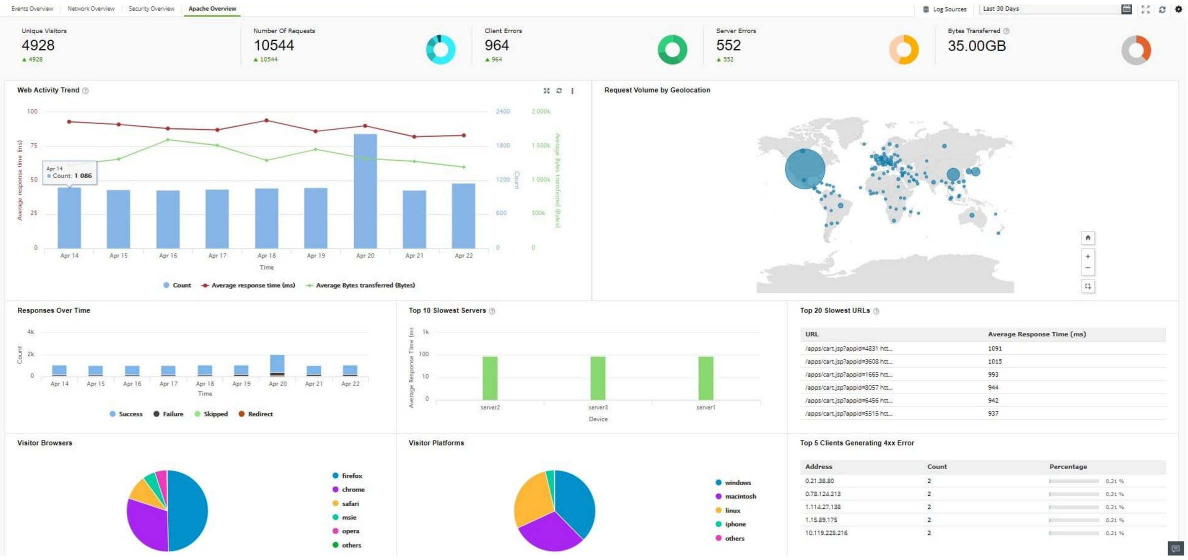
> Note Requires modlog_io to be enabled https://httpd.apache.org/docs/2.4/mod/mod_logio.html

The modified log has 2 directives in addition to the commonly used Combined Log Format. These directives are present at the end of the format, therefore, the combined log format will continue to be parsed as it was parsed in the previous versions.

Procedure to change the Apache log format

> Note The configuration files by default are located at /etc/apache2/ in Debian/Ubuntu/Linux Mint or, /etc/httpd/conf on Red Hat/Fedora/CentOS

1. Define a new log format and assign a label to it.
2. The label can be used to reference the new format string as the customLog directive.
3. The new format will go into effect when the webserver is restarted.
   After the log files have been imported, the updated Apache Overview dashboard has been displayed below:



Top 20 Slowest URLs

URL	Average Response Time (ms)
/apps/cart.jsp?appid=4831 htt...	1091
/apps/cart.jsp?appid=3608 htt...	1015
/apps/cart.jsp?appid=1665 htt...	993
/apps/cart.jsp?appid=8057 htt...	944
/apps/cart.jsp?appid=6456 htt...	942
/apps/cart.jsp?appid=5515 htt...	937

Top 5 Clients Generating 4xx Error

Address	Count	Percentage
0.21.38.80	2	0.21 %
0.78.124.213	2	0.21 %
1.114.27.138	2	0.21 %
1.15.89.175	2	0.21 %
10.119.225.216	2	0.21 %

1.11.1. Configuring the Syslog Service on VMware

Last updated on: September 12, 2025

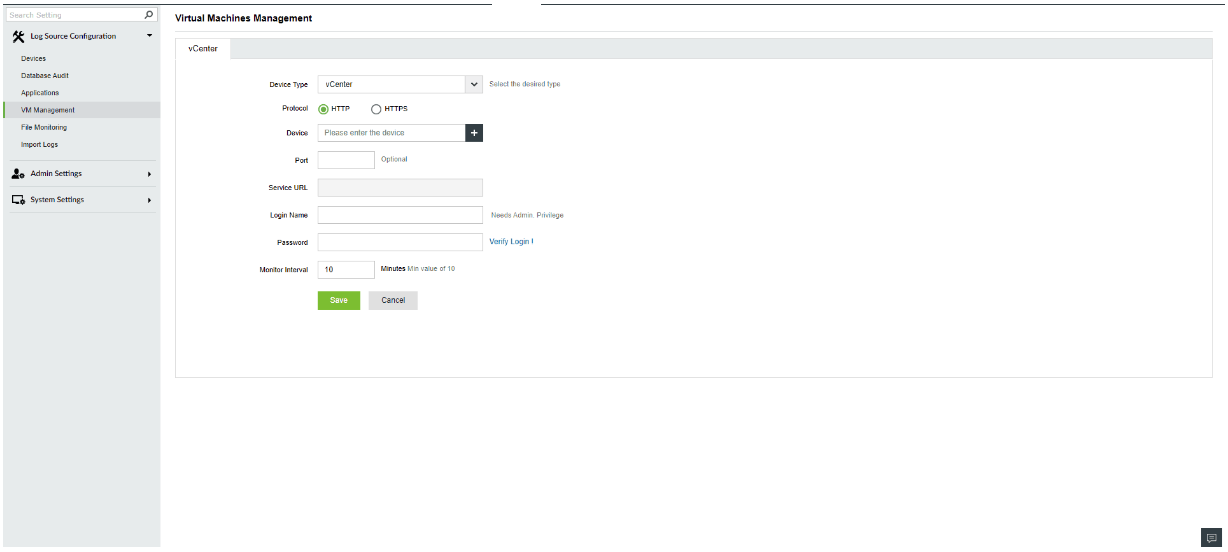
All ESX and ESXi devices run a syslog service (syslogd), which logs messages from the VMkernel and other system components to a file.
To configure the syslog service on an ESX device::
Neither vSphere Client nor vicfg-syslog can be used to configure syslog behavior for an ESX device. To configure syslog for an ESX device, you must edit the /etc/syslog.conf file.
To configure the syslog service on an ESXi device:

1. On ESXi devices, you can use the vSphere Client or the vSphere CLI command vicfg-syslog to configure the following options:
   - Log file path: Specifies a datastore path to the file where syslogd logs all messages.
   - Remote host: Specifies a remote device to which syslog messages are forwarded. In order to receive the forwarded syslog messages, your remote host must have a syslog service installed.
   - Remote port: Specifies the port used by the remote host to receive syslog messages.
2. Configuration using vSphere CLI command: For more information on vicfg-syslog, refer the vSphere Command-Line Interface Installation and Reference Guide.
3. Configuration using vSphere Client:
   - In the vSphere Client inventory, click on the host.
   - Click the Configuration tab.
   - Click Advanced Settings under Software.
   - Select Syslog in the tree control.
   - In the Syslog.Local.DatastorePath text box, enter the datastore path to the file where syslog will log messages. If no path is specified, the default path is /var/log/messages.
     The datastore path format is [<datastorename>] </path/to/file> where the path is relative to the root of the volume backing the datastore.
     Example: The datastore path [storage1] var/log/messages maps to the path /vmfs/volumes/storage1/var/log/messages.
   - In the Syslog.Remote.Devicename text box, enter the name of the remote host where syslog data will be forwarded. If no value is specified, no data is forwarded.
   - In the Syslog.Remote.Port text box, enter the port on the remote host where syslog data will be forwarded. By default Syslog.Remote.Port is set to 514, the default UDP port used by syslog. Changes to Syslog.Remote.Port only take effect if Syslog.Remote.Devicename is configured.
   - Click OK.

1.11.2. Adding vCenter

Last updated on: September 12, 2025

The vCenter servers to be monitored by EventLog Analyzer can be added by navigating to Settings > Log Source Configuration > VM Management and using the Add vCenter button. You can also view and manage the vCenter servers that are being monitored.



Virtual Machines Management

Device Type: vCenter — Select the desired type

Protocol: ● HTTP ○ HTTPS

Device: Please enter the device +

Port: — Optional

Service URL:

Login Name: — Needs Admin. Privilege

Password: — Verify Login !

Monitor Interval: 10 Minutes Min value of 10

Chapter 1.12

Vulnerability Scanners

1.12.1. Exporting data from vulnerability scanners

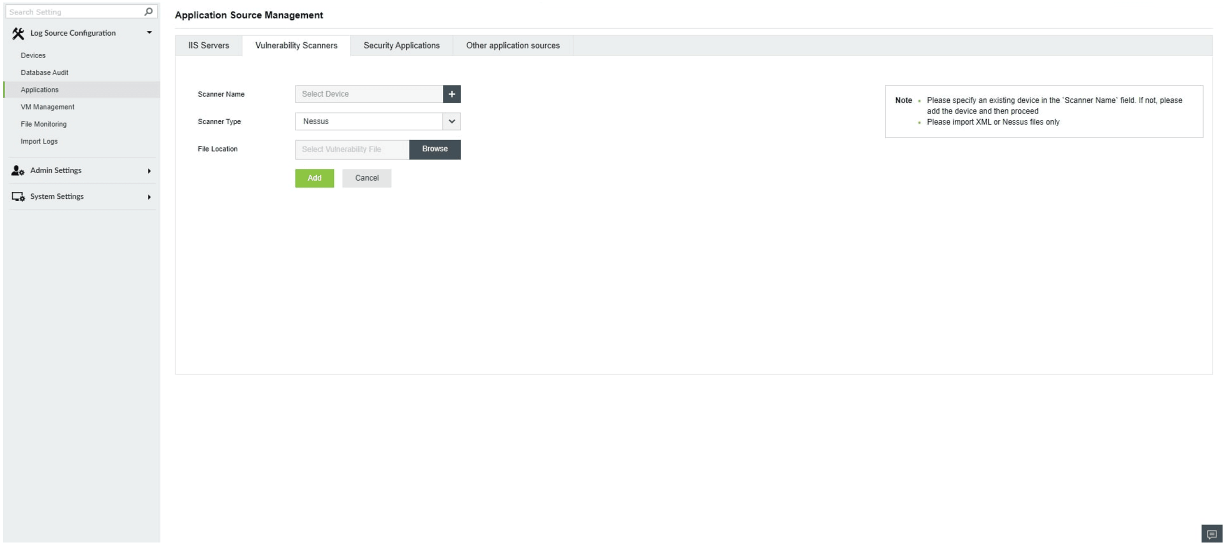
Last updated on: September 12, 2025

EventLog Analyzer analyses data from vulnerability scanners and provides insights to help identify vulnerabilities within the network. For this you need to export data from the respective vulnerability scanners and then import it to EventLog Analyzer. You can export the data by following the steps below

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

Adding vulnerability scanners to EventLog Analyzer

To monitor vulnerability scanner data in EventLog Analyzer, you need to import the corresponding log data to the EventLog Analyzer server. You can import log data by navigating to Settings > Vulnerability Data Analysis > Import.



Scanner Name: Select Device

Scanner Type: Nessus

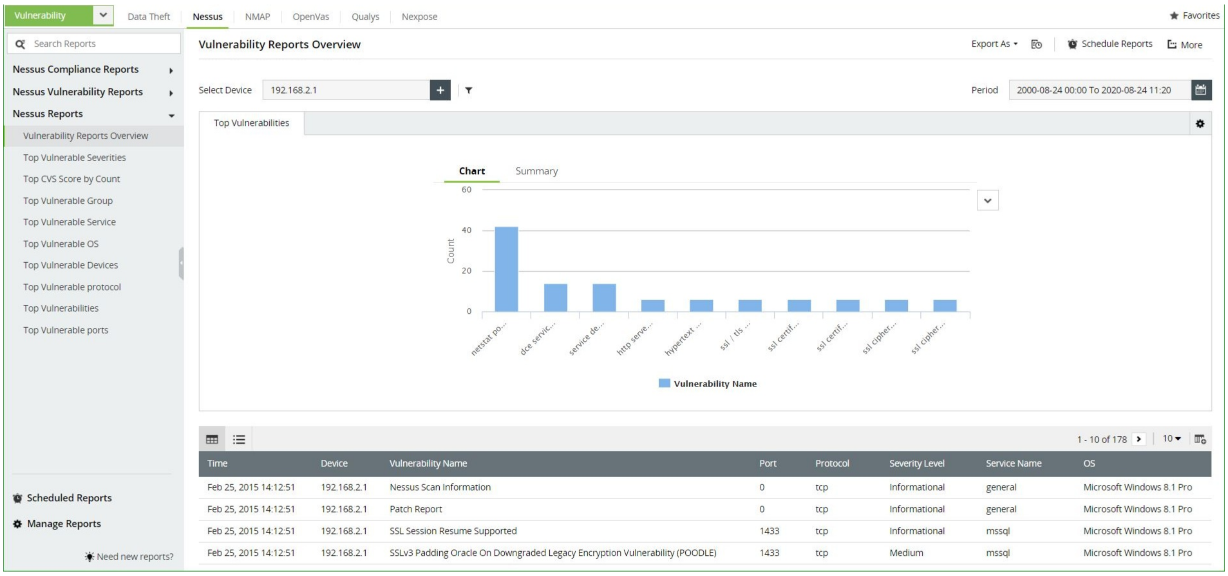
File Location: Select Vulnerability File

Note
- Please specify an existing device in the `Scanner Name` field. If not, please add the device and then proceed
- Please import XML or Nessus files only

1. Enter the vulnerability scanner's name.
2. Choose the vulnerability scanner's application type.
3. Specify the location of the log file which has to be imported.
4. Click on Import.

Reports on Nessus vulnerability data

The information on potential vulnerabilities in a network including credential failures, elevated privilege failures, registry access failures gathered from Nessus are provided as reports. The information in the reports is also 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.



Select Device: 192.168.2.1

Period: 2000-08-24 00:00 To 2020-08-24 11:20

Time	Device	Vulnerability Name	Port	Protocol	Severity Level	Service Name	OS
Feb 25, 2015 14:12:51	192.168.2.1	Nessus Scan Information	0	tcp	Informational	general	Microsoft Windows 8.1 Pro
Feb 25, 2015 14:12:51	192.168.2.1	Patch Report	0	tcp	Informational	general	Microsoft Windows 8.1 Pro
Feb 25, 2015 14:12:51	192.168.2.1	SSL Session Resume Supported	1433	tcp	Informational	mssql	Microsoft Windows 8.1 Pro
Feb 25, 2015 14:12:51	192.168.2.1	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	1433	tcp	Medium	mssql	Microsoft Windows 8.1 Pro

Available reports:

- GHOST in Linux - This report lists any detected instance of the GHOST vulnerability in Linux.
- Shellshock Report - This report contains information on the detected instances of the Shellshock privilege escalation vulnerability in Linux systems in your network.
- Admin Discovery Report - An overview of all the admin accounts in a network will be available in this report.
- Top exploitable vulnerabilities - An overview of the vulnerabilities in your network that are most prone to attacks will be available here.
- Credential failures report - An account of all instances of credential failures in your network will be displayed here.
- Elevated privilege failures report - Failed attempts at privilege escalation will be displayed here.
- Registry access failures - Failed attempts at accessing the Windows Registry will be recorded here.
- Patch report - A report of all the patches applied in the device will be displayed.
- Overall Nessus report - An overview of events in Nessus vulnerabilty scanners in your network will be available here.

Ensuring Compliance to regulatory mandates:

EventLog Analyzer helps in complying with regulatory mandates such as the GDPR, PCI DSS and NIST. These regulations mandate that critical events in devices and applications that could potentially lead to a data breach need to be monitored. If any indication of a breach is detected, remediating action has to be taken to mitigate this risk. Information from vulnerability scanners like Nessus form a critical part of the data that needs to be monitored.

For instance, the risk assessment (ID.RA) section of NIST compliance that states,

"The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. Threat and vulnerability information is received from information sharing forums and sources."

The data from vulnerability scanners that can be used to ensure compliance to regulations are also categorized according to the device types, in EventLog Analyzer. The solution categorizes the reports as follows based on the devices' data that Nessus analyzes.

- Windows devices
- Unix devices
- Databases
- Cisco IOS
- Huawei
- Unix file contents
- IBM iSeries
- SonicWall, SonicOS
- Citrix XenServer
- VMware, nessus, and vSphere infrastructure

Once the Nessus vulnerability scanner is added, this data from Nessus can be manually imported into EventLog Analyzer or automated imports can be scheduled. This data is then collated into comprehensive reports to comply with PCI DSS requirements.

- Denial of remote access software
- Denial of insecure communication
- Handling false positives

1.12.2. Exporting data from vulnerability scanners

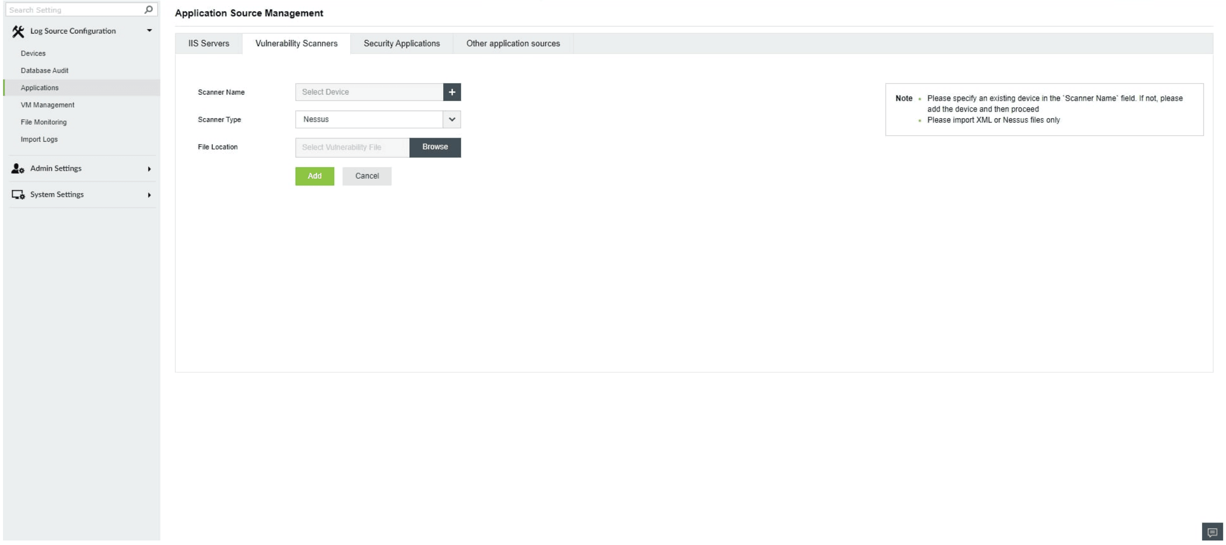
Last updated on: September 12, 2025

EventLog Analyzer analyses data from vulnerability scanners and provides insights to help identify vulnerabilities within the network. For this you need to export data from the respective vulnerability scanners and then import it to EventLog Analyzer. You can export the data by following the steps below:

1. Go to the Scan menu and select the scan that you want to save.
2. Click Save Scan.
3. In the Save dialog box, choose the format as Nmap XML format

Adding vulnerability scanners to EventLog Analyzer

To monitor vulnerability scanner data in EventLog Analyzer, you need to import the corresponding log data to the EventLog Analyzer server. You can import log data by navigating to Settings > Vulnerability Data Analysis > Import.



Scanner Name: Select Device

Scanner Type: Nessus

File Location: Select Vulnerability File

Note
- Please specify an existing device in the `Scanner Name` field. If not, please add the device and then proceed
- Please import XML or Nessus files only

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.

1.12.3. Exporting data from vulnerability scanners

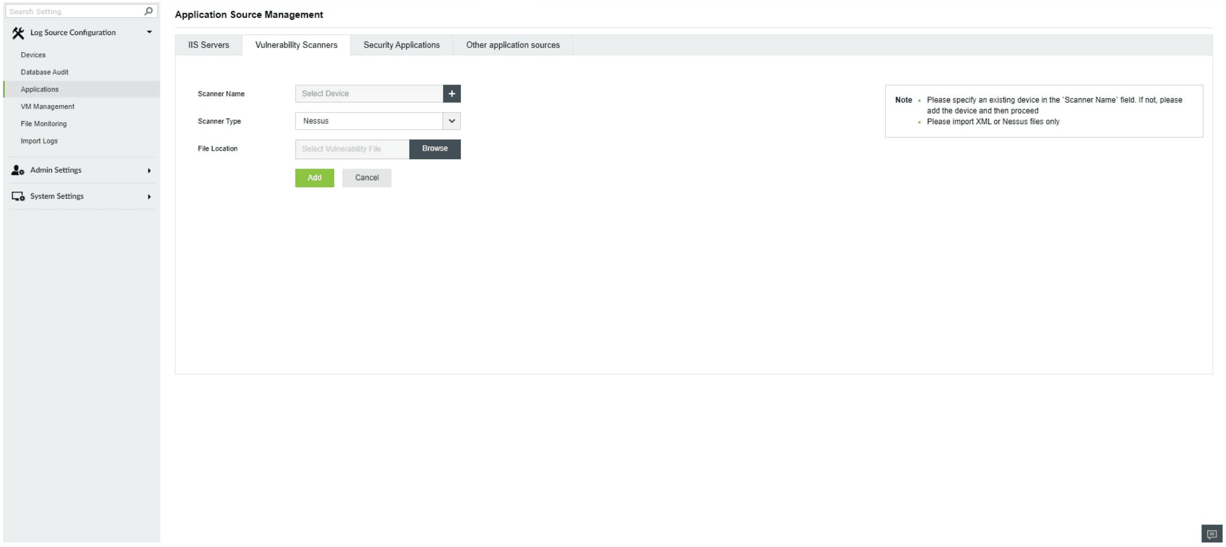
Last updated on: September 12, 2025

EventLog Analyzer analyses data from vulnerability scanners and provides insights to help identify vulnerabilities within the network. For this you need to export data from the respective vulnerability scanners and then import it to EventLog Analyzer. You can export the data by following the steps given below:

1. Click the Reports icon.
2. Under the Create a report tab select Export.
3. Select XML Export or XML Export 2.0.
4. Add the site and then click Save and run report.

Adding vulnerability scanners to EventLog Analyzer

To monitor vulnerability scanner data in EventLog Analyzer, you need to import the corresponding log data to the EventLog Analyzer server. You can import log data by navigating to Settings > Vulnerability Data Analysis > Import.



Scanner Name: Select Device

Scanner Type: Nessus

File Location: Select Vulnerability File

Note
- Please specify an existing device in the `Scanner Name` field. If not, please add the device and then proceed
- Please import XML or Nessus files only

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.

1.12.4. Exporting data from vulnerability scanners

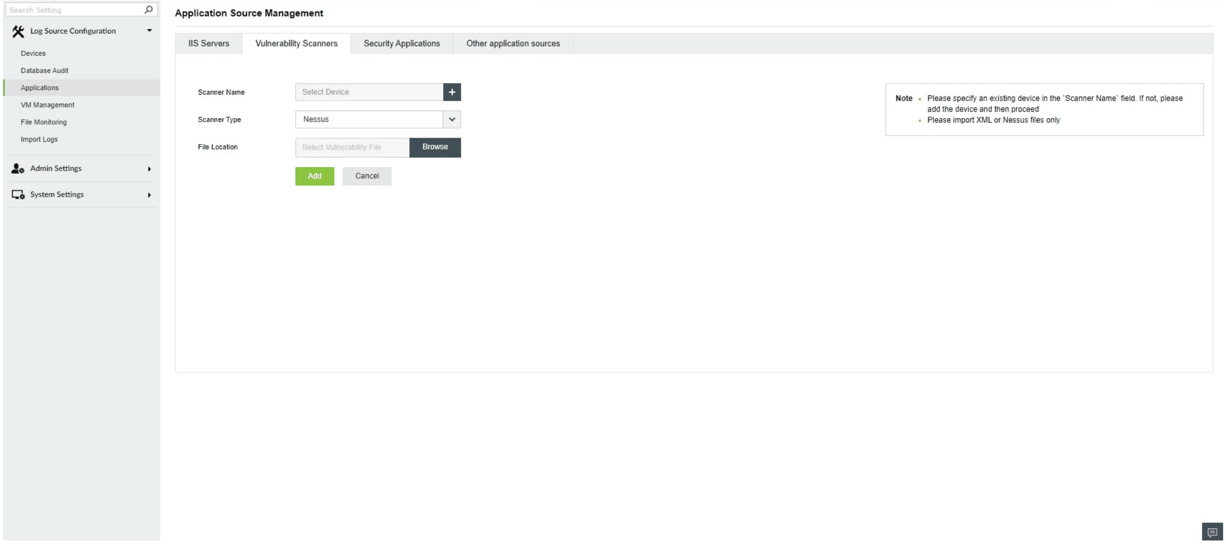
Last updated on: September 12, 2025

EventLog Analyzer analyses data from vulnerability scanners and provides insights to help identify vulnerabilities within the network. For this you need to export data from the respective vulnerability scanners and then import it to EventLog Analyzer. You can export the data by following the steps given for each of the vulnerability scanners.

1. Under the Scans menu, select Vulnerabilities
2. If there is no Vulnerabilities tab, choose Results.
3. Click Export page contents from the bottom right corner.

Adding vulnerability scanners to EventLog Analyzer

To monitor vulnerability scanner data in EventLog Analyzer, you need to import the corresponding log data to the EventLog Analyzer server. You can import log data by navigating to Settings > Vulnerability Data Analysis > Import.



Scanner Name: Select Device

Scanner Type: Nessus

File Location: Select Vulnerability File

Note
- Please specify an existing device in the `Scanner Name` field. If not, please add the device and then proceed
- Please import XML or Nessus files only

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.

1.12.5. Exporting data from vulnerability scanners

Last updated on: September 12, 2025

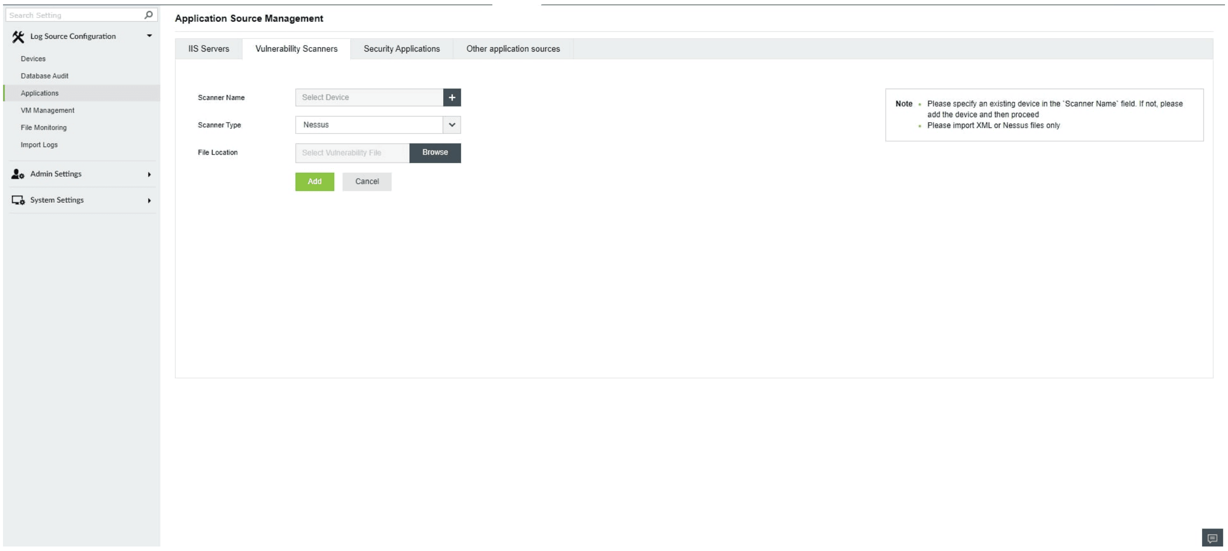
EventLog Analyzer analyses data from vulnerability scanners and provides insights to help identify vulnerabilities within the network. For this you need to export data from the respective vulnerability scanners and then import it to EventLog Analyzer. You can export the data by following the steps given fbelow:

1. Go to the Scans menu in the dashboard.
2. Right-click the scan report that you need to export.
3. Select Download from the Quick Actions menu.
4. Select Download Format as Extensible Markup Language(XML).

Once you have exported the data from the corresponding scanners, you need to import the log data to the EventLog Analyzer server.

Adding vulnerability scanners to EventLog Analyzer

To monitor vulnerability scanner data in EventLog Analyzer, you need to import the corresponding log data to the EventLog Analyzer server. You can import log data by navigating to Settings > Vulnerability Data Analysis > Import.



Scanner Name: Select Device

Scanner Type: Nessus

File Location: Select Vulnerability File

Note
- Please specify an existing device in the `Scanner Name` field. If not, please add the device and then proceed
- Please import XML or Nessus files only

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.

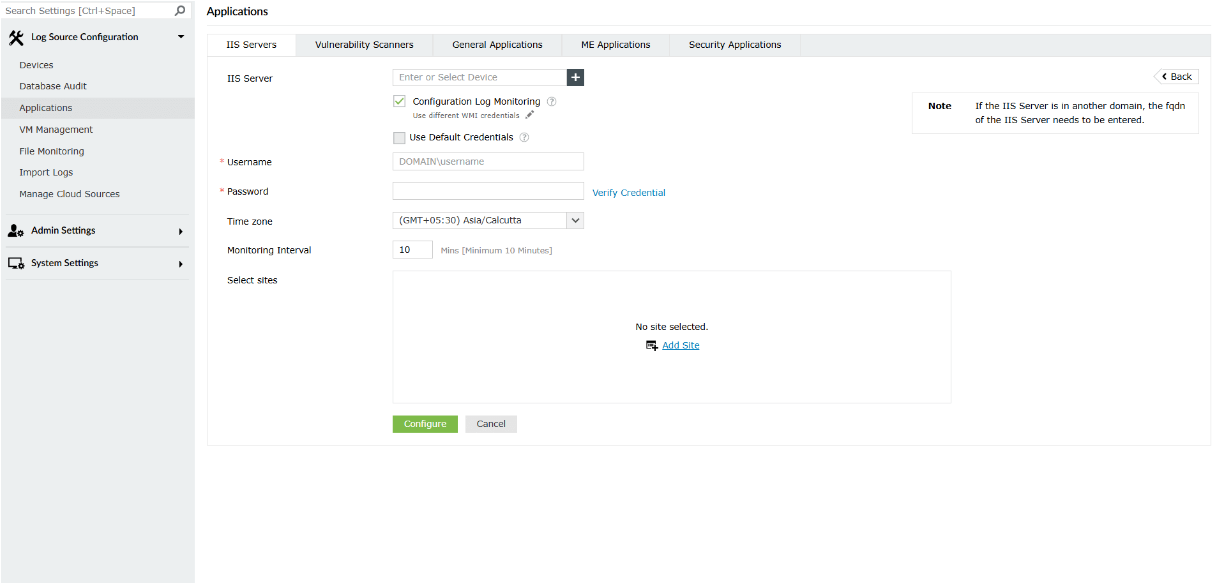
Web Servers

1.13.1. Adding an IIS server

Last updated on: September 12, 2025

Prerequisite for adding an IIS server

When configuring IIS log source in EventLog Analyzer for the first time, administrative privileges are required. (Administrator shares privileges are required eg : Admin$,c$)



IIS Server: Enter or Select Device

☑ Configuration Log Monitoring

Use different WMI credentials

□ Use Default Credentials

* Username: DOMAIN\username

* Password:

Time zone: (GMT+05:30) Asia/Calcutta

Monitoring Interval: 10 Mins [Minimum 10 Minutes]

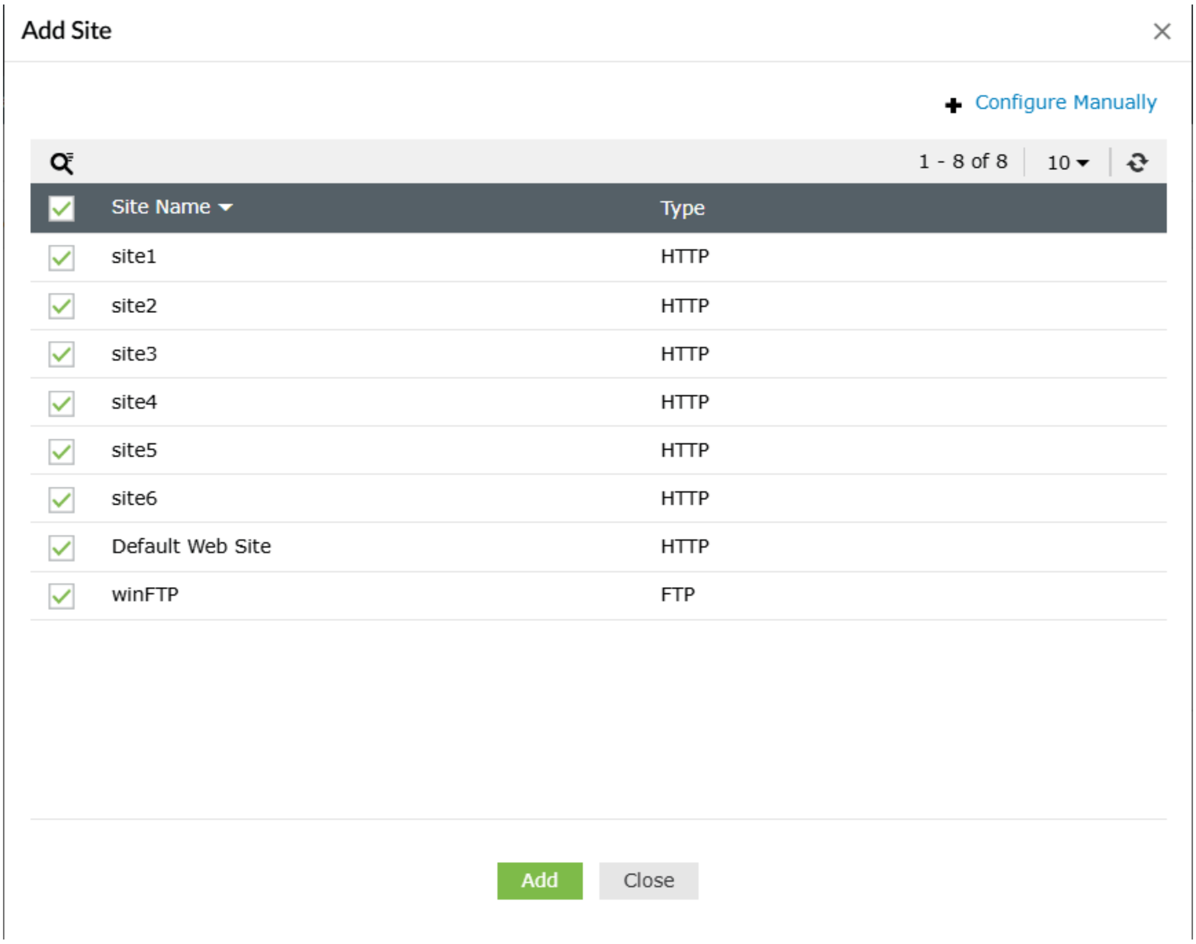
Select sites: No site selected.

Note If the IIS Server is in another domain, the fqdn of the IIS Server needs to be entered.

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



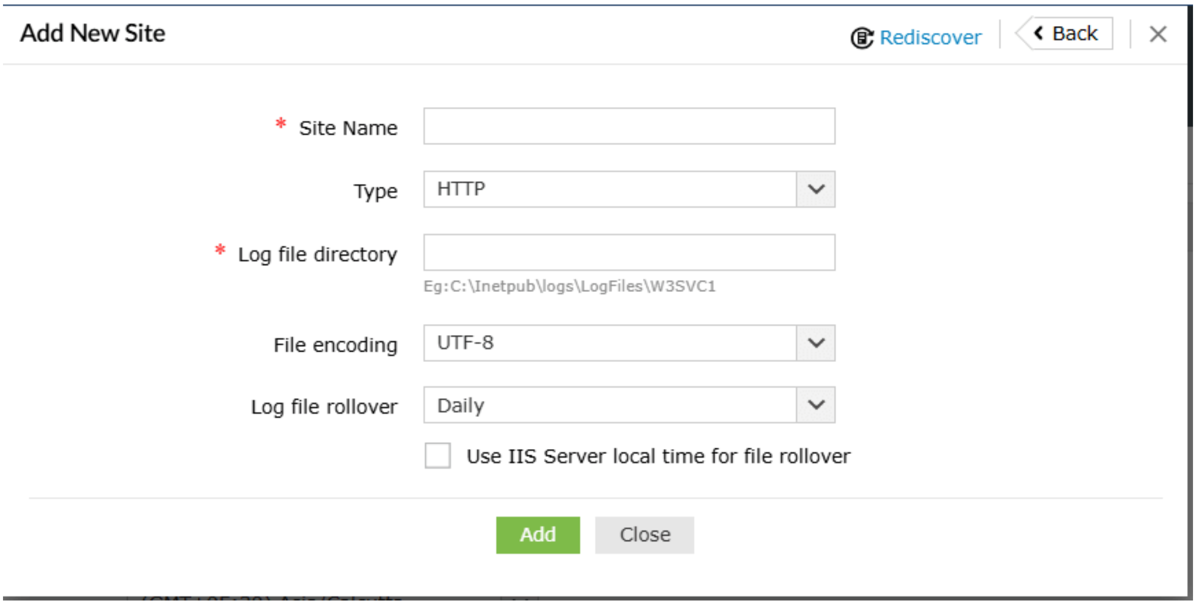
Add Site

✚ Configure Manually

1 - 8 of 8 | 10 ▾

☑	Site Name ▾	Type
☑	site1	HTTP
☑	site2	HTTP
☑	site3	HTTP
☑	site4	HTTP
☑	site5	HTTP
☑	site6	HTTP
☑	Default Web Site	HTTP
☑	winFTP	FTP

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.



Add New Site

* Site Name	
Type	HTTP
* Log file directory	Eg:C:\Inetpub\logs\LogFiles\W3SVC1
File encoding	UTF-8
Log file rollover	Daily
	□ Use IIS Server local time for 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

Once the initial configuration is complete, the account can be modified to be used as a service account.

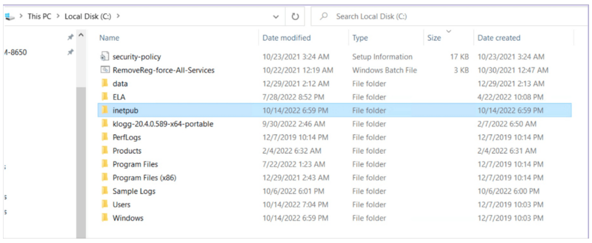
Configuring an IIS site for non-admin users

Note

Any Configuration Changes made in IIS Manager will not be synced on next scheduling if non admin credentials is used

Steps to configure the IIS site in EventLog Analyzer for non-admin users:

1. In the IIS server, navigate to the C directory (Note: The default location may vary)

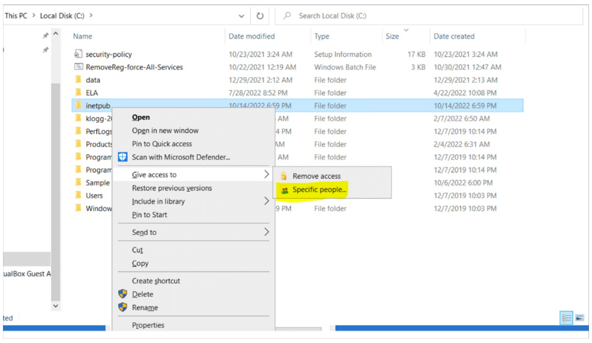


This PC > Local Disk (C:) >

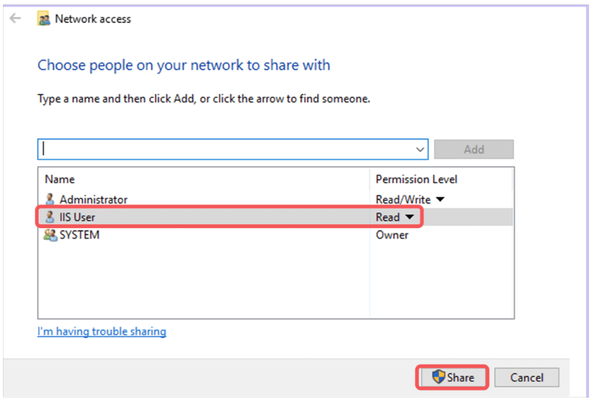
Search Local Disk (C:)

Name	Date modified	Type	Size	Date created
security-policy	10/23/2021 3:24 AM	Setup Information	17 KB	10/23/2021 3:24 AM
RemoveReg-force-All-Services	10/22/2021 12:19 AM	Windows Batch File	3 KB	10/30/2021 12:47 AM
data	12/29/2021 2:12 AM	File folder		12/29/2021 2:13 AM
ELA	7/28/2022 8:52 PM	File folder		4/22/2022 10:08 PM
inetpub	10/14/2022 6:59 PM	File folder		10/14/2022 6:59 PM
klogg-20.4.0.589-x64-portable	9/30/2022 2:46 AM	File folder		2/7/2022 6:50 AM
PerfLogs	12/7/2019 10:14 PM	File folder		12/7/2019 10:14 PM
Products	2/4/2022 6:32 AM	File folder		2/4/2022 6:31 AM
Program Files	7/22/2022 1:23 AM	File folder		12/7/2019 10:14 PM
Program Files (x86)	12/29/2021 2:43 AM	File folder		12/7/2019 10:14 PM
Sample Logs	10/6/2022 6:01 PM	File folder		10/6/2022 6:00 PM
Users	10/14/2022 7:04 PM	File folder		12/7/2019 10:03 PM
Windows	10/14/2022 6:59 PM	File folder		12/7/2019 10:03 PM

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



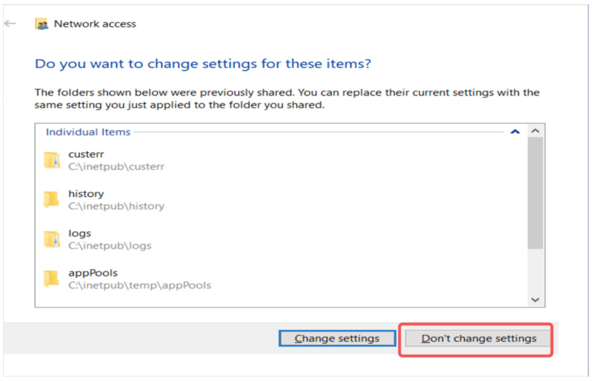
Network access

Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Administrator	Read/Write
IIS User	Read
SYSTEM	Owner

4. If the pop-up occurs, click on Don't change settings.



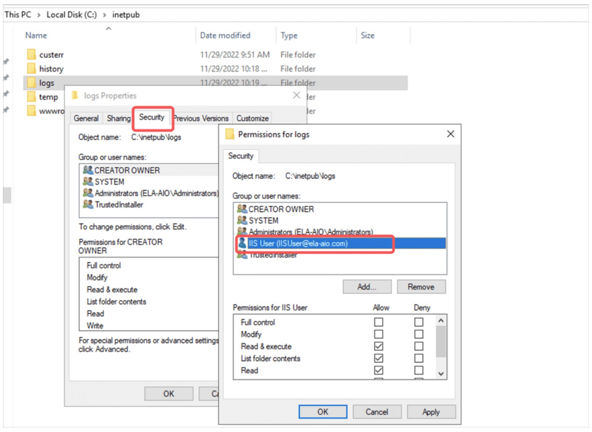
Do you want to change settings for these items?

The folders shown below were previously shared. You can replace their current settings with the same setting you just applied to the folder you shared.

Individual Items

- custerr C:\inetpub\custerr
- history C:\inetpub\history
- logs C:\inetpub\logs
- appPools C:\inetpub\temp\appPools

5. Navigate to inetpub → logs → properties → Security → add the service account with read access permission. (Note: The default location may vary)



Name	Date modified	Type	Size
custerr	11/29/2022 9:51 AM	File folder	
history	11/29/2022 10:18 ...	File folder	
logs	11/29/2022 10:19 ...	File folder	
temp		...ler	
wwwro...		...ler	

Object name: C:\inetpub\logs

Group or user names:
CREATOR OWNER
SYSTEM
Administrators (ELA-AIO\Administrators)
IIS User (IISUser@ela-aio.com)
TrustedInstaller

To change permissions, click Edit.

Permissions for CREATOR OWNER
Full control
Modify
Read & execute
List folder contents
Read
Write

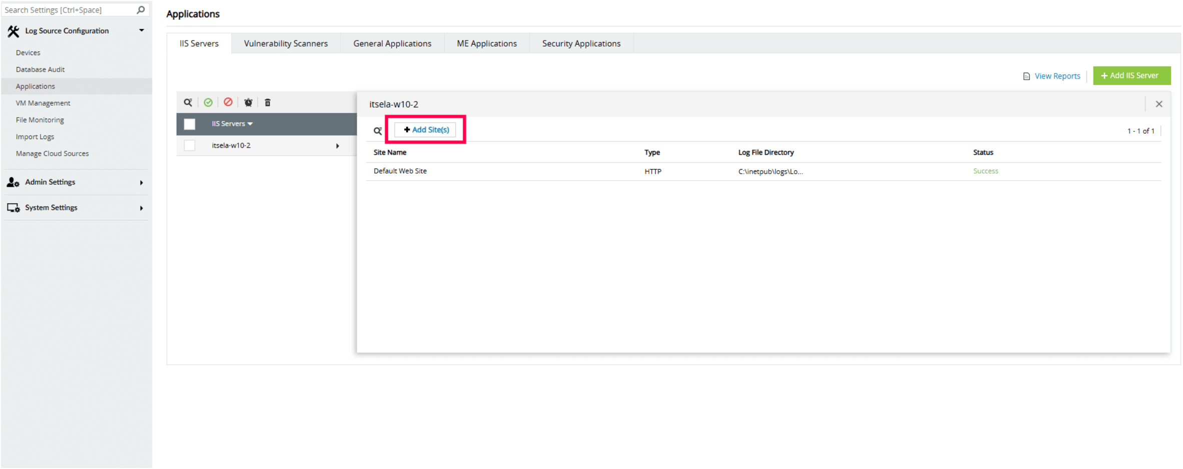
For special permissions or advanced settings, click Advanced.

Permissions for IIS User	Allow	Deny
Full control	☐	☐
Modify	☐	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

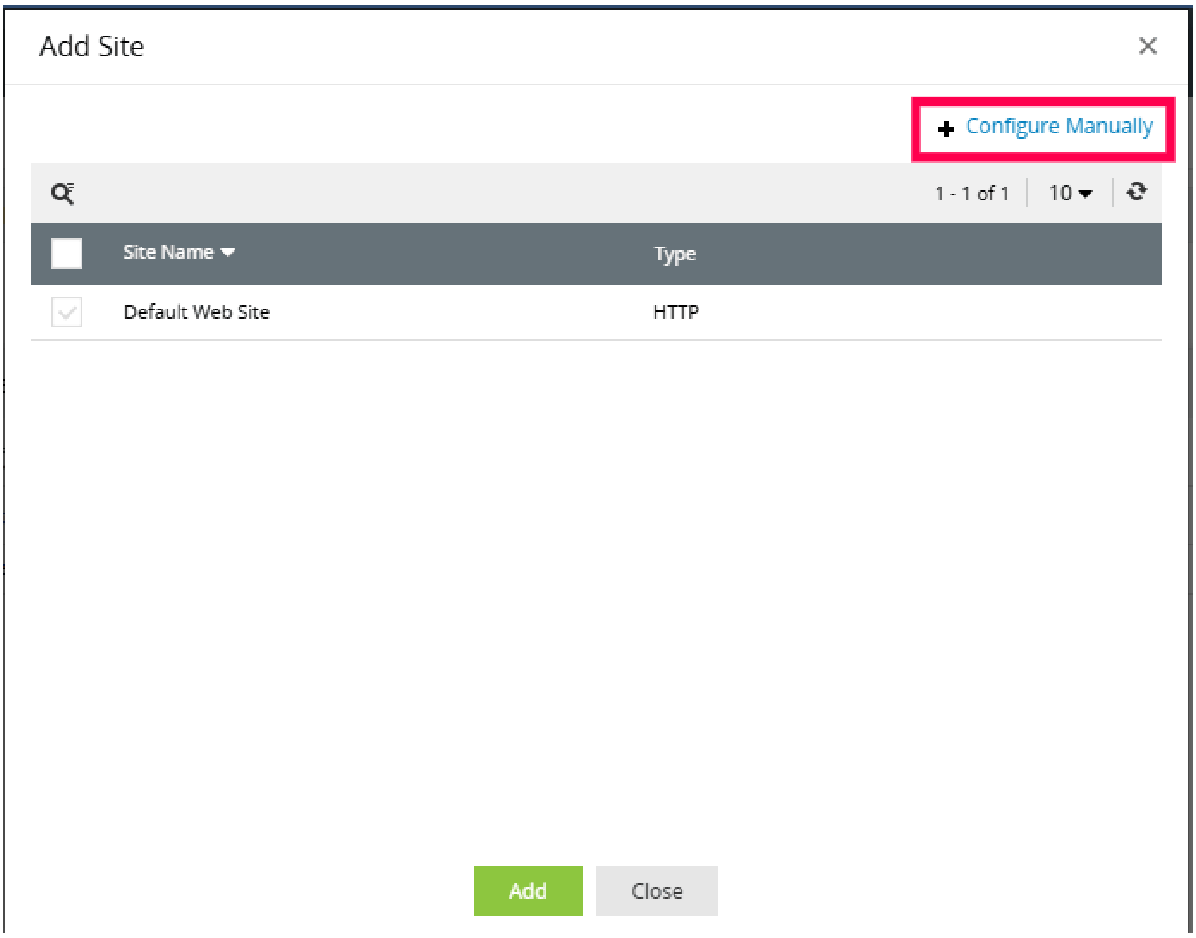
Note

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



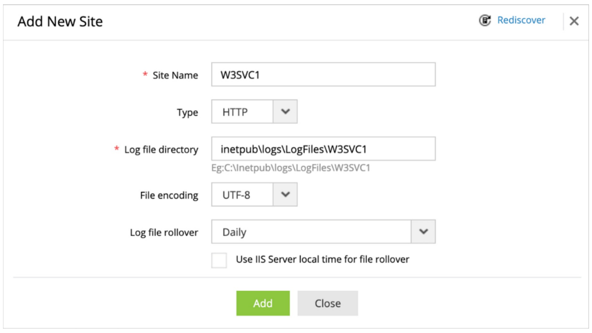
Site Name	Type	Log File Directory	Status
Default Web Site	HTTP	C:\inetpub\logs\Lo...	Success



Add Site

Site Name	Type
Default Web Site	HTTP

7. Enter the IIS site name, path → Add and configure



Add New Site

* Site Name: W3SVC1

Type: HTTP

* Log file directory: inetpub\logs\LogFiles\W3SVC1

Eg:C:\Inetpub\logs\LogFiles\W3SVC1

File encoding: UTF-8

Log file rollover: Daily

□ Use IIS Server local time for file rollover

IIS Configuration Change Logs

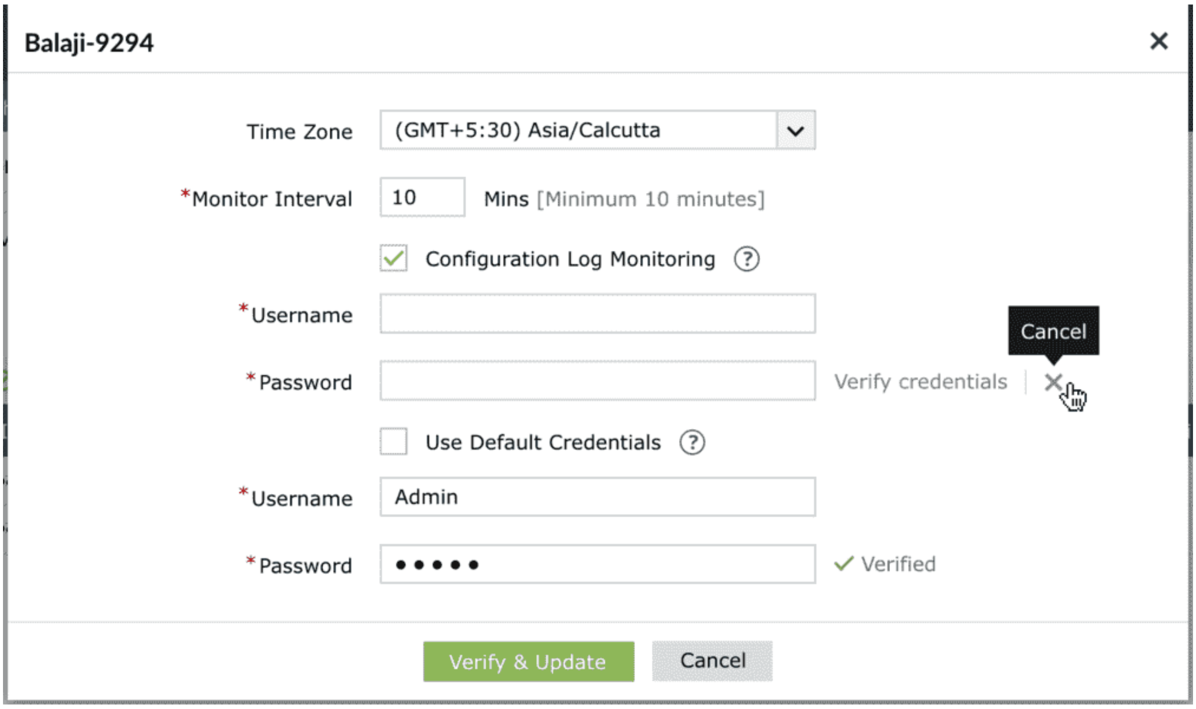
Configuration change logs are collected in the IIS similar to how logs are collected for Windows. These logs are collected through the Microsoft-IIS-Configuration/Operational event source file.

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

3. Ensure that the Microsoft-IIS-Configuration/Operational option is enabled in the configure event source file for the device. This option can be enabled in the Manage Devices tab.

4. The Configuration log monitoring credential provided must have the WMI access.



Balaji-9294

Time Zone: (GMT+5:30) Asia/Calcutta

*Monitor Interval: 10 Mins [Minimum 10 minutes]

☑ Configuration Log Monitoring

*Username:

*Password: Verify credentials

□ Use Default Credentials

*Username: Admin

*Password: ●●●●● ✓ Verified

1.14.1.1. Microsoft 365

Last updated on: September 12, 2025

In this page

Overview

Log360 provides centralized visibility into user activities, administrative actions, and security events across Microsoft 365. It collects audit logs from services such as Microsoft Entra ID, Exchange Online, SharePoint Online, M365 General (including Teams, OneDrive, and other M365 services), and Exchange MailTrace, consolidating them into a single platform for monitoring, analysis, and compliance.
Organizations can monitor critical activities such as user sign-ins, mailbox access, file sharing, and collaboration. Reports provide insights from all Microsoft 365 sources, including Entra ID, Exchange Online, SharePoint, OneDrive, and Microsoft Teams, covering mailbox traffic, spam and malware incidents, inactive users, and soon-to-expire licenses, etc. The product console also offers compliance reports for these services to help organizations meet regulatory standards such as HIPAA, SOX, and PCI-DSS.
Administrators can also configure alerts to receive notifications about important activities, define which mailboxes to monitor for unusual behavior, and get detailed information on the actions triggering each alert. By combining reporting, alerting, and management into a unified workflow, the product helps organizations maintain security, simplify investigations, and ensure compliance across their Microsoft 365 environment.

Key functionalities

- Track critical activity: Gain visibility into user sign-ins, mailbox access, file sharing, and collaboration across Microsoft 365 services to monitor day-to-day operations.
- Detect suspicious behavior: Identify unusual patterns such as Login from an anonymized IP address, role changes, or unauthorized changes to mailbox permissions.
- Strengthen compliance posture: Securely retain audit logs and generate detailed reports to support compliance with IT regulations and standards.
- Accelerate incident analysis: Use consolidated logs, reports, and real-time alerts to analyze and respond to incidents.
- Object synchronization and filtering: Sync Active Directory objects such as users, groups, and service principals using object filters. The synced data show details of the entity (user or service principal) that initiated the action in the Incident Workbench and used in the Rules module for log enrichment.

Read also

This document explains managing, reporting, and alerting for Microsoft 365 tenants using the product console and its key functionalities. To set up and manage Microsoft 365 tenants, see the articles below:

- Tenant configuration
- Adding data source
- Managing M365 accounts

1.14.1.2. Adding data source

Last updated on: September 12, 2025

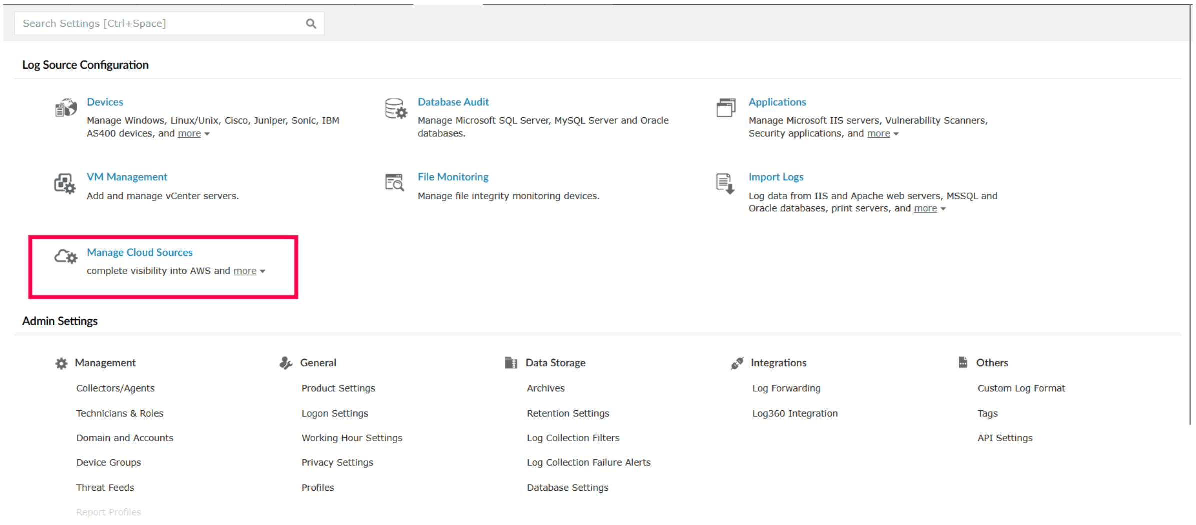
In this page

Overview

This page explains how to add Microsoft 365 services as data sources in the product console after configuring a tenant. Once the tenant is configured, you can select the account and add any of the following services as data sources to enable log collection: Exchange Online, SharePoint Online, M365 General, and Exchange MailTrace.

Steps to add a data source

1. In your product console, navigate to the Settings tab.
2. Under Log Configuration, select Manage Cloud Sources.

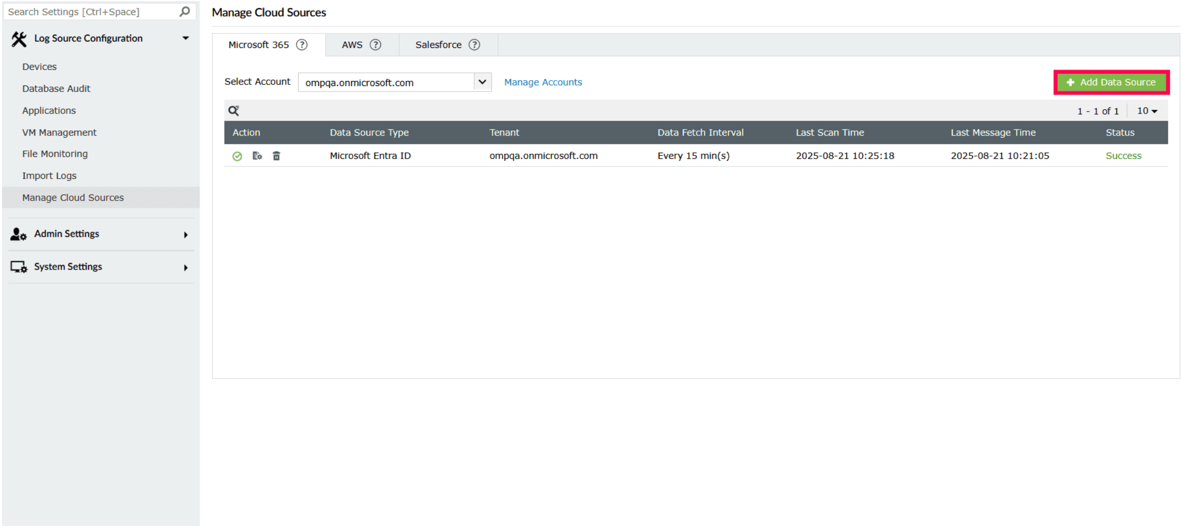


Search Settings [Ctrl+Space]
Log Source Configuration
Devices
Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more
Database Audit
Manage Microsoft SQL Server, MySQL Server and Oracle databases.
Applications
Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more
VM Management
Add and manage vCenter servers.
File Monitoring
Manage file integrity monitoring devices.
Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more
Manage Cloud Sources
complete visibility into AWS and more
Admin Settings
Management
Collectors/Agents
Technicians & Roles
Domain and Accounts
Device Groups
Threat Feeds
Report Profiles
General
Product Settings
Logon Settings
Working Hour Settings
Privacy Settings
Profiles
Data Storage
Archives
Retention Settings
Log Collection Filters
Log Collection Failure Alerts
Database Settings
Integrations
Log Forwarding
Log360 Integration
Others
Custom Log Format
Tags
API Settings

Figure 1: Navigating to Manage Cloud Sources

3. On the Manage Cloud Sources page, click Add Data Source in the top-right corner.

> ⓘ NOTE
>
> Microsoft Entra ID will be added as a data source by default.



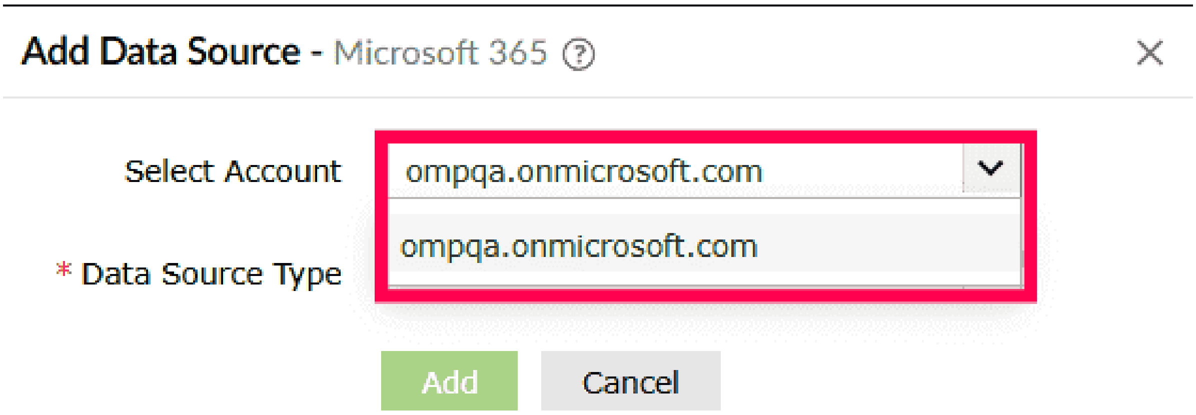
Manage Cloud Sources

Select Account: ompqa.onmicrosoft.com

Action	Data Source Type	Tenant	Data Fetch Interval	Last Scan Time	Last Message Time	Status
	Microsoft Entra ID	ompqa.onmicrosoft.com	Every 15 min(s)	2025-08-21 10:25:18	2025-08-21 10:21:05	Success

Figure 2: Adding a data source

4. In the Add Data Source window, select an account from the Select Account drop-down.



Add Data Source - Microsoft 365

Select Account: ompqa.onmicrosoft.com

ompqa.onmicrosoft.com

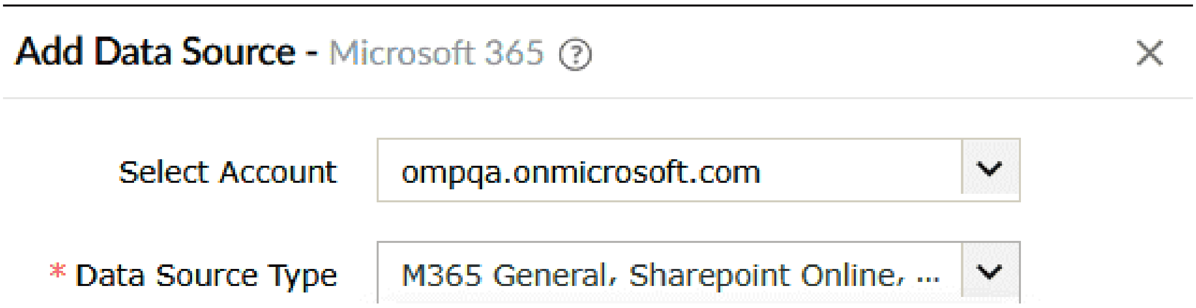
* Data Source Type

Figure 3: Selecting an account

5. From the Data Source Type drop-down, choose the Microsoft 365 service(s) you want to add.

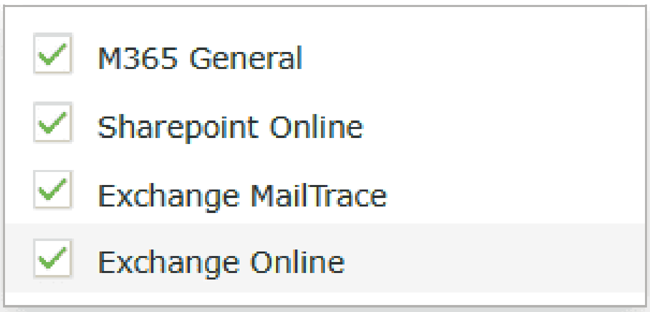
NOTE

You can add one or more services at a time. The available options are: Microsoft Entra ID, Exchange Online, SharePoint Online, M365 General, and Exchange MailTrace.


Add Data Source - Microsoft 365

Select Account: ompqa.onmicrosoft.com

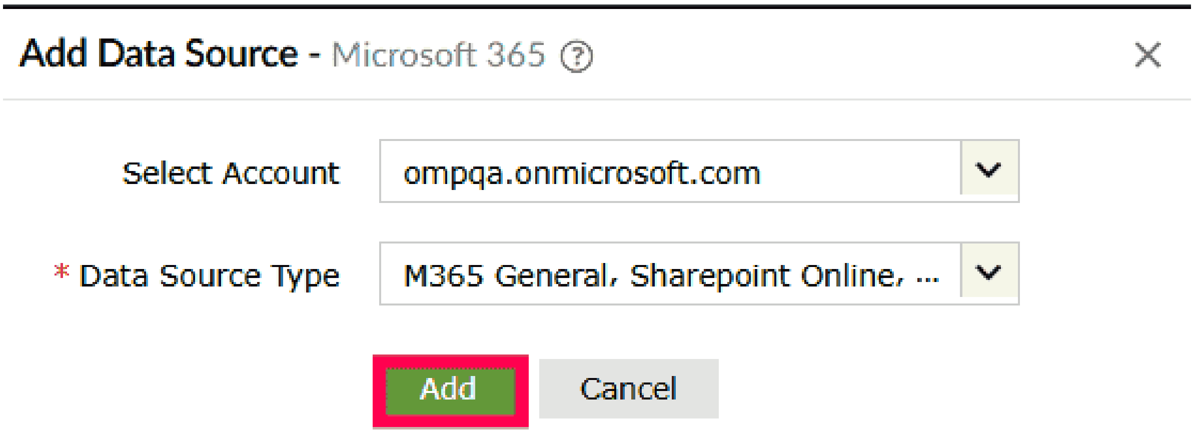
* Data Source Type: M365 General, Sharepoint Online, ...



☑ M365 General
☑ Sharepoint Online
☑ Exchange MailTrace
☑ Exchange Online

Figure 4: Selecting data source types

6. Click Add to add the selected data sources.



Add Data Source - Microsoft 365

Select Account: ompqa.onmicrosoft.com

* Data Source Type: M365 General, Sharepoint Online, ...

Figure 4: Selecting data source types

Read also

This page detailed how to add Microsoft 365 services as data sources in the product console after configuring a tenant. To learn more about related configurations, see the articles below:

- Managing Microsoft 365 accounts
- Managing cloud sources

1.14.2. Troubleshooting Microsoft 365

Last updated on: September 12, 2025

In this page

Overview

This section provides troubleshooting steps for common Microsoft 365 integration issues in Log360. Errors may occur due to missing configurations, expired credentials, or disabled settings in the Microsoft 365 environment. The following guidance will help you identify and resolve these issues.

Common integration issues

1. Audit Logging must be turned on to fetch data

Cause:
Audit logging is not enabled in the Microsoft 365 environment, which prevents user and admin activity from being recorded and fetched into Log360.
Solution:
Enable audit logging using either of the following methods:

- Through the Microsoft 365 portal
  - Log in to the Microsoft 365 portal and navigate to the Admin tab.
  - Go to Admin centers > Compliance > Solutions > Audit. Alternatively, directly open Audit Log Search.
  - If auditing is not turned on, a banner will prompt you to enable activity recording.
  - Select Start recording user and admin activity.

  > NOTE
  >
  > Changes may take up to 60 minutes to take effect

- Turn on audit logging through PowerShell
  - Run the following cmdlets in PowerShell.
  - $UserCredential = Get-Credential;$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection;Import-PSSession $Session -CommandName Set-AdminAuditLogConfig
  - Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled:$True

    - Remove-PSSession $Session

2. Invalid Application Password

Cause:
This error occurs if the configured Microsoft 365 application password is deleted or has expired.
Solution:
Create a new application password in Microsoft 365 and update it in the product's Tenant Settings.

3. Missing Microsoft Entra ID Application

Cause:
This error occurs if the Microsoft Entra ID application associated with Log360 has been deleted from the Azure portal.
Solution:
Reconfigure the application in the Azure portal. Follow the manual configuration steps outlined here.
Read also
This page explained common Microsoft 365 integration issues and their solutions, such as enabling audit logging, handling expired application passwords, and reconfiguring deleted applications.
For more details, refer to:

- Adding a data source
- Configuring and managing

1.14.3. Amazon Web Services (AWS)

Last updated on: September 12, 2025

To monitor your AWS environment, EventLog Analyzer requires a valid IAM user with necessary permissions. The solution will use the designated IAM user to collect logs from your AWS environment.

> Note
>
> EventLog Analyzer supports all AWS regions, except the AWS China (Beijing) region.

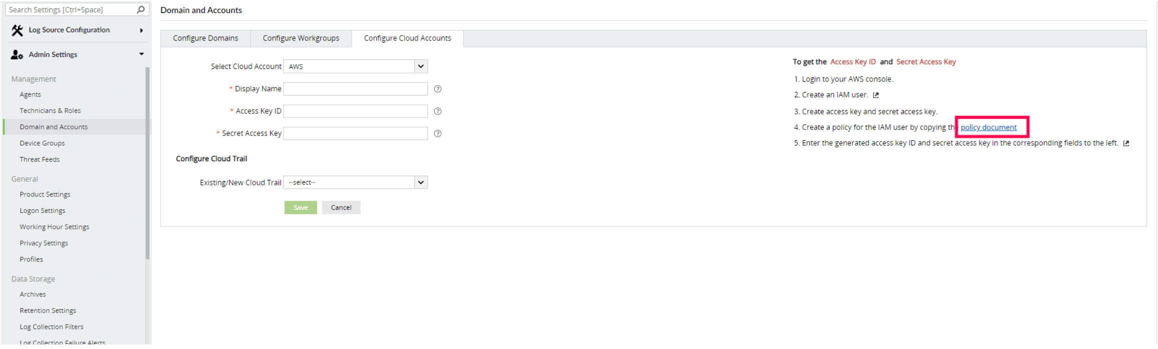
Creating a new IAM user in the AWS console

An IAM user is an entity that you create in AWS to represent the person or service that uses it to interact with AWS.

To create a new IAM user, follow these steps.

1. Login to the AWS console.
2. Navigate to IAM
   - Go to AWS Services → Security, Identity and Compliance → IAM.
3. Create a new user:
   - Select Users from the Left pane and click on Create User.
   - Enter an appropriate User name and click Next.
4. Attach Policies
   - Click on Attach policies directly and then Click on Create Policy.
   - A new tab named Create Policy will open. Select JSON.
   - Depending on whether you want to manually or automatically configure CloudTrail, copy and paste the inline policies accordingly.
     - Auto-configuration: For automatic CloudTrail configuration by EventLog Analyzer, copy and paste the provided inline policy.
     - Manual configuration: For manual CloudTrail configuration, copy and paste the provided inline policy.

   You can find the inline policy in the highlighted section of the image below.



Select Cloud Account: AWS

* Display Name

* Access Key ID

* Secret Access Key

Configure Cloud Trail

Existing/New Cloud Trail: --select--

To get the Access Key ID and Secret Access Key

1. Login to your AWS console.
2. Create an IAM user.
3. Create access key and secret access key.
4. Create a policy for the IAM user by copying the policy document
5. Enter the generated access key ID and secret access key in the corresponding fields to the left.

- Click Next.
- Fill in the Policy Name field and click Create Policy.
- Return to the previous tab, refresh the policy table, select the newly created policy, and click Next.

5. Finalize the user creation
    - Verify the details and click Create user.
6. Create security credentials
    - Click on the created User.
    - Go to Security Credentials and click on Create access key under the Access keys section.
    - Choose Third-party service and check the confirmation box.
    - Click Next and then click Create access key.
    - Download the .csv file to save the Access key and Secret access Key.

The generated access key and secret key pair should be used inside EventLog Analyzer to configure the AWS account.

Enter AWS credentials in EventLog Analyzer

- Go to the EventLog Analyzer console.
- Click on EventLog Analyzer Account Settings
- Click on Add Account
- Select the Cloud Type as AWS.
- Enter a Display name in the given box.
- Enter the Access Key ID and Secret Access Key of the IAM user in the given fields.
- Add CloudTrail.
    - Auto-configuration: Select the Region. EventLog Analyzer automatically creates and configures CloudTrail. Click Save.

> Note: EventLog Analyzer will create the following resources:

- S3 bucket: (accountnumber)-cloudtraillogs-(region)
- SNS topic: cloudtrailtopic
- SQS queue: cloudtrailqueue

    - SQS queue: cloudtrailqueue
    - CloudTrail: cloudtrail
  - Manual configuration: Click Connect an existing CloudTrail and follow the steps given in the Logging setup for AWS CloudTrail.

To setup logging for your AWS environment, refer S3 server access logging and ELB access logging.

Manage Cloud Sources:

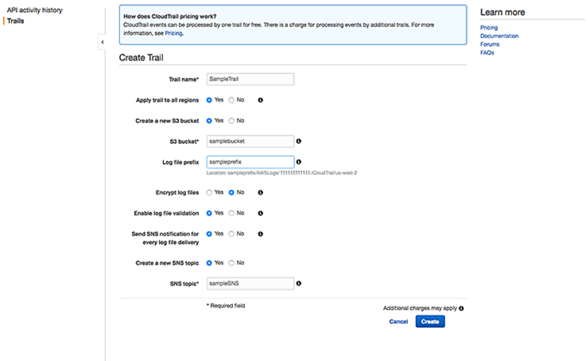
- Logging setup: Amazon CloudTrail Logs
- Logging setup: Amazon S3 server access logs
- Logging setup: Amazon ELB access logs
- Enable/disable cloud source
- Delete a cloud source

Logging setup: Amazon CloudTrail Logs

CloudTrail is an API log monitoring web service offered by AWS. It enables AWS customers to record API calls and sends these log files to Amazon S3 buckets for storage. The service provides details of API activity such as the identity of the API caller, the time of the API call, the source IP address of the API caller, the requests made and response elements returned by the AWS service. In addition, it captures a few non-API events (AWS service events and AWS console sign-in events).
CloudTrail can also be configured to publish a notification for every log file that is delivered, allowing users to take action upon log file delivery.
(I) Enable CloudTrail

- Login to the AWS console.
- Go to AWS Services → Management Tools → CloudTrail.
- Click Add new trail.
- Click Advanced and fill in the missing information.

(II) Configure an SNS topic
Create an SNS topic. Select the following options: Apply trail to all regions → Yes Create a new S3 bucket → Yes S3 bucket → Provide a new name Log file prefix → Provide the prefix Encrypt log fies → No Enable log file validation → Yes Send SMS notification for every log file delivery → Yes Create a new SNS topic → Yes New SNS topic → Name the topic Select → Create



How does CloudTrail pricing work?
CloudTrail events can be processed by one trail for free. There is a charge for processing events by additional trails. For more information, see Pricing.

Create Trail

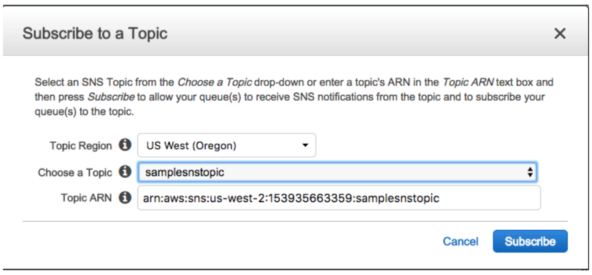
Trail name*: SampleTrail
Apply trail to all regions: ● Yes ○ No
Create a new S3 bucket: ● Yes ○ No
S3 bucket*: samplebucket
Log file prefix: sampleprefix
Location: sampleprefix/AWSLogs/ 111111111111 /CloudTrail/us-west-2
Encrypt log files: ○ Yes ● No
Enable log file validation: ● Yes ○ No
Send SNS notification for every log file delivery: ● Yes ○ No
Create a new SNS topic: ● Yes ○ No
SNS topic*: sampleSNS

* Required field

Additional charges may apply

(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.



Select an SNS Topic from the *Choose a Topic* drop-down or enter a topic's ARN in the *Topic ARN* text box and then press *Subscribe* to allow your queue(s) to receive SNS notifications from the topic and to subscribe your queue(s) to the topic.

Topic Region: US West (Oregon)

Choose a Topic: samplesnstopic

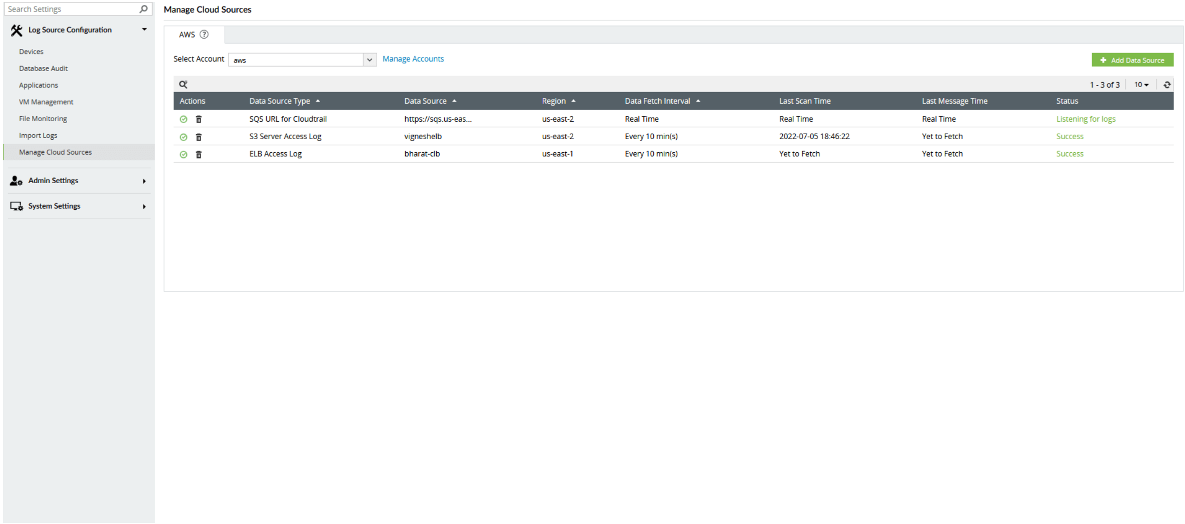
Topic ARN: arn:aws:sns:us-west-2:153935663359:samplesnstopic

Note

Amazon SNS raw message delivery needs to be disabled.

(IV) Add the created SQS queue as a data source in EventLog Analyzer

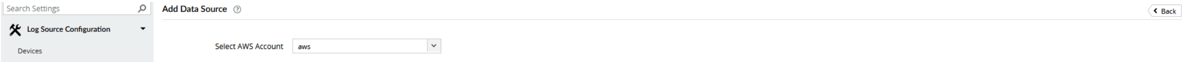
- Login to the EventLog Analyzer console.
- Go to Settings and click on Manage Data Source.



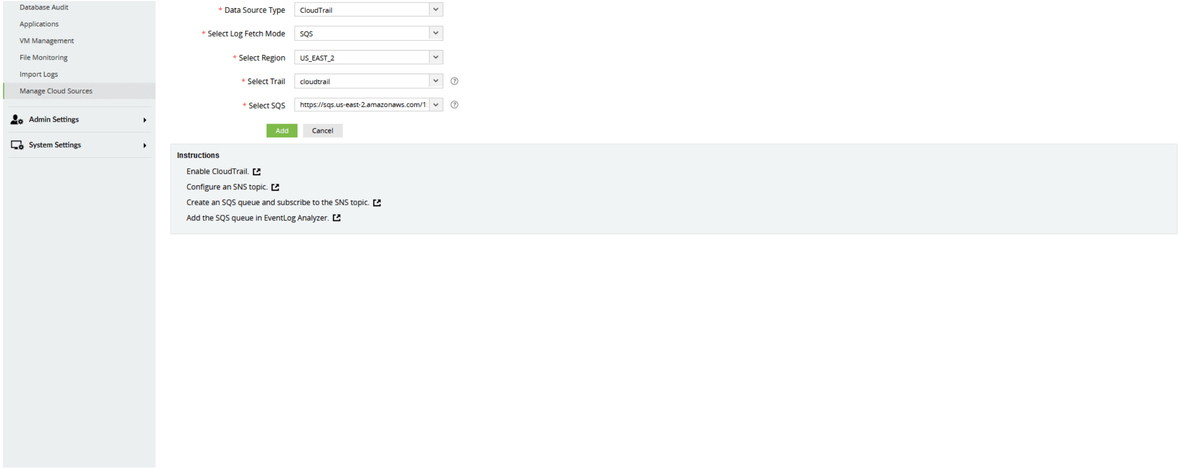
Select Account: aws

Actions	Data Source Type	Data Source	Region	Data Fetch Interval	Last Scan Time	Last Message Time	Status
	SQS URL for Cloudtrail	https://sqs.us-eas...	us-east-2	Real Time	Real Time	Real Time	Listening for logs
	S3 Server Access Log	vigneshelb	us-east-2	Every 10 min(s)	2022-07-05 18:46:22	Yet to Fetch	Success
	ELB Access Log	bharat-clb	us-east-1	Every 10 min(s)	Yet to Fetch	Yet to Fetch	Success

- Select CloudTrail from the Data source drop-down menu.
- Choose the AWS region, the trail and the SQS queue.



Select AWS Account: aws



* Data Source Type: CloudTrail

* Select Log Fetch Mode: SQS

* Select Region: US_EAST_2

* Select Trail: cloudtrail

* Select SQS: https://sqs.us-east-2.amazonaws.com/1

Instructions

Enable CloudTrail.

Configure an SNS topic.

Create an SQS queue and subscribe to the SNS topic.

Add the SQS queue in EventLog Analyzer.

- Click Save.

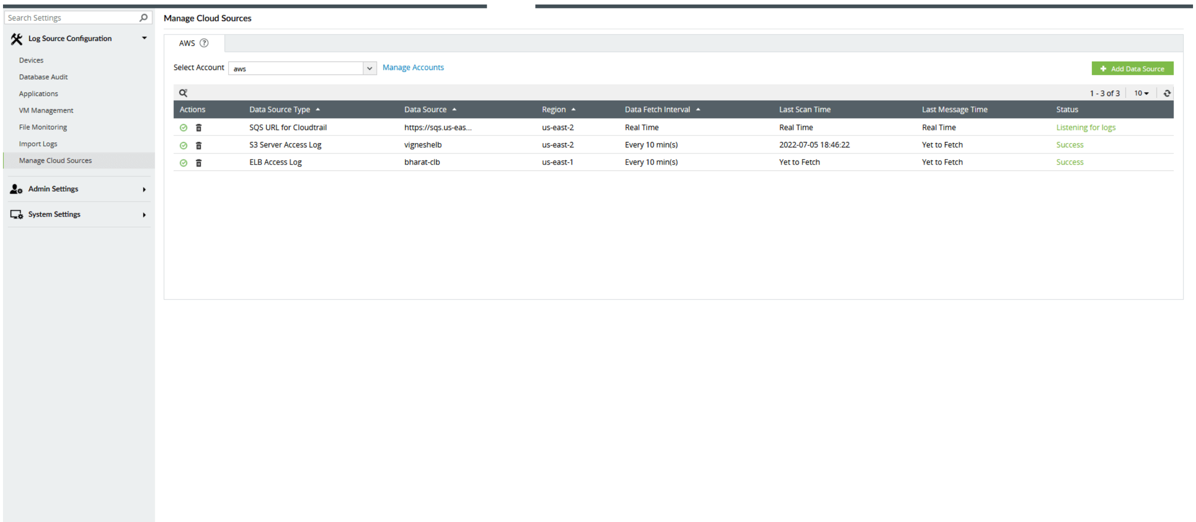
Logging Setup: Amazon S3 server access logs

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.

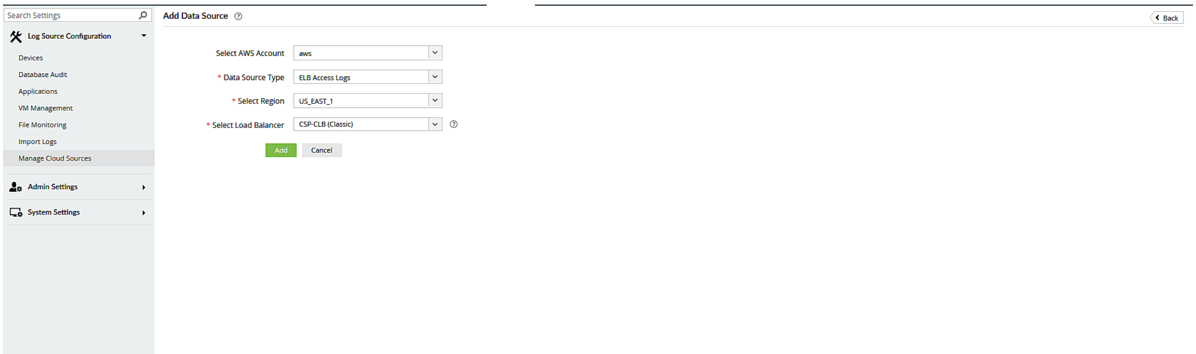


Select Account: aws

Actions	Data Source Type	Data Source	Region	Data Fetch Interval	Last Scan Time	Last Message Time	Status
✓ 🗑	SQS URL for Cloudtrail	https://sqs.us-eas...	us-east-2	Real Time	Real Time	Real Time	Listening for logs
✓ 🗑	S3 Server Access Log	vigneshelb	us-east-2	Every 10 min(s)	2022-07-05 18:46:22	Yet to Fetch	Success
✓ 🗑	ELB Access Log	bharat-clb	us-east-1	Every 10 min(s)	Yet to Fetch	Yet to Fetch	Success

- 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 AWS Account: aws

* Data Source Type: ELB Access Logs

* Select Region: US_EAST_1

* Select Load Balancer: CSP-CLB (Classic)

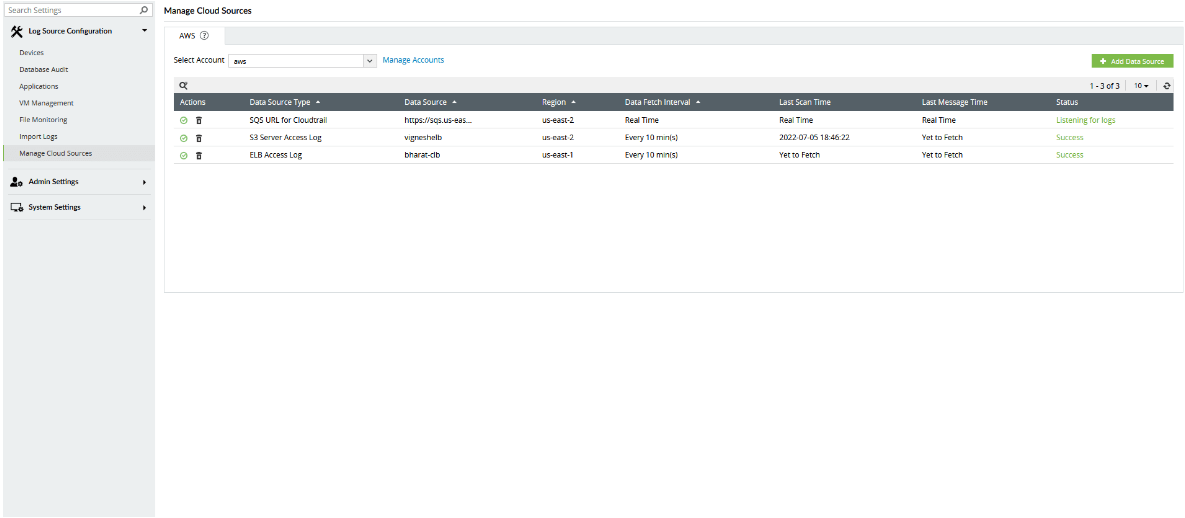
- Select the S3 Bucket for which you want to enable access logging.
- Click Configure..

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

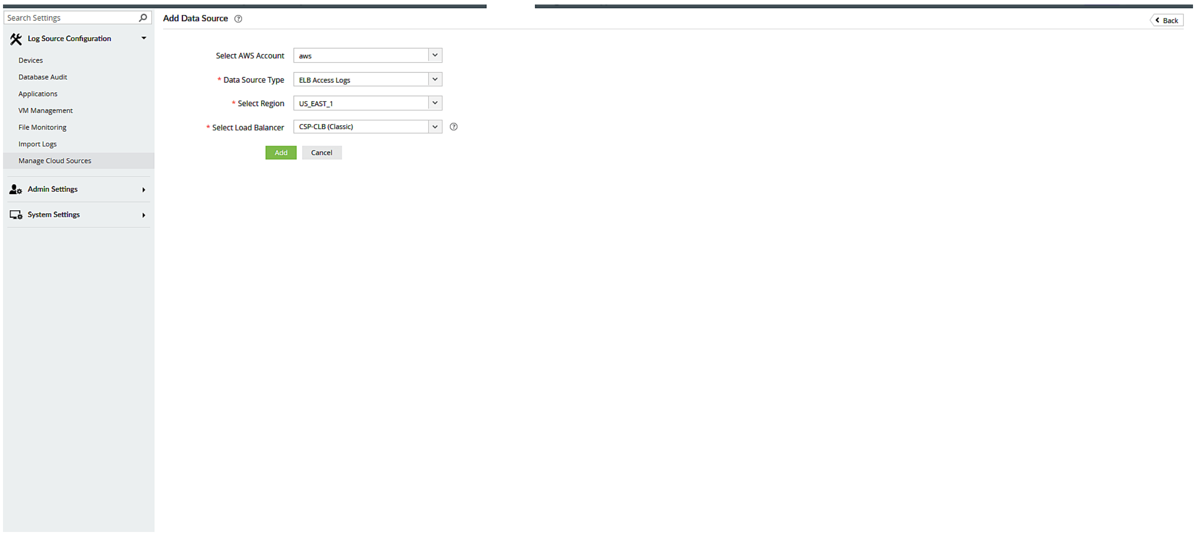
- Login to the EventLog Analyzer console.
- Go to Settings > Configuration > Manage Cloud Sources and click on Add DataSources.



Select Account: aws

Actions	Data Source Type	Data Source	Region	Data Fetch Interval	Last Scan Time	Last Message Time	Status
✓ 🗑	SQS URL for Cloudtrail	https://sqs.us-eas...	us-east-2	Real Time	Real Time	Real Time	Listening for logs
✓ 🗑	S3 Server Access Log	vigneshelb	us-east-2	Every 10 min(s)	2022-07-05 18:46:22	Yet to Fetch	Success
✓ 🗑	ELB Access Log	bharat-clb	us-east-1	Every 10 min(s)	Yet to Fetch	Yet to Fetch	Success

- 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.



Select AWS Account: aws

* Data Source Type: ELB Access Logs

* Select Region: US_EAST_1

* Select Load Balancer: CSP-CLB (Classic)

- Click Configure.

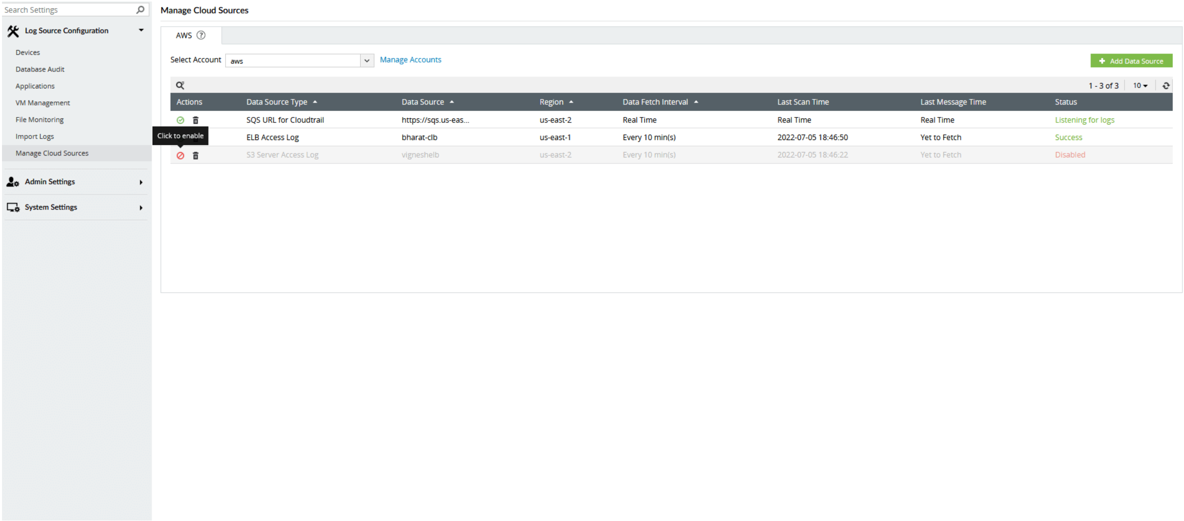
> Note
>
> Currently EventLog Analyzer only supports classic load balancers. Network and application load balancers are not supported.

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.



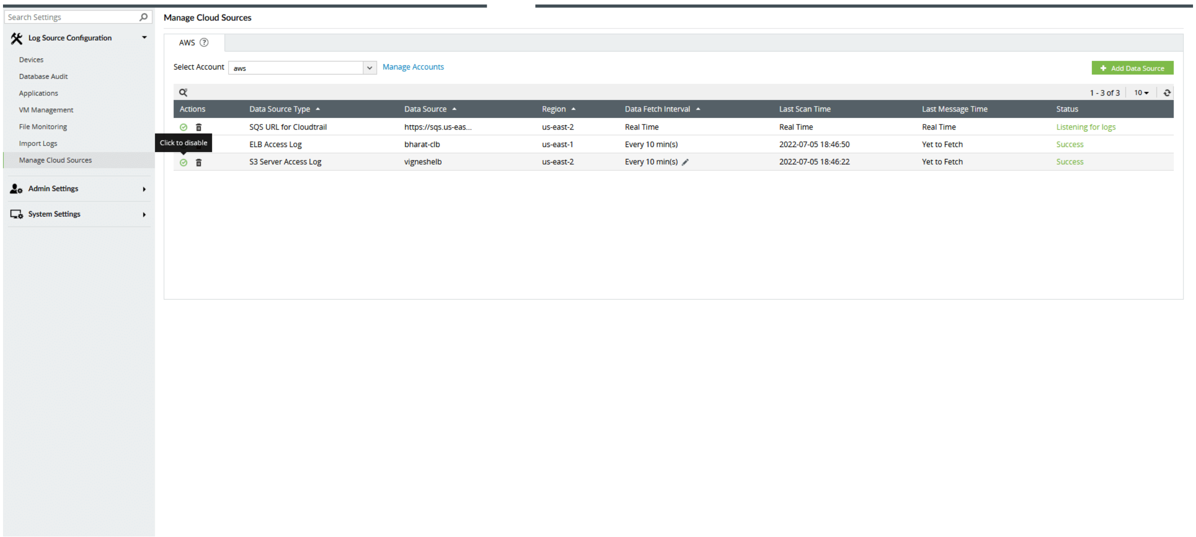
Actions	Data Source Type	Data Source	Region	Data Fetch Interval	Last Scan Time	Last Message Time	Status
✓ 🗑	SQS URL for Cloudtrail	https://sqs.us-eas...	us-east-2	Real Time	Real Time	Real Time	Listening for logs
	ELB Access Log	bharat-clb	us-east-1	Every 10 min(s)	2022-07-05 18:46:50	Yet to Fetch	Success
⊘ 🗑	S3 Server Access Log	vigneshelb	us-east-2	Every 10 min(s)	2022-07-05 18:46:22	Yet to Fetch	Disabled

- 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.



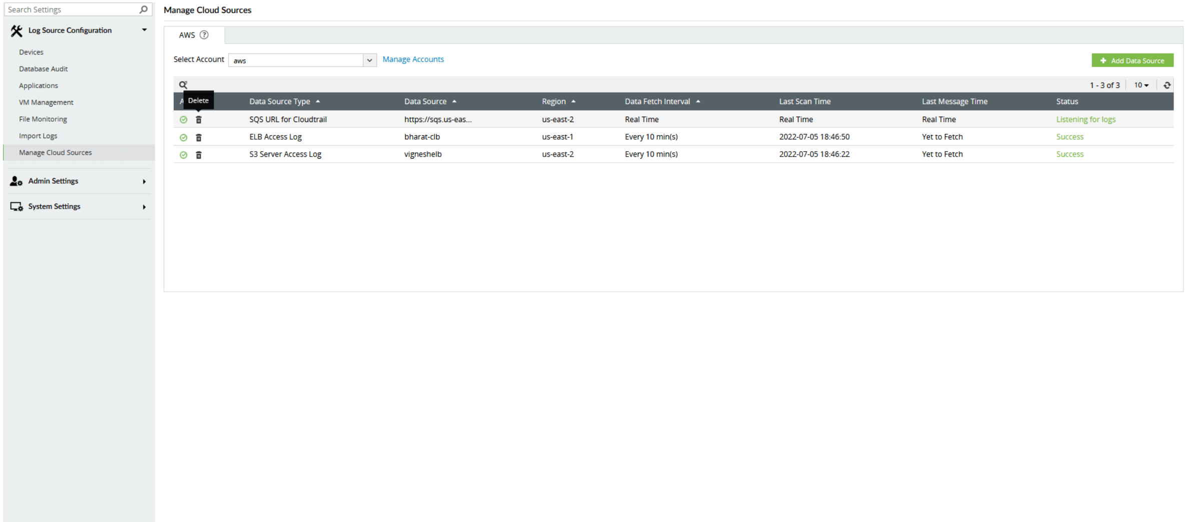
Actions	Data Source Type	Data Source	Region	Data Fetch Interval	Last Scan Time	Last Message Time	Status
✓ 🗑	SQS URL for Cloudtrail	https://sqs.us-eas...	us-east-2	Real Time	Real Time	Real Time	Listening for logs
	ELB Access Log	bharat-clb	us-east-1	Every 10 min(s)	2022-07-05 18:46:50	Yet to Fetch	Success
✓ 🗑	S3 Server Access Log	vigneshelb	us-east-2	Every 10 min(s)	2022-07-05 18:46:22	Yet to Fetch	Success

- 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.



A	Data Source Type	Data Source	Region	Data Fetch Interval	Last Scan Time	Last Message Time	Status
✓ 🗑	SQS URL for Cloudtrail	https://sqs.us-eas...	us-east-2	Real Time	Real Time	Real Time	Listening for logs
✓ 🗑	ELB Access Log	bharat-clb	us-east-1	Every 10 min(s)	2022-07-05 18:46:50	Yet to Fetch	Success
✓ 🗑	S3 Server Access Log	vigneshelb	us-east-2	Every 10 min(s)	2022-07-05 18:46:22	Yet to Fetch	Success

- The data source will be deleted.

Salesforce

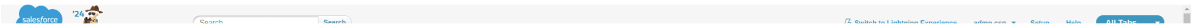
EventLog Analyzer helps you analyze Salesforce user activity within the wider context of your overall security posture. By monitoring Salesforce activities, you will be able to spot suspicious login attempts, track privileged user activity, and identify unauthorized access attempts or data modification.

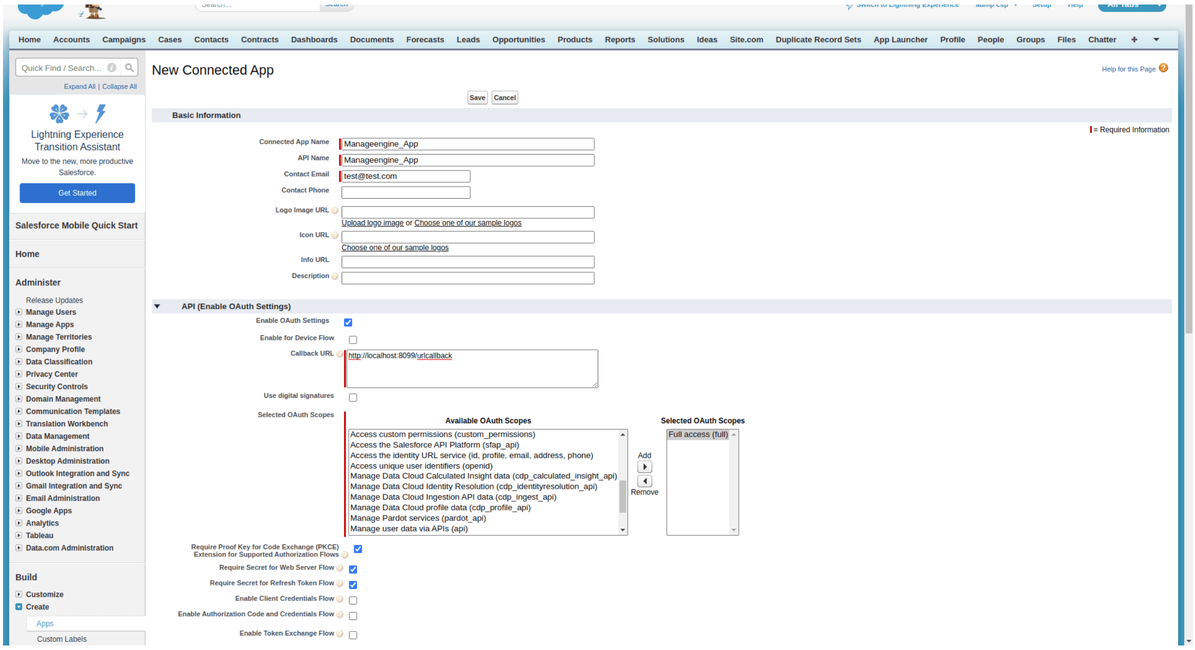
Creating a Connected App with permissions in Saleforce

- 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.





New Connected App

Basic Information

Connected App Name: Manageengine_App
API Name: Manageengine_App
Contact Email: test@test.com
Contact Phone:
Logo Image URL:
Upload logo image or Choose one of our sample logos
Icon URL:
Choose one of our sample logos
Info URL:
Description:

API (Enable OAuth Settings)

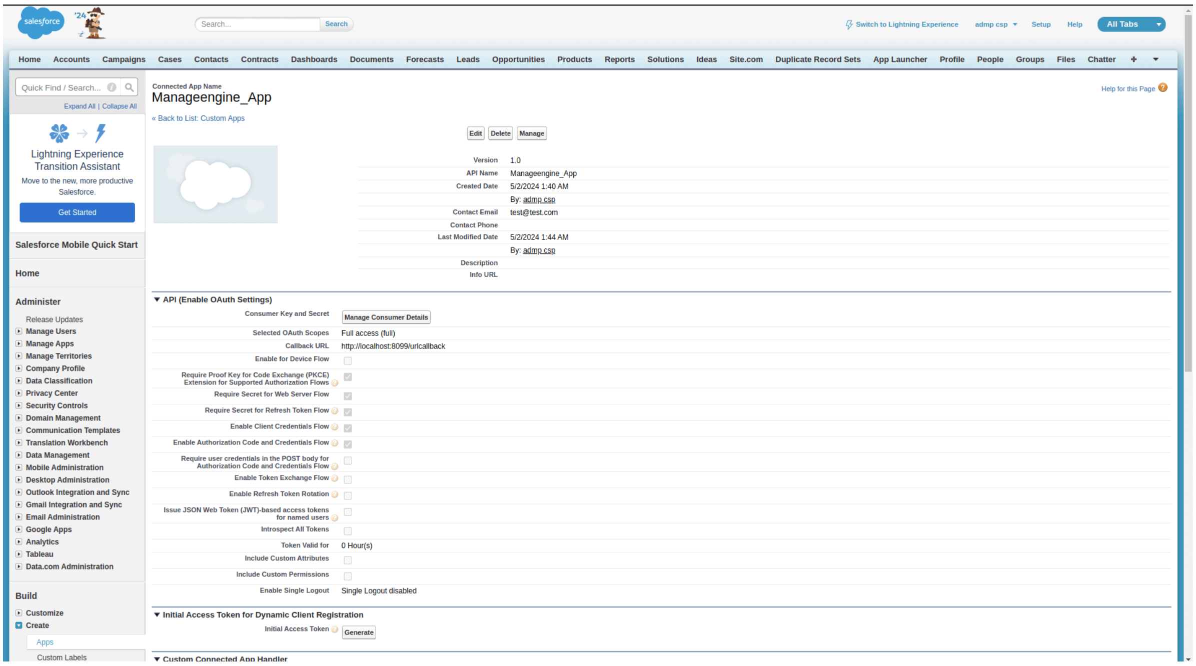
Enable OAuth Settings ☑
Enable for Device Flow □
Callback URL: http://localhost:8099/urlcallback
Use digital signatures □
Selected OAuth Scopes

Available OAuth Scopes:
Access custom permissions (custom_permissions)
Access the Salesforce API Platform (sfap_api)
Access the identity URL service (id, profile, email, address, phone)
Access unique user identifiers (openid)
Manage Data Cloud Calculated Insight data (cdp_calculated_insight_api)
Manage Data Cloud Identity Resolution (cdp_identityresolution_api)
Manage Data Cloud Ingestion API data (cdp_ingest_api)
Manage Data Cloud profile data (cdp_profile_api)
Manage Pardot services (pardot_api)
Manage user data via APIs (api)

Selected OAuth Scopes: Full access (full)

Require Proof Key for Code Exchange (PKCE) Extension for Supported Authorization Flows ☑
Require Secret for Web Server Flow ☑
Require Secret for Refresh Token Flow ☑
Enable Client Credentials Flow □
Enable Authorization Code and Credentials Flow □
Enable Token Exchange Flow □

- 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.



Connected App Name
Manageengine_App

« Back to List: Custom Apps

Version: 1.0
API Name: Manageengine_App
Created Date: 5/2/2024 1:40 AM
By: admp csp
Contact Email: test@test.com
Contact Phone:
Last Modified Date: 5/2/2024 1:44 AM
By: admp csp
Description:
Info URL:

API (Enable OAuth Settings)

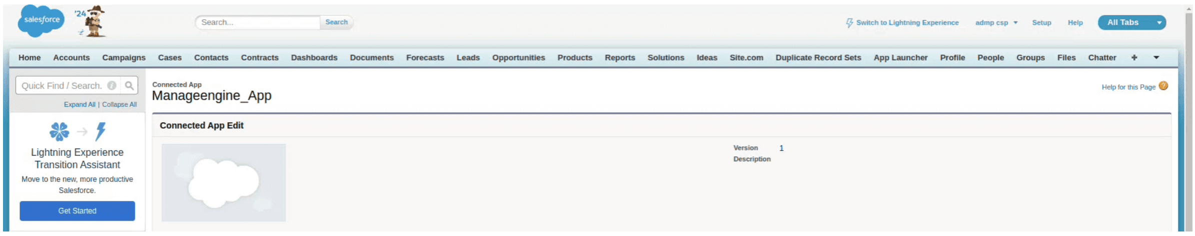
Consumer Key and Secret: Manage Consumer Details
Selected OAuth Scopes: Full access (full)
Callback URL: http://localhost:8099/urlcallback
Enable for Device Flow □
Require Proof Key for Code Exchange (PKCE) Extension for Supported Authorization Flows ☑
Require Secret for Web Server Flow ☑
Require Secret for Refresh Token Flow ☑
Enable Client Credentials Flow ☑
Enable Authorization Code and Credentials Flow ☑
Require user credentials in the POST body for Authorization Code and Credentials Flow □
Enable Token Exchange Flow □
Enable Refresh Token Rotation □
Issue JSON Web Token (JWT)-based access tokens for named users □
Introspect All Tokens □
Token Valid for: 0 Hour(s)
Include Custom Attributes □
Include Custom Permissions □
Enable Single Logout: Single Logout disabled

Initial Access Token for Dynamic Client Registration

Initial Access Token: Generate

Custom Connected App Handler

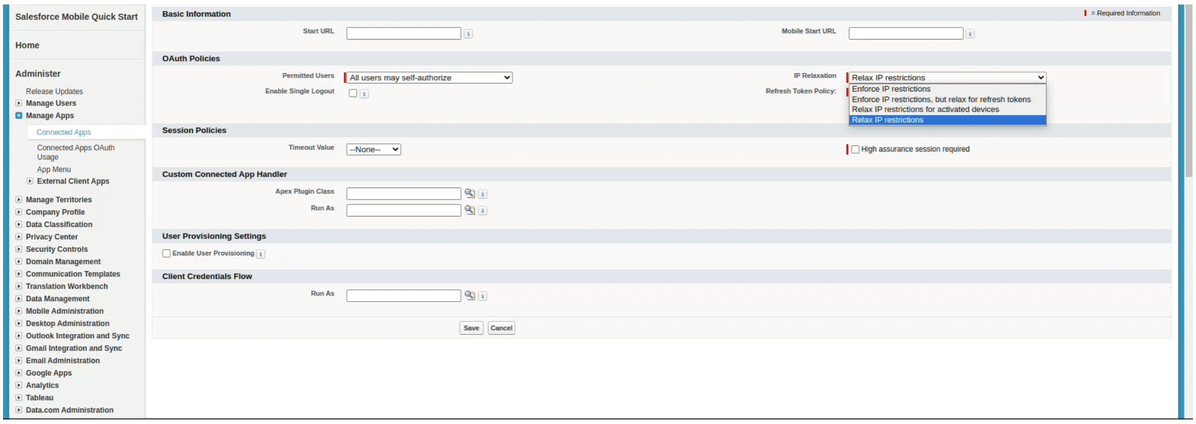
- Navigate to Setup → Administer → Manage Apps → Connected Apps .
- Click on the newly created Connected App. Under OAuth Policies > IP Relaxation, select Relax IP restrictions from the drop-down.



Connected App
Manageengine_App

Connected App Edit

Version: 1
Description:



Basic Information

Start URL:

Mobile Start URL:

OAuth Policies

Permitted Users: All users may self-authorize

Enable Single Logout: □

IP Relaxation: Relax IP restrictions

Refresh Token Policy:

Session Policies

Timeout Value: --None--

□ High assurance session required

Custom Connected App Handler

Apex Plugin Class:

Run As:

User Provisioning Settings

□ Enable User Provisioning

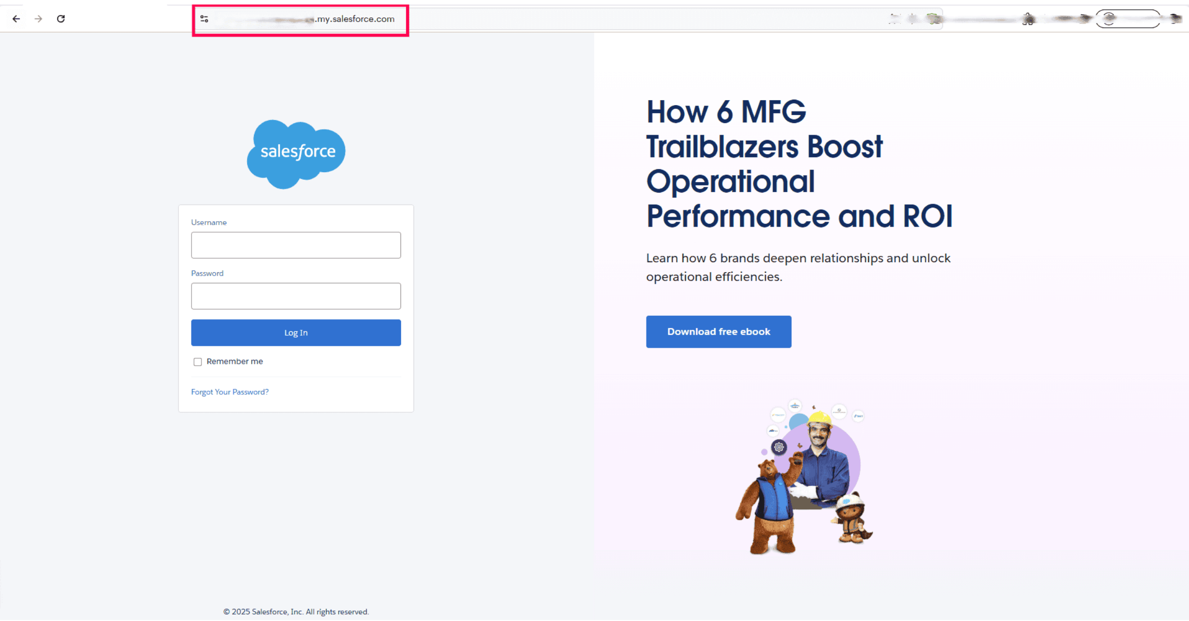
Client Credentials Flow

Run As:

- Click Save.

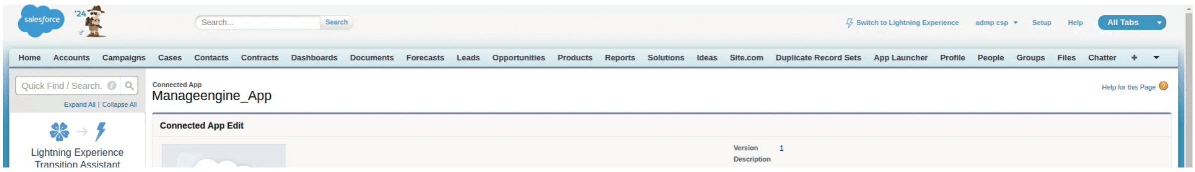
How to get the Salesforce-client-url

1. Go to the Salesforce login page and copy the URL from your browser's address bar.
2. Paste the URL in the Login URL field(e.g., https://testingtech-ap48.my.salesforce.com).


.my.salesforce.com
salesforce
Username
Password
Log In
Remember me
Forgot Your Password?
© 2025 Salesforce, Inc. All rights reserved.
How 6 MFG Trailblazers Boost Operational Performance and ROI
Learn how 6 brands deepen relationships and unlock operational efficiencies.
Download free ebook

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.



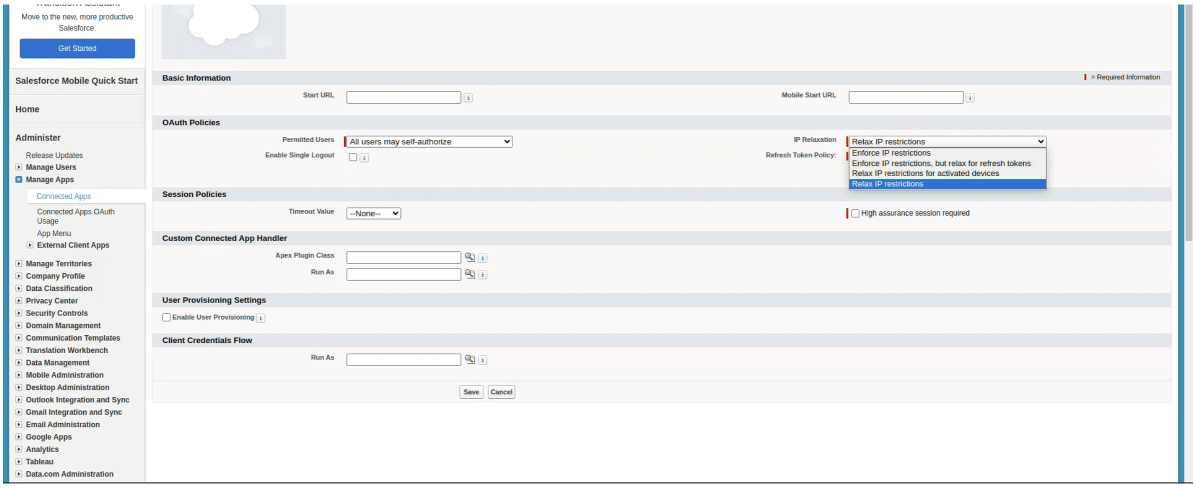
Connected App

Managengine_App

Connected App Edit

Version: 1

Description:



Basic Information | = Required Information

Start URL:

Mobile Start URL:

OAuth Policies

Permitted Users: All users may self-authorize

Enable Single Logout: □

IP Relaxation: Relax IP restrictions
- Enforce IP restrictions
- Enforce IP restrictions, but relax for refresh tokens
- Relax IP restrictions for activated devices
- Relax IP restrictions

Refresh Token Policy:

Session Policies

Timeout Value: --None--

□ High assurance session required

Custom Connected App Handler

Apex Plugin Class:

Run As:

User Provisioning Settings

□ Enable User Provisioning

Client Credentials Flow

Run As:

2.1.1. User Interface Tabs

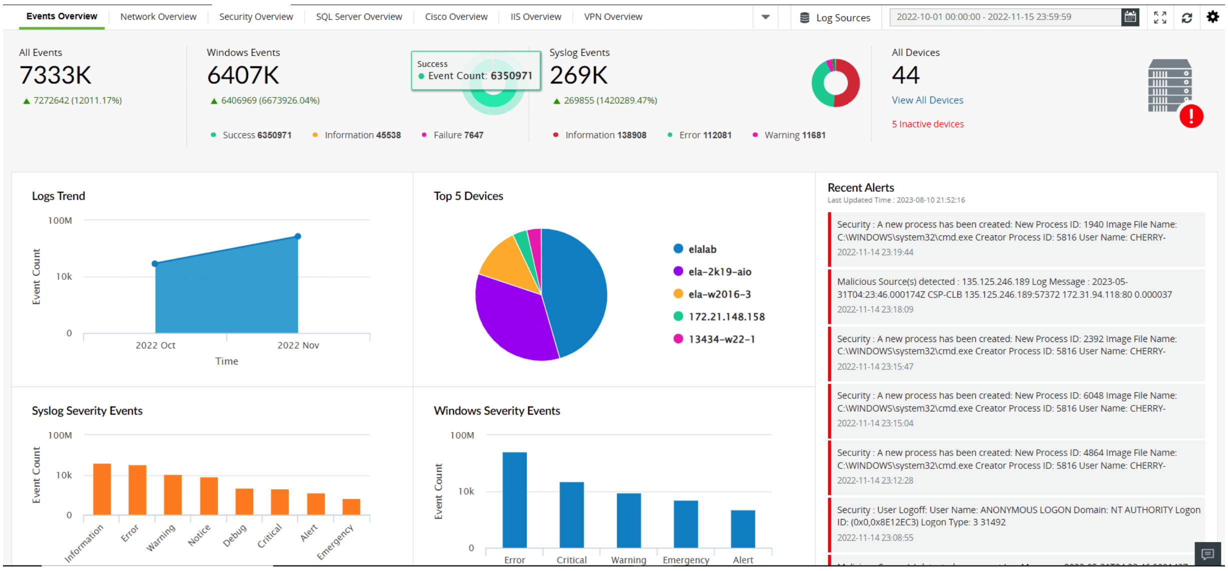
Last updated on: September 12, 2025

EventLog Analyzer's user interface tabs help you navigate to different sections of the product. The tabs include:

Dashboard tab

The Dashboard tab contains multiple dashboards that give you insights into important network activities. The below dashboards are present by default when you click on the Dashboard tab:

- Events Overview
- Network Overview
- Security Overview
- VPN Overview
- Incident Overview



Security : A new process has been created: New Process ID: 1940 Image File Name: C:\WINDOWS\system32\cmd.exe Creator Process ID: 5816 User Name: CHERRY-
2022-11-14 23:19:44

Malicious Source(s) detected : 135.125.246.189 Log Message : 2023-05-31T04:23:46.000174Z CSP-CLB 135.125.246.189:57372 172.31.94.118:80 0.000037
2022-11-14 23:18:09

Security : A new process has been created: New Process ID: 2392 Image File Name: C:\WINDOWS\system32\cmd.exe Creator Process ID: 5816 User Name: CHERRY-
2022-11-14 23:15:47

Security : A new process has been created: New Process ID: 6048 Image File Name: C:\WINDOWS\system32\cmd.exe Creator Process ID: 5816 User Name: CHERRY-
2022-11-14 23:15:04

Security : A new process has been created: New Process ID: 4864 Image File Name: C:\WINDOWS\system32\cmd.exe Creator Process ID: 5816 User Name: CHERRY-
2022-11-14 23:12:28

Security : User Logoff: User Name: ANONYMOUS LOGON Domain: NT AUTHORITY Logon ID: (0x0,0x8E12EC3) Logon Type: 3 31492
2022-11-14 23:08:55

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

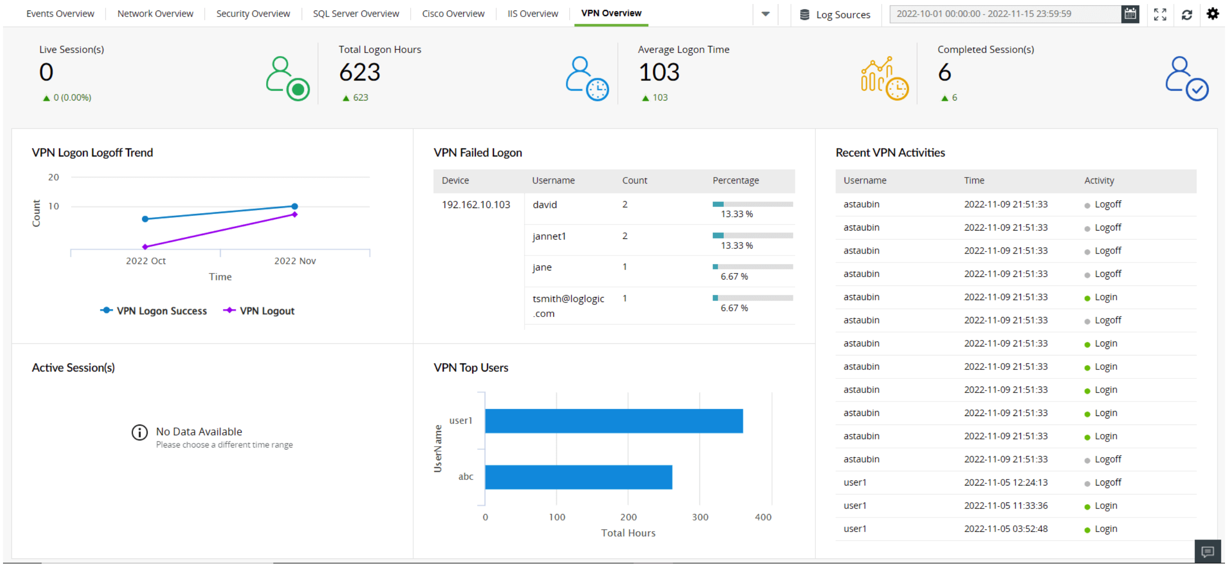
This tab gives you information about network traffic in your environment. It provides details on the traffic trend, allowed and denied network connections, and more to help you track events of interest.

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.



Live Session(s)
0
▲ 0 (0.00%)

Total Logon Hours
623
▲ 623

Average Logon Time
103
▲ 103

Completed Session(s)
6
▲ 6

VPN Failed Logon

Device	Username	Count	Percentage
192.162.10.103	david	2	13.33 %
	jannet1	2	13.33 %
	jane	1	6.67 %
	tsmith@loglogic.com	1	6.67 %

Active Session(s)

No Data Available
Please choose a different time range

Recent VPN Activities

Username	Time	Activity
astaubin	2022-11-09 21:51:33	● Logoff
astaubin	2022-11-09 21:51:33	● Logoff
astaubin	2022-11-09 21:51:33	● Logoff
astaubin	2022-11-09 21:51:33	● Logoff
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Logoff
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Logoff
user1	2022-11-05 12:24:13	● Logoff
user1	2022-11-05 11:33:36	● Login
user1	2022-11-05 03:52:48	● Login

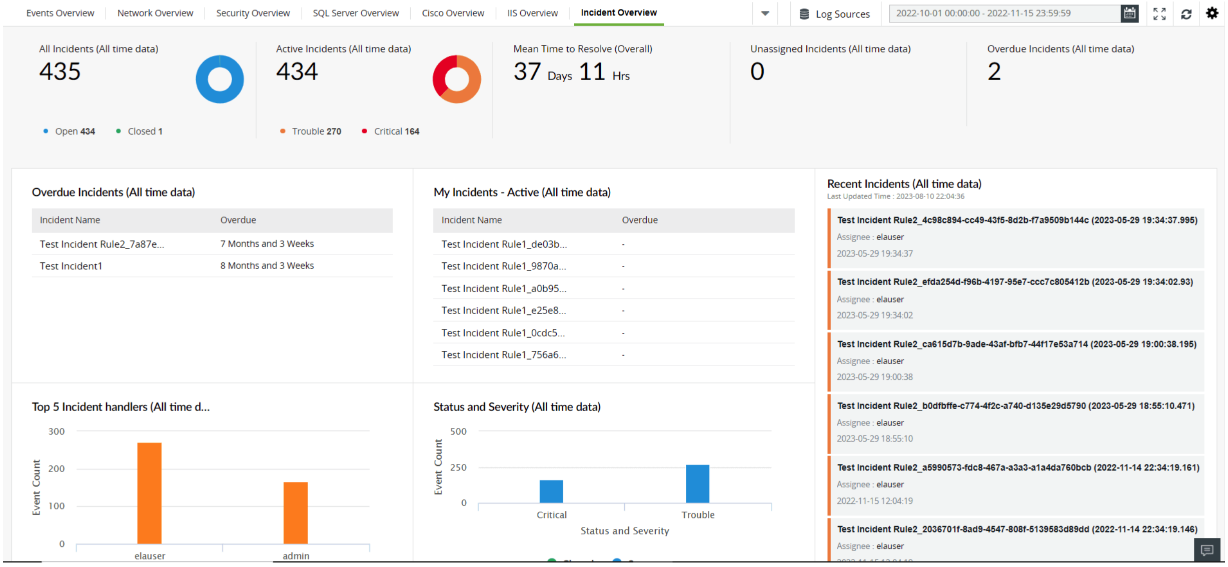
Incident Overview

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

- User-specific mean time to resolve the incidents.

> Note
>
> mean time to resolve refers to the average time taken to resolve an incident.



All Incidents (All time data) 435 — Open 434, Closed 1

Active Incidents (All time data) 434 — Trouble 270, Critical 164

Mean Time to Resolve (Overall) 37 Days 11 Hrs

Unassigned Incidents (All time data) 0

Overdue Incidents (All time data) 2

Overdue Incidents (All time data)

Incident Name	Overdue
Test Incident Rule2_7a87e...	7 Months and 3 Weeks
Test Incident1	8 Months and 3 Weeks

My Incidents - Active (All time data)

Incident Name	Overdue
Test Incident Rule1_de03b...	-
Test Incident Rule1_9870a...	-
Test Incident Rule1_a0b95...	-
Test Incident Rule1_e25e8...	-
Test Incident Rule1_0cdc5...	-
Test Incident Rule1_756a6...	-

Recent Incidents (All time data)
Last Updated Time : 2023-08-10 22:04:36

Test Incident Rule2_4c98c894-cc49-43f5-8d2b-f7a9509b144c (2023-05-29 19:34:37.995)
Assignee : elauser
2023-05-29 19:34:37

Test Incident Rule2_efda254d-f96b-4197-95e7-ccc7c805412b (2023-05-29 19:34:02.93)
Assignee : elauser
2023-05-29 19:34:02

Test Incident Rule2_ca615d7b-9ade-43af-bfb7-44f17e53a714 (2023-05-29 19:00:38.195)
Assignee : elauser
2023-05-29 19:00:38

Test Incident Rule2_b0dfbffe-c774-4f2c-a740-d135e29d5790 (2023-05-29 18:55:10.471)
Assignee : elauser
2023-05-29 18:55:10

Test Incident Rule2_a5990573-fdc8-467a-a3a3-a1a4da760bcb (2022-11-14 22:34:19.161)
Assignee : elauser
2022-11-15 12:04:19

Test Incident Rule2_2036701f-8ad9-4547-808f-5139583d89dd (2022-11-14 22:34:19.146)
Assignee : elauser

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.

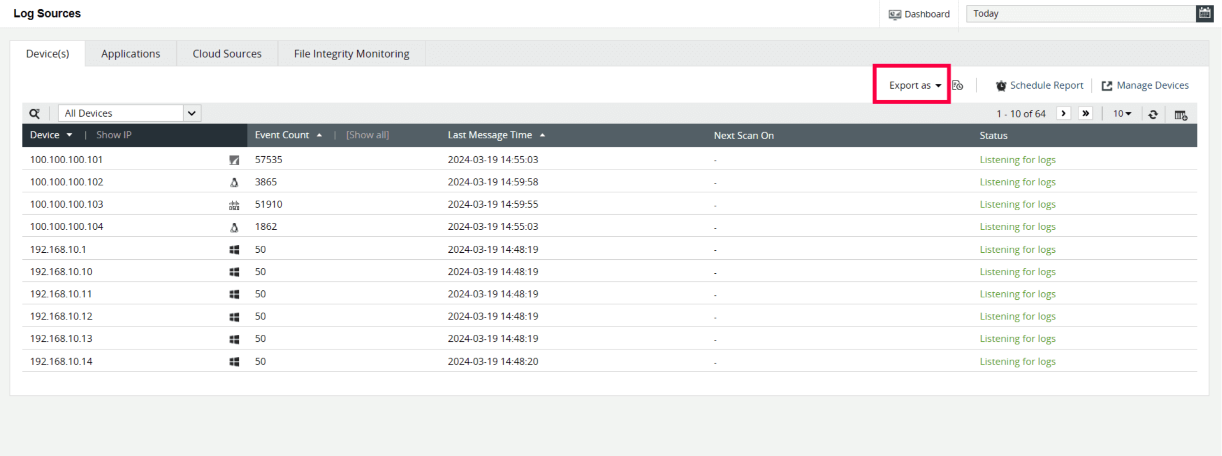
You can even customize the columns you would like to display in the device table by clicking the column selector icon or increase the number of devices that are displayed per page (from a minimum of 5 devices per page to a maximum of 200 devices per page). Using the drop down menu, you can list out only 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.



Device | Show IP	Event Count | [Show all]	Last Message Time	Next Scan On	Status
100.100.100.101	57535	2024-03-19 14:55:03	-	Listening for logs
100.100.100.102	3865	2024-03-19 14:59:58	-	Listening for logs
100.100.100.103	51910	2024-03-19 14:59:55	-	Listening for logs
100.100.100.104	1862	2024-03-19 14:55:03	-	Listening for logs
192.168.10.1	50	2024-03-19 14:48:19	-	Listening for logs
192.168.10.10	50	2024-03-19 14:48:19	-	Listening for logs
192.168.10.11	50	2024-03-19 14:48:19	-	Listening for logs
192.168.10.12	50	2024-03-19 14:48:19	-	Listening for logs
192.168.10.13	50	2024-03-19 14:48:19	-	Listening for logs
192.168.10.14	50	2024-03-19 14:48:20	-	Listening for logs

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

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

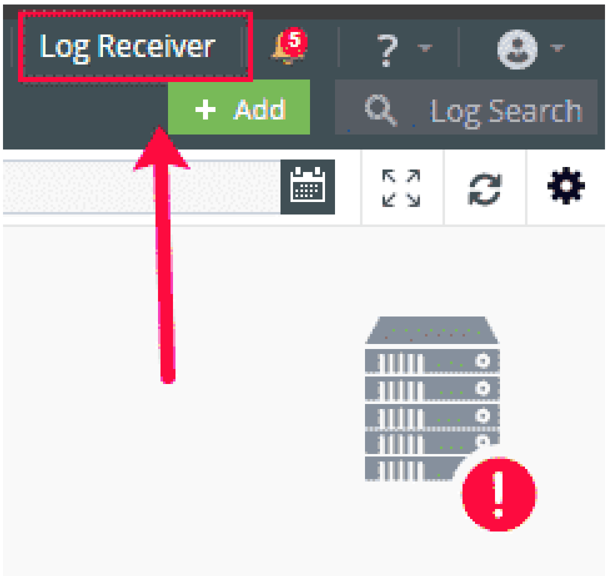
This tab allows you to easily add log sources from Devices and Applications. It also has the provision to let you import logs from other sources. You can add Alert Profiles, Log Filters and create custom Reports from this tab.

2.1.2. Log Receiver

Last updated on: September 12, 2025

In this page

EventLog Analyzer includes a functionality called Log Receiver which is a packet capturing tool that displays real-time packets being received at a specified port.
It helps the security analysts by providing supplementary information like live logs being received, and the details related to the server such as server-name,TCP ports and IP address where EventLog Analyzer is set up. (Refer Fig 1)



The Log Receiver tab comes with two default sub-tabs:

1. Syslog Viewer
2. Server Details

Syslog Viewer

The Syslog Viewer tab showcases real-time logs that are currently being forwarded to the EventLog Analyzer server through the default ports (513, 514).

Note

- The list shows the live packets being received at the specified port in your machine. This does not guarantee that EventLog Analyzer has received the Syslog packets.
- The Log Receiver will listen for logs for up to three minutes or until 1000 packets are received.

After reaching this limit, the Log Receiver requires a manual restart to resume listening. Click on Start Listening to resume the process. The option to restart is available under the Syslog Viewer tab.

Point 1: Receiving Syslog packets 280 Packets received. Stop Listening-

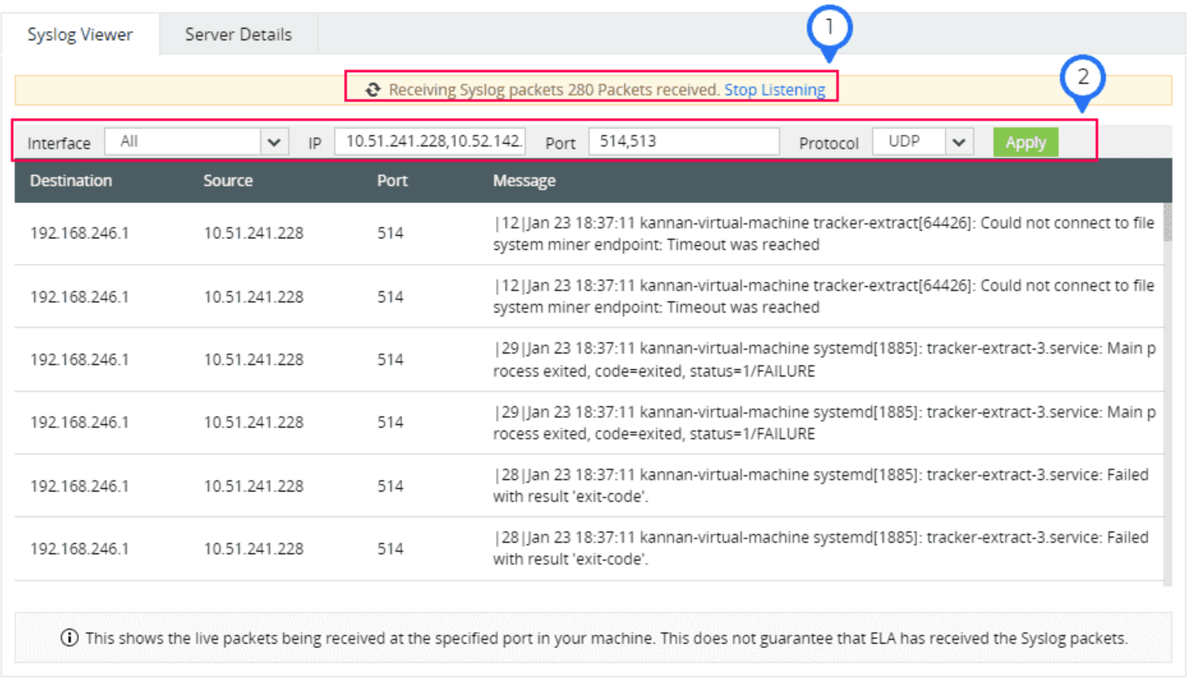
It indicates the log count received and the status, specifying whether the product is actively listening to the logs or not. It can be halted and restarted as needed. (Refer Fig 2)

Point 2 - Apply

It indicates the configurations that can be adjusted to display the live logs received on the server. You can find the associated details below:

- Interface - It showcases all available network interfaces on the EventLog Analyzer server machine. To examine live logs for a specific interface, you can choose it from the dropdown box. Otherwise, it can be left as "All."
- IP - To verify whether logs from a specific device are received on the server machine, enter the IP address of the machines forwarding logs to EventLog Analyzer. For multiple devices, input their IP addresses with comma-separated values. To check for all devices, leave the field blank.
- Port - Specify the ports to which the logs are being forwarded to the EventLog Analyzer Server.The logs are forwarded to the EventLog Analyzer Server by default on ports 513 or 514.
- Protocol - You can specify the protocol as either UDP or TCP.

Click "Apply" to verify the logs received by the EventLog Analyzer server. The logs will be presented with details such as source IP, destination IP, port, and accompanied by the respective messages.



Receiving Syslog packets 280 Packets received. Stop Listening

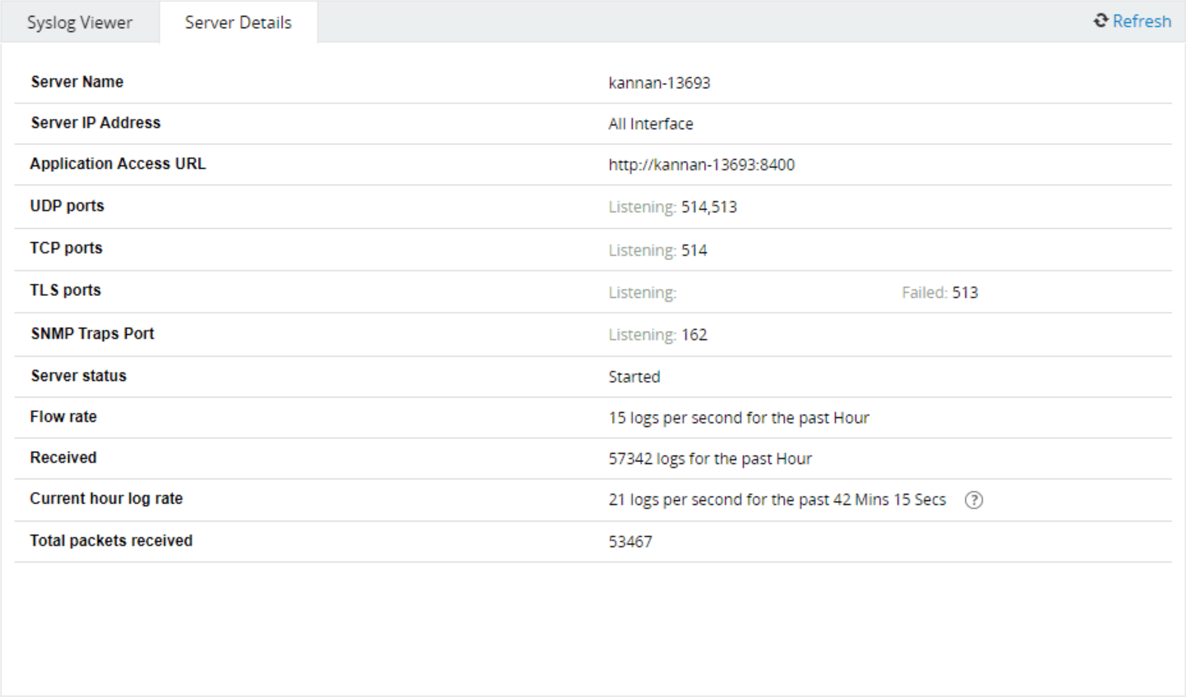
Interface All IP 10.51.241.228,10.52.142. Port 514,513 Protocol UDP

Destination	Source	Port	Message
192.168.246.1	10.51.241.228	514	|12|Jan 23 18:37:11 kannan-virtual-machine tracker-extract[64426]: Could not connect to file system miner endpoint: Timeout was reached
192.168.246.1	10.51.241.228	514	|12|Jan 23 18:37:11 kannan-virtual-machine tracker-extract[64426]: Could not connect to file system miner endpoint: Timeout was reached
192.168.246.1	10.51.241.228	514	|29|Jan 23 18:37:11 kannan-virtual-machine systemd[1885]: tracker-extract-3.service: Main p rocess exited, code=exited, status=1/FAILURE
192.168.246.1	10.51.241.228	514	|29|Jan 23 18:37:11 kannan-virtual-machine systemd[1885]: tracker-extract-3.service: Main p rocess exited, code=exited, status=1/FAILURE
192.168.246.1	10.51.241.228	514	|28|Jan 23 18:37:11 kannan-virtual-machine systemd[1885]: tracker-extract-3.service: Failed with result 'exit-code'.
192.168.246.1	10.51.241.228	514	|28|Jan 23 18:37:11 kannan-virtual-machine systemd[1885]: tracker-extract-3.service: Failed with result 'exit-code'.

ⓘ This shows the live packets being received at the specified port in your machine. This does not guarantee that ELA has received the Syslog packets.

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)



Server Name	kannan-13693	
Server IP Address	All Interface	
Application Access URL	http://kannan-13693:8400	
UDP ports	Listening: 514,513	
TCP ports	Listening: 514	
TLS ports	Listening:	Failed: 513
SNMP Traps Port	Listening: 162	
Server status	Started	
Flow rate	15 logs per second for the past Hour	
Received	57342 logs for the past Hour	
Current hour log rate	21 logs per second for the past 42 Mins 15 Secs ?	
Total packets received	53467	

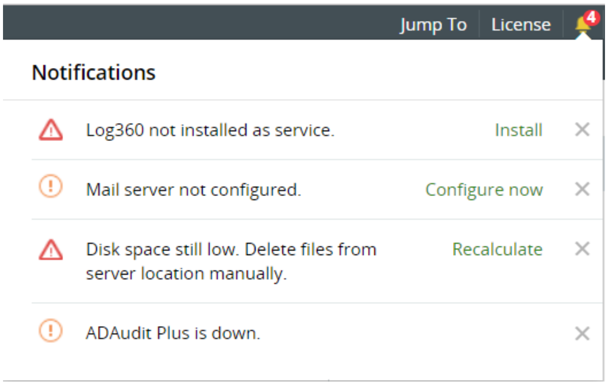
1. Server Name - The name of the current server or machine where EventLog Analyzer is installed.
2. Server IP Address - It indicates the network adapter linked to EventLog Analyzer; if none is specified, it displays "All Interface."
3. Application Access URL - The URL utilized for accessing the EventLog 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

2.1.3. Notification Center

Last updated on: September 12, 2025

Log360 delivers instant alerts and notifications on any event that requires your attention. These alerts can be accessed from anywhere within the product.

Click the 🔔 icon in the top right corner of the screen to view alerts from the product.



Notifications

Log360 not installed as service. Install

Mail server not configured. Configure now

Disk space still low. Delete files from server location manually. Recalculate

ADAudit Plus is down.

Alert generating events in Log360

- Reminder to install Log360 as a service.
- Reminder to configure mail server to receive mail notifications.
- Low disk space alert.
- Component down-time alert.

Manage Alerts

Log360 allows administrators to easily manage alerts, either by making the process of resolution simpler or by deleting alerts that you feel are not important.

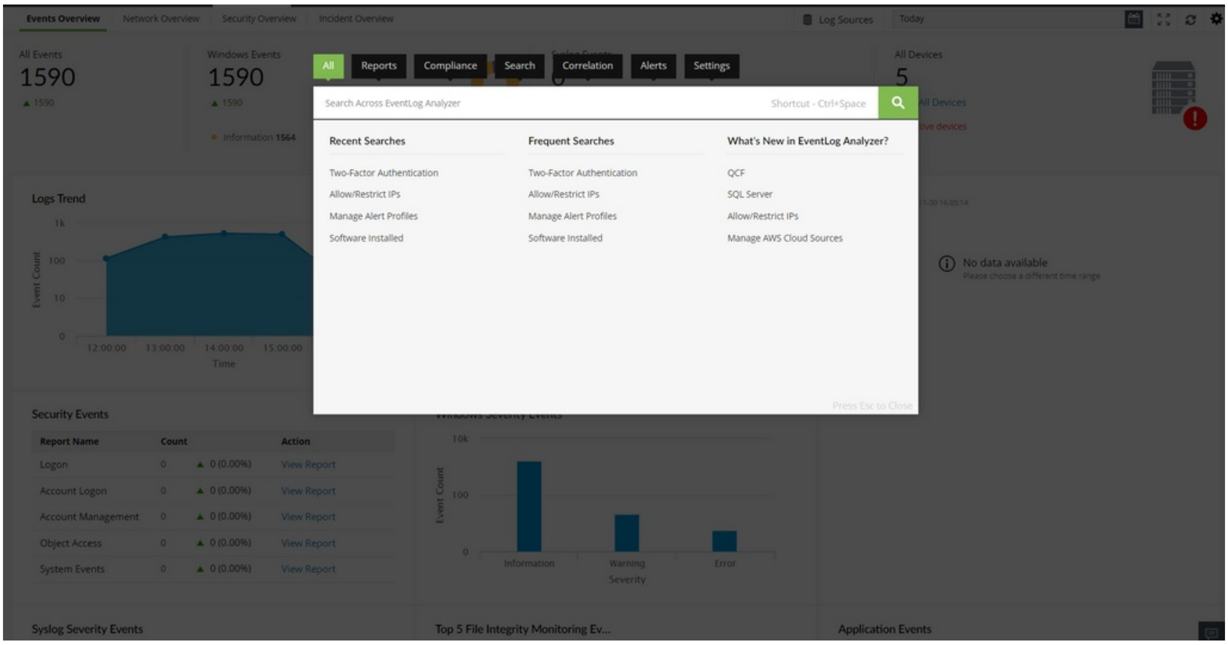
- To resolve, click on the action link corresponding to the alert. You will be directed to the screen where changes have to be made.
- To delete, click the ✕ icon to hide the alert from your notification tray.

2.1.4. Global Search

Last updated on: September 12, 2025

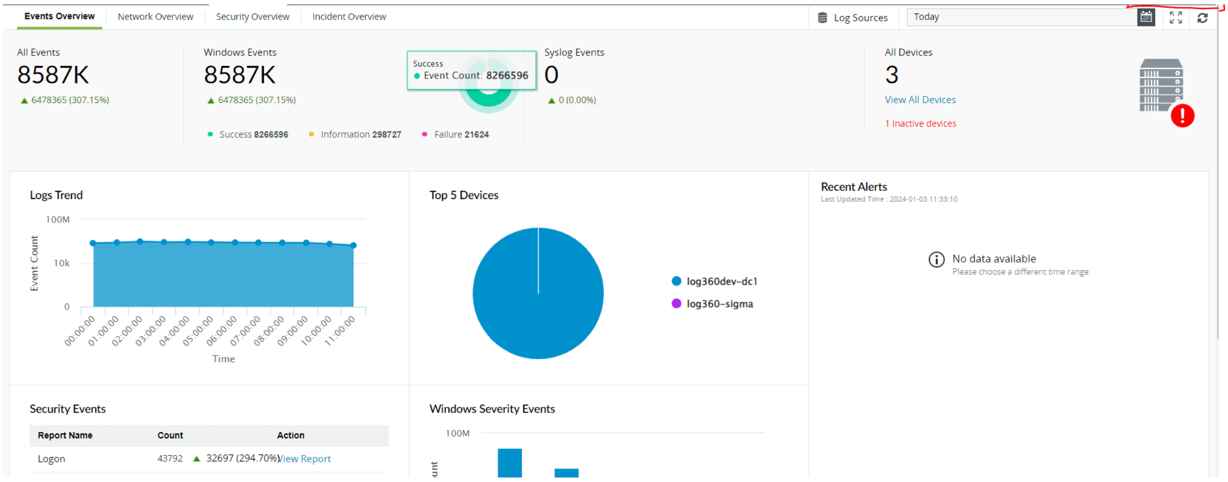
The global search feature can be used to search across all sections of EventLog Analyzer including Reports, Compliance, Correlation, Alerts, and Settings. This will help in finding particular sections of the product faster, and improves productivity of the SOC team.

For instance, to search for reports related to Windows, type "Windows" in the global search bar. All relevant Reports, and Settings will be displayed in the search screen. This feature can also provide quick access to particular compliance mandates such as HIPAA and PCI-DSS.



Report Name	Count	Action
Logon	0 ▲ 0 (0.00%)	View Report
Account Logon	0 ▲ 0 (0.00%)	View Report
Account Management	0 ▲ 0 (0.00%)	View Report
Object Access	0 ▲ 0 (0.00%)	View Report
System Events	0 ▲ 0 (0.00%)	View Report

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.



Report Name	Count	Action
Logon	43792 ▲ 32697 (294.70%)	View Report

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.

2.2.1. User Interface Tabs

Last updated on: September 12, 2025

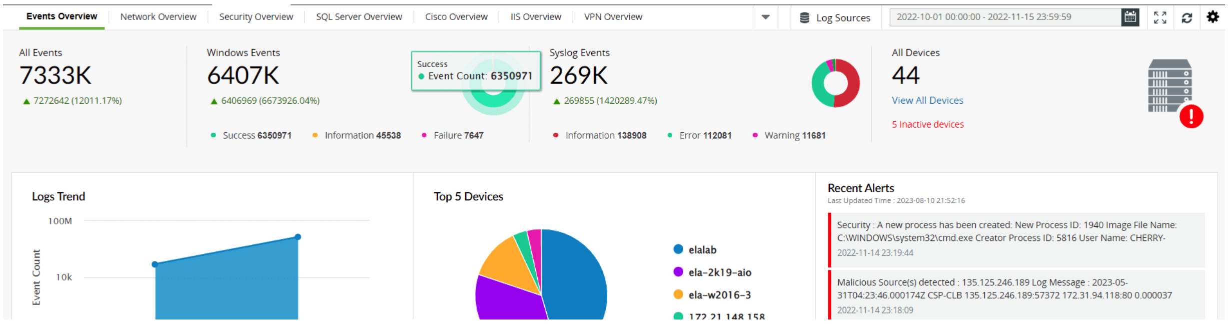
In this page

EventLog Analyzer's user interface tabs help you navigate to different sections of the product. The tabs include:

Dashboard tab

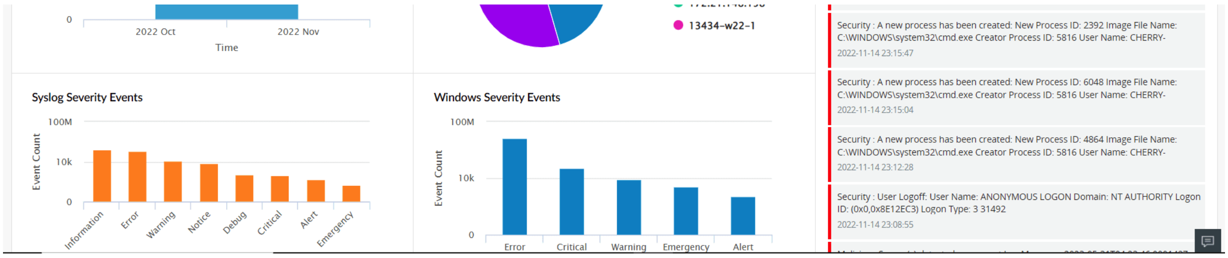
The Dashboard tab contains multiple dashboards that give you insights into important network activities. The below dashboards are present by default when you click on the Dashboard tab:

- Events Overview
- Network Overview
- Security Overview
- VPN Overview
- Incident Overview



Security : A new process has been created: New Process ID: 1940 Image File Name: C:\WINDOWS\system32\cmd.exe Creator Process ID: 5816 User Name: CHERRY-
2022-11-14 23:19:44

Malicious Source(s) detected : 135.125.246.189 Log Message : 2023-05-31T04:23:46.000174Z CSP-CLB 135.125.246.189:57372 172.31.94.118:80 0.000037
2022-11-14 23:18:09



Security : A new process has been created: New Process ID: 2392 Image File Name: C:\WINDOWS\system32\cmd.exe Creator Process ID: 5816 User Name: CHERRY-
2022-11-14 23:15:47

Security : A new process has been created: New Process ID: 6048 Image File Name: C:\WINDOWS\system32\cmd.exe Creator Process ID: 5816 User Name: CHERRY-
2022-11-14 23:15:04

Security : A new process has been created: New Process ID: 4864 Image File Name: C:\WINDOWS\system32\cmd.exe Creator Process ID: 5816 User Name: CHERRY-
2022-11-14 23:12:28

Security : User Logoff: User Name: ANONYMOUS LOGON Domain: NT AUTHORITY Logon ID: (0x0,0x8E12EC3) Logon Type: 3 31492
2022-11-14 23:08:55

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.

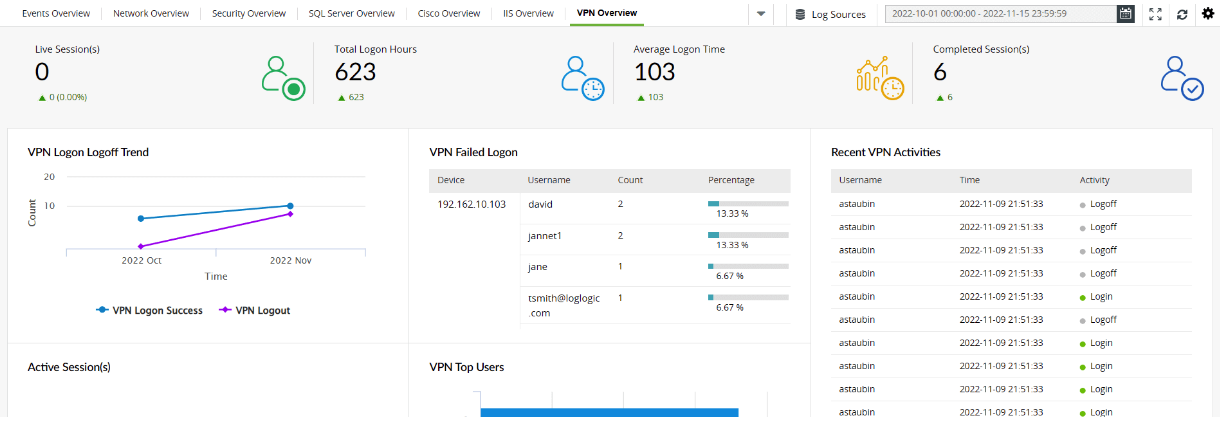
Security Overview

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.

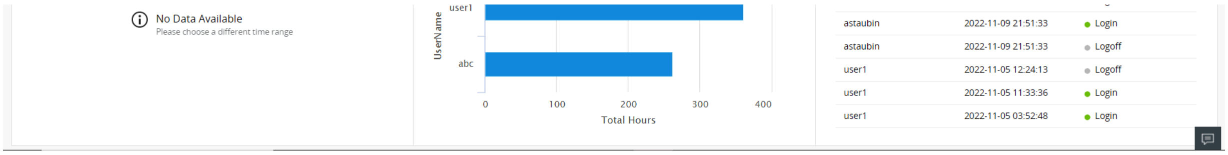


VPN Failed Logon

Device	Username	Count	Percentage
192.162.10.103	david	2	13.33 %
	jannet1	2	13.33 %
	jane	1	6.67 %
	tsmith@loglogic.com	1	6.67 %

Recent VPN Activities

Username	Time	Activity
astaubin	2022-11-09 21:51:33	● Logoff
astaubin	2022-11-09 21:51:33	● Logoff
astaubin	2022-11-09 21:51:33	● Logoff
astaubin	2022-11-09 21:51:33	● Logoff
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Logoff
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Login


No Data Available
Please choose a different time range

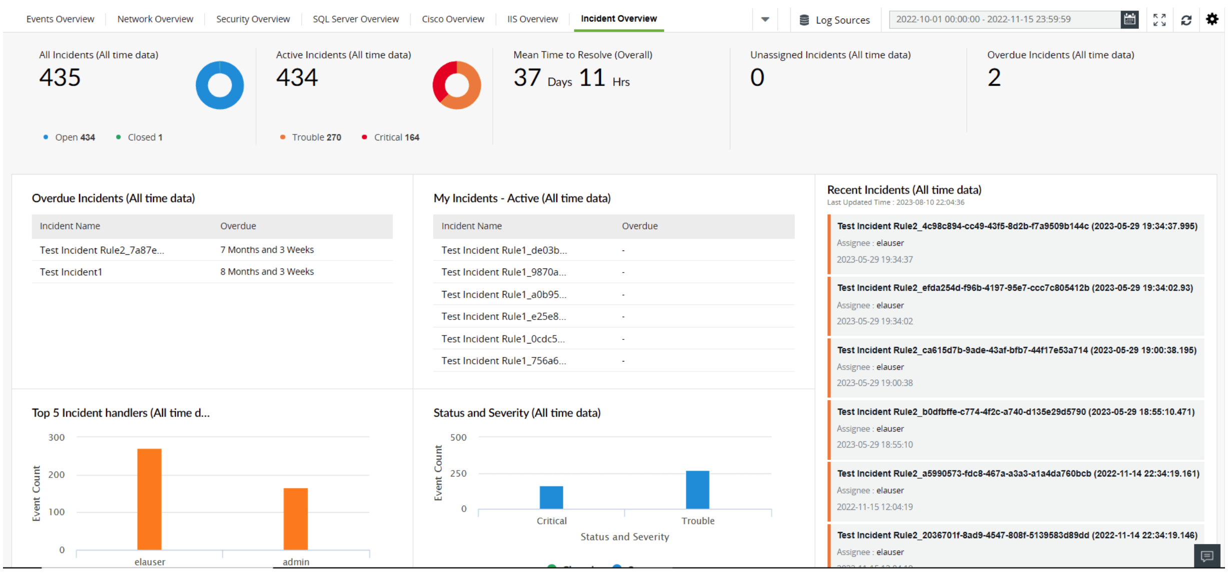
astaubin	2022-11-09 21:51:33	● Login
astaubin	2022-11-09 21:51:33	● Logoff
user1	2022-11-05 12:24:13	● Logoff
user1	2022-11-05 11:33:36	● Login
user1	2022-11-05 03:52:48	● Login

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.



2022-10-01 00:00:00 - 2022-11-15 23:59:59

All Incidents (All time data)
435
● Open 434 ● Closed 1

Active Incidents (All time data)
434
● Trouble 270 ● Critical 164

Mean Time to Resolve (Overall)
37 Days 11 Hrs

Unassigned Incidents (All time data)
0

Overdue Incidents (All time data)
2

Overdue Incidents (All time data)

Incident Name	Overdue
Test Incident Rule2_7a87e...	7 Months and 3 Weeks
Test Incident1	8 Months and 3 Weeks

My Incidents - Active (All time data)

Incident Name	Overdue
Test Incident Rule1_de03b...	-
Test Incident Rule1_9870a...	-
Test Incident Rule1_a0b95...	-
Test Incident Rule1_e25e8...	-
Test Incident Rule1_0cdc5...	-
Test Incident Rule1_756a6...	-

Recent Incidents (All time data)
Last Updated Time : 2023-08-10 22:04:36

Test Incident Rule2_4c98c894-cc49-43f5-8d2b-f7a9509b144c (2023-05-29 19:34:37.995)
Assignee : elauser
2023-05-29 19:34:37

Test Incident Rule2_efda254d-f96b-4197-95e7-ccc7c805412b (2023-05-29 19:34:02.93)
Assignee : elauser
2023-05-29 19:34:02

Test Incident Rule2_ca615d7b-9ade-43af-bfb7-44f17e53a714 (2023-05-29 19:00:38.195)
Assignee : elauser
2023-05-29 19:00:38

Test Incident Rule2_b0dfbffe-c774-4f2c-a740-d135e29d5790 (2023-05-29 18:55:10.471)
Assignee : elauser
2023-05-29 18:55:10

Test Incident Rule2_a5990573-fdc8-467a-a3a3-a1a4da760bcb (2022-11-14 22:34:19.161)
Assignee : elauser
2022-11-15 12:04:19

Test Incident Rule2_2036701f-8ad9-4547-808f-5139583d89dd (2022-11-14 22:34:19.146)
Assignee : elauser

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.

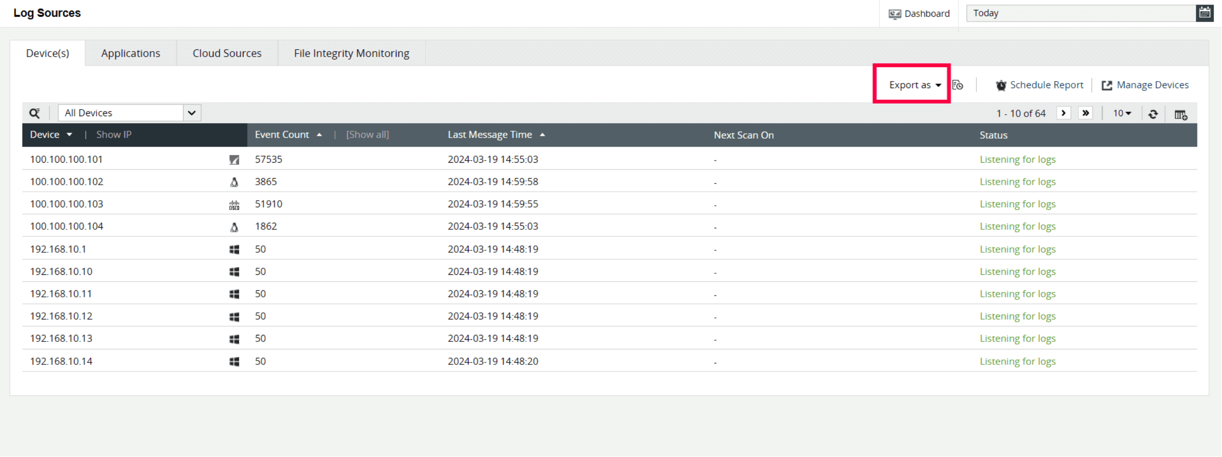
Scheduled Reports

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.



Device | Show IP	Event Count | [Show all]	Last Message Time	Next Scan On	Status
100.100.100.101	57535	2024-03-19 14:55:03	-	Listening for logs
100.100.100.102	3865	2024-03-19 14:59:58	-	Listening for logs
100.100.100.103	51910	2024-03-19 14:59:55	-	Listening for logs
100.100.100.104	1862	2024-03-19 14:55:03	-	Listening for logs
192.168.10.1	50	2024-03-19 14:48:19	-	Listening for logs
192.168.10.10	50	2024-03-19 14:48:19	-	Listening for logs
192.168.10.11	50	2024-03-19 14:48:19	-	Listening for logs
192.168.10.12	50	2024-03-19 14:48:19	-	Listening for logs
192.168.10.13	50	2024-03-19 14:48:19	-	Listening for logs
192.168.10.14	50	2024-03-19 14:48:20	-	Listening for logs

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.

2.2.2. Predefined tabs and widgets

Last updated on: September 12, 2025

In this page

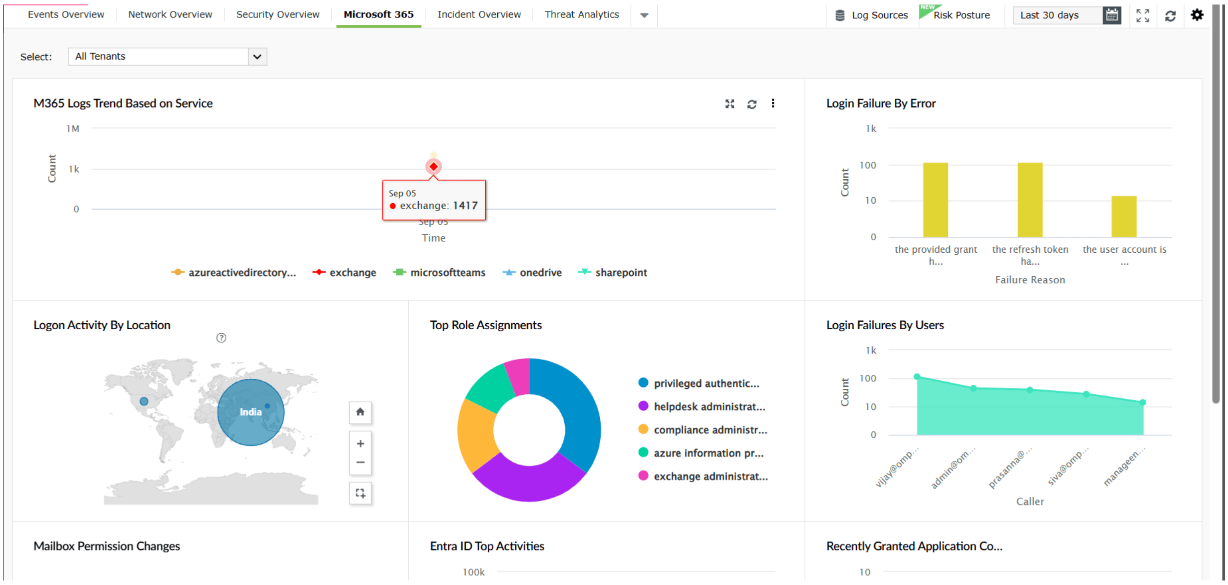
Overview

The Log360 dashboard provides a near real-time view of security-related data through graphs and charts. It helps you identify anomalies, analyze threats and attack patterns, and understand log trends at a glance. The dashboard is organized into tabs, each containing widgets that present specific security information.This guide explains the purpose of each dashboard tab and describes how the widgets help visualize key security data.

Dashboard tabs:

The dashboard comes with the following default subtabs:

- Events Overview
- Network Overview
- Security Overview
- M365
- Incident Overview
- Threat Analytics
- Detection Overview
- AD Audit



Select: All Tenants

Last 30 days

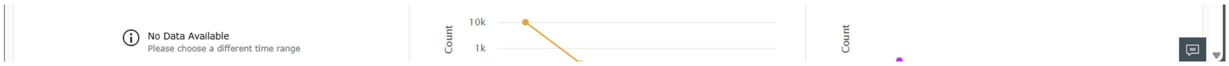


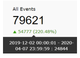
Figure 1: Navigating to the dashboard

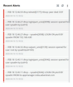
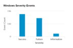
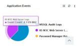
Each tab comprises numerous widgets.

Events Overview

This tab presents an overview of various key events monitored by the product console. The widgets in this dashboard provide insights on the various critical events generated in the network within the specified time frame.

The Events Overview tab has the following widgets:

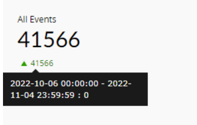
Widget Name	Function	Widget image
All Events	This widget presents the total number of events/logs collected by the SIEM module within the given time frame.	 All Events 79621 ▲ 54777 (220.48%) 2019-12-02 00:00:01 - 2020-04-07 23:59:59 : 24844
Windows Events	This widget presents the total number of Windows-based events collected by the SIEM module within the chosen time frame. In addition to that, the pie chart splits the Windows Events into error events, failure events, and warning events. Success/info events are filtered and not displayed.	 Windows Events 42047K Error 88539 Failure 1124 Warning 42
Syslog Events	This widget presents the total number of Syslog events collected within the given time frame. Furthermore, the pie chart splits the syslog events into warning, error, and critical events.	
All Devices	This widget provides a count of all the enabled devices from which log data is being collected. The server image in the corner will have a green tick if all logs are being collected successfully. A warning icon indicates that logs aren't being collected from some of the devices. Additionally, this widget has a View All Devices link. Clicking on the link will redirect you to the device dashboard page, which will provide detailed information of each device. Clicking on All Device will take you to the Devices tab, from where you can create a new list of Scheduled Reports	
Logs Trend	This widget presents a time-based log count trend of all events/logs ingested into the SIEM module. The X-axis represents the time range, which is based on the calendar range you choose. If you choose the time range as less than 24 hours, then the graph will present you with hourly log trend data. The Y-axis represents the Event Count.	

Widget Name	Function	Widget image
Top 5 Devices	This widget presents the top 5 devices based on event count.	
Recent Alerts	This widget presents the 50 most recent alerts for the given time range.	
Security Events	This widget shows a summary of various security events such as Logon, Account Logon, Account Management, and Object Access.	
Windows Severity Events	This widget displays a graph in which the X-axis represents the Severity of a Windows Event and the Y-axis represents the Event Count.	
Syslog Severity Events	This widget displays a graph in which the X-axis represents the Severity of a Syslog Event and the Y-axis represents the Event Count.	
Top 5 File Integrity Monitoring Events	This widget presents a 3D graph which displays the details of the top 5 file servers based on the log count. Each row contains additional data of various file-based events.	
Application Events	This widget displays a pie chart of the top 10 applications like IIS, DHCP etc based on event count.	

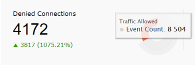
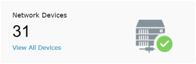
Network Overview

This tab gives an overview of various network-related events monitored by generating graphical reports. The widgets in this dashboard provide insights on the various critical events generated in the network within the specified time frame.

The Network Overview tab has the following widgets:

Widget Name	Function	Widget image
All Events	This widget presents the total number of network-based events collected by the SIEM module within the given time frame. Network-based events refer to events collected from network devices such as firewalls, switches, and routers.	 All Events 41566 ▲ 41566 2022-10-06 00:00:00 - 2022-11-04 23:59:59 : 0
Allowed Connections	This widget presents the count of all the connections that were allowed by the network device. The pie chart highlights the allowed connections from the total number of connections that occurred in the network within the specified time	 Allowed Connections 8504 ▲ 4372 (105.81%) Traffic Blocked ● Event Count: 4 172

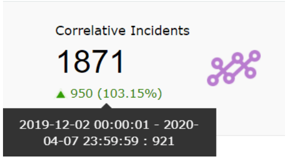
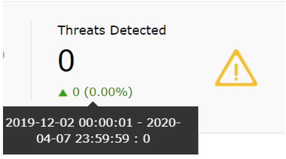
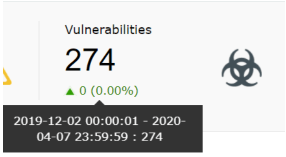
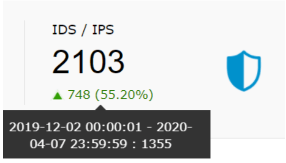
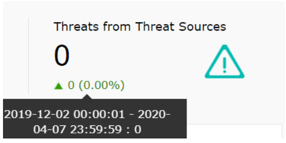
specified time.

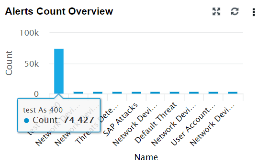
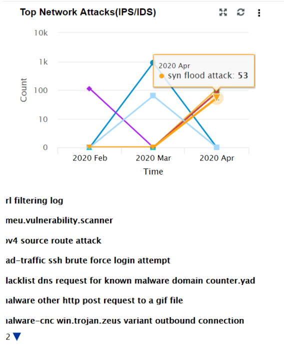
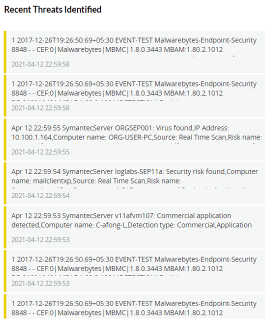
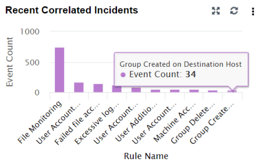
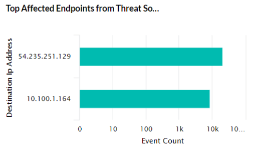
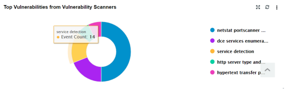
Widget Name	Function	Widget image
Denied Connections	This widget presents the count of all the connections that were denied by the network device. The pie chart highlights the denied connections from the total number of connections that occurred in the network within the specified time.	 Denied Connections 4172 ▲ 3817 (1075.21%) Traffic Allowed ● Event Count: 8 504
Network Devices	This widget provides a total count of network devices that are added for monitoring.	 Network Devices 31 View All Devices

Security Overview

This tab provides an overview of the key security events monitored. The widgets in this dashboard provide insights on the various critical events generated in the network within the specified time frame.

The Security Overview tab has the following Widgets:

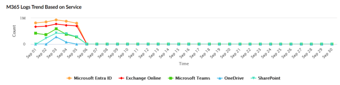
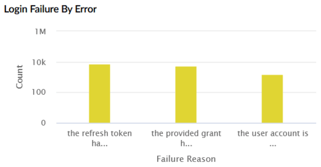
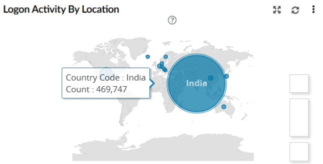
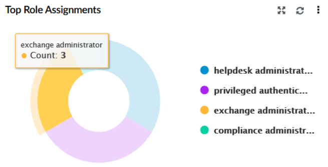
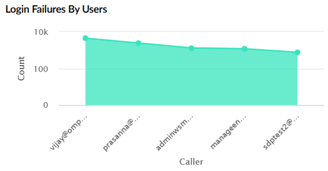
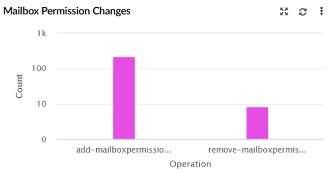
Widget Name	Function	Widget image
Correlative Incidents	This widget refers to the number of incidents detected via SIEM module's correlation engine.	 Correlative Incidents 1871 ▲ 950 (103.15%) 2019-12-02 00:00:01 - 2020-04-07 23:59:59 : 921
Threats Detected	This widget shows the logs from Threat Sources that are identified as threats by the SIEM module. These logs are selected based on predefined detection rules.	 Threats Detected 0 ▲ 0 (0.00%) 2019-12-02 00:00:01 - 2020-04-07 23:59:59 : 0
Vulnerabilities	This widget displays the total number of vulnerabilities detected by the vulnerability scanner(s) whose data are being imported into SIEM module.	 Vulnerabilities 274 ▲ 0 (0.00%) 2019-12-02 00:00:01 - 2020-04-07 23:59:59 : 274
IDS/IPS	This widget presents the total count of IDS/IPS events within the chosen time frame.	 IDS / IPS 2103 ▲ 748 (55.20%) 2019-12-02 00:00:01 - 2020-04-07 23:59:59 : 1355
Threats from Threat Sources	This widget presents the total number of threats from the configured Threat Sources (such as Symantec, McAfee, Malwarebytes etc) within the chosen time frame.	 Threats from Threat Sources 0 ▲ 0 (0.00%) 2019-12-02 00:00:01 - 2020-04-07 23:59:59 : 0

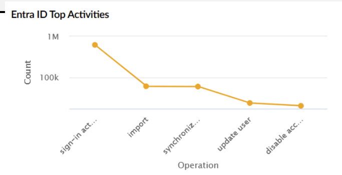
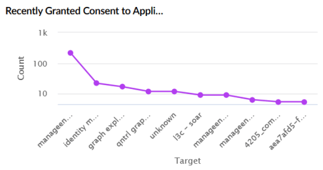
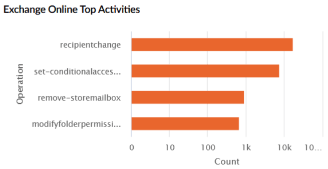
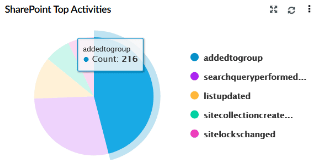
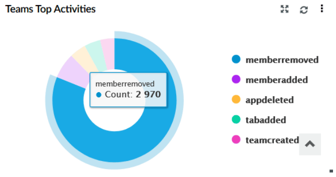
Widget Name	chosen time frame. Function	Widget image
Alert Count Overview	This widget provides an overview of each configured alert profile. The X-axis denotes the alert profile, and the Y-axis denotes the count.	
Top Network Attacks (IPS/IDS)	This widget includes a graph showing a time based trend for IDS/IPS events. The X-axis represents the time range. It will be based on the calendar range you choose. The Y-axis represents the event count, and the Z-axis represents the IDS/IPS event type. Top 10 events are displayed based on the event count.	
Recent Threats Identified	This widget displays the most recent 50 threats based on the calendar range.	Recent Threats Identified 1 2017-12-26T19:26:50.69+05:30 EVENT-TEST Malwarebytes-Endpoint-Security 8848 - - CEF:0|Malwarebytes|MBMC|1.8.0.3443 MBAM:1.80.2.1012 2021-04-12 22:59:58 1 2017-12-26T19:26:50.69+05:30 EVENT-TEST Malwarebytes-Endpoint-Security 8848 - - CEF:0|Malwarebytes|MBMC|1.8.0.3443 MBAM:1.80.2.1012 2021-04-12 22:59:58 Apr 12 22:59:55 SymantecServer ORGSEP001: Virus found,IP Address: 10.100.1.164,Computer name: ORG-USER-PC,Source: Real Time Scan,Risk name: 2021-04-12 22:59:55 Apr 12 22:59:54 SymantecServer loglabs-SEP11a: Security risk found,Computer name: mailclientxp,Source: Real Time Scan,Risk name: 2021-04-12 22:59:54 Apr 12 22:59:53 SymantecServer v11afvm107: Commercial application detected,Computer name: C-afong-L,Detection type: Commercial,Application 2021-04-12 22:59:53 1 2017-12-26T19:26:50.69+05:30 EVENT-TEST Malwarebytes-Endpoint-Security 8848 - - CEF:0|Malwarebytes|MBMC|1.8.0.3443 MBAM:1.80.2.1012 2021-04-12 22:59:53 1 2017-12-26T19:26:50.69+05:30 EVENT-TEST Malwarebytes-Endpoint-Security 8848 - - CEF:0|Malwarebytes|MBMC|1.8.0.3443 MBAM:1.80.2.1012
Recent Correlated Incidents	This widget is similar to Alert Count Review. It provides an overview of the recent correlated incidents. The X-axis denotes the correlation rule, and the Y-axis denotes the event count.	
Top Affected Endpoints from Threat Sources	This widget shows the Top 5 endpoint devices in which threats were detected by Threat Sources (Symantec, McAfee, etc)	
Top Vulnerabilities from Vulnerability Scanners	This widget includes a pie chart that displays the top 5 vulnerabilities (selected on the basis of event count) detected in endpoint devices by the vulnerability scanner.	

Microsoft 365

This tab provides an overview of activities and security events from various Microsoft 365 services. The widgets in this dashboard help you monitor login activity, role assignments, service usage, and activity trends across Exchange Online, SharePoint, Teams, OneDrive, and Entra ID.

The M365 Overview tab has the following widgets:

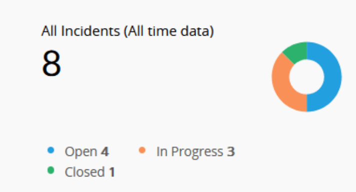
Widget Name	Function	Widget image
M365 Logs Trend Based on Service	Displays the total number of logs received from M365 services (Microsoft Entra ID, Exchange Online, Teams, OneDrive, and SharePoint) over the selected time period. The X-axis represents the time range, and the Y-axis represents the log count.	
Login Failure by Error	Shows failed login attempts categorized by error type, along with their count. The X-axis represents the failure reason, and the Y-axis represents the count.	
Logon Activity by Location	Displays a world map of user login activity by country, highlighting the geographic distribution of sign-ins. Each circle corresponds to the logon count.	 Logon Activity By Location Country Code : India Count : 469,747 India
Top Role Assignments	Lists the most assigned roles in the organization, such as global administrator.	
Login Failures by Users	Shows the number of login failures per user within the chosen time range. The X-axis represents users, and the Y-axis represents the failure count.	
Mailbox Permission Changes	Displays mailbox permission modifications performed by users specifically add and remove operations. The X-axis represents the type of operation, and the Y-axis represents the count.	

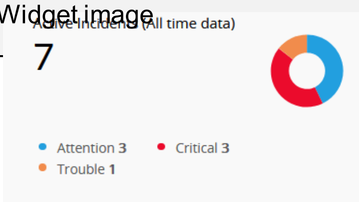
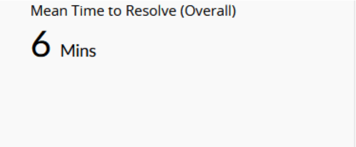
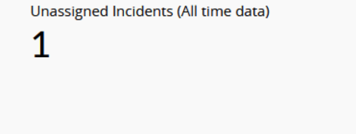
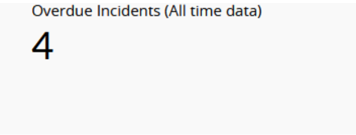
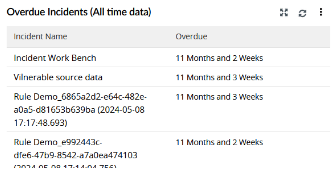
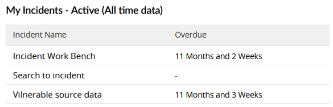
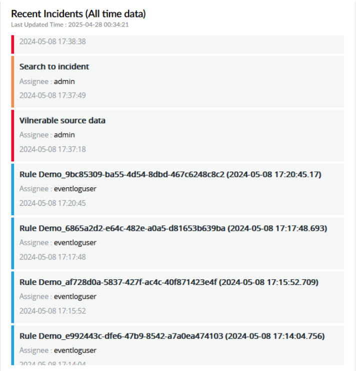
Widget Name	Function	Widget image
Entra ID Top Activities	Shows the most common operations performed in Entra ID such as sign-in activity, import, synchronize, update user, and disable account. The X-axis represents the operation type, and the Y-axis represents the count.	
Recently Granted Consent Applications	Displays applications to which users or admins recently granted consent. The X-axis represents the application name, and the Y-axis represents the permission grant count.	
Exchange Online Top Activities	Lists the top Exchange Online operations performed. The X-axis represents the operation, and the Y-axis represents the count.	
SharePoint Top Activities	Displays a pie chart of the top SharePoint activities such as group additions, search queries, list updates, and site creation.	
Teams Top Activities	Displays a pie chart of the top Teams operations such as member added/removed, team creation, app added, and tab added.	

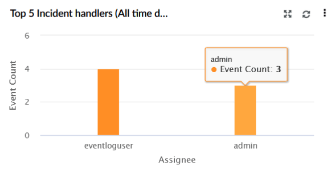
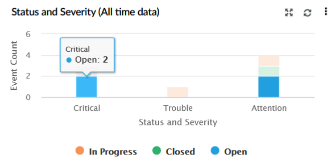
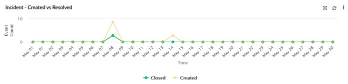
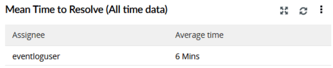
Incident Overview

This tab presents an overview of various security incidents. The widgets in this dashboard provide insights on the various critical incidents detected in the network within the specified time frame.

The Incident Overview tab has the following Widgets:

Widget Name	Function	Widget image
All Incidents (All time data)	This widget displays the total number of incidents raised till date, categorized by status: Open (blue), In Progress (orange), and Closed (green).	

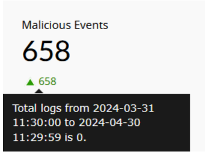
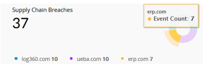
Widget Name	Function	Widget image
Active Incidents (All time data)	This widget represents incidents that are currently Open or In Progress, categorized based on severity: Attention (blue), Trouble (orange), and Critical (red).	 Active Incidents (All time data) 7 ● Attention 3 ● Critical 3 ● Trouble 1
Mean Time to Resolve (Overall)	This widget displays the average time taken to resolve incidents from the time they were created.	 Mean Time to Resolve (Overall) 6 Mins
Unassigned Incidents (All time data)	This widget indicates the number of incidents that have not yet been assigned to any user.	 Unassigned Incidents (All time data) 1
Overdue Incidents (All time data)	This widget shows the count of incidents that have passed their expected resolution date. This helps track unresolved tasks beyond due dates.	 Overdue Incidents (All time data) 4
Overdue Incidents (All time data)	This widget displays a table listing the names of overdue incidents along with their overdue duration.	 Overdue Incidents (All time data) Incident Name — Overdue Incident Work Bench — 11 Months and 2 Weeks Vilnerable source data — 11 Months and 3 Weeks Rule Demo_6865a2d2-e64c-482e-a0a5-d81653b639ba (2024-05-08 17:17:48.693) — 11 Months and 3 Weeks Rule Demo_e992443c-dfe6-47b9-8542-a7a0ea474103 (2024-05-08 17:14:04.756) — 11 Months and 2 Weeks
My Incidents - Active (All time data)	This widget displays active incidents specifically assigned to the current user, along with overdue details.	 My Incidents - Active (All time data) Incident Name — Overdue Incident Work Bench — 11 Months and 2 Weeks Search to incident — - Vilnerable source data — 11 Months and 3 Weeks
Recent Incidents (All time data)	This widget lists the 50 most recent incidents created, including incident name, assignee, and timestamp.	 Recent Incidents (All time data) Last Updated Time : 2025-04-28 00:34:21 2024-05-08 17:38:38 Search to incident Assignee : admin 2024-05-08 17:37:49 Vilnerable source data Assignee : admin 2024-05-08 17:37:18 Rule Demo_9bc85309-ba55-4d54-8dbd-467c6248c8c2 (2024-05-08 17:20:45.17) Assignee : eventloguser 2024-05-08 17:20:45 Rule Demo_6865a2d2-e64c-482e-a0a5-d81653b639ba (2024-05-08 17:17:48.693) Assignee : eventloguser 2024-05-08 17:17:48 Rule Demo_af728d0a-5837-427f-ac4c-40f871423e4f (2024-05-08 17:15:52.709) Assignee : eventloguser 2024-05-08 17:15:52 Rule Demo_e992443c-dfe6-47b9-8542-a7a0ea474103 (2024-05-08 17:14:04.756) Assignee : eventloguser 2024-05-08 17:14:04

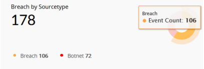
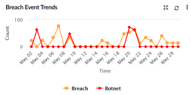
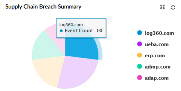
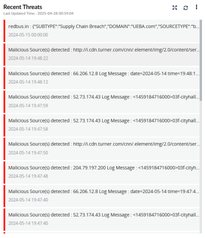
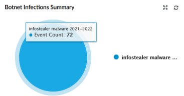
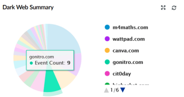
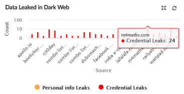
Widget Name	Function	Widget image
Top 5 Incident Handlers (All time data)	This widget represents a bar chart that shows the top 5 users (assignees) based on the number of incidents they are handling. X-axis represents the Asignee, Y-axis shows Event Count.	
Status and Severity (All time data)	This widget represents a bar chart displaying incidents based on both their status (Open, In Progress, Closed) and severity (Critical, Trouble, Attention). X-axis represents Status and Severity, and Y-axis represents Event Count.	
Incident - Created vs Resolved	This widget represents a line graph comparing the number of incidents created (yellow) versus those closed (green) over time. X-axis represents Time, Y-axis representsCount.	
Mean Time to Resolve (All time data)	This widget represents a table showing the average resolution time for each assignee.	Mean Time to Resolve (All time data) Assignee Average time eventloguser 6 Mins

Threat Analytics

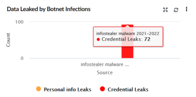
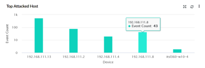
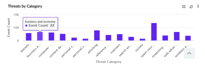
This tab presents an overview of various threat-related activities monitored. The widgets in this dashboard provide insights on the various critical threats identified in the network within the specified time frame.

The Threat Analytics tab has the following Widgets:

Widget Name	Function	Widget image
Malicious Events	This widget displays the total number of events flagged as malicious based on the threat feeds from the configured threat sources like STIX/TAXII and ATA threat servers.	Malicious Events 658 ▲ 658 Total logs from 2024-03-31 11:30:00 to 2024-04-30 11:29:59 is 0.
Supply Chain Breaches	This widget displays the number of breaches attributed to third-party applications or vendors, helping assess external risk exposure through the supply chain.	 Supply Chain Breaches 37 erp.com Event Count: 7 log360.com 10 ueba.com 10 erp.com 7

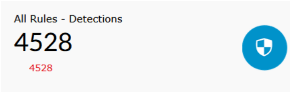
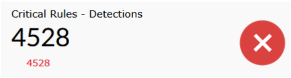
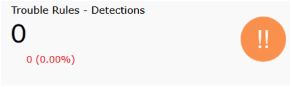
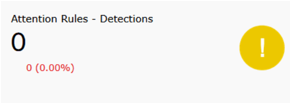
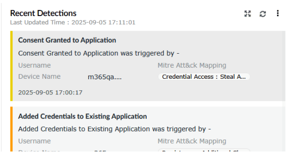
Widget Name	Function	Widget image
Breach by Category	This widget categorizes breaches by the type of data exposed, such as Credential Leaks or Personal Info Leaks, giving insights into the nature of the stolen data.	Breach by Category 178 Credential Leaks Event Count: 178 Credential Leaks 178
Breach by Sourcetype	This widget presents breaches based on their origin, which can be either from Botnet or Breach. Botnet refers to breaches caused by malware infections, while Breach refers to data exposed on the dark web through unknown sources.	 Breach by Sourcetype 178 Breach Event Count: 106 Breach 106 Botnet 72
Breach Event Trends	This widget represents a time-based graph showing the frequency of botnet and breach-related events over the selected date range. The X-axis represents the time range, which is based on the calendar range you choose. If you choose the time range as less than 24 hours, then the graph will present you with hourly log trend data. The Y-axis represents the Count.	 Breach Event Trends 100 0 Count May 02 May 04 May 06 May 08 May 10 May 12 May 14 May 16 May 18 May 20 May 22 May 24 May 26 May 28 Time Breach Botnet
Supply Chain Breach Summary	This widget represents a pie chart showing the distribution of breaches across affected third-party services or vendors, offering insight into which external platforms are most compromised.	 Supply Chain Breach Summary log360.com Event Count: 10 log360.com ueba.com erp.com admp.com adap.com
Recent Threats	This widget is a real-time feed of the recent threat alerts, both from dark web sources and malicious event detections.	 Recent Threats Last Updated Time : 2025-04-28 00:59:04 redbus.in : {"SUBTYPE":"Supply Chain Breach","DOMAIN":"UEBA.com","SOURCETYPE":"b... 2024-05-15 00:00:00 Malicious Source(s) detected : http://i.cdn.turner.com/cnn/.element/img/2.0/content/ser... 2024-05-14 19:48:22 Malicious Source(s) detected : 66.206.12.8 Log Message : date=2024-05-14 time=19:48:1... 2024-05-14 19:48:12 Malicious Source(s) detected : 52.73.174.43 Log Message : <1459184716000>03f-cityhall... 2024-05-14 19:47:59 Malicious Source(s) detected : 52.73.174.43 Log Message : <1459184716000>03f-cityhall... 2024-05-14 19:47:58 Malicious Source(s) detected : http://i.cdn.turner.com/cnn/.element/img/2.0/content/ser... 2024-05-14 19:47:50 Malicious Source(s) detected : 204.79.197.200 Log Message : <1459184716000>03f-cityh... 2024-05-14 19:47:48 Malicious Source(s) detected : 66.206.12.8 Log Message : date=2024-05-14 time=19:47:4... 2024-05-14 19:47:40 Malicious Source(s) detected : 52.73.174.43 Log Message : <1459184716000>03f-cityhall... 2024-05-14 19:47:40
Botnet Infections Summary	This widget represents a pie chart summarising botnet-related activity by malware type.	 Botnet Infections Summary infostealer malware 2021–2022 Event Count: 72 infostealer malware ...
Dark Web Summary	This widget represents a pie chart of leaked data detected across various dark web sources.	 Dark Web Summary m4maths.com wattpad.com canva.com gonitro.com cit0day gonitro.com Event Count: 9 1/6
Data Leaked in Dark Web	This widget represents a bar chart displaying the volume of leaked data found on the dark web. X-axis represents the breached source domains, and Y-axis indicates the count of leaked data instances. It distinguishes between Personal Info Leaks (orange) and Credential Leaks (red)	 Data Leaked in Dark Web 100 10 0 Count apollo.io bookchor.... cit0day combo list... combo list... combo list... dubsmash... facebook ... india e-c... lafalafa.com m4maths... railyatri... wattpad.c... m4maths.com Credential Leaks: 24 Source Personal info Leaks Credential Leaks

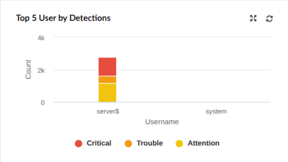
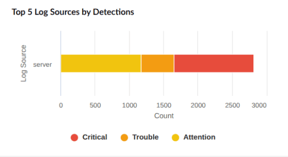
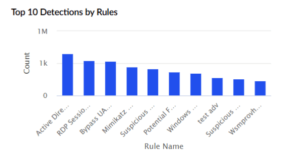
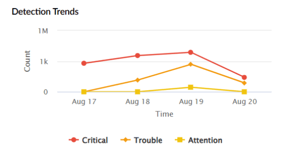
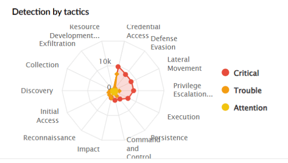
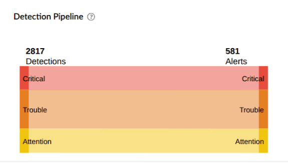
Personal Info Leaks (orange) and Credential Leaks (red).

Widget Name	Function	Widget image
Data Leaked by Botnet Infections	This widget represents a bar chart summarising data leaked specifically due to botnet malware. The X-axis shows the malware type, while the Y-axis represents the count of leaked credentials.	
Top Attacked Host	This widget displays a bar graph listing the most frequently targeted devices. X-axis represents the IP addresses or device names, and Y-axis shows the Event Count.	
Threats by Category	This widget displays a bar chart of malicious events, comparing them based on their threat category. The X-axis lists threat types (e.g., phishing, botnets), while the Y-axis represents the event count, providing insights into which threats have occurred most frequently.	

Detection Overview

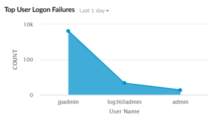
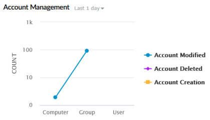
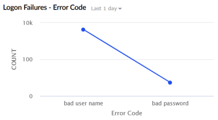
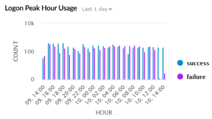
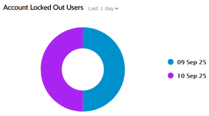
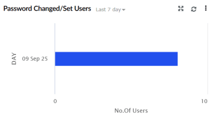
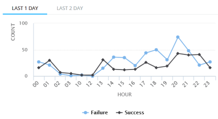
The tab provides a centralized view of detections across your environment. It helps security teams monitor threats, analyze patterns, and prioritize incidents using real-time visuals and context-driven insights.

Widget Name	Function	Widget image
All Rules - Detections	Displays the total number of detections triggered by all rules within the selected time frame.	
Critical Rules - Detections	Shows the total number of detections triggered by rules categorized as Critical during the selected time frame.	
Trouble Rules - Detections	Shows the total number of detections triggered by rules categorized as Trouble during the selected time frame.	
Attention Rules - Detections	Shows the total number of detections triggered by rules categorized as Attention during the selected time frame.	
Recent Detections	Lists the most recent detections triggered, along with details such as rule name, username, device	 Recent Detections Last Updated Time : 2025-09-05 17:11:01 Consent Granted to Application Consent Granted to Application was triggered by - Username Device Name m365qa.... Mitre Att&ck Mapping Credential Access : Steal A... 2025-09-05 17:00:17 Added Credentials to Existing Application Added Credentials to Existing Application was triggered by - Username Mitre Att&ck Mapping

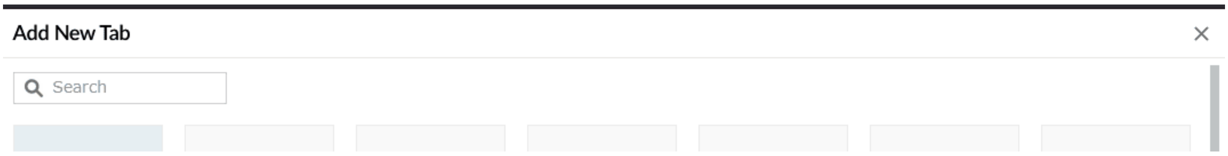
Widget Name	Function	Widget image
	name, and mapped MITRE ATT&CK tactic.	 Device Name m365qa.... Persistence : Additional Cl... 2025-09-05 16:59:51 Multiple Service Principals Created by User Multiple Service Principals Created by User was triggered by - Username Mitre Att&ck Mapping Device Name m365qa.... Persistence : Cloud Accoun... 2025-09-05 16:59:51
Top 5 Users by Detections	Shows the top five users who have generated the highest number of detections, further categorized by severity.	
Top 5 Log Sources by Detections	Displays the top five log sources based on detection count, categorized by severity.	
Top 10 Detections by Rules	Highlights the ten rules that triggered most frequently within the selected time range. The X-axis represents rule identifiers, and the Y-axis shows the detection count.	
Detection Trends	Provides a time-based view of detections. The X-axis represents the time period selected, while the Y-axis shows the count of detections categorized by severity.	
Detection by Tactics	Displays a radar chart of detections mapped to MITRE ATT&CK tactics such as Credential Access, Persistence, Defense Evasion, etc. You can filter by severity.	
Detection Pipeline	Summarizes detections based on severity and shows how many alerts were triggered for each severity type.	

AD Audit

This tab provides an overview of Active Directory logon activities, account changes, GPO modifications, and password resets. The widgets in this dashboard help administrators detect logon anomalies, track object modifications, and monitor account lockouts within the AD environment.
The AD Audit tab has the following widgets:

Widget Name	Function	Widget image
Top User Logon Failures	Displays the users with the most failed logon attempts within the selected time range. The X-axis represents the User Name, and the Y-axis represents the Count of failed logons.	
Account Management	Tracks account-related operations across users, groups, and computers. This includes account creation, deletion, and modification. The X-axis represents the Object Type (User, Group, Computer), and the Y-axis represents the Event Count.	
Logon Failures - Error Code	Categorizes logon failures by error type such as invalid username and invalid password. The X-axis represents the Error Code, and the Y-axis represents the Count.	
Logon Peak Hour Usage	Shows logon activity trends by time of day. The X-axis represents the Hour of the Day, and the Y-axis represents the Logon Count.	
Account Locked Out Users	Displays users whose accounts were locked due to repeated failed login attempts during the selected time period.	
Password Changed/Set Users	Tracks user password resets and change attempts. The X-axis represents the Type of Operation (Password Set, Password Change Attempt), and the Y-axis represents the Number of Users.	
ADFS Logon History	Displays logon activity for Active Directory Federation Services. The X-axis represents the Hour of the Day, and the Y-axis represents the Logon Count, categorized into successful and failed attempts.	

In addition to the above, there are multiple predefined templates available for dedicated monitoring. Select the ⚙ icon and click Add tab to view the list of tabs available.



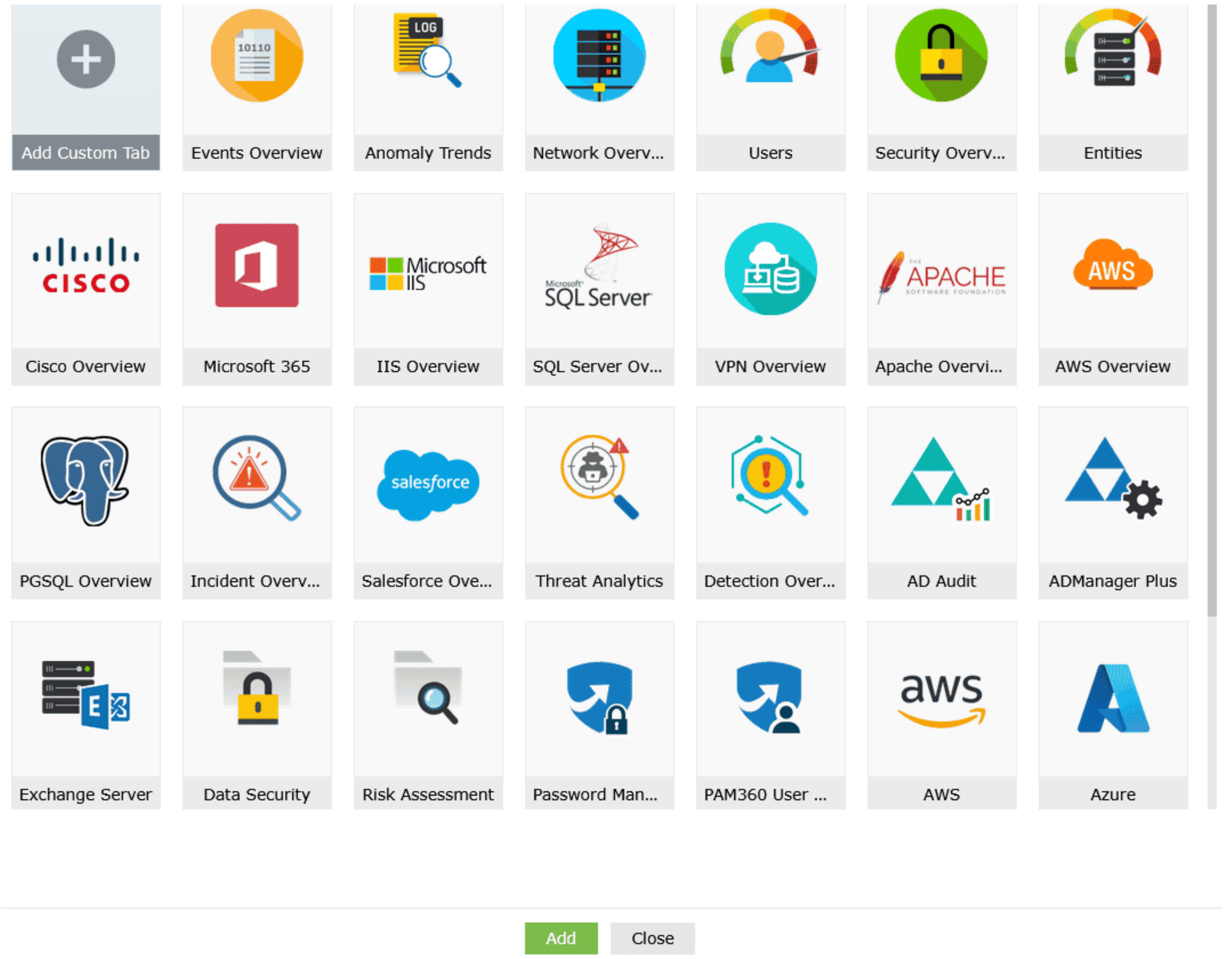


Figure 2: Viewing pre-defined tabs

Read also

This page explained about the predefined dashboard tabs and widgets in Log360. To learn how to customize dashboards and manage widgets, refer to the following documents:

- Customize Dashboard Views

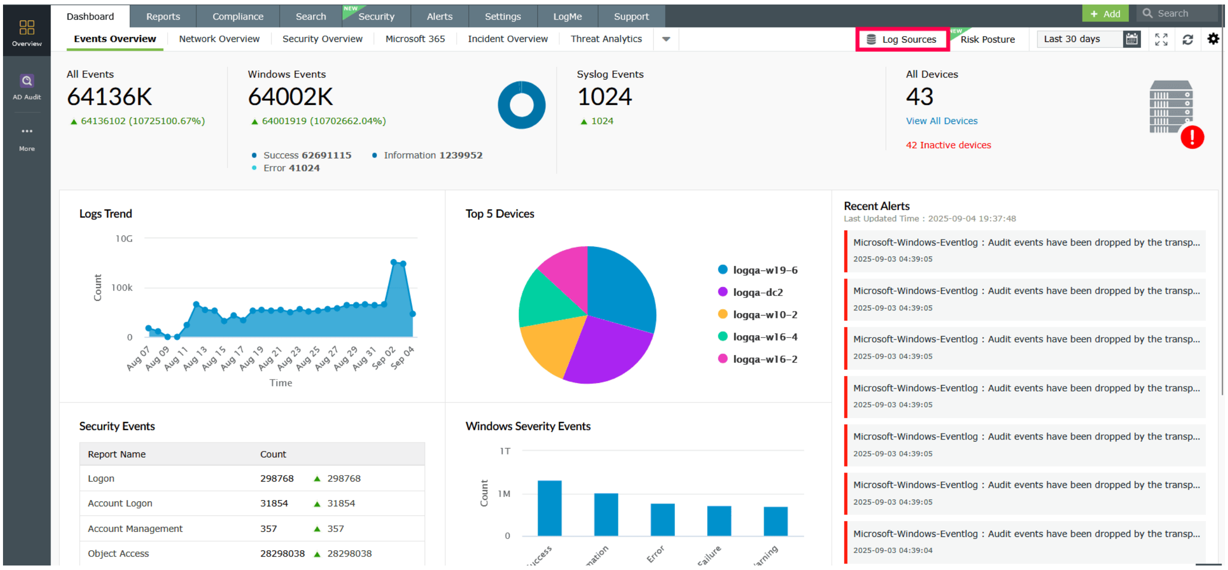
2.2.3. Customize Dashboard Views

Last updated on: September 12, 2025

In this page

Overview

Customizing the Log360 SIEM dashboard lets you tailor the view to highlight the data most relevant to your log sources.You can add, remove, or reorder tabs and widgets, and modify layout options to create a personalized dashboard that streamlines monitoring and improves visibility. The dashboard is populated using the data collected from various log sources. Click Log Sources on the top-right corner of the dashboard to view the list of devices, applications, and monitored files from which the data is being collected.



Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038

Recent Alerts

Last Updated Time : 2025-09-04 19:37:48

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

System Events	76	▲ 76

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...

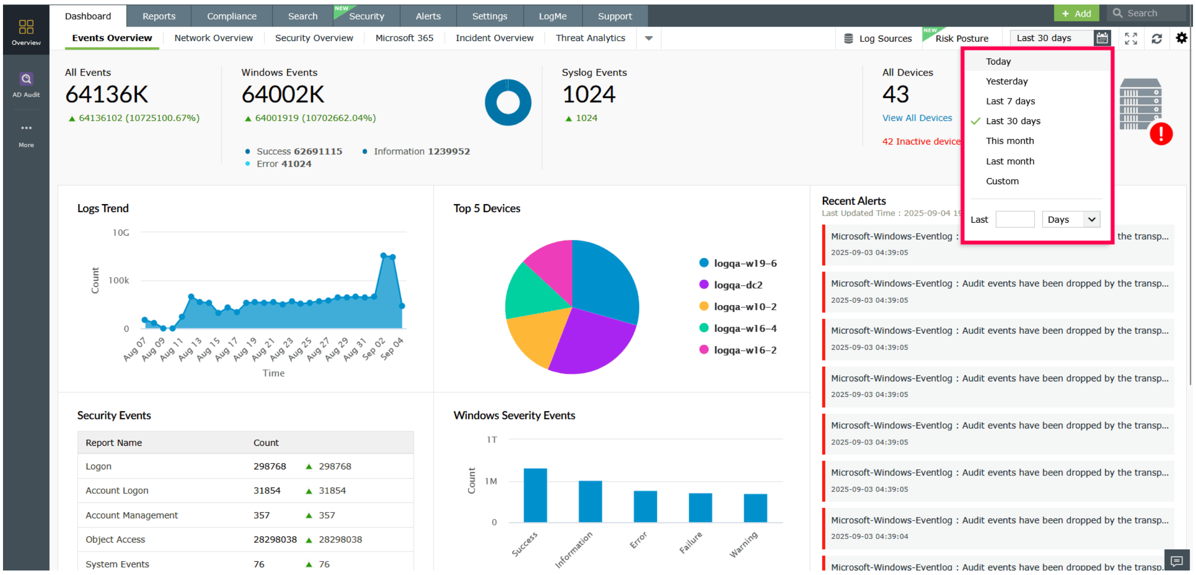
Figure 1: Accessing Log Sources in the dashboard

This page explains the customization options available and how they can be used to tailor a dashboard that fits your monitoring needs.

Filtering data by time range

You can filter the data displayed on the dashboard by selecting a time range.

1. In the top-right corner of the dashboard, click the drop-down.
2. Choose from predefined options such as Today, Yesterday, Last 7 days, Last 30 days, This month, Last month.



Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

Microsoft-Windows-Eventlog : ... the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

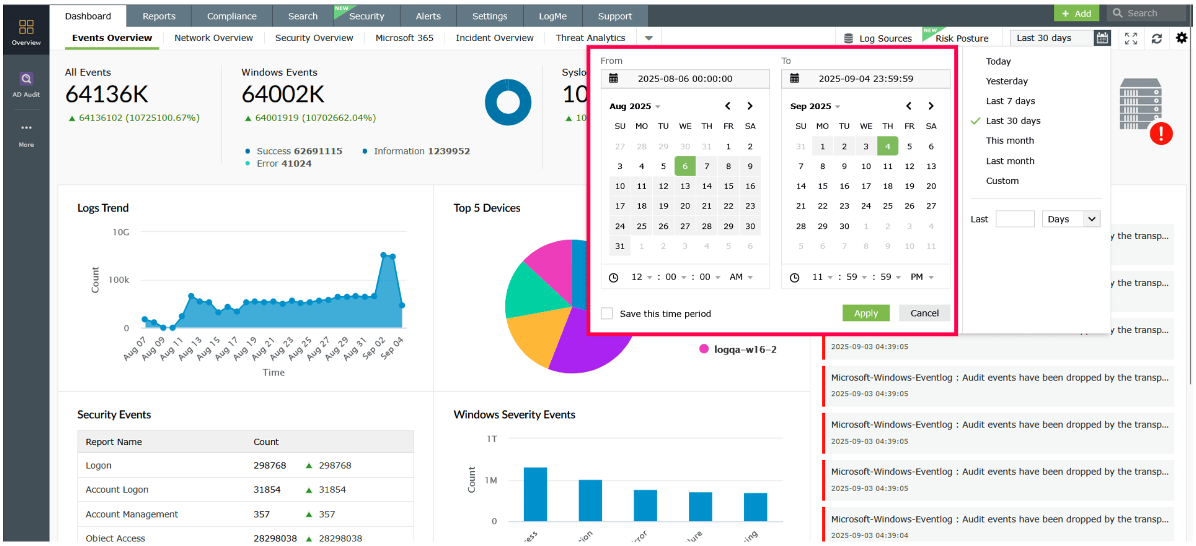
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...

Figure 2: Selecting a time range

3. To define your own range, select Custom and specify the From and To dates and times using the calendar and time fields.



From: 2025-08-06 00:00:00

To: 2025-09-04 23:59:59

From time: 12 : 00 : 00 AM

To time: 11 : 59 : 59 PM

All Events 64136K ▲ 64136102 (10725100.67%)

Windows Events 64002K ▲ 64001919 (10702662.04%)

● Success 62691115 ● Information 1239952 ● Error 41024

Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

System Events 76 ▲ 76

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...

Figure 3: Selecting a time range

4. Alternatively, you can use the Last field to set a relative time range.

5. Click Apply to update the dashboard data for the selected period.

Adding a new tab

To add a new tab to the dashboard,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Add Tab.

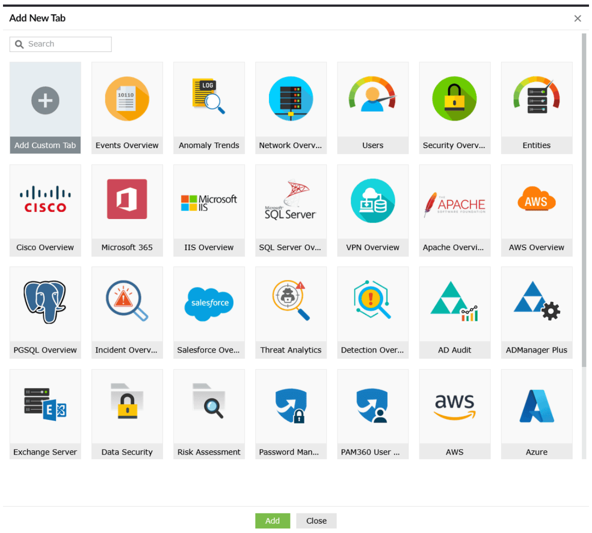


Figure 4: Adding a New Tab in the dashboard

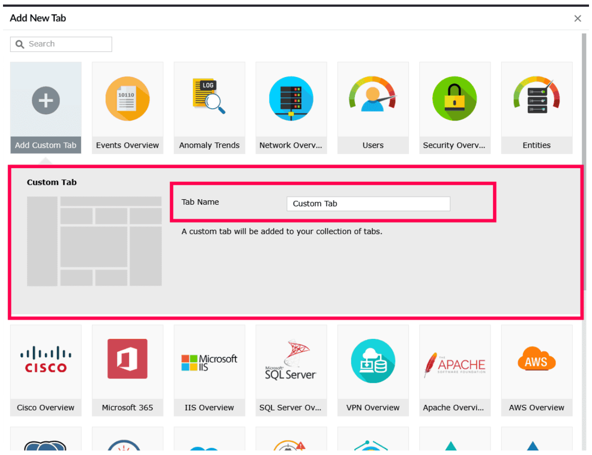
2. In the pop-up box that appears, you can see the following:

3. Default tabs: Events Overview, Network Overview, Security Overview, M365 Overview, Incident Overview, Detection Overview, Threat Analytics, and AD Audit.

4. Other predefined templates

5. Add Custom Tab option

6. Click Add Custom Tab. Enter a name for the tab in the given field and click Add.



Custom Tab

Tab Name: Custom Tab

A custom tab will be added to your collection of tabs.

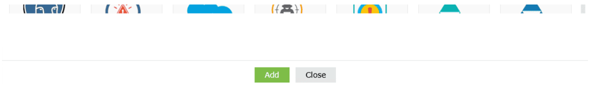
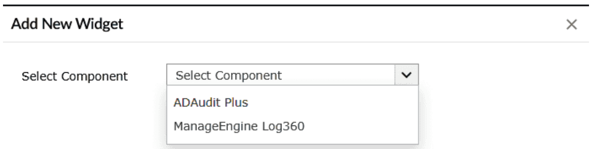


Figure 5: Adding a Custom Tab

Adding a new widget to a tab

To add a new widget,

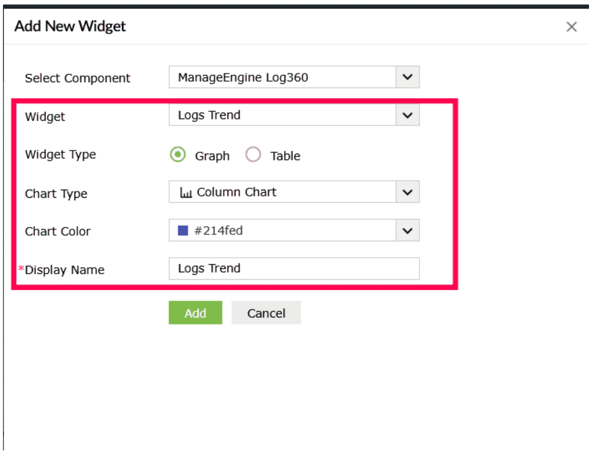
1. In the dashboard, click the ⚙ icon on the top-right corner and select Add Widgets.
2. In the Add New Widget window, choose a component from the Select Component drop-down.


Add New Widget

Select Component: Select Component
- ADAudit Plus
- ManageEngine Log360

Figure 6: Selecting a component

3. Specify the widget, widget type, chart type, chart color, and provide a display name for the widget.


Add New Widget

Select Component: ManageEngine Log360

Widget: Logs Trend

Widget Type: ● Graph ○ Table

Chart Type: Column Chart

Chart Color: #214fed

*Display Name: Logs Trend

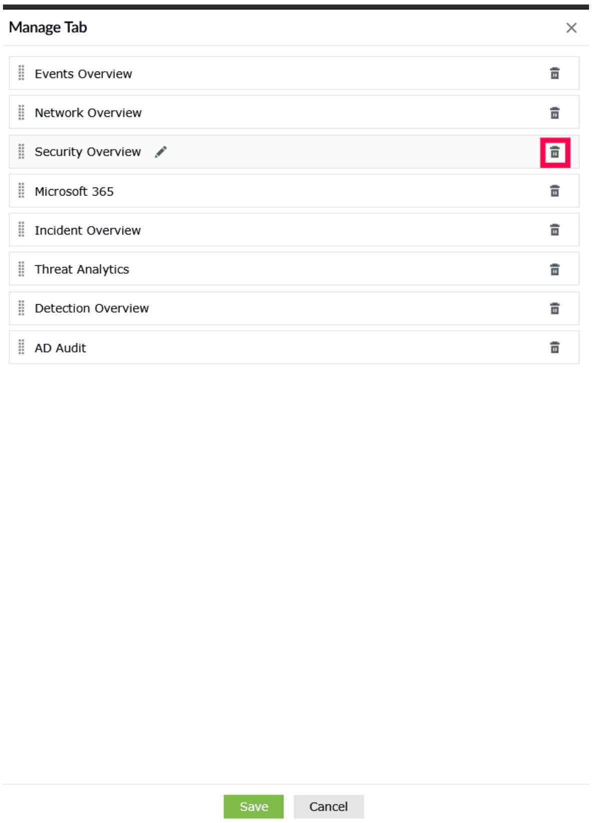
Figure 7: Configuring a New Widget in the dashboard

4. Once configured, select Add to save the widget.

Editing, deleting and reordering tabs

To delete tabs from the dashboard,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Manage Tabs.



Manage Tab

- Events Overview
- Network Overview
- Security Overview
- Microsoft 365
- Incident Overview
- Threat Analytics
- Detection Overview
- AD Audit

Figure 8: Deleting tabs in the dashboard

2. In the Manage Tab dialog box that appears, click the 🗑 icon corresponding to that tab that you want to delete.

3. In the pop-up confirmation box, click Yes to confirm the deletion of the tab.

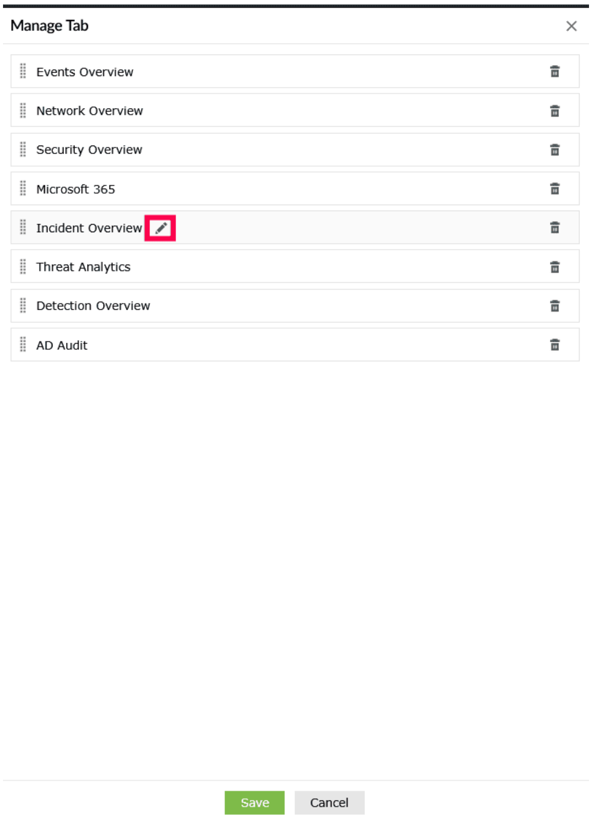
4. Click Save to apply the changes to the dashboard.

To reorder the tabs in the dashboard,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Manage Tabs.
2. Click the ⠿ icon and drag and drop the tabs in the order of your choice.
3. Click Save to apply the changes to the dashboard.

To edit a dashboard tab:

1. In the dashboard, click the ⚙ icon on the top-right corner and select Manage Tabs.
2. Hover over the tab you want to edit and click the edit icon.

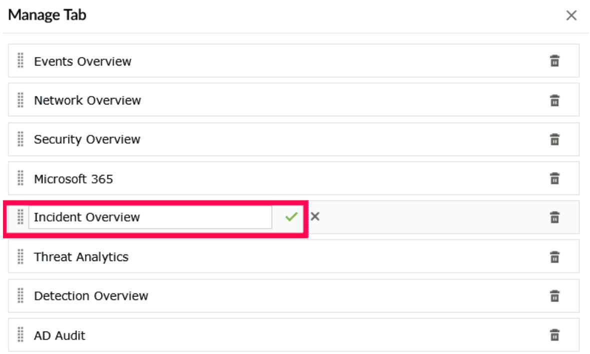


Manage Tab ×

- Events Overview
- Network Overview
- Security Overview
- Microsoft 365
- Incident Overview
- Threat Analytics
- Detection Overview
- AD Audit

Figure 9: Editing a dashboard tab

3. Modify the tab name and click the ✓ icon to confirm.



Manage Tab ×

- Events Overview
- Network Overview
- Security Overview
- Microsoft 365
- Incident Overview ✓ ×
- Threat Analytics
- Detection Overview
- AD Audit

Figure 10: Modifying the tab name

4. Click Save to apply the changes to the dashboard.

Reordering and resizing widgets

To reorder the widgets in a tab,

1. In the dashboard, go to the tab containing the widgets you want to reorder.

2. Click the ⚙ icon on the top-right corner and select Reorder Widgets.

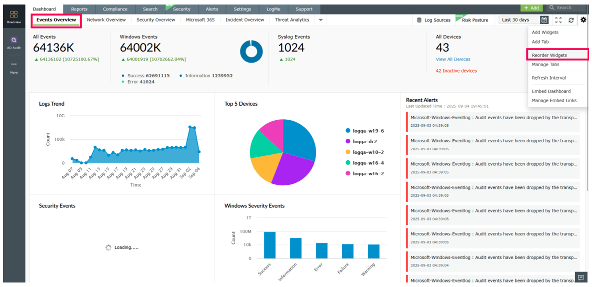
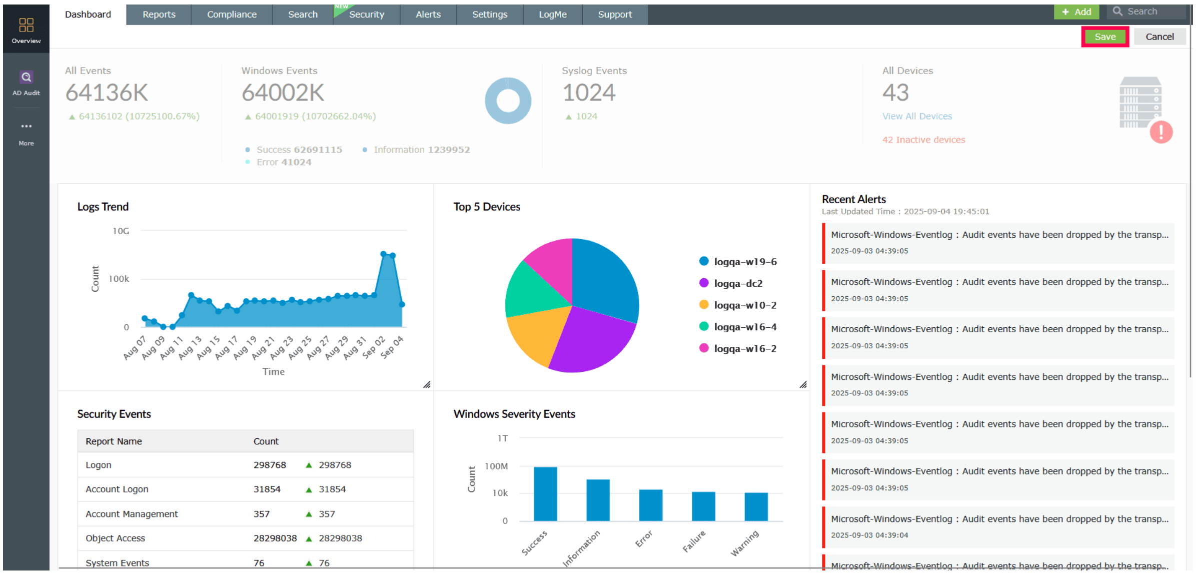


Figure 11: Reordering widgets in the dashboard

3. Click and drag the widgets to your desired positions.

4. Click Save in the top-right corner to apply the changes to the dashboard.



Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

Recent Alerts
Last Updated Time : 2025-09-04 19:45:01

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...

Figure 12: Saving changes to the dashboard

To resize the widgets in a tab

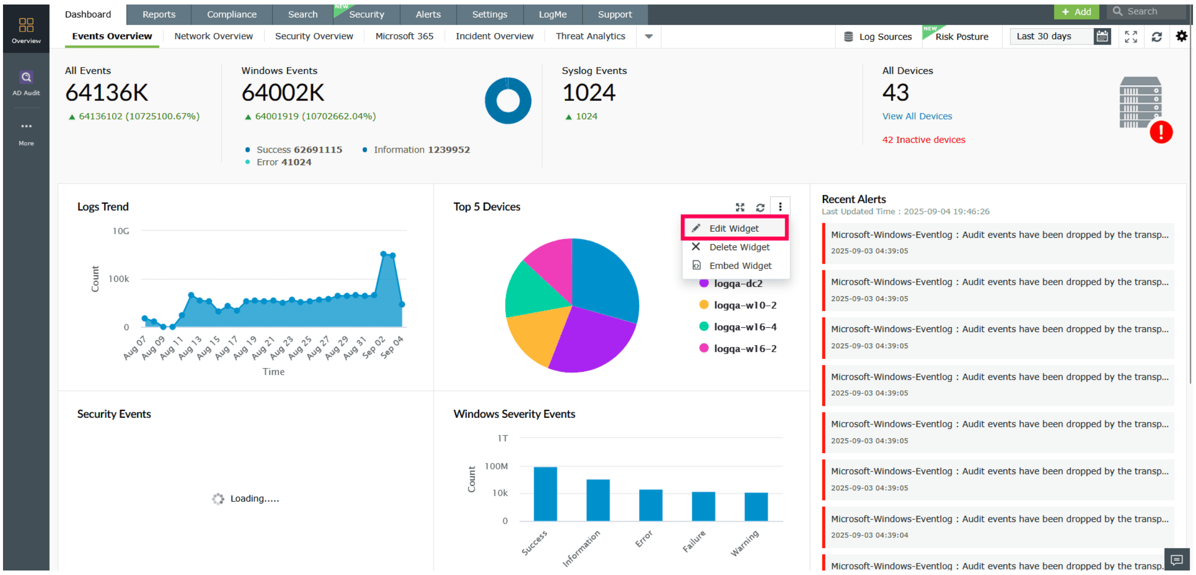
To resize the widgets in a tab,

1. In the dashboard, navigate to the tab whose widgets you want to resize.
2. Click the ⚙ icon on the top-right corner and select Reorder Widgets.
3. Hover over the widget you want to resize, click the ⤡ icon, and drag from the bottom-right corner to adjust the size as needed.
4. Click Save in the top-right corner to apply the changes to the dashboard.

Editing and deleting widgets

To edit a widget in a tab,

1. In the dashboard, click the ⋮ icon and select Edit Widget corresponding to the widget that you want to edit.



Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

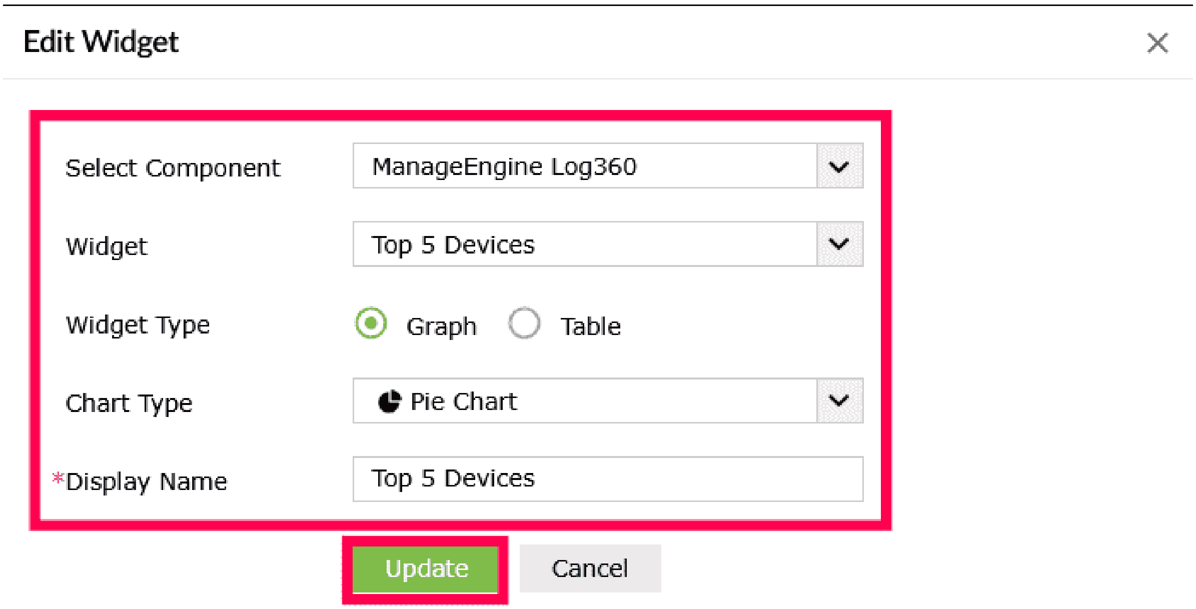
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...

Figure 13: Editing a widget

2. Update the necessary information and click Update.



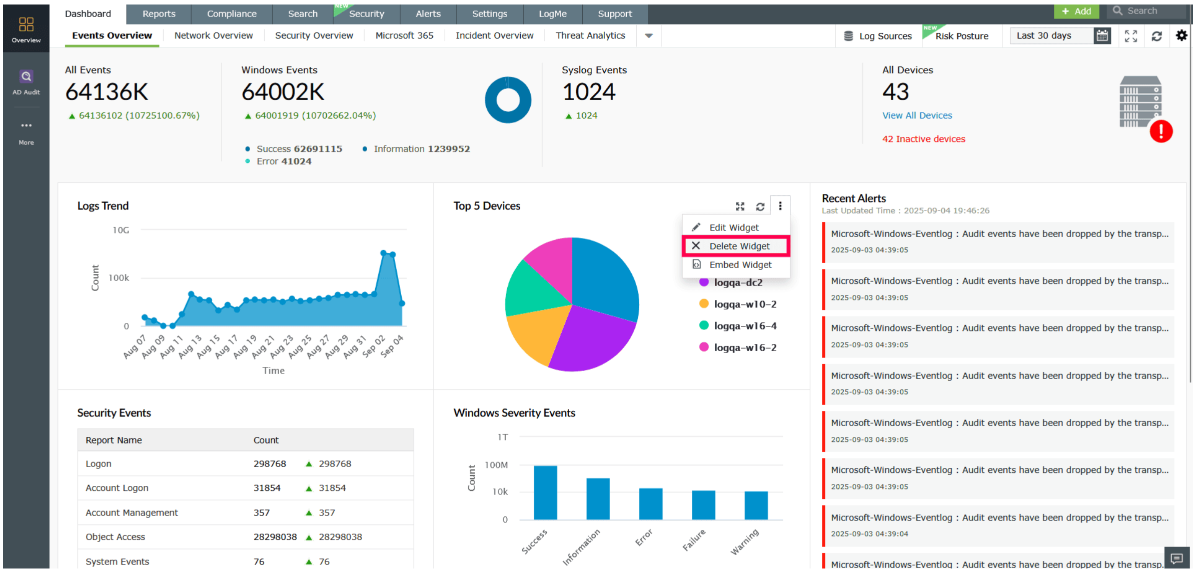
Edit Widget

Select Component	ManageEngine Log360
Widget	Top 5 Devices
Widget Type	● Graph ○ Table
Chart Type	Pie Chart
*Display Name	Top 5 Devices

Figure 14: Editing a widget

To delete a widget from a tab,

1. In the dashboard, click the ⋮ icon corresponding to the widget that you want to delete.
2. Select Delete Widget.



Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

Recent Alerts
Last Updated Time : 2025-09-04 19:46:26

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

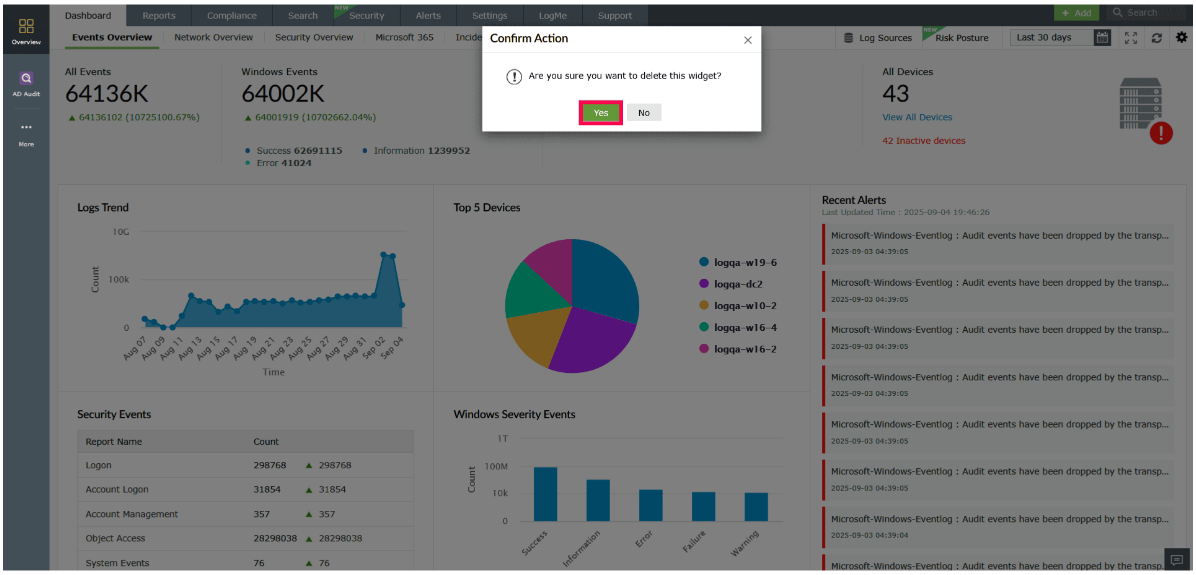
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp.

Figure 15: Deleting a widget

3. Click Yes in the pop-up box to complete the deletion.



Confirm Action

Are you sure you want to delete this widget?

Yes No

Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

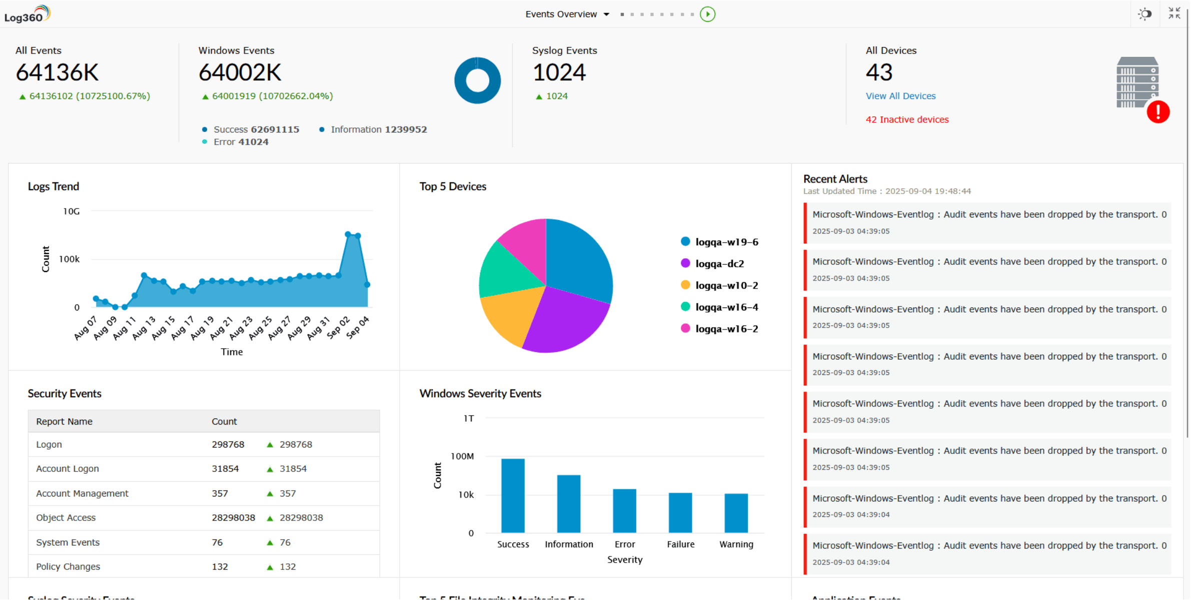
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Figure 16: Confirming deletion of a widget

Viewing the dashboard in full screen mode

To view the dashboard in full screen,

1. In the dashboard, click the ⛶ icon on the top-right corner.



Security Events

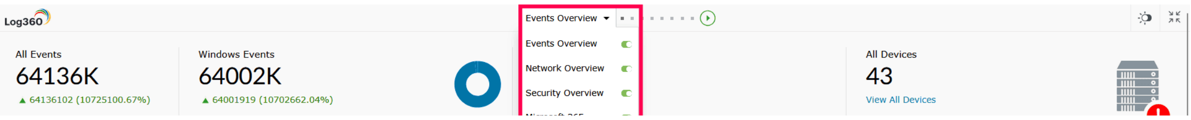
Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76
Policy Changes	132	▲ 132

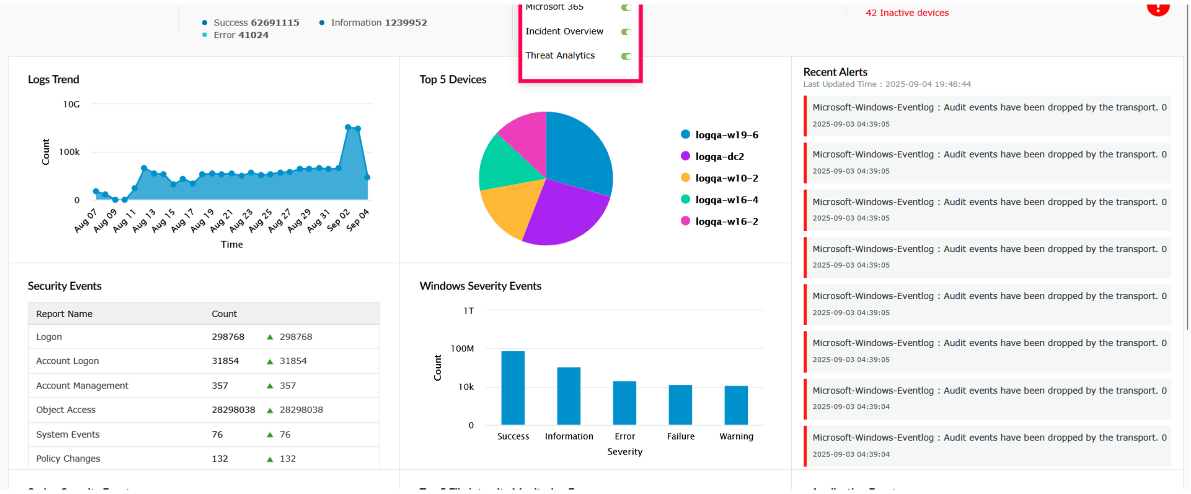
Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Figure 17: Viewing the dashboard in full screen mode

2. To start a slideshow of the tabs, click the play icon at the top of the screen.

3. To switch between tabs, click the drop-down button ▼ at the top of the screen.





Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76
Policy Changes	132	▲ 132

Recent Alerts
Last Updated Time : 2025-09-04 19:48:44

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

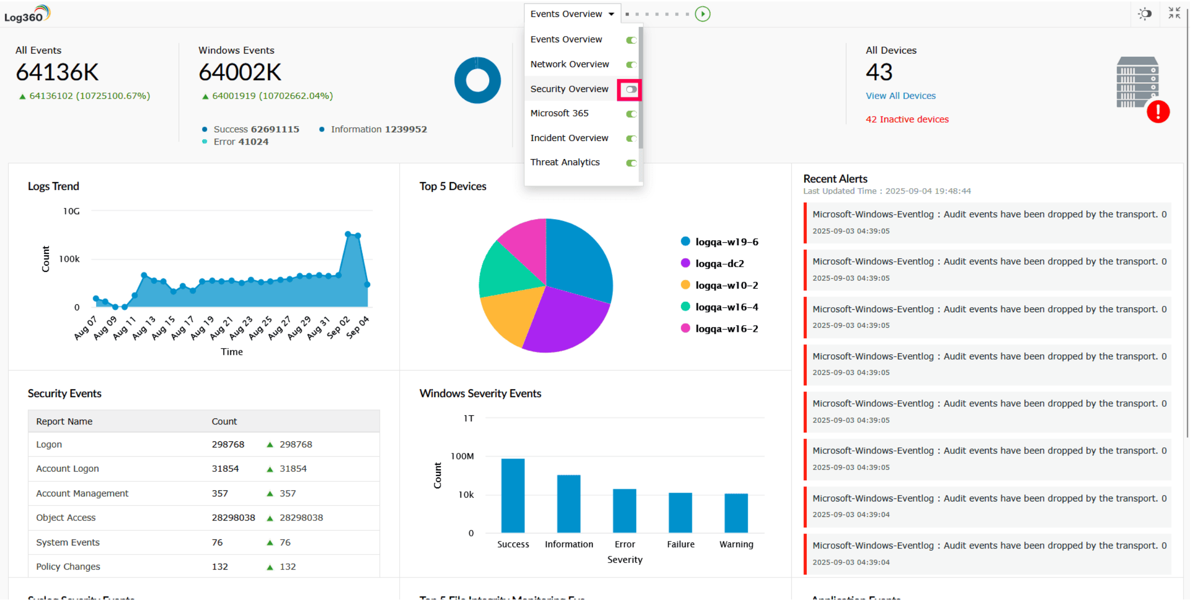
Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:04

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:04

Figure 18: Switching between tabs

4. To remove a particular tab from the slideshow, click the toggle button ⬤ next to the tab name in the drop-down list.



Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76
Policy Changes	132	▲ 132

Recent Alerts
Last Updated Time : 2025-09-04 19:48:44

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

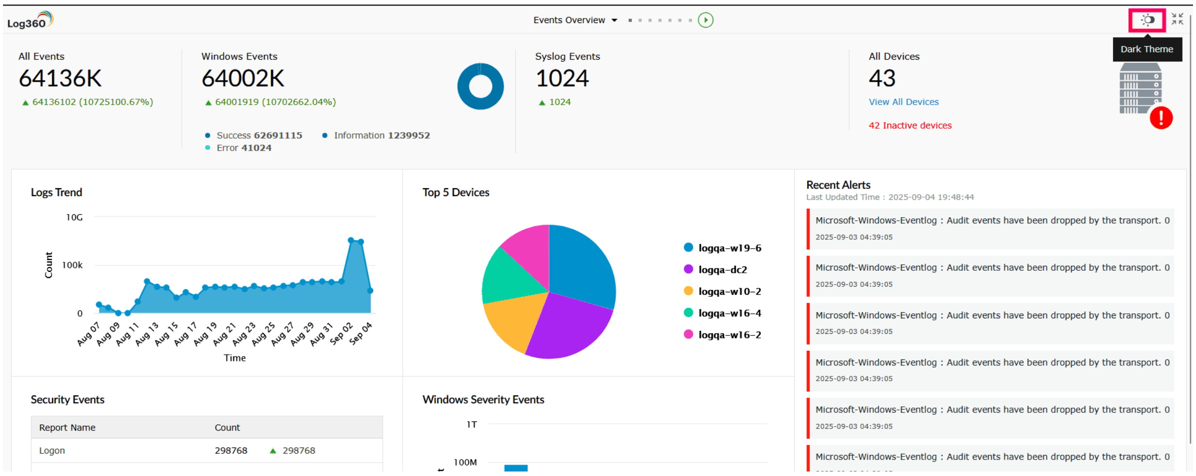
Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:04

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:04

Figure 19: Removing a tab from the slideshow

5. To switch to dark mode, click the toggle button at the top-right corner of the screen.



Security Events

Report Name	Count	
Logon	298768	▲ 298768

Recent Alerts
Last Updated Time : 2025-09-04 19:48:44

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

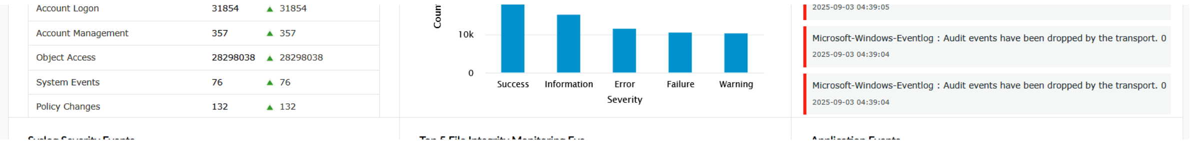
Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0



Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76
Policy Changes	132	▲ 132

2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:04

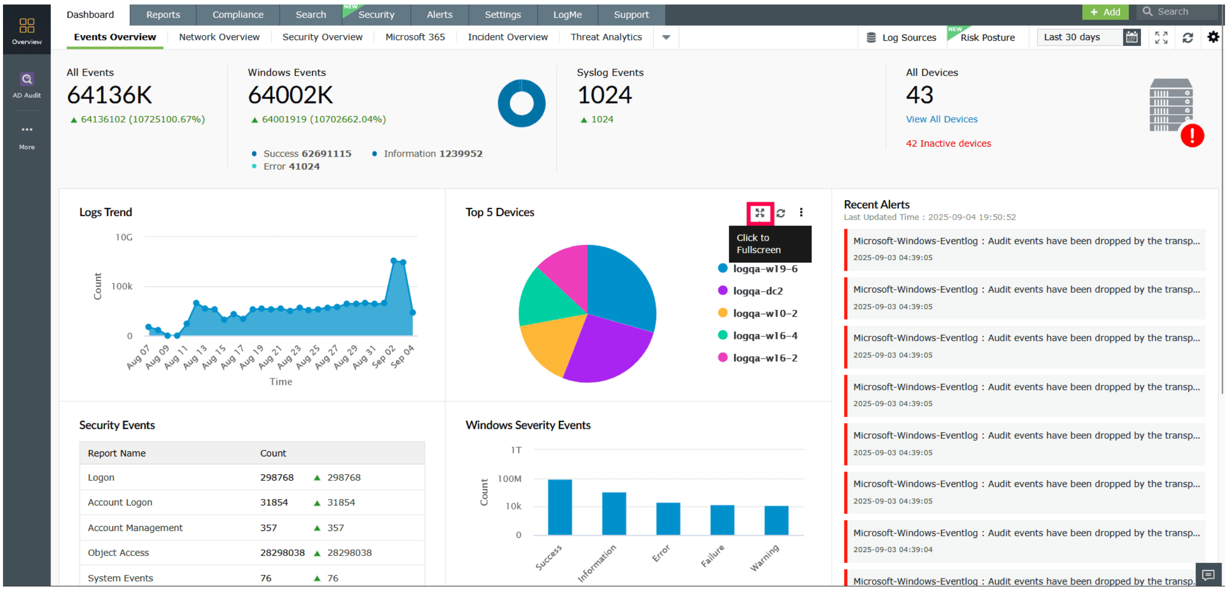
Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0
2025-09-03 04:39:04

Figure 20: Switching to dark mode

6. To exit full screen mode, click the ⛶ icon.

Viewing a widget in full screen mode

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



All Events
64136K
▲ 64136102 (10725100.67%)

Windows Events
64002K
▲ 64001919 (10702662.04%)
● Success 62691115 ● Information 1239952
● Error 41024

Syslog Events
1024
▲ 1024

All Devices
43
View All Devices
42 Inactive devices

Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

Recent Alerts
Last Updated Time : 2025-09-04 19:50:52

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

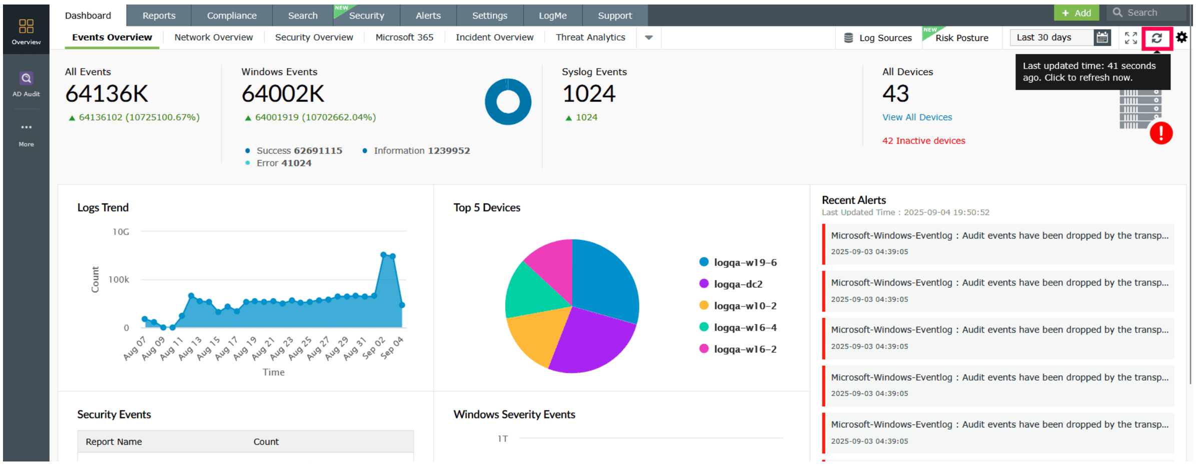
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...

Figure 21: Viewing a widget in full screen mode

Refreshing the dashboard and widgets

To refresh the entire dashboard,

1. In the dashboard, click the ↻ icon on the top-right corner of the screen.



All Events
64136K
▲ 64136102 (10725100.67%)

Windows Events
64002K
▲ 64001919 (10702662.04%)
● Success 62691115 ● Information 1239952
● Error 41024

Syslog Events
1024
▲ 1024

All Devices
43
View All Devices
42 Inactive devices

Last updated time: 41 seconds ago. Click to refresh now.

Recent Alerts
Last Updated Time : 2025-09-04 19:50:52

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

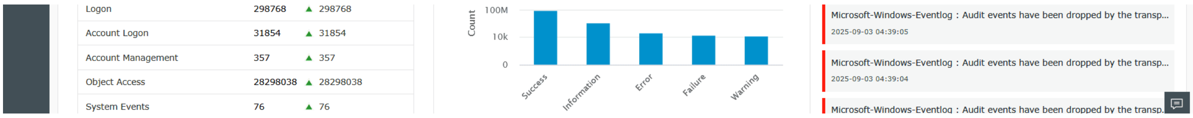
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Security Events

Report Name	Count



Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

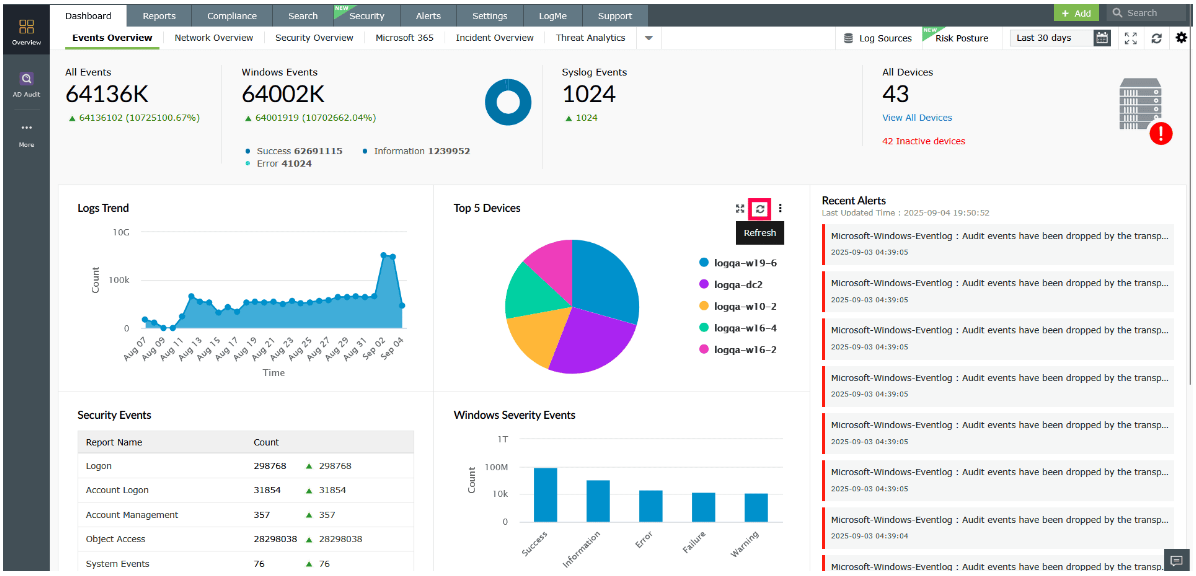
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...

Figure 22: Refreshing the dashboard

To refresh a particular widget,

1. In the dashboard, click the ⟳ icon on the top-right corner of the specific widget.



All Events
64136K
▲ 64136102 (10725100.67%)

Windows Events
64002K
▲ 64001919 (10702662.04%)
● Success 62691115 ● Information 1239952
● Error 41024

Syslog Events
1024
▲ 1024

All Devices
43
View All Devices
42 Inactive devices

Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

Recent Alerts
Last Updated Time : 2025-09-04 19:50:52

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

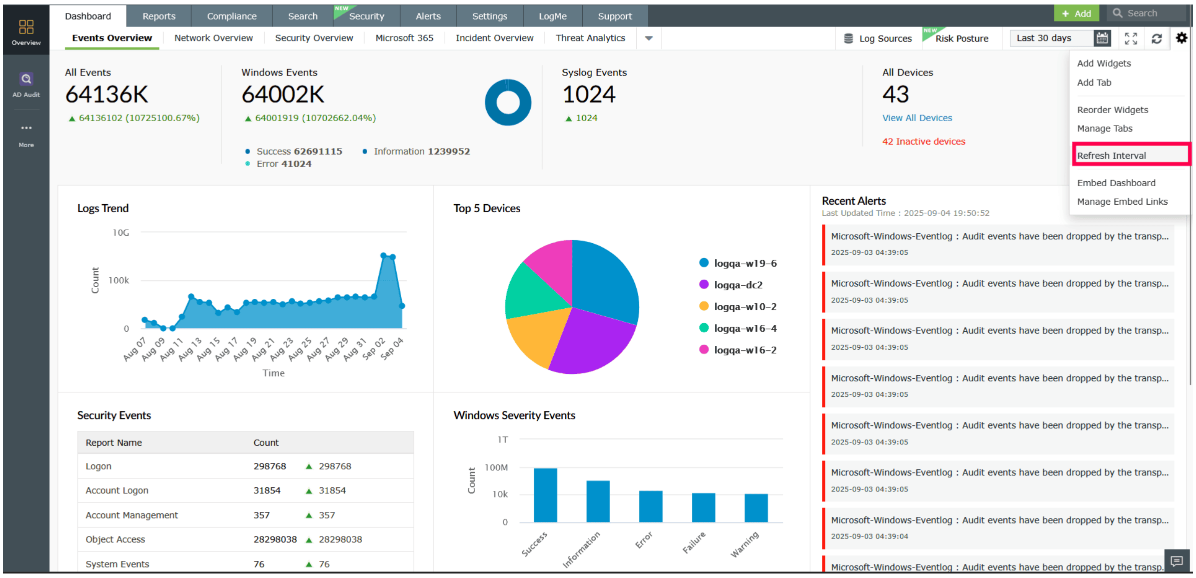
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...

Figure 23: Refreshing a widget

Changing refresh interval

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

1. In the dashboard, click the ⚙ icon on the top-right corner and select Refresh Interval.



All Events
64136K
▲ 64136102 (10725100.67%)

Windows Events
64002K
▲ 64001919 (10702662.04%)
● Success 62691115 ● Information 1239952
● Error 41024

Syslog Events
1024
▲ 1024

All Devices
43
View All Devices
42 Inactive devices

Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

Recent Alerts
Last Updated Time : 2025-09-04 19:50:52

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

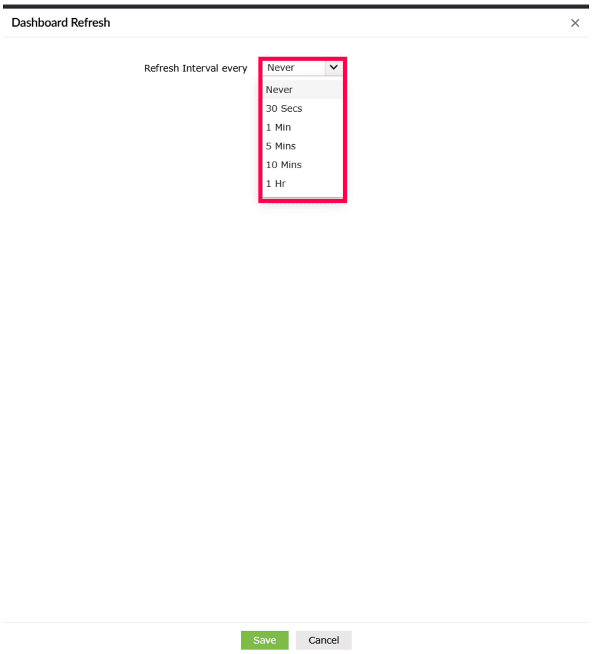
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...

Figure 24: Configuring Refresh Interval in the dashboard

2. In the Dashboard Refresh window, select the refresh interval: Never, 30 seconds, 1 minute, 5 minutes, 10 minutes, or 1 hour.
   NOTE If you select Never, the dashboard will not refresh automatically. You will need to refresh it manually.



Dashboard Refresh

Refresh Interval every: Never

Figure 25: Changing the refresh interval

3. Click Save to apply the changes to the dashboard.

ⓘ NOTE

Watch this video for a step-by-step demonstration of customizing the dashboard.

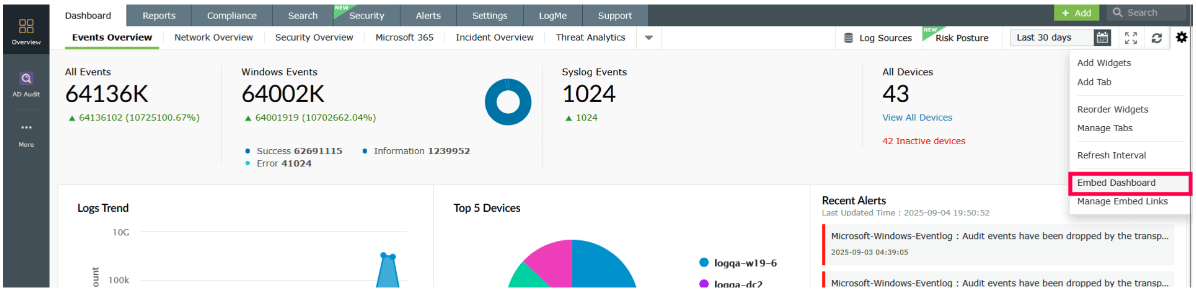
Configuring Embed link for dashboard and widgets

The Embed link enhances data sharing by allowing the creation of external share links for specific tabs or widgets. This enables precise and targeted access to dashboard data, supporting collaboration and visibility across platforms.

To embed a dashboard,

1. In the dashboard, navigate to the tab you want to embed.

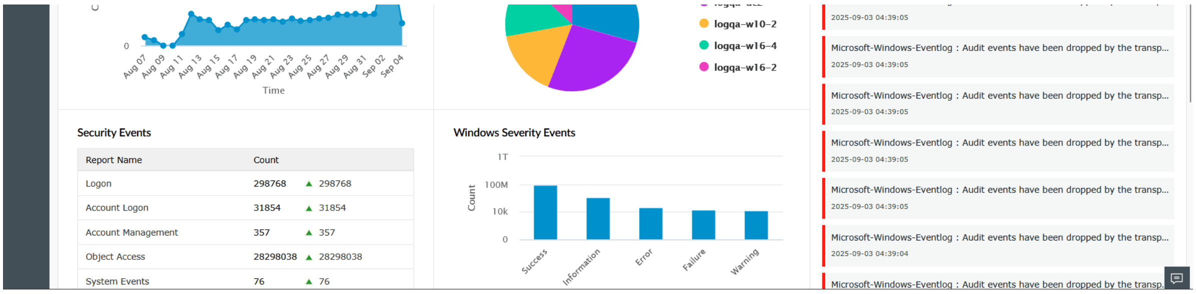
2. In the top-right corner, click the ⚙ icon and select Embed Dashboard.



Recent Alerts
Last Updated Time : 2025-09-04 19:50:52

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...



Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

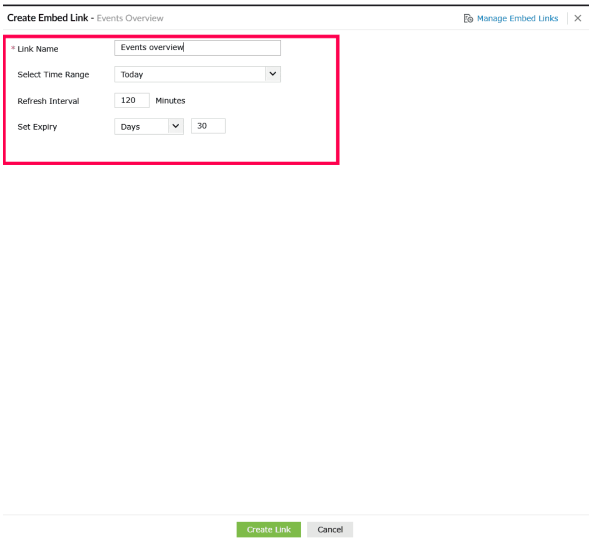
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp.

Figure 26: Navigating to Embed Dashboard

3. Provide a unique Link Name.

4. Select the desired Time Range from the drop-down menu.

5. Configure the Refresh Time (60 - 1440 minutes) and Expiry (1 - 365 days) using the drop-down options.



Create Embed Link - Events Overview

* Link Name: Events overview

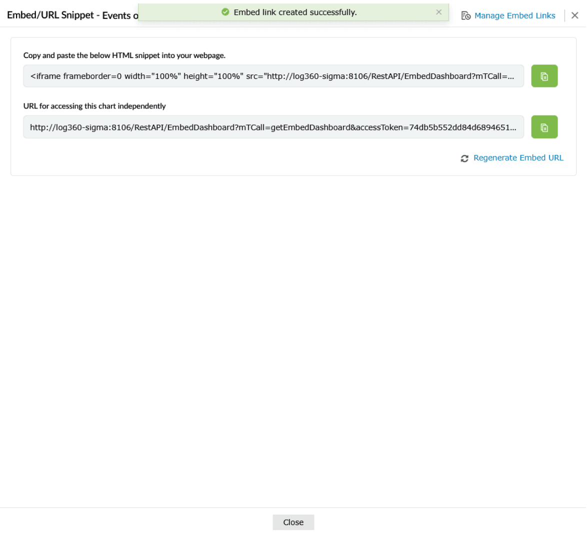
Select Time Range: Today

Refresh Interval: 120 Minutes

Set Expiry: Days 30

Figure 27: Creating an embed link

6. Click Create Link to generate the embed link for the dashboard.



Embed/URL Snippet - Events o

Embed link created successfully.

Copy and paste the below HTML snippet into your webpage.

```
<iframe frameborder=0 width="100%" height="100%" src="http://log360-sigma:8106/RestAPI/EmbedDashboard?mTCall=...
```

URL for accessing this chart independently

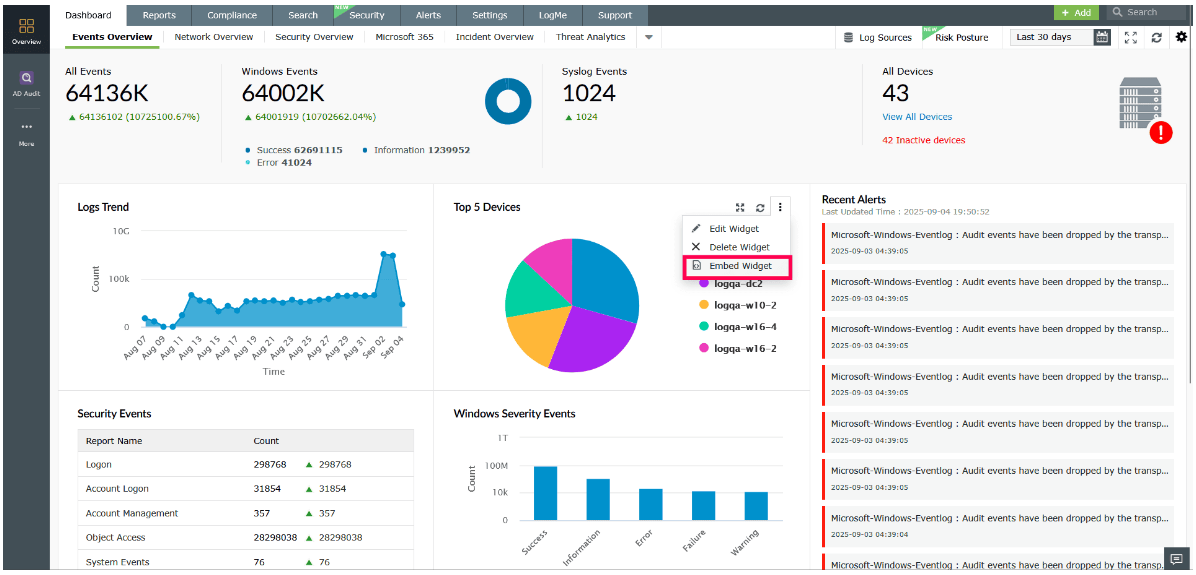
```
http://log360-sigma:8106/RestAPI/EmbedDashboard?mTCall=getEmbedDashboard&accessToken=74db5b552dd84d6894651...
```

Figure 28: Creating an embed link

7. To regenerate the link, click Regenerate Embed URL.

To embed a widget,

1. In the dashboard, click the ⋮ icon and select Embed Widget corresponding to the widget that you want to embed.



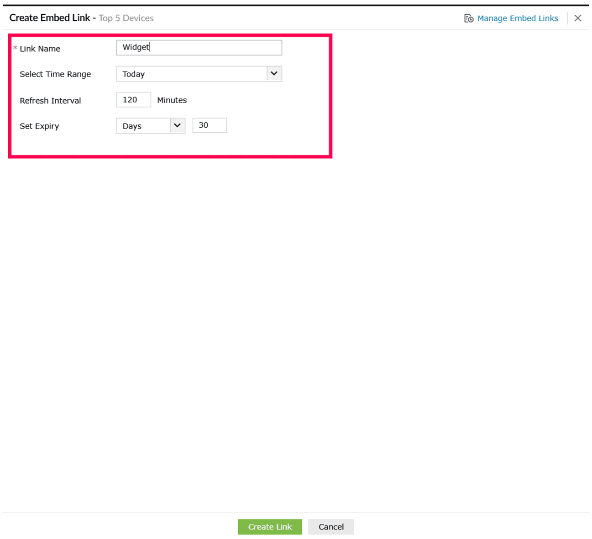
Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

Figure 29: Embedding a widget in the dashboard

2. Provide a unique Link Name.

3. Select the desired Time Range from the drop-down menu.

4. Configure the Refresh Time (60 - 1440 minutes) and Expiry (1- 365 days) using the drop-down options.

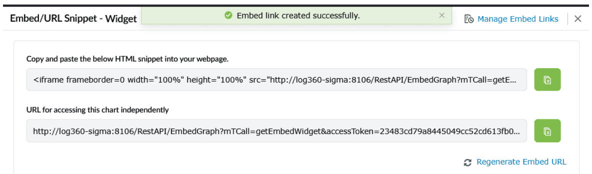


Create Embed Link - Top 5 Devices

* Link Name	Widget
Select Time Range	Today
Refresh Interval	120 Minutes
Set Expiry	Days 30

Figure 30: Configuring an Embed widget link

5. Click Create Link to generate the embed widget link.



Embed/URL Snippet - Widget

Embed link created successfully.

Copy and paste the below HTML snippet into your webpage.

```
<iframe frameborder=0 width="100%" height="100%" src="http://log360-sigma:8106/RestAPI/EmbedGraph?mTCall=getE...
```

URL for accessing this chart independently

```
http://log360-sigma:8106/RestAPI/EmbedGraph?mTCall=getEmbedWidget&accessToken=23483cd79a8445049cc52cd613fb0...
```

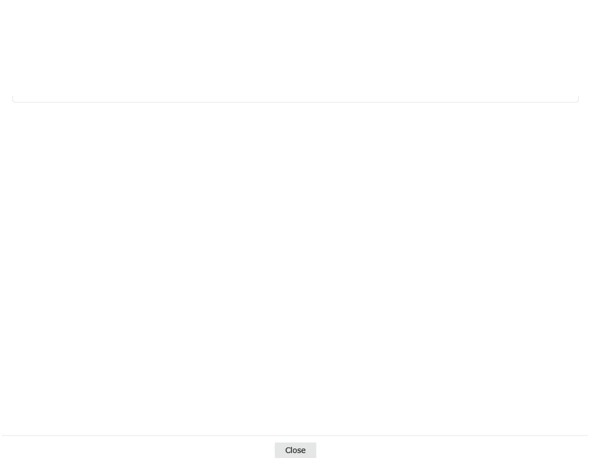


Figure 31: Creating Embed widget links

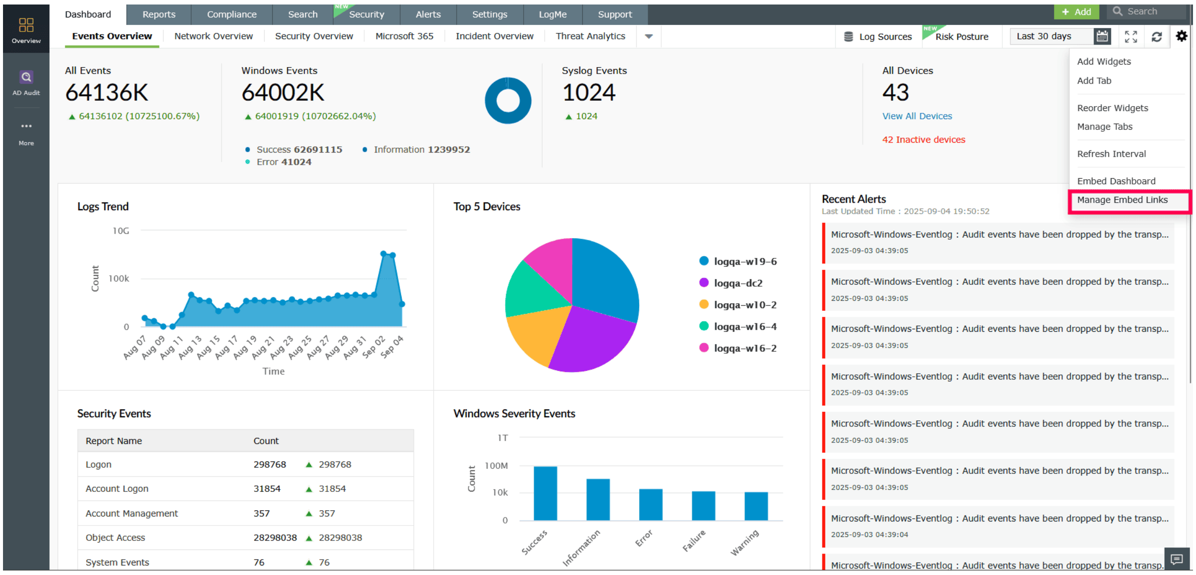
6. To regenerate the link, click Regenerate Embed URL.

> NOTE
>
> - The embedded widget will refresh automatically at the specified interval.
> - The generated external share link will remain valid only until the specified expiry date.

Managing embed links

To manage embed dashboard links,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Manage Embed Links.



Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

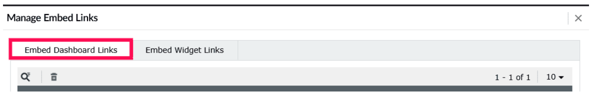
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05

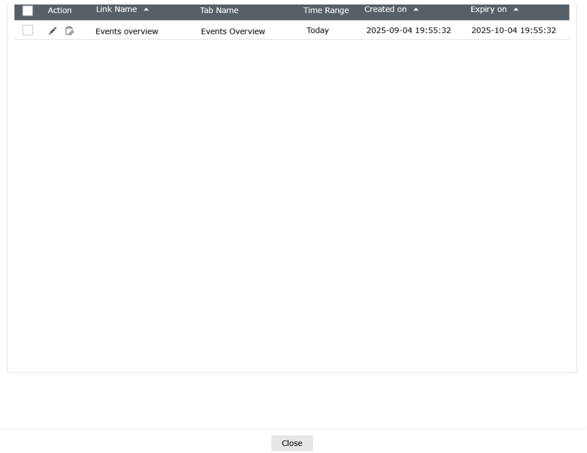
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04

Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...

Figure 32: Accessing Manage Embed Links

2. A table will appear displaying all the Active Dashboard Links. Go to Embed Dashboard Links.

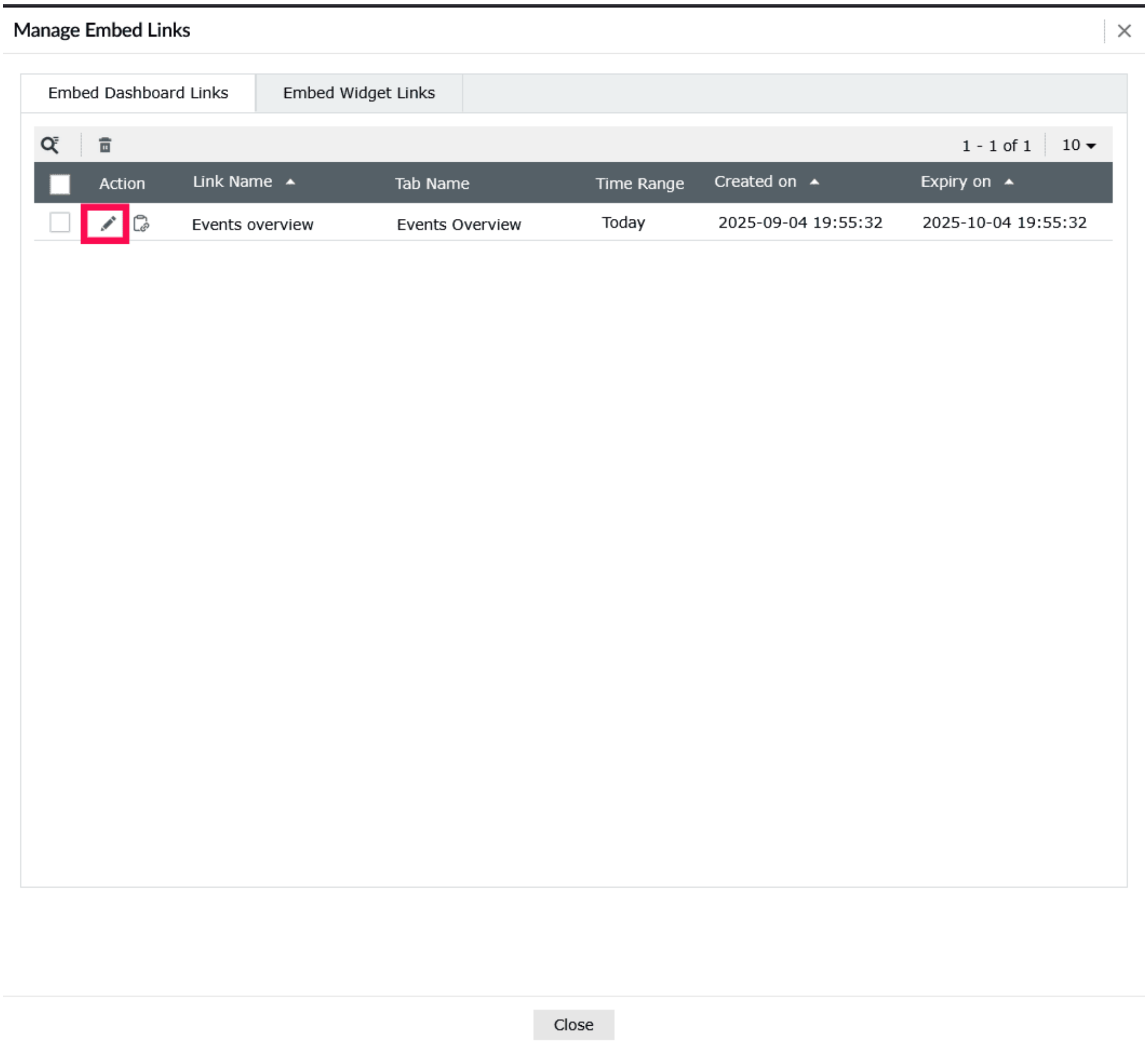




□	Action	Link Name ▲	Tab Name	Time Range	Created on ▲	Expiry on ▲
□		Events overview	Events Overview	Today	2025-09-04 19:55:32	2025-10-04 19:55:32

Figure 33: Viewing Active Dashboard Links

3. To edit a specific link, locate the desired entry and click the Edit option next to it.



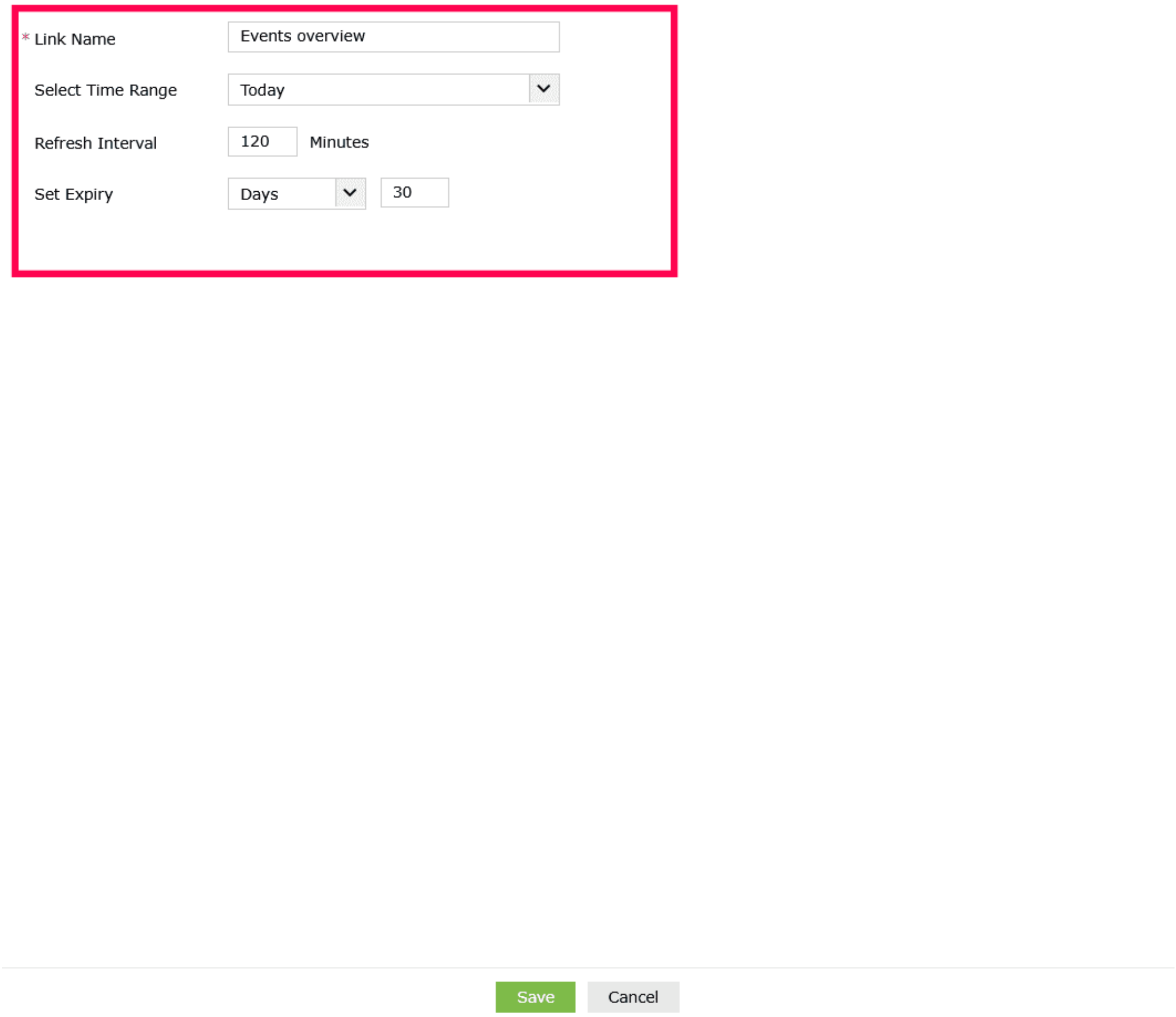
Manage Embed Links

□	Action	Link Name ▲	Tab Name	Time Range	Created on ▲	Expiry on ▲
□		Events overview	Events Overview	Today	2025-09-04 19:55:32	2025-10-04 19:55:32

Figure 34: Editing Embed Widget Links

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

Edit Embed Link - Events Overview

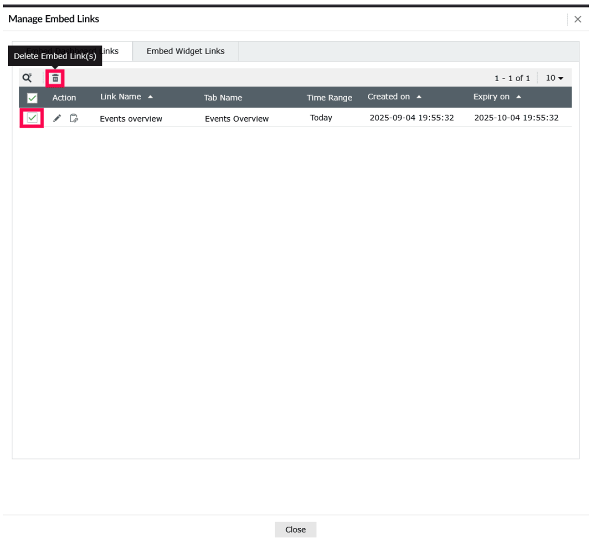


* Link Name	Events overview
Select Time Range	Today
Refresh Interval	120 Minutes
Set Expiry	Days 30

Figure 35: Configuring Edit Embed Link

5. Once done, click Save to apply the updates to the Active Dashboard Link.

6. To delete, select the checkbox next to the entry you want to remove and click the 🗑 icon.



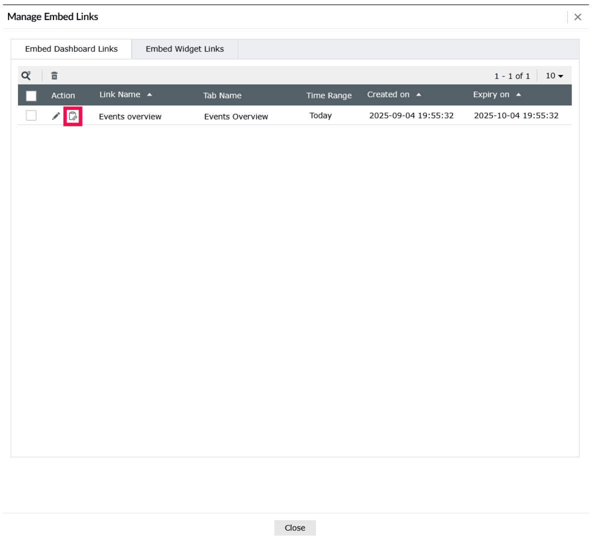
Manage Embed Links

☑	Action	Link Name	Tab Name	Time Range	Created on	Expiry on
☑		Events overview	Events Overview	Today	2025-09-04 19:55:32	2025-10-04 19:55:32

Figure 36: Deleting an embed link

7. In the confirmation pop-up, click Yes to delete the embed link from the list permanently.

8. To regenerate the link, select the icon. In the window that opens, click Regenerate Embed URL to generate a new embed URL while retaining the existing configuration.



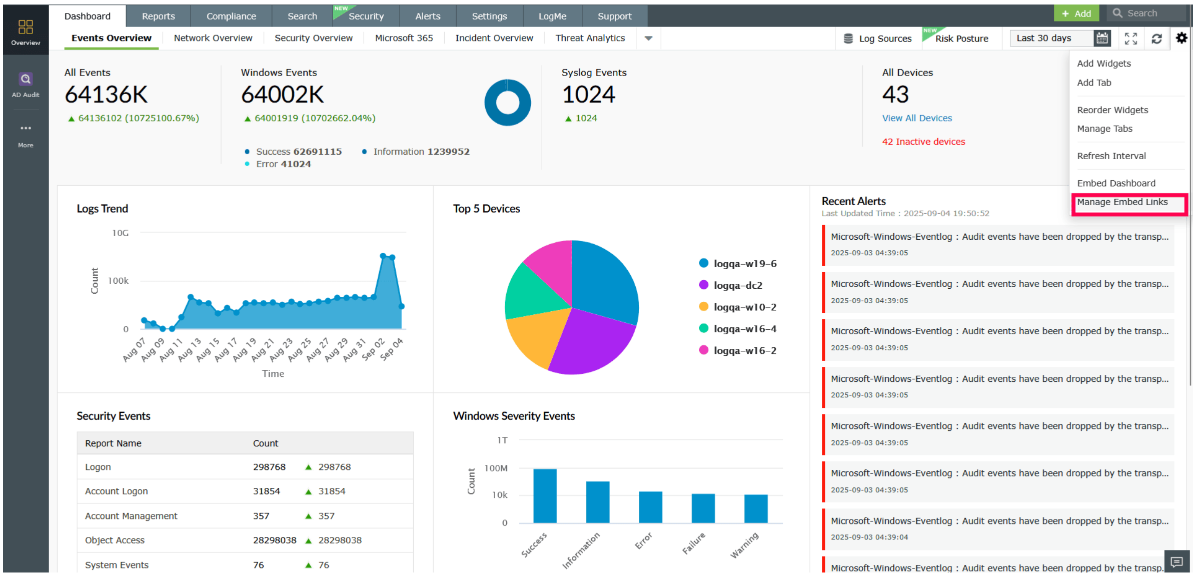
Manage Embed Links

□	Action	Link Name ▲	Tab Name	Time Range	Created on ▲	Expiry on ▲
□		Events overview	Events Overview	Today	2025-09-04 19:55:32	2025-10-04 19:55:32

Figure 37: Regenerating Embed URL

To manage embed widget links,

1. In the dashboard, click the ⚙ icon on the top-right corner and select Manage Embed Links.



All Events
64136K
▲ 64136102 (10725100.67%)

Windows Events
64002K
▲ 64001919 (10702662.04%)
● Success 62691115 ● Information 1239952
● Error 41024

Syslog Events
1024
▲ 1024

All Devices
43
View All Devices
42 Inactive devices

Security Events

Report Name	Count	
Logon	298768	▲ 298768
Account Logon	31854	▲ 31854
Account Management	357	▲ 357
Object Access	28298038	▲ 28298038
System Events	76	▲ 76

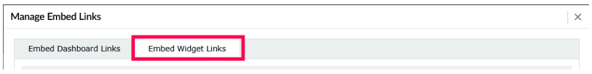
Recent Alerts
Last Updated Time : 2025-09-04 19:50:52

```
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:05
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
2025-09-03 04:39:04
Microsoft-Windows-Eventlog : Audit events have been dropped by the transp...
```

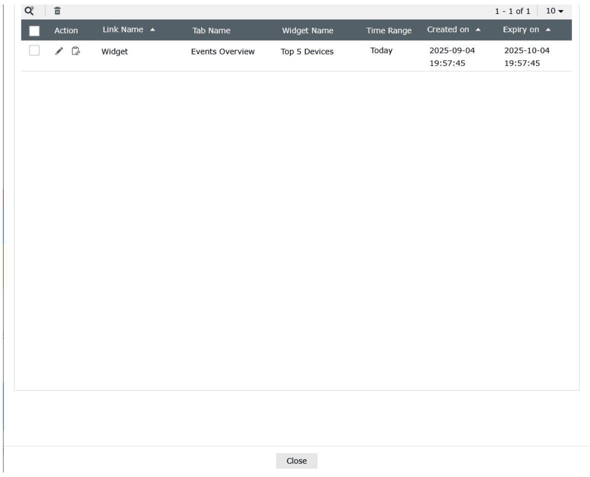
Figure 38: Accessing Manage Embed Links

2. A table will appear displaying all the Active Dashboard Links. Go to Embed Widget Links.

> ⓘ NOTE
>
> Follow the instructions from this step to edit, delete, or regenerate the embed link for a widget.



Manage Embed Links



1 - 1 of 1 | 10

□	Action	Link Name	Tab Name	Widget Name	Time Range	Created on	Expiry on
□		Widget	Events Overview	Top 5 Devices	Today	2025-09-04 19:57:45	2025-10-04 19:57:45

Figure 39: Viewing Active Dashboard Links

Read also

This page explained about customizing the Log360 dashboard to tailor tabs and widgets. To learn more about predefined dashboard views and widget management, refer to the following documents:

- Predefined tabs and widgets

Chapter 2.3 **Reports**

2.3.1. EventLog Analyzer Reports

Last updated on: September 12, 2025

In this page

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.

2.3.2. Manage Predefined Reports

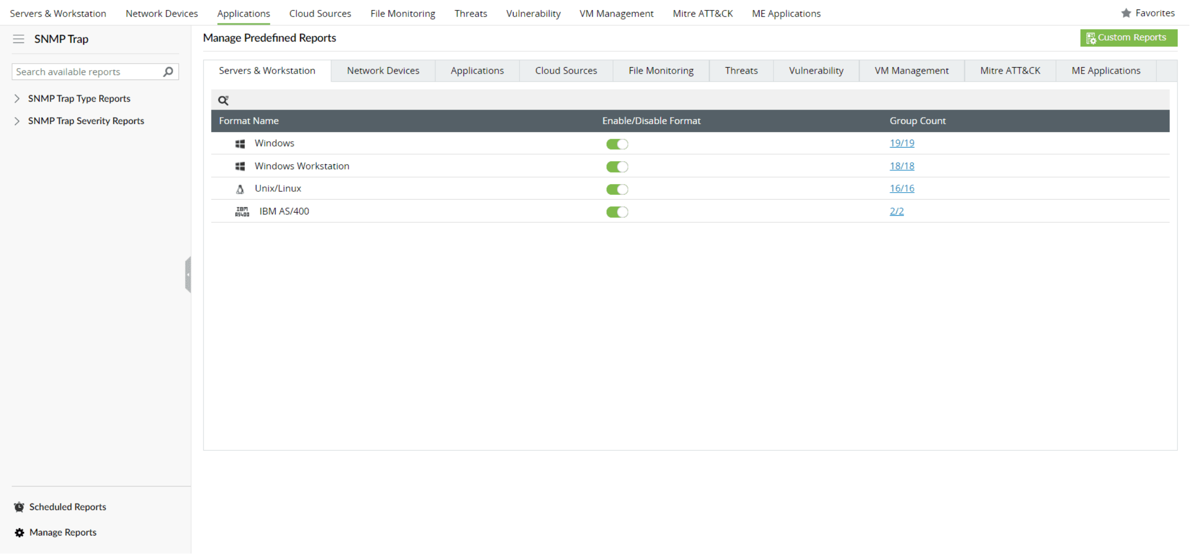
Last updated on: September 12, 2025

EventLog Analyzer allows you to personalize the appearance of the reports page as required. You can customize the arrangement of reports and report groups.

Customizing the arrangement of reports and report groups

To customize the arrangement of reports and report groups, follow the steps given below.

- Open EventLog Analyzer and click on the Reports tab.
- Click on Manage Reports at the bottom of the left panel. Then, click on Manage Predefined Reports at the top right corner.
- Select the required log source by clicking on the corresponding tab.
- The arrangement of the sub-categories of the log sources, as seen on the top bar of the reports page, will be displayed. For example, when Devices is chosen as the log source, the top bar will display the first few devices and the rest is displayed in a drop-down list. You can choose to have your most-used devices displayed first in the top bar to ensure easy access.

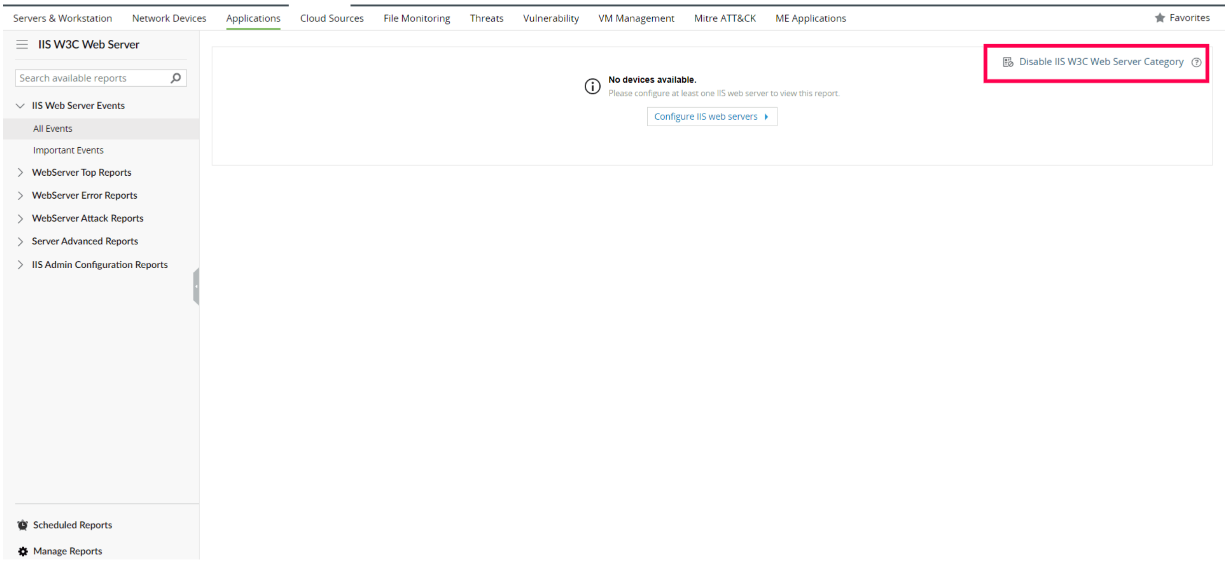


Manage Predefined Reports

Format Name	Enable/Disable Format	Group Count
Windows	●	19/19
Windows Workstation	●	18/18
Unix/Linux	●	16/16
IBM AS/400	●	2/2

- 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.

Category" button available in the top right corner.



No devices available.

Please configure at least one IIS web server to view this report.

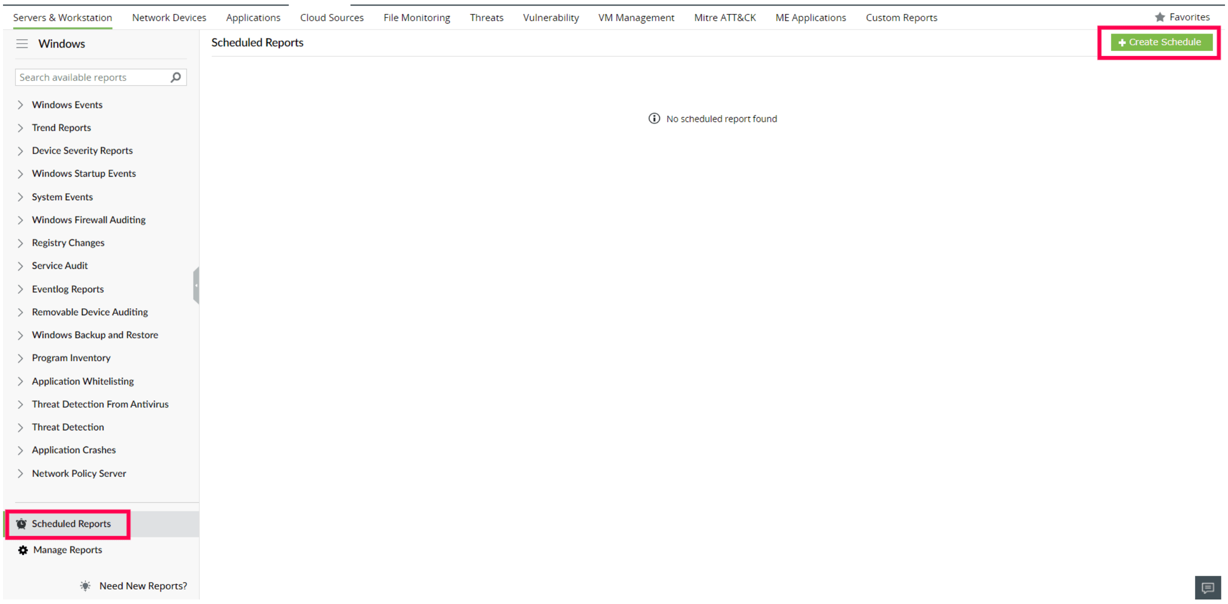
2.3.3. Schedule Reports

Last updated on: September 12, 2025

In this page

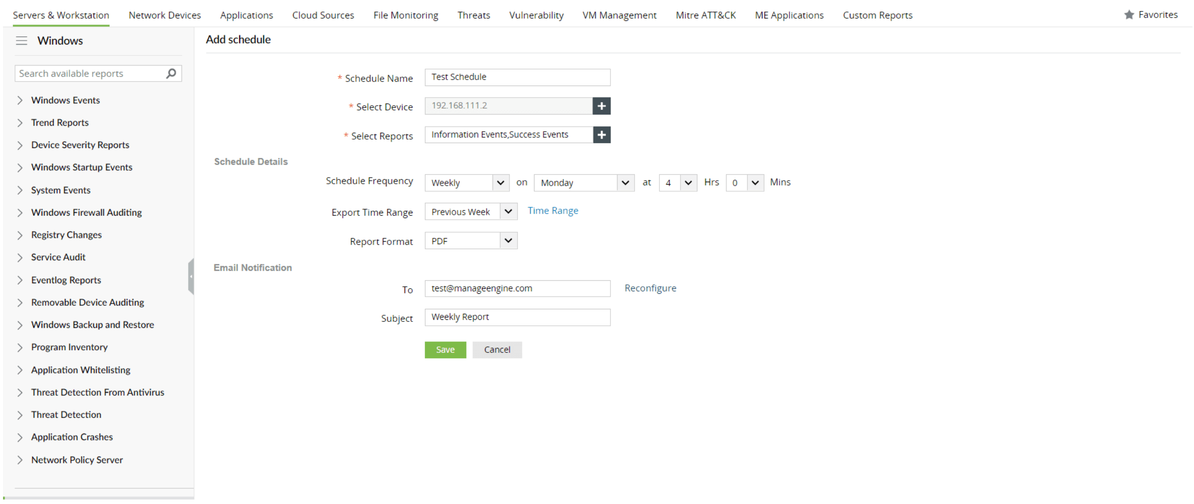
EventLog Analyzer lets you schedule report generation, export, and redistribution over email. This page elaborates on the procedure to create and manage report schedules.

Creating a New Report Schedule



No scheduled report found

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.



Add schedule

* Schedule Name: Test Schedule

* Select Device: 192.168.111.2

* Select Reports: Information Events,Success Events

Schedule Details

Schedule Frequency: Weekly on Monday at 4 Hrs 0 Mins

Export Time Range: Previous Week

Report Format: PDF

Email Notification

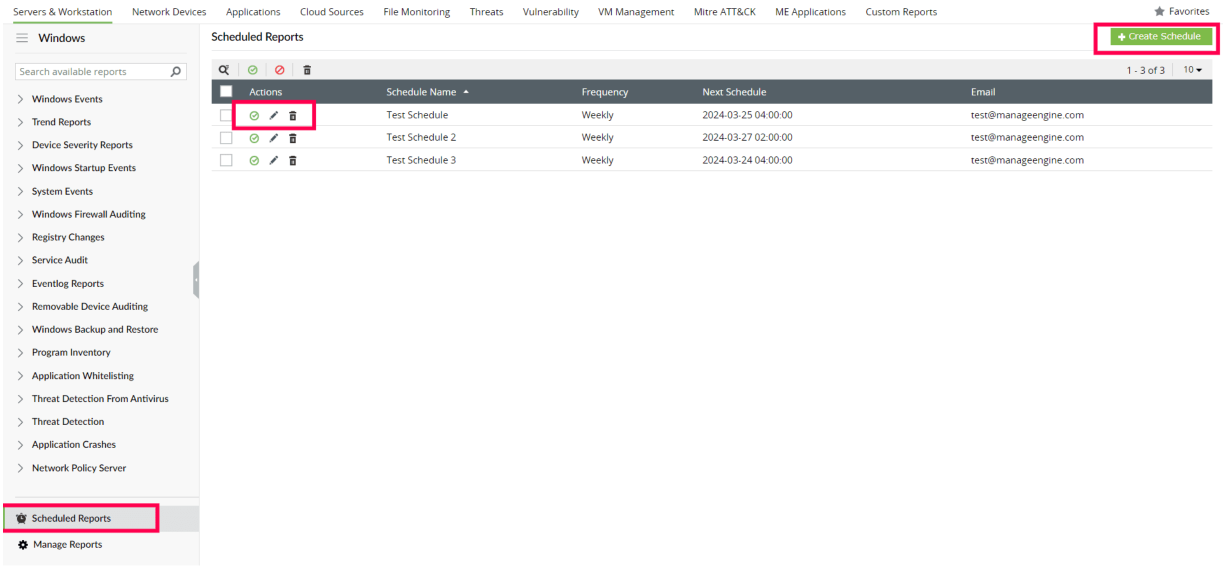
To: test@manageengine.com

Subject: Weekly Report

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.



Actions	Schedule Name	Frequency	Next Schedule	Email
✓ ✎ 🗑	Test Schedule	Weekly	2024-03-25 04:00:00	test@manageengine.com
✓ ✎ 🗑	Test Schedule 2	Weekly	2024-03-27 02:00:00	test@manageengine.com
✓ ✎ 🗑	Test Schedule 3	Weekly	2024-03-24 04:00:00	test@manageengine.com

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.

2.3.4. Custom Reports

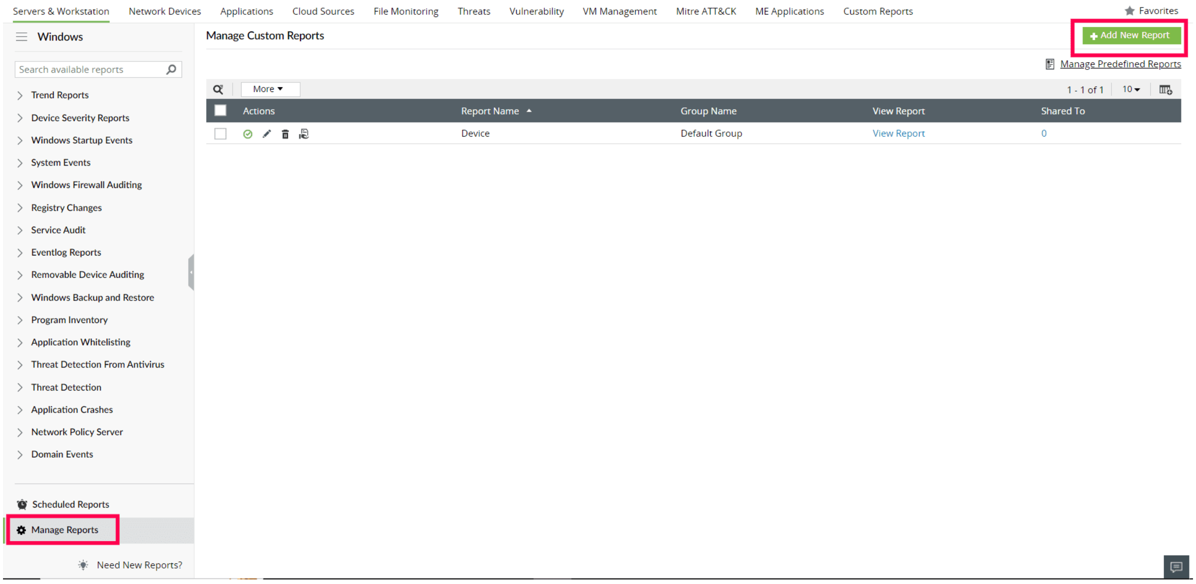
Last updated on: September 12, 2025

In this page

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

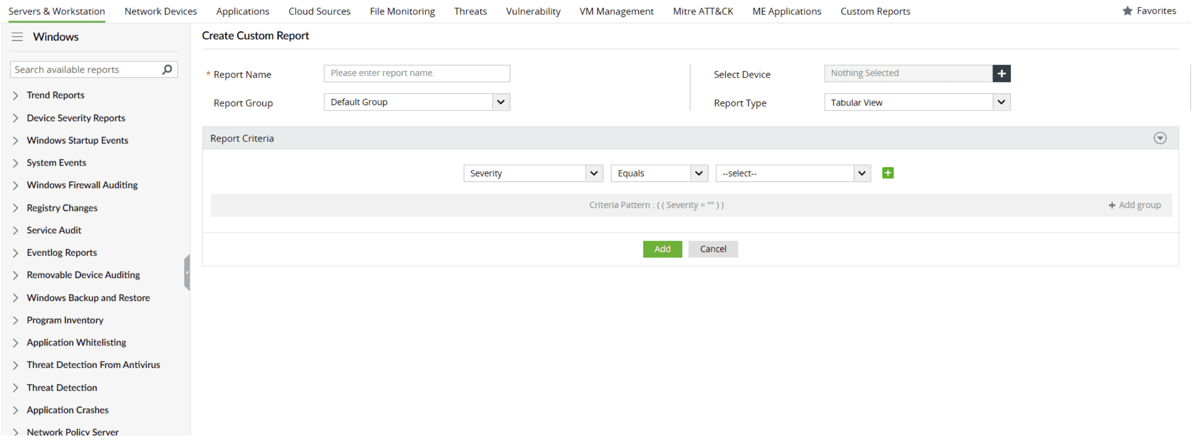
1. Navigate to Reports and select Manage Reports at the bottom-left. In the Manage Reports dashboard, click +Add new reports button on the top-right.



Manage Custom Reports

Actions	Report Name	Group Name	View Report	Shared To
	Device	Default Group	View Report	0

2. In the Create Custom Report dashboard, enter a name for your report.



Create Custom Report

* Report Name: Please enter report name.

Report Group: Default Group

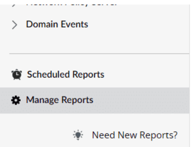
Select Device: Nothing Selected

Report Type: Tabular View

Report Criteria

Severity | Equals | --select--

Criteria Pattern : ((Severity = ""))



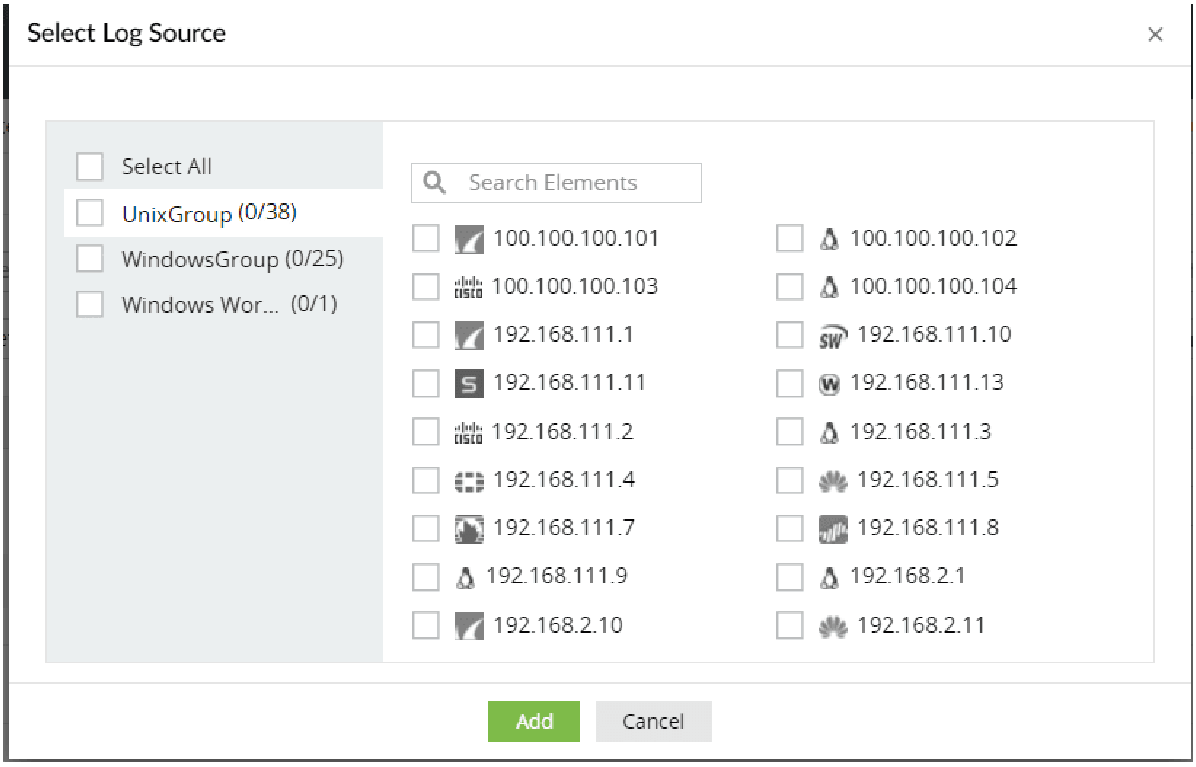
Domain Events

Scheduled Reports

Manage Reports

Need New Reports?

3. Click Select Device to generate reports for specific devices or applications.



Select Log Source

□ Select All

□ UnixGroup (0/38)

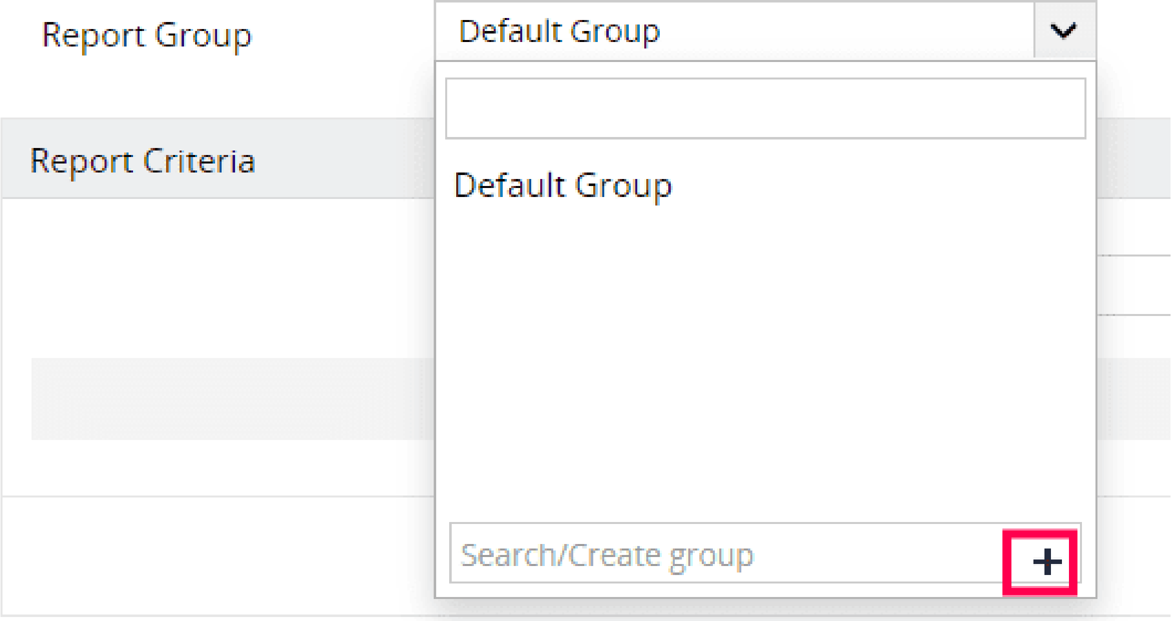
□ WindowsGroup (0/25)

□ Windows Wor... (0/1)

Search Elements

□ 100.100.100.101	□ 100.100.100.102
□ 100.100.100.103	□ 100.100.100.104
□ 192.168.111.1	□ 192.168.111.10
□ 192.168.111.11	□ 192.168.111.13
□ 192.168.111.2	□ 192.168.111.3
□ 192.168.111.4	□ 192.168.111.5
□ 192.168.111.7	□ 192.168.111.8
□ 192.168.111.9	□ 192.168.2.1
□ 192.168.2.10	□ 192.168.2.11

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.



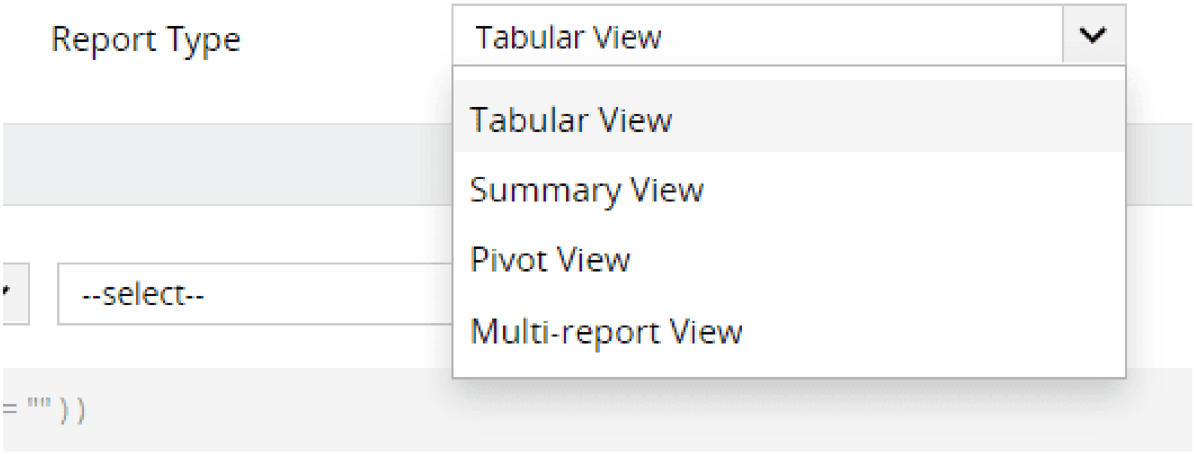
Report Group: Default Group

Report Criteria

Default Group

Search/Create group

5. Select the type of view for your report (see types of view).



Report Type: Tabular 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.

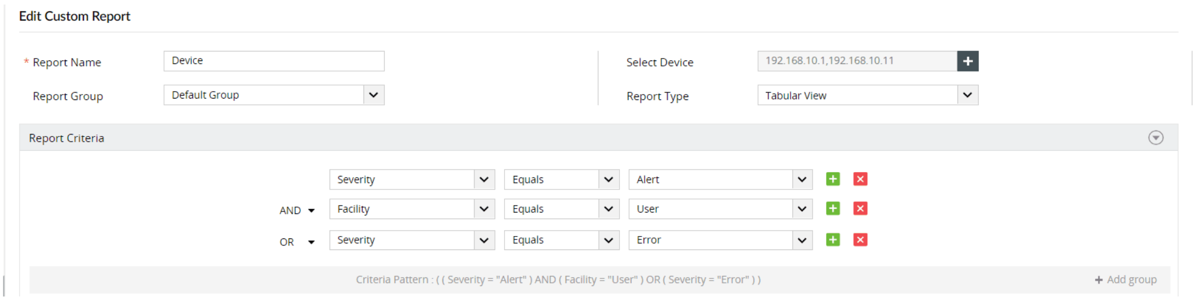
> ⓘ Note
>
> - When the given criteria is separated by commas, it is treated as a separate criteria with OR condition. (Eg: If the criteria is given as EventID = 4678,4679 , then it is treated as EventID= 4678 OR 4679).
> - If you intend to give a single criteria with a comma character, please use "&comma;" 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.



Edit Custom Report

* Report Name: Device

Report Group: Default Group

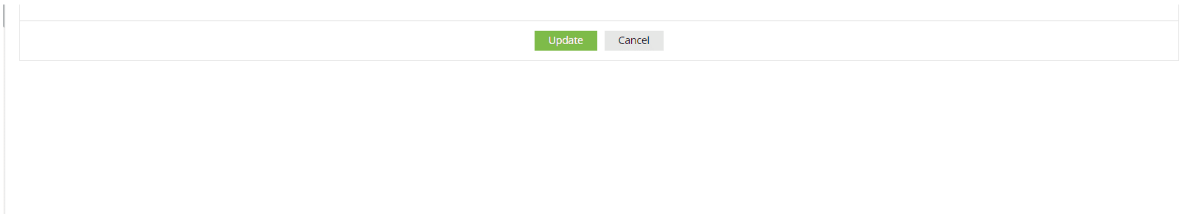
Select Device: 192.168.10.1,192.168.10.11

Report Type: Tabular View

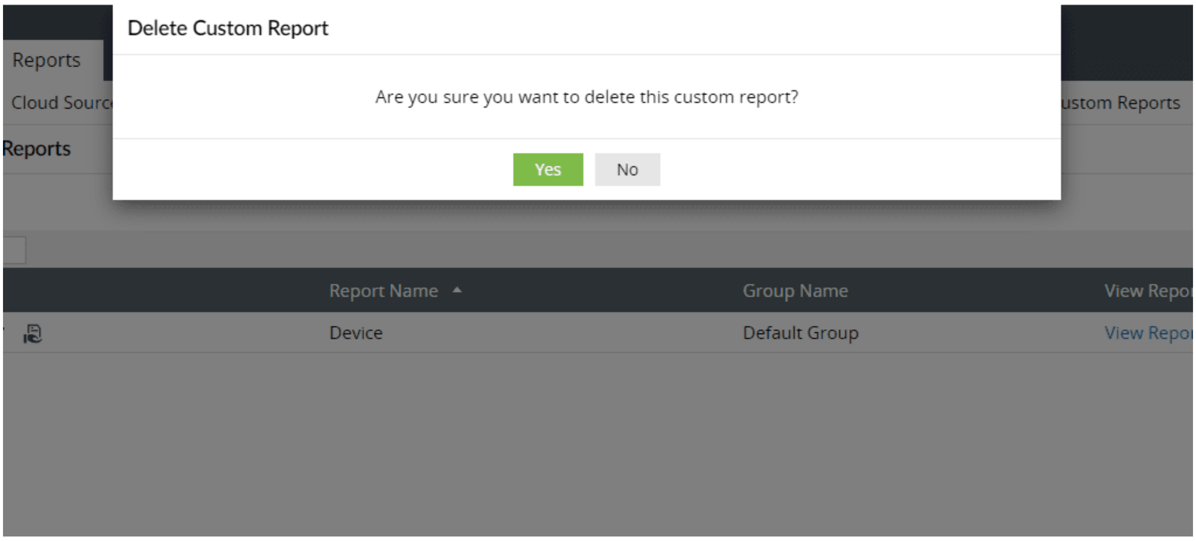
Report Criteria

	Severity	Equals	Alert
AND	Facility	Equals	User
OR	Severity	Equals	Error

Criteria Pattern : ((Severity = "Alert") AND (Facility = "User") OR (Severity = "Error"))



3. To delete a custom-made report, click on the adjacent delete icon. Click Yes in the pop-up box that appears.

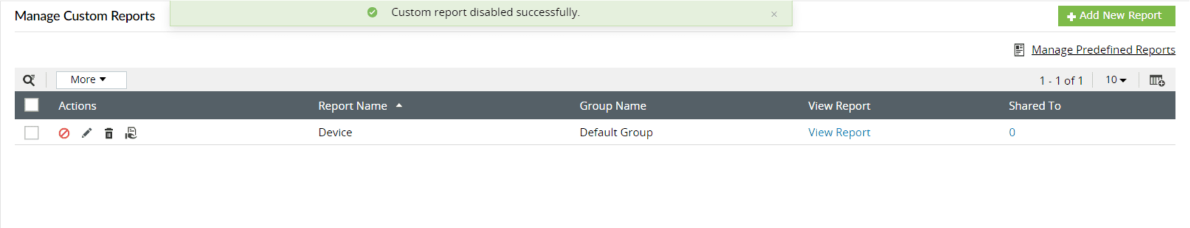


Delete Custom Report

Are you sure you want to delete this custom report?

Report Name	Group Name	View Repo
Device	Default Group	View Repo

4. To disable a custom-made report, click on the corresponding tick box in the Status column.

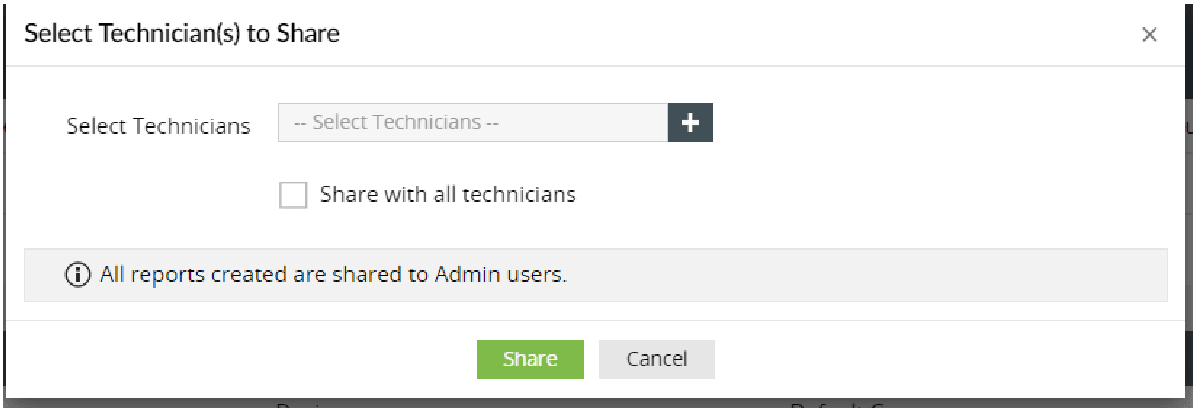


Manage Custom Reports

Custom report disabled successfully.

Actions	Report Name	Group Name	View Report	Shared To
	Device	Default Group	View Report	0

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.



Select Technician(s) to Share

Select Technicians: -- Select Technicians --

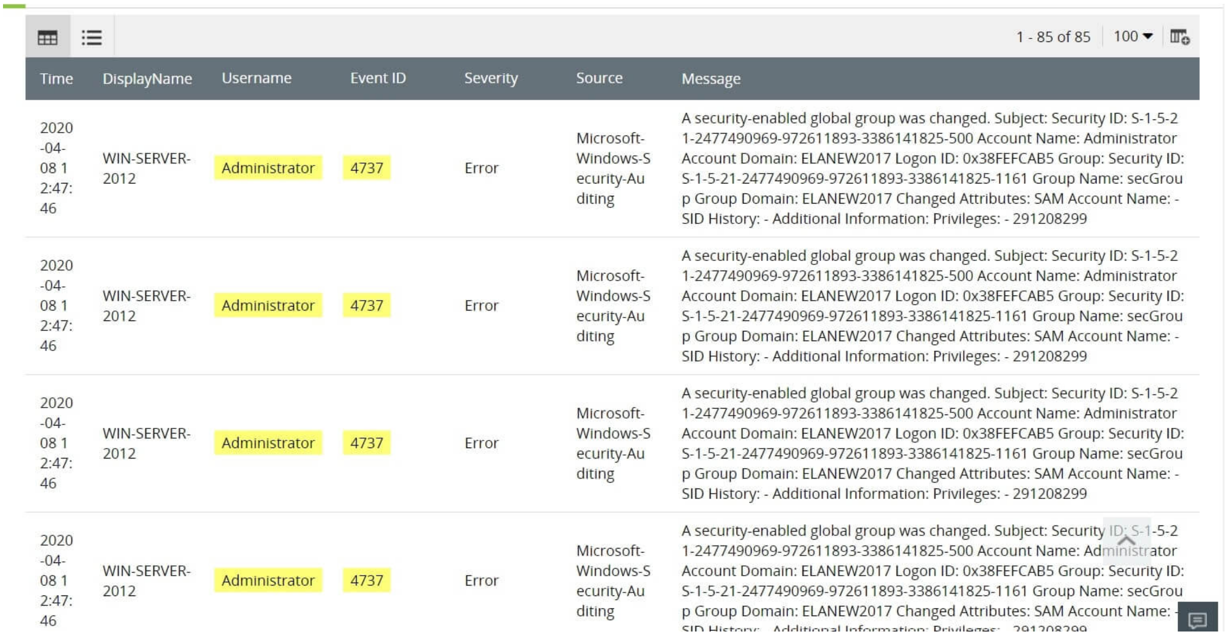
□ Share with all technicians

All reports created are shared to Admin users.

Types of views

Tabular View

This view displays the data in the form of a simple table. You just need to frame the criteria for selecting logs for the report. You can generate different views of the same tabular view report. To create a new view, refer the Manage Report Views section.

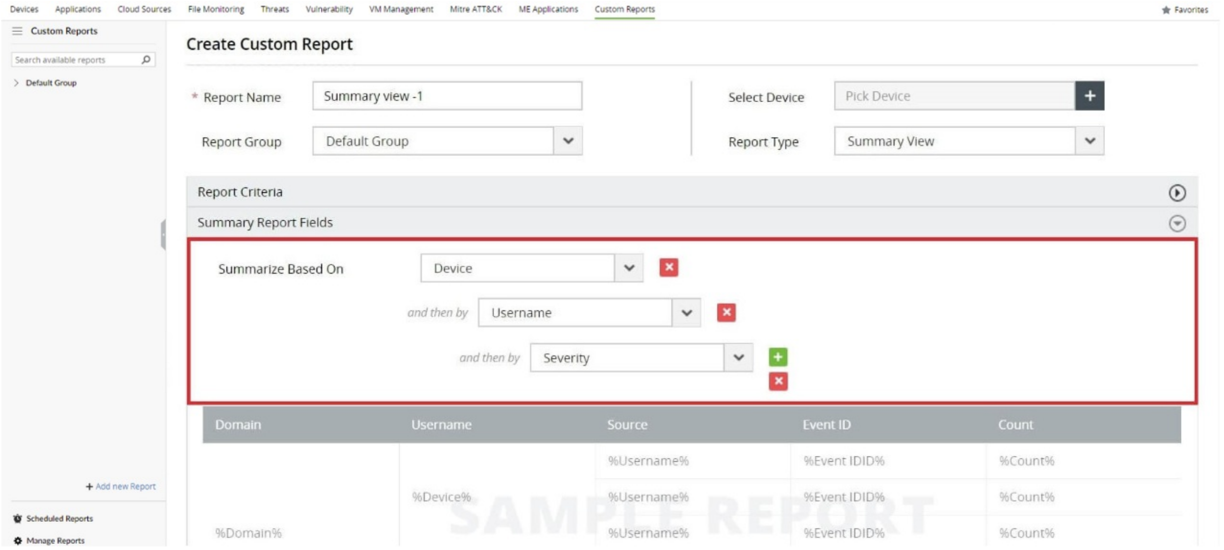


1 - 85 of 85 | 100

Time	DisplayName	Username	Event ID	Severity	Source	Message
2020-04-08 12:47:46	WIN-SERVER-2012	Administrator	4737	Error	Microsoft-Windows-Security-Auditing	A security-enabled global group was changed. Subject: Security ID: S-1-5-21-2477490969-972611893-3386141825-500 Account Name: Administrator Account Domain: ELANEW2017 Logon ID: 0x38FEFCAB5 Group: Security ID: S-1-5-21-2477490969-972611893-3386141825-1161 Group Name: secGroup Group Domain: ELANEW2017 Changed Attributes: SAM Account Name: - SID History: - Additional Information: Privileges: - 291208299
2020-04-08 12:47:46	WIN-SERVER-2012	Administrator	4737	Error	Microsoft-Windows-Security-Auditing	A security-enabled global group was changed. Subject: Security ID: S-1-5-21-2477490969-972611893-3386141825-500 Account Name: Administrator Account Domain: ELANEW2017 Logon ID: 0x38FEFCAB5 Group: Security ID: S-1-5-21-2477490969-972611893-3386141825-1161 Group Name: secGroup Group Domain: ELANEW2017 Changed Attributes: SAM Account Name: - SID History: - Additional Information: Privileges: - 291208299
2020-04-08 12:47:46	WIN-SERVER-2012	Administrator	4737	Error	Microsoft-Windows-Security-Auditing	A security-enabled global group was changed. Subject: Security ID: S-1-5-21-2477490969-972611893-3386141825-500 Account Name: Administrator Account Domain: ELANEW2017 Logon ID: 0x38FEFCAB5 Group: Security ID: S-1-5-21-2477490969-972611893-3386141825-1161 Group Name: secGroup Group Domain: ELANEW2017 Changed Attributes: SAM Account Name: - SID History: - Additional Information: Privileges: - 291208299
2020-04-08 12:47:46	WIN-SERVER-2012	Administrator	4737	Error	Microsoft-Windows-Security-Auditing	A security-enabled global group was changed. Subject: Security ID: S-1-5-21-2477490969-972611893-3386141825-500 Account Name: Administrator Account Domain: ELANEW2017 Logon ID: 0x38FEFCAB5 Group: Security ID: S-1-5-21-2477490969-972611893-3386141825-1161 Group Name: secGroup Group Domain: ELANEW2017 Changed Attributes: SAM Account Name: - SID History: - Additional Information: Privileges: - 291208299

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.



Create Custom Report

* Report Name: Summary view -1

Report Group: Default Group

Select Device: Pick Device

Report Type: Summary View

Report Criteria

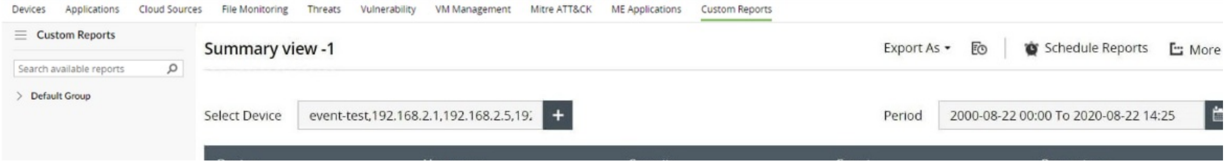
Summary Report Fields

Summarize Based On: Device

and then by: Username

and then by: Severity

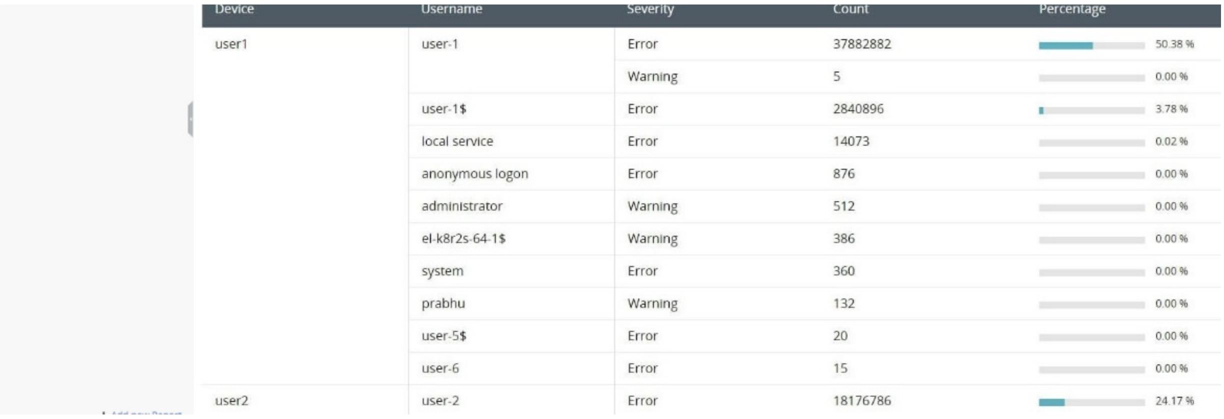
Domain	Username	Source	Event ID	Count
		%Username%	%Event IDID%	%Count%
	%Device%	%Username%	%Event IDID%	%Count%
%Domain%		%Username%	%Event IDID%	%Count%



Summary view -1

Select Device: event-test,192.168.2.1,192.168.2.5,19:

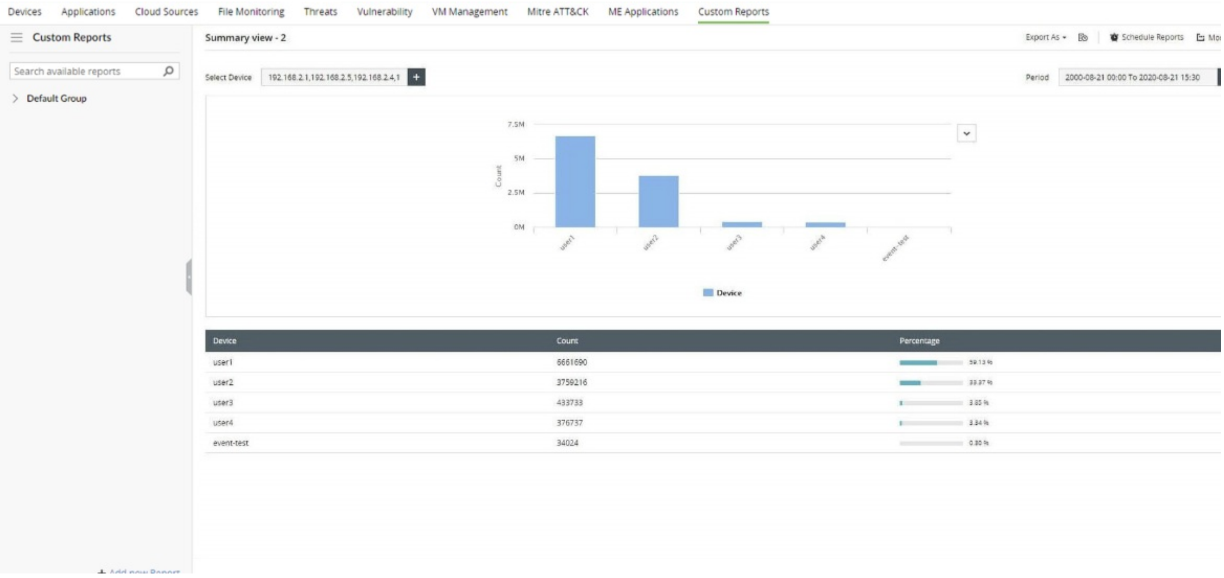
Period: 2000-08-22 00:00 To 2020-08-22 14:25



Device	Username	Severity	Count	Percentage
user1	user-1	Error	37882882	50.38 %
		Warning	5	0.00 %
	user-1$	Error	2840896	3.78 %
	local service	Error	14073	0.02 %
	anonymous logon	Error	876	0.00 %
	administrator	Warning	512	0.00 %
	el-k8r2s-64-1$	Warning	386	0.00 %
	system	Error	360	0.00 %
	prabhu	Warning	132	0.00 %
	user-5$	Error	20	0.00 %
	user-6	Error	15	0.00 %
user2	user-2	Error	18176786	24.17 %

ⓘ Note

When you apply onlyone criteria, a graph would be generated. When you apply more than one criteria, a graph would not get generated, but the data would be displayed in a table.



Summary view - 2

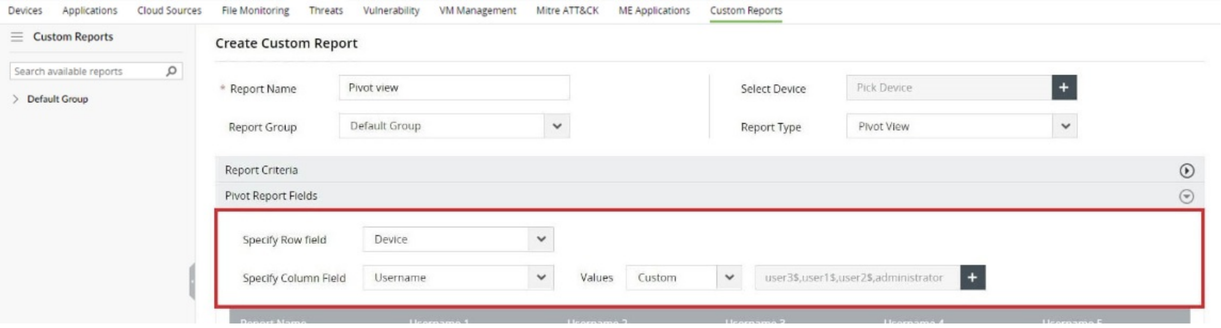
Select Device 192.168.2.1,192.168.2.5,192.168.2.4,1

Period 2000-08-21 00:00 To 2020-08-21 15:30

Device	Count	Percentage
user1	6661690	59.13 %
user2	3759216	33.37 %
user3	433733	3.85 %
user4	376737	3.34 %
event-test	34024	0.30 %

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'.



Create Custom Report

* Report Name: Pivot view

Report Group: Default Group

Select Device: Pick Device

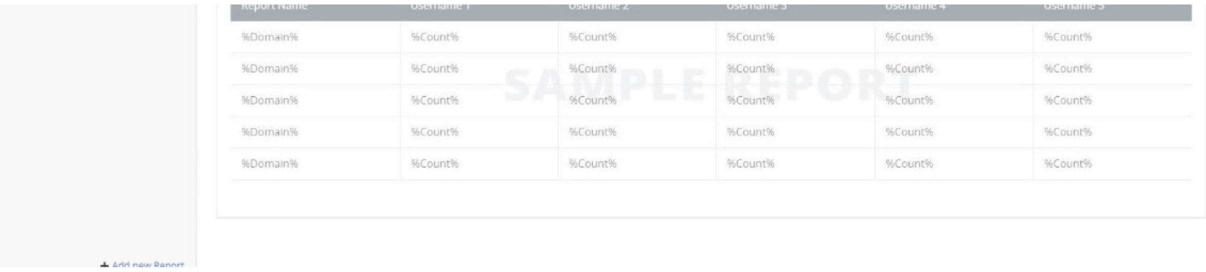
Report Type: Pivot View

Specify Row field: Device

Specify Column Field: Username

Values: Custom

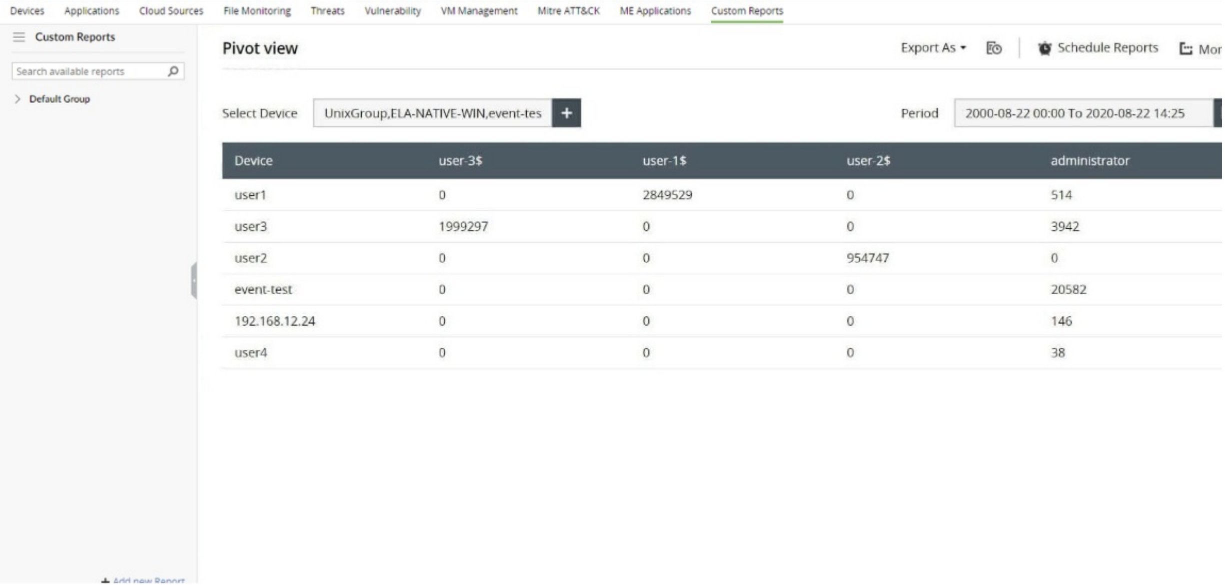
user3$,user1$,user2$,administrator



Report Name	Username 1	Username 2	Username 3	Username 4	Username 5
%Domain%	%Count%	%Count%	%Count%	%Count%	%Count%
%Domain%	%Count%	%Count%	%Count%	%Count%	%Count%
%Domain%	%Count%	%Count%	%Count%	%Count%	%Count%
%Domain%	%Count%	%Count%	%Count%	%Count%	%Count%
%Domain%	%Count%	%Count%	%Count%	%Count%	%Count%

Note

A maximum of five values can be chosen for monitoring.



Pivot view

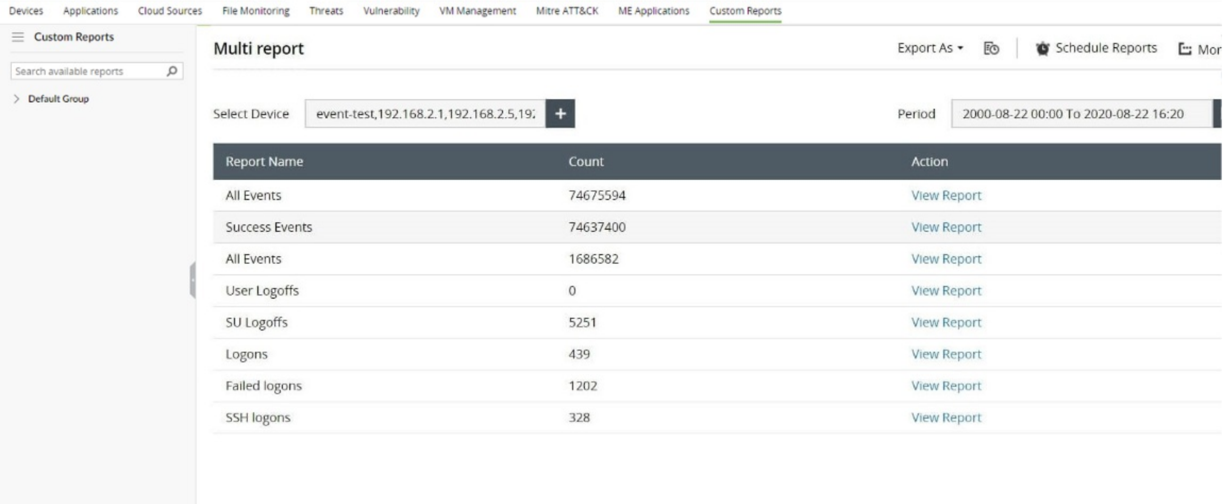
Select Device UnixGroup,ELA-NATIVE-WIN,event-tes

Period 2000-08-22 00:00 To 2020-08-22 14:25

Device	user-3$	user-1$	user-2$	administrator
user1	0	2849529	0	514
user3	1999297	0	0	3942
user2	0	0	954747	0
event-test	0	0	0	20582
192.168.12.24	0	0	0	146
user4	0	0	0	38

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.



Multi report

Select Device event-test,192.168.2.1,192.168.2.5,19:

Period 2000-08-22 00:00 To 2020-08-22 16:20

Report Name	Count	Action
All Events	74675594	View Report
Success Events	74637400	View Report
All Events	1686582	View Report
User Logoffs	0	View Report
SU Logoffs	5251	View Report
Logons	439	View Report
Failed logons	1202	View Report
SSH logons	328	View Report

+ Add new Report

2.3.5. Manage Report Views

Last updated on: September 12, 2025

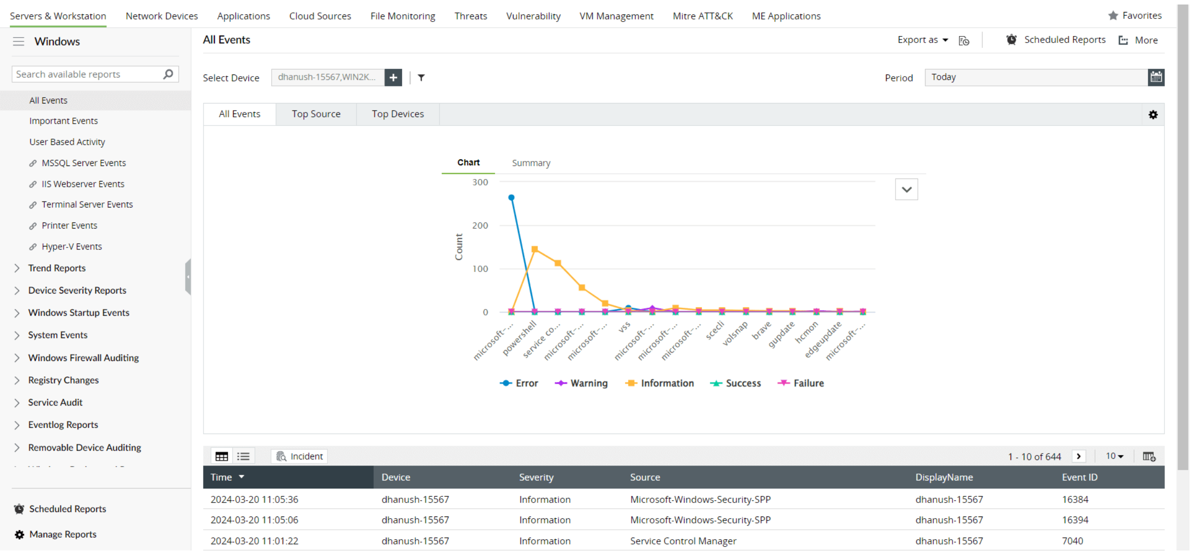
EventLog Analyzer allows you to create multiple views of the same report. This enables you to view the report based on different parameters such as time, domain, source, etc. The different views will be generated from the same set of log data.

In this help document, you will learn to perform the following operations.

Creating a new report view

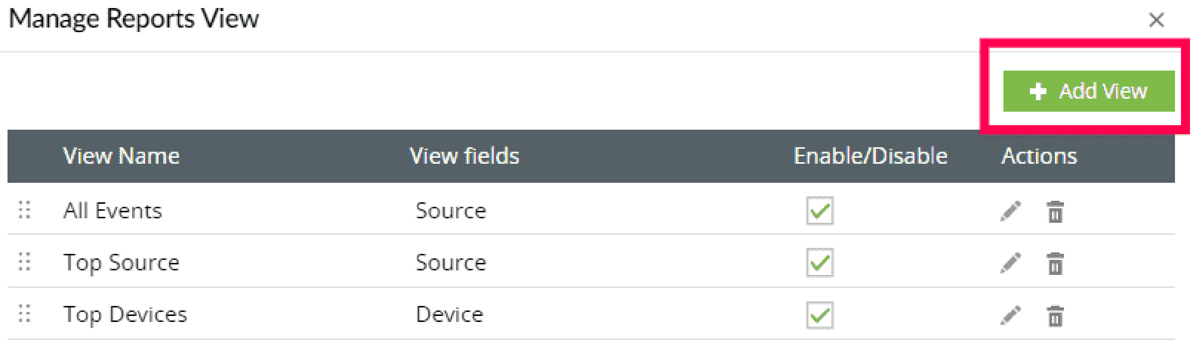
To create a new report view,

- Open EventLog Analyzer and select the Reports tab.
- Choose the required report and click on the ⚙ (Manage Custom Views) icon present on the right corner.



Time	Device	Severity	Source	DisplayName	Event ID
2024-03-20 11:05:36	dhanush-15567	Information	Microsoft-Windows-Security-SPP	dhanush-15567	16384
2024-03-20 11:05:06	dhanush-15567	Information	Microsoft-Windows-Security-SPP	dhanush-15567	16394
2024-03-20 11:01:22	dhanush-15567	Information	Service Control Manager	dhanush-15567	7040

- In the pop-up window that appears, click on +Add View.



View Name	View fields	Enable/Disable	Actions
All Events	Source	✓	
Top Source	Source	✓	
Top Devices	Device	✓	

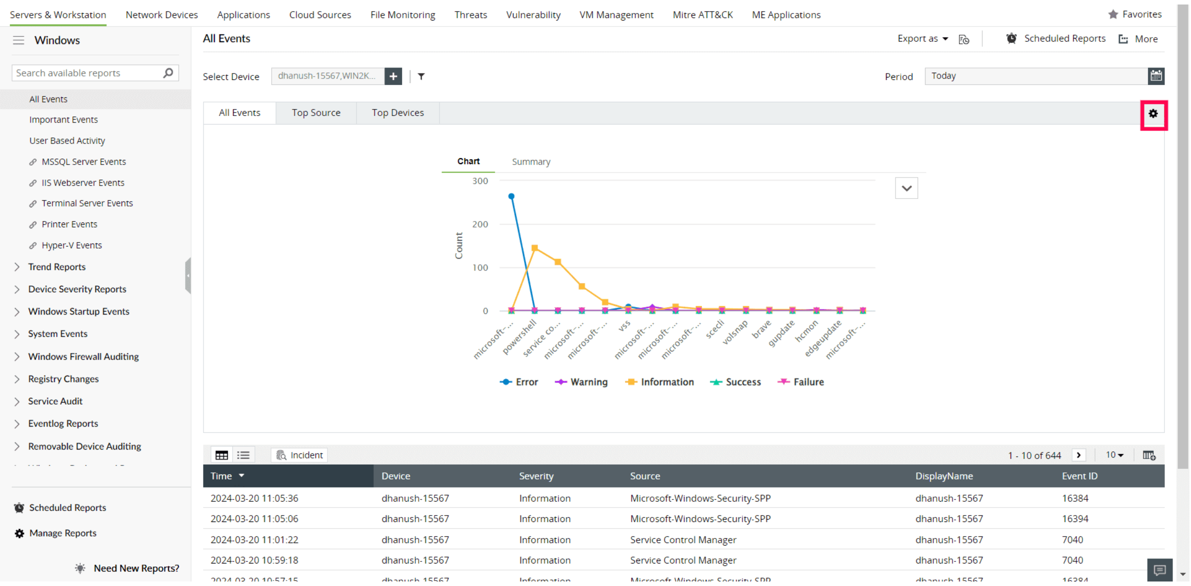
Close

- 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

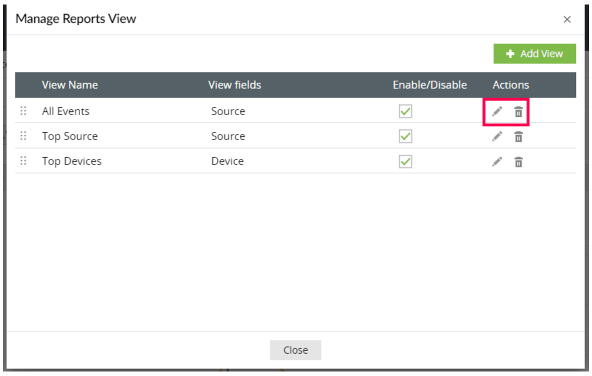
To edit, delete, or disable the views that have been created:

- 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.



Time	Device	Severity	Source	DisplayName	Event ID
2024-03-20 11:05:36	dhanush-15567	Information	Microsoft-Windows-Security-SPP	dhanush-15567	16384
2024-03-20 11:05:06	dhanush-15567	Information	Microsoft-Windows-Security-SPP	dhanush-15567	16394
2024-03-20 11:01:22	dhanush-15567	Information	Service Control Manager	dhanush-15567	7040
2024-03-20 10:59:18	dhanush-15567	Information	Service Control Manager	dhanush-15567	7040
2024-03-20 10:57:15	dhanush-15567	Information	Microsoft-Windows-Security-SPP	dhanush-15567	16384

- In the pop-up that appears you can see a list of views for that report.



View Name	View fields	Enable/Disable	Actions
All Events	Source	☑	✎ 🗑
Top Source	Source	☑	✎ 🗑
Top Devices	Device	☑	✎ 🗑

- 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.

2.3.6. Adding reports to the Favorites section

Last updated on: September 12, 2025

In this page

> Adding a report to the Favorites Section
>
> Adding a widget to the EventLog Analyzer Dashboard

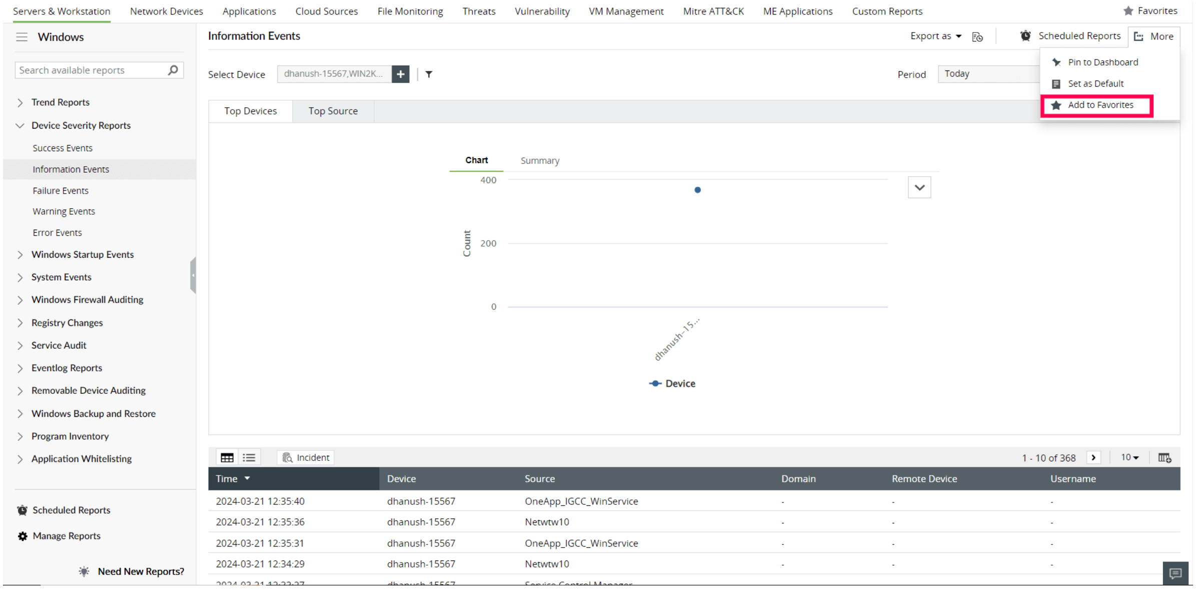
If you have reports that you frequently refer to, these can either be added to the "Favorites" section or they can be pinned as a widget in the dashboard for quick access.

Adding a report to the Favorites Section

From the list of available reports, you can select up to 20 reports to be added to the Favorites section.

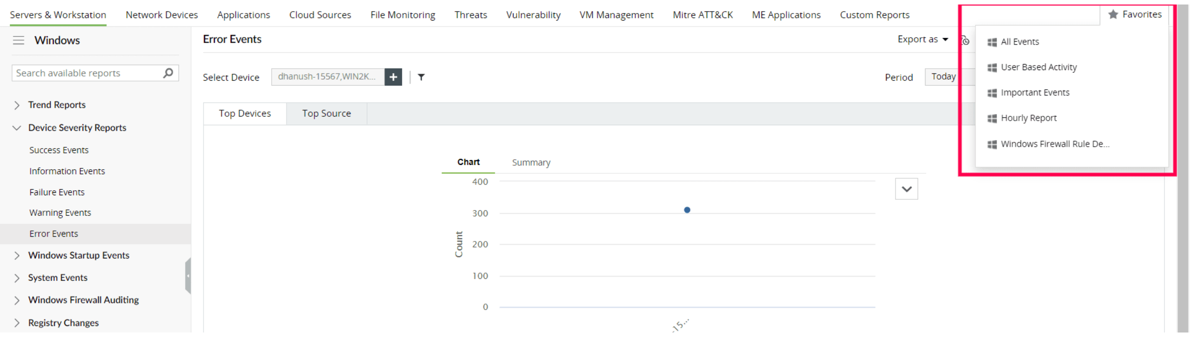
To add reports to Favorites,

- Navigate to the required report.



Time	Device	Source	Domain	Remote Device	Username
2024-03-21 12:35:40	dhanush-15567	OneApp_IGCC_WinService	-	-	-
2024-03-21 12:35:36	dhanush-15567	Netwtw10	-	-	-
2024-03-21 12:35:31	dhanush-15567	OneApp_IGCC_WinService	-	-	-
2024-03-21 12:34:29	dhanush-15567	Netwtw10	-	-	-
2024-03-21 12:33:37	dhanush-15567	Service Control Manager			

- 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,

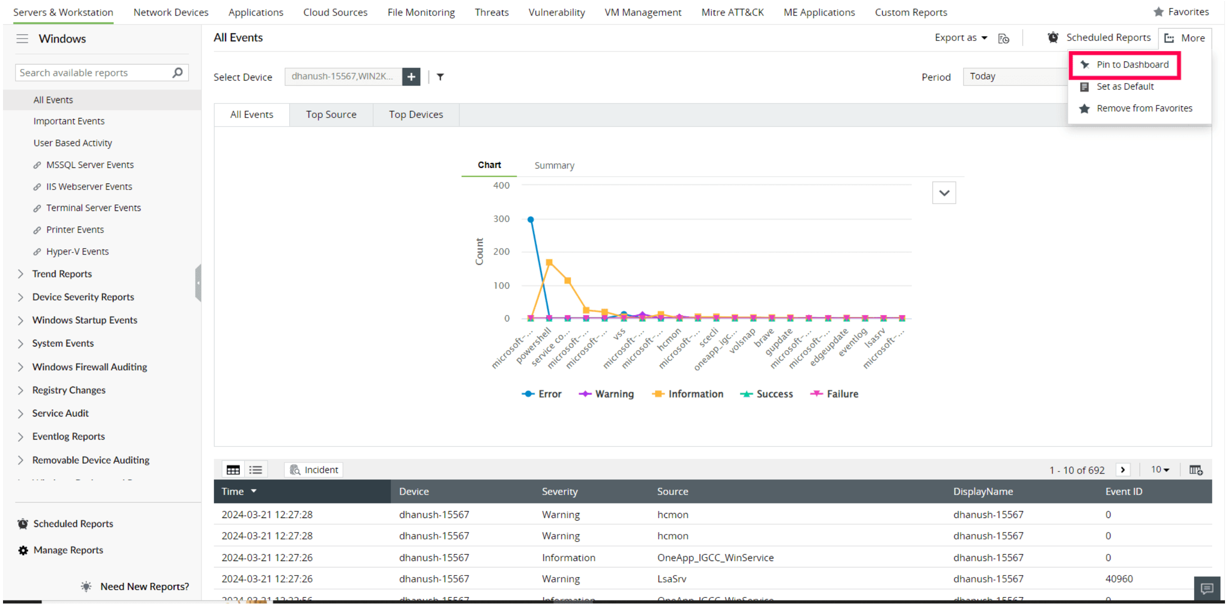
- Navigate to the report which you want to remove from Favorites.
- On the right top corner of the tab, click More and select Remove from Favorites.

> 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.



Time	Device	Severity	Source	DisplayName	Event ID
2024-03-21 12:27:28	dhanush-15567	Warning	hcmon	dhanush-15567	0
2024-03-21 12:27:28	dhanush-15567	Warning	hcmon	dhanush-15567	0
2024-03-21 12:27:26	dhanush-15567	Information	OneApp_IGCC_WinService	dhanush-15567	0
2024-03-21 12:27:26	dhanush-15567	Warning	LsaSrv	dhanush-15567	40960

2.3.7. Report export and customization

Last updated on: September 12, 2025

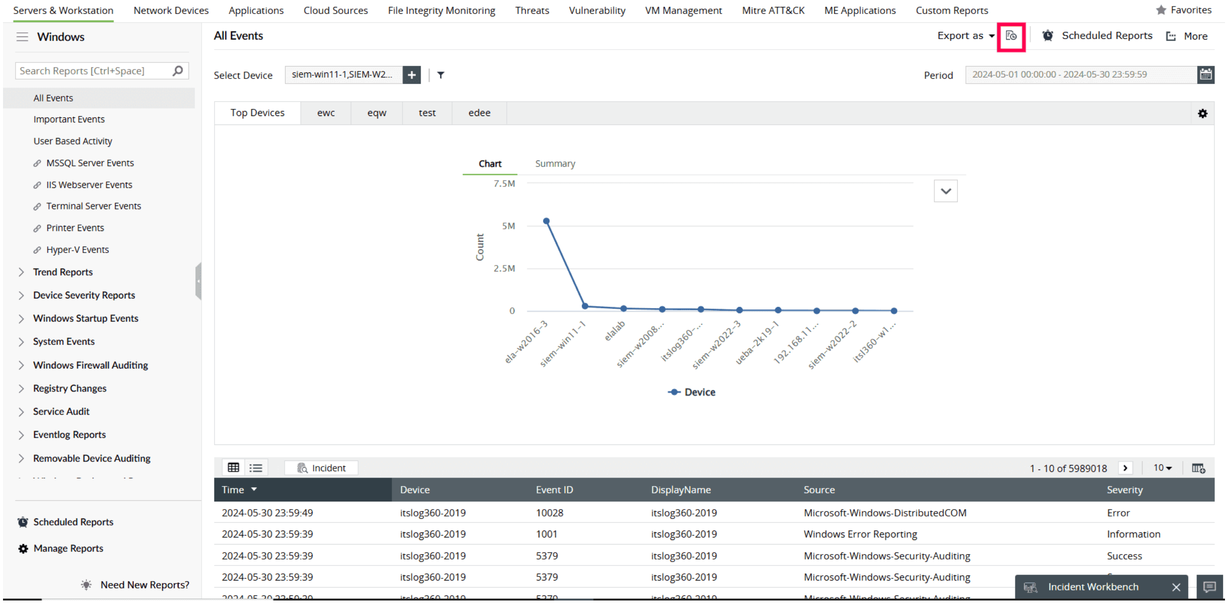
EventLog Analyzer allows you to export reports, add or remove columns in a report and pin the graph to the dashboard.
In this help document, you will learn to perform the following operations.

Report exporting:

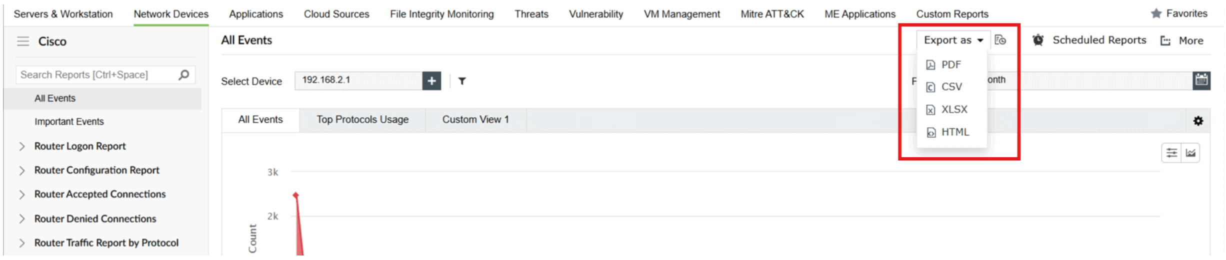
EventLog Analyzer gives users the ability to export reports as PDF, CSV, XLSX(Exports data with a default limit of 50,000 records per sheet) and HTML(Exports data into an HTML file for easier viewing in browsers)
To export reports,

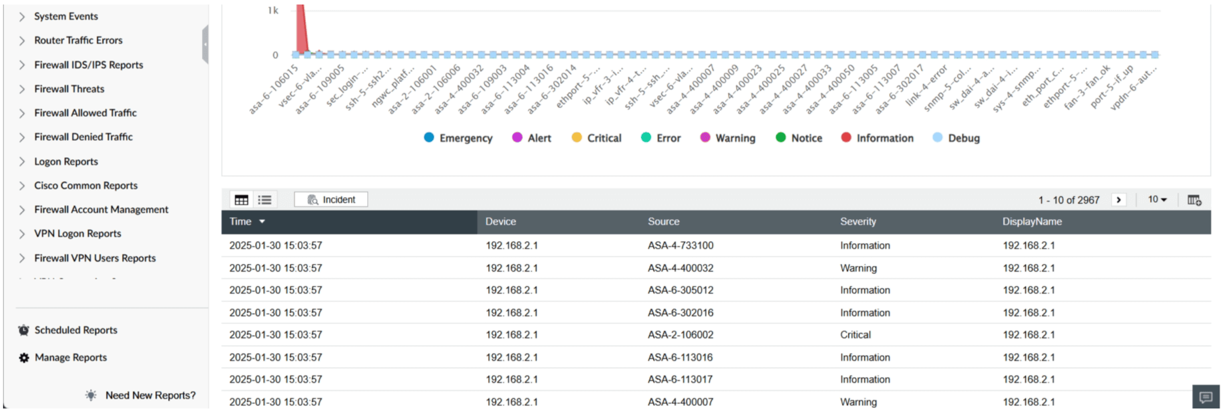
- Select the report you want to export and click the Export as drop-down button on the top-right corner of the report.
- Select the format(PDF, CSV, XLSX and HTML.) in which you want the report to be exported.
- The export history section will open automatically to display the export queue.
- For each export, you have the option of downloading the report from the queue by selecting an appropriate option.

To view export history, click the 🗋 at the top-right corner of a report. A list of the most recently exported reports will be displayed.



Time	Device	Event ID	DisplayName	Source	Severity
2024-05-30 23:59:49	itslog360-2019	10028	itslog360-2019	Microsoft-Windows-DistributedCOM	Error
2024-05-30 23:59:39	itslog360-2019	1001	itslog360-2019	Windows Error Reporting	Information
2024-05-30 23:59:39	itslog360-2019	5379	itslog360-2019	Microsoft-Windows-Security-Auditing	Success
2024-05-30 23:59:39	itslog360-2019	5379	itslog360-2019	Microsoft-Windows-Security-Auditing	





Time	Device	Source	Severity	DisplayName
2025-01-30 15:03:57	192.168.2.1	ASA-4-733100	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-4-400032	Warning	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-305012	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-302016	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-2-106002	Critical	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-113016	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-113017	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-4-400007	Warning	192.168.2.1

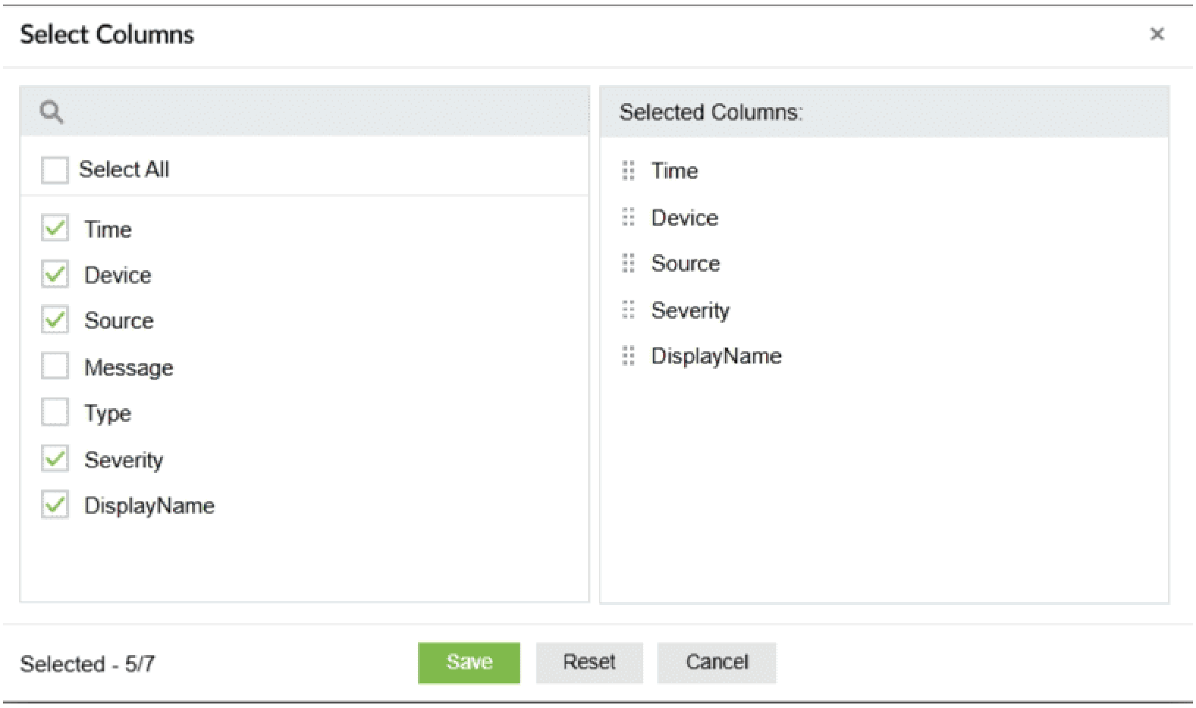
> ⓘ Note
>
> XLSX and HTML exports will include only tabular data and will not include graphs.

Adding or removing columns:

EventLog Analyzer gives users the ability to add or remove columns to the reports.

To add or remove columns:

- Select the report you want to add or remove columns and click ▥ on the top-right corner of the report.
- In the pop-up window, select the fields you want to display in the search results by ticking the corresponding boxes. To exclude fields, simply leave the boxes unticked.



Select Columns ×

□ Select All

☑ Time
☑ Device
☑ Source
□ Message
□ Type
☑ Severity
☑ DisplayName

Selected Columns:

Time
Device
Source
Severity
DisplayName

Selected - 5/7

- You can also rearrange the selected columns by dragging and dropping the column names accordingly, in the Selected Columns section.

- Click Save to apply your preferences.
- Now you have the options to Select all and Reset back to default settings.

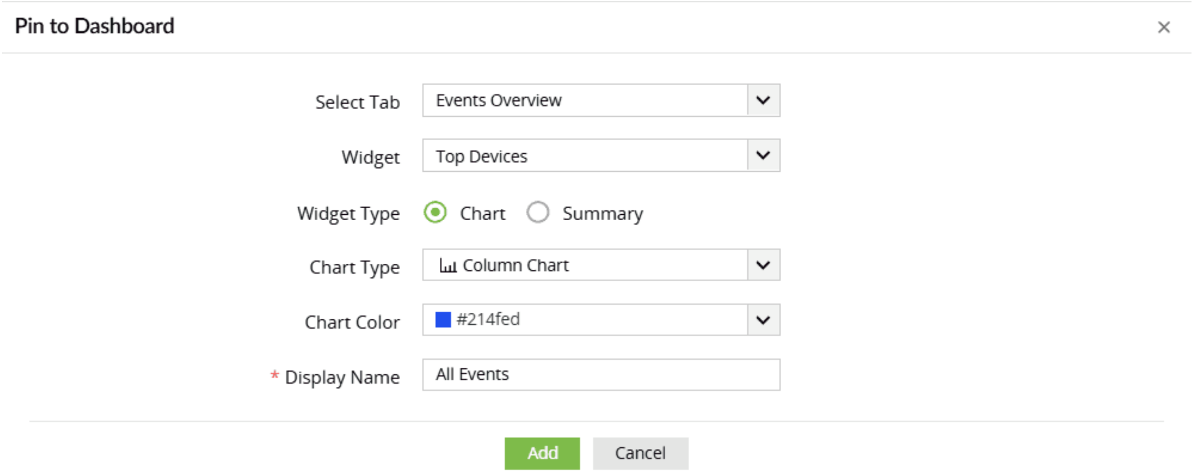
> Note:
>
> - When the reports are exported, the columns that have been selected will be represented.
> - Select All will be shown only when the Number of Fields is less than 10.

Pinning the graph to the dashboard:

EventLog Analyzer gives users the ability to pin graphs to the dashboard.

To pin a graph:

- Select the report you want to pin.
- Click the More drop-down button on the top right corner and select Pin to Dashboard.
- In the pop-up window, you can select the tab, widget, widget type, and display name of the widget that you'd like to pin.



Pin to Dashboard ×

Select Tab: Events Overview

Widget: Top Devices

Widget Type: ● Chart ○ Summary

Chart Type: Column Chart

Chart Color: 🟦 #214fed

* Display Name: All Events

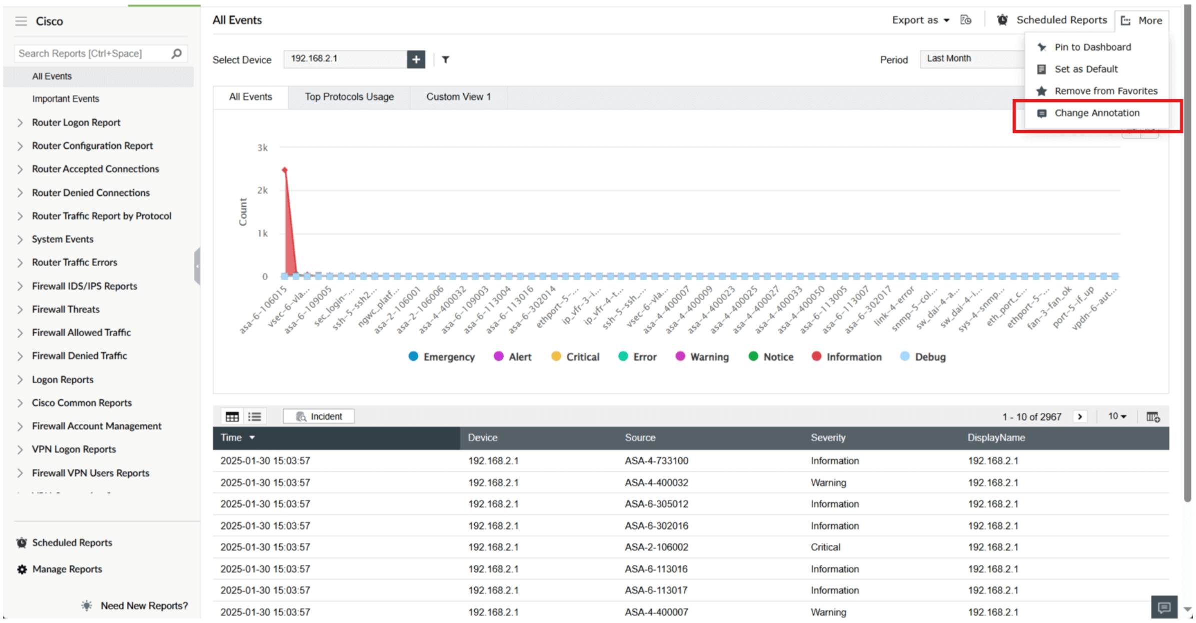
- Click Add to save your preferences.

Adding Annotation to Report Export

You can add custom annotations for the reports. These annotations will be displayed in PDF, HTML, and XLSX Report exports.

To add annotation,

- Navigate to the report you want to add Annotation.
- In the top-right corner of the report, click More and select Change Annotation.



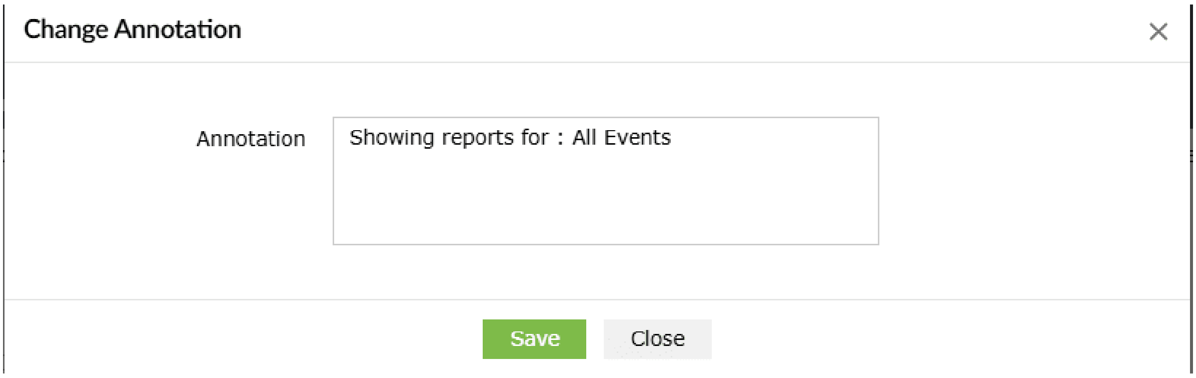
Select Device: 192.168.2.1

Period: Last Month

1 - 10 of 2967

Time	Device	Source	Severity	DisplayName
2025-01-30 15:03:57	192.168.2.1	ASA-4-733100	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-4-400032	Warning	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-305012	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-302016	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-2-106002	Critical	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-113016	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-113017	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-4-400007	Warning	192.168.2.1

- Update the annotation to the desired requirement. Click "Save".



Change Annotation

Annotation: Showing reports for : All Events

- All the above-mentioned exports of this report will have Custom Annotation from now on.

Calendar Functionality

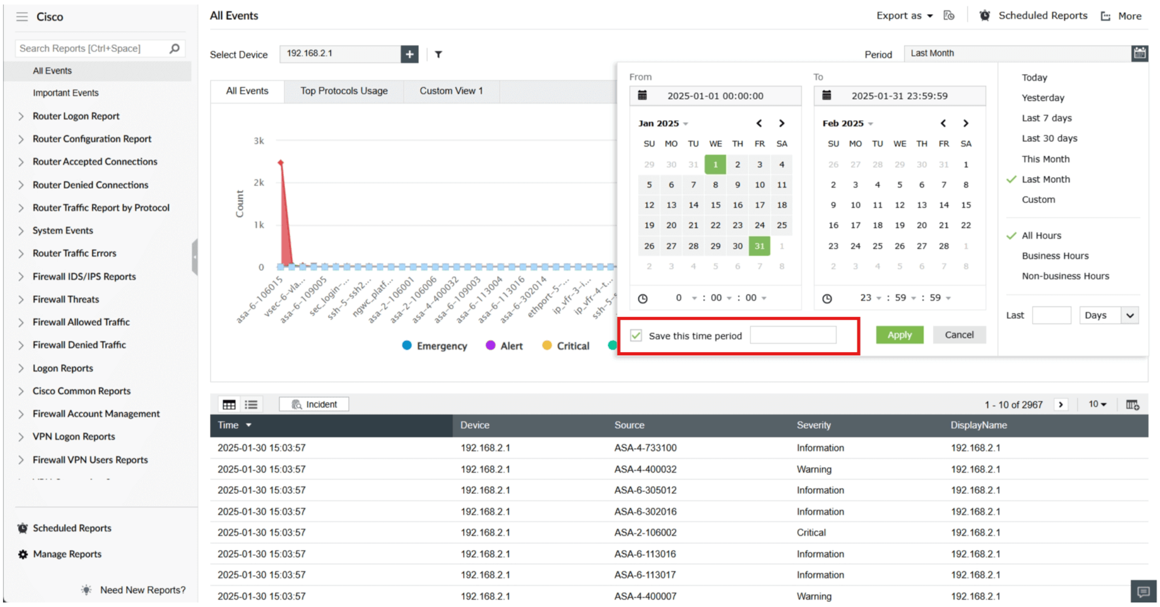
The Calendar Functionality feature introduces enhanced options for managing date ranges. This functionality provides greater flexibility and efficiency when working with date-specific data.

> NOTE: The calendar functionality is also accessible through dashboard, search, correlation, alerts, workflow-history, reindex and compliance tabs.

The date ranges can be managed in two ways as follows:

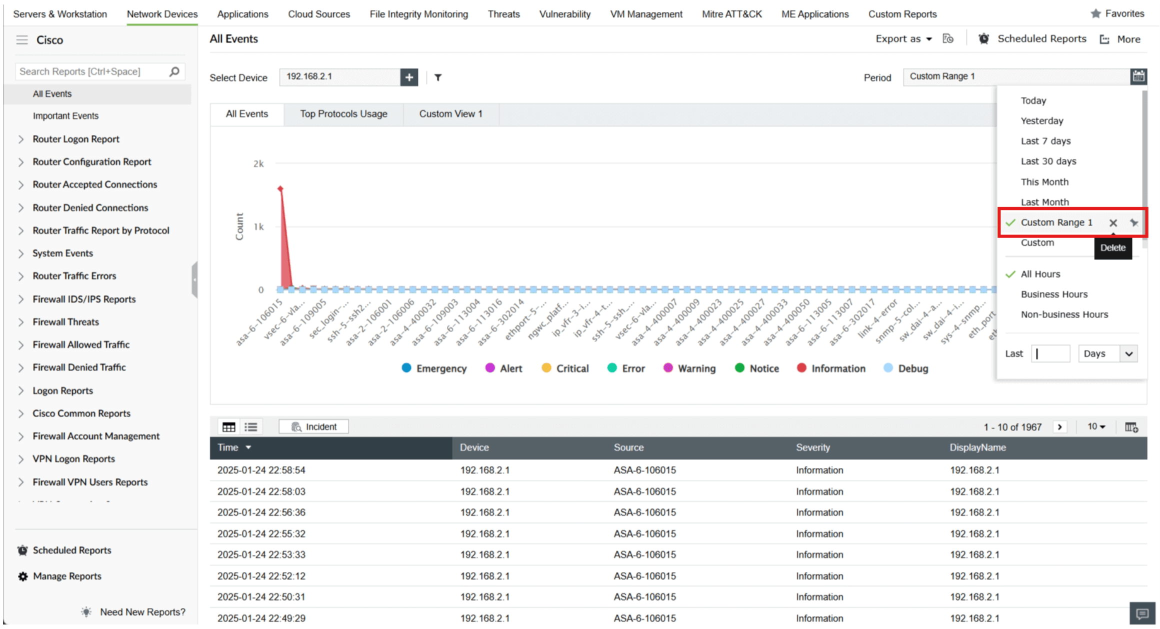
1. Custom Ranges:

   - Create new date ranges by selecting the Custom Range option.



Time	Device	Source	Severity	DisplayName
2025-01-30 15:03:57	192.168.2.1	ASA-4-733100	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-4-400032	Warning	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-305012	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-302016	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-2-106002	Critical	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-113016	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-6-113017	Information	192.168.2.1
2025-01-30 15:03:57	192.168.2.1	ASA-4-400007	Warning	192.168.2.1

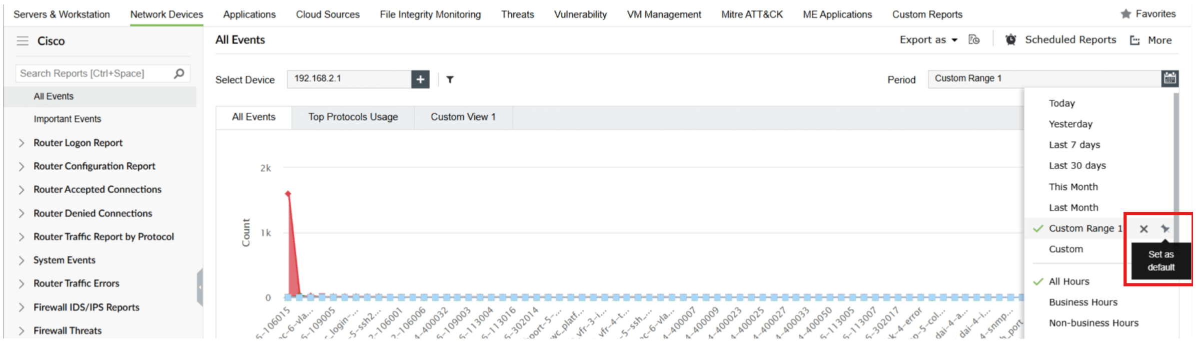
- Easily delete any custom ranges that are no longer needed.

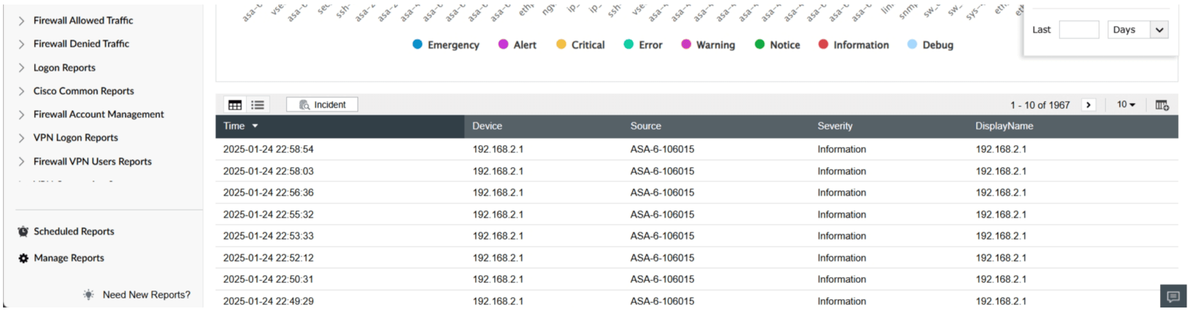


Time	Device	Source	Severity	DisplayName
2025-01-24 22:58:54	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:58:03	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:56:36	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:55:32	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:53:33	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:52:12	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:50:31	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:49:29	192.168.2.1	ASA-6-106015	Information	192.168.2.1

2. 2. Pinned Calendar Ranges:

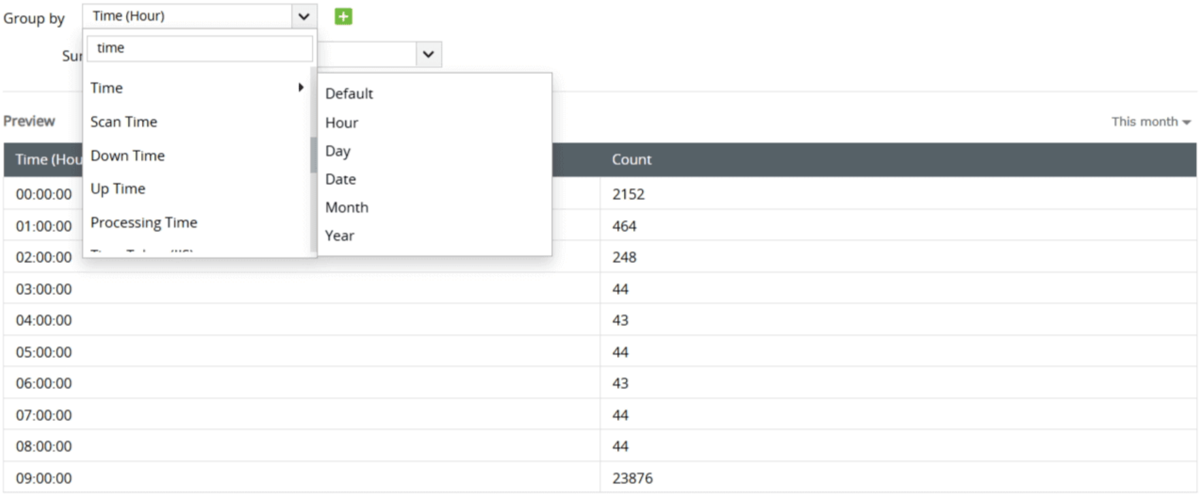
- Pin a specific calendar range to a report.
- The pinned range will automatically load each time the report is accessed or reloaded, ensuring consistency and saving time.





Time	Device	Source	Severity	DisplayName
2025-01-24 22:58:54	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:58:03	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:56:36	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:55:32	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:53:33	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:52:12	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:50:31	192.168.2.1	ASA-6-106015	Information	192.168.2.1
2025-01-24 22:49:29	192.168.2.1	ASA-6-106015	Information	192.168.2.1

Field Units



Group by: Time (Hour)

Time (Hou	Count
00:00:00	2152
01:00:00	464
02:00:00	248
03:00:00	44
04:00:00	43
05:00:00	44
06:00:00	43
07:00:00	44
08:00:00	44
09:00:00	23876

When creating a Custom Report or Report Views based on summary or pivot view, the following units are available for the field Time, which will determine the unit of time:

Hour - The time will be represented hour-wise.

Day - The time will be represented day-wise (by days of the week).

Date - The time will be represented date-wise (by dates of the month).

Month - The time will be represented month-wise (by months of the year).

Year - The time will be represented year-wise.

Default - The time unit will adjust dynamically based on the selected time range in the date range picker. For example, if the time range is more than one hour, the time will be shown hour-wise; if the range exceeds one day, it will be displayed date-wise, and so on.

> Note
>
> If a custom report or report view is based on the time unit "Hour", the time range is restricted to a maximum of 12 months for viewing data.

2.4.1. Log Search in EventLog Analyzer

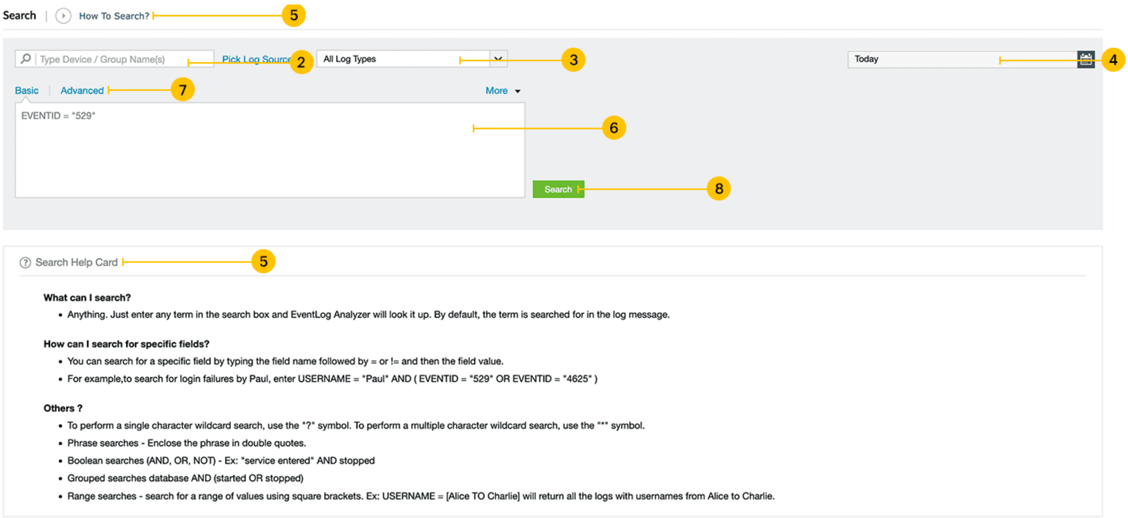
Last updated on: September 12, 2025

In this page

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.



EVENTID = "529"

What can I search?

- Anything. Just enter any term in the search box and EventLog Analyzer will look it up. By default, the term is searched for in the log message.

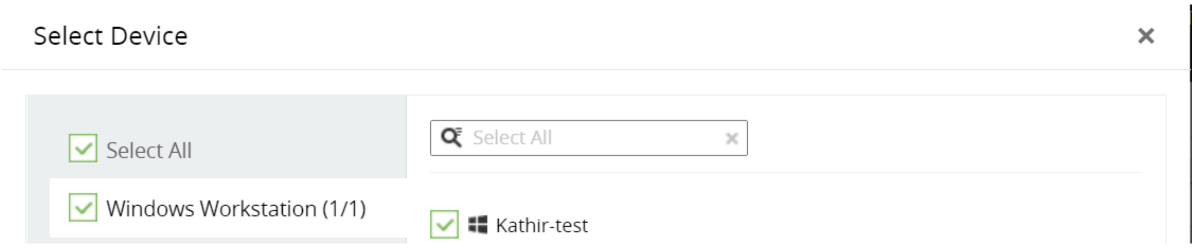
How can I search for specific fields?

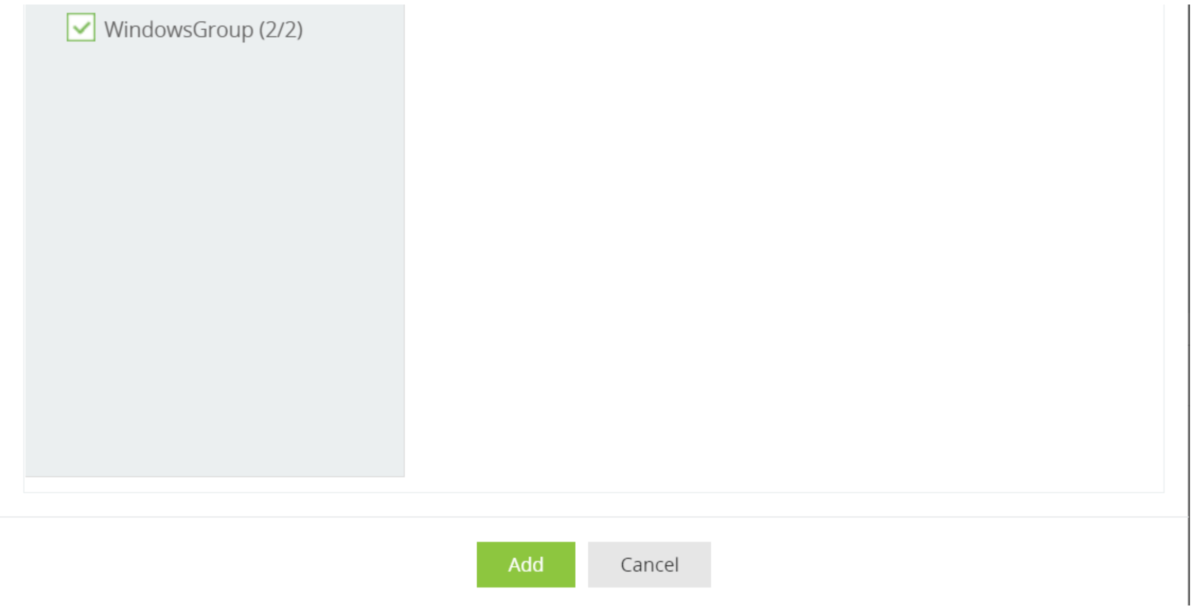
- You can search for a specific field by typing the field name followed by = or != and then the field value.
- For example,to search for login failures by Paul, enter USERNAME = "Paul" AND (EVENTID = "529" OR EVENTID = "4625")

Others ?

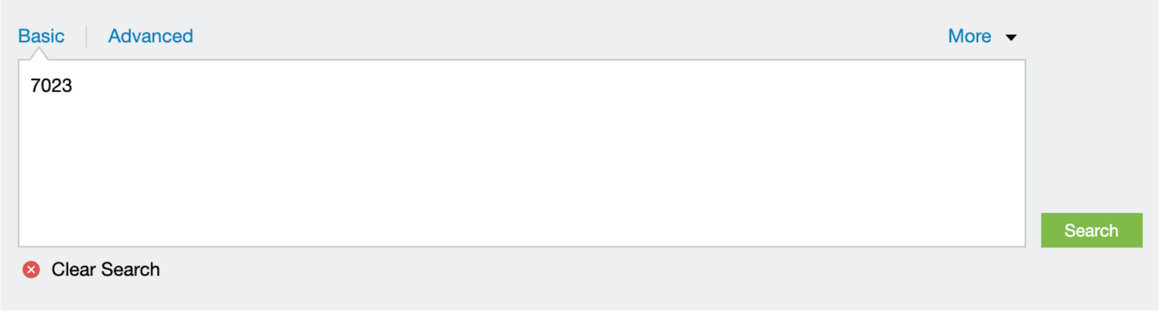
- To perform a single character wildcard search, use the "?" symbol. To perform a multiple character wildcard search, use the "*" symbol.
- Phrase searches - Enclose the phrase in double quotes.
- Boolean searches (AND, OR, NOT) - Ex: "service entered" AND stopped
- Grouped searches database AND (started OR stopped)
- Range searches - search for a range of values using square brackets. Ex: USERNAME = [Alice TO Charlie] will return all the logs with usernames from Alice to Charlie.

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.

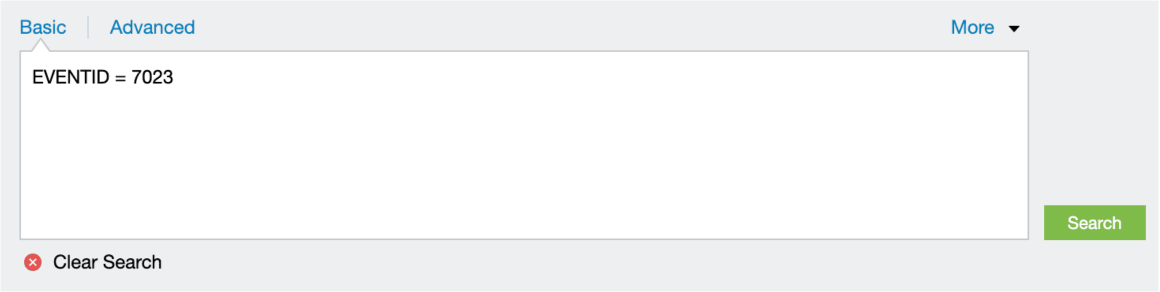



☑ WindowsGroup (2/2)

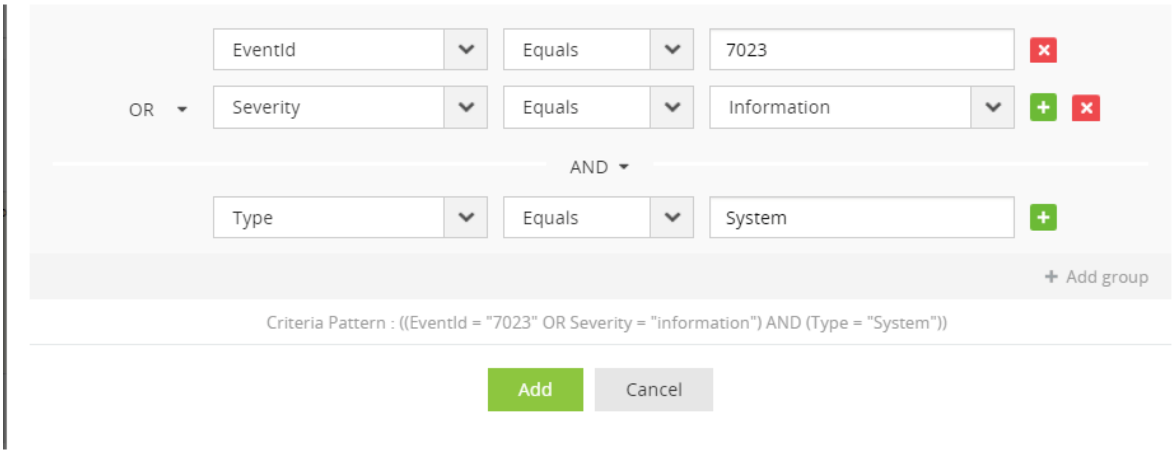
3. Select log type from the drop-down box. By default the selection is All Log Types, and the search is carried out across all log types.
4. Select the period as required.
5. Search Help Card is a built-in guide that lists the types of search queries you can perform in the search box. You can also watch how to search tutorials.
6. Use Basic search to enter your own search string/search criteria.
   - Type the field value into the Search box.


7023

   - Type the field name and value into the Search box.


EVENTID = 7023

7. To build complex search expressions with the interactive search builder, click Advanced.



EventId Equals 7023

Severity Equals Information

Type Equals System

Criteria Pattern : ((EventId = "7023" OR Severity = "information") AND (Type = "System"))

- 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:

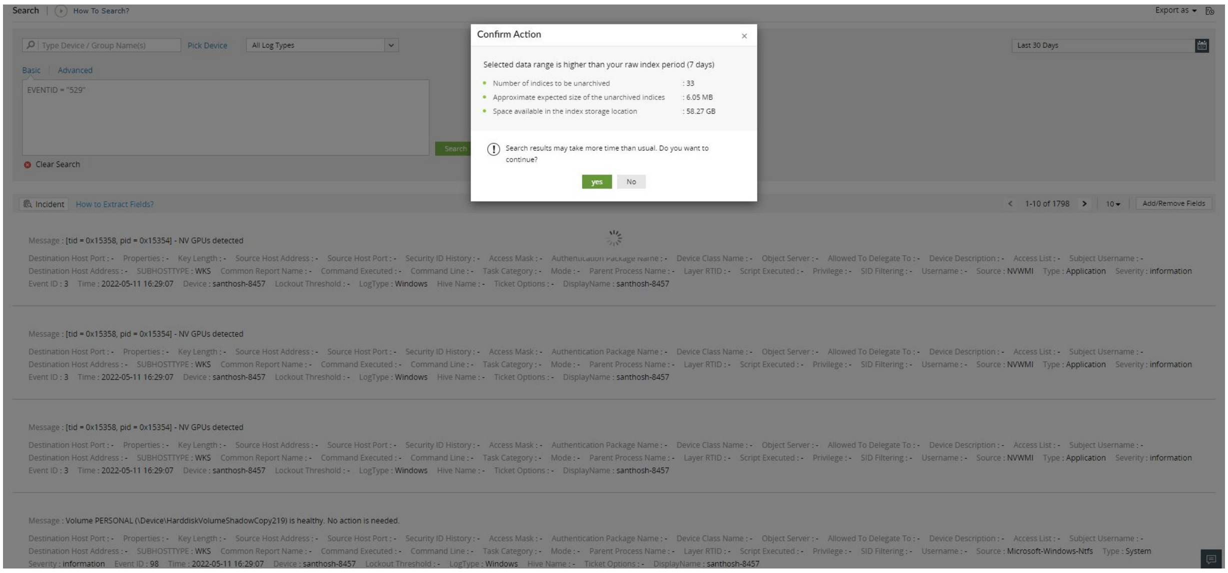
Use double quotes ("") to specify a phrase as the field value.
Syntax: <field name> = "<partial field value>"
Example: MESSAGE = "session"

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.



EVENTID = "529"

Confirm Action

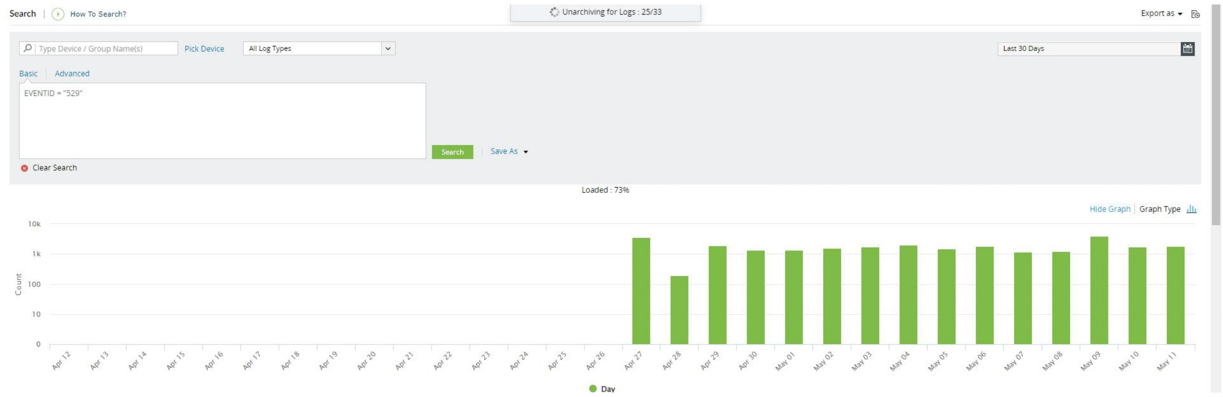
Selected data range is higher than your raw index period (7 days)

- Number of indices to be unarchived : 33
- Approximate expected size of the unarchived indices : 6.05 MB
- Space available in the index storage location : 58.27 GB

Search results may take more time than usual. Do you want to continue?

yes No

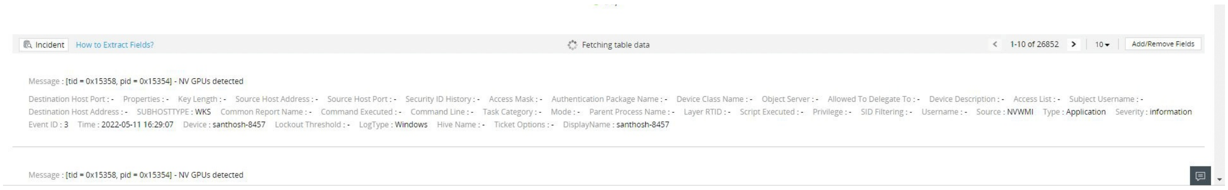
```
Message : [tid = 0x15358, pid = 0x15354] - NV GPUs detected
Destination Host Port : -   Properties : -   Key Length : -   Source Host Address : -   Source Host Port : -   Security ID History : -   Access Mask : -   Authentication Package Name : -   Device Class Name : -   Object Server : -   Allowed To Delegate To : -   Device Description : -   Access List : -   Subject Username : -
Destination Host Address : -   SUBHOSTTYPE : WKS   Common Report Name : -   Command Executed : -   Command Line : -   Task Category : -   Mode : -   Parent Process Name : -   Layer RTID : -   Script Executed : -   Privilege : -   SID Filtering : -   Username : -   Source : NVWMI   Type : Application   Severity : information
Event ID : 3   Time : 2022-05-11 16:29:07   Device : santhosh-8457   Lockout Threshold : -   LogType : Windows   Hive Name : -   Ticket Options : -   DisplayName : santhosh-8457

Message : [tid = 0x15358, pid = 0x15354] - NV GPUs detected
Destination Host Port : -   Properties : -   Key Length : -   Source Host Address : -   Source Host Port : -   Security ID History : -   Access Mask : -   Authentication Package Name : -   Device Class Name : -   Object Server : -   Allowed To Delegate To : -   Device Description : -   Access List : -   Subject Username : -
Destination Host Address : -   SUBHOSTTYPE : WKS   Common Report Name : -   Command Executed : -   Command Line : -   Task Category : -   Mode : -   Parent Process Name : -   Layer RTID : -   Script Executed : -   Privilege : -   SID Filtering : -   Username : -   Source : NVWMI   Type : Application   Severity : information
Event ID : 3   Time : 2022-05-11 16:29:07   Device : santhosh-8457   Lockout Threshold : -   LogType : Windows   Hive Name : -   Ticket Options : -   DisplayName : santhosh-8457

Message : [tid = 0x15358, pid = 0x15354] - NV GPUs detected
Destination Host Port : -   Properties : -   Key Length : -   Source Host Address : -   Source Host Port : -   Security ID History : -   Access Mask : -   Authentication Package Name : -   Device Class Name : -   Object Server : -   Allowed To Delegate To : -   Device Description : -   Access List : -   Subject Username : -
Destination Host Address : -   SUBHOSTTYPE : WKS   Common Report Name : -   Command Executed : -   Command Line : -   Task Category : -   Mode : -   Parent Process Name : -   Layer RTID : -   Script Executed : -   Privilege : -   SID Filtering : -   Username : -   Source : NVWMI   Type : Application   Severity : information
Event ID : 3   Time : 2022-05-11 16:29:07   Device : santhosh-8457   Lockout Threshold : -   LogType : Windows   Hive Name : -   Ticket Options : -   DisplayName : santhosh-8457

Message : Volume PERSONAL (\Device\HarddiskVolumeShadowCopy219) is healthy. No action is needed.
Destination Host Port : -   Properties : -   Key Length : -   Source Host Address : -   Source Host Port : -   Security ID History : -   Access Mask : -   Authentication Package Name : -   Device Class Name : -   Object Server : -   Allowed To Delegate To : -   Device Description : -   Access List : -   Subject Username : -
Destination Host Address : -   SUBHOSTTYPE : WKS   Common Report Name : -   Command Executed : -   Command Line : -   Task Category : -   Mode : -   Parent Process Name : -   Layer RTID : -   Script Executed : -   Privilege : -   SID Filtering : -   Username : -   Source : Microsoft-Windows-Ntfs   Type : System
Severity : information   Event ID : 98   Time : 2022-05-11 16:29:07   Device : santhosh-8457   Lockout Threshold : -   LogType : Windows   Hive Name : -   Ticket Options : -   DisplayName : santhosh-8457
```



Unarchiving for Logs : 25/33

EVENTID = "529"

Loaded : 73%



```
Message : [tid = 0x15358, pid = 0x15354] - NV GPUs detected
Destination Host Port : -   Properties : -   Key Length : -   Source Host Address : -   Source Host Port : -   Security ID History : -   Access Mask : -   Authentication Package Name : -   Device Class Name : -   Object Server : -   Allowed To Delegate To : -   Device Description : -   Access List : -   Subject Username : -
Destination Host Address : -   SUBHOSTTYPE : WKS   Common Report Name : -   Command Executed : -   Command Line : -   Task Category : -   Mode : -   Parent Process Name : -   Layer RTID : -   Script Executed : -   Privilege : -   SID Filtering : -   Username : -   Source : NVWMI   Type : Application   Severity : information
Event ID : 3   Time : 2022-05-11 16:29:07   Device : santhosh-8457   Lockout Threshold : -   LogType : Windows   Hive Name : -   Ticket Options : -   DisplayName : santhosh-8457

Message : [tid = 0x15358, pid = 0x15354] - NV GPUs detected
```

ⓘ 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.

2.4.2. Custom Log Parser

Last updated on: September 12, 2025

In this page

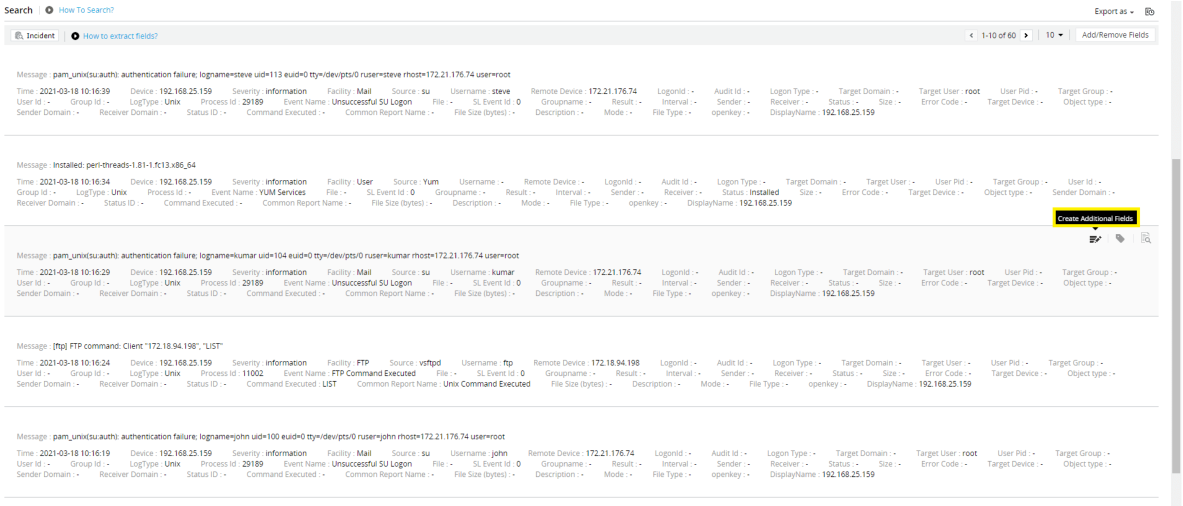
Network administrators are always in need of more information and insights from their log data. There are times when an IT administrator would identify some log information which is useful and would like to have it indexed automatically as a new field. Having more fields being indexed makes your log 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.

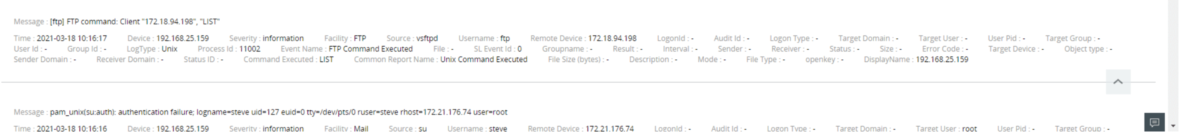
How to extract additional fields using EventLog Analyzer?

- 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.

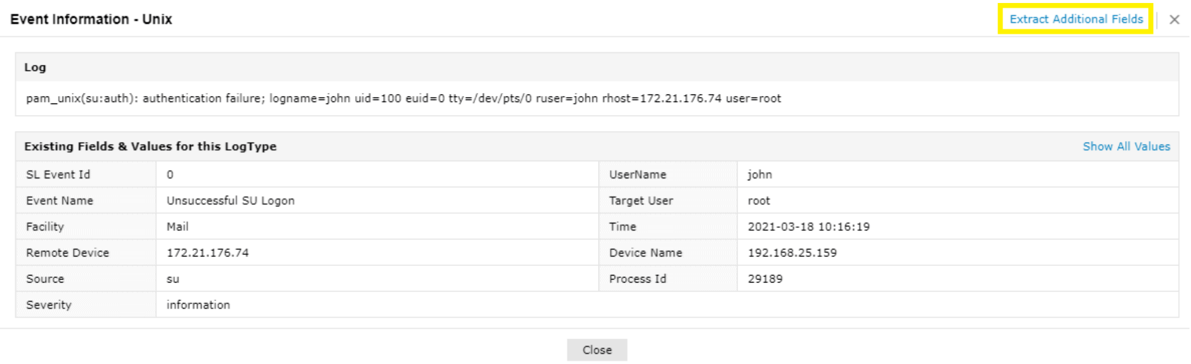


```
Message : pam_unix(su:auth): authentication failure; logname=steve uid=113 euid=0 tty=/dev/pts/0 ruser=steve rhost=172.21.176.74 user=root
Time : 2021-03-18 10:16:39   Device : 192.168.25.159   Severity : information   Facility : Mail   Source : su   Username : steve   Remote Device : 172.21.176.74   LogonId : -   Audit Id : -   Logon Type : -   Target Domain : -   Target User : root   User Pid : -   Target Group : -
User Id : -   Group Id : -   LogType : Unix   Process Id : 29189   Event Name : Unsuccessful SU Logon   File : -   SL Event Id : 0   Groupname : -   Result : -   Interval : -   Sender : -   Receiver : -   Status : -   Size : -   Error Code : -   Target Device : -   Object type : -
Sender Domain : -   Receiver Domain : -   Status ID : -   Command Executed : -   Common Report Name : -   File Size (bytes) : -   Description : -   Mode : -   File Type : -   openkey : -   DisplayName : 192.168.25.159

Message : Installed: perl-threads-1.81-1.fc13.x86_64
Time : 2021-03-18 10:16:34   Device : 192.168.25.159   Severity : information   Facility : User   Source : Yum   Username : -   Remote Device : -   LogonId : -   Audit Id : -   Logon Type : -   Target Domain : -   Target User : -   User Pid : -   Target Group : -   User Id : -
Group Id : -   LogType : Unix   Process Id : -   Event Name : YUM Services   File : -   SL Event Id : 0   Groupname : -   Result : -   Interval : -   Sender : -   Receiver : -   Status : Installed   Size : -   Error Code : -   Target Device : -   Object type : -   Sender Domain : -
Receiver Domain : -   Status ID : -   Command Executed : -   Common Report Name : -   File Size (bytes) : -   Description : -   Mode : -   File Type : -   openkey : -   DisplayName : 192.168.25.159

Message : pam_unix(su:auth): authentication failure; logname=kumar uid=104 euid=0 tty=/dev/pts/0 ruser=kumar rhost=172.21.176.74 user=root
Time : 2021-03-18 10:16:29   Device : 192.168.25.159   Severity : information   Facility : Mail   Source : su   Username : kumar   Remote Device : 172.21.176.74   LogonId : -   Audit Id : -   Logon Type : -   Target Domain : -   Target User : root   User Pid : -   Target Group : -
User Id : -   Group Id : -   LogType : Unix   Process Id : 29189   Event Name : Unsuccessful SU Logon   File : -   SL Event Id : 0   Groupname : -   Result : -   Interval : -   Sender : -   Receiver : -   Status : -   Size : -   Error Code : -   Target Device : -   Object type : -
Sender Domain : -   Receiver Domain : -   Status ID : -   Command Executed : -   Common Report Name : -   File Size (bytes) : -   Description : -   Mode : -   File Type : -   openkey : -   DisplayName : 192.168.25.159

Message : [ftp] FTP command: Client "172.18.94.198", "LIST"
Time : 2021-03-18 10:16:24   Device : 192.168.25.159   Severity : information   Facility : FTP   Source : vsftpd   Username : ftp   Remote Device : 172.18.94.198   LogonId : -   Audit Id : -   Logon Type : -   Target Domain : -   Target User : -   User Pid : -   Target Group : -
User Id : -   Group Id : -   LogType : Unix   Process Id : 11002   Event Name : FTP Command Executed   File : -   SL Event Id : 0   Groupname : -   Result : -   Interval : -   Sender : -   Receiver : -   Status : -   Size : -   Error Code : -   Target Device : -   Object type : -
Sender Domain : -   Receiver Domain : -   Status ID : -   Command Executed : LIST   Common Report Name : Unix Command Executed   File Size (bytes) : -   Description : -   Mode : -   File Type : -   openkey : -   DisplayName : 192.168.25.159

Message : pam_unix(su:auth): authentication failure; logname=john uid=100 euid=0 tty=/dev/pts/0 ruser=john rhost=172.21.176.74 user=root
Time : 2021-03-18 10:16:19   Device : 192.168.25.159   Severity : information   Facility : Mail   Source : su   Username : john   Remote Device : 172.21.176.74   LogonId : -   Audit Id : -   Logon Type : -   Target Domain : -   Target User : root   User Pid : -   Target Group : -
User Id : -   Group Id : -   LogType : Unix   Process Id : 29189   Event Name : Unsuccessful SU Logon   File : -   SL Event Id : 0   Groupname : -   Result : -   Interval : -   Sender : -   Receiver : -   Status : -   Size : -   Error Code : -   Target Device : -   Object type : -
Sender Domain : -   Receiver Domain : -   Status ID : -   Command Executed : -   Common Report Name : -   File Size (bytes) : -   Description : -   Mode : -   File Type : -   openkey : -   DisplayName : 192.168.25.159
```



```
Message : [ftp] FTP command: Client "172.18.94.198", "LIST"
Time : 2021-03-18 10:16:17    Device : 192.168.25.159    Severity : information    Facility : FTP    Source : vsftpd    Username : ftp    Remote Device : 172.18.94.198    LogonId : -    Audit Id : -    Logon Type : -    Target Domain : -    Target User : -    User Pid : -    Target Group : -
User Id : -    Group Id : -    LogType : Unix    Process Id : 11002    Event Name : FTP Command Executed    File : -    SL Event Id : 0    Groupname : -    Result : -    Interval : -    Sender : -    Receiver : -    Status : -    Size : -    Error Code : -    Target Device : -    Object type : -
Sender Domain : -    Receiver Domain : -    Status ID : -    Command Executed : LIST    Common Report Name : Unix Command Executed    File Size (bytes) : -    Description : -    Mode : -    File Type : -    openkey : -    DisplayName : 192.168.25.159

Message : pam_unix(su:auth): authentication failure; logname=steve uid=127 euid=0 tty=/dev/pts/0 ruser=steve rhost=172.21.176.74 user=root
Time : 2021-03-18 10:16:16    Device : 192.168.25.159    Severity : information    Facility : Mail    Source : su    Username : steve    Remote Device : 172.21.176.74    LogonId : -    Audit Id : -    Logon Type : -    Target Domain : -    Target User : root    User Pid : -    Target Group : -
```

- 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.



Log

```
pam_unix(su:auth): authentication failure; logname=john uid=100 euid=0 tty=/dev/pts/0 ruser=john rhost=172.21.176.74 user=root
```

Existing Fields & Values for this LogType

SL Event Id	0	UserName	john
Event Name	Unsuccessful SU Logon	Target User	root
Facility	Mail	Time	2021-03-18 10:16:19
Remote Device	172.21.176.74	Device Name	192.168.25.159
Source	su	Process Id	29189
Severity	information		

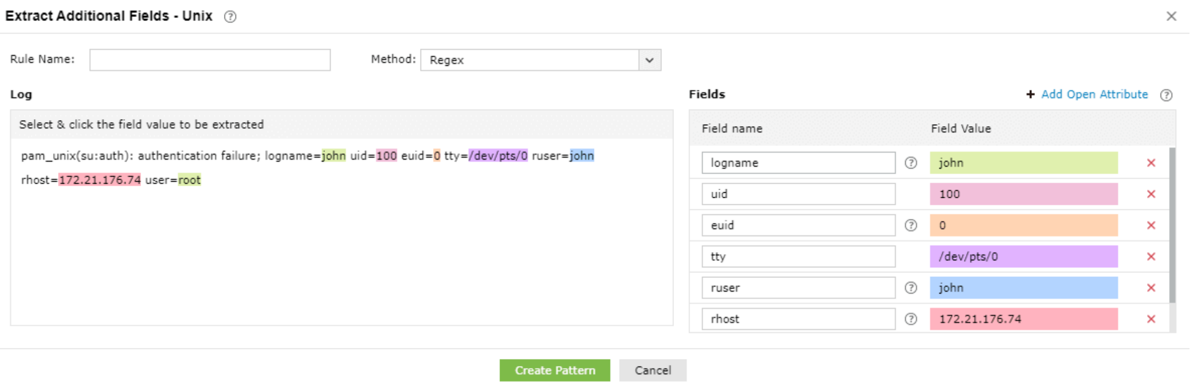
Specifying custom field values

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.



Rule Name:

Method: Regex

Log

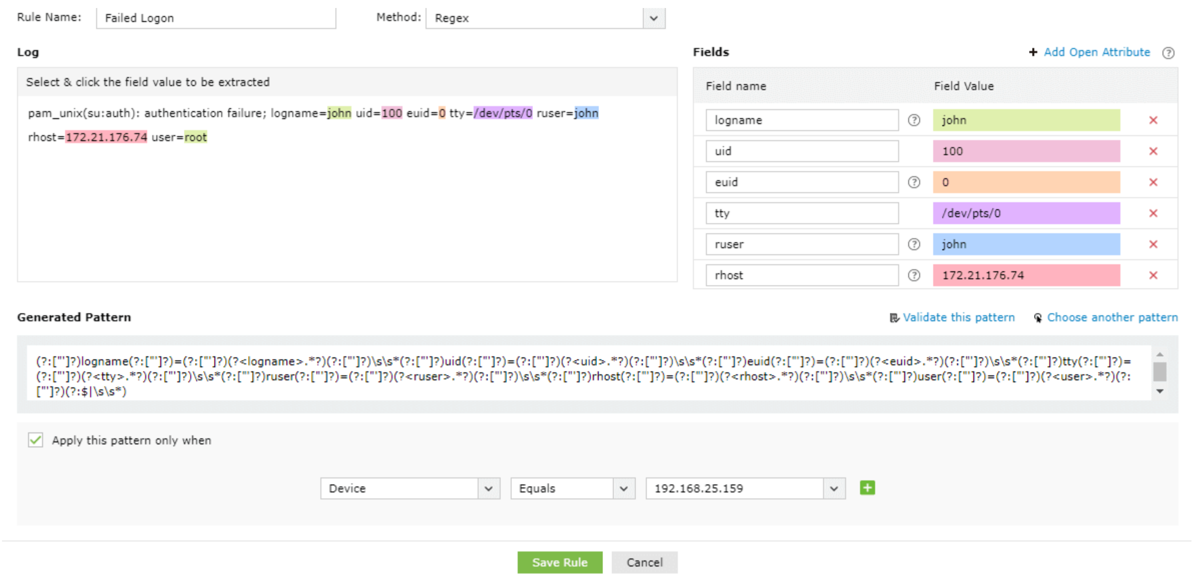
Select & click the field value to be extracted

```
pam_unix(su:auth): authentication failure; logname=john uid=100 euid=0 tty=/dev/pts/0 ruser=john
rhost=172.21.176.74 user=root
```

Fields

Field name	Field Value
logname	john
uid	100
euid	0
tty	/dev/pts/0
ruser	john
rhost	172.21.176.74

- 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.



Rule Name: Failed Logon Method: Regex

Log

Select & click the field value to be extracted

```
pam_unix(su:auth): authentication failure; logname=john uid=100 euid=0 tty=/dev/pts/0 ruser=john
rhost=172.21.176.74 user=root
```

Fields + Add Open Attribute

Field name	Field Value
logname	john
uid	100
euid	0
tty	/dev/pts/0
ruser	john
rhost	172.21.176.74

Generated Pattern Validate this pattern Choose another pattern

```
(?:["']?)logname(?:["']?)=(?:["']?)(?<logname>.*?)(?:["']?)\s\s*(?:["']?)uid(?:["']?)=(?:["']?)(?<uid>.*?)(?:["']?)\s\s*(?:["']?)euid(?:["']?)=(?:["']?)(?<euid>.*?)(?:["']?)\s\s*(?:["']?)tty(?:["']?)=
(?:["']?)(?<tty>.*?)(?:["']?)\s\s*(?:["']?)ruser(?:["']?)=(?:["']?)(?<ruser>.*?)(?:["']?)\s\s*(?:["']?)rhost(?:["']?)=(?:["']?)(?<rhost>.*?)(?:["']?)\s\s*(?:["']?)user(?:["']?)=(?:["']?)(?<user>.*?)(?:
["']?)(?:$|\s\s*)
```

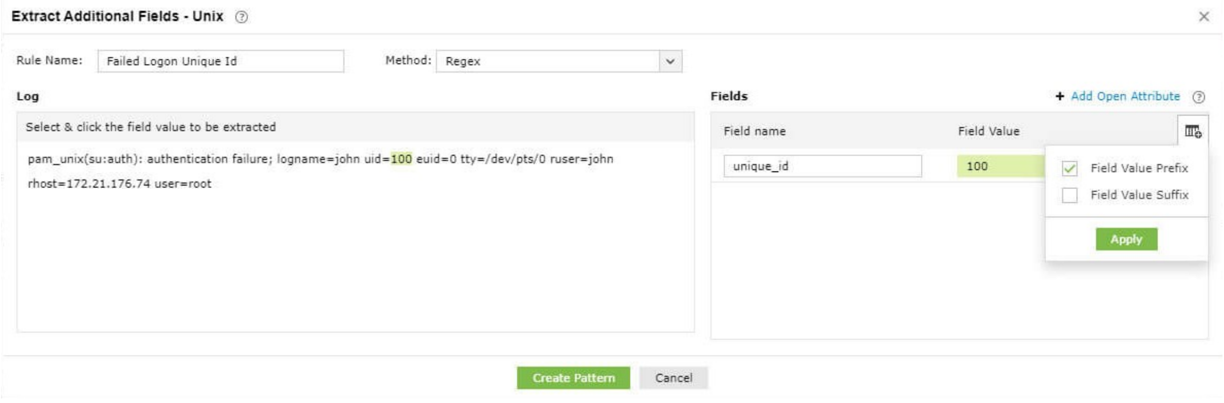
☑ Apply this pattern only when

Device Equals 192.168.25.159

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.



Extract Additional Fields - Unix

Rule Name: Failed Logon Unique Id Method: Regex

Log

Select & click the field value to be extracted

```
pam_unix(su:auth): authentication failure; logname=john uid=100 euid=0 tty=/dev/pts/0 ruser=john
rhost=172.21.176.74 user=root
```

Fields + Add Open Attribute

Field name	Field Value
unique_id	100

☑ Field Value Prefix
☐ Field Value Suffix

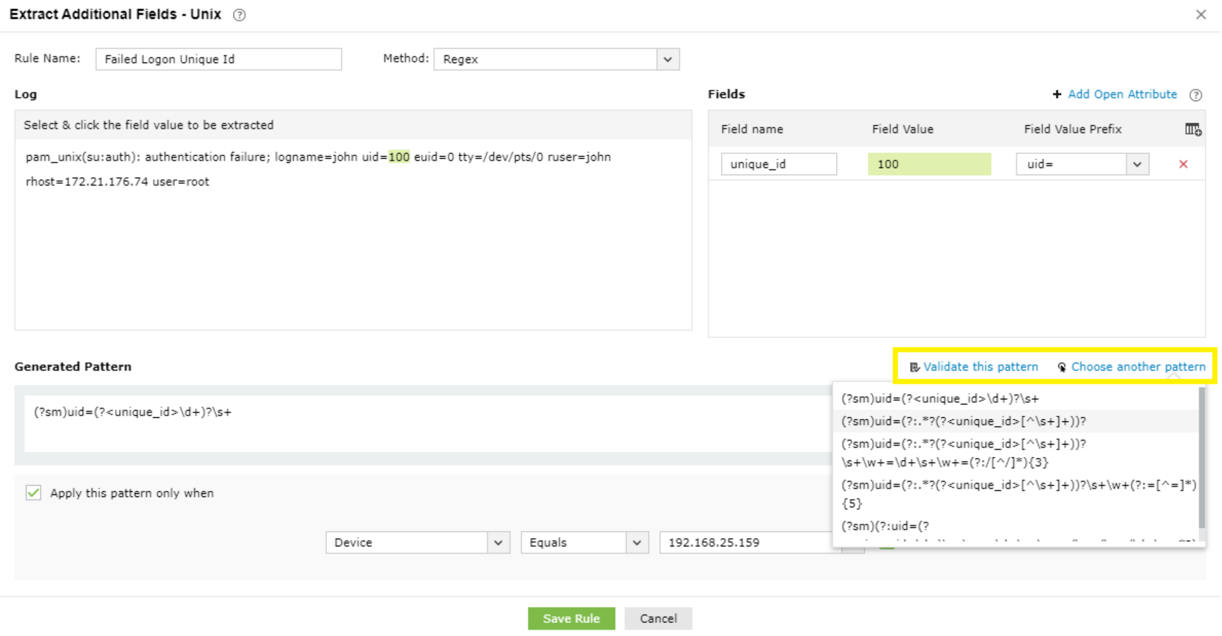
Validating the pattern

A parser rule pattern is created using the field definition. You can edit the generated pattern manually, if you are

A parser rule pattern is created using the field definition. You can edit the generated pattern manually, if you are familiar with regular expressions.

Validate link is used to test the generated pattern against the previous search results. You can manually check the suitability of the pattern by analyzing the 'Matched Log Messages' and 'Unmatched Log Messages' displayed.

- Click on Choose another pattern to choose a pattern from the list of patterns generated by the application.
- You can define any existing field matching criteria to apply the pattern for this specific log type.
- Save the pattern to extract the field(s) from the upcoming logs.



Extract Additional Fields - Unix

Rule Name: Failed Logon Unique Id

Method: Regex

Log

Select & click the field value to be extracted

```
pam_unix(su:auth): authentication failure; logname=john uid=100 euid=0 tty=/dev/pts/0 ruser=john
rhost=172.21.176.74 user=root
```

Fields

Field name	Field Value	Field Value Prefix
unique_id	100	uid=

Generated Pattern

```
(?sm)uid=(?<unique_id>\d+)?\s+
```

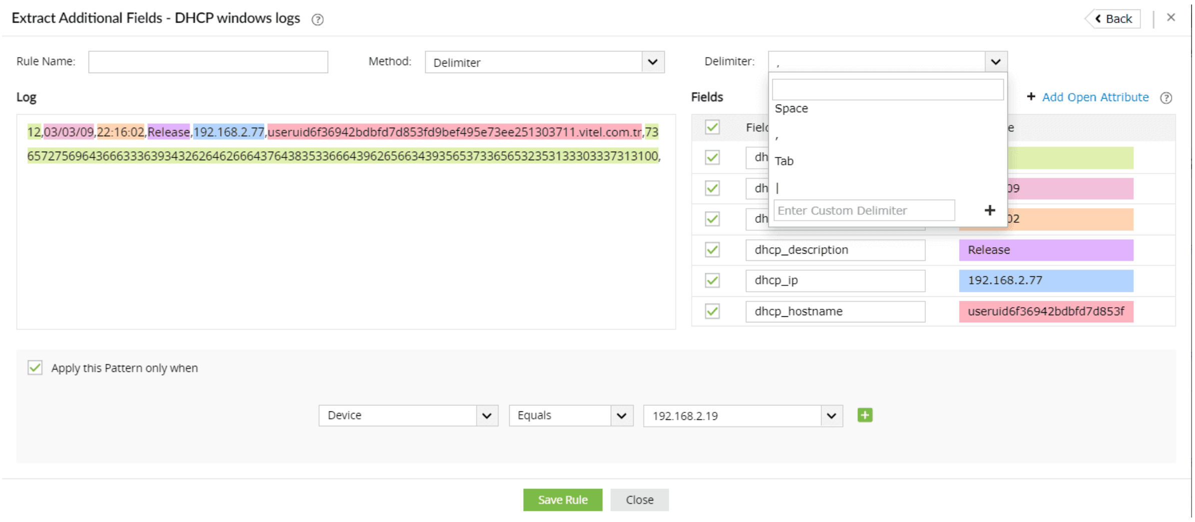
```
(?sm)uid=(?<unique_id>\d+)?\s+
(?sm)uid=(?:.*?(?<unique_id>[^\s+]+))?
(?sm)uid=(?:.*?(?<unique_id>[^\s+]+))?
\s+\w+=\d+\s+\w+=(?:/[^/]*){3}
(?sm)uid=(?:.*?(?<unique_id>[^\s+]+))?\s+\w+(?:=[^=]*)
{5}
(?sm)(?:uid=(?
```

☑ Apply this pattern only when

Device | Equals | 192.168.25.159

Delimiter method

- Provide a rule name.
- You can use the Delimiter to extract fields using delimiters such as Space, Comma, Tab, or Pipe.



Extract Additional Fields - DHCP windows logs

Rule Name:

Method: Delimiter

Delimiter: ,

Log

```
12,03/03/09,22:16:02,Release,192.168.2.77,useruid6f36942bdbfd7d853fd9bef495e73ee251303711.vitel.com.tr,73
6572756964366633363934326264626664376438353366643962656634393565373365653235313330333731310 0,
```

Fields

	Field name	Field value
☑	dh	
☑	dh	09
☑	dh	02
☑	dhcp_description	Release
☑	dhcp_ip	192.168.2.77
☑	dhcp_hostname	useruid6f36942bdbfd7d853f

☑ Apply this Pattern only when

Device | Equals | 192.168.2.19

- To save the created rule, click Save rule.

2.4.3. Saving search and exporting search results

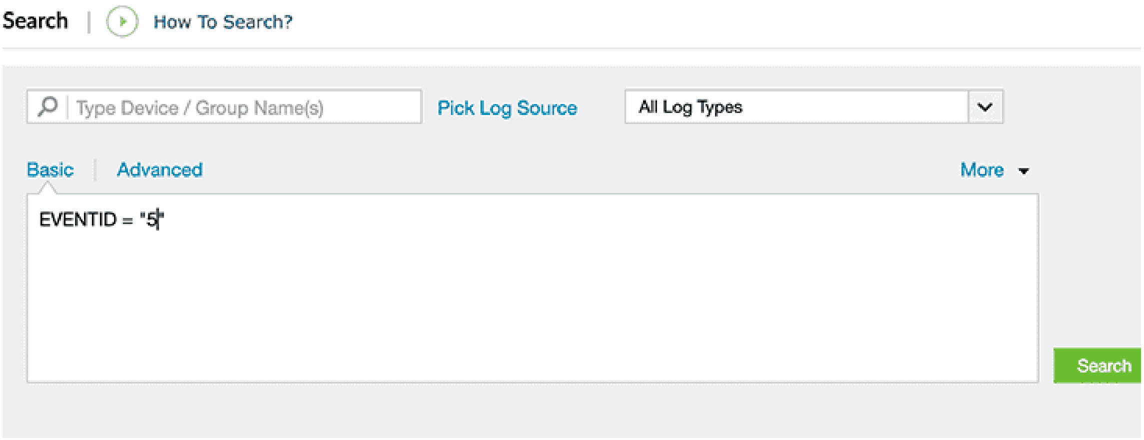
Last updated on: September 12, 2025

In this page

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.

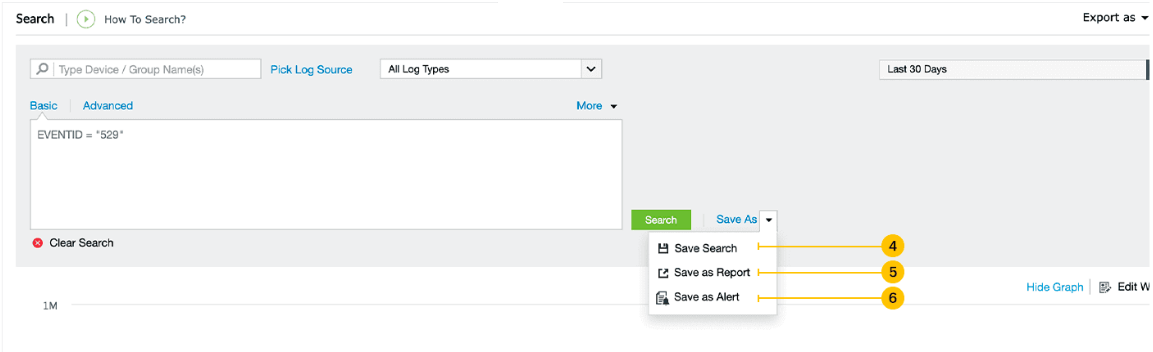
How to save search?

1. Go to the Search tab and enter the search criteria as required (see how to search).
2. Click Search for the results.



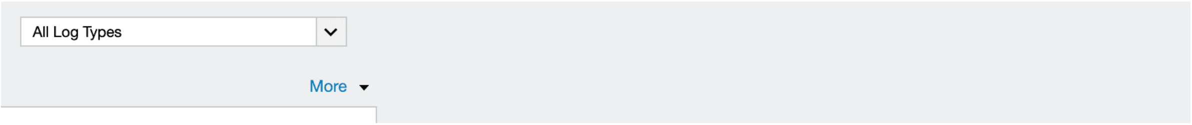
EVENTID = "5

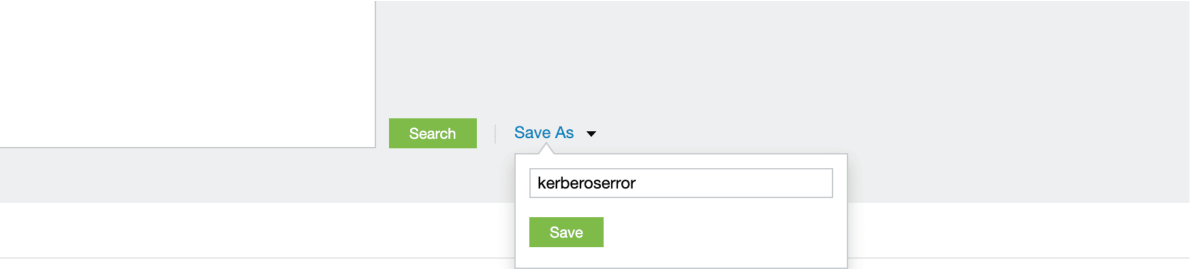
3. You can save the search criteria as search, reports or alerts.



EVENTID = "529"

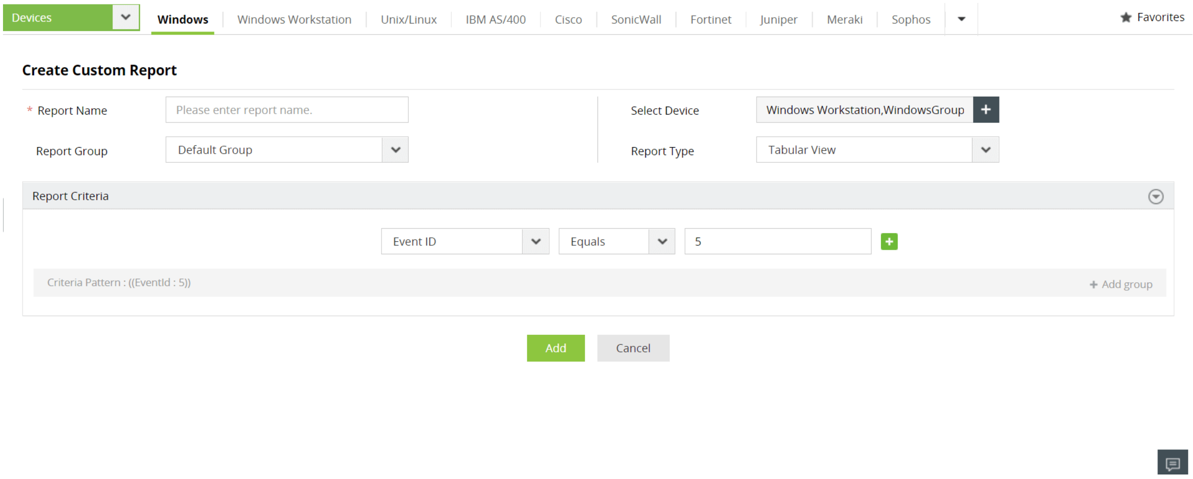
4. To save as search, click Save Search. Enter a name without space. Click Save.





kerberoserror

5. To save as report, click Save as Report. Enter Report name and click Add (see create reports).



Create Custom Report

* Report Name: Please enter report name.

Report Group: Default Group

Select Device: Windows Workstation,WindowsGroup

Report Type: Tabular View

Report Criteria

Event ID | Equals | 5

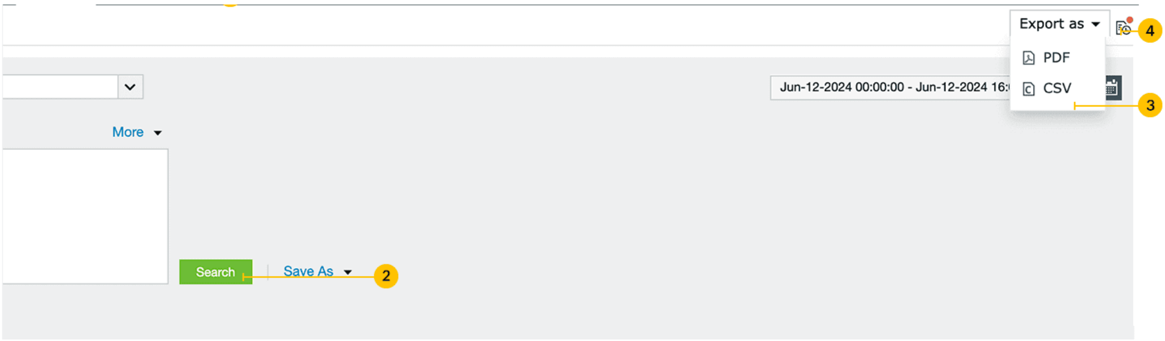
Criteria Pattern : ((EventId : 5))

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.

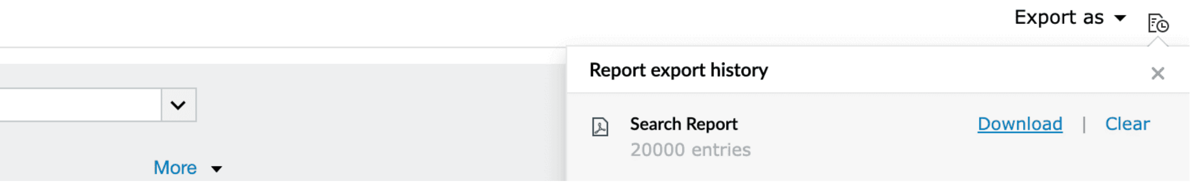
2. Click Search.



Jun-12-2024 00:00:00 - Jun-12-2024 16:

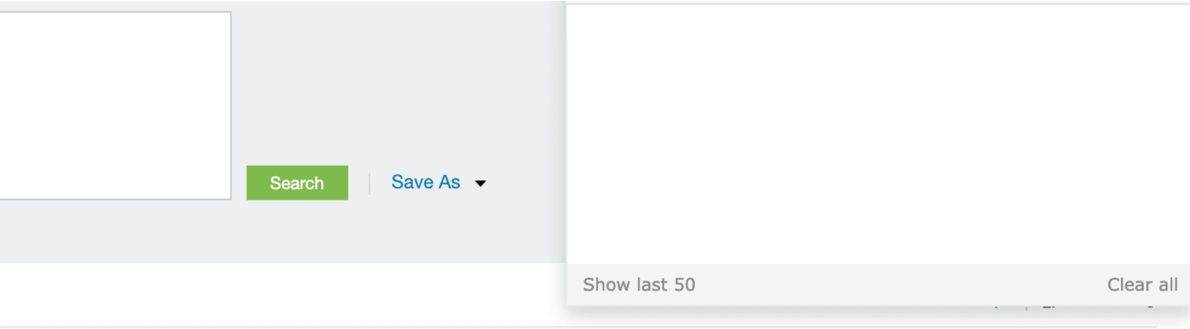
3. Click Export as on the top-right corner. Select the format.

4. View the report export history by clicking on the icon, which can then be downloaded if required.



Report export history

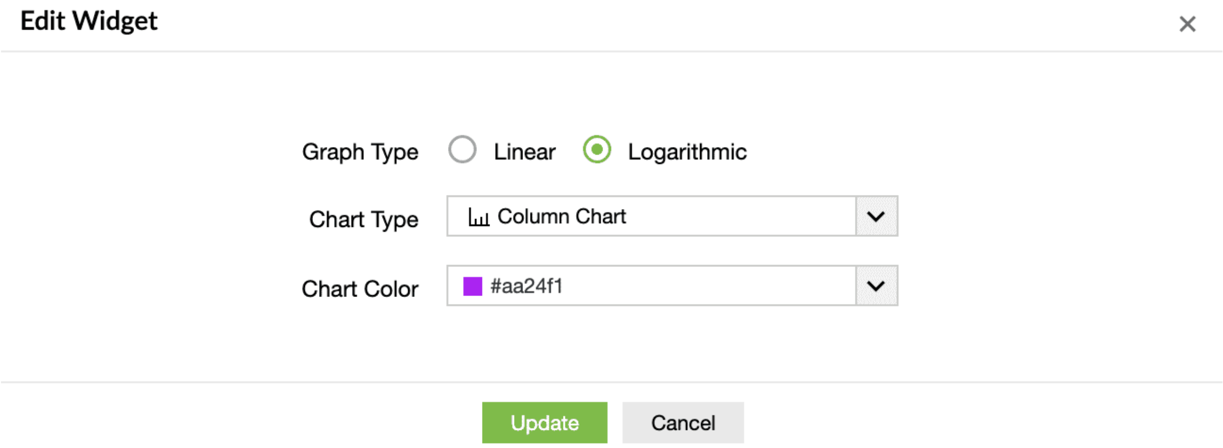
Search Report
20000 entries



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.


Edit Widget

Graph Type ○ Linear ● Logarithmic

Chart Type: Column Chart

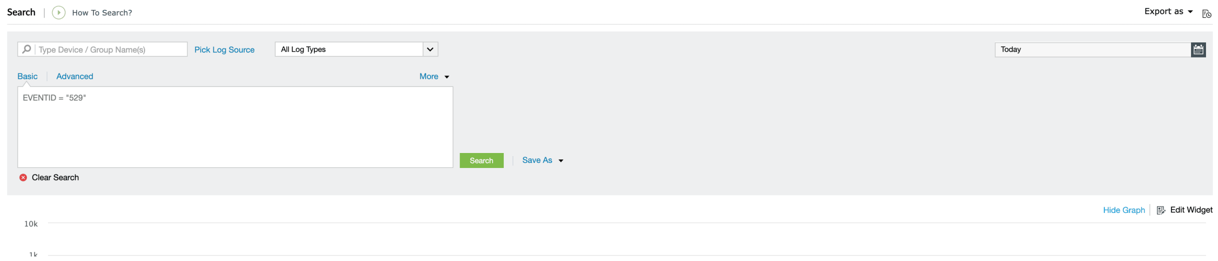
Chart Color: #aa24f1

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.

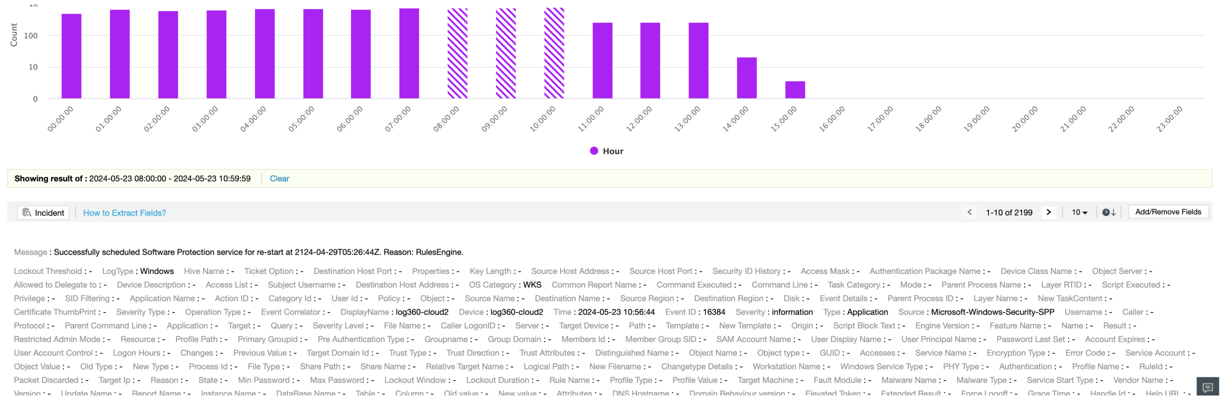
Graph selection:

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.


EVENTID = "529"

Today

All Log Types



Showing result of : 2024-05-23 08:00:00 - 2024-05-23 10:59:59

```
Message : Successfully scheduled Software Protection service for re-start at 2124-04-29T05:26:44Z. Reason: RulesEngine.
Lockout Threshold : -  LogType : Windows  Hive Name : -  Ticket Option : -  Destination Host Port : -  Properties : -  Key Length : -  Source Host Address : -  Source Host Port : -  Security ID History : -  Access Mask : -  Authentication Package Name : -  Device Class Name : -  Object Server : -
Allowed to Delegate to : -  Device Description : -  Access List : -  Subject Username : -  Destination Host Address : -  OS Category : WKS  Common Report Name : -  Command Executed : -  Command Line : -  Task Category : -  Mode : -  Parent Process Name : -  Layer RTID : -  Script Executed : -
Privilege : -  SID Filtering : -  Application Name : -  Action ID : -  Category Id : -  User Id : -  Policy : -  Object : -  Source Name : -  Destination Name : -  Source Region : -  Destination Region : -  Disk : -  Event Details : -  Parent Process ID : -  Layer Name : -  New TaskContent : -
Certificate ThumbPrint : -  Severity Type : -  Operation Type : -  Event Correlator : -  DisplayName : log360-cloud2  Device : log360-cloud2  Time : 2024-05-23 10:56:44  Event ID : 16384  Severity : information  Type : Application  Source : Microsoft-Windows-Security-SPP  Username : -  Caller : -
Protocol : -  Parent Command Line : -  Application : -  Target : -  Query : -  Severity Level : -  File Name : -  Caller LogonID : -  Server : -  Target Device : -  Path : -  Template : -  New Template : -  Origin : -  Script Block Text : -  Engine Version : -  Feature Name : -  Name : -  Result : -
Restricted Admin Mode : -  Resource : -  Profile Path : -  Primary Groupid : -  Pre Authentication Type : -  Groupname : -  Group Domain : -  Members Id : -  Member Group SID : -  SAM Account Name : -  User Display Name : -  User Principal Name : -  Password Last Set : -  Account Expires : -
User Account Control : -  Logon Hours : -  Changes : -  Previous Value : -  Target Domain Id : -  Trust Type : -  Trust Direction : -  Trust Attributes : -  Distinguished Name : -  Object Name : -  Object type : -  GUID : -  Accesses : -  Service Name : -  Encryption Type : -  Error Code : -  Service Account : -
Object Value : -  Old Type : -  New Type : -  Process Id : -  File Type : -  Share Path : -  Share Name : -  Relative Target Name : -  Logical Path : -  New Filename : -  Changetype Details : -  Workstation Name : -  Windows Service Type : -  PHY Type : -  Authentication : -  Profile Name : -  RuleId : -
Packet Discarded : -  Target Ip : -  Reason : -  State : -  Min Password : -  Max Password : -  Lockout Window : -  Lockout Duration : -  Rule Name : -  Profile Type : -  Profile Value : -  Target Machine : -  Fault Module : -  Malware Name : -  Malware Type : -  Service Start Type : -  Vendor Name : -
Version : -  Update Name : -  Report Name : -  Instance Name : -  DataBase Name : -  Table : -  Column : -  Old value : -  New value : -  Attributes : -  DNS Hostname : -  Domain Behaviour version : -  Elevated Token : -  Extended Result : -  Force Logoff : -  Grace Time : -  Handle Id : -  Help URL : -
```

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.

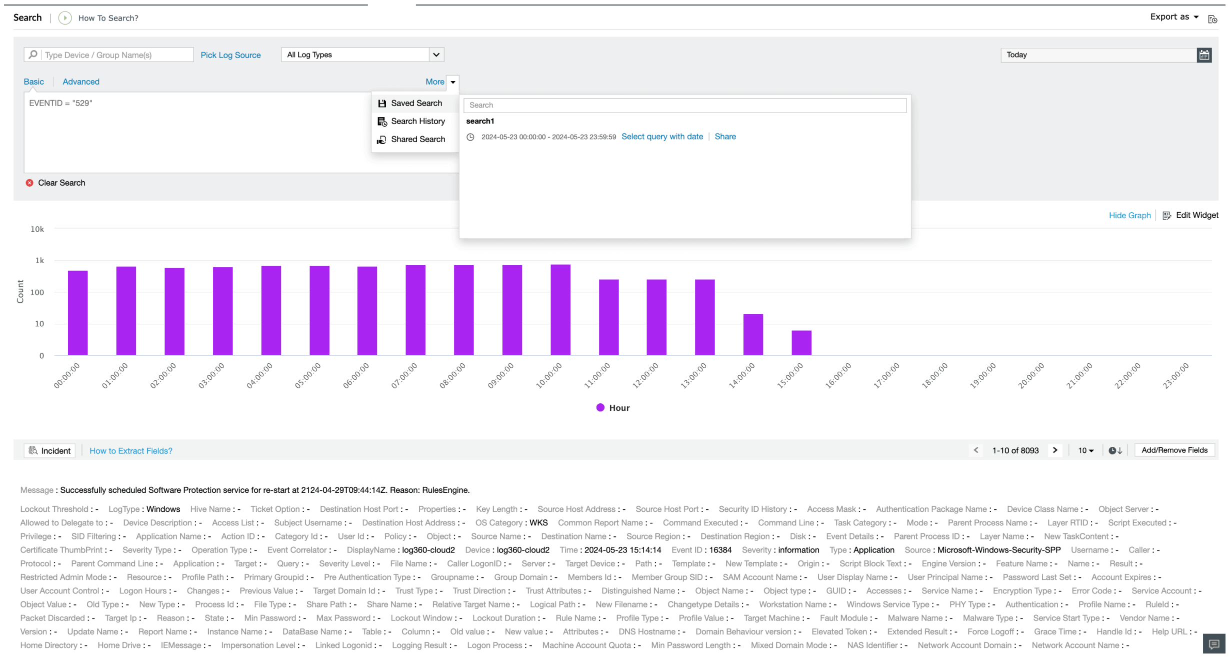
How to use Saved Search

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.



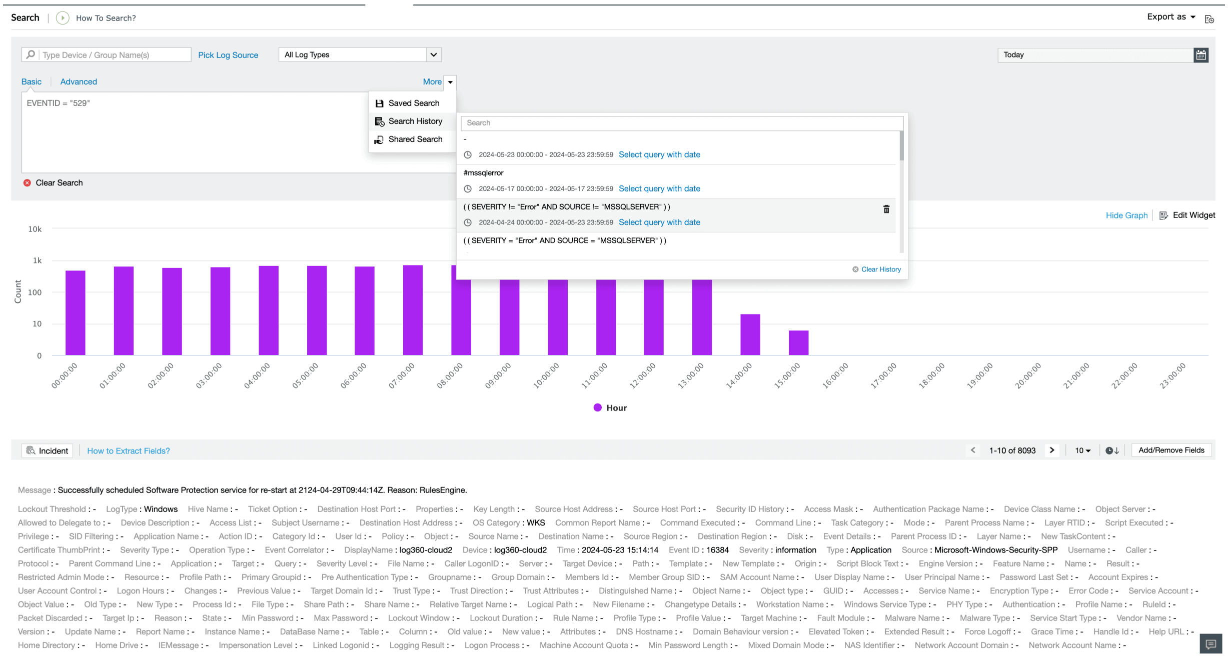
EVENTID = "529"

search1: 2024-05-23 00:00:00 - 2024-05-23 23:59:59

```
Message : Successfully scheduled Software Protection service for re-start at 2124-04-29T09:44:14Z. Reason: RulesEngine.
Lockout Threshold : -  LogType : Windows  Hive Name : -  Ticket Option : -  Destination Host Port : -  Properties : -  Key Length : -  Source Host Address : -  Source Host Port : -  Security ID History : -  Access Mask : -  Authentication Package Name : -  Device Class Name : -  Object Server : -
Allowed to Delegate to : -  Device Description : -  Access List : -  Subject Username : -  Destination Host Address : -  OS Category : WKS  Common Report Name : -  Command Executed : -  Command Line : -  Task Category : -  Mode : -  Parent Process Name : -  Layer RTID : -  Script Executed : -
Privilege : -  SID Filtering : -  Application Name : -  Action ID : -  Category Id : -  User Id : -  Policy : -  Object : -  Source Name : -  Destination Name : -  Source Region : -  Destination Region : -  Disk : -  Event Details : -  Parent Process ID : -  Layer Name : -  New TaskContent : -
Certificate ThumbPrint : -  Severity Type : -  Operation Type : -  Event Correlator : -  DisplayName : log360-cloud2  Device : log360-cloud2  Time : 2024-05-23 15:14:14  Event ID : 16384  Severity : information  Type : Application  Source : Microsoft-Windows-Security-SPP  Username : -  Caller : -
Protocol : -  Parent Command Line : -  Application : -  Target : -  Query : -  Severity Level : -  File Name : -  Caller LogonID : -  Server : -  Target Device : -  Path : -  Template : -  New Template : -  Origin : -  Script Block Text : -  Engine Version : -  Feature Name : -  Name : -  Result : -
Restricted Admin Mode : -  Resource : -  Profile Path : -  Primary Groupid : -  Pre Authentication Type : -  Groupname : -  Group Domain : -  Members Id : -  Member Group SID : -  SAM Account Name : -  User Display Name : -  User Principal Name : -  Password Last Set : -  Account Expires : -
User Account Control : -  Logon Hours : -  Changes : -  Previous Value : -  Target Domain Id : -  Trust Type : -  Trust Direction : -  Trust Attributes : -  Distinguished Name : -  Object Name : -  Object type : -  GUID : -  Accesses : -  Service Name : -  Encryption Type : -  Error Code : -  Service Account : -
Object Value : -  Old Type : -  New Type : -  Process Id : -  File Type : -  Share Path : -  Share Name : -  Relative Target Name : -  Logical Path : -  New Filename : -  Changetype Details : -  Workstation Name : -  Windows Service Type : -  PHY Type : -  Authentication : -  Profile Name : -  RuleId : -
Packet Discarded : -  Target Ip : -  Reason : -  State : -  Min Password : -  Max Password : -  Lockout Window : -  Lockout Duration : -  Rule Name : -  Profile Type : -  Profile Value : -  Target Machine : -  Fault Module : -  Malware Name : -  Malware Type : -  Service Start Type : -  Vendor Name : -
Version : -  Update Name : -  Report Name : -  Instance Name : -  DataBase Name : -  Table : -  Column : -  Old value : -  New value : -  Attributes : -  DNS Hostname : -  Domain Behaviour version : -  Elevated Token : -  Extended Result : -  Force Logoff : -  Grace Time : -  Handle Id : -  Help URL : -
Home Directory : -  Home Drive : -  IEMessage : -  Impersonation Level : -  Linked Logonid : -  Logging Result : -  Logon Process : -  Machine Account Quota : -  Min Password Length : -  Mixed Domain Mode : -  NAS Identifier : -  Network Account Domain : -  Network Account Name : -
```

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.



EVENTID = "529"

-
2024-05-23 00:00:00 - 2024-05-23 23:59:59 Select query with date

#mssqlerror
2024-05-17 00:00:00 - 2024-05-17 23:59:59 Select query with date

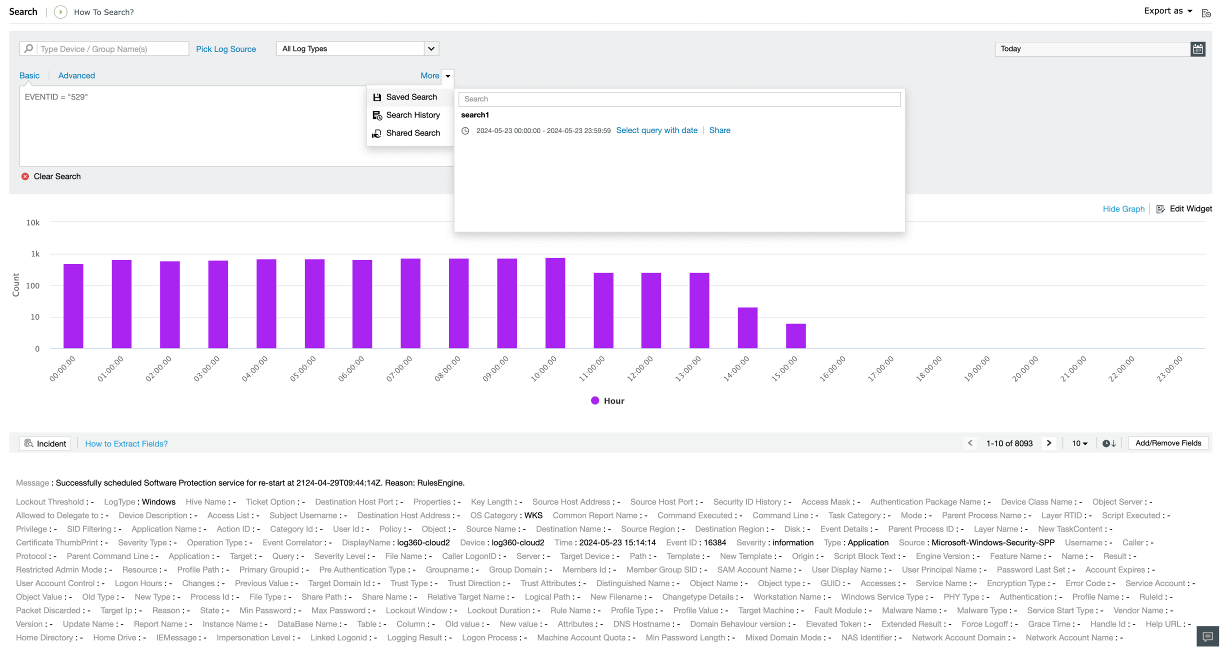
((SEVERITY != "Error" AND SOURCE != "MSSQLSERVER"))
2024-04-24 00:00:00 - 2024-05-23 23:59:59 Select query with date

((SEVERITY = "Error" AND SOURCE = "MSSQLSERVER"))

```
Message : Successfully scheduled Software Protection service for re-start at 2124-04-29T09:44:14Z. Reason: RulesEngine.
Lockout Threshold : -   LogType : Windows   Hive Name : -   Ticket Option : -   Destination Host Port : -   Properties : -   Key Length : -   Source Host Address : -   Source Host Port : -   Security ID History : -   Access Mask : -   Authentication Package Name : -   Device Class Name : -   Object Server : -
Allowed to Delegate to : -   Device Description : -   Access List : -   Subject Username : -   Destination Host Address : -   OS Category : WKS   Common Report Name : -   Command Executed : -   Command Line : -   Task Category : -   Mode : -   Parent Process Name : -   Layer RTID : -   Script Executed : -
Privilege : -   SID Filtering : -   Application Name : -   Action ID : -   Category Id : -   User Id : -   Policy : -   Object : -   Source Name : -   Destination Name : -   Source Region : -   Destination Region : -   Disk : -   Event Details : -   Parent Process ID : -   Layer Name : -   New TaskContent : -
Certificate ThumbPrint : -   Severity Type : -   Operation Type : -   Event Correlator : -   DisplayName : log360-cloud2   Device : log360-cloud2   Time : 2024-05-23 15:14:14   Event ID : 16384   Severity : information   Type : Application   Source : Microsoft-Windows-Security-SPP   Username : -   Caller : -
Protocol : -   Parent Command Line : -   Application : -   Target : -   Query : -   Severity Level : -   File Name : -   Caller LogonID : -   Server : -   Target Device : -   Path : -   Template : -   New Template : -   Origin : -   Script Block Text : -   Engine Version : -   Feature Name : -   Name : -   Result : -
Restricted Admin Mode : -   Resource : -   Profile Path : -   Primary Groupid : -   Pre Authentication Type : -   Groupname : -   Group Domain : -   Members Id : -   Member Group SID : -   SAM Account Name : -   User Display Name : -   User Principal Name : -   Password Last Set : -   Account Expires : -
User Account Control : -   Logon Hours : -   Changes : -   Previous Value : -   Target Domain Id : -   Trust Type : -   Trust Direction : -   Trust Attributes : -   Distinguished Name : -   Object Name : -   Object type : -   GUID : -   Accesses : -   Service Name : -   Encryption Type : -   Error Code : -   Service Account : -
Object Value : -   Old Type : -   New Type : -   Process Id : -   File Type : -   Share Path : -   Share Name : -   Relative Target Name : -   Logical Path : -   New Filename : -   Changetype Details : -   Workstation Name : -   Windows Service Type : -   PHY Type : -   Authentication : -   Profile Name : -   RuleId : -
Packet Discarded : -   Target Ip : -   Reason : -   State : -   Min Password : -   Max Password : -   Lockout Window : -   Lockout Duration : -   Rule Name : -   Profile Type : -   Profile Value : -   Target Machine : -   Fault Module : -   Malware Name : -   Malware Type : -   Service Start Type : -   Vendor Name : -
Version : -   Update Name : -   Report Name : -   Instance Name : -   DataBase Name : -   Table : -   Column : -   Old value : -   New value : -   Attributes : -   DNS Hostname : -   Domain Behaviour version : -   Elevated Token : -   Extended Result : -   Force Logoff : -   Grace Time : -   Handle Id : -   Help URL : -
Home Directory : -   Home Drive : -   IEMessage : -   Impersonation Level : -   Linked Logonid : -   Logging Result : -   Logon Process : -   Machine Account Quota : -   Min Password Length : -   Mixed Domain Mode : -   NAS Identifier : -   Network Account Domain : -   Network Account Name : -
```

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.



EVENTID = "529"

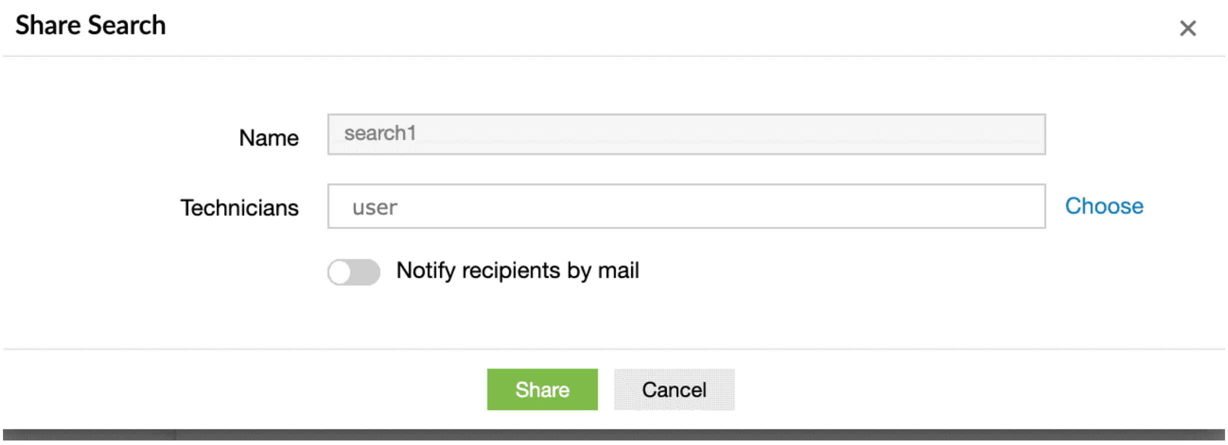
search1
2024-05-23 00:00:00 - 2024-05-23 23:59:59 Select query with date | Share

```
Message : Successfully scheduled Software Protection service for re-start at 2124-04-29T09:44:14Z. Reason: RulesEngine.
Lockout Threshold : -   LogType : Windows   Hive Name : -   Ticket Option : -   Destination Host Port : -   Properties : -   Key Length : -   Source Host Address : -   Source Host Port : -   Security ID History : -   Access Mask : -   Authentication Package Name : -   Device Class Name : -   Object Server : -
Allowed to Delegate to : -   Device Description : -   Access List : -   Subject Username : -   Destination Host Address : -   OS Category : WKS   Common Report Name : -   Command Executed : -   Command Line : -   Task Category : -   Mode : -   Parent Process Name : -   Layer RTID : -   Script Executed : -
Privilege : -   SID Filtering : -   Application Name : -   Action ID : -   Category Id : -   User Id : -   Policy : -   Object : -   Source Name : -   Destination Name : -   Source Region : -   Destination Region : -   Disk : -   Event Details : -   Parent Process ID : -   Layer Name : -   New TaskContent : -
Certificate ThumbPrint : -   Severity Type : -   Operation Type : -   Event Correlator : -   DisplayName : log360-cloud2   Device : log360-cloud2   Time : 2024-05-23 15:14:14   Event ID : 16384   Severity : information   Type : Application   Source : Microsoft-Windows-Security-SPP   Username : -   Caller : -
Protocol : -   Parent Command Line : -   Application : -   Target : -   Query : -   Severity Level : -   File Name : -   Caller LogonID : -   Server : -   Target Device : -   Path : -   Template : -   New Template : -   Origin : -   Script Block Text : -   Engine Version : -   Feature Name : -   Name : -   Result : -
Restricted Admin Mode : -   Resource : -   Profile Path : -   Primary Groupid : -   Pre Authentication Type : -   Groupname : -   Group Domain : -   Members Id : -   Member Group SID : -   SAM Account Name : -   User Display Name : -   User Principal Name : -   Password Last Set : -   Account Expires : -
User Account Control : -   Logon Hours : -   Changes : -   Previous Value : -   Target Domain Id : -   Trust Type : -   Trust Direction : -   Trust Attributes : -   Distinguished Name : -   Object Name : -   Object type : -   GUID : -   Accesses : -   Service Name : -   Encryption Type : -   Error Code : -   Service Account : -
Object Value : -   Old Type : -   New Type : -   Process Id : -   File Type : -   Share Path : -   Share Name : -   Relative Target Name : -   Logical Path : -   New Filename : -   Changetype Details : -   Workstation Name : -   Windows Service Type : -   PHY Type : -   Authentication : -   Profile Name : -   RuleId : -
Packet Discarded : -   Target Ip : -   Reason : -   State : -   Min Password : -   Max Password : -   Lockout Window : -   Lockout Duration : -   Rule Name : -   Profile Type : -   Profile Value : -   Target Machine : -   Fault Module : -   Malware Name : -   Malware Type : -   Service Start Type : -   Vendor Name : -
Version : -   Update Name : -   Report Name : -   Instance Name : -   DataBase Name : -   Table : -   Column : -   Old value : -   New value : -   Attributes : -   DNS Hostname : -   Domain Behaviour version : -   Elevated Token : -   Extended Result : -   Force Logoff : -   Grace Time : -   Handle Id : -   Help URL : -
Home Directory : -   Home Drive : -   IEMessage : -   Impersonation Level : -   Linked Logonid : -   Logging Result : -   Logon Process : -   Machine Account Quota : -   Min Password Length : -   Mixed Domain Mode : -   NAS Identifier : -   Network Account Domain : -   Network Account Name : -
```

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.

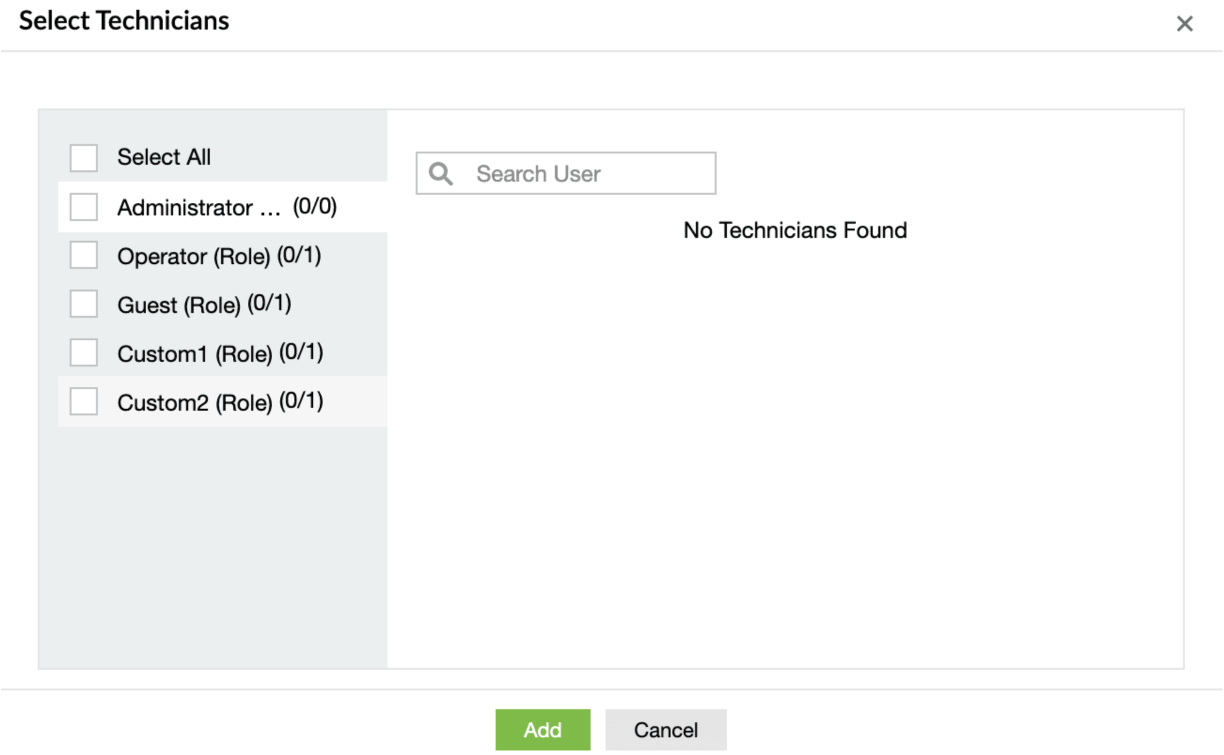


Share Search ✕

Name: search1

Technicians: user

After clicking the Share option, you can select technicians to notify via email by toggling the Notify recipients via mail button.

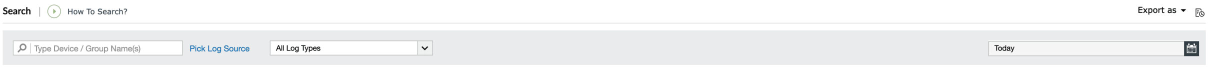


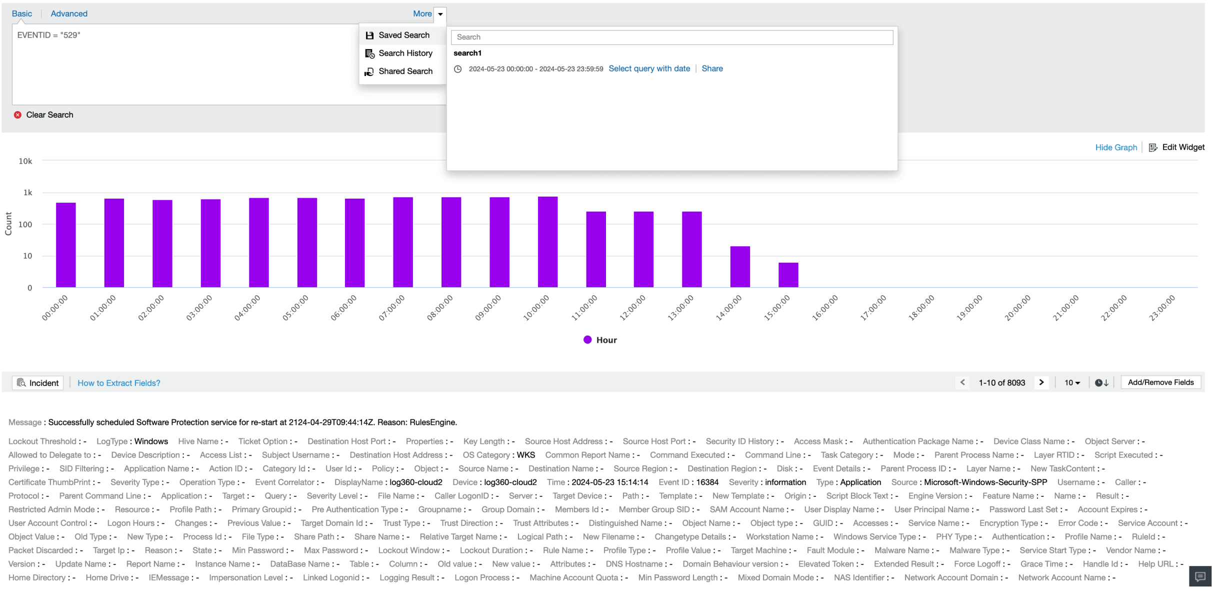
Select Technicians ✕

□ Select All
□ Administrator ... (0/0)
□ Operator (Role) (0/1)
□ Guest (Role) (0/1)
□ Custom1 (Role) (0/1)
□ Custom2 (Role) (0/1)

No Technicians Found

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.





EVENTID = "529"

search1

2024-05-23 00:00:00 - 2024-05-23 23:59:59 Select query with date | Share

Message : Successfully scheduled Software Protection service for re-start at 2124-04-29T09:44:14Z. Reason: RulesEngine.

Lockout Threshold : - LogType : Windows Hive Name : - Ticket Option : - Destination Host Port : - Properties : - Key Length : - Source Host Address : - Source Host Port : - Security ID History : - Access Mask : - Authentication Package Name : - Device Class Name : - Object Server : -
Allowed to Delegate to : - Device Description : - Access List : - Subject Username : - Destination Host Address : - OS Category : WKS Common Report Name : - Command Executed : - Command Line : - Task Category : - Mode : - Parent Process Name : - Layer RTID : - Script Executed : -
Privilege : - SID Filtering : - Application Name : - Action ID : - Category Id : - User Id : - Policy : - Object : - Source Name : - Destination Name : - Source Region : - Destination Region : - Disk : - Event Details : - Parent Process ID : - Layer Name : - New TaskContent : -
Certificate ThumbPrint : - Severity Type : - Operation Type : - Event Correlator : - DisplayName : log360-cloud2 Device : log360-cloud2 Time : 2024-05-23 15:14:14 Event ID : 16384 Severity : information Type : Application Source : Microsoft-Windows-Security-SPP Username : - Caller : -
Protocol : - Parent Command Line : - Application : - Target : - Query : - Severity Level : - File Name : - Caller LogonID : - Server : - Target Device : - Path : - Template : - New Template : - Origin : - Script Block Text : - Engine Version : - Feature Name : - Name : - Result : -
Restricted Admin Mode : - Resource : - Profile Path : - Primary Groupid : - Pre Authentication Type : - Groupname : - Group Domain : - Members Id : - Member Group SID : - SAM Account Name : - User Display Name : - User Principal Name : - Password Last Set : - Account Expires : -
User Account Control : - Logon Hours : - Changes : - Previous Value : - Target Domain Id : - Trust Type : - Trust Direction : - Trust Attributes : - Distinguished Name : - Object Name : - Object type : - GUID : - Accesses : - Service Name : - Encryption Type : - Error Code : - Service Account : -
Object Value : - Old Type : - New Type : - Process Id : - File Type : - Share Path : - Share Name : - Relative Target Name : - Logical Path : - New Filename : - Changetype Details : - Workstation Name : - Windows Service Type : - PHY Type : - Authentication : - Profile Name : - RuleId : -
Packet Discarded : - Target Ip : - Reason : - State : - Min Password : - Max Password : - Lockout Window : - Lockout Duration : - Rule Name : - Profile Type : - Profile Value : - Target Machine : - Fault Module : - Malware Name : - Malware Type : - Service Start Type : - Vendor Name : -
Version : - Update Name : - Report Name : - Instance Name : - DataBase Name : - Table : - Column : - Old value : - New value : - Attributes : - DNS Hostname : - Domain Behaviour version : - Elevated Token : - Extended Result : - Force Logoff : - Grace Time : - Handle Id : - Help URL : -
Home Directory : - Home Drive : - IEMessage : - Impersonation Level : - Linked Logonid : - Logging Result : - Logon Process : - Machine Account Quota : - Min Password Length : - Mixed Domain Mode : - NAS Identifier : - Network Account Domain : - Network Account Name : -

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.

2.4.4. Tagging tool

Last updated on: September 12, 2025

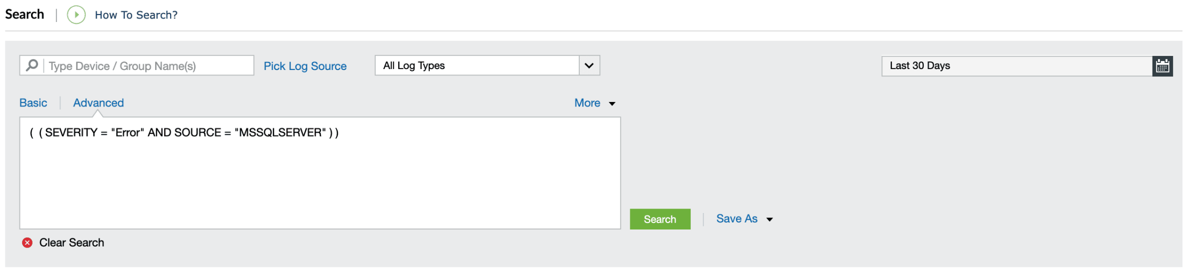
In this page

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?

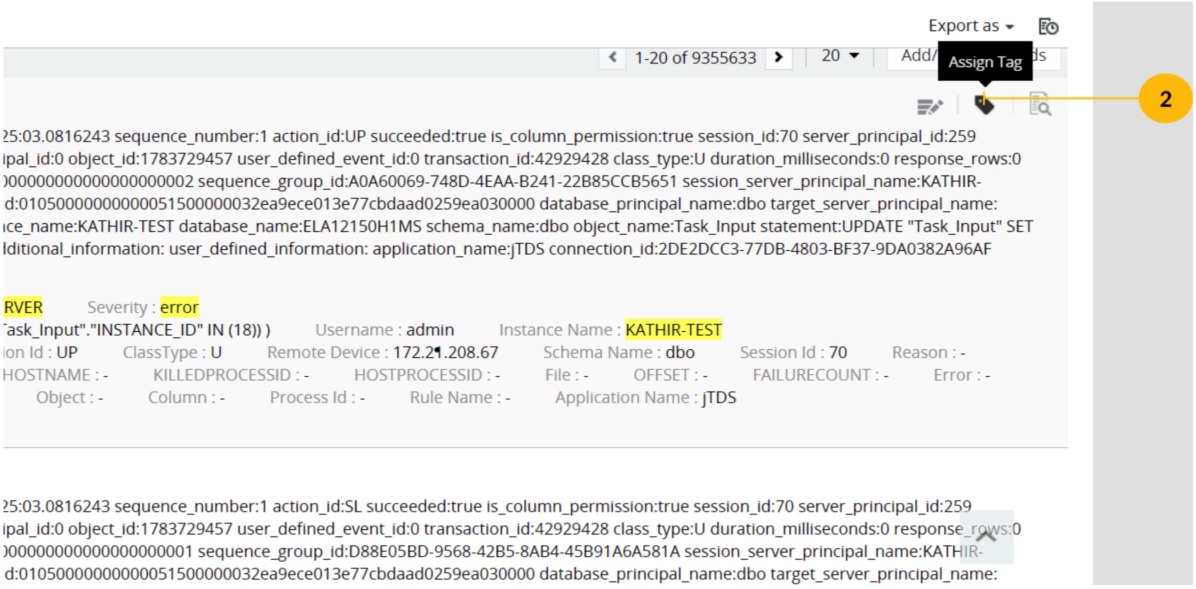
To create a tag, go to Search tab and follow the below steps:

1. Specify all the search criteria which you wish to associate with your new tag and click Search.



```
( ( SEVERITY = "Error" AND SOURCE = "MSSQLSERVER" ) )
```

2. Click on the tag icon on the right side of any log entry in the displayed search result.

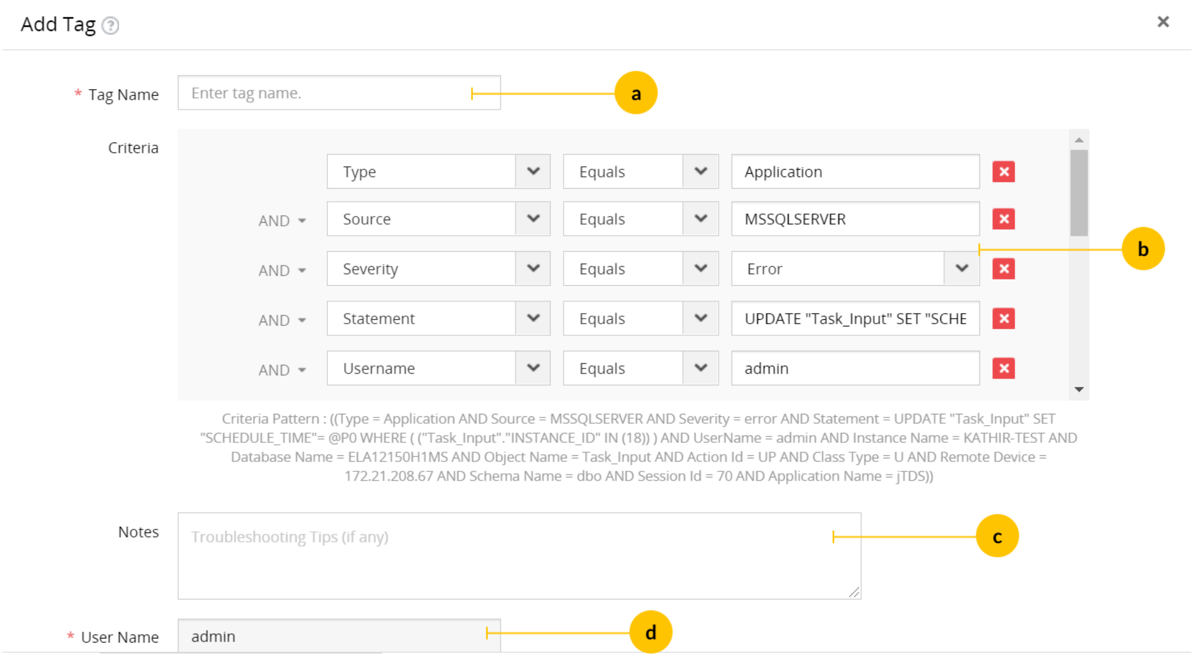


```
25:03.0816243 sequence_number:1 action_id:UP succeeded:true is_column_permission:true session_id:70 server_principal_id:259
ipal_id:0 object_id:1783729457 user_defined_event_id:0 transaction_id:42929428 class_type:U duration_milliseconds:0 response_rows:0
)000000000000000000002 sequence_group_id:A0A60069-748D-4EAA-B241-22B85CCB5651 session_server_principal_name:KATHIR-
d:0105000000000000051500000032ea9ece013e77cbdaad0259ea030000 database_principal_name:dbo target_server_principal_name:
ıce_name:KATHIR-TEST database_name:ELA12150H1MS schema_name:dbo object_name:Task_Input statement:UPDATE "Task_Input" SET
lditional_information: user_defined_information: application_name:jTDS connection_id:2DE2DCC3-77DB-4803-BF37-9DA0382A96AF
```

RVER   Severity : error
Task_Input"."INSTANCE_ID" IN (18)))   Username : admin   Instance Name : KATHIR-TEST
ion Id : UP   ClassType : U   Remote Device : 172.21.208.67   Schema Name : dbo   Session Id : 70   Reason : -
HOSTNAME : -   KILLEDPROCESSID : -   HOSTPROCESSID : -   File : -   OFFSET : -   FAILURECOUNT : -   Error : -
Object : -   Column : -   Process Id : -   Rule Name : -   Application Name : jTDS

```
25:03.0816243 sequence_number:1 action_id:SL succeeded:true is_column_permission:true session_id:70 server_principal_id:259
ipal_id:0 object_id:1783729457 user_defined_event_id:0 transaction_id:42929428 class_type:U duration_milliseconds:0 response_rows:0
)000000000000000000001 sequence_group_id:D88E05BD-9568-42B5-8AB4-45B91A6A581A session_server_principal_name:KATHIR-
d:0105000000000000051500000032ea9ece013e77cbdaad0259ea030000 database_principal_name:dbo target_server_principal_name:
```

3. Fill the required details in the Add Tag pop-up:



Add Tag

* Tag Name
Enter tag name.

Criteria:

	Type	Equals	Application
AND	Source	Equals	MSSQLSERVER
AND	Severity	Equals	Error
AND	Statement	Equals	UPDATE "Task_Input" SET "SCHE
AND	Username	Equals	admin

Criteria Pattern : ((Type = Application AND Source = MSSQLSERVER AND Severity = error AND Statement = UPDATE "Task_Input" SET "SCHEDULE_TIME"= @P0 WHERE (("Task_Input"."INSTANCE_ID" IN (18))) AND UserName = admin AND Instance Name = KATHIR-TEST AND Database Name = ELA12150H1MS AND Object Name = Task_Input AND Action Id = UP AND Class Type = U AND Remote Device = 172.21.208.67 AND Schema Name = dbo AND Session Id = 70 AND Application Name = jTDS))

Notes: Troubleshooting Tips (if any)

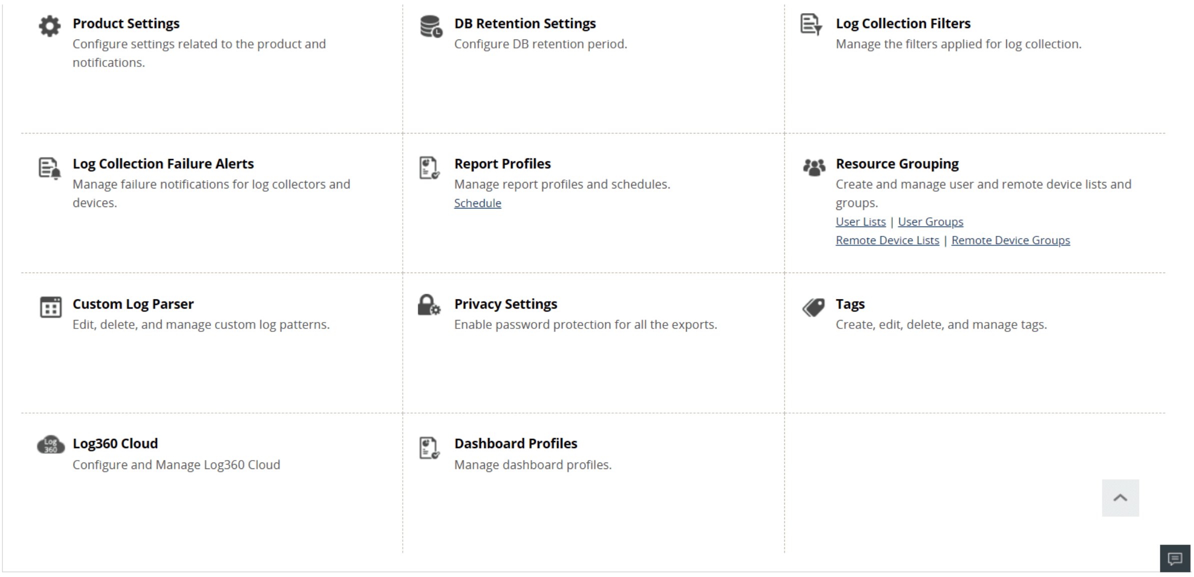
* User Name
admin

- 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.



Product Settings
Configure settings related to the product and notifications.

DB Retention Settings
Configure DB retention period.

Log Collection Filters
Manage the filters applied for log collection.

Log Collection Failure Alerts
Manage failure notifications for log collectors and devices.

Report Profiles
Manage report profiles and schedules.
Schedule

Resource Grouping
Create and manage user and remote device lists and groups.
User Lists | User Groups
Remote Device Lists | Remote Device Groups

Custom Log Parser
Edit, delete, and manage custom log patterns.

Privacy Settings
Enable password protection for all the exports.

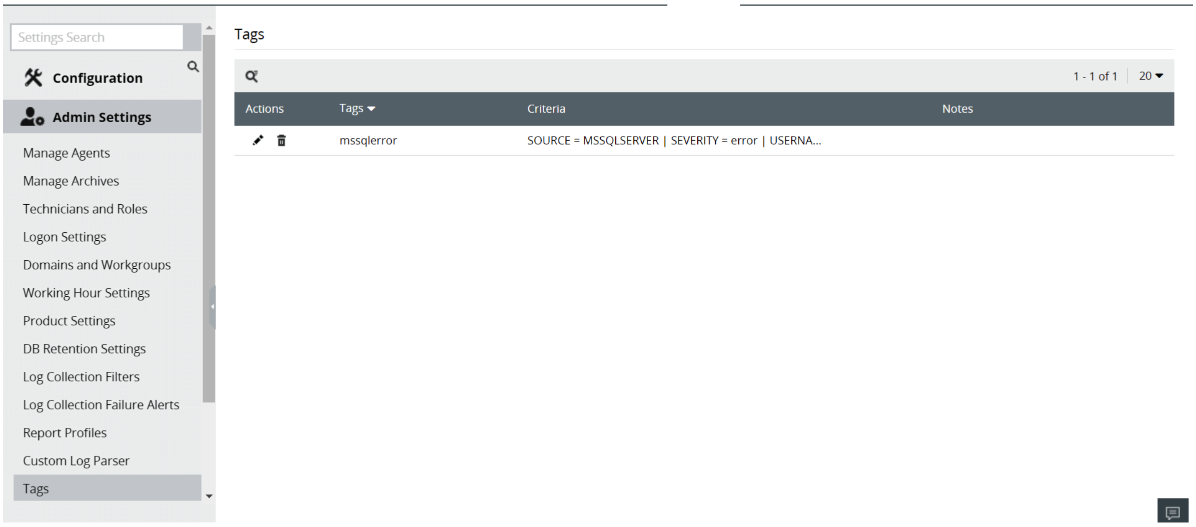
Tags
Create, edit, delete, and manage tags.

Log360 Cloud
Configure and Manage Log360 Cloud

Dashboard Profiles
Manage dashboard profiles.

2. Click the edit icon next to the tag

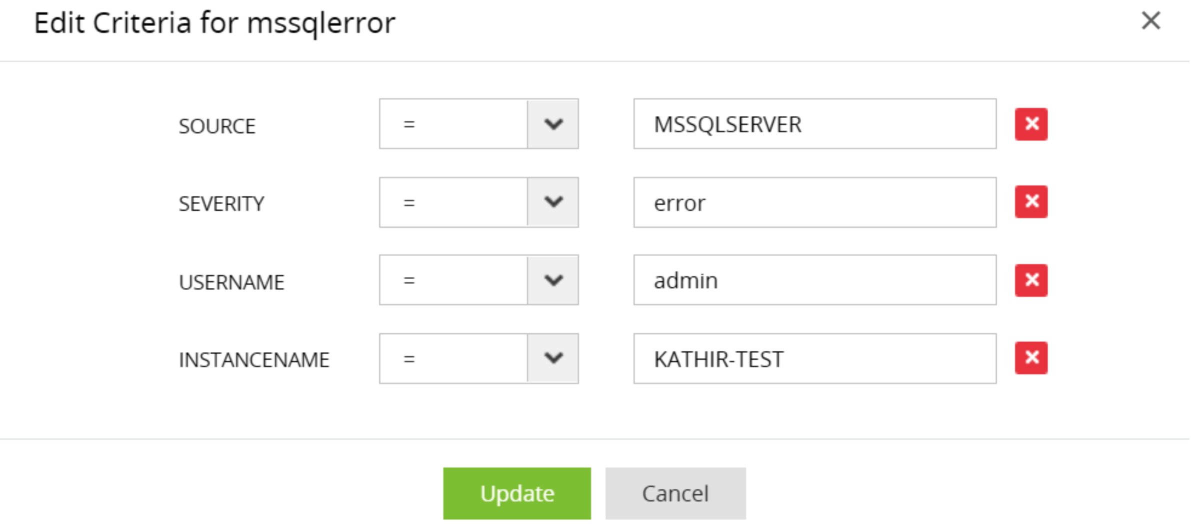
2. Click the edit icon next to the tag.



Tags

Actions	Tags	Criteria	Notes
	mssqlerror	SOURCE = MSSQLSERVER | SEVERITY = error | USERNA...	

3. Modify the tag criteria.



Edit Criteria for mssqlerror

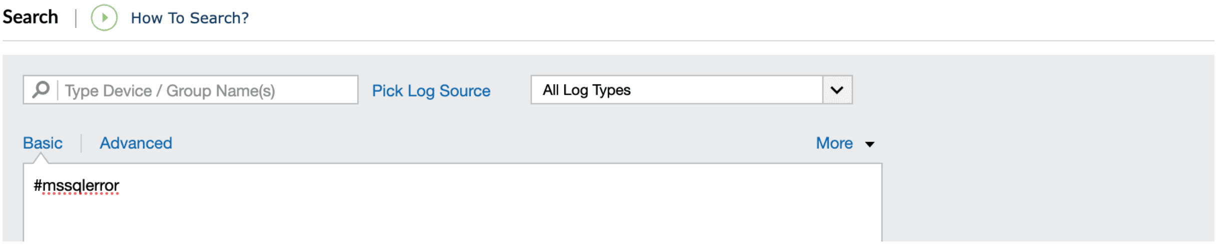
SOURCE	=	MSSQLSERVER
SEVERITY	=	error
USERNAME	=	admin
INSTANCENAME	=	KATHIR-TEST

Note

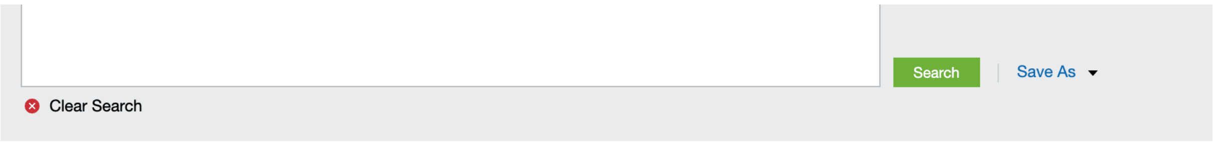
You can also edit tags on the search results page by clicking the edit icon below the tag name.

How to perform log search using a tag

You can search for tags by their name, prefixed with #, in the search query text box.



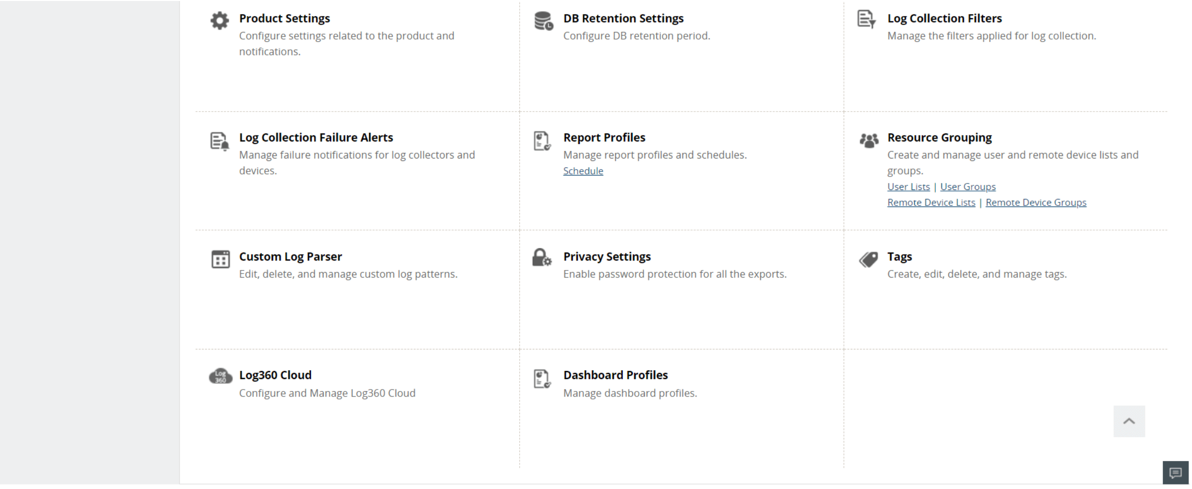
#mssqlerror



> ⓘ 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.



Product Settings
Configure settings related to the product and notifications.

DB Retention Settings
Configure DB retention period.

Log Collection Filters
Manage the filters applied for log collection.

Log Collection Failure Alerts
Manage failure notifications for log collectors and devices.

Report Profiles
Manage report profiles and schedules.
Schedule

Resource Grouping
Create and manage user and remote device lists and groups.
User Lists | User Groups
Remote Device Lists | Remote Device Groups

Custom Log Parser
Edit, delete, and manage custom log patterns.

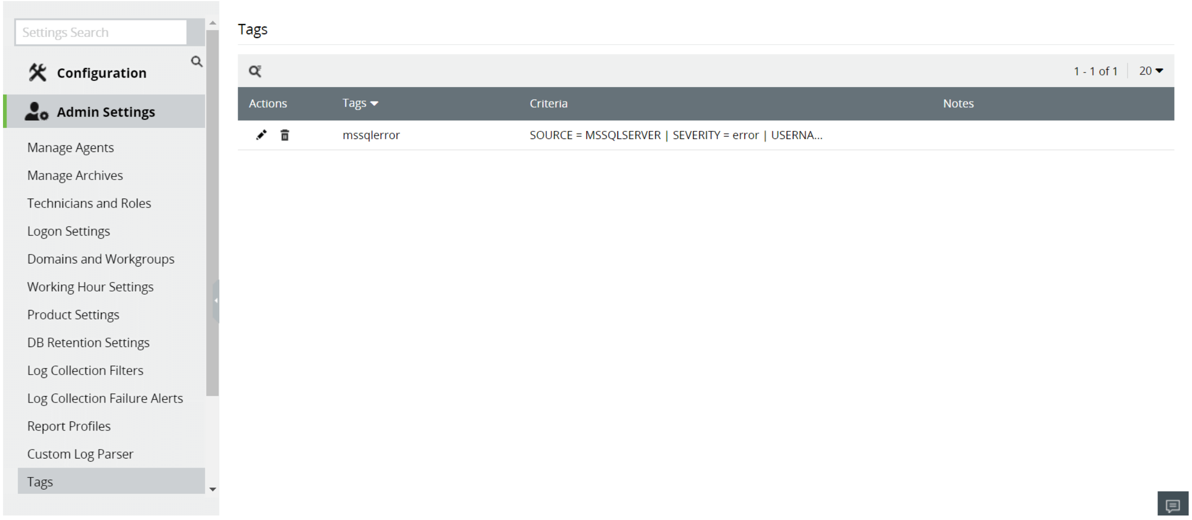
Privacy Settings
Enable password protection for all the exports.

Tags
Create, edit, delete, and manage tags.

Log360 Cloud
Configure and Manage Log360 Cloud

Dashboard Profiles
Manage dashboard profiles.

2. Click on the delete icon beside the tag name in the tag table. Click Yes in the pop-up.



Tags

1 - 1 of 1 | 20

Actions	Tags	Criteria	Notes
✎ 🗑	mssqlerror	SOURCE = MSSQLSERVER | SEVERITY = error | USERNA...	

- 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.

3.1.1. Product Settings

Last updated on: September 12, 2025

You can change the following settings of Log360 from this tab.

- Connection Type
- Security Hardening
- General

Connection Type

1. Choose your connection type. You can choose to use either http or https.
2. Specify the port number of your choice after choosing they type of connection.
   - Default ports - HTTP : 8095, HTTPS : 8458.
3. To enable LDAP SSL, mark the check-box against the Enable LDAP SSL field.
4. Click Save to store the configured settings.

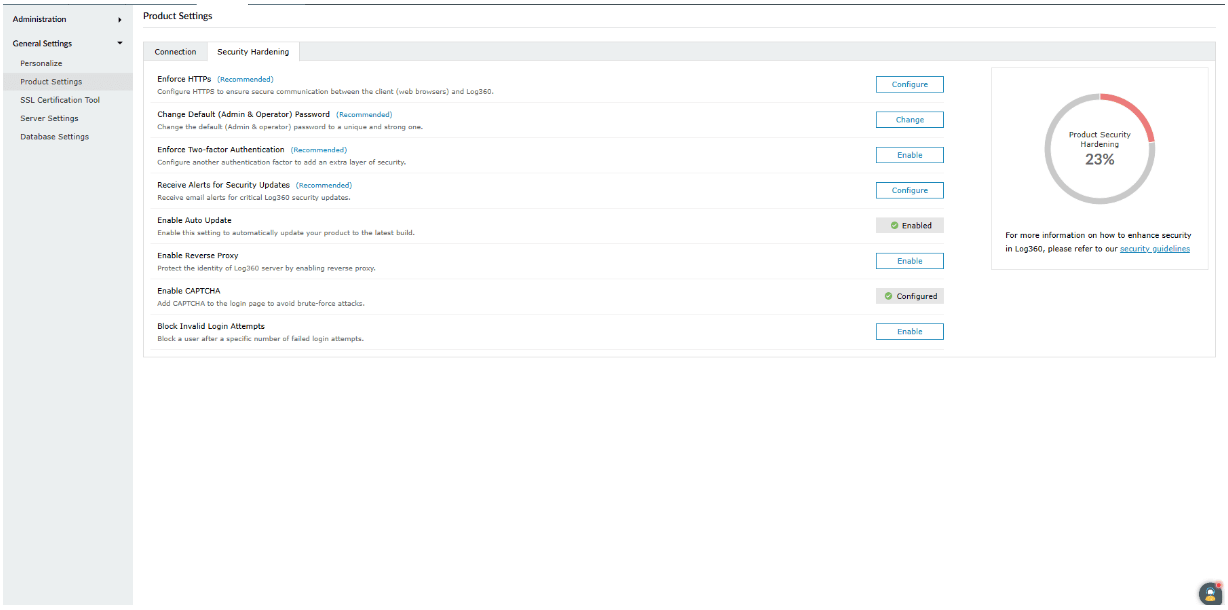
General

1. Be alerted when the available disk space falls below a pre-defined level (1 GB, 2 GB or 5 GB), by selecting the appropriate value from the drop-down box.
2. Select the Session Expiry Time, which is the time for which a user session would last, from the drop-down box.
3. Select the level of logs that is to be collected by the product. The default working mode for Log360 is Normal with minimal set of debugging information. Select Debug to collect detailed log reports.
4. Enable or disable collection of anonymous usage statistics gathering to be sent to us.
5. Click Save to store the configured settings.

3.1.2. Security Hardening

Last updated on: September 12, 2025

Security hardening feature helps you manage and configure the security settings of Log360. This tab also displays a security score which is calculated based upon the weightage given to each configuration.
To manage individual settings, click the Configure or Enable option corresponding to that security setting and make the required changes. Once configured, the setting will have a green ticked Configured/Enabled ✓ icon next to it, as shown in the image below.



Enforce HTTPs (Recommended)
Configure HTTPS to ensure secure communication between the client (web browsers) and Log360. Configure

Change Default (Admin & Operator) Password (Recommended)
Change the default (Admin & operator) password to a unique and strong one. Change

Enforce Two-factor Authentication (Recommended)
Configure another authentication factor to add an extra layer of security. Enable

Receive Alerts for Security Updates (Recommended)
Receive email alerts for critical Log360 security updates. Configure

Enable Auto Update
Enable this setting to automatically update your product to the latest build. ✓ Enabled

Enable Reverse Proxy
Protect the identity of Log360 server by enabling reverse proxy. Enable

Enable CAPTCHA
Add CAPTCHA to the login page to avoid brute-force attacks. ✓ Configured

Block Invalid Login Attempts
Block a user after a specific number of failed login attempts. Enable

For more information on how to enhance security in Log360, please refer to our security guidelines

We recommend you to configure all the settings and ensure your product security score is 100%. The security settings alert will be displayed in the notification center (🔔 icon on the top-right corner) until a security score of 100% is reached.

Note

For licensed customers, the alert will also be displayed after every successful login until all the mandatory security configurations (marked with * under List of security settings) are done.

List of security settings:

1. Enforce HTTPS*
   Configuring HTTPS helps you secure connection between the web browser and the Log360 server. See how to enable HTTPS.

2. Change Default (Admin & Operator) Password*
   It is recommended to use a strong password to access Log360 dashboard. Use this setting to change both the admin and operator password.

3. Enforce Two-factor Authentication*
   Two-factor authentication adds an additional layer of security. See how to configure two-factor authentication

Two-factor authentication adds an additional layer of security. See how to configure two-factor authentication.

4. Receive Alerts for Security Updates*
   Configuring this setting allows you to receive email notifications on the release of important security patches. This ensures that you are well-informed about important security updates for the product, enabling you to update it as soon as possible.

5. Enable Auto Update
   Enable this setting to automatically update your product to the latest build. Click on Configure to navigate to the auto-update settings tab. See how to enable auto-update.

6. Enable Reverse Proxy
   Enabling reverse proxy helps protect the identity of Log360 server. Click on Configure to navigate to the reverse proxy settings tab. See how to enable reverse proxy settings.

7. Enable CAPTCHA
   This setting adds captcha to the login page to avoid brute-force attacks. See how to add captcha.

8. Block Invalid Login Attempts
   This setting allows you to block a specific user who fails to login after a specific number of attempts. See how to block invalid login attempts.

> ⓘ Note
>
> The first three settings given in the above list are mandatory for Log360.

3.2.1.1. Listener ports overview

Last updated on: September 12, 2025

In this page

Overview

The Listener Port console provides an interface for configuring and managing ports used to receive incoming logs and messages. Log360 supports both Syslog listener ports (UDP/TCP/TLS) and SNMP Traps listener ports (UDP) for receiving logs. With these ports, external devices and applications send logs and traps to the collector/agent.

Prerequisites

- Port availability: Ensure that the configured ports are not used by any other applications or services on the Log360 server.
- Firewall and antivirus rules:
  - Allow all incoming traffic on the specified ports on the agent/machine running the Log360 server's firewall.
  - Some antivirus software may block unknown or custom ports by default. Ensure that your antivirus tool is

also configured to permit traffic on the configured listener ports.

- Network devices configuration: Configure the external devices to send Syslog messages/SNMP Traps to the server's IP address and the designated port.

Need for listener port configuration

Without properly configured listener ports, the server cannot receive, process, or analyze the incoming log data.

Key functionalities

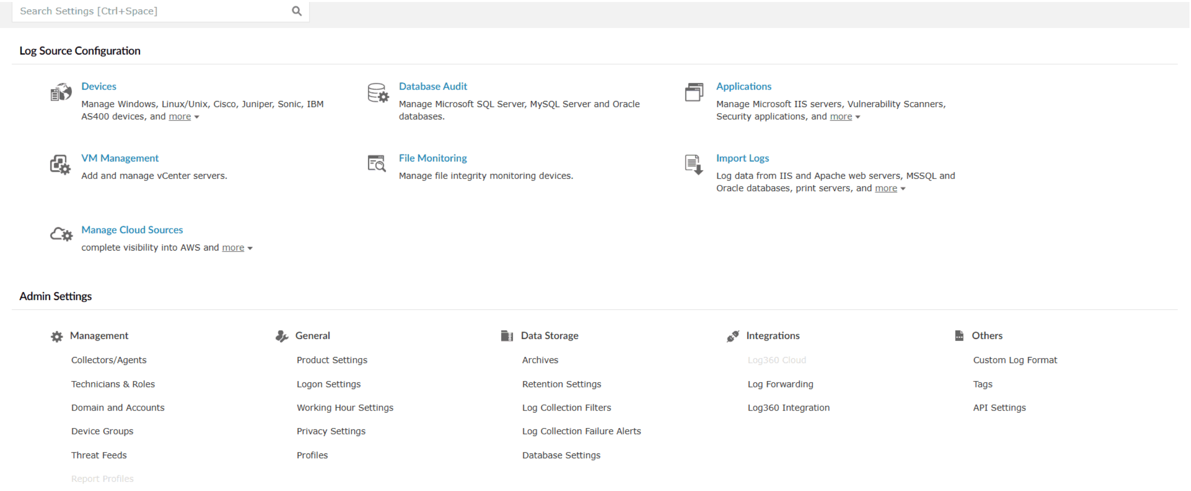
- Seamless log collection: Logs from the network devices can be received only when the appropriate ports are open and listening.
- Protocol flexibility: You can configure multiple ports for different protocols (UDP, TCP, TLS) based on your network's security and reliability requirements.
- Security and access control: By selectively enabling or disabling ports per collector/agent, you can restrict log intake to trusted sources and minimize your attack surface.

Configuring Syslog listener ports

The Listener Ports module lets you manage the ports used to receive incoming logs from external devices. You can assign protocols (UDP, TCP, TLS), configure default Syslog ports, and control which collectors or agents listen on specific ports. This section explains how to access the configuration interface for the Syslog listener ports and perform actions like adding new Syslog listener ports, editing existing ones, and managing port-to-collector/agent mappings to streamline log intake.

Accessing Syslog listener ports settings

1. In the product console, navigate to the Settings tab and click on Listener ports listed under System Settings as shown in the below image.



Search Settings [Ctrl+Space]

Log Source Configuration

Devices
Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more ▾

Database Audit
Manage Microsoft SQL Server, MySQL Server and Oracle databases.

Applications
Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more ▾

VM Management
Add and manage vCenter servers.

File Monitoring
Manage file integrity monitoring devices.

Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more ▾

Manage Cloud Sources
complete visibility into AWS and more ▾

Admin Settings

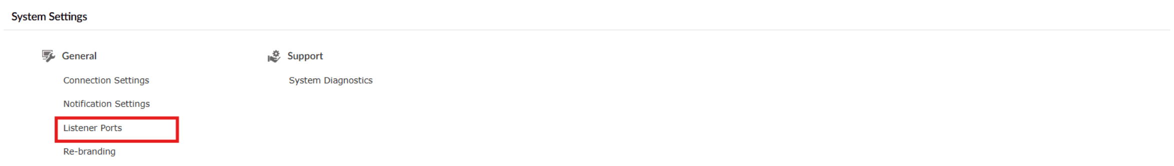
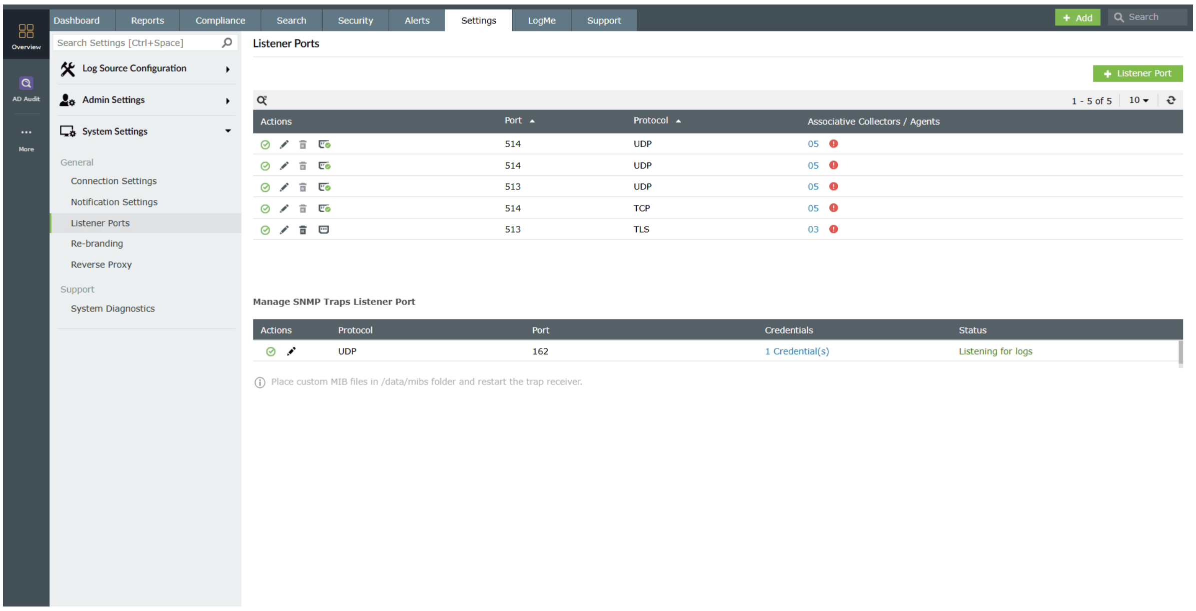


Image 1: Accessing listener ports settings

2. The Listener Ports module for Syslog ports configuration provides you with:

- Port: Displays the port number
- Action: Option to enable/disable, edit, delete or make default the listener port(s).
- Protocol: Displays the operating protocol for that particular port.
- Associated Collectors/Agents: Displays all the collectors/agents associated with the corresponding port number.



Listener Ports

Actions	Port	Protocol	Associative Collectors / Agents
	514	UDP	05
	514	UDP	05
	513	UDP	05
	514	TCP	05
	513	TLS	03

Manage SNMP Traps Listener Port

Actions	Protocol	Port	Credentials	Status
	UDP	162	1 Credential(s)	Listening for logs

Place custom MIB files in /data/mibs folder and restart the trap receiver.

Image 2: Listener ports configuration via the Settings tab

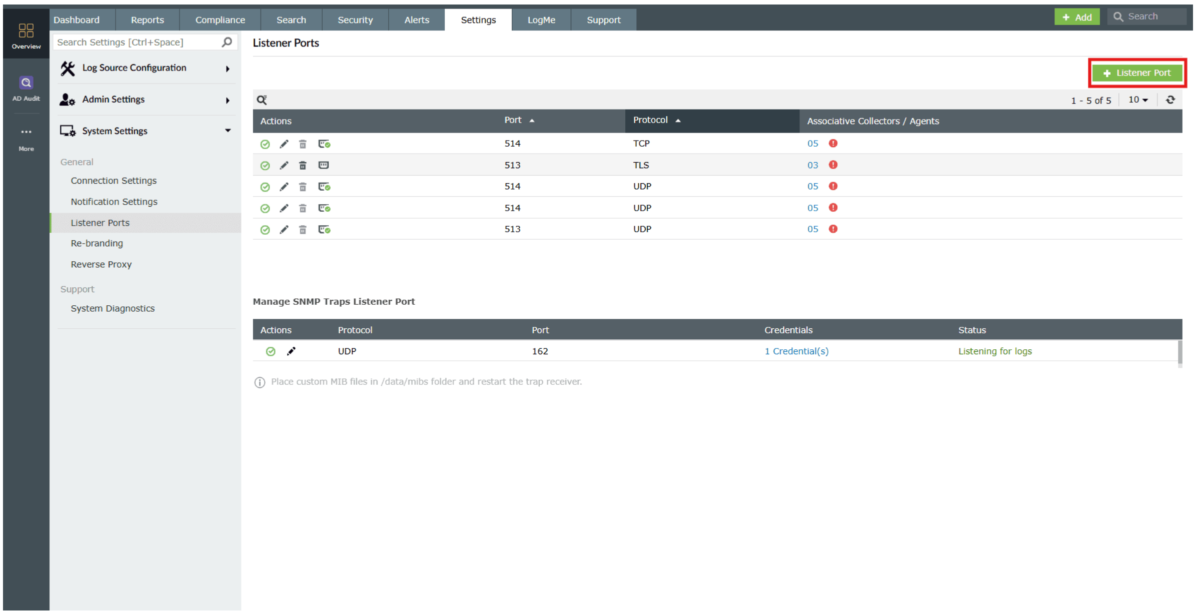
Manage Syslog listener ports

The following are the available actions for the syslog ports under listener port configuration:

- Add a Syslog port
- Manage default Syslog port
- Delete a Syslog port
- Enable/disable a Syslog port
- Enable/disable a Syslog port for selective collectors/agents
- Edit an existing Syslog port

Adding a Syslog port

1. Navigate to the Listener Ports module in the product console and click on the +Listener Port button as highlighted below.



Listener Ports

Actions	Port	Protocol	Associative Collectors / Agents
	514	TCP	05
	513	TLS	03
	514	UDP	05
	514	UDP	05
	513	UDP	05

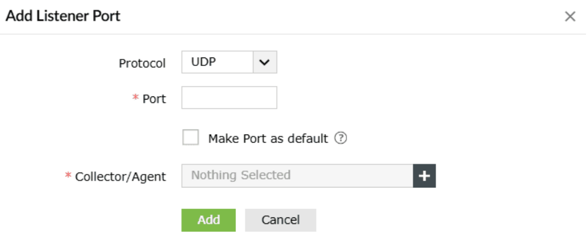
Manage SNMP Traps Listener Port

Actions	Protocol	Port	Credentials	Status
	UDP	162	1 Credential(s)	Listening for logs

Place custom MIB files in /data/mibs folder and restart the trap receiver.

Image 3: Adding a listener port via the Settings tab

2. The Add Listener Port pop-up slides in.



Protocol: UDP

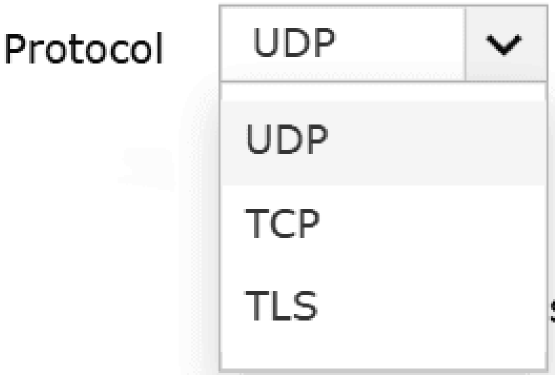
* Port:

□ Make Port as default

* Collector/Agent: Nothing Selected

3. Fill in the required fields:

- Protocol: Select the protocol from the drop-down.



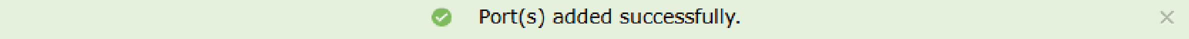
- Port: Specify the port number for log collection.
  - Fill in the check-box provided if you wish to make that specific port the default port number that will be

- Fill in the check-box provided if you wish to make that specific port the default port number that will be automatically associated to newly added collector/agents in future configurations. Ensure the pre-requisites are met before filling in the port number.

- Add Collector/Agent: Select the Collector/Agent(s) on which this port can be enabled.

> ⓘ NOTE
>
> - The Select Collector/Agent option will be visible only if a remote collector/agent has been added in the server.
> - For each protocol, you can add only 6 ports.

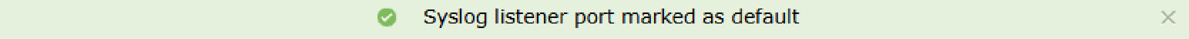
4. Click on Add.
5. Upon successful completion of the action, the below pop-up appears.



Port(s) added successfully.

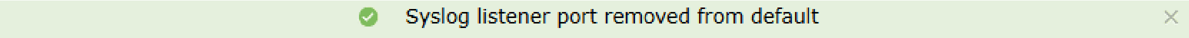
Manage default Syslog listener port

1. To make a port as a default port for syslog collection, click the icon under the Actions tab.
2. Upon successful completion of the action, the below pop-up appears.



Syslog listener port marked as default

3. Similarly, to remove a port from being default, click on the remove as default port icon .
4. Upon successful completion of the action, the below pop-up appears.



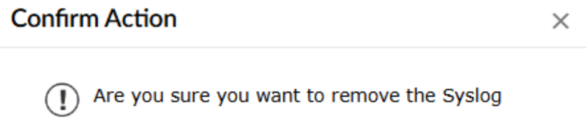
Syslog listener port removed from default

Once you make the port default, all collector/agent(s) will listen through that specific port.

Deleting a Syslog port

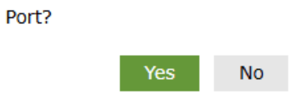
> ⓘ Note
>
> Default ports cannot be deleted. You must remove a port as default port first to delete it.

1. Click on the Delete icon under the Actions column to delete a listener port.
2. A Confirm Action pop-up appears. Click on Yes.

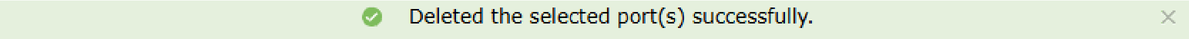


Confirm Action

Are you sure you want to remove the Syslog


Port?

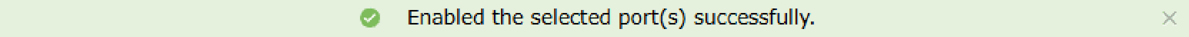
3. Upon successful completion of the action, the below pop-up appears.


Deleted the selected port(s) successfully.

Enable/disable a Syslog listener port

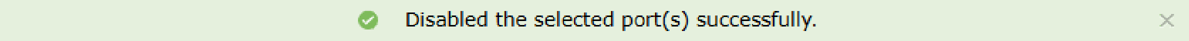
Enabling a Syslog listener port

1. Click on the currently disabled icon ⊘ under the Actions column to enable the port.
2. As soon as you perform this action, the icon indicates that the port is now enabled ✓ and the below pop-up message appears briefly.


Enabled the selected port(s) successfully.

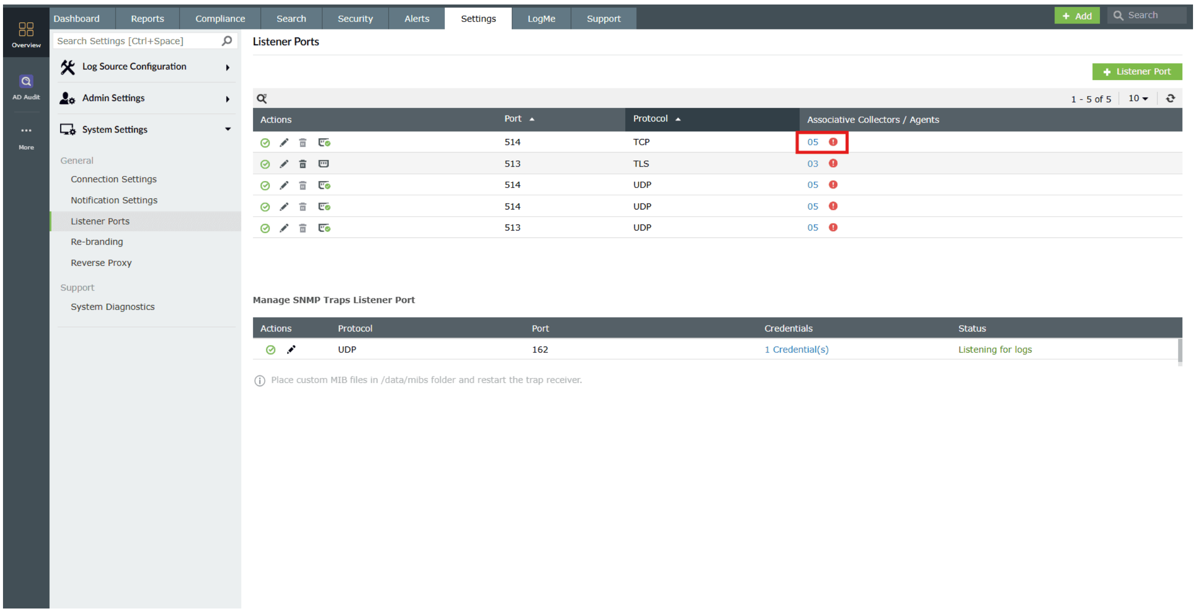
Disabling a Syslog listener port

1. Click on the currently enabled icon ✓ under the Actions column to disable the port.
2. As soon as you perform this action, the icon indicates that the port is now disabled ⊘ and the below pop-up message appears briefly.


Disabled the selected port(s) successfully.

Enable/disable a Syslog listener port for selective collectors/agents

1. Click on the corresponding number in the Associated Collectors/Agents column for the port you wish to view the associated collectors/agents for.



Listener Ports

Actions	Port	Protocol	Associative Collectors / Agents
	514	TCP	05
	513	TLS	03
	514	UDP	05
	514	UDP	05
	513	UDP	05

Manage SNMP Traps Listener Port

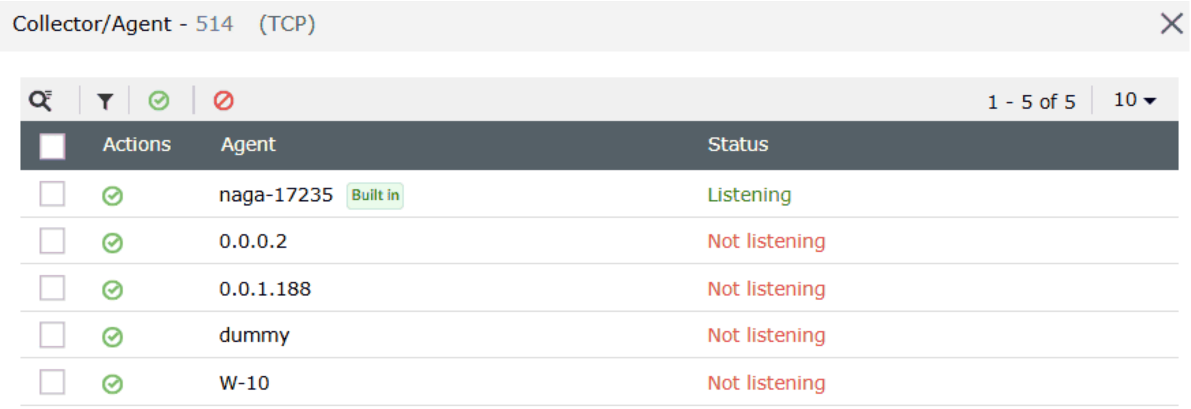
Actions	Protocol	Port	Credentials	Status
	UDP	162	1 Credential(s)	Listening for logs

Place custom MIB files in /data/mibs folder and restart the trap receiver.

Image 4: Associated collectors/agents for the syslog listener ports

2. This will open the list of Collectors/Agents and their status along with a troubleshooting link , in the case of an

error.



Collector/Agent - 514 (TCP)

1 - 5 of 5 10

□	Actions	Agent	Status
□	✓	naga-17235 Built in	Listening
□	✓	0.0.0.2	Not listening
□	✓	0.0.1.188	Not listening
□	✓	dummy	Not listening
□	✓	W-10	Not listening

Image 4: Associated collectors/agents for the syslog listener ports

Note

By default, all Collectors/Agents are in an enabled state.

To enable:

1. Click on the currently disabled icon ⊘ under the Actions column to enable the port for that specific collector/agent.
2. As soon as you perform this action, the icon indicates that the port is now enabled ✓ for that particular collector/agent, and the below pop-up message appears briefly.

To disable:

1. Click on the currently enabled icon ✓ under the Actions column to disable the port for that specific

collector/agent.

2. As soon as you perform this action, the icon indicates that the port is now disabled ⊘ for that particular collector/agent, and the below pop-up message appears briefly.

To enable/disable a port for multiple collectors at once:

1. Select the desired collectors by clicking on the checkboxes provided and click on the enable/disable icon at the top.
2. Upon successfully enabling, the below pop-up appears.

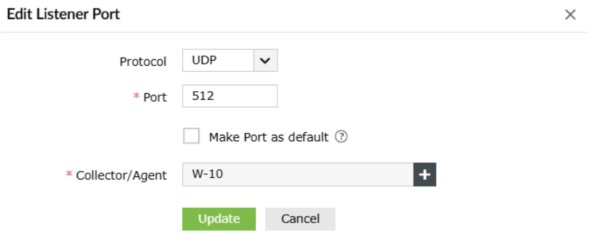
Enabled the port for collector(s) successfully.

3. Upon successfully disabling, the below pop-up appears.

Disabled the port for collector(s) successfully.

Edit a Syslog listener port

1. Click on the Edit icon ✎ under the Actions column to edit the respective port.
2. The Edit Listener Port box will be displayed. Make the necessary edits and click on Save.



Edit Listener Port

Protocol: UDP

* Port: 512

□ Make Port as default

* Collector/Agent: W-10

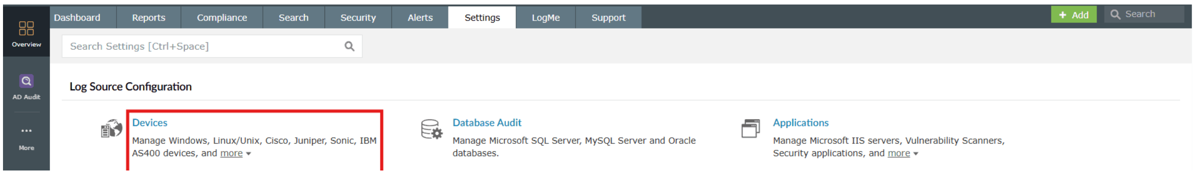
3. The changes are updated instantly. Upon successful completion of the action, the below pop-up appears.

Port(s) updated successfully.

Associating a collector/agent for a device

Use this interface to select a collector or agent while configuring the device/application or the listener port(s).

1. In the product console, navigate to the Settings tab and click on Devices.

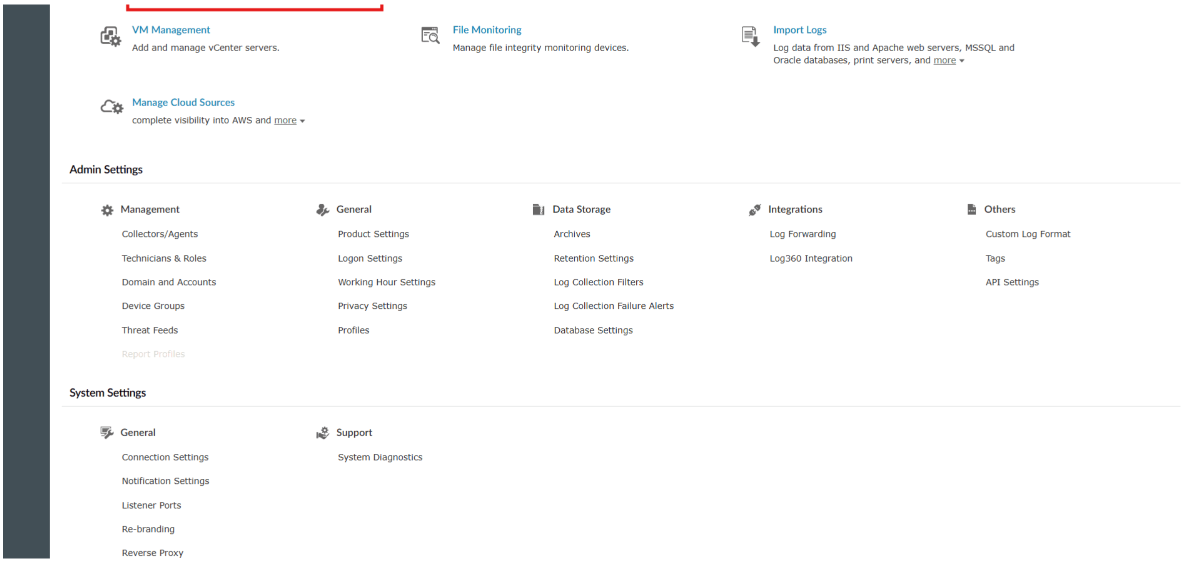


Log Source Configuration

Devices: Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more ▾

Database Audit: Manage Microsoft SQL Server, MySQL Server and Oracle databases.

Applications: Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more ▾



VM Management
Add and manage vCenter servers.

File Monitoring
Manage file integrity monitoring devices.

Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more

Manage Cloud Sources
complete visibility into AWS and more

Admin Settings

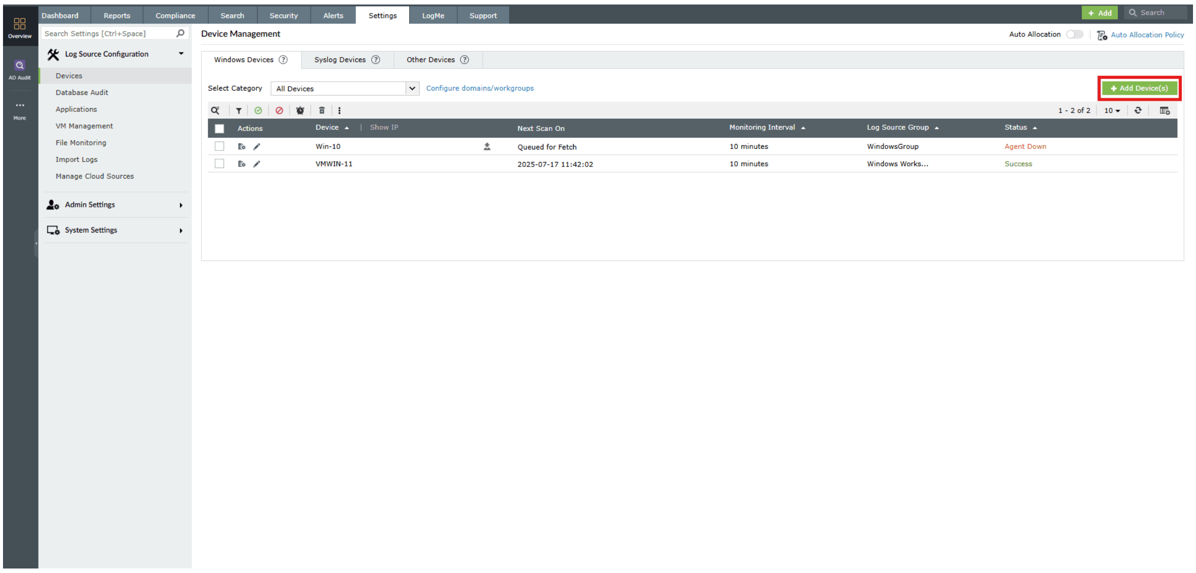
Management	General	Data Storage	Integrations	Others
Collectors/Agents	Product Settings	Archives	Log Forwarding	Custom Log Format
Technicians & Roles	Logon Settings	Retention Settings	Log360 Integration	Tags
Domain and Accounts	Working Hour Settings	Log Collection Filters		API Settings
Device Groups	Privacy Settings	Log Collection Failure Alerts		
Threat Feeds	Profiles	Database Settings		
Report Profiles				

System Settings

General	Support
Connection Settings	System Diagnostics
Notification Settings	
Listener Ports	
Re-branding	
Reverse Proxy	

Image 5: Add devices via the Settings tab

2. Click on the +Add Device(s) button as highlighted below.



Device Management

Auto Allocation | Auto Allocation Policy

Windows Devices | Syslog Devices | Other Devices

Select Category: All Devices | Configure domains/workgroups

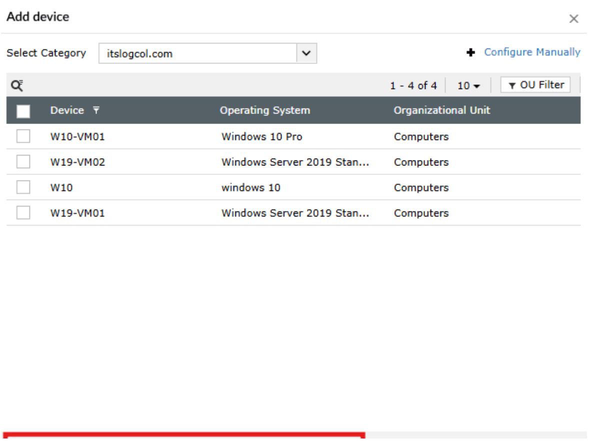
+ Add Device(s)

1 - 2 of 2 | 10

	Actions	Device | Show IP	Next Scan On	Monitoring Interval	Log Source Group	Status
□		Win-10	Queued for Fetch	10 minutes	WindowsGroup	Agent Down
□		VMWIN-11	2025-07-17 11:42:02	10 minutes	Windows Works...	Success

Image 6: Adding a device to a listener port configuration

3. The Add device pop-up box appears. In the Collector/Agent field as highlighted below, click the plus + icon to display the list of available collectors/agents.

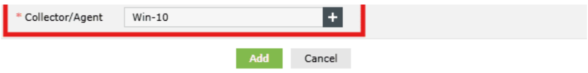


Add device ×

Select Category: itslogcol.com | + Configure Manually

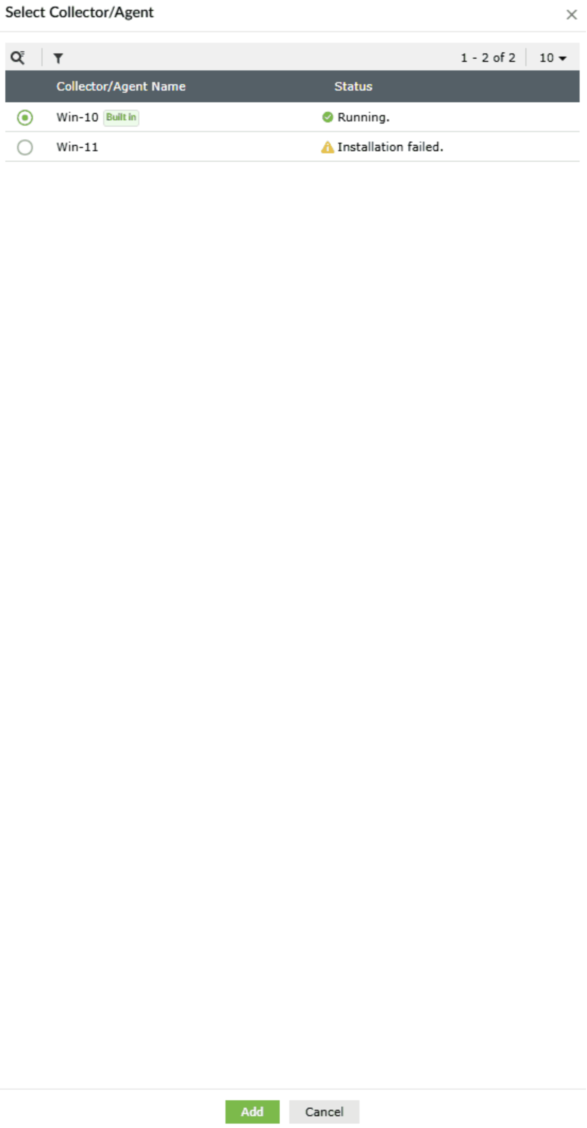
1 - 4 of 4 | 10 | OU Filter

□	Device	Operating System	Organizational Unit
□	W10-VM01	Windows 10 Pro	Computers
□	W19-VM02	Windows Server 2019 Stan...	Computers
□	W10	windows 10	Computers
□	W19-VM01	Windows Server 2019 Stan...	Computers



* Collector/Agent: Win-10

4. Select the appropriate collector/agent from the list that appears on the screen.



Select Collector/Agent

1 - 2 of 2 | 10

	Collector/Agent Name	Status
●	Win-10 Built in	✓ Running.
○	Win-11	⚠ Installation failed.

5. Click on Add to confirm your choice and proceed.

Read also

This document explained how to configure and manage listener ports (Syslog listener ports) in the product console, covering prerequisites, key features, and selective control options. For more on enhancing log collection and device integration, refer to the related pages below:

- SNMP Traps port management

3.2.1.2. SNMP Traps port management

Last updated on: September 12, 2025

In this page

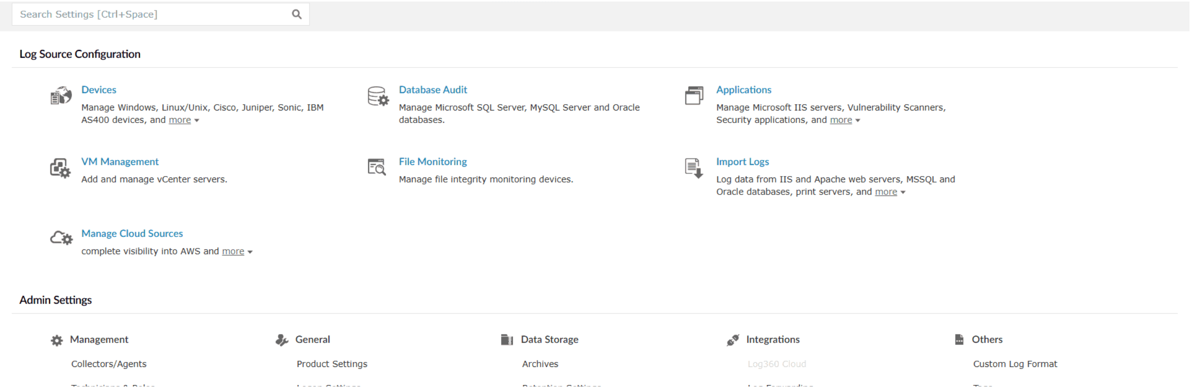
Overview

The SNMP Trap listener port management capability allows you to configure and control how SNMP traps are received from devices that are added for monitoring. This includes setting up trap destination ports, enabling or disabling the SNMP Trap listener ports, editing port values, and managing SNMP credentials for various protocol levels (V1, V2c, V3). This helps maintain secure and accurate log ingestion from SNMP-supported devices.

Configuring a device to send SNMP traps

> NOTE
>
> To configure a network device to send SNMP traps, ensure that SNMP is enabled in the product, and then enable traps in your network device.

1. In the product console, navigate to the Settings tab and click on Listener ports listed under System Settings as shown in the below image.



Search Settings [Ctrl+Space]

Log Source Configuration

Devices
Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more

Database Audit
Manage Microsoft SQL Server, MySQL Server and Oracle databases.

Applications
Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more

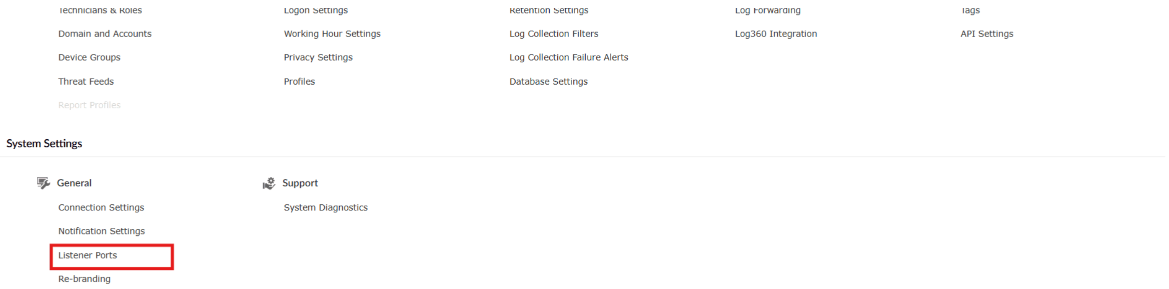
VM Management
Add and manage vCenter servers.

File Monitoring
Manage file integrity monitoring devices.

Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more

Manage Cloud Sources
complete visibility into AWS and more

Admin Settings



Technicians & Roles
Domain and Accounts
Device Groups
Threat Feeds
Report Profiles

Logon Settings
Working Hour Settings
Privacy Settings
Profiles

Retention Settings
Log Collection Filters
Log Collection Failure Alerts
Database Settings

Log Forwarding
Log360 Integration

Tags
API Settings

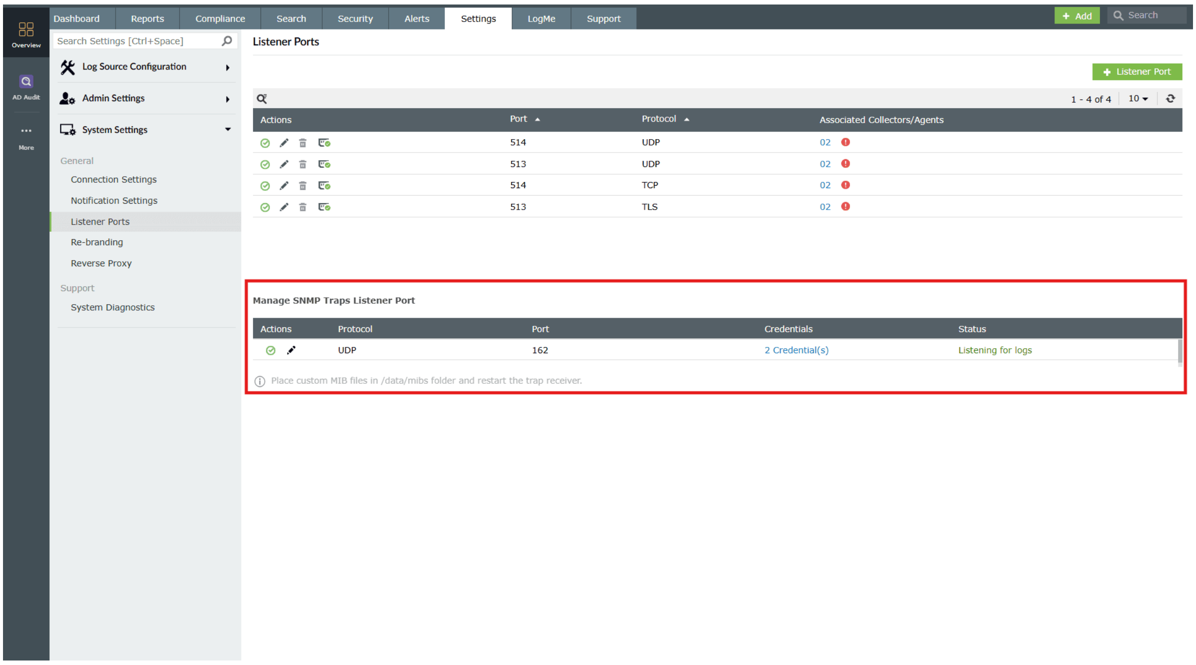
System Settings

General
Connection Settings
Notification Settings
Listener Ports
Re-branding

Support
System Diagnostics

Image 1: SNMP Traps listener ports configuration via the Settings tab

2. You will be taken to the Listener Ports segment. You can find the fields listed under Manage SNMP Traps Listener Port, as highlighted below.



Listener Ports

Actions	Port	Protocol	Associated Collectors/Agents
	514	UDP	02
	513	UDP	02
	514	TCP	02
	513	TLS	02

Manage SNMP Traps Listener Port

Actions	Protocol	Port	Credentials	Status
	UDP	162	2 Credential(s)	Listening for logs

Place custom MIB files in /data/mibs folder and restart the trap receiver.

Image 2: Managing SNMP Traps ports under the listener ports configuration

3. In your device settings configuration, set the trap destination host address to the IP address or the hostname of the corresponding product's server.

4. Set the trap destination port to 162 or to the SNMP port configured in the product—Log360, EventLog Analyzer, and Log360 Cloud.

5. Specify the SNMP credentials that are already configured.

6. Save the configuration.

> NOTE
>
> By default, the product's server listens to port 162 (UDP) for SNMP traps.

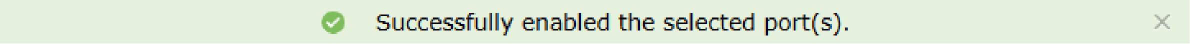
Manage SNMP Trap listener port

Manage SNMP Trap listener ports

Enable/disable SNMP Trap listener port

Enabling an SNMP Trap listener port

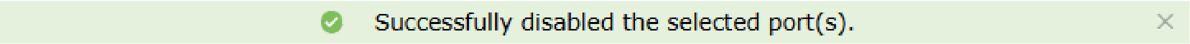
1. Click on the currently disabled icon ⊘ under the Actions column to enable the port.
2. As soon as you perform this action, the icon indicates that the port is now enabled ✓ and the below pop-up message appears briefly.



✓ Successfully enabled the selected port(s). ×

Disabling an SNMP Trap listener port

1. Click on the currently enabled icon ✓ under the Actions column to disable the port.
2. As soon as you perform this action, the icon indicates that the port is now disabled ⊘ and the below pop-up message appears briefly.

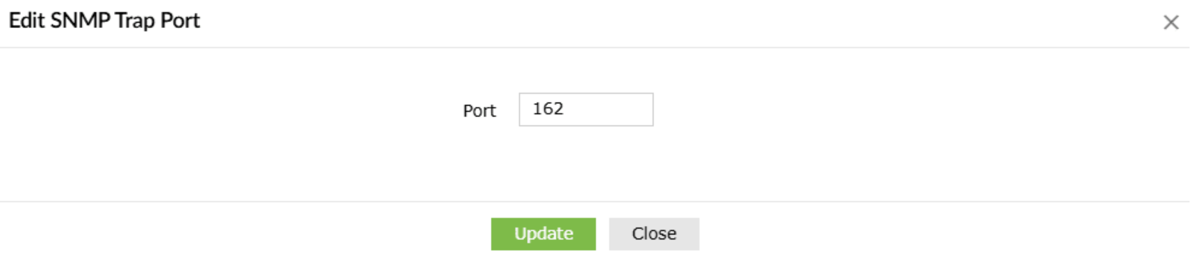


✓ Successfully disabled the selected port(s). ×

Edit SNMP Trap listener port

To edit the port using which Log360 listens to SNMP traps:

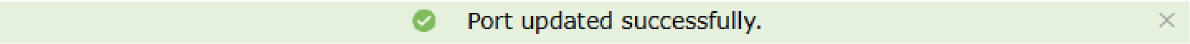
1. Click on the Edit icon under the Actions column to edit the respective SNMP Trap port. The Edit SNMP Trap listener Port pop-up appears as shown below.



Edit SNMP Trap Port

Port: 162

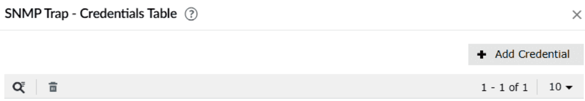
2. Enter the desired port number and click on Update.
3. Upon successfully enabling, the below pop-up appears. The edits are instantly made, and you can see the updated configuration in the console.



✓ Port updated successfully. ×

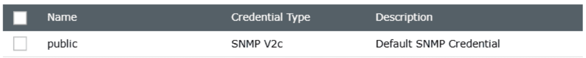
Updating credentials for SNMP Trap

1. Click on the Credentials button under the Credentials field. The SNMP Trap - Credentials Table pop-up appears.



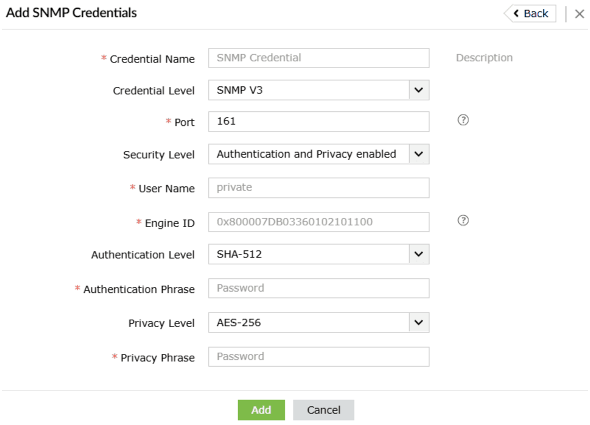
SNMP Trap - Credentials Table

1 - 1 of 1 | 10



□	Name	Credential Type	Description
□	public	SNMP V2c	Default SNMP Credential

2. Click on the Add Credential button to add a new SNMP credential. The Add SNMP Credentials pop-up appears as below.



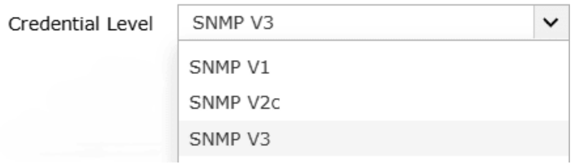
Add SNMP Credentials

* Credential Name	SNMP Credential	Description
Credential Level	SNMP V3	
* Port	161	ⓘ
Security Level	Authentication and Privacy enabled	
* User Name	private	
* Engine ID	0x800007DB03360102101100	ⓘ
Authentication Level	SHA-512	
* Authentication Phrase	Password	
Privacy Level	AES-256	
* Privacy Phrase	Password	

3. Fill in the required fields

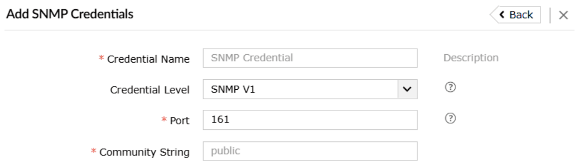
- Enter the Credential Name for SNMP Credential.
- Select the required Credential Level.
- Enter the desired Port number. This port will only be used by the workflow and syslog device discovery modules.

  There are two different cases based on the Credential Level you have chosen.



Credential Level: SNMP V3

Case 1: If the required Credential Level is chosen as either V1 or V2c

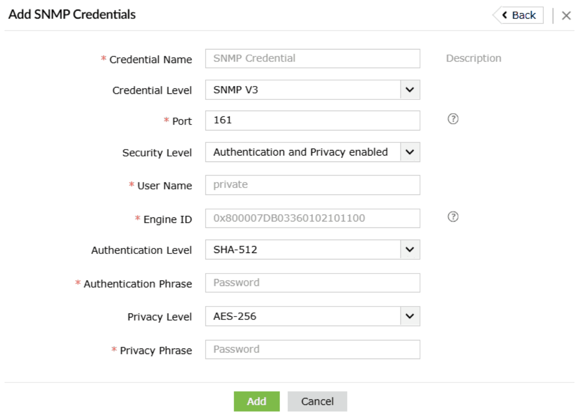


Add SNMP Credentials

* Credential Name	SNMP Credential	Description
Credential Level	SNMP V1	ⓘ
* Port	161	ⓘ
* Community String	public	

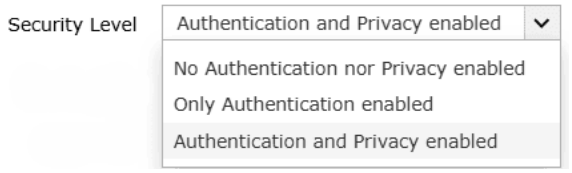
The SNMP V1/V2C will also require you to provide the Community String for SNMP Trap and discovery.

Case 2: If the required Credential Level is chosen as V3


Add SNMP Credentials

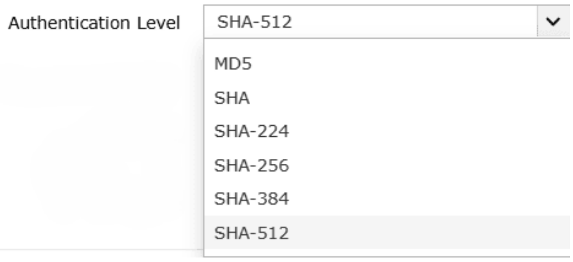
* Credential Name	SNMP Credential	Description
Credential Level	SNMP V3	
* Port	161	
Security Level	Authentication and Privacy enabled	
* User Name	private	
* Engine ID	0x800007DB03360102101100	
Authentication Level	SHA-512	
* Authentication Phrase	Password	
Privacy Level	AES-256	
* Privacy Phrase	Password	

- Choose a Security Level from the drop-down.

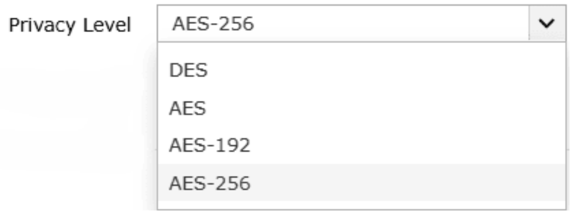

Security Level: Authentication and Privacy enabled

No Authentication nor Privacy enabled
Only Authentication enabled
Authentication and Privacy enabled

- Enter the User Name.
- Enter the Engine ID. This will be used for trap collection and sending traps in workflows.
- Select the SNMPV3 credential's Authentication Level.


Authentication Level: SHA-512

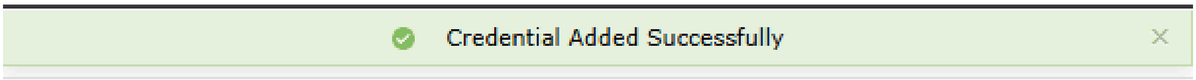
- Enter the Authentication Phrase for SNMPv3 credential.
- Select the SNMPV3 credential's Privacy Level.


Privacy Level: AES-256

- Enter Privacy Phrase for SNMPv3 credential.

4. After filling all the required fields, click on Add.

5. Upon successful completion of the action, the below pop-up appears.



Credential Added Successfully

ⓘ NOTE

When a device not added to the product's server starts sending SNMP traps to the product, it will automatically be listed under Other Devices in Settings > Configuration > Manage Devices. Additionally, it will be listed under General Applications as SNMP Trap Application.
The credentials added here can be used when discovering devices via Settings > Configuration > Manage Devices > Syslog Devices and credentials added while discovering devices can be used for SNMP trap collection.

Read also
This document covered how to configure SNMP Trap listener ports, enable or disable port access, and update SNMP credentials in Log360. For more on network device integration and log ingestion methods, refer to the following page:

- Configure listener ports

3.2.2. System Diagnostics

Last updated on: September 12, 2025

- System Info
- System Utilization
- Database Access
- System Resource Calculator
- Log Level Settings

Chapter 3.3 **Configurations**

3.3.1. Steps to configure external applications

Last updated on: September 12, 2025

Configuring ManageEngine Password Manager Pro

Here are the steps to configure Password Manager Pro.

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

Configuring ManageEngine OpManager

The following are the steps to configure ManageEngine OpManager.

1. Login to OpManager.
2. Navigate to Settings -> Notifications.
3. Click Add.
   Profile Type
   Select Syslog Profile and enter the following details.
    - Destination Host - EventLog Analyzer server name or IP address.
    - Destination Port - Any port that the EventLog Analyzer instance is listening to.
    - Severity and Facility must be the default values i.e. $severity and kernel.

   For EventLog Analyzer to parse logs from OpManager, the message variables in the syslog profile of OpManager should be entered in the following format:
   Mandatory message variables
    - ALARM_MESSAGE:$message
    - ALARM_ID:$alarmid
    - ALARM_CODE:$alarmid

   Other important message variables
    - ALARM_SOURCE:$displayName

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

4. Click Next.

Criteria

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

Device Selection

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

Schedule

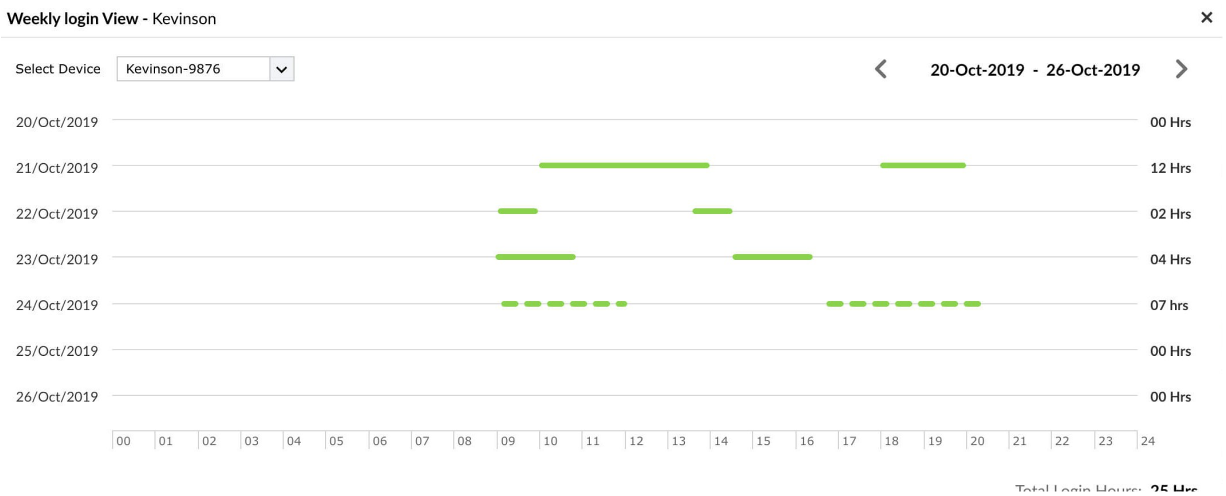
- You don't have to configure anything in this section. Click Next.

Preview

- Enter a profile name and click Save.

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

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

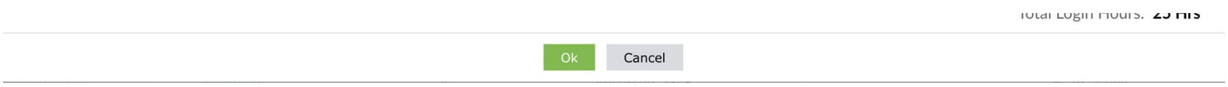


Weekly login View - Kevinson

Select Device: Kevinson-9876

20-Oct-2019 - 26-Oct-2019

Total Login Hours: 25 Hrs



Total Login Hours: 25 Hrs

3.3.2.1. Device Auto Allocation in Log360 | Overview

Last updated on: September 12, 2025

In this page

What is device auto allocation?

Device auto allocation is the process of automatically assigning the discovered Windows devices from workgroups and domains, to collectors. In case of an agent-based collection, the allocation happens through agents where policies with defined rules and collector load will define device mapping to the appropriate agent. And in the case of agent-less log collection method, direct allocation of device(s) to the native or local collector takes place. - Device allocation in Log360 is governed by user-defined policies called Auto Allocation Policies that specify the criteria like domain names, OU (Organizational Unit) filters, workgroups, and device limits. This auto allocation capability will help you streamline the onboarding of devices into a centralized monitoring system, reducing manual work and ensuring that every device in your organization's large network is monitored.

Key functionalities

- Device onboarding automation: Replaces manual device allocation by auto-assigning devices or scheduling runs, based on pre-defined policies. The allocation is performed either on the domain basis or workgroup.
- Granular control:
  - With the help of multiple policies, define allocation rules based on workgroups, OUs, set device count limits, include OU filter for domains and more, per agent or collector.
  - You can include or exclude OUs under specific domains depending upon your requirements.
  - Each policy maps to an agent/local native collector.
- Load balancing: To ensure even distribution and prevent congestion, devices will be automatically assigned to collectors with the least load.
- Failsafe conditions: Clear status is notified in case the policies are not applicable or if a collector's device limits are reached.

NOTE

If Auto Allocation is-

Disabled during execution: The device allocation stops immediately.

Enabled: The device allocation will start instantly and will be scheduled to run daily at 12 PM, thereafter.

1. Auto allocation

Process where the solution automatically assigns discovered Windows devices to collectors or agents based on predefined rules and configured criterion, eliminating the need for manual assignment.

2. Auto allocation policies

User-defined rules that decide how and where devices should be assigned based on criteria like domain, OU, or workgroup.

3. Collector or local native collector

A server or component that receives and processes logs from devices. In agent-less setups, the local native collector on the same machine handles the respective device's logs.

4. Agent

A specific software installed on a device with the purpose of collection and sending of log data to Log360. Used in agent-based auto allocation for more granular control.

Pre-requisites

Role-based access control

Only admins of the console can define, access, and modify the auto allocation policies.

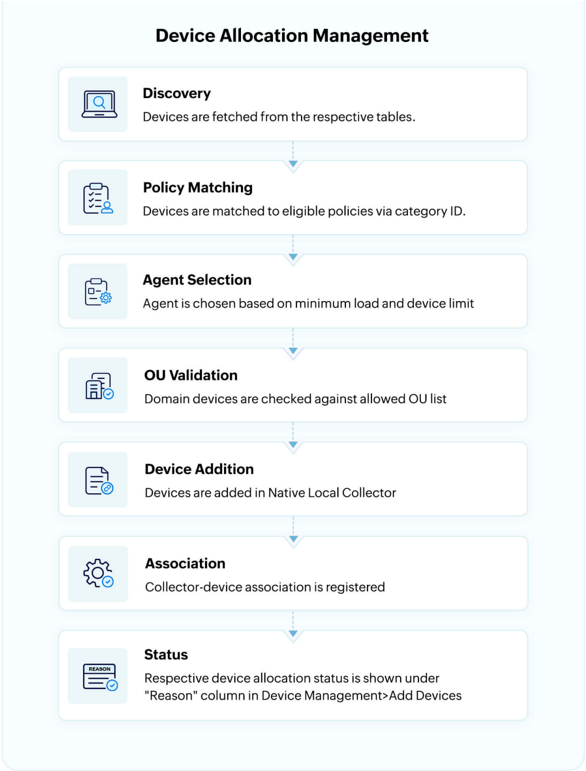
Supported devices

Windows devices

Domain or workgroup pre-requisites

- Ensure that the devices must be discovered in the device discovery process before the allocation.
- The devices to be auto-allocated must belong to a recognized domain or workgroup.
- The said domain must also be configured in the product console with the available OUs for policy mapping.
- For domain-based policies, it must be ensured that the OU structure or hierarchy is synchronized properly.

Allocation flow



Device Allocation Management

Discovery
Devices are fetched from the respective tables.

Policy Matching
Devices are matched to eligible policies via category ID.

Agent Selection
Agent is chosen based on minimum load and device limit

OU Validation
Domain devices are checked against allowed OU list

Device Addition
Devices are added in Native Local Collector

Association
Collector-device association is registered

Status
Respective device allocation status is shown under "Reason" column in Device Management>Add Devices

NOTE

- In the case of an agent-less device collection, the "Agent selection" step is omitted in the workflow of device auto allocation and the "OU validation" step is carried out after which the device(s) will be automatically allocated to the native/local collector.
- Only one agent/collector can be mapped per policy.
- In case an agent is deleted, the agent is also dynamically removed from all the existing internal mappings during task execution.

Use cases

1. Dynamic scaling of SIEM infrastructure across business units

Use case

Regional divisions of a global company are operated with distributed agents handling logs from the different locations/business units.

With Device Auto Allocation

Devices can be routed automatically in each location or business unit to their respective local collector or agent with collector load-balancing and OU-based filters. This will also help divisional teams ensure that every endpoint is allocated promptly, efficient fault isolation, and region-specific threat visibility.

2. Zero touch onboarding for compliance-ready log collection

Use case

In large enterprises with thousands of endpoints across their AD domains and workgroups, there is a higher scope for human error when each and every device from all those endpoints is to be accounted for in the SIEM (Security Information and Event Management) solution for audit and compliance purposes like HIPAA, PCI-DSS, GDPR and more.

With Device Auto Allocation

The Auto Allocation feature ensures that as soon as a device is discovered, it is assigned to an agent/collector and that no device goes unmonitored. With this, human error is eliminated and onboarding is sped up, while ensuring complete audit trails right from Day 1.

> ⓘ MITRE ATT&CK framework
>
> Device Auto Allocation can help you eliminate onboarding blind spots that are commonly exploited by attackers during their initial entry phase. Can mitigate T1133 (External Remote Services) Exploitation

Read also

This document elaborated the configuration, prerequisites, and functionality of the Device Auto Allocation feature in Log360. For related features and extended device management capabilities, refer to the articles below:

- Auto Allocation Configuration
- Auto Allocation Policy Configuration
- Check Unallocated Device(s) status
- Sync Settings

3.3.2.2. Configuring auto allocation

Last updated on: September 12, 2025

In this page

Overview

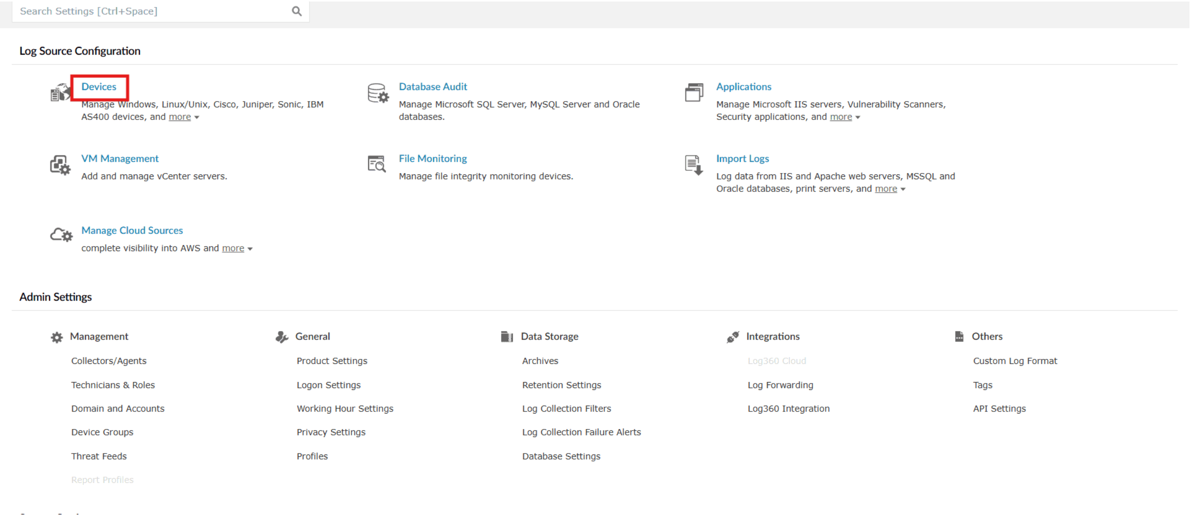
The auto allocation capability must be manually enabled to begin assigning discovered Windows devices to the appropriate collectors. Once enabled, the system automatically evaluates devices against configured policies and performs scheduled allocations. This section guides you through enabling or disabling the feature and explains what happens when it's turned on or off.

Configuring auto allocation (enable/disable)

Enabling auto allocation

> NOTE
>
> By default, the auto allocation feature is in a disabled state. It must be manually enabled in order to make use of its functionality.

1. In the product console, navigate to the Settings tab and click on Devices.



Search Settings [Ctrl+Space]

Log Source Configuration

Devices
Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more ▾

Database Audit
Manage Microsoft SQL Server, MySQL Server and Oracle databases.

Applications
Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more ▾

VM Management
Add and manage vCenter servers.

File Monitoring
Manage file integrity monitoring devices.

Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more ▾

Manage Cloud Sources
complete visibility into AWS and more ▾

Admin Settings

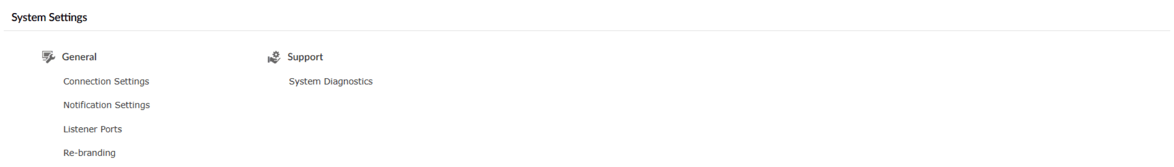
Management
- Collectors/Agents
- Technicians & Roles
- Domain and Accounts
- Device Groups
- Threat Feeds
- Report Profiles

General
- Product Settings
- Logon Settings
- Working Hour Settings
- Privacy Settings
- Profiles

Data Storage
- Archives
- Retention Settings
- Log Collection Filters
- Log Collection Failure Alerts
- Database Settings

Integrations
- Log360 Cloud
- Log Forwarding
- Log360 Integration

Others
- Custom Log Format
- Tags
- API Settings



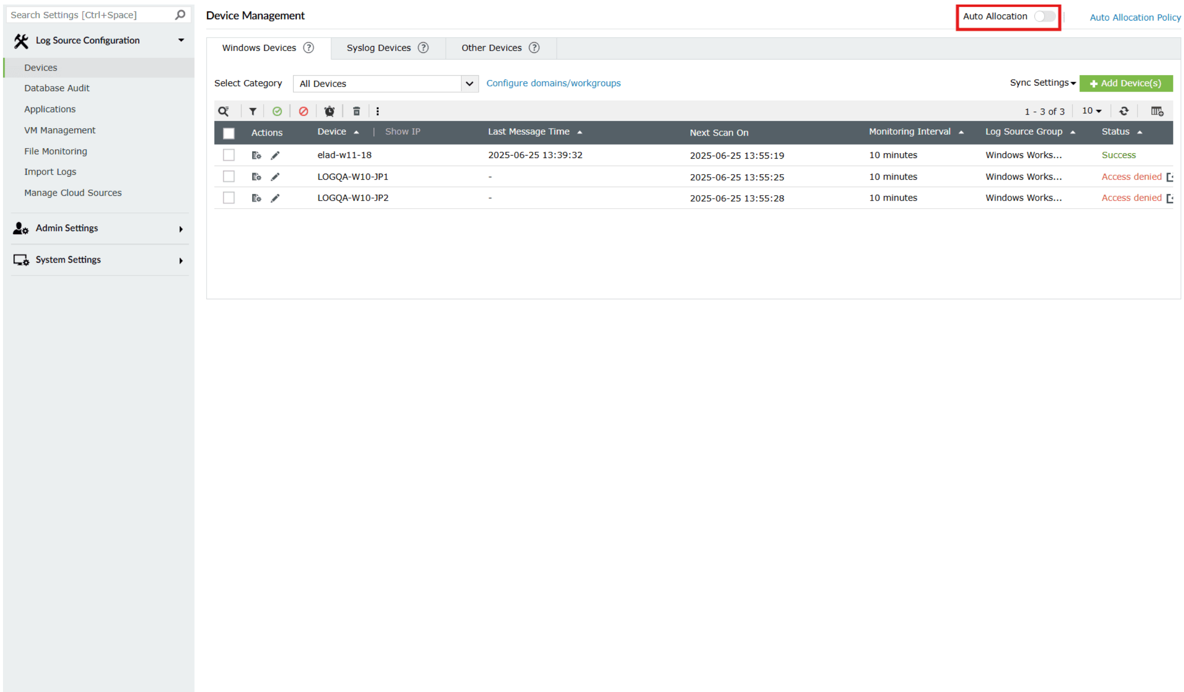
System Settings

General
- Connection Settings
- Notification Settings
- Listener Ports
- Re-branding

Support
- System Diagnostics

Image 1: Device settings

2. You will be taken to the Device Management module. On the right-hand side, you can find the toggle to enable/disable Auto Allocation. Click on the toggle to enable this function.



Device Management

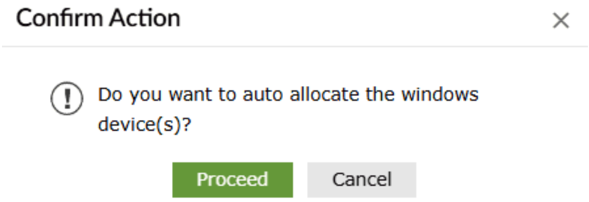
Auto Allocation | Auto Allocation Policy

Select Category: All Devices | Configure domains/workgroups

□	Actions	Device | Show IP	Last Message Time	Next Scan On	Monitoring Interval	Log Source Group	Status
□		elad-w11-18	2025-06-25 13:39:32	2025-06-25 13:55:19	10 minutes	Windows Works...	Success
□		LOGQA-W10-JP1	-	2025-06-25 13:55:25	10 minutes	Windows Works...	Access denied
□		LOGQA-W10-JP2	-	2025-06-25 13:55:28	10 minutes	Windows Works...	Access denied

Image 2: Auto allocation in the product console

3. After you click on the toggle to enable auto allocation, a Confirm Action pop-up is displayed to enable auto allocation in Windows. Click on Proceed.

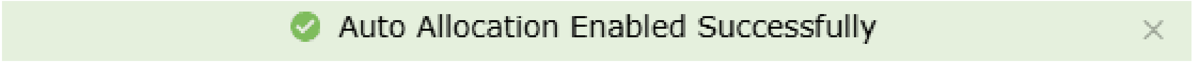


Confirm Action

Do you want to auto allocate the windows device(s)?

Proceed | Cancel

4. As soon as you select proceed, the toggle turns from Auto Allocation ○ to Auto Allocation ● and the below pop-up appears briefly as a confirmation of the successful changes made.



Auto Allocation Enabled Successfully

5. Now, auto allocation is enabled, and the product starts allocating devices immediately and will perform a daily allocation check at the scheduled time.

What happens after enabling auto allocation?

- Discovered devices from Workgroups and Domains will be evaluated against all the currently active Auto Allocation Policies.
- The system:
  - Matches devices based on policy rules (OU, domain, workgroup)
  - Selects the agent/collector with the lowest load at that moment, within the defined limits.
  - Allocates the device(s) and logs its status in the Device Management > Add Devices popup under the Reason column.

Disabling auto allocation

1. Follow the same steps- Step 1 and Step 2 as Enabling auto allocation to locate the toggle. Click on the (currently enabled) toggle.
2. As soon as you perform the above action, the toggle turns from Auto Allocation to and the below pop-up appears.

Auto Allocation Disabled Successfully

Read also

This document explained how to enable or disable the device auto allocation feature and what happens after activation. For further information on managing device assignments and policies, refer to the articles below:

- Configuring auto allocation policies
- Check unallocated device(s) status
- Sync settings

3.3.2.3. Configuring auto allocation policies

Last updated on: September 12, 2025

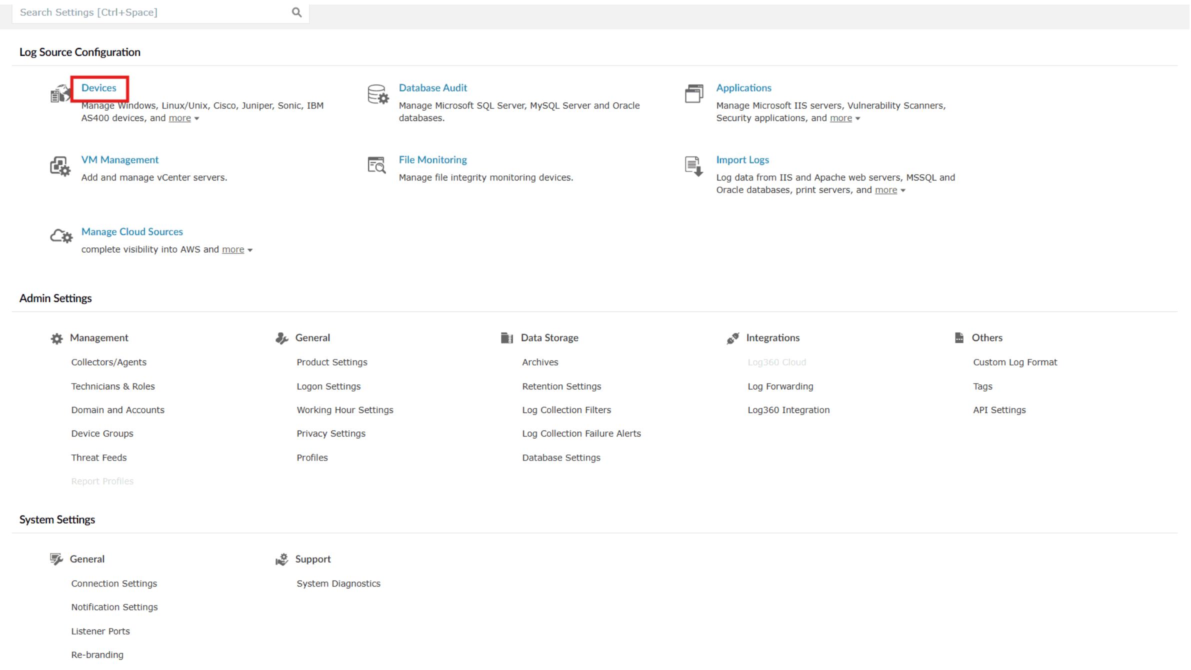
In this page

Overview

Auto Allocation Policies define how discovered devices are assigned to collectors in the product, based on criteria like domains, workgroups, and Organizational Units (OUs). This section explains how to manage these policies—enabling or disabling them, editing policy rules, and instantly triggering allocation—so that devices are automatically and efficiently onboarded into the monitoring system.

Configuring auto allocation policies

1. Navigate to the Settings tab and click on Devices.



Search Settings [Ctrl+Space]

Log Source Configuration

Devices
Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more

Database Audit
Manage Microsoft SQL Server, MySQL Server and Oracle databases.

Applications
Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more

VM Management
Add and manage vCenter servers.

File Monitoring
Manage file integrity monitoring devices.

Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more

Manage Cloud Sources
complete visibility into AWS and more

Admin Settings

Management
Collectors/Agents
Technicians & Roles
Domain and Accounts
Device Groups
Threat Feeds
Report Profiles

General
Product Settings
Logon Settings
Working Hour Settings
Privacy Settings
Profiles

Data Storage
Archives
Retention Settings
Log Collection Filters
Log Collection Failure Alerts
Database Settings

Integrations
Log360 Cloud
Log Forwarding
Log360 Integration

Others
Custom Log Format
Tags
API Settings

System Settings

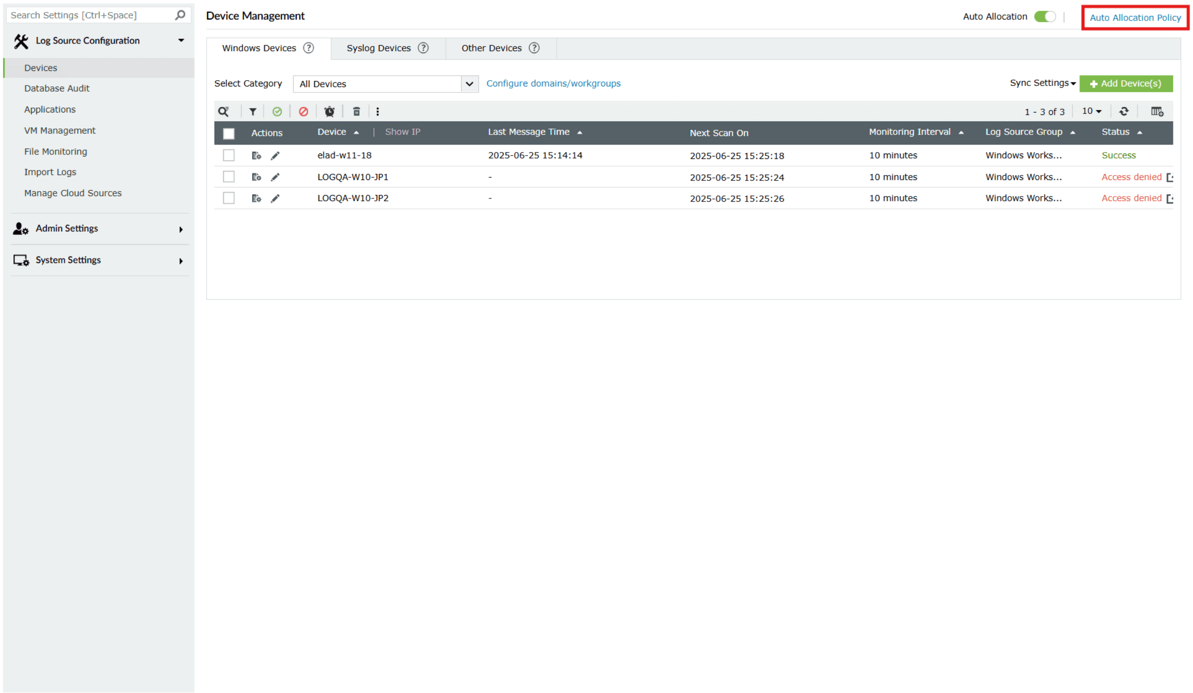
General
Connection Settings
Notification Settings
Listener Ports
Re-branding

Support
System Diagnostics

Image 1: Device settings in the product console

Image 1: Device settings in the product console

2. You will be taken to the Device Management module. On the right-hand side, you will find Auto Allocation Policy as shown below. Click on it.

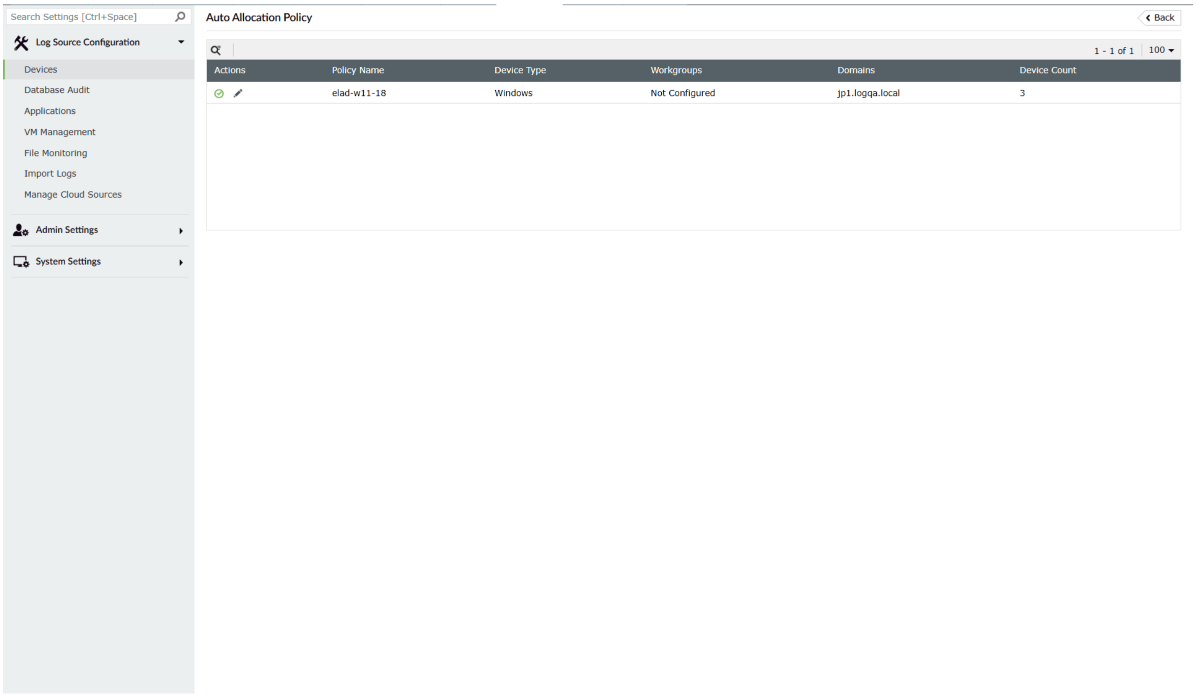


Actions	Device	Last Message Time	Next Scan On	Monitoring Interval	Log Source Group	Status
	elad-w11-18	2025-06-25 15:14:14	2025-06-25 15:25:18	10 minutes	Windows Works...	Success
	LOGQA-W10-JP1	-	2025-06-25 15:25:24	10 minutes	Windows Works...	Access denied
	LOGQA-W10-JP2	-	2025-06-25 15:25:26	10 minutes	Windows Works...	Access denied

Image 2: Auto allocation policy in the product console

3. You will be taken to the list of all policies. Here, you can:

- Check the status of the policies and/or enable/disable the policies.
- Edit a policy.
- You can trigger auto allocation for all policies at any time. (Only when the auto allocation feature is in an enabled state.)



Actions	Policy Name	Device Type	Workgroups	Domains	Device Count
✓	elad-w11-18	Windows	Not Configured	jp1.logqa.local	3

Image 3: Device auto allocation policy in the product console

> ⓘ NOTE
>
> By default, the auto allocation policy is configured for the localhost server.

Enabling/disabling a policy

Enabling a policy

1. Click on the disabled icon ⊘ under the Actions column to enable the policy.
2. As soon as you perform this action, the icon indicates that the policy is now enabled ✓ and the below pop-up message appears briefly.

✓ Auto Allocation Policy Enabled Successfully ×

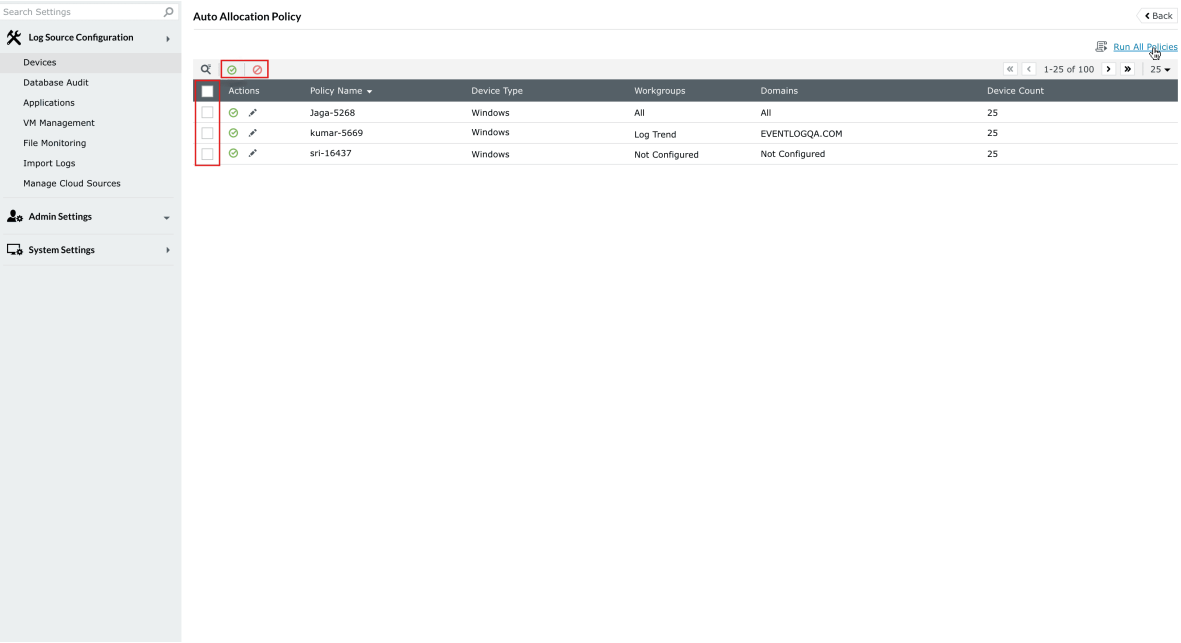
Disabling a policy

1. Click on the enabled icon ✓ under the Actions column to disable the policy.
2. As soon as you perform this action, the icon indicates that the policy is now disabled ⊘ and the below pop-up message appears briefly.

✓ Auto Allocation Policy Disabled Successfully ×

Enable/Disable multiple policies at once

1. Click on the empty checkbox(es) in the first column in order to select the respective policies.
2. Click on the Enable/Disable icons in the ribbon above the rules list.



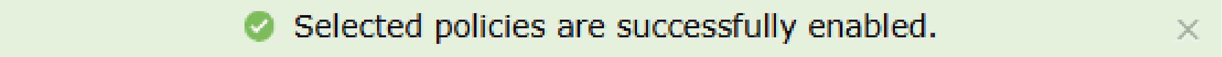
Auto Allocation Policy

□	Actions	Policy Name	Device Type	Workgroups	Domains	Device Count
□	✓ ✎	Jaga-5268	Windows	All	All	25
□	✓ ✎	kumar-5669	Windows	Log Trend	EVENTLOGQA.COM	25
□	✓ ✎	sri-16437	Windows	Not Configured	Not Configured	25

Image 4: Enable/Disable multiple policies at once

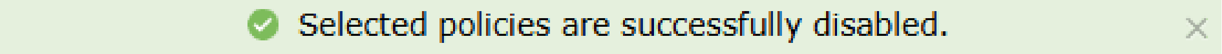
3. Upon successful completion of the action, the below pop-up appears.

When enabled successfully:



✓ Selected policies are successfully enabled. ×

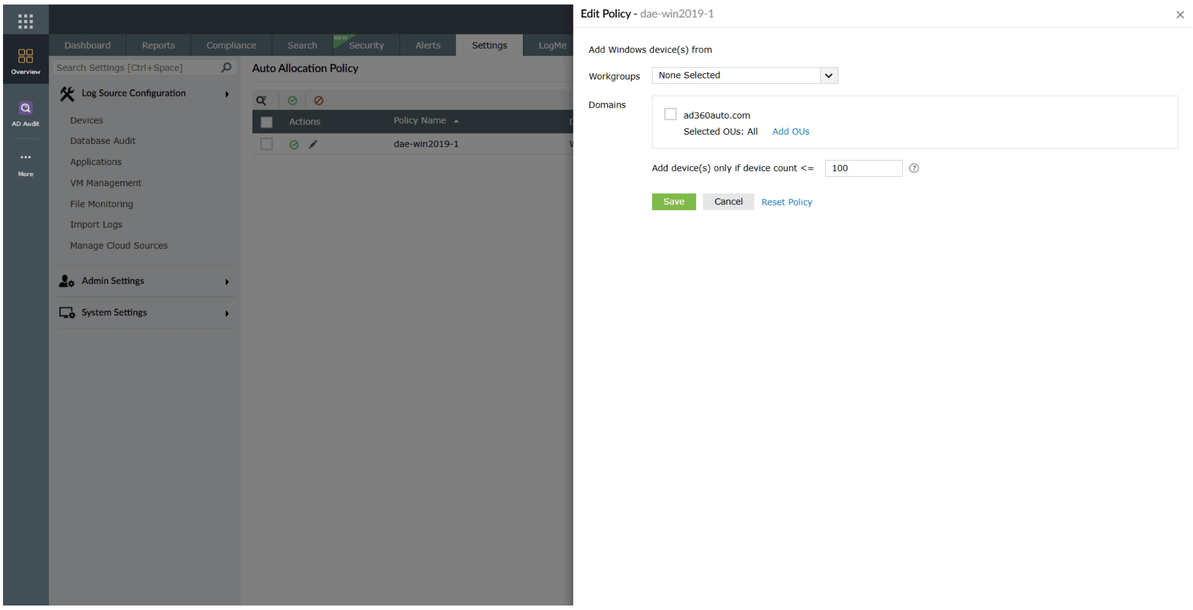
When disabled successfully:



✓ Selected policies are successfully disabled. ×

Edit a policy

1. To edit a policy, click on the Edit icon ✎ under the Actions column. A slider appears that includes the fields for editing the policy.



Edit Policy - dae-win2019-1 ×

Add Windows device(s) from

Workgroups: None Selected

Domains: ☐ ad360auto.com
Selected OUs: All Add OUs

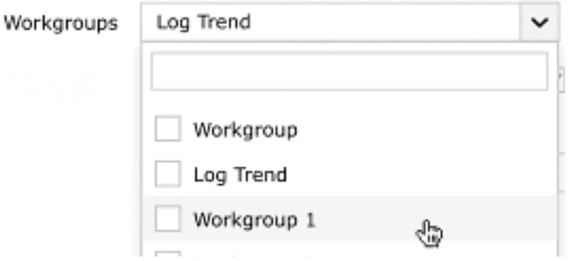
Add device(s) only if device count <= 100

Save Cancel Reset Policy

Image 5: Editing an auto allocation policy

2. Fill out the fields according to your requirements.

- Workgroups: You can select the workgroup to add devices from those workgroups only.

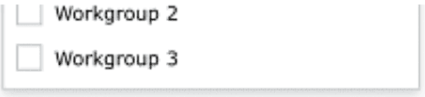


Workgroups: Log Trend

☐ Workgroup

☐ Log Trend

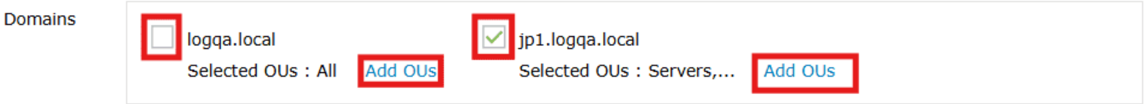
☐ Workgroup 1



□ Workgroup 2

□ Workgroup 3

- Domains: Add devices only from selected OUs (Organizational Units) in the selected domains. Use the checkbox to select or deselect the domains to add devices.

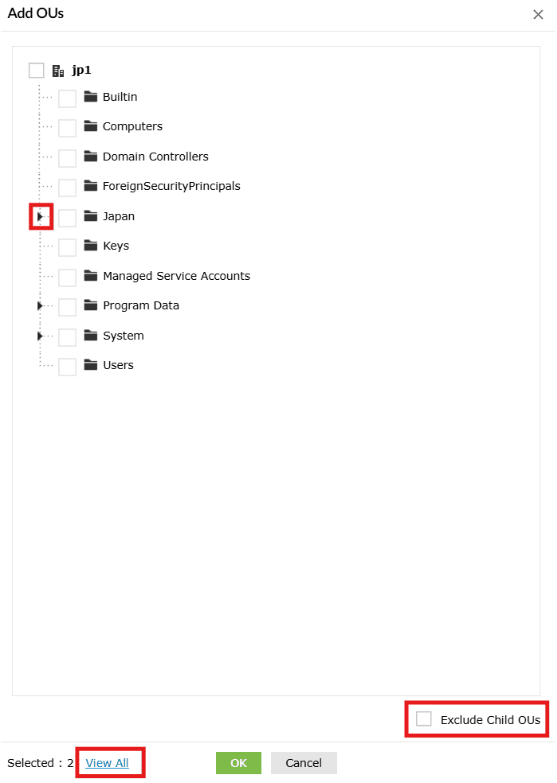


Domains

□ logqa.local
Selected OUs : All

☑ jp1.logqa.local
Selected OUs : Servers,...

  - Click Add OUs to add devices by filter the selected OUs.



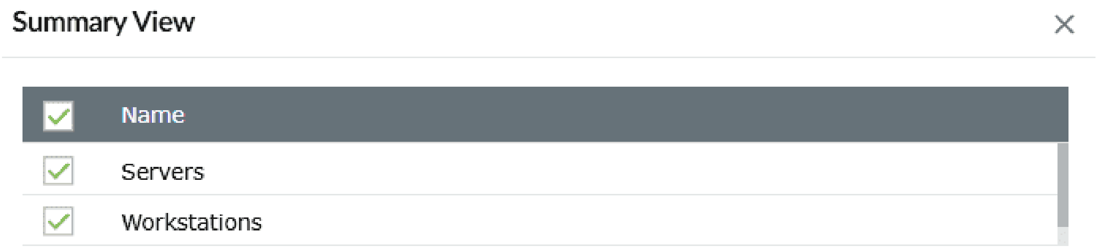
Add OUs

□ jp1
- □ Builtin
- □ Computers
- □ Domain Controllers
- □ ForeignSecurityPrincipals
- □ Japan
- □ Keys
- □ Managed Service Accounts
- □ Program Data
- □ System
- □ Users

□ Exclude Child OUs

Selected : 2

    - Click on the button to expand the OUs that include sub-folder(s).
    - Use Exclude Child OUs option to select parent OUs only.
    - Use View All button to see the selected OUs in Summary View



Summary View

☑	Name
☑	Servers
☑	Workstations

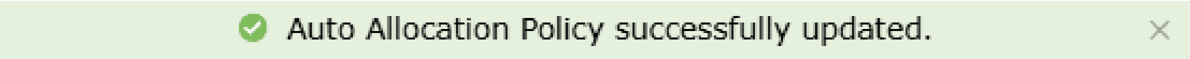
    - Click OK button to finalize the selected OUs.

  - Add Device(s) only if device count <= :
    - Device count must be between 1 & 100

  - Device count also includes Non-Windows Devices

> ⓘ NOTE
>
> The specified device count limit applies to only the associated devices with a speciifc collector.

3. Click on the Save button after you have made all the necessary changes.
4. Upon successful completion of the action, the below pop-up appears.



✓ Auto Allocation Policy successfully updated. ×

Trigger auto allocation manually

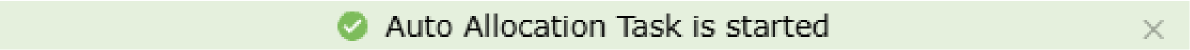
This function allows you to run the device allocation process instantly. This is useful when any changes have been made to the allocation policies and you don't want to wait for the next scheduled run. This, in turn, ensures that the policy updates take immediate effect.

Steps to trigger auto allocation manually

1. In the Auto Allocation Policy module itself, click on the Run All Policies button to allocate devices as per all policies immediately.

> ⓘ NOTE
>
> This option will not be available unless auto allocation is enabled.

2. As soon as you click on it, the below pop-up appears, indicating the instant start of a new auto allocation run with the updated policy.



✓ Auto Allocation Task is started ×

Read also

This document covered how to configure and manage auto allocation policies in the product. For more related functionalities, refer to the following articles:

- Check unallocated device(s) status
- Sync settings

3.3.2.4. Check unallocated device(s) status

Last updated on: September 12, 2025

In this page

Overview

This section guides you through accessing the unallocated device(s) list, understanding the reasons for unallocation, and taking corrective action to ensure full monitoring coverage.

Check unallocated device status

To view devices that couldn't be assigned through auto allocation, you can check the status of unallocated devices and gain insights as to why certain devices remain unallocated and take corrective action, if needed.

Steps to check status of unallocated device(s)

1. Navigate to the Settings tab and click on Devices.

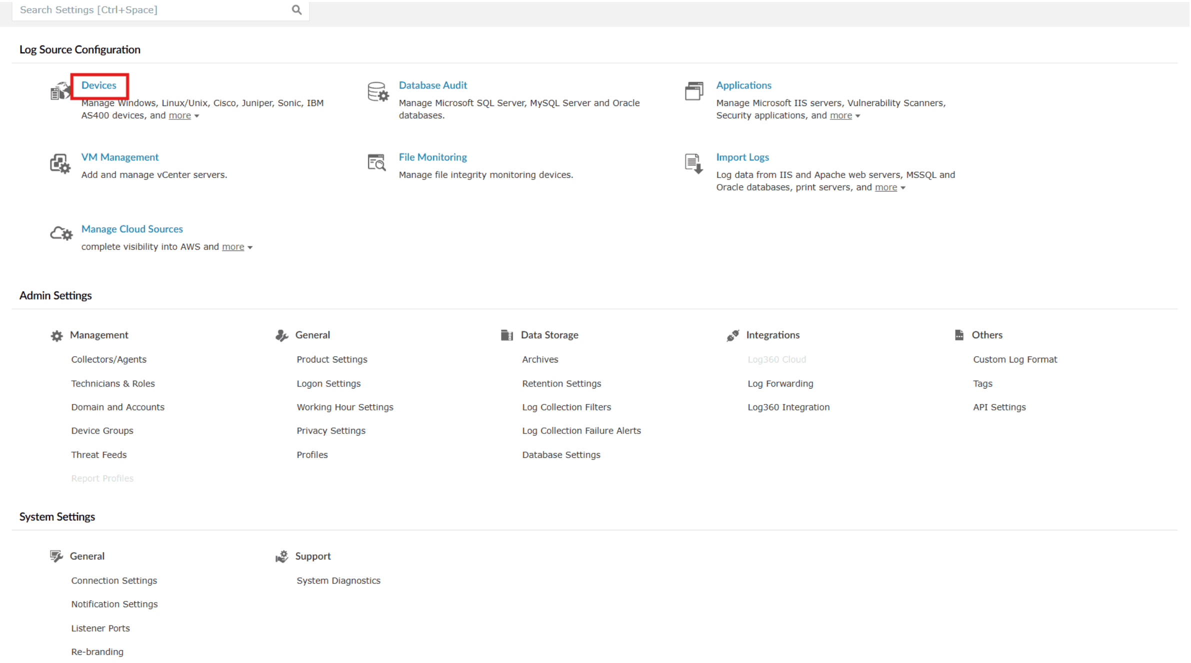
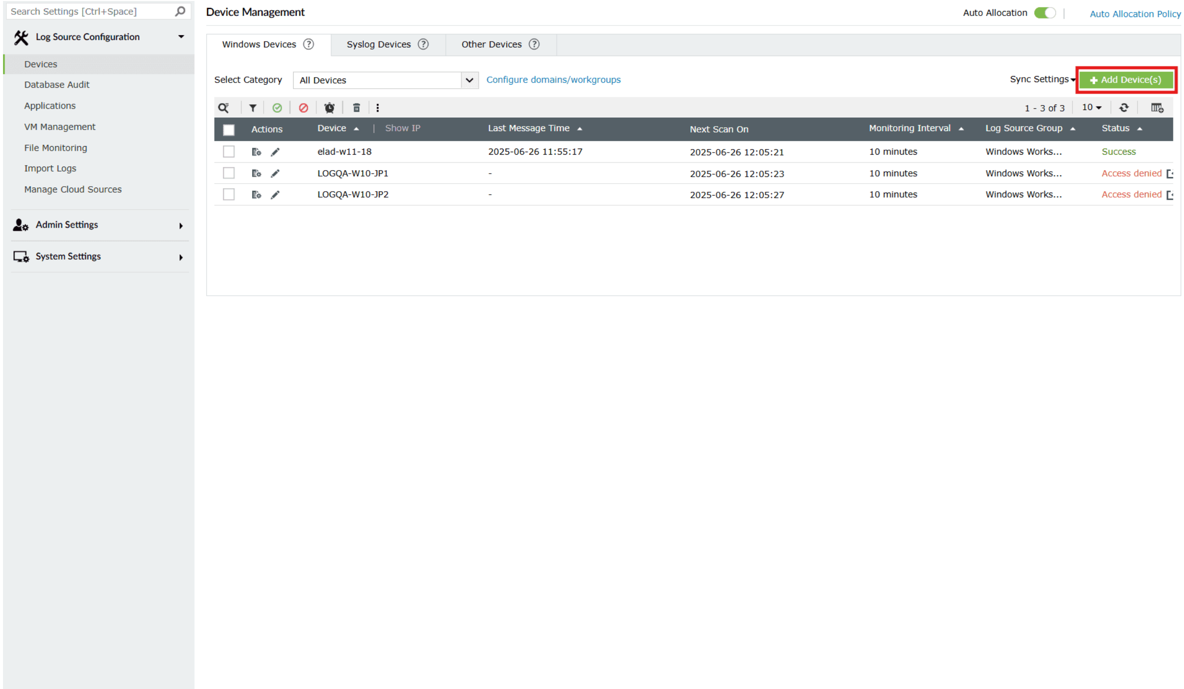


Image 1: Device settings in the product console

2. You will be taken to the Device Management module. Click on the Add Device(s) button to check the status of unallocated devices.

NOTE

Status will be shown only when the auto allocation feature is in an enabled state.



Device Management

Auto Allocation | Auto Allocation Policy

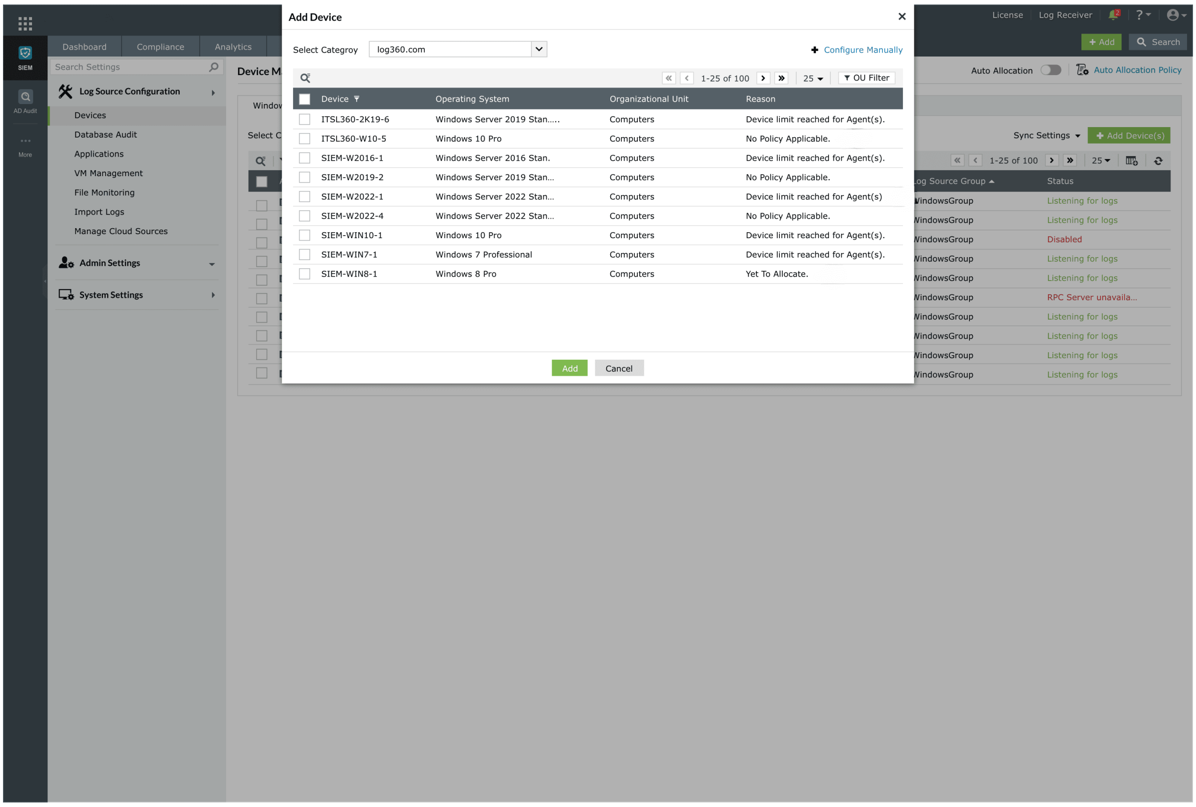
Select Category: All Devices | Configure domains/workgroups

1 - 3 of 3 | 10

Actions	Device | Show IP	Last Message Time	Next Scan On	Monitoring Interval	Log Source Group	Status
	elad-w11-18	2025-06-26 11:55:17	2025-06-26 12:05:21	10 minutes	Windows Works...	Success
	LOGQA-W10-JP1	-	2025-06-26 12:05:23	10 minutes	Windows Works...	Access denied
	LOGQA-W10-JP2	-	2025-06-26 12:05:27	10 minutes	Windows Works...	Access denied

Image 2: Device allocation settings in the product console

3. A pop-up box appears along with a list of the Unallocated Device(s), their Operating System, the Organizational Unit they belong to, and the Reason for being unallocated.



Add Device

Select Categroy: log360.com | ✚ Configure Manually

1-25 of 100 | 25 | OU Filter

Device	Operating System	Organizational Unit	Reason
ITSL360-2K19-6	Windows Server 2019 Stan.....	Computers	Device limit reached for Agent(s).
ITSL360-W10-5	Windows 10 Pro	Computers	No Policy Applicable.
SIEM-W2016-1	Windows Server 2016 Stan.	Computers	Device limit reached for Agent(s).
SIEM-W2019-2	Windows Server 2019 Stan...	Computers	No Policy Applicable.
SIEM-W2022-1	Windows Server 2022 Stan...	Computers	Device limit reached for Agent(s)
SIEM-W2022-4	Windows Server 2022 Stan...	Computers	No Policy Applicable.
SIEM-WIN10-1	Windows 10 Pro	Computers	Device limit reached for Agent(s).
SIEM-WIN7-1	Windows 7 Professional	Computers	Device limit reached for Agent(s).
SIEM-WIN8-1	Windows 8 Pro	Computers	Yet To Allocate.

Add | Cancel

Image 3: Device auto allocation in the product console

Hover the mouse pointer over the reason you would like to read completely, and a tool-tip highlighting the full version of the reason appears. There are three different types of status that could be listed under the possible reason(s) for the unallocation as listed below:

- No Policy Applicable: The device does not match the criteria of the policy with respect to the selected domain, OU (Organizational Unit) container or the workgroup in the policy.
- Device limit reached for Agent(s): The Auto Allocation Policy's device count limit has been reached.
- Yet to Allocate: Device is yet to be allocated in the upcoming schedule.

Read also

This document explained how to check the status of devices that were not allocated through auto allocation. For more details on related features, see the articles below:

- Sync settings

3.3.2.5. Sync settings

Last updated on: September 12, 2025

In this page

Overview

Log360 allows two-way synchronization of device data with its identity threat detection and response component, ADAudit Plus. This section explains how to enable or disable the addition sync settings, helping you control whether devices are synced from ADAudit Plus to Log360 and vice versa, based on your configuration needs.

> NOTE
>
> Device Auto Allocation is supported only for Windows instances and not for Linux environments.

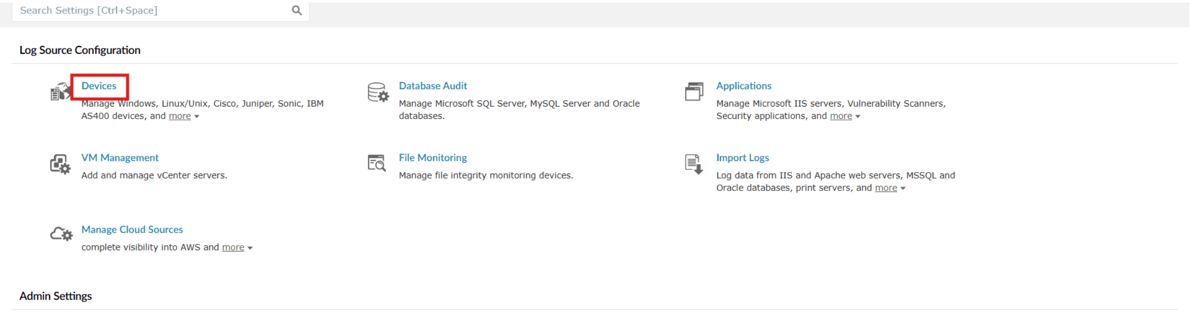
Enable/disable sync settings

> NOTE:
>
> This function is available only to the users who have integrated their ADAudit Plus to their Log360 console.

This settings will help you control the regular synchronization of device(s) data between ADAudit Plus and Log360.

Steps to enable device addition sync settings

1. In Log360 console, navigate to the Settings tab and click on Devices.



Log Source Configuration

Devices
Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more ▾

Database Audit
Manage Microsoft SQL Server, MySQL Server and Oracle databases.

Applications
Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more ▾

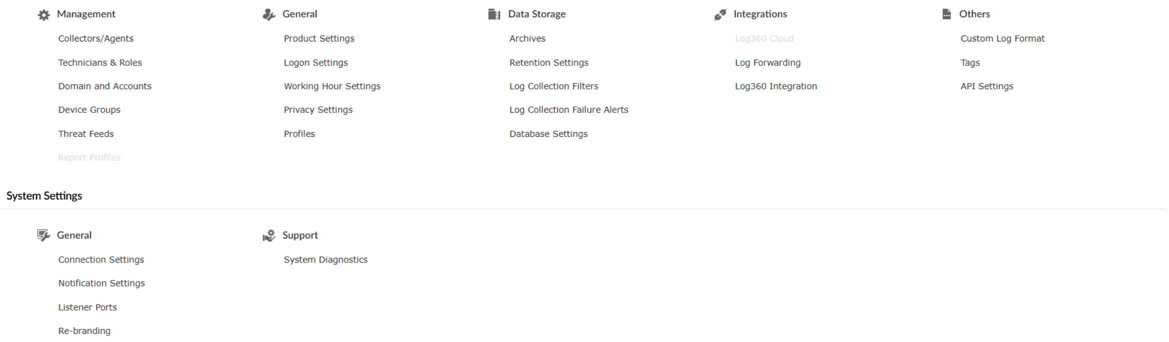
VM Management
Add and manage vCenter servers.

File Monitoring
Manage file integrity monitoring devices.

Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more ▾

Manage Cloud Sources
complete visibility into AWS and more ▾

Admin Settings



Management
- Collectors/Agents
- Technicians & Roles
- Domain and Accounts
- Device Groups
- Threat Feeds
- Report Profiles

General
- Product Settings
- Logon Settings
- Working Hour Settings
- Privacy Settings
- Profiles

Data Storage
- Archives
- Retention Settings
- Log Collection Filters
- Log Collection Failure Alerts
- Database Settings

Integrations
- Log360 Cloud
- Log Forwarding
- Log360 Integration

Others
- Custom Log Format
- Tags
- API Settings

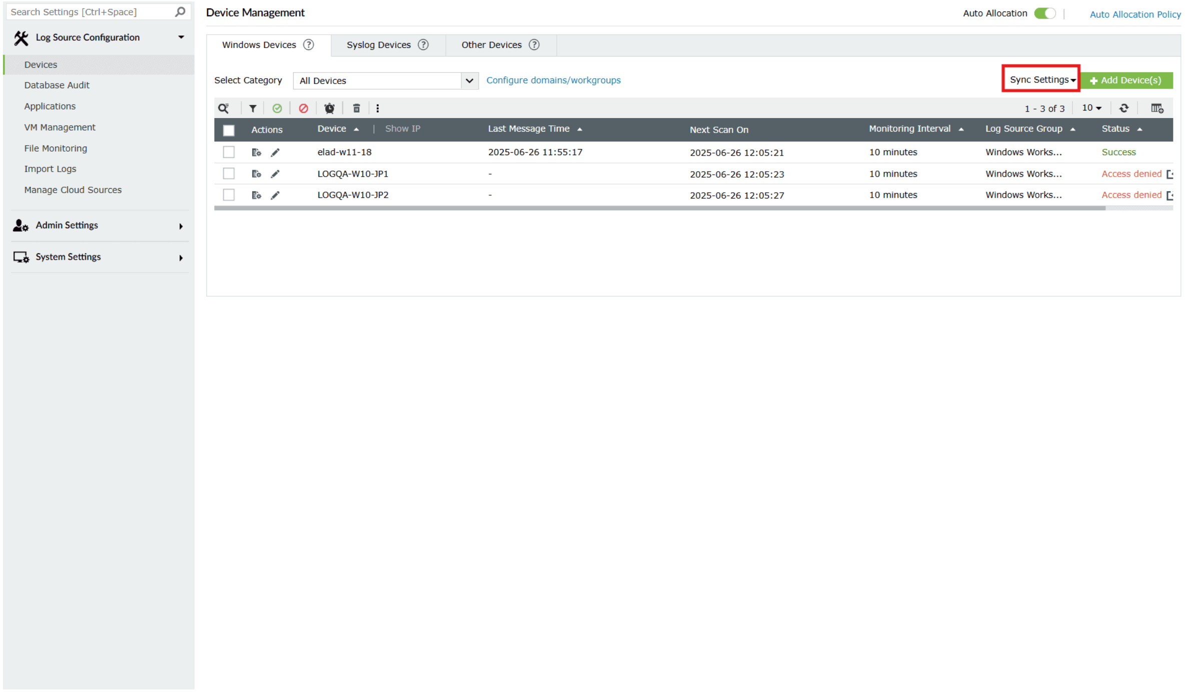
System Settings

General
- Connection Settings
- Notification Settings
- Listener Ports
- Re-branding

Support
- System Diagnostics

Image 1: Device auto allocation

2. You will be taken to the Device Management module. Click on the Sync Settings button.



Device Management

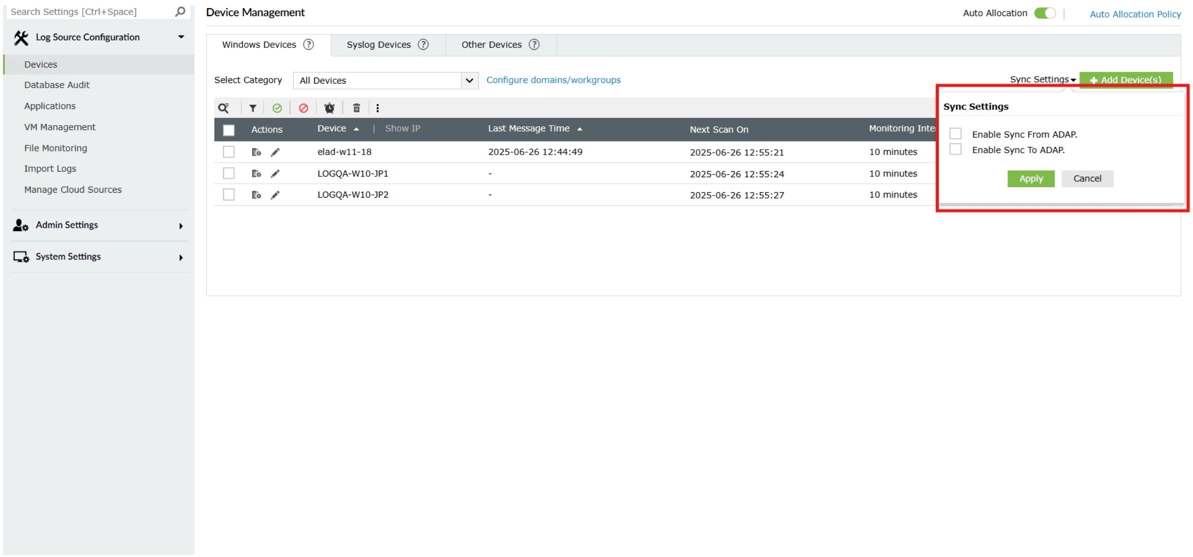
Auto Allocation | Auto Allocation Policy

Select Category: All Devices — Configure domains/workgroups

□	Actions	Device | Show IP	Last Message Time	Next Scan On	Monitoring Interval	Log Source Group	Status
□		elad-w11-18	2025-06-26 11:55:17	2025-06-26 12:05:21	10 minutes	Windows Works...	Success
□		LOGQA-W10-JP1	-	2025-06-26 12:05:23	10 minutes	Windows Works...	Access denied
□		LOGQA-W10-JP2	-	2025-06-26 12:05:27	10 minutes	Windows Works...	Access denied

Image 2: Sync settings in device allocation in the product console

3. The Sync Settings popup will appear like the below.



Device Management

Auto Allocation | Auto Allocation Policy

Select Category: All Devices — Configure domains/workgroups

□	Actions	Device | Show IP	Last Message Time	Next Scan On	Monitoring Inte
□		elad-w11-18	2025-06-26 12:44:49	2025-06-26 12:55:21	10 minutes
□		LOGQA-W10-JP1	-	2025-06-26 12:55:24	10 minutes
□		LOGQA-W10-JP2	-	2025-06-26 12:55:27	10 minutes

Sync Settings

□ Enable Sync From ADAP.

□ Enable Sync To ADAP.

Image 3: ADAudit Plus Sync settings in device allocation in the product console

4. Click on:

   - Enable Sync From ADAudit Plus checkbox: To sync the devices from ADAudit Plus to Log360. If it's not selected, then the device will not sync to Log360 which is integrated with ADAudit Plus.
   - Enable Sync To ADAudit Plus checkbox: To sync the devices from Log360 to ADAudit Plus. If it's not selected, then the device will not sync to ADAudit Plus which is integrated with Log360.

   In case you wish to enable the sync, ensure that the checkbox is ticked. In case you wish the sync to be disabled, ensure that the checkbox is empty.

5. Once you have made the necessary settings, click on the Apply button to save your configuration.
6. Upon successful completion of the action, the below pop-up appears.

✓ Sync Settings updated successfully. ×

NOTE

Only Device addition will sync inbetween products. enable and disable actions will not sync. On Deletion, it will ask in deletion popup weather to sync the delete to other product or not. For more information about deletion sync refer this.

Read also

This document explained how to configure sync settings between the product console and ADAudit Plus. For related configuration and device management topics, refer to:

- What is Device auto allocation?
- Configuring auto allocation

Chapter 4.1.1 **Security Dashboard**

4.1.1.1. Security dashboard

Last updated on: September 12, 2025

In this page

Overview

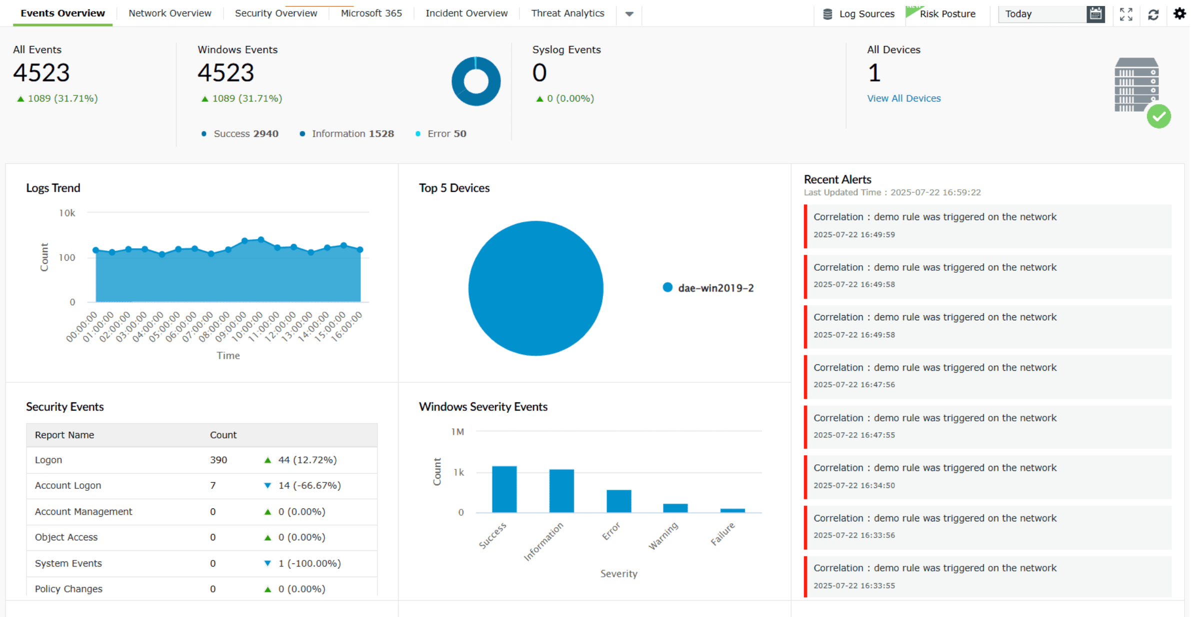
The Security Analytics Dashboard offers a unified view of your organization's threat landscape, turning detection data into actionable insights. Key elements of this dashboard:

- Visual representation of high-level metrics
- MITRE ATT&CK mapping
- Historical trends

With compact widgets for quick decision-making and expanded views for deep investigations, the dashboard helps monitor evolving threats, uncover patterns, and streamline incident response with precision.

Security tab in the dashboard

1. In the product console, click on the Security tab in the dashboard as highlighted below.



All Events
4523
▲ 1089 (31.71%)

Windows Events
4523
▲ 1089 (31.71%)

● Success **2940** ● Information **1528** ● Error **50**

Syslog Events
0
▲ 0 (0.00%)

All Devices
1
View All Devices

Logs Trend

Top 5 Devices

Security Events

Report Name	Count	
Logon	390	▲ 44 (12.72%)
Account Logon	7	▼ 14 (-66.67%)
Account Management	0	▲ 0 (0.00%)
Object Access	0	▲ 0 (0.00%)
System Events	0	▼ 1 (-100.00%)
Policy Changes	0	▲ 0 (0.00%)

Windows Severity Events

Recent Alerts
Last Updated Time : 2025-07-22 16:59:22

Correlation : demo rule was triggered on the network
2025-07-22 16:49:59

Correlation : demo rule was triggered on the network
2025-07-22 16:49:58

Correlation : demo rule was triggered on the network
2025-07-22 16:49:58

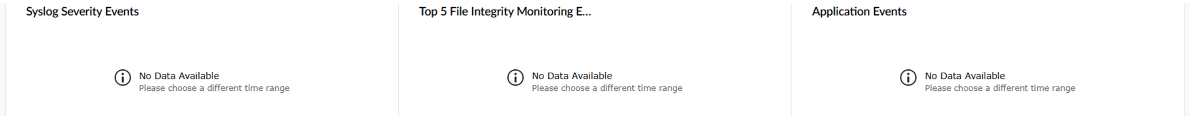
Correlation : demo rule was triggered on the network
2025-07-22 16:47:56

Correlation : demo rule was triggered on the network
2025-07-22 16:47:55

Correlation : demo rule was triggered on the network
2025-07-22 16:34:50

Correlation : demo rule was triggered on the network
2025-07-22 16:33:56

Correlation : demo rule was triggered on the network
2025-07-22 16:33:55


Syslog Severity Events

No Data Available
Please choose a different time range

Top 5 File Integrity Monitoring E...

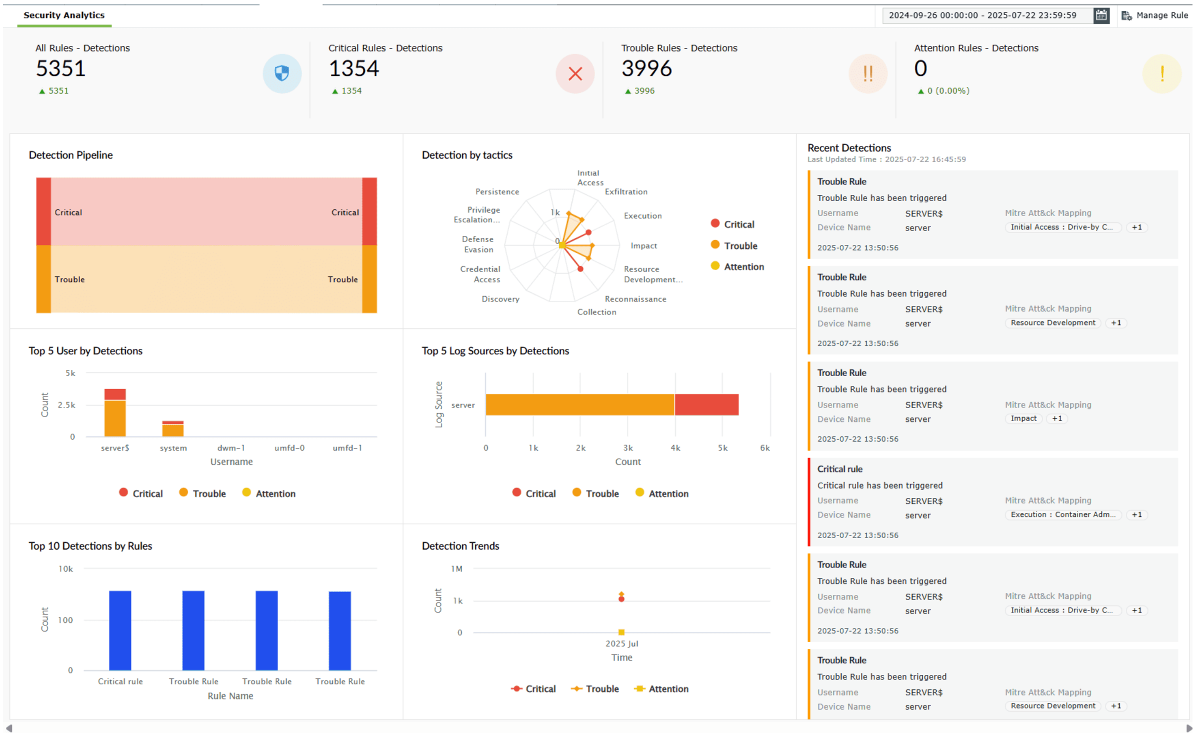
No Data Available
Please choose a different time range

Application Events

No Data Available
Please choose a different time range

Image 1: Security tab in the dashboard

2. You will be taken to the Security Analytics dashboard.


Security Analytics

2024-09-26 00:00:00 - 2025-07-22 23:59:59

Manage Rule

All Rules - Detections
5351
▲ 5351

Critical Rules - Detections
1354
▲ 1354

Trouble Rules - Detections
3996
▲ 3996

Attention Rules - Detections
0
▲ 0 (0.00%)

Detection Pipeline

Detection by tactics

Recent Detections
Last Updated Time : 2025-07-22 16:45:59

Trouble Rule
Trouble Rule has been triggered
Username SERVER$
Device Name server
Mitre Att&ck Mapping
Initial Access : Drive-by C... +1
2025-07-22 13:50:56

Trouble Rule
Trouble Rule has been triggered
Username SERVER$
Device Name server
Mitre Att&ck Mapping
Resource Development +1
2025-07-22 13:50:56

Trouble Rule
Trouble Rule has been triggered
Username SERVER$
Device Name server
Mitre Att&ck Mapping
Impact +1
2025-07-22 13:50:56

Critical rule
Critical rule has been triggered
Username SERVER$
Device Name server
Mitre Att&ck Mapping
Execution : Container Adm... +1
2025-07-22 13:50:56

Trouble Rule
Trouble Rule has been triggered
Username SERVER$
Device Name server
Mitre Att&ck Mapping
Initial Access : Drive-by C... +1
2025-07-22 13:50:56

Trouble Rule
Trouble Rule has been triggered
Username SERVER$
Device Name server
Mitre Att&ck Mapping
Resource Development +1

Top 5 User by Detections

Top 5 Log Sources by Detections

Top 10 Detections by Rules

Detection Trends

Image 2: Security analytics dashboard

Read further to understand the role of each widget in this tab and how it contributes to your network's security analytics.

> ⓘ NOTE
>
> To make the best use of this dashboard make sure that the rules for the detection are active and properly configured since this dashboard provides data and insights based on the currently active rules and their unique configurations.

Security Analytics- A breakdown of the dashboard

Data in precise numbers

The four compact elements in the top-most ribbon of the Security Analytics dashboard offer a high-level snapshot of detection activities across all three severity levels with accurate numbers, providing quick visibility into the total number of detections classified based on their distribution in severity levels of the rules as follows:

- All Rules - Detections

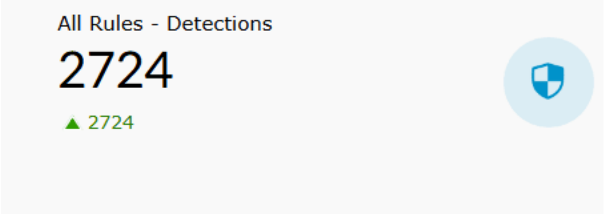
- Critical Rules - Detections
- Trouble Rules - Detections
- Attention Rules - Detections

These shall assist the security teams instantly gauge the overall threat landscape, prioritize the incident response efforts, and also monitor trends in the detection volumes over time.

A. Compact views

1. All Rules - Detections

This component provides the total count of all the detections made across every configured rule, offering a quick overview of your organization's threat landscape.



All Rules - Detections

2724

▲ 2724

Details displayed

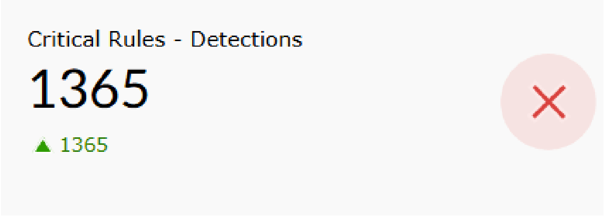
- Detection count: Total number of triggered detections across all rules.
- Growth/decline indicator: A green arrow highlights the decrease in detection counts, whereas a red one indicates an increase.

Role in Security Analytics

- Acts as the primary metric for overall threat volume.
- Helps track total security events within a given time frame.
- Serves as a baseline for comparing the distribution of critical and trouble detections.

2. Critical Rules - Detections

This component focuses on detections triggered by high-severity (critical) rules that require immediate attention.



Critical Rules - Detections

1365

▲ 1365

Details displayed

- Detection count: Total number of critical detections.
- Visual indicator: A red icon emphasizes the high-priority nature of these events.
- Growth/decline trend: Green arrow indicates a decrease in detection volume, whereas a red one indicates an increase.

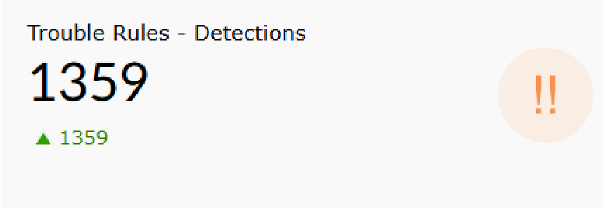
Role in Security Analytics

- Highlights security events with the highest risk and urgency.

- Helps prioritize immediate incident response actions.
- Serves as a key metric for assessing serious vulnerabilities or ongoing attacks.

3. Trouble Rules - Detections

This component displays the count of detections flagged by medium-severity (trouble) rules, representing potential risks or suspicious activities.



Trouble Rules - Detections

1359

▲ 1359

Details displayed

- Detection count: Total number of trouble-level detections.
- Visual indicator: Orange icon signals events that need closer monitoring.
- Growth/decline trend: Green arrow indicates changes in detection volume, whereas a red one indicates a decline.

Role in Security Analytics

- Helps monitor and investigate potential threats before they escalate.
- Provides visibility into less urgent but still relevant anomalies.
- Assists in tuning detection rules for medium-risk scenarios.

4. Attention Rules - Detections

This component tracks detections triggered by low-severity (attention) rules, indicating minor anomalies or early warning signs.

Details displayed

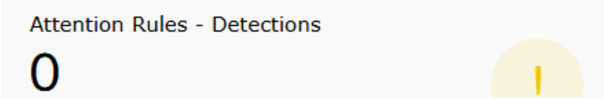
- Detection count: Total number of attention-level detections.
- Visual indicator: Yellow icon signifies a lower risk level.
- Growth/decline trend: Green arrow indicates changes in detection volume, whereas a red one indicates a decline.

Role in Security Analytics

- Offers context for early detection of unusual behavior.
- Helps identify non-critical patterns that could develop into threats.
- Complements higher-severity detections by providing a broader security overview.

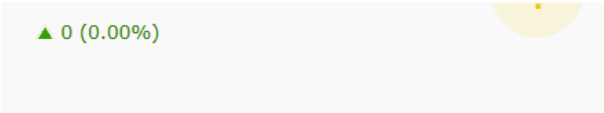
B. Expanded view of all four components

While the compact displays offer quick yet effective insights, clicking on the displayed count of any of these four components provides an expanded view of the same, which includes added details and context surrounding these detections.



Attention Rules - Detections

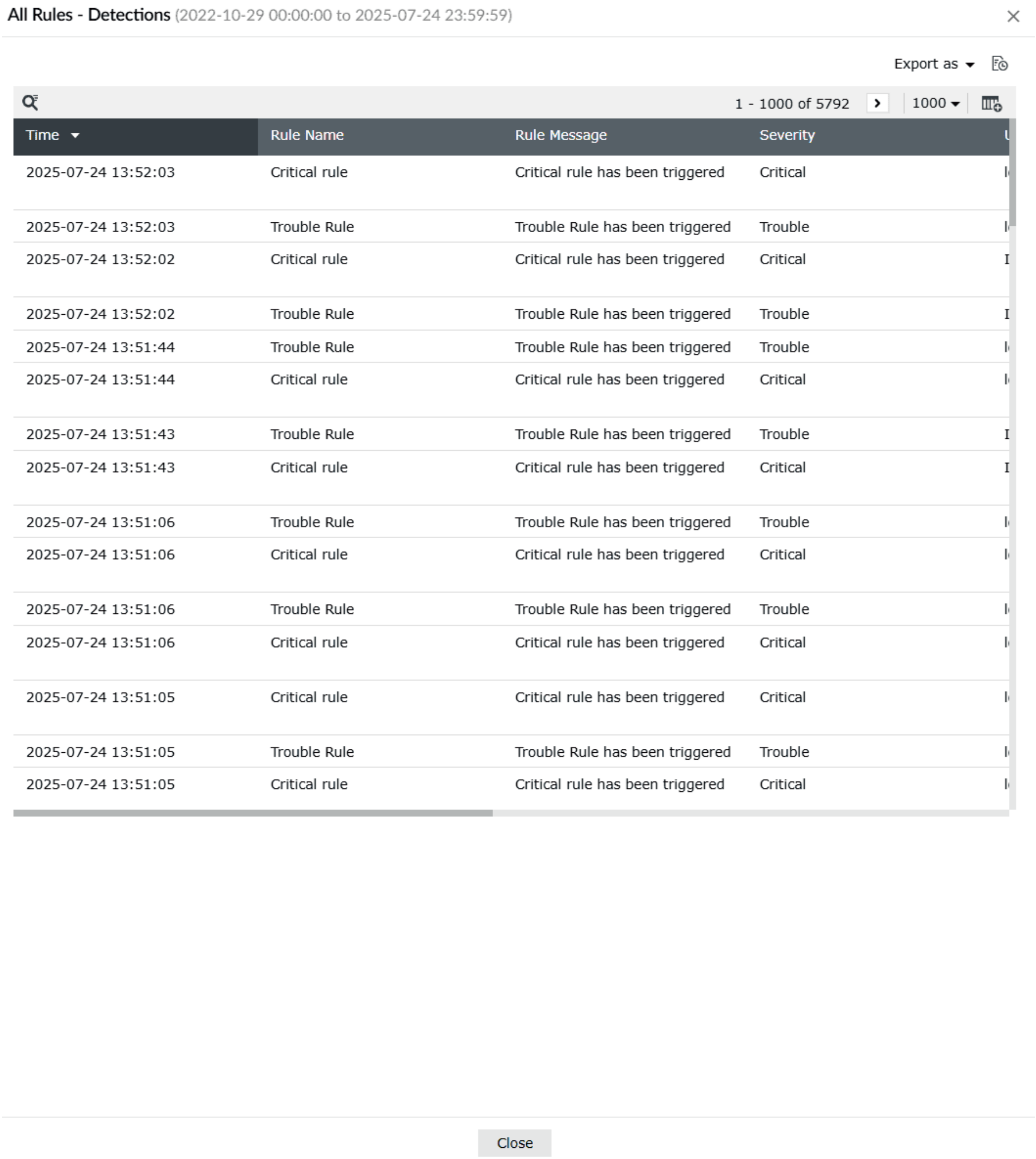
0



Upon clicking on the total count displayed in the compact view of any of the components, the expanded view appears with data arranged in an array of columns as shown above.

Available actions

- Clicking on the Export as ▼ button allows you to choose a format to export the said data either in a PDF format or a CSV file.
- Clicking on the Report export history icon allows you to view the complete history of the past data exports that have taken place for that particular report.



All Rules - Detections (2022-10-29 00:00:00 to 2025-07-24 23:59:59)

Time ▼	Rule Name	Rule Message	Severity
2025-07-24 13:52:03	Critical rule	Critical rule has been triggered	Critical
2025-07-24 13:52:03	Trouble Rule	Trouble Rule has been triggered	Trouble
2025-07-24 13:52:02	Critical rule	Critical rule has been triggered	Critical
2025-07-24 13:52:02	Trouble Rule	Trouble Rule has been triggered	Trouble
2025-07-24 13:51:44	Trouble Rule	Trouble Rule has been triggered	Trouble
2025-07-24 13:51:44	Critical rule	Critical rule has been triggered	Critical
2025-07-24 13:51:43	Trouble Rule	Trouble Rule has been triggered	Trouble
2025-07-24 13:51:43	Critical rule	Critical rule has been triggered	Critical
2025-07-24 13:51:06	Trouble Rule	Trouble Rule has been triggered	Trouble
2025-07-24 13:51:06	Critical rule	Critical rule has been triggered	Critical
2025-07-24 13:51:06	Trouble Rule	Trouble Rule has been triggered	Trouble
2025-07-24 13:51:06	Critical rule	Critical rule has been triggered	Critical
2025-07-24 13:51:05	Critical rule	Critical rule has been triggered	Critical
2025-07-24 13:51:05	Trouble Rule	Trouble Rule has been triggered	Trouble
2025-07-24 13:51:05	Critical rule	Critical rule has been triggered	Critical

Image 3: All rules detections in security analytics dashboard

- Clicking on the ⊞ icon on the top-right corner of the data table allows you to select/deselect and Apply what data you wish to view separated by columns.

Details displayed (list of available columns)

- Time: Timestamp for when the rule was triggered.
- Rule Name: Detected rules categorized by their severity level- Critical, Trouble, or Attention.
- Rule Message: A brief descriptive message about the triggered detection.
- Severity: Indicates the severity of the rule detected.
- Username: The account responsible for the activity.
- Log Source: Source system or device associated with the detected activity.
- MITRE ATT&CK Mapping: Tactic and technique classification aligned with the MITRE ATT&CK framework.
- Tags: Additional contextual tags, such as industry verticals.

Role in Security Analytics

- Enables deep investigation of every triggered rule by showing when and where it occurred.
- Assists in prioritizing response based on severity, helping SOC teams act swiftly on critical alerts.
- Maps suspicious activities to known threat tactics (via MITRE ATT&CK) for quicker threat attribution and analysis.
- Enhances visibility into user behavior, log source reliability, and attack patterns.
- Supports fine-tuning of rules by providing granular, real-time feedback on their effectiveness and noise levels.

Read also

This page explained the security dashboard's purpose, how to access it, and the role of its widgets. You also learned how compact and expanded views help track detections by severity, uncover patterns, and prioritize response.

- Security dashboard widgets

4.1.1.2. Security dashboard widgets

Last updated on: September 12, 2025

In this page

Overview

The Security Dashboard provides a centralized view of detections across your environment. It helps security teams monitor threats, analyze patterns, and prioritize incidents using real-time visuals and context-driven insights.

Dashboard widgets

Widgets provide real-time snapshots of the detections, trends, and key security metrics made by the detection engine, helping you quickly assess and respond to threats proactively. In the widgets containing graphs, clicking on a severity type removes data corresponding to it from the said graph(s).

There are a total of 7 widgets available in the Security Analytics dashboard:

1. Detection Pipeline
2. Detection by Tactics
3. Recent Detections
4. Top 5 Users by Detections
5. Top 5 Log Sources by Detections
6. Top 10 Rules by Detections
7. Detection Trend

Every widget in this dashboard includes two icons in its top-right corner:

Expand ⛶: This option provides an expanded view of that widget, offering more, and deeper insights related to it.

Refresh ⟳: Clicking on the Refresh icon instantly re-assesses the real-time log data and updates the widget with the same, ensuring you never miss even a second worth of key findings from your network's security analysis.

Severity colors

Security events (excluding the Top 10 rules by detections widget) are categorized by severity levels as set during the rules configuration, represented through distinct colors for quick identification as listed below:

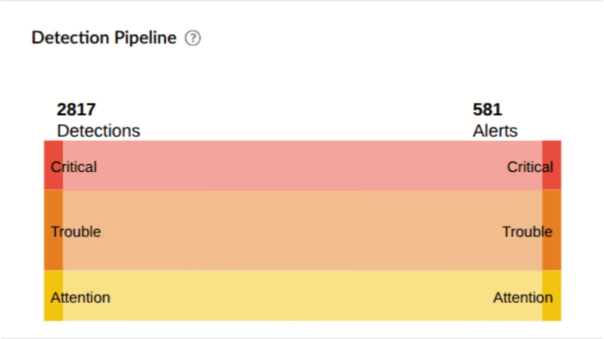
- Red- Critical: Represent severe, high-priority security detections that require immediate attention and possible mitigation steps.
- Orange- Trouble: Indicate medium-level events/incidents hinting at potential risks, suspicious activities, or policy violations that demand prompt investigation.
- Yellow- Attention: Denote low-level detections that require monitoring but pose no immediate risk.

Below is a complete breakdown of all the widgets that the Security Analytics dashboard is comprised of:

1. Detection Pipeline

The Detection Pipeline visualizes the flow of the detections and alerts across the three severity levels. It provides a quick overview of how many events were detected, categorized, and then escalated into actionable alerts.

A. Concise widget view



Details displayed

- Detections: The total count of events flagged by the system.
- Alerts: Number of detections that have been flagged as alerts.
- Severity distribution: Each of the three severity levels is displayed with its corresponding event(s) count.

Role in Security Analytics

The Detection Pipeline widget acts as the starting point for threat monitoring by helping analysts:

- Quickly identify the severity distribution of all the current threats.
- Detect spikes or anomalies in alert generation.
- Streamline the investigation process by focusing on high-priority alerts.

B. Expanded widget view

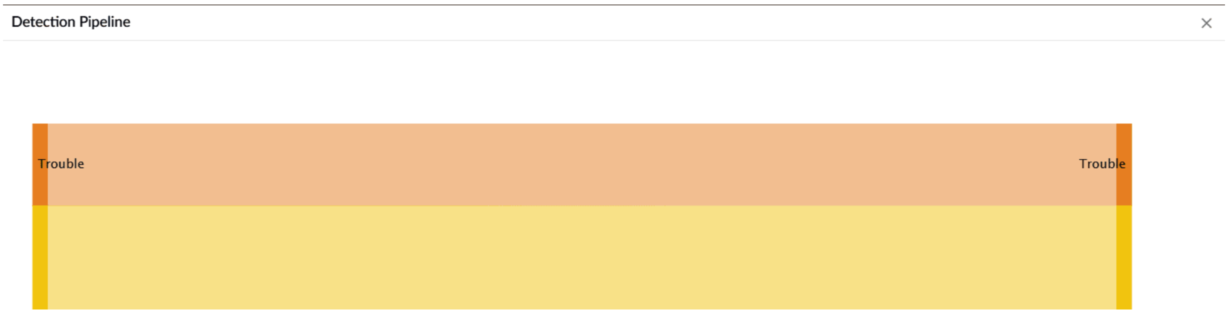


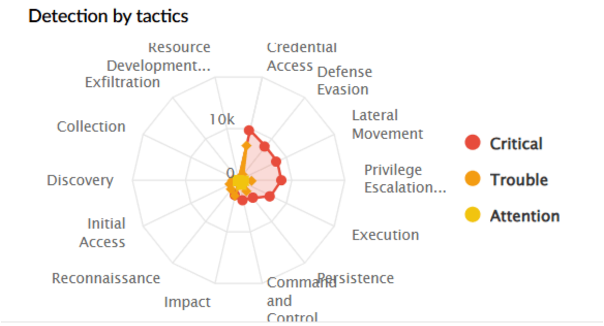
Image 1: Detection pipeline widget in security analytics dashboard

The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.

2. Detection by Tactics

The Detection by Tactics chart maps all the flagged events to the MITRE ATT&CK framework. It shows which stages of the cyberattack lifecycle, such as Initial Access, Execution, Privilege Escalation, are being set in motion via simultaneous events/activities.

A. Concise widget view



Details displayed

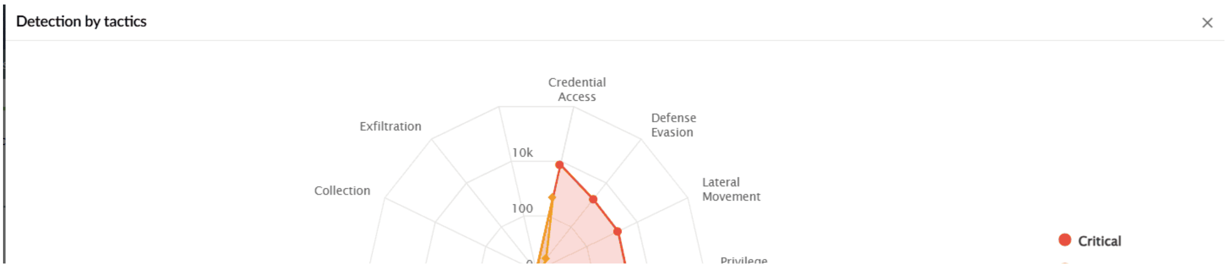
- Tactic categories: Includes the possible common attack stages like Initial Access, Discovery, Exfiltration, and Lateral Movement.
- Severity overlay: Each tactic is color-coded by the three severity levels.

Role in Security Analytics

This widget provides a tactical view of potential adversary behavior, helping teams:

- Analyze and understand attack patterns and prevalent tactics in their environment.
- Prioritize security controls for the most frequently targeted attack phases.
- Align detection rules with industry-recognized attack models for enhanced defense.

B. Expanded widget view



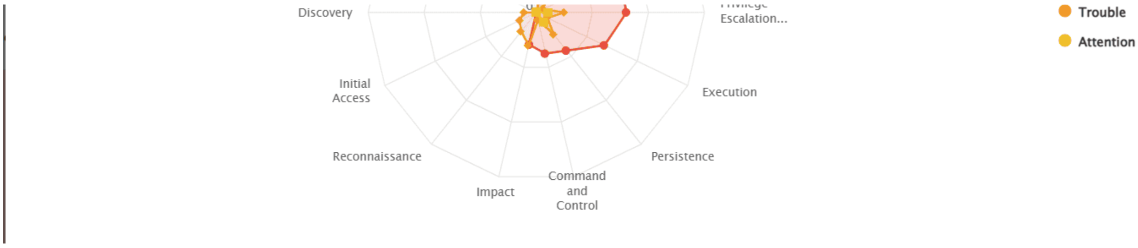


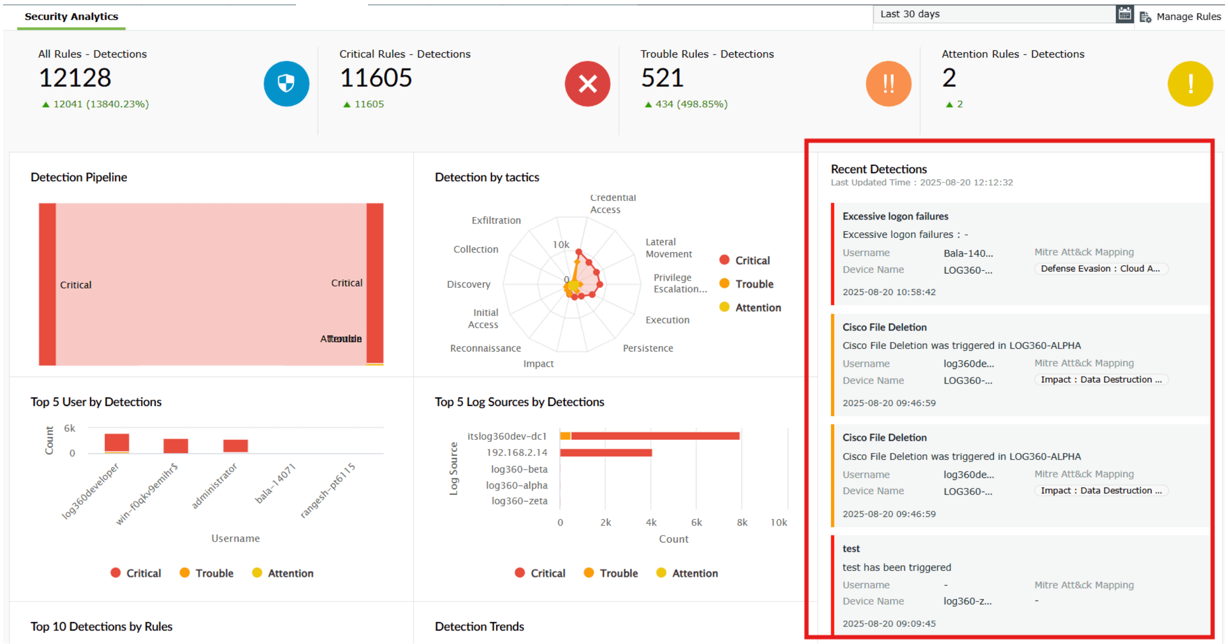
Image 2: Detection by tactics widget in security analytics dashboard

- The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.
- Clicking on any data point representing a detection count slides open the data table for that particular rule severity level, similar to the expanded view of the four components.

3. Recent Detections

The Recent Detections widget provides a chronological list of the events triggered most recently, enabling real-time incident visibility.

A. Concise widget view



Recent Detections
Last Updated Time : 2025-08-20 12:12:32

Excessive logon failures
Excessive logon failures : -
Username Bala-140... Mitre Att&ck Mapping
Device Name LOG360-... Defense Evasion : Cloud A...
2025-08-20 10:58:42

Cisco File Deletion
Cisco File Deletion was triggered in LOG360-ALPHA
Username log360de... Mitre Att&ck Mapping
Device Name LOG360-... Impact : Data Destruction ...
2025-08-20 09:46:59

Cisco File Deletion
Cisco File Deletion was triggered in LOG360-ALPHA
Username log360de... Mitre Att&ck Mapping
Device Name LOG360-... Impact : Data Destruction ...
2025-08-20 09:46:59

test
test has been triggered
Username - Mitre Att&ck Mapping
Device Name log360-z... -
2025-08-20 09:09:45

Image 3: Recent detections widget in security analytics dashboard

Details displayed

- Rule name: The name of the rule that is associated with the detection triggered.
- Description: Brief summary of the detection. For example, "Interactive Logon – A process deleted a system backup".
- Username: Identifies the username of the account associated with the event/activity.
- Log Source: Specifies the origin device or system.

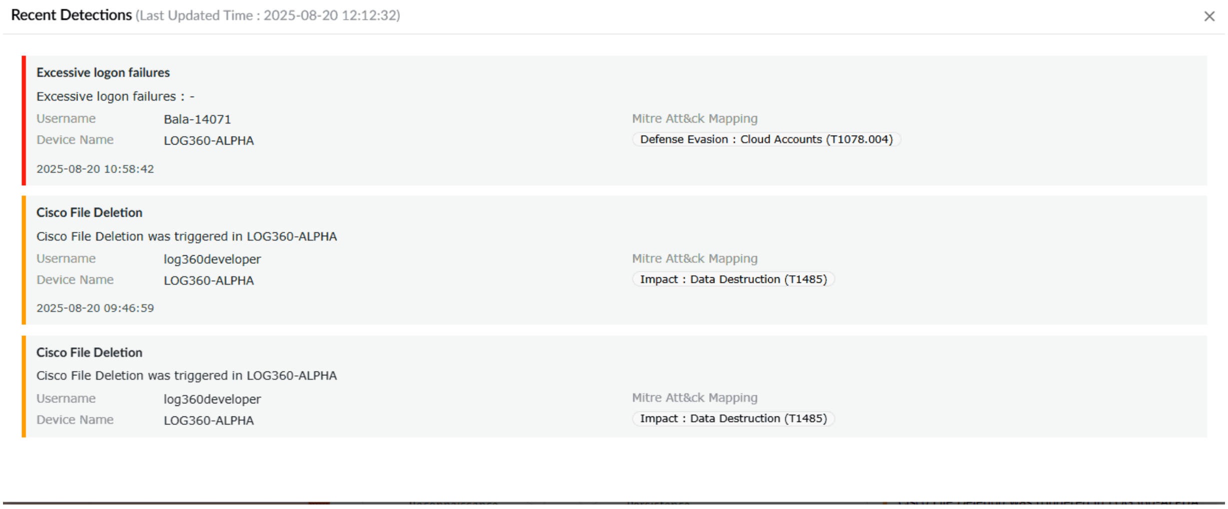
- MITRE ATT&CK Mapping: Associates the detection with a specific technique(s) or tactic(s) from the MITRE ATT&CK framework.
- Timestamp: Captures the exact date and time of the event occurrence.

Role in Security Analytics

This widget serves as a real-time threat feed, helping security analysts:

- Quickly detect and respond to emerging threats.
- Correlate events with specific users and devices.
- Perform rapid triage using MITRE mappings to understand the nature of attacks.

B. Expanded widget view



Recent Detections (Last Updated Time : 2025-08-20 12:12:32)

Excessive logon failures

Excessive logon failures : -

Username	Bala-14071	Mitre Att&ck Mapping	
Device Name	LOG360-ALPHA	Defense Evasion : Cloud Accounts (T1078.004)	

2025-08-20 10:58:42

Cisco File Deletion

Cisco File Deletion was triggered in LOG360-ALPHA

Username	log360developer	Mitre Att&ck Mapping
Device Name	LOG360-ALPHA	Impact : Data Destruction (T1485)

2025-08-20 09:46:59

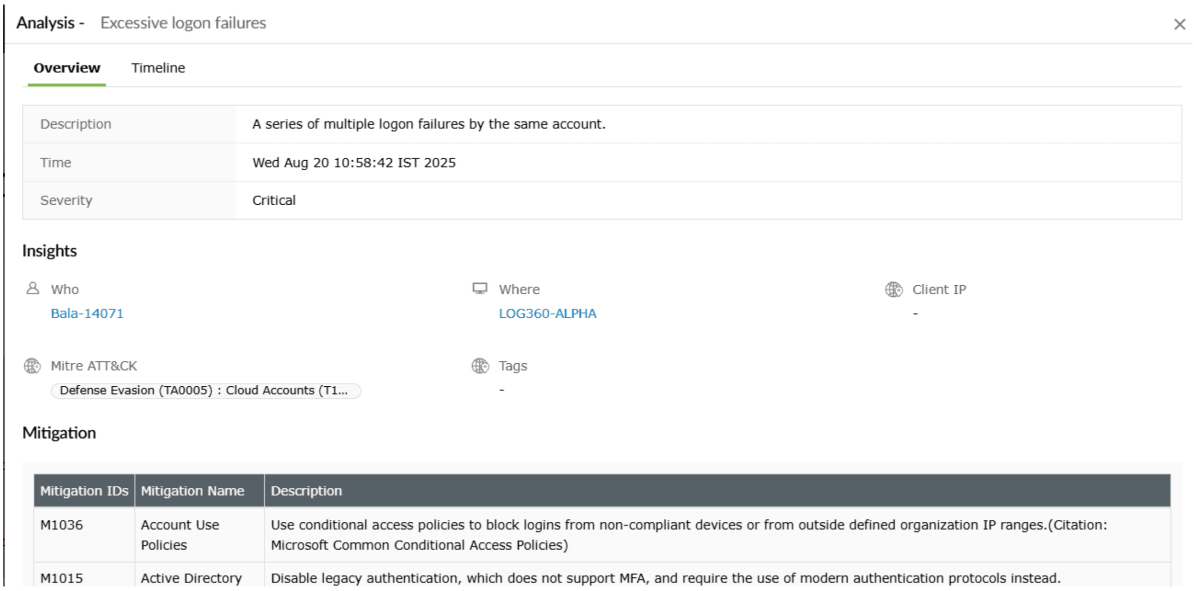
Cisco File Deletion

Cisco File Deletion was triggered in LOG360-ALPHA

Username	log360developer	Mitre Att&ck Mapping
Device Name	LOG360-ALPHA	Impact : Data Destruction (T1485)

Image 4: Recent detections widget in security analytics dashboard

- The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the details of the most recent detections.
- Upon clicking on any rule from this view (or compact view), a complete analysis of that rule slides open as shown below.



Analysis - Excessive logon failures

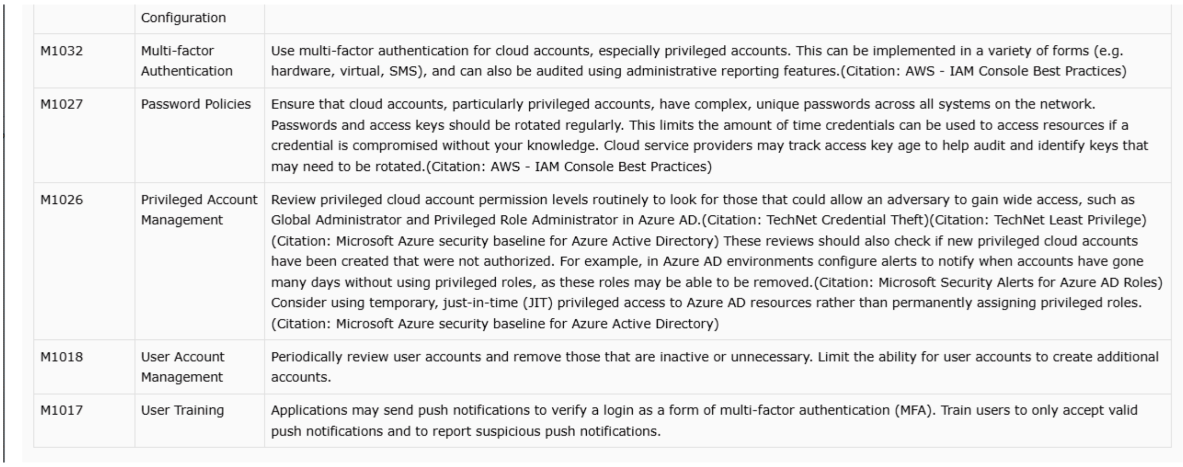
Description	A series of multiple logon failures by the same account.
Time	Wed Aug 20 10:58:42 IST 2025
Severity	Critical

Insights

Who	Where	Client IP
Bala-14071	LOG360-ALPHA	-
Mitre ATT&CK	Tags	
Defense Evasion (TA0005) : Cloud Accounts (T1...	-	

Mitigation

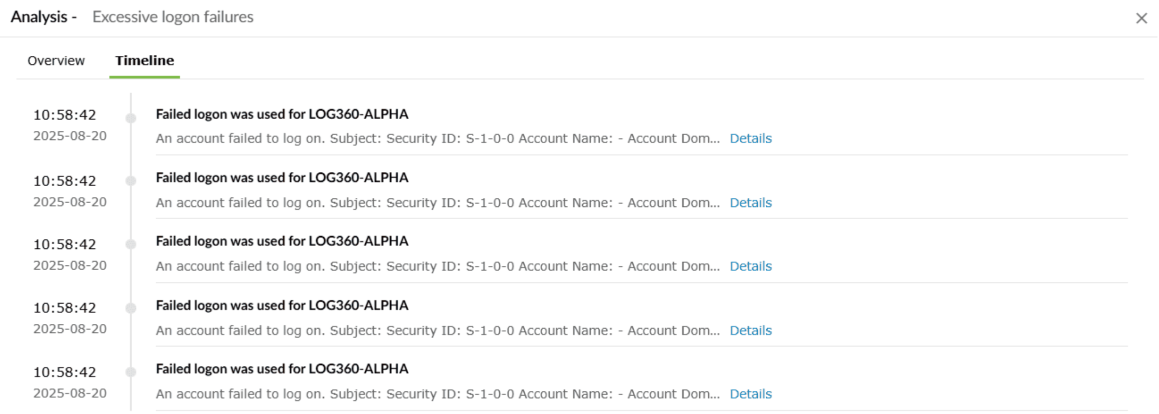
Mitigation IDs	Mitigation Name	Description
M1036	Account Use Policies	Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges.(Citation: Microsoft Common Conditional Access Policies)
M1015	Active Directory	Disable legacy authentication, which does not support MFA, and require the use of modern authentication protocols instead.



	Configuration	
M1032	Multi-factor Authentication	Use multi-factor authentication for cloud accounts, especially privileged accounts. This can be implemented in a variety of forms (e.g. hardware, virtual, SMS), and can also be audited using administrative reporting features.(Citation: AWS - IAM Console Best Practices)
M1027	Password Policies	Ensure that cloud accounts, particularly privileged accounts, have complex, unique passwords across all systems on the network. Passwords and access keys should be rotated regularly. This limits the amount of time credentials can be used to access resources if a credential is compromised without your knowledge. Cloud service providers may track access key age to help audit and identify keys that may need to be rotated.(Citation: AWS - IAM Console Best Practices)
M1026	Privileged Account Management	Review privileged cloud account permission levels routinely to look for those that could allow an adversary to gain wide access, such as Global Administrator and Privileged Role Administrator in Azure AD.(Citation: TechNet Credential Theft)(Citation: TechNet Least Privilege)(Citation: Microsoft Azure security baseline for Azure Active Directory) These reviews should also check if new privileged cloud accounts have been created that were not authorized. For example, in Azure AD environments configure alerts to notify when accounts have gone many days without using privileged roles, as these roles may be able to be removed.(Citation: Microsoft Security Alerts for Azure AD Roles) Consider using temporary, just-in-time (JIT) privileged access to Azure AD resources rather than permanently assigning privileged roles.(Citation: Microsoft Azure security baseline for Azure Active Directory)
M1018	User Account Management	Periodically review user accounts and remove those that are inactive or unnecessary. Limit the ability for user accounts to create additional accounts.
M1017	User Training	Applications may send push notifications to verify a login as a form of multi-factor authentication (MFA). Train users to only accept valid push notifications and to report suspicious push notifications.

Image 5: Recent detections analysis in security analytics dashboard

- This analysis contains the following-
  - Overview tab:
    - Description- Text field summarizing what the rule is about (empty in this case).
    - Time- Exact timestamp of when the rule was triggered.
    - Severity- Indicates the impact level of the rule triggered - here, it is Critical.
    - Insights section-
      - Who: Username involved in the triggered rule.
      - Where: Device or host where the event occurred.
      - Client IP: IP address of the client involved in the incident.
      - MITRE ATT&CK: Mapping to known adversarial tactics/techniques.
      - Tags: Labels giving contextual information
    - Mitigation section-
      - Mitigation: Recommended or recorded response actions.
  - Timeline tab: Inserts the detection in a chain of consecutive events providing a larger picture of all the occurring activities in a context that fits.



10:58:42
2025-08-20
Failed logon was used for LOG360-ALPHA
An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Dom... Details

10:58:42
2025-08-20
Failed logon was used for LOG360-ALPHA
An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Dom... Details

10:58:42
2025-08-20
Failed logon was used for LOG360-ALPHA
An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Dom... Details

10:58:42
2025-08-20
Failed logon was used for LOG360-ALPHA
An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Dom... Details

10:58:42
2025-08-20
Failed logon was used for LOG360-ALPHA
An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Dom... Details

Image 6: Recent detections analysis in security analytics dashboard

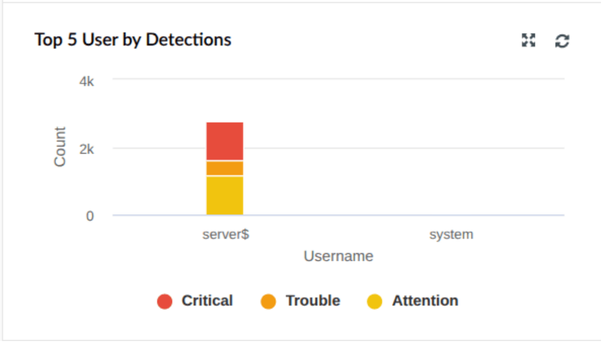
- Clicking on the Details button prompts open a pane containing ALL details of that particular event associated with that rule detection. Below is the list of details provided:
  - Risk Level
  - Message
  - Source
  - Remote DeviceIp
  - Logon Type
  - Process Id
  - OS Category
  - Host Type
  - LogonId
  - Task Category
  - Member Group SID
  - Authentication Package Name
  - Event Name
  - Device
  - GUID
  - Logon Process
  - Severity
  - Key Length
  - Event ID
  - ACTION_TAG
  - Type
  - Caller LogonID
  - Username

- Username
- Security Id
- Source Port Number
- Domain

4. Top 5 Users by Detections

This chart highlights in a statistical view the top five user accounts with the highest detection counts, broken down by severity.

A. Concise widget view



Details displayed

- Username: Displays the usernames of the accounts of the top 5 users on the x-axis.
- Count: Total number of detections per user on the y-axis.
- Severity breakdown: Stacked bars visualize the proportion of the three severity levels of the alerts per user.

Role in Security Analytics

- Identifies compromised accounts or potential insider threats.
- Helps prioritize account audits for high-risk users.
- Provides a behavioral snapshot of every suspicious user's activity patterns.

B. Expanded widget view

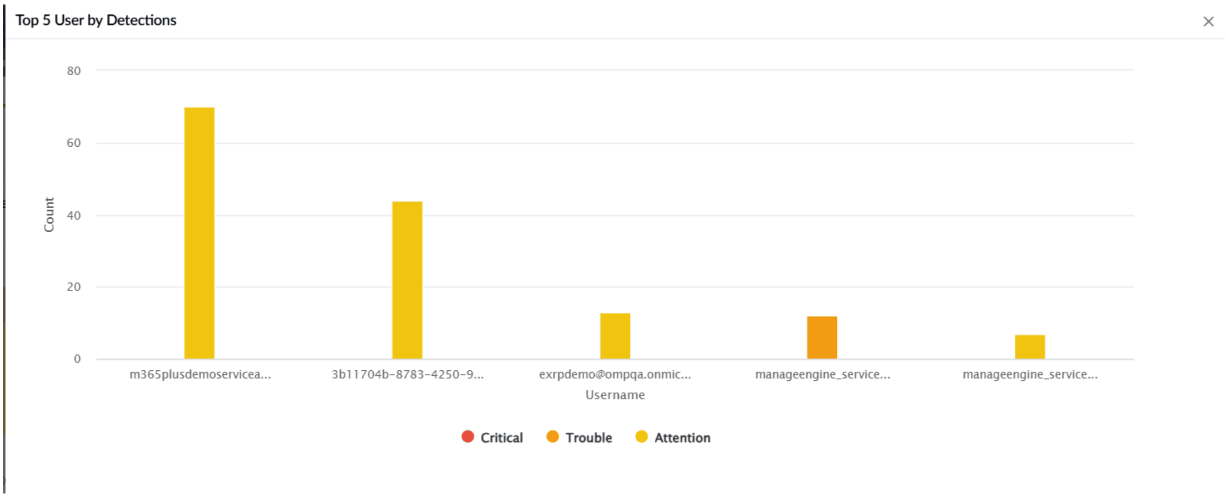


Image 7: Top 5 users by detections widget in security analytics dashboard

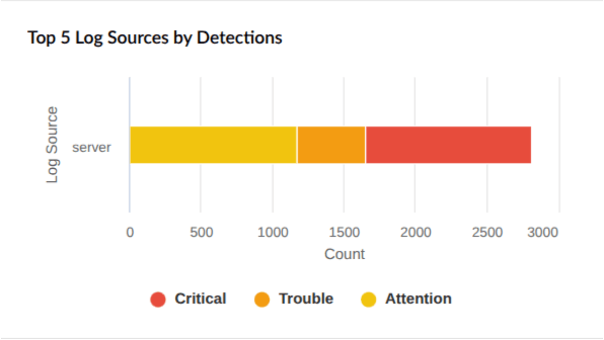
Image 7: Top 5 users by detections widget in security analytics dashboard

The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.

5. Top 5 Log Sources by Detections

This chart shows the devices or systems contributing the highest in order to the total detection counts.

A. Concise widget view



Details displayed

- Log Source: Specifies the origin device or system on the y-axis.
- Count: Number of detections per log source on the x-axis.
- Severity split: Bars of the graph, color coded with the three severity levels indicate which devices are generating alerts of varied severity.

Role in Security Analytics:

- Highlights the most vulnerable or frequently attacked devices.
- Helps you focus on device hardening efforts on potential high-risk systems.
- Provides insights into log source health and configurations.

B. Expanded widget view

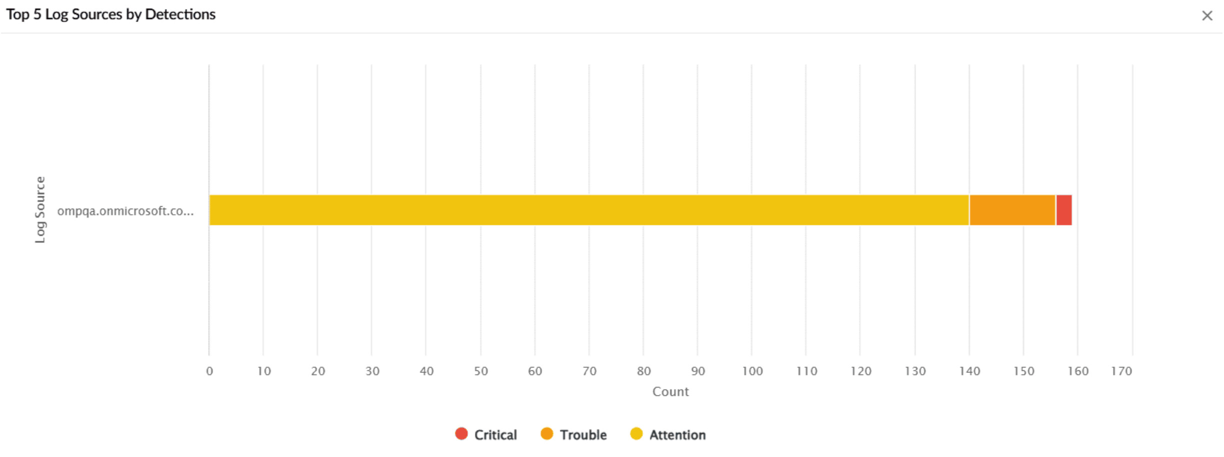


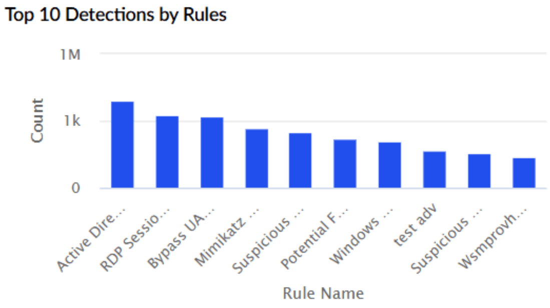
Image 8: Top 5 log sources by detections widget in security analytics dashboard

The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.

6. Top 10 Detections by Rules

This bar chart displayed here ranks the top 10 detection rules based on the frequency of detected triggers.

A. Concise widget view



Details displayed

- Rule Name: Includes rules such as Excessive file access, Repeated operations, or Brute force on the x-axis
- Count: Displays how many times each rule was triggered on the y-axis.

Role in Security Analytics

- Identifies recurring threats or common triggers.
- Assists in fine-tuning detection rules to reduce false positives.
- Provides data to optimize threat hunting and response strategies.

B. Expanded widget view

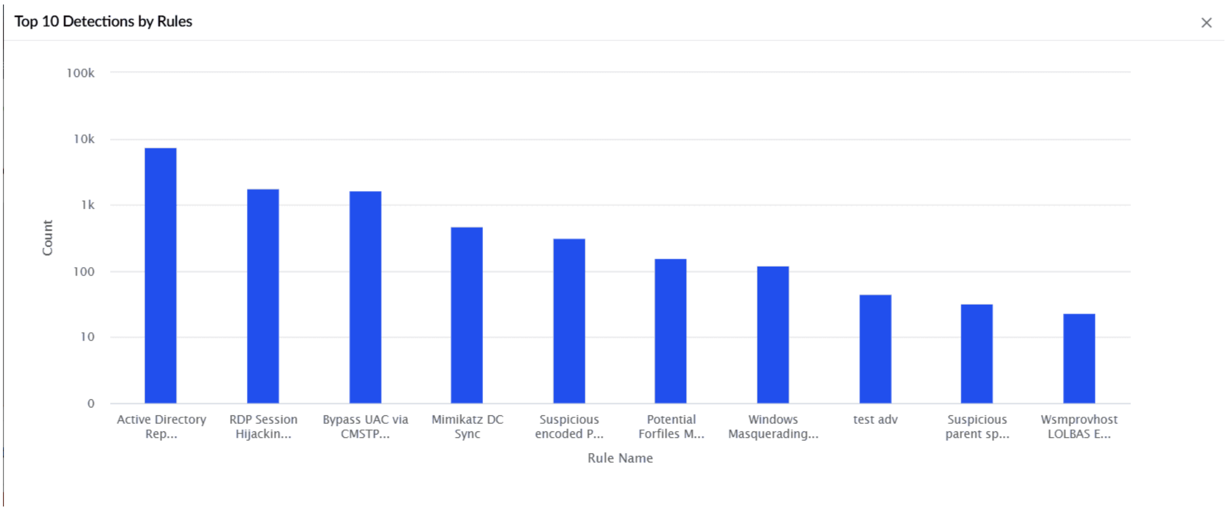


Image 9: Top 10 detections by rules widget in security analytics dashboard

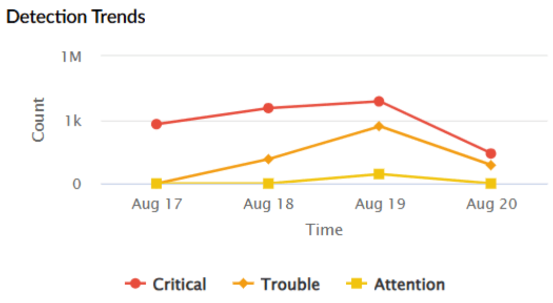
- The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.

- Clicking on any data bar representing detection count slides open the data table for that particular rule severity level, similar to the expanded view of the four components.

7. Detection Trends

The Detection Trends chart tracks detection activity over time, segmented by severity.

A. Concise widget view



Details displayed

- Time: Displays yearly or monthly detection counts spread across the x-axis.
- Count: Displays the total count of detections across time periods on the y-axis.
- Severity trend lines: Separate lines of the graph track the detections assorted based on the three severity levels.

Role in Security Analytics

- Helps spot anomalies or sudden spikes in activity.
- Provides historical context for incident analysis.
- Aids in capacity and resource planning for security operations.

B. Expanded widget view

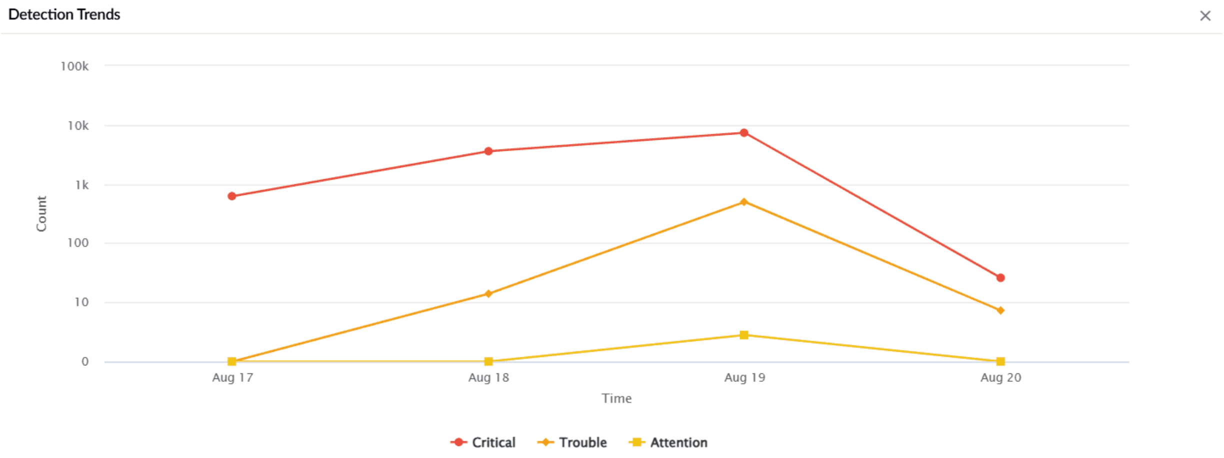


Image 10: Detections trends widget in security analytics dashboard

The expanded widget view displayed upon clicking on the expand icon provides a clearer representation of the rules spread across the severity levels.

Actions available in the Security Analytics dashboard

There are two mainly available actions in this tab:

1. Custom time range: For data analysis in the form of widgets.
2. Manage Rules: To view the rule management module. It acts as the backbone of the security analytics capability of Log360 by creating a highly effective framework that is followed by the analysis-identification-detection cycle by the SIEM (Security Information and Event Management) solution that assists you in safeguarding your enterprise network and enforcement of active threat detection and proactive threat response mechanisms.

Custom time range

1. Navigate to the Security Analytics dashboard via the Security tab and click anywhere in the highlighted area as shown below.

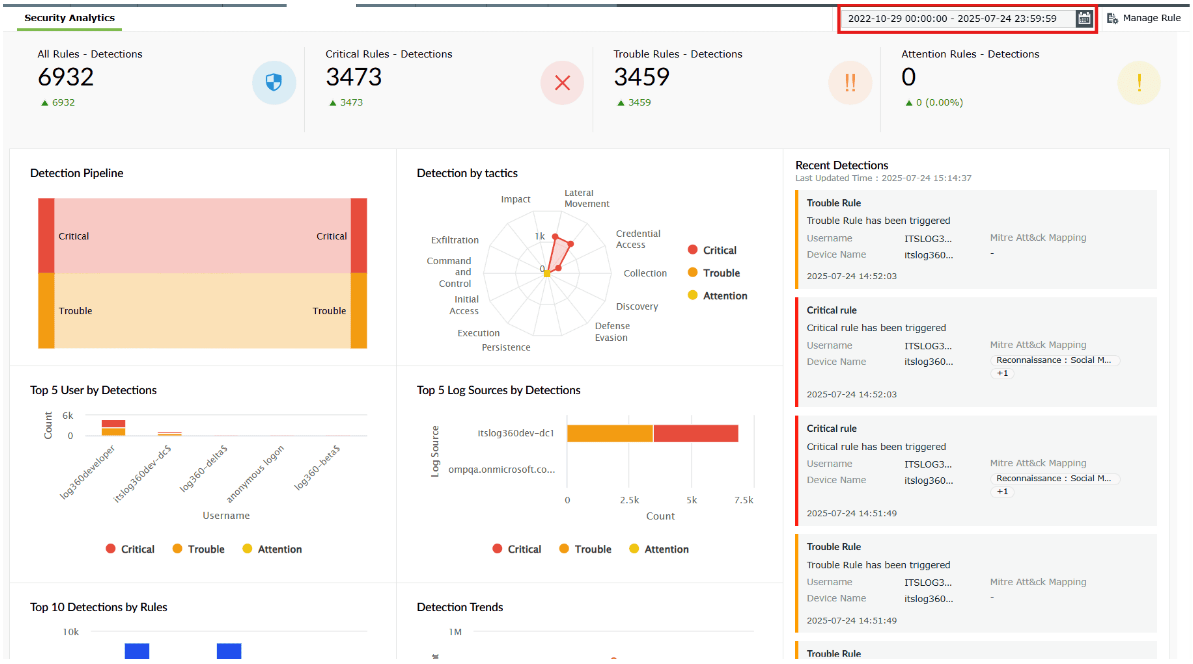
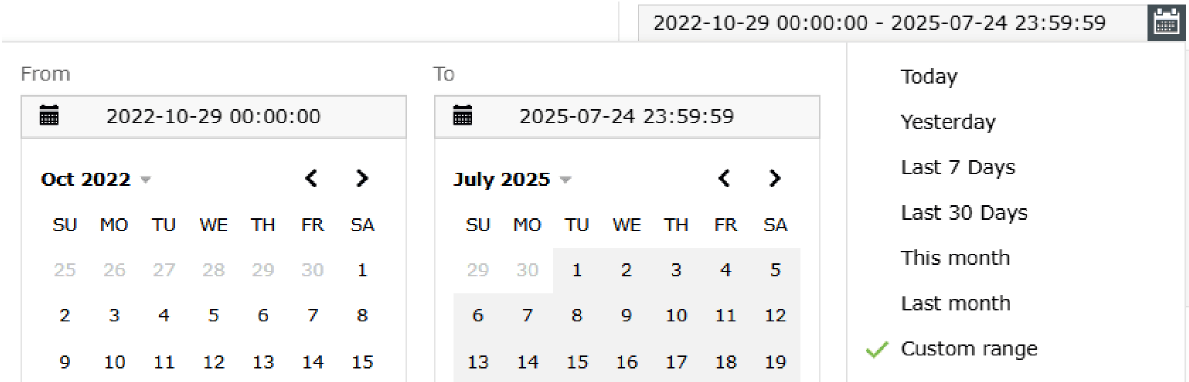
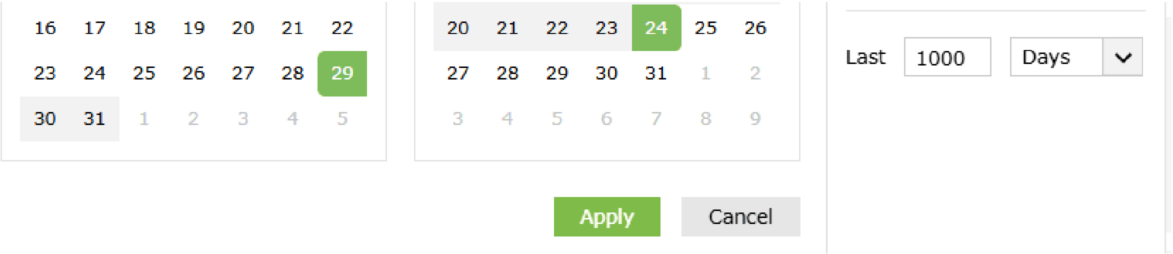


Image 11: Configuring detections time period in security analytics dashboard

2. The action prompts open the calendar view along with predefined time ranges for you to choose from.





3. You can:
   - Select the start date and end date for your desired time range.
   - Click on any of the predefined time ranges available that suits your requirements.
   - Click on Custom range and then proceed to enter a number in the box provided below that will represent the past number of days worth of data you wish to view.
4. Click on Apply.
5. Upon completion of action, you will see that the Security Analytics dashboard is instantly updated according to the time range you have selected.

Manage Rules

1. Navigate to the Security Analytics dashboard via the Security tab and click on the Manage Rule option as highlighted in the below image.

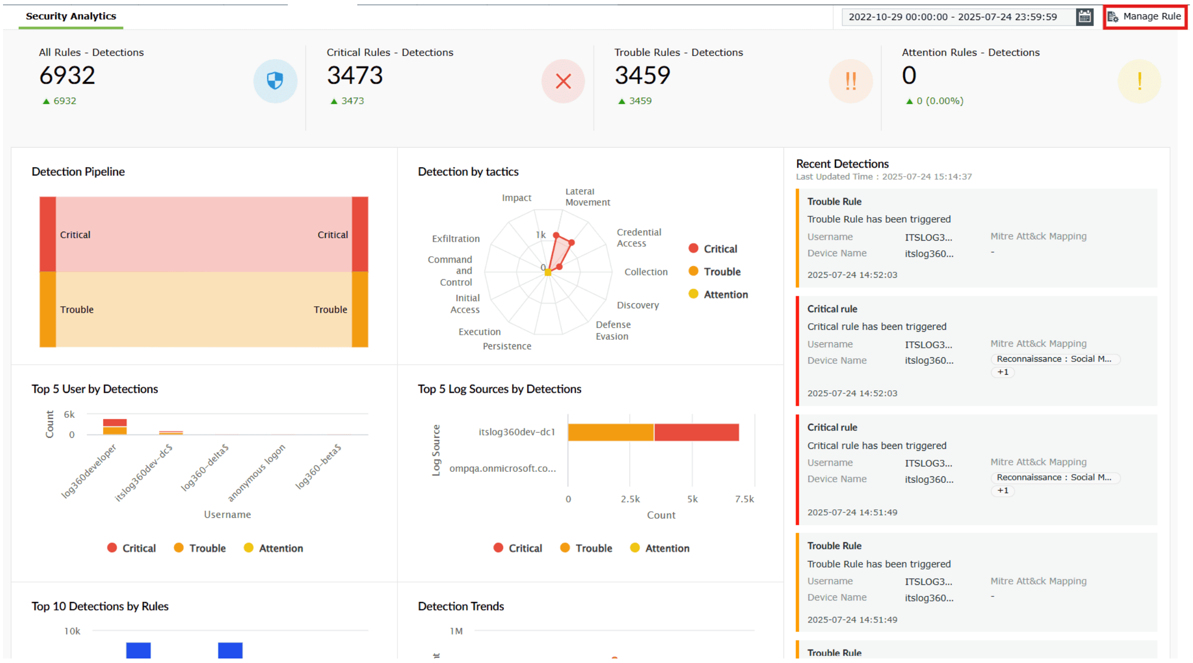
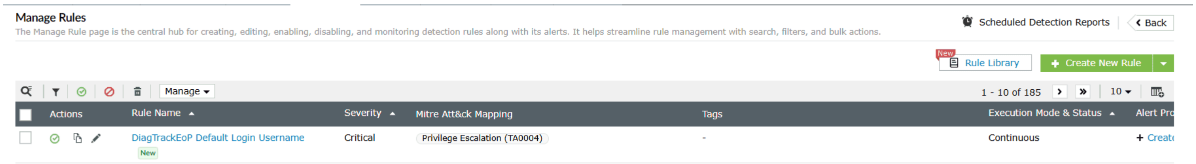


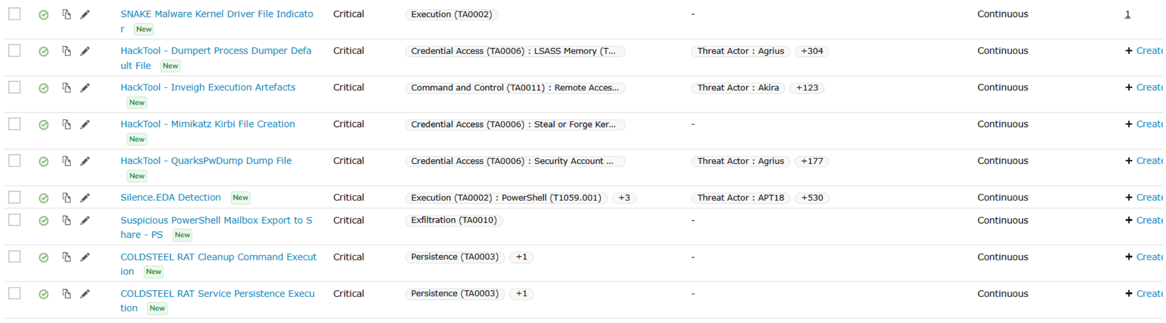
Image 12: Manage rules button in the security tab

2. You will be taken to the Manage Rules module, which is the central hub for managing rules, allowing you to configure rules efficiently.


Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

Actions	Rule Name	Severity	Mitre Att&ck Mapping	Tags	Execution Mode & Status	Alert Pro
	DiagTrackEoP Default Login Username New	Critical	Privilege Escalation (TA0004)	-	Continuous	+ Create



□	SNAKE Malware Kernel Driver File Indicator New	Critical	Execution (TA0002)	-	Continuous	1
□	HackTool - Dumpert Process Dumper Default File New	Critical	Credential Access (TA0006) : LSASS Memory (T...	Threat Actor : Agrius +304	Continuous	+ Create
□	HackTool - Inveigh Execution Artefacts New	Critical	Command and Control (TA0011) : Remote Acces...	Threat Actor : Akira +123	Continuous	+ Create
□	HackTool - Mimikatz Kirbi File Creation New	Critical	Credential Access (TA0006) : Steal or Forge Ker...	-	Continuous	+ Create
□	HackTool - QuarksPwDump Dump File New	Critical	Credential Access (TA0006) : Security Account ...	Threat Actor : Agrius +177	Continuous	+ Create
□	Silence.EDA Detection New	Critical	Execution (TA0002) : PowerShell (T1059.001) +3	Threat Actor : APT18 +530	Continuous	+ Create
□	Suspicious PowerShell Mailbox Export to Share - PS New	Critical	Exfiltration (TA0010)	-	Continuous	+ Create
□	COLDSTEEL RAT Cleanup Command Execution New	Critical	Persistence (TA0003) +1	-	Continuous	+ Create
□	COLDSTEEL RAT Service Persistence Execution New	Critical	Persistence (TA0003) +1	-	Continuous	+ Create

Image 13: Manage rules module via the security tab

Click here to learn more about rule management and how to configure rules.

Dashboard customization

The Security Analytics tab in itself cannot be customized via the Security tab. Instead, the same sub-tab is provided in the product as the Detection Overview sub-tab in the Dashboard tab.

The Detection Overview dashboard includes everything that is provided in the Security Analytics tab while also allowing you to customize the dashboard and the widgets in it.

To learn how to customize your Detection Overview dashboard in the main Dashboard tab, refer to the Dashboard View help document.

Read also

This page detailed all seven security dashboard widgets, their compact and expanded views, and how they help you monitor threats, analyze adversary tactics, and identify high-risk users, rules, and devices.

- Security dashboard overview

Chapter 4.1.2 **Rule management**

4.1.2.1. Rule management overview

Last updated on: September 12, 2025

In this page

Overview

This page covers why and how rule management plays a crucial role in anomaly detection within your network. By managing rules you effectively optimize Log360's UEBA engine to monitor specific behaviors you want to watch for. This helps in narrowing down the scope and saving time and resources by focusing on relevant events and thus receiving alerts as per the conditions defined. When the defined conditions are met, the ML model detects and flags the behavior as anomalous.

Rule Management

- Functionality: The Rule Management capability is a centralized platform designed to streamline the management of all rule types, including ATA (Advanced Threat Analytics), MITRE, Correlation, and UEBA (User and Entity Behavior Analytics). This unified interface eliminates the need for navigating disparate tools, providing a seamless and efficient experience for users managing security rules.
- Rule management allows you to define the conditions under which a specific user or entity will be flagged as anomalous. The Machine Learning model first establishes a baseline behavior of all the users and entities in your network during the training phase in order to be able to differentiate the deviation from the usual behavior. Rule configuration provides the foundation for the ML model to spot these deviations, thus providing a framework for the anomaly detection logic.

Why is Rule Management important for threat detection?

Probing into every event log out of the hundreds that are collected each day is a tedious and near-impossible task. Rules help narrow down the scope for threat detection by targeting specific or widely known risky and unusual behaviors in your environment for threats like insider attacks, brute-force attacks, data exfiltration, etc.
Rule configuration will add an advantage of being able to scan such threats from every angle, like monitoring the usual login times, performing an unusually high number of actions in a time range, or specific files being modified or accessed, and so on.
In short, rules will allow your security admins to specify what to watch for in logs to automatically raise an alert when those specific events occur.

Predefined Rules

The product offers a set of built-in rules that will help you get started with threat detection and security analysis of your enterprise network. These pre-defined rules are tailored to meet all the criteria of some of the most common threat patterns like privilege escalations, malware indicators, etc.
From a user's point of view, these rules not only save your time but also serve as templates for you to clone and customize as per your organization's growing needs via custom rule creation. Fine-tune the anomaly detection scope by optimizing event filter criteria, severity, specific actions to be targeted, etc.
Pre-defined rules are installed in an enabled state by default. For On-Premise (OP) deployments, there are no restrictions. However, for On-Demand (OD) deployments, if the license count is exceeded, the rules will be installed in a disabled state.Rule enablement on installation:

- High-severity rules are enabled by default after installation, provided a valid license is available.
- Rules that require high computational resources will also be enabled automatically.
- Standard rules are enabled by default.

Types of Rules

There are three categories of rules provided:

- Standard Rules
  Standard rules are simple rules which serve the purpose of filtering and identifying specific events based on the action chosen in the configuration.
- Anomaly Rules
  These rules are single-event/action based rules that leverage the anomaly model. They trigger when the specified event or action exceeds the configured limit or violates the conditions defined in the anomaly model.
- Advanced Rules
  These are rules whose scope of anomaly detection is broader as they are configured with a set of sequential events/actions that serve as the criteria. These rules are designed to detect complex, multi-step attack patterns.

How does rule management logic guide anomaly detection?

The UEBA engine uses rule management logic to scan for anomalies in two ways:

- Real-time, as soon as event logs are collected. For this, Real-time anomaly detection (RT) must be enabled.

- Scheduled logs, by default, are scheduled for intervals of one hour each. Therefore, all the logs in the span of the past hour will be forwarded for anomaly detection.
- Intelligent mode: When an anomaly action is selected, the rule's default execution mode is set to Intelligent.

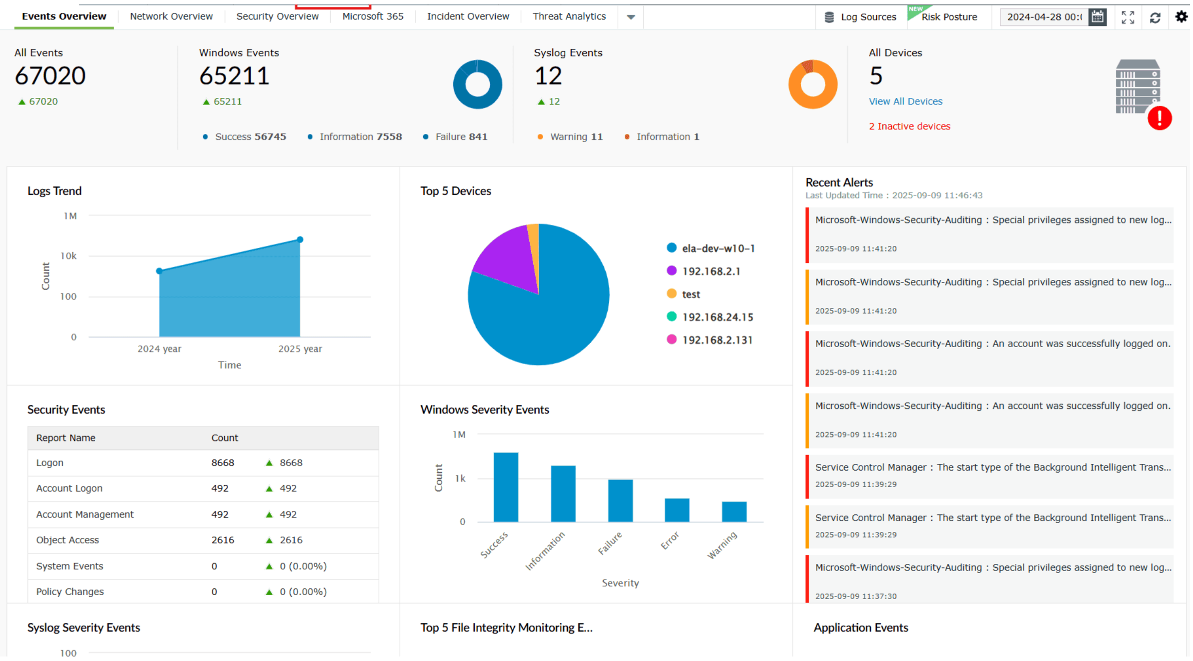
1. Event ingestion: Event logs are collected by the log collector in real-time (or in scheduled batches.)
2. Event queuing: The incoming events are parsed and then queued for analysis.
3. Rule evaluation: Each queued event is analyzed by the ML model against the currently active set of rules. Anomaly rules test the events the anomaly models configured in the rules, while Advanced rules are inclusive of multiple actions or criteria or; sequences linked to multiple actions.
4. Anomaly detection and risk scoring: The ML model uses the behavioral baselines it gathered during its training phase in order to detect anomalies, if any. Any match of events with the active rules contributes to the risk score attribution to the users and entities associated with those events.

In this way, rule management ensures that relevant anomalies are triggered as soon as such events are logged and the configured behavioral patterns and thresholds are matched

How to configure rules?

To configure the rules, follow the below steps:

1. In the product console, navigate to the Security tab. You will be taken to the Security Analytics Overview sub-tab.



Security Events

Report Name	Count	
Logon	8668	▲ 8668
Account Logon	492	▲ 492
Account Management	492	▲ 492
Object Access	2616	▲ 2616
System Events	0	▲ 0 (0.00%)
Policy Changes	0	▲ 0 (0.00%)

Recent Alerts
Last Updated Time : 2025-09-09 11:46:43

Microsoft-Windows-Security-Auditing : Special privileges assigned to new log...
2025-09-09 11:41:20

Microsoft-Windows-Security-Auditing : Special privileges assigned to new log...
2025-09-09 11:41:20

Microsoft-Windows-Security-Auditing : An account was successfully logged on.
2025-09-09 11:41:20

Microsoft-Windows-Security-Auditing : An account was successfully logged on.
2025-09-09 11:41:20

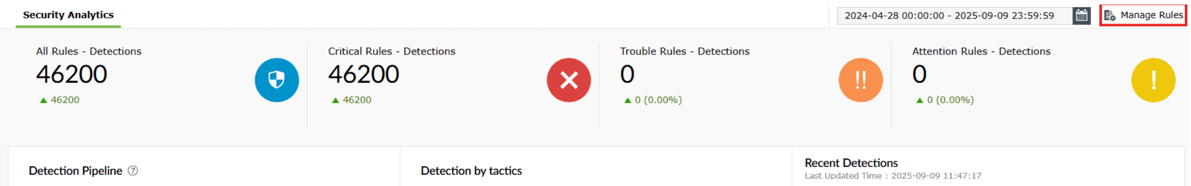
Service Control Manager : The start type of the Background Intelligent Trans...
2025-09-09 11:39:29

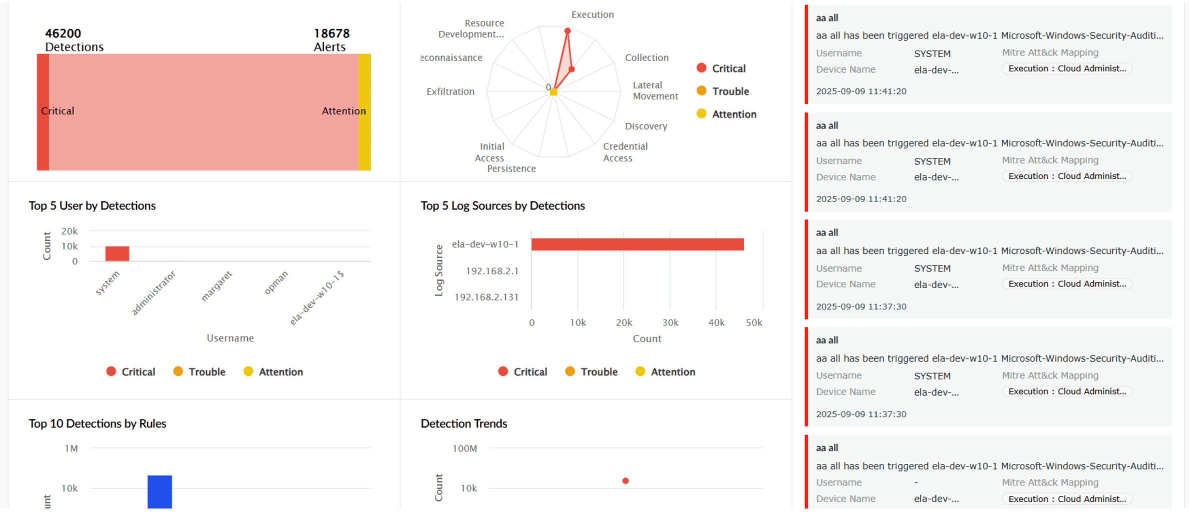
Service Control Manager : The start type of the Background Intelligent Trans...
2025-09-09 11:39:29

Microsoft-Windows-Security-Auditing : Special privileges assigned to new log...
2025-09-09 11:37:30

Image 1: Security tab in dashboard

2. Click on the Manage Rule button on the extreme right of the sub-tabs ribbon.





aa all
aa all has been triggered ela-dev-w10-1 Microsoft-Windows-Security-Auditi...
Username SYSTEM Mitre Att&ck Mapping
Device Name ela-dev-... Execution : Cloud Administ...
2025-09-09 11:41:20

aa all
aa all has been triggered ela-dev-w10-1 Microsoft-Windows-Security-Auditi...
Username SYSTEM Mitre Att&ck Mapping
Device Name ela-dev-... Execution : Cloud Administ...
2025-09-09 11:41:20

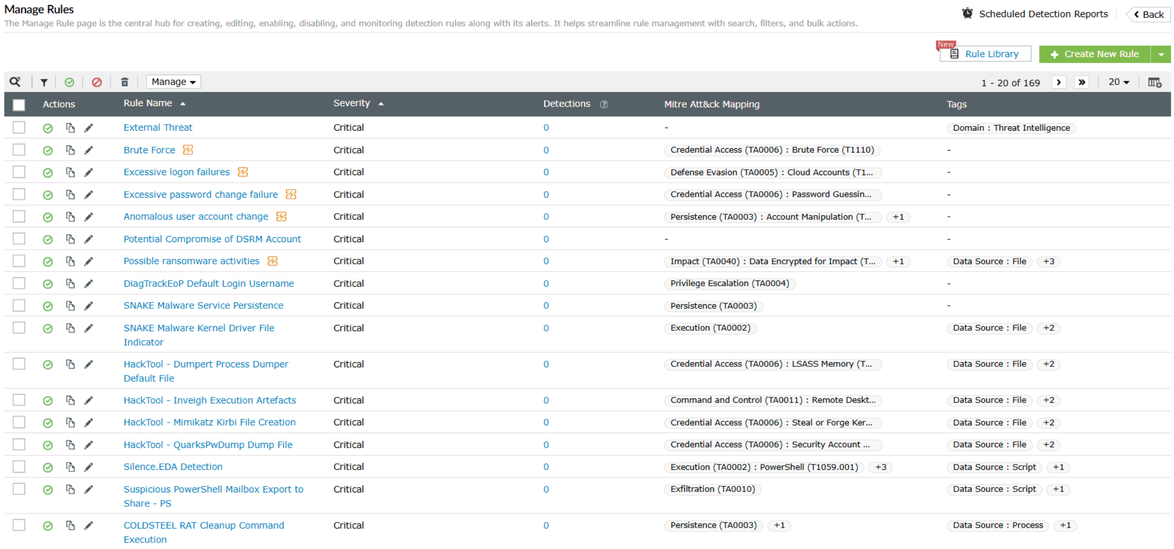
aa all
aa all has been triggered ela-dev-w10-1 Microsoft-Windows-Security-Auditi...
Username SYSTEM Mitre Att&ck Mapping
Device Name ela-dev-... Execution : Cloud Administ...
2025-09-09 11:37:30

aa all
aa all has been triggered ela-dev-w10-1 Microsoft-Windows-Security-Auditi...
Username SYSTEM Mitre Att&ck Mapping
Device Name ela-dev-... Execution : Cloud Administ...
2025-09-09 11:37:30

aa all
aa all has been triggered ela-dev-w10-1 Microsoft-Windows-Security-Auditi...
Username - Mitre Att&ck Mapping
Device Name ela-dev-... Execution : Cloud Administ...

Image 2: Manage rules in security dashboard

3. You will then be taken to the Manage Rules module. This is the centralized hub for managing rules, rule creation, editing, etc.



Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

Actions	Rule Name	Severity	Detections	Mitre Att&ck Mapping	Tags
□	External Threat	Critical	0	-	Domain : Threat Intelligence
□	Brute Force	Critical	0	Credential Access (TA0006) : Brute Force (T1110)	-
□	Excessive logon failures	Critical	0	Defense Evasion (TA0005) : Cloud Accounts (T1...	-
□	Excessive password change failure	Critical	0	Credential Access (TA0006) : Password Guessin...	-
□	Anomalous user account change	Critical	0	Persistence (TA0003) : Account Manipulation (T... +1	-
□	Potential Compromise of DSRM Account	Critical	0	-	-
□	Possible ransomware activities	Critical	0	Impact (TA0040) : Data Encrypted for Impact (T... +1	Data Source : File +3
□	DiagTrackEoP Default Login Username	Critical	0	Privilege Escalation (TA0004)	-
□	SNAKE Malware Service Persistence	Critical	0	Persistence (TA0003)	-
□	SNAKE Malware Kernel Driver File Indicator	Critical	0	Execution (TA0002)	Data Source : File +2
□	HackTool - Dumpert Process Dumper Default File	Critical	0	Credential Access (TA0006) : LSASS Memory (T...	Data Source : File +2
□	HackTool - Inveigh Execution Artefacts	Critical	0	Command and Control (TA0011) : Remote Deskt...	Data Source : File +2
□	HackTool - Mimikatz Kirbi File Creation	Critical	0	Credential Access (TA0006) : Steal or Forge Ker...	Data Source : File +2
□	HackTool - QuarksPwDump Dump File	Critical	0	Credential Access (TA0006) : Security Account ...	Data Source : File +2
□	Silence.EDA Detection	Critical	0	Execution (TA0002) : PowerShell (T1059.001) +3	Data Source : Script +1
□	Suspicious PowerShell Mailbox Export to Share - PS	Critical	0	Exfiltration (TA0010)	Data Source : Script +1
□	COLDSTEEL RAT Cleanup Command Execution	Critical	0	Persistence (TA0003) +1	Data Source : Process +1

Image 3: Manage rules module via the security dashboard

Use Cases

Template-based onboarding of rule coverage for new teams

Use case

A new business unit with similar operational workflows is onboarded into the organization's cloud environment.

With effective rule management

Administrators can clone pre-defined rules like "Unusual login location" or "Failed logons", customize them for the new users and entities, and activate those rules. Once active, the rules start monitoring activity based on the configured logic, helping speed up deployment while maintaining consistent monitoring standards across the organization.

Detecting account takeover attempts - Privilege Escalation

Use case

A user with read-only access is now suddenly involved in admin-level activities like modifying user permissions or security settings.

With effective rule management

Pre-defined rule associated with privilege escalation can be activated and tailored (if needed) with filters like device type, or role-based user group to monitor such spikes in privilege use which could be potential Insider Threat. The ML model flags such activities against the user's usual behavioral baselines, enabling a speedy remediation.

Focused Anomaly detection for critical roles or systems

Use case

The finance department is the integral aspect of an organization, demanding attention and scrutiny.

For example: Access to payroll files during non-business hours.

Scenario A- Anomaly rules: A sales user attempts to access the payroll files.

Scenario B- Advanced rules: A sales user attempts to access the payroll files, that too during non-business hours.

With effective rule management

Security admins can configure rules to be role-specific and monitor abnormal activity specifically focusing on the finance department.

The ML engine formulates and uses the baseline behavior per role to involve contextual accuracy in anomaly detection.

Read also

This document explained how rule management helps optimize anomaly detection, from using predefined rules to configuring advanced rules for complex attack patterns.

- Understanding rules
- Creating custom rules
- Query grammar
- Managing rules
- Scheduled detection reports

4.1.2.2. Understanding rules

Last updated on: September 12, 2025

In this page

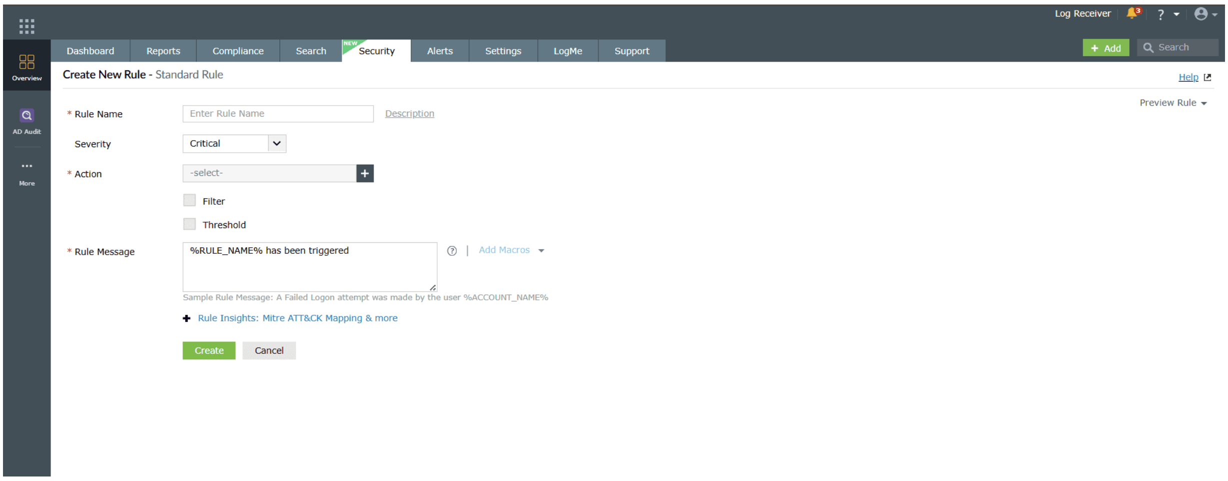
Overview

This page explains the three types of rules used in security analytics: standard rules for basic event filtering, anomaly rules for detecting unusual single-event behavior, and advanced rules for identifying complex attack sequences. Each rule type comes with configuration fields, filters, thresholds, and anomaly models to provide flexible monitoring and precise threat detection.

Standard Rules

Standard rules are basic rules that will merely identify and filter specific events from the collected logs depending on the selected action. In this simple configuration, the desired action is chosen with the optional filters or thresholds. Standard rules do not involve anomaly models or behavioral baselining. They are simply just to view and monitor log data that matched the exact conditions, so that you can focus on other events of interest.

Understanding the rule configuration fields



Create New Rule - Standard Rule

* Rule Name: Enter Rule Name

Severity: Critical

* Action: -select-

□ Filter

□ Threshold

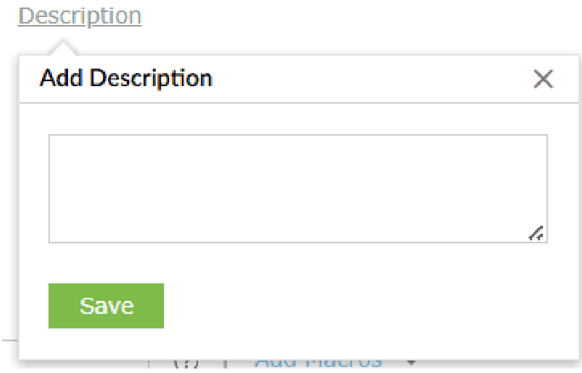
* Rule Message: %RULE_NAME% has been triggered

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

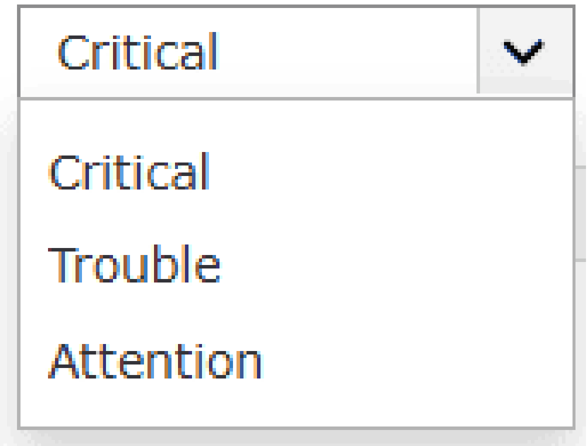
+ Rule Insights: Mitre ATT&CK Mapping & more

Image 1: Creating standard rule

- Rule Name: Give a unique name for the rule for identification.
- Description (optional): A brief explanation about the rule and its purpose.



- Severity: Choose a severity level you wish to associate this rule with. For instance, trouble level criteria indicate a moderate level of severity. The three levels of severity are:
  - Critical
  - Trouble
  - Attention

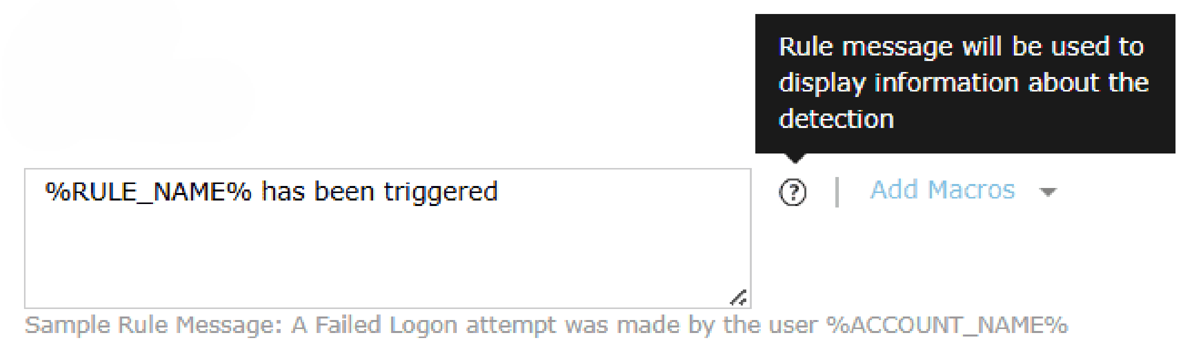


- Action: Select the log event type you want the rule to monitor. Read further for a detailed list of Log Types supported by all the three rule types associated with 600+ actions available.
  If you wish to Create Custom Action, refer to the Creating Custom rules help document.
- Filter (optional): Add one or more criteria for the log events to be filtered based upon. This will narrow down log events for rule application.

NOTE:

A maximum of only 5 filters can be set for any rule.

- Threshold (optional):
    - Define a distinct or count based event occurrence limit for repetition over a period of time. Upon exceeding the limit, the rule is triggered.
    - You can also configure Sum and Average (Avg) thresholds in addition to count-based thresholds.
    - Threshold conditions can be applied based on a group-by of specific fields, allowing more granular detection and control.
- Rule Message: Include the text you wish for the alert message to display when the rule is triggered.



Rule message will be used to display information about the detection

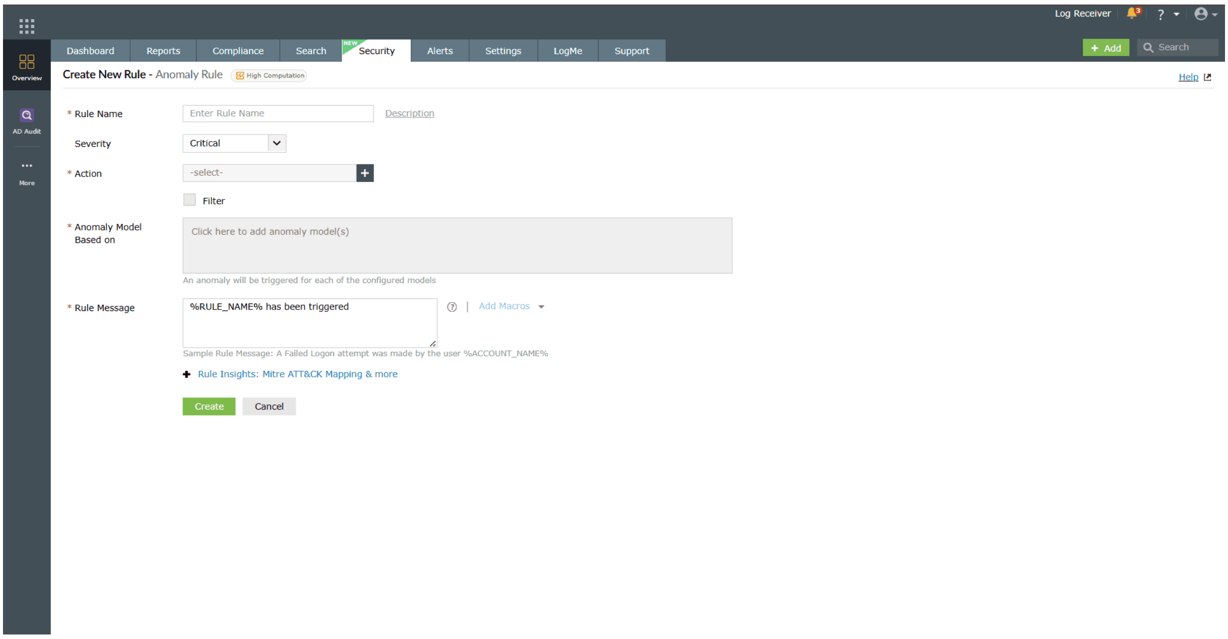
%RULE_NAME% has been triggered

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

Anomaly Rules

Anomaly rules in the rules category of security analytics are configurations specific to anomaly detection relevant to only a single action from the rule criteria. Each anomaly rule applies to one selected event type- the action. For example, "Failed File Accesses", "Account Deleted", "Group Deleted".

Understanding the rule configuration fields



Create New Rule - Anomaly Rule

* Rule Name: Enter Rule Name

Severity: Critical

* Action: -select-

□ Filter

* Anomaly Model Based on: Click here to add anomaly model(s)

An anomaly will be triggered for each of the configured models

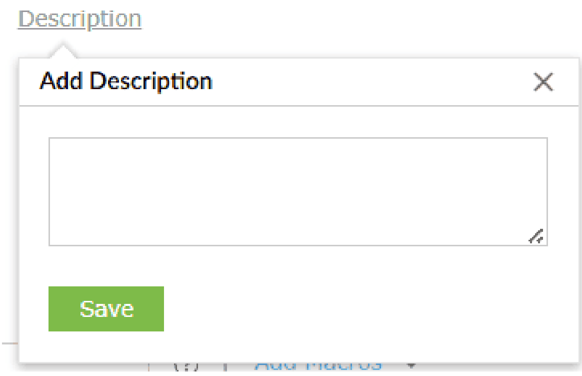
* Rule Message: %RULE_NAME% has been triggered

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

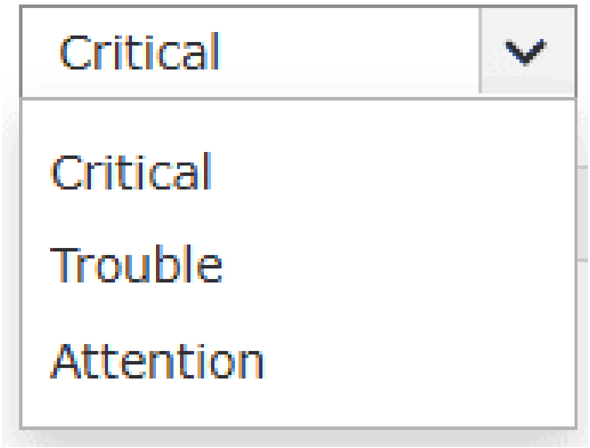
Rule Insights: Mitre ATT&CK Mapping & more

Image 2: Creating anomaly rule

- Rule Name: Give a unique name for the rule for identification.
- Description (optional): A brief explanation about the rule and its purpose.



- Severity: Choose a severity level you wish to associate this rule with. For instance, trouble level criteria indicate a moderate level of severity. The three levels of severity are:
  - Critical
  - Trouble
  - Attention

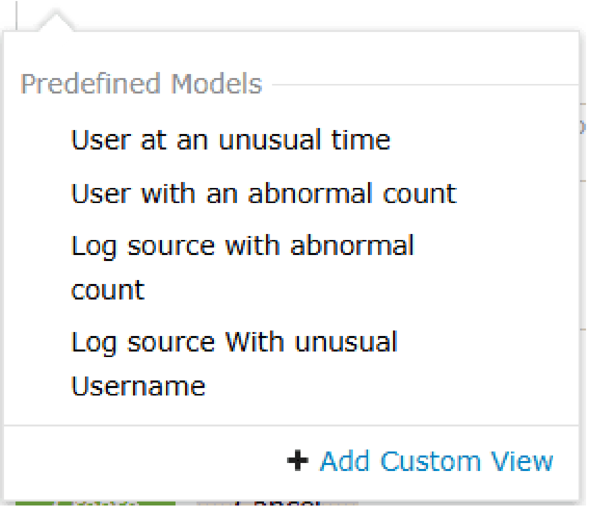


- Action: Select the log event type you want the rule to monitor. Read further for a detailed list of Log Types supported by all the three rule types associated with 600+ actions available in Log360.
  If you wish to Create Custom Action refer to the Creating custom rules help document.

> ⓘ NOTE:
>
> Only 1 action may be selected per anomaly rule.

- Filter (optional): Add one or more criteria for the log events to be filtered based upon. This will narrow down log events for rule application.

- Anomaly Model Based on: Choose the anomaly model(s) to define how deviations from normal behavior will be detected. An anomaly will be triggered for each of the configured models and two behavioral constructors - On Host, By User. There are five primary anomaly models:
  - User at an unusual time: To detect user activity that occurs outside of the user's typical login/access hours.
  - User with an abnormal count: To detect users that perform an action more or less frequently than their usual behavior.
  - Log source at an unusual time: To detect log sources that generate events outside of their usual operating hours or expected activity windows.
  - Log source with abnormal count: To detect the log sources that generate an unusually high or low volume of events.
  - Log source with unusual username: To detect the log sources associated by a certain username, which is not the one the log source is typically associated with.



Predefined Models

User at an unusual time

User with an abnormal count

Log source with abnormal count

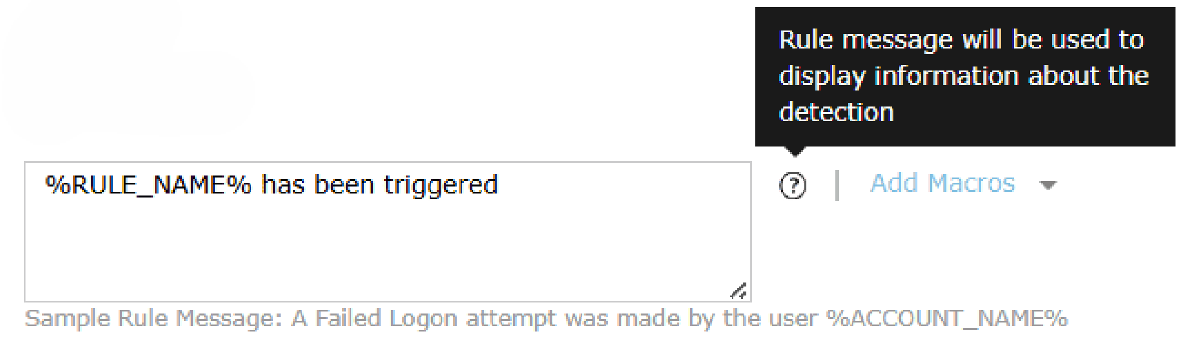
Log source With unusual Username

+ Add Custom View

ⓘ NOTE:

A maximum of only 5 anomaly models can be set for a rule.

- Rule Message: Include the text you wish for the alert message to display when the rule is triggered.



Rule message will be used to display information about the detection

%RULE_NAME% has been triggered

? | Add Macros ▾

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

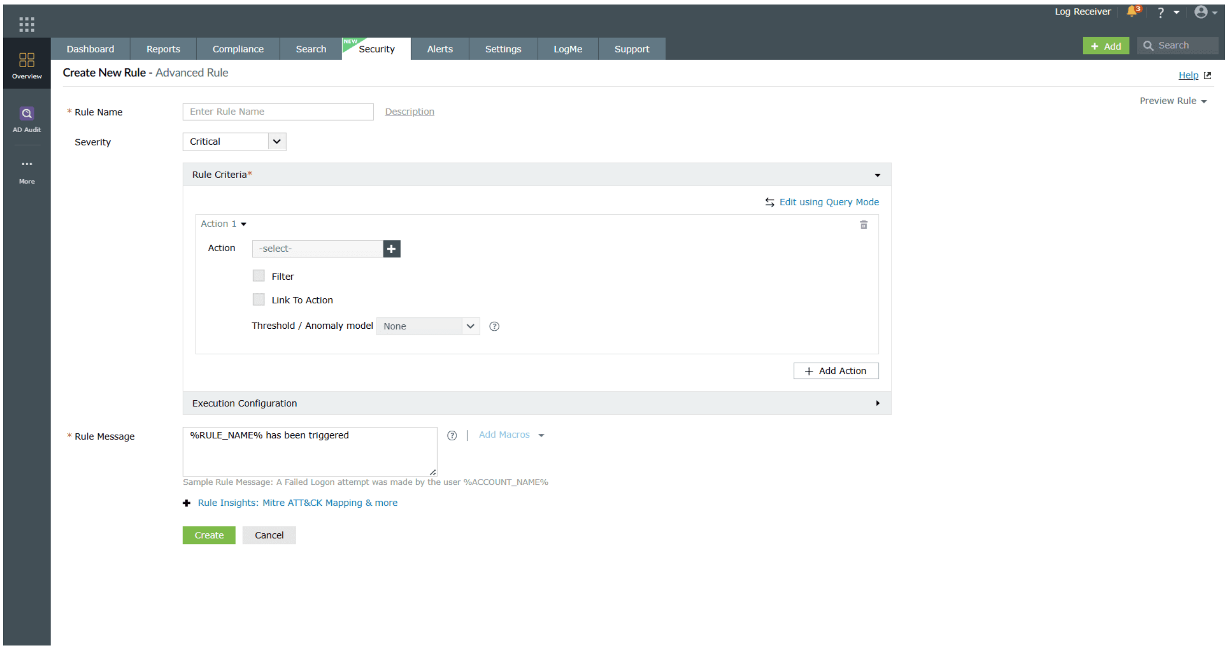
Advanced Rules

Advanced Rules

Unlike Anomaly rules that primarily focus only on a single action for anomaly detection, Advanced rules help in detection of complex, multi-step incidents by correlating sequences of events corresponding to multiple actions. Additionally, by linking actions in sequence, you can spot attack patterns that span over several event types, for instance, several logon failures followed by a successful login.

The action sequences are defined in order, and the rule will be triggered when the full pattern of actions occurs. Each action can further be fine-tuned by configuring field-based filters to narrow down the events to those meeting all specified conditions.

Understanding the rule configuration fields



Create New Rule - Advanced Rule

* Rule Name: Enter Rule Name | Description

Severity: Critical

Rule Criteria*

Action 1

Action: -select-

□ Filter

□ Link To Action

Threshold / Anomaly model: None

Execution Configuration

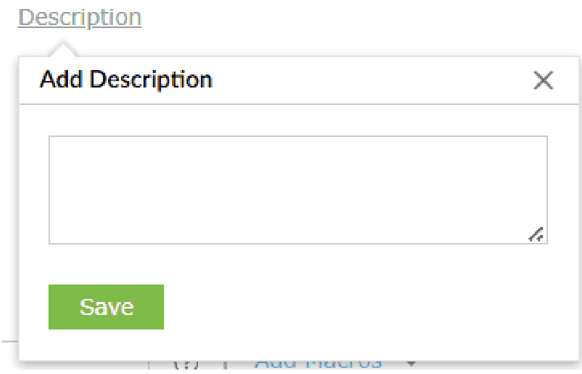
* Rule Message: %RULE_NAME% has been triggered

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

Rule Insights: Mitre ATT&CK Mapping & more

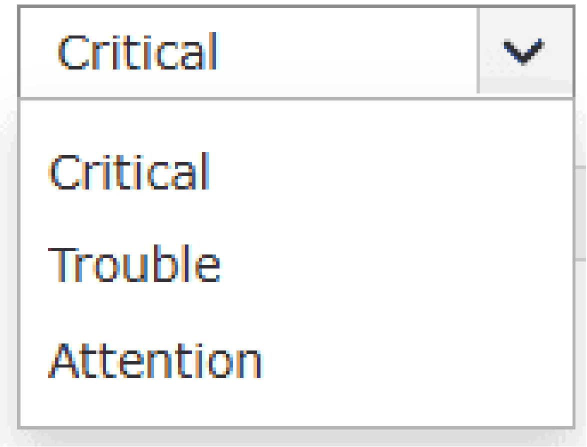
Image 3: Creating advanced rule

- Rule Name: Give a unique name for the rule for identification.
- Description (optional): A brief explanation about the rule and its purpose.



- Severity: Choose a severity level you wish to associate this rule with. For instance, trouble level criteria indicates a moderate level of severity. The three levels of severity are:
  - Critical
  - Trouble

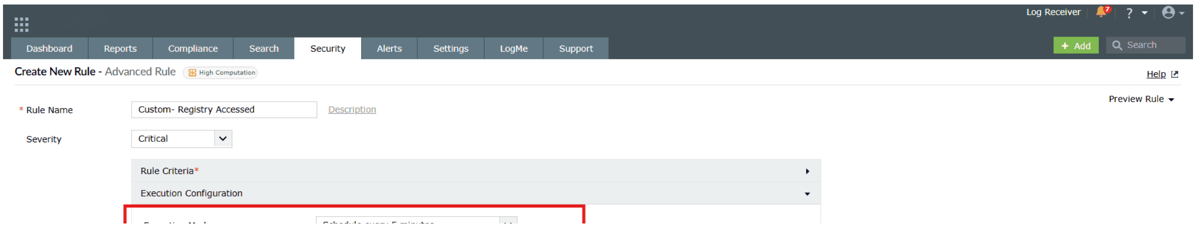
- Trouble
- Attention



- Rule Criteria
- Action: Select the log event type you want the rule to monitor. For Advanced rules, multiple actions can be selected. Read further for a detailed list of Log Types supported by all the three rule types associated with 600+ actions available in Log360.
  If you wish to Create Custom Action refer to the Creating custom rules help document
- Filter (optional): Add one or more criteria for the log events to be filtered based upon. This will narrow down log events for rule application.
- Link To Action: In the case where you have chosen multiple actions, you can link those actions to one another so that events involving those actions can be correlated and monitored for suspicious activity.
- Threshold/Anomaly model:
  - Threshold (optional): Define a distinct or count based event occurrence limit for repetition over a period of time. Upon exceeding the limit, the rule is triggered.
  - Anomaly Model: Choose the anomaly model(s) to define how deviations from normal behavior will be detected. An anomaly will be triggered for each of the configured models.

> ⓘ NOTE:
>
> Either Threshold or Anomaly Model configuration can only be selected, but not both, as they cannot function together. This limitation applies to the entire rule, with only one option allowed across all actions.

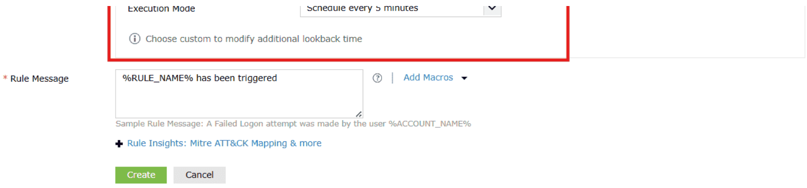
- Execution configuration: The Execution configuration option can be used in order to schedule a rule as per the requirement. This option is available only for the advanced rules.



Create New Rule - Advanced Rule High Computation

* Rule Name: Custom- Registry Accessed

Severity: Critical



Execution Mode: Schedule every 5 minutes

ⓘ Choose custom to modify additional lookback time

* Rule Message: %RULE_NAME% has been triggered

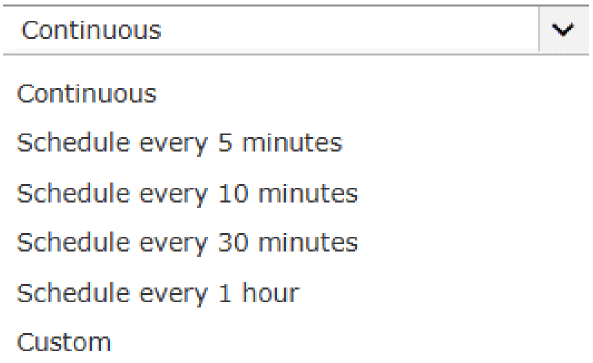
Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

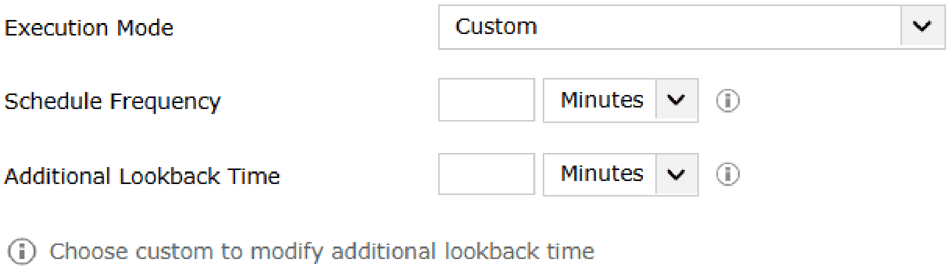
Image 4: Configuring the execution mode

This setting includes Continuous and predefined scheduled time ranges like 5 minutes, 10 minutes, 30 minutes, 1 hour along with an additional custom option, where Schedule Frequency and Additional Lookback Time will have to be configured.

ⓘ NOTE:

In case an anomaly action is selected for the rule, the execution configuration operates in the intelligent mode, wherein the execution mode will be automatically assigned based on the rule and its criteria. You cannot manually configure the execution configuration.





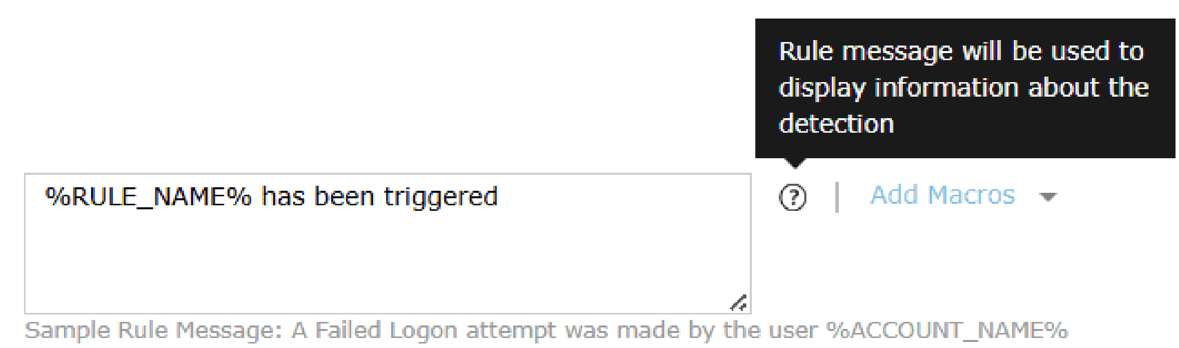
Execution Mode: Custom

Schedule Frequency: Minutes

Additional Lookback Time: Minutes

ⓘ Choose custom to modify additional lookback time

- Rule Message: Include the text you wish for the alert message to display when the rule is triggered.


Rule message will be used to display information about the detection

%RULE_NAME% has been triggered

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

Actions - Log Types supported

Below is the list of all Log Types supported by all three rule types associated with 600+ actions available in Log360.

Stormshield Device	HP Device
Topsec Device	FirePower Device
Sangfor Device	ForcePoint Device
Dell Device	H3C Device
CEF Format	pfSense Device
Malwarebytes	SNMP Trap
McAfee	IBM AS/400
Apache Access Logs	Cisco Device
DHCP linux logs	F5 Device
DHCP windows logs	Unix
MsSQL logs	FIM

MySQL Logs	FIM
MSSQL Server Logs	Threat Analytics
Terminal	Darkweb
Printer	vCenter
SAP ERP audit Logs	Hypervisor/ESXi
Oracle	FireEye
Syslog Archive File	Symantec Endpoint Protection
Syslog	Symantec DLP
Windows Archive File	Nessus
DB2 Logs	Qualys
PostgreSQL Logs	OpenVAS
Password Manager Pro	Nmap
ITOM Solution	Nexpose
ADAudit Plus	Trend Micro
ADManager Plus	IIS W3C FTP Logs
ADSelf Service Plus	IIS W3C Web Server Logs
Endpoint Central	IBM Maximo Logs

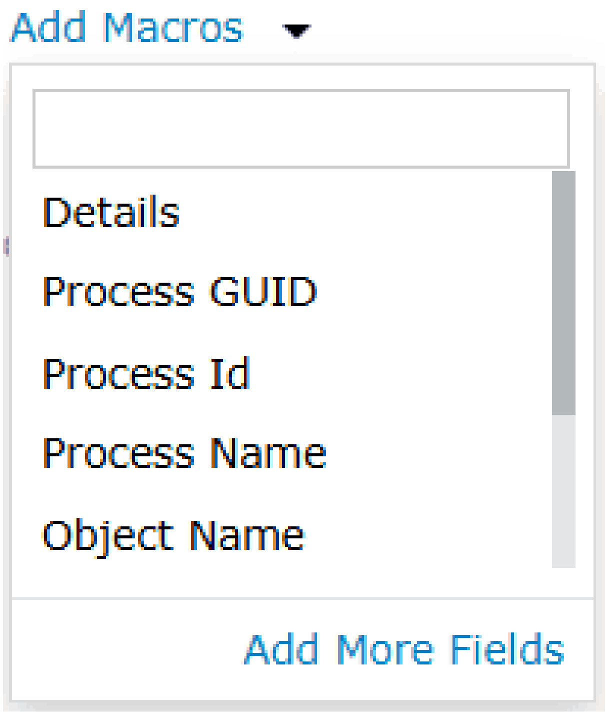
Service Desk Plus	Syslog Application
Windows	SQL Server
SonicWall Device	Sysmon
Juniper Device	AWS CloudTrail
PaloAlto Device	AWS S3
Fortinet Device	AWS ELB
CheckPoint Device	AWS ALB
Arista Device	AWS NLB
Barracuda Device	Salesforce Event Log
WatchGuard Device	Salesforce Setup Audit Trail
Sophos Device	Microsoft Entra ID
Huawei Device	Exchange Online
Meraki Device	M365 General
NetScreen Device	Sharepoint Online

If you wish to choose all the Log Types at once, click on the Select All checkbox.

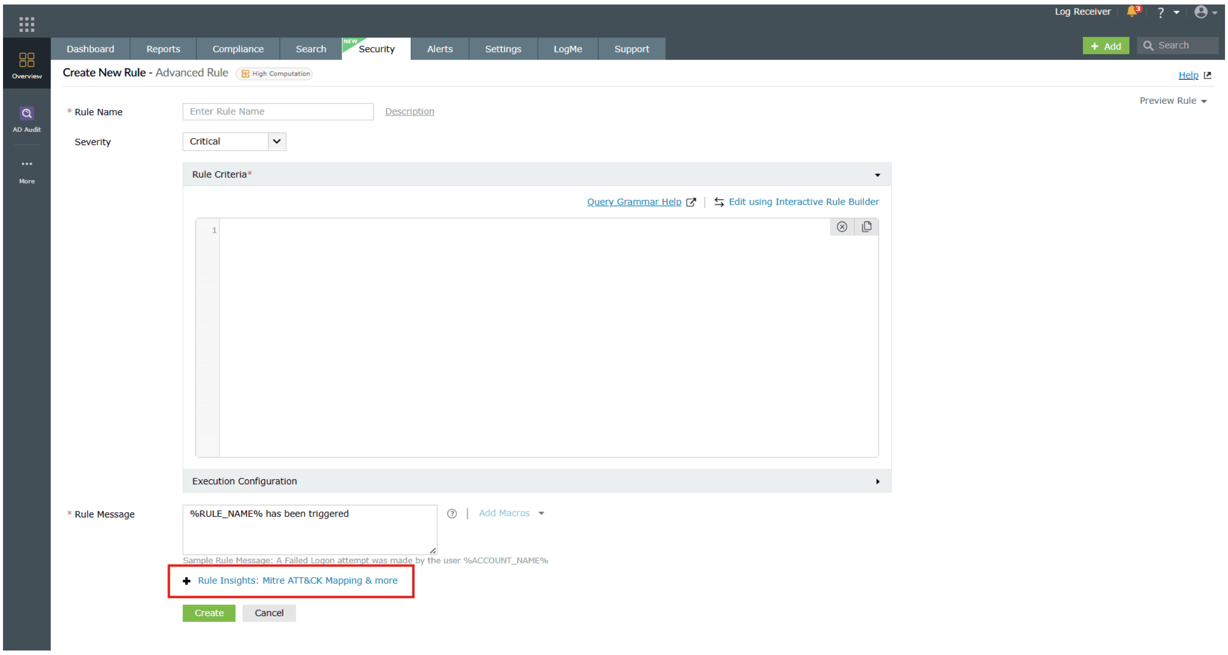
Other fields

1. Add Macros

The Macros field in all the three rule types contains the list of field names. Upon selecting one for a rule, that particular field name is used for generating the rule message when that rule is triggered. The complete field options in Macro varies from action to action that has been selected in the rule creation.



2. Rule Insights: MITRE ATT&CK Mapping & more



Create New Rule - Advanced Rule High Computation

* Rule Name: Enter Rule Name Description

Severity: Critical

* Rule Message: %RULE_NAME% has been triggered

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

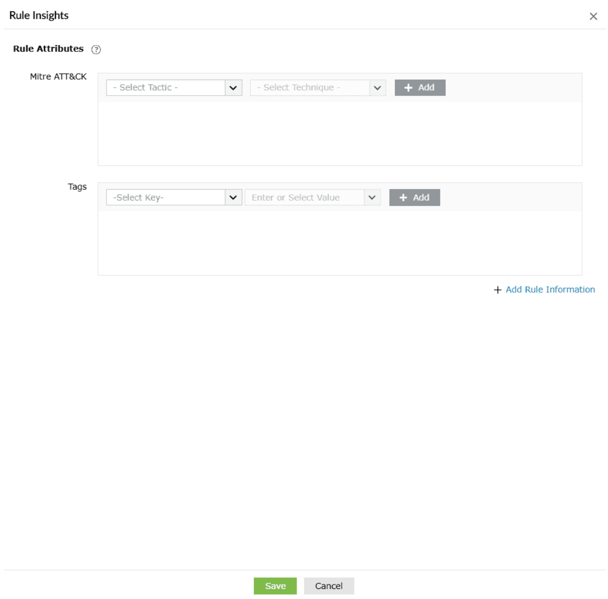
+ Rule Insights: Mitre ATT&CK Mapping & more

Image 5: Configuring the rule information

This option will help you by providing context for the selected rule by mapping it to any relevant MITRE ATT&CK techniques and tactics. You can then understand the threat behavior this rule is aligning with, in turn, aiding in threat investigation and response effectively. By providing tagging, MITRE mappings, and enriched contextual details for all rule types, the system ensures that you can create robust, organized, and actionable rules tailored to your security needs.

Clicking on it will slide open the fields box for Rule Insights

Clicking on it will slide open the fields box for Rule Insights.



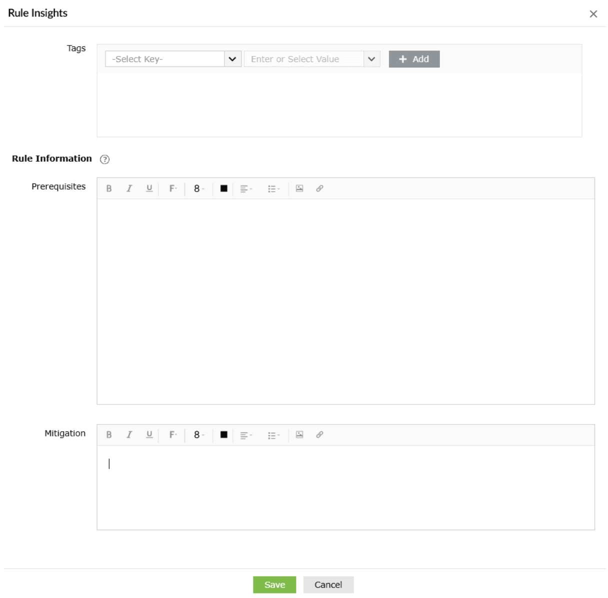
Rule Attributes

Rule Attributes enable mapping and tagging rules with specific attributes for better organization and actionable insights. They are used to help efficiently manage rules and help with data enrichment.

MITRE ATT&CK

- List of tactics will be given as a dropdown with a search option as well.
- When a tactic is selected, its associated technique will be listed in the technique dropdown.
- If a technique has a sub-technique, it will be listed under that technique.
- If both tactic and technique are selected, an Add option will be given and it will add to the list.
- Cancel icon will delete a row from the added list.

For more information, refer MITRE ATT&CK TTP(S) Framework Integration.
When you click on Add Rule Information, the below appears on the screen.

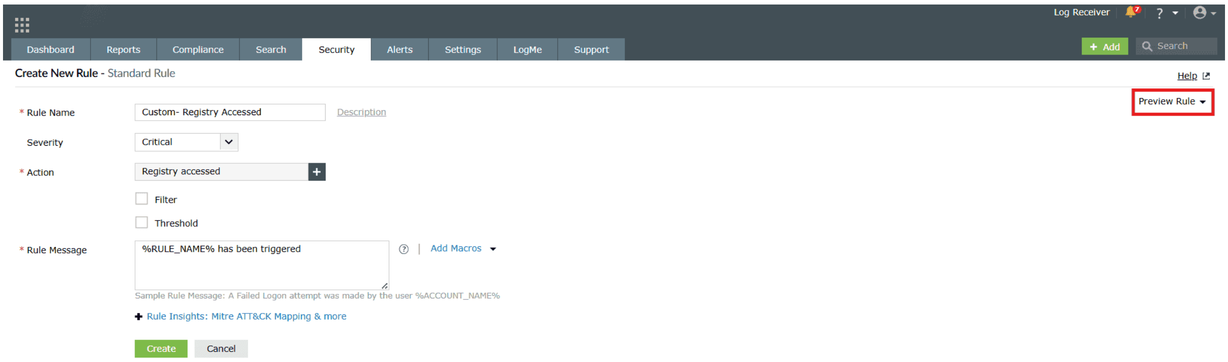


Rule information

Rule information provides additional contextual information about rule execution and mitigation strategies. It helps technicians make configuration changes and take preventive actions to enhance detections and keep the environment secure.

- Prerequisites
  - Prerequisites define the conditions or requirements that must be in place for a security rule to work effectively. They ensure that the rule can function as intended and produce accurate detections.
  - This will be shown in the Security Rule's reports page when there is no data found for this particular report, and also in the Rule summary drilldown.
- Mitigation
  - Mitigation outlines the steps to respond to or neutralize threats detected by the security rule. It provides actionable guidance to minimize the impact of a security event.

2. Preview Rule



Create New Rule - Standard Rule

* Rule Name: Custom- Registry Accessed

Severity: Critical

* Action: Registry accessed

□ Filter

□ Threshold

* Rule Message: %RULE_NAME% has been triggered

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

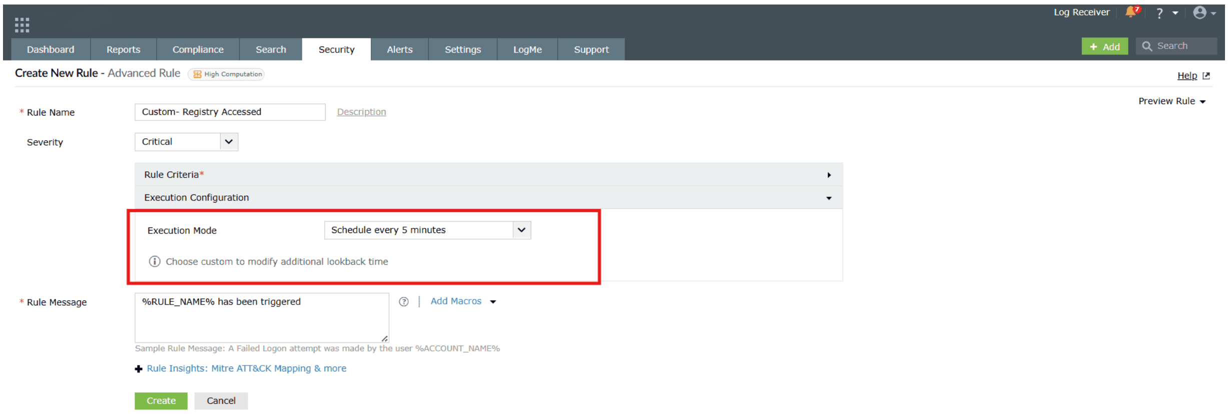
+ Rule Insights: Mitre ATT&CK Mapping & more

Image 6: Rule preview option of a rule

- The Preview Rule option is visible only after an action is selected in the rule configurations.
- You can also have an option to select a date range via the calendar.
- If additional criteria is added or removed, the preview can be reloaded using the reload preview option.
- Detection reports will only be applicable for the data triggered after the rule is created, but the preview rule will be based on the already collected logs as well.

- In Advanced Rule creation, the overall rule preview will be displayed first, and you can then switch to corresponding action previews, if needed.

Execution mode: Differences in operator modes (Continuous vs. Scheduled)



Create New Rule - Advanced Rule

* Rule Name: Custom- Registry Accessed

Severity: Critical

Rule Criteria*

Execution Configuration

Execution Mode: Schedule every 5 minutes

Choose custom to modify additional lookback time

* Rule Message: %RULE_NAME% has been triggered

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

Image 7: Configuring the execution mode

Loopback time

Definition:

Loopback time is an additional period configured to extend the log search window for scheduled rules. For example, if the schedule interval is set to 5 minutes and the loopback time is also configured as 5 minutes, the system analyzes a total of 10 minutes of logs (the current 5 minutes plus the previous 5 minutes).

Purpose:

This ensures that events occurring just before the scheduled interval are also considered during rule evaluation, minimizing the risk of missing detections that span across schedule boundaries.

Disadvantage:

Enabling loopback can lead to data overlap across consecutive schedules. Since the same set of logs may be re-evaluated in multiple intervals, this may result in duplicate detections.

Standard rule (Single action rule)

Condition	Continuous Mode	Scheduled Mode

Condition	Continuous Mode	Scheduled Mode
	- Every log is analyzed.	- If the schedule runs at 11:05, the search query is initiated from 11:00 to 11:05 with that action filter.
Threshold: 10 events within 10 min (Schedule 5 min, LoopBack 0)	- If the log matches the action, data is maintained until the threshold is reached. - Maximum time to maintain un-triggered data is 24 hours. - If 100 events are received within that time, 10 detection reports are triggered.	- Threshold time is 10 min, but in this case, only 5 min logs are retrieved as per schedule execution time. - If the result has 10 or more events, the detection is triggered. - If 100 events are received, all are triggered in a single detection report. - If partial logs are received in-between schedules within the threshold time, those events will not trigger because previous schedule data is not maintained in memory.
Threshold: 10 events within 10 min (Schedule 5 min, LoopBack 5 min)	No change in the above flow.	- If the schedule runs at 11:05, the query is initiated from 10:55 to 11:05 with the action filter. - Logs from 10:55 to 11:00 are already analyzed in the previous schedule, so duplicates may occur.
Threshold: 10 events within 10 min (Schedule 30 min, LoopBack 0 min)	No change in the above flow.	- If the schedule runs at 11:30, queries are split based on schedule time divided by threshold time: - Q1=11:00–11:10, - Q2=11:10–11:20, - Q3=11:20–11:30. - If the action and threshold are matched within a query, a detection report is triggered. - If partial logs are received in-between queries within threshold time, those events will not trigger because previous query data is not maintained in memory.
Threshold: 10 events within 10 min (Schedule 25 min, LoopBack 0 min)	No change in the above flow.	Same as the above case but queries are split as: - Q1=11:00–11:10, - Q2=11:10–11:20, - Q3=11:20–11:25.
		Same as the above case but queries are split as:

Condition	Continuous Mode	Scheduled Mode
Threshold: 10 events within 10 min (Schedule 30 min, LoopBack 20 min)	No change in the above flow.	• Q1=10:40–10:50, • Q2=10:50–11:00, • Q3=11:00–11:10, • Q4=11:10–11:20, • Q5=11:20–11:30.

Advanced rule (More-than one action rule)

Condition	Continuous Mode	Scheduled Mode
Action 1: 10 events within 10 min, Followed By 5 minAction 2: 9 events within 10 min, Followed By 12 minAction 3: 5 events within 5 min (Schedule 10 min, LoopBack 0 min)	• Same as the continuous execution standard rule flow for Action 1. • Followed by working given below: • Action 2 first event (E1) must trigger within “A1.E10 time + FB1”. • Remaining events must meet Action 2 condition, then success is achieved. • Action 3 first event (E1) must trigger within “A2.E9 time + FB2”. • Remaining events must meet Action 3 threshold condition, then success is achieved. • Example :- • A1 event is triggered between time period 10:50–10:54 (E1=10:51, E10=10:54). • If A1 succeeds, A2.E1 must trigger between	• Same as the scheduled execution standard rule for Action 1. • At threshold time ≤ schedule + loopback time, a single query is generated. • Followed by working given below: • A2 threshold must be met within “A1.E1 + FB1”. • If FB1 / threshold time < 1, the followed by time is taken as max; threshold is not considered. • A3 threshold must be met within “A2.E1 + FB2”. • If FB2 / threshold time > 1 (e.g., 2.4), queries are split as below: • A3.Q1=first 5 min, • A3.Q2=second 5 min, • A3.Q3=remaining min. • If logs fall between 2 queries, events will not trigger. • If schedule time exits, events will not trigger. • Schedule working: • Queries are framed only between schedule + loopback. • Example:A1.Q1=10:50–11:00. A1.E1=10:51, remaining A1.E2–E10=10:52–10:59. • If A1 succeeds, A2 events must trigger within 10:51–10:56 (A1.E1+FB1). • If A2 succeeds, A3 events must trigger within

Condition	Continuous Mode	Scheduled Mode
	must trigger between 10:54–10:59 (Example: A2.E5=10:58, A2.E9=10:58). • If A2 succeeds, A3.E1 must trigger between 10:58–11:10. (Example: A3.E1=11:09, A3.E2=11:14).	A3.Q1=10:53–10:58 or A3.Q2=10:58–11:00. • If A3 matches one query, 1 detection is triggered. • If both queries match, 2 detections are triggered. • Reports generated: • Report 1 – A1, A2, A3Q1 events. • Report 2 – A1, A2, A3Q2 events.
Action 1: 10 events within 10 min, Followed By 25 minAction 2: 9 events within 10 min, Followed By 12 minAction 3: 5 events within 5 min (Schedule 30 min, LoopBack 20 min)	No change in the above flow.	• Schedule starts at 11:00. • A1 – Number of queries = (schedule + loopback) / A1 threshold = (30+20)/10=5.A1.Q1=10:10–10:20, then: A1.Q2=10:20–10:30, A1.Q3=10:30–10:40, A1.Q4=10:40–10:50, A1.Q5=10:50–11:00. • If events match in multiple queries, each query is considered a separate detection. • Example: A1.Q2, A1.Q3, A1. • Q5 has success data (A1.Q2.E1=10:26, A1.Q3.E1=10:34, A1.Q5.E1=10:56). • A2 – If FB1 > A2 threshold, queries are split 25/10=2.5: • A2.Q1A=10:26–10:36, • A2.Q1B=10:36–10:46, • A2.Q1C=10:46–10:51. • A2.Q2A=10:34–10:44, • A2.Q2B=10:44–10:54, • A2.Q2C=10:54–10:59. • A2.Q3A=10:56–11:00 (remaining schedule only). • If multiple queries match, each is considered a separate detection. • Example: A2.Q1B, A2.Q2B, A2.Q2C have success (a separate detection. • Example: Q2B & A1.Q3, S3: A2.Q2C & A1.Q3). • A3 – Queries split like FB1 > A2 threshold, 12/5=2.4:

Condition	Continuous Mode	Scheduled Mode
		- A3.Q1A=10:41–10:46, - A3.Q1B=10:46–10:51, - A3.Q1C=10:51–10:53. - A3.Q2A=10:53–10:58, - A3.Q2B=10:58–11:00. - A3.Q3A=10:57–11:00. - If logs fall between schedules, they will not trigger. - If all queries match, 6 detections are shown with A1 and A2 duplicate logs.

Rule specific use cases

Anomaly rules

1. Brute-Force login attempt

Use case

A service account logs 20 failed login events in a very short window of time. This is a strong indicator of an ongoing attempt for a Brute-Force or credential-stuffing attack.

With Anomaly rules

An active Anomaly rule of "Logon Failure" action paired with a count-based anomaly model aids in a rapid threat detection of account compromise attempts. As a threat response, the window for attacker(s) to pivot into the network may be blocked.

> ⓘ NOTE:
>
> In addition to the said anomaly rule, an advanced rule can take threat detection to another level by correlating the failed logins with a subsequent successful login from the same account.

2. Suspicious third-party account activity

Use case

A managed-service vendor account starts configuring changes after the usual business hours.

With Anomaly rules

"Configuration change" action could be paired with a time-based anomaly model for a focused monitoring of activities taking place during non-business hours. For instance, 9 AM to 6 PM are the usual working hours for

this user, who is now performing actions at 3 AM. Additionally, location-based anomaly model can help flag changes made from unexpected geo locations.
These deviations from the established baselines trigger an anomaly, helping the security team to investigate promptly and prevent possible credential compromise or session hijacking.

Advanced rules

1. Data Exfiltration via bulk modifications

Use case

An unauthorized user deleted or renamed large batches of files on a critical file server.
With Advanced rules
An advanced rule correlating "file deletion" actions with "bulk file rename" events along with a threshold on total file access count within a 10-minute window and filters will narrow down the scope to the unauthorized critical server access.

2. Unauthorized application deployment in QA environment

Use case

A non-DevOps user deploys/runs an unauthorized executable in a staging environment.
With Advanced rules
An advanced rule correlating "executable creation" with "scheduled task creation" on QA-tagged machines and filters on user roles with a threshold on event sequence within 10 minutes flags such unauthorized deployment activity early on.
Read also
This document explained how standard, anomaly, and advanced rules work, their configuration options, and practical use cases such as brute-force attempts, suspicious account activity, and data exfiltration.

- Rule management overview
- Creating custom rules
- Query grammar
- Managing rules
- Scheduled detection reports

4.1.2.3. Creating custom rules

Last updated on: September 12, 2025

In this page

Overview

This page explains the process of building custom rules to detect security events. You can create standard rules for basic filtering, anomaly rules for unusual single-event behavior, or advanced rules for complex multi-step patterns. Each rule type supports fields like severity, filters, thresholds, anomaly models, and MITRE ATT&CK mappings to add context and make detections more actionable.

Rule creation

Functionality:

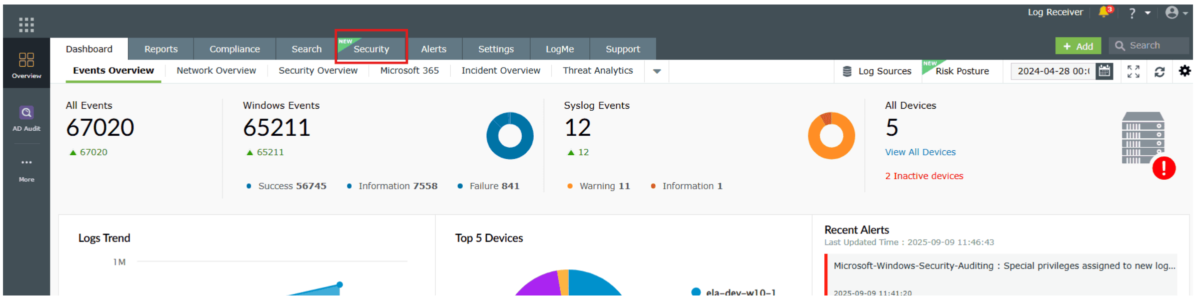
A simple and robust way of building security rules that are required for their environment.

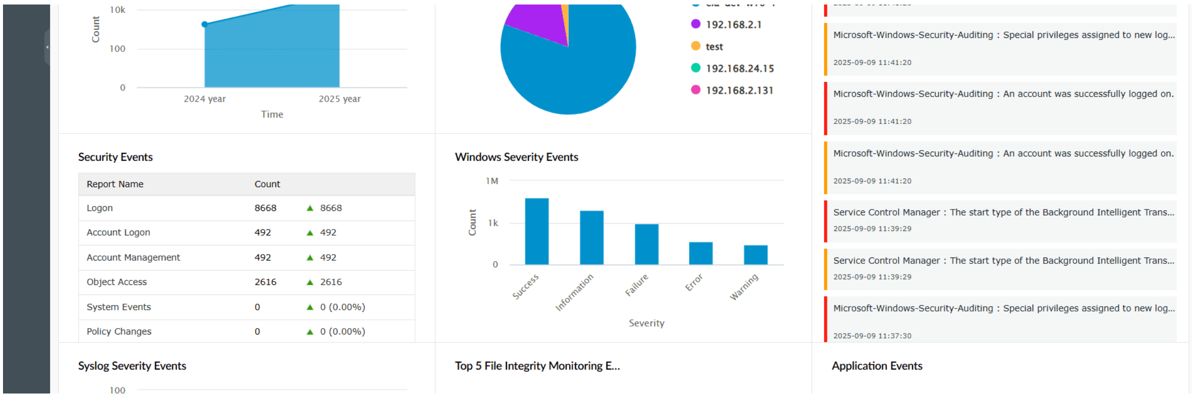
Use case:

To create security rules of any type (standard, anomaly-based, or advanced) with detailed tagging, MITRE ATT&CK mappings, and additional context like prerequisites and mitigations for better organization and actionable insights.

How to create a new rule?

1. In the product console, click on the Security tab.





Security Events

Report Name	Count	
Logon	8668	▲ 8668
Account Logon	492	▲ 492
Account Management	492	▲ 492
Object Access	2616	▲ 2616
System Events	0	▲ 0 (0.00%)
Policy Changes	0	▲ 0 (0.00%)

Microsoft-Windows-Security-Auditing : Special privileges assigned to new log...
2025-09-09 11:41:20

Microsoft-Windows-Security-Auditing : An account was successfully logged on.
2025-09-09 11:41:20

Microsoft-Windows-Security-Auditing : An account was successfully logged on.
2025-09-09 11:41:20

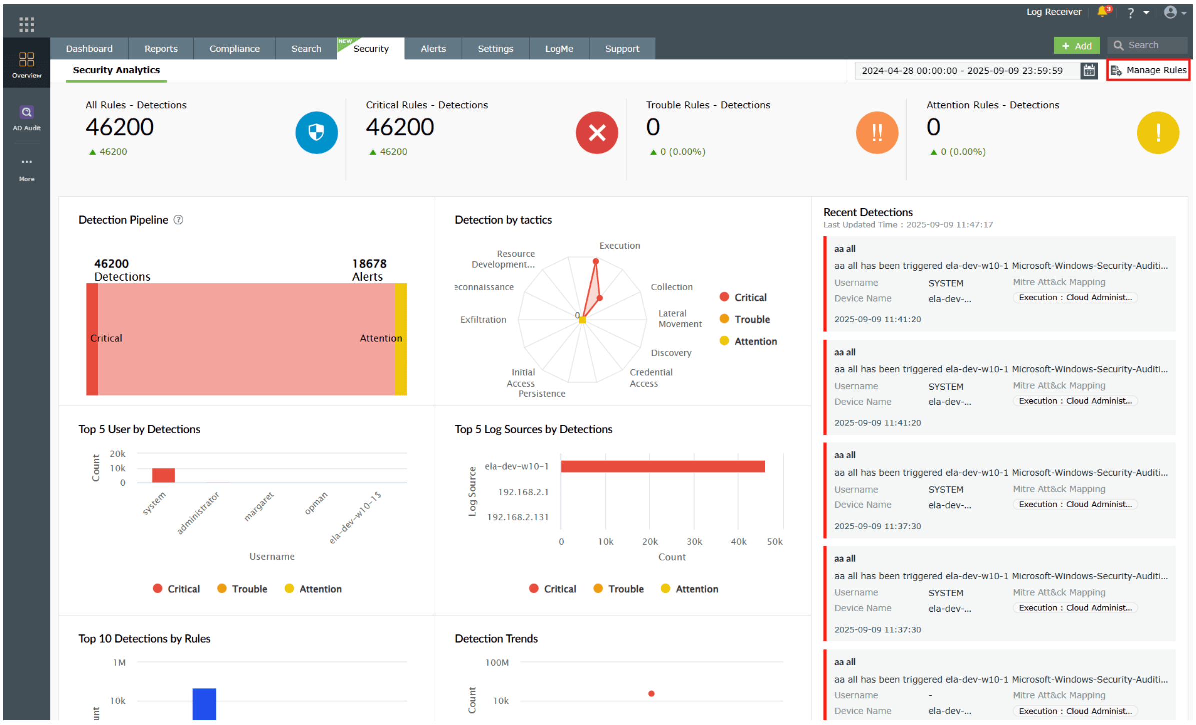
Service Control Manager : The start type of the Background Intelligent Trans...
2025-09-09 11:39:29

Service Control Manager : The start type of the Background Intelligent Trans...
2025-09-09 11:39:29

Microsoft-Windows-Security-Auditing : Special privileges assigned to new log...
2025-09-09 11:37:30

Image 1: Security tab in dashboard

2. Click on the Manage Rule option in the right end.



All Rules - Detections
46200
▲ 46200

Critical Rules - Detections
46200
▲ 46200

Trouble Rules - Detections
0
▲ 0 (0.00%)

Attention Rules - Detections
0
▲ 0 (0.00%)

Recent Detections
Last Updated Time : 2025-09-09 11:47:17

aa all
aa all has been triggered ela-dev-w10-1 Microsoft-Windows-Security-Auditi...
Username SYSTEM Mitre Att&ck Mapping
Device Name ela-dev-... Execution : Cloud Administ...
2025-09-09 11:41:20

aa all
aa all has been triggered ela-dev-w10-1 Microsoft-Windows-Security-Auditi...
Username SYSTEM Mitre Att&ck Mapping
Device Name ela-dev-... Execution : Cloud Administ...
2025-09-09 11:41:20

aa all
aa all has been triggered ela-dev-w10-1 Microsoft-Windows-Security-Auditi...
Username SYSTEM Mitre Att&ck Mapping
Device Name ela-dev-... Execution : Cloud Administ...
2025-09-09 11:37:30

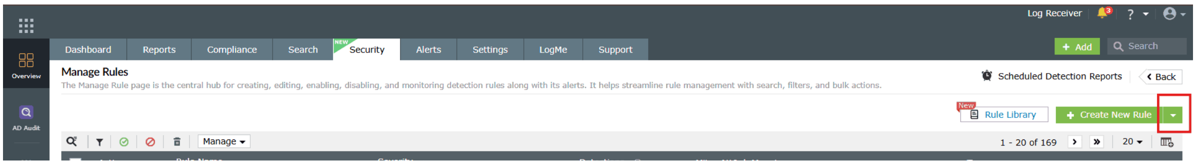
aa all
aa all has been triggered ela-dev-w10-1 Microsoft-Windows-Security-Auditi...
Username SYSTEM Mitre Att&ck Mapping
Device Name ela-dev-... Execution : Cloud Administ...
2025-09-09 11:37:30

aa all
aa all has been triggered ela-dev-w10-1 Microsoft-Windows-Security-Auditi...
Username - Mitre Att&ck Mapping
Device Name ela-dev-... Execution : Cloud Administ...

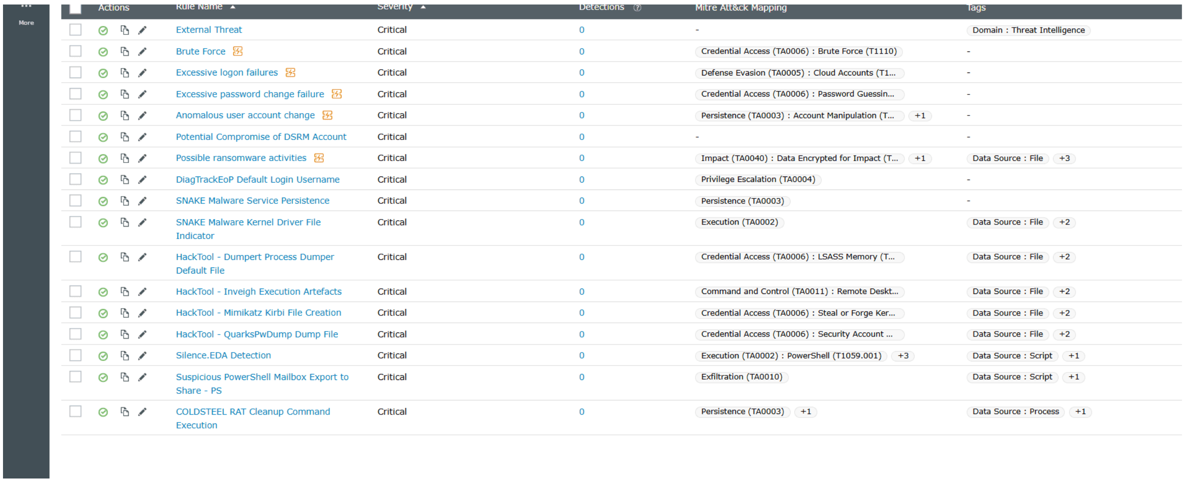
Image 2: Manage rules in security dashboard

3. You will be taken to the page with the complete list of rules. In the right side, you will find "Create New Rule". Click on the drop-down button available for this option.

> ⓘ NOTE:
>
> If you click directly on Create New Rule, you will be directly taken to the Standard Rule creation page.



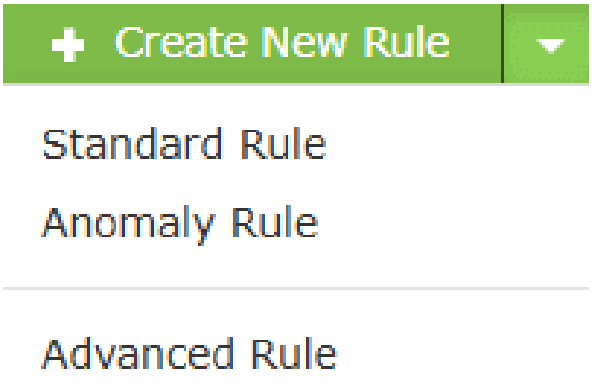
Manage Rules
The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.



□	Actions	Rule Name	Severity	Detections	Mitre Att&ck Mapping	Tags
□		External Threat	Critical	0	-	Domain : Threat Intelligence
□		Brute Force	Critical	0	Credential Access (TA0006) : Brute Force (T1110)	-
□		Excessive logon failures	Critical	0	Defense Evasion (TA0005) : Cloud Accounts (T1...	-
□		Excessive password change failure	Critical	0	Credential Access (TA0006) : Password Guessin...	-
□		Anomalous user account change	Critical	0	Persistence (TA0003) : Account Manipulation (T... +1	-
□		Potential Compromise of DSRM Account	Critical	0	-	-
□		Possible ransomware activities	Critical	0	Impact (TA0040) : Data Encrypted for Impact (T... +1	Data Source : File +3
□		DiagTrackEoP Default Login Username	Critical	0	Privilege Escalation (TA0004)	-
□		SNAKE Malware Service Persistence	Critical	0	Persistence (TA0003)	-
□		SNAKE Malware Kernel Driver File Indicator	Critical	0	Execution (TA0002)	Data Source : File +2
□		HackTool - Dumpert Process Dumper Default File	Critical	0	Credential Access (TA0006) : LSASS Memory (T...	Data Source : File +2
□		HackTool - Inveigh Execution Artefacts	Critical	0	Command and Control (TA0011) : Remote Deskt...	Data Source : File +2
□		HackTool - Mimikatz Kirbi File Creation	Critical	0	Credential Access (TA0006) : Steal or Forge Ker...	Data Source : File +2
□		HackTool - QuarksPwDump Dump File	Critical	0	Credential Access (TA0006) : Security Account ...	Data Source : File +2
□		Silence.EDA Detection	Critical	0	Execution (TA0002) : PowerShell (T1059.001) +3	Data Source : Script +1
□		Suspicious PowerShell Mailbox Export to Share - PS	Critical	0	Exfiltration (TA0010)	Data Source : Script +1
□		COLDSTEEL RAT Cleanup Command Execution	Critical	0	Persistence (TA0003) +1	Data Source : Process +1

Image 3: Manage rules module via the security dashboard

4. The drop-down expands into the Standard Rule, Anomaly Rule, and Advanced Rule options of rule creations. Click on your preferred rule type based on your requirements.

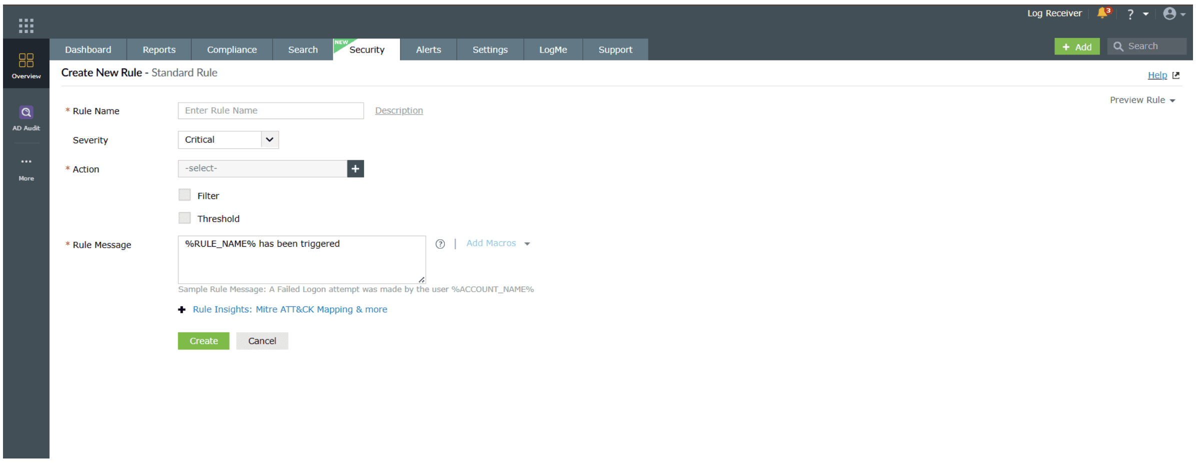


Read further on how to create a rule in each of the three rule types.

Standard Rule

Steps to create a Standard rule

1. Navigate to the Standard Rule type. You will be taken to the page consisting of fields that define the rule criteria, like in the below image. To understand more about the fields refer to the Understanding rules help document.



Create New Rule - Standard Rule

* Rule Name	Enter Rule Name Description
Severity	Critical
* Action	-select- +
	□ Filter
	□ Threshold
* Rule Message	%RULE_NAME% has been triggered ? | Add Macros

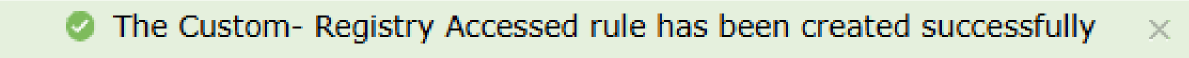
Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

+ Rule Insights: Mitre ATT&CK Mapping & more

Create Cancel

Image 4: Create a standard rule

2. Rule Name should be given, and a description for a rule is optional. Click on Description, and a popup will open for the same in case you want to add description.
3. Choose a Severity level from Critical, Trouble, and Attention. This field will be Critical by default.
4. Choose the Action based on which you wish to create the rule. Read further to know how to Create Custom Action.
   - Filter can be applied but only if a rule needs to run for just a specific case.
   - List of fields will be displayed with respect to the selected action and its log format.
   - If the list of fields exceeds 5, a search option will be shown to find and navigate to that field.
   - Threshold can be applied if a rule needs to run after a certain threshold value.
5. Rule Message can also be given to provide a formatted message across the detection reports for the triggered rule.
   - Fields in the message will be defined from Macros.
6. Rule Insights: MITRE ATT&CK Mapping & more is optional and can also be configured for a rule.
7. After entering the required fields, click on Create.
8. Upon successful completion of the action, the below pop-up appears.

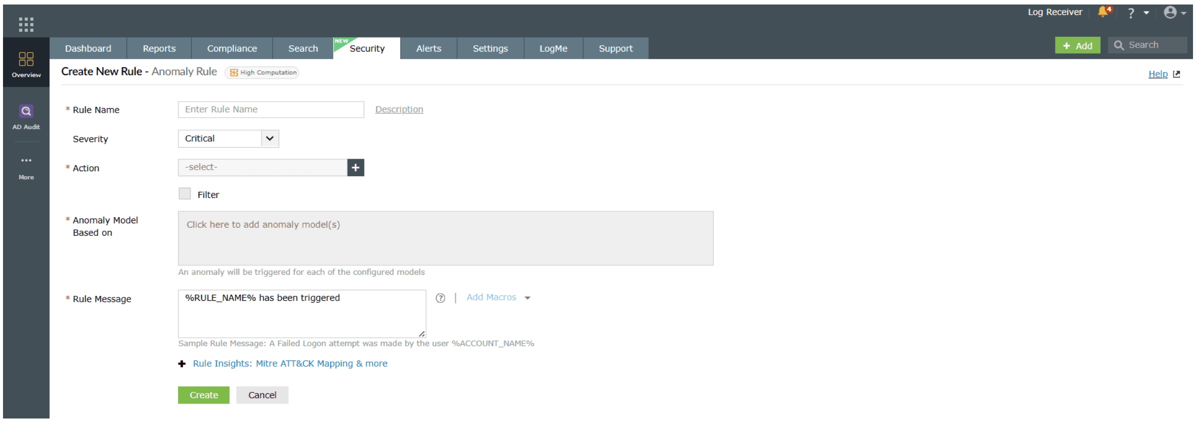


✓ The Custom- Registry Accessed rule has been created successfully ×

Anomaly Rule

Steps to create an Anomaly rule

1. Navigate to the Anomaly Rule type. You will be taken to the page consisting of fields that define the rule criteria, like in the below image. To understand more about the fields refer to the Understanding rules help document.



Create New Rule - Anomaly Rule

* Rule Name: Enter Rule Name | Description

Severity: Critical

* Action: -select-

□ Filter

* Anomaly Model Based on: Click here to add anomaly model(s)

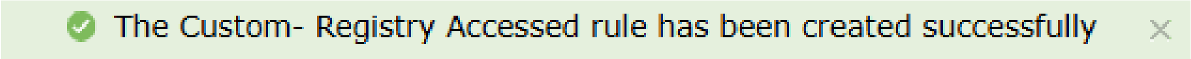
An anomaly will be triggered for each of the configured models

* Rule Message: %RULE_NAME% has been triggered

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

Image 5: Create an anomaly rule

2. Rule Name should be given, and Description for a rule is optional. Click on description, and a popup will open for the same in case you want to add description.
3. Choose a Severity level from Critical, Trouble, and Attention. This field will be Critical by default.
4. Choose the Action based on which you wish to create the rule. Read further to know how to Create Custom Action.
   - Filter can be applied but only if a rule needs to run for just a specific case.
   - List of fields will be displayed with respect to the selected action and its log format.
   - If the list of fields exceeds 5, a search option will be shown to find and navigate to that field.
   - Threshold can be applied if a rule needs to run after a certain threshold value.
5. Choose the Anomaly Model Based on to define how deviations from normal behavior will be detected. A maximum of 5 models can be selected.
6. Rule Message can also be given to provide a formatted message across the detection reports for the triggered rule. Fields in the message will be defined from Macros.
7. Rule Insights: MITRE ATT&CK Mapping & more is optional and can also be configured for a rule.
8. After entering the required fields, click on Create.
9. Upon successful completion of the action, the below pop-up appears.

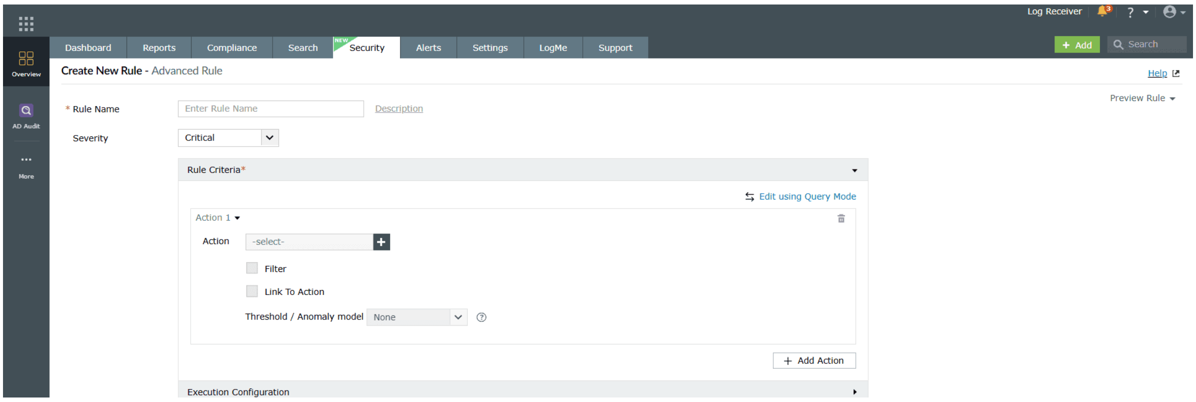


✓ The Custom- Registry Accessed rule has been created successfully ✕

Advanced Rule

Steps to create an Advanced rule

1. Navigate to the Advanced Rule type. You will be taken to the page consisting of fields that define the rule criteria, like in the below image. To understand more about the fields refer Understanding rules page.



Create New Rule - Advanced Rule

* Rule Name: Enter Rule Name — Description

Severity: Critical

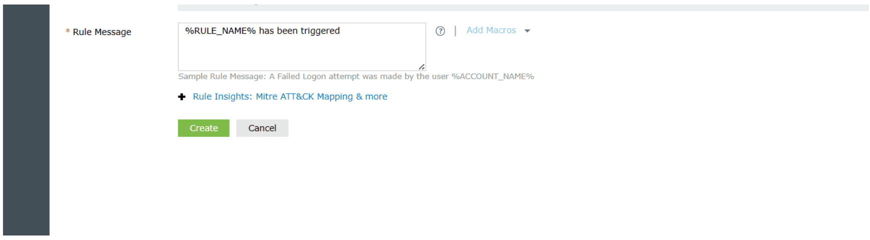
Rule Criteria*

Action: -select-

□ Filter

□ Link To Action

Threshold / Anomaly model: None



* Rule Message: %RULE_NAME% has been triggered

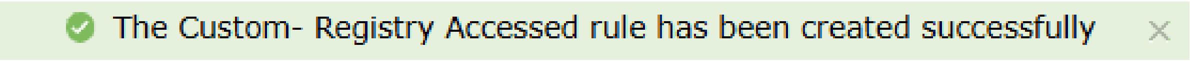
Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

+ Rule Insights: Mitre ATT&CK Mapping & more

Image 6: Create an advanced rule

2. Rule Name should be given, and Description for a rule is optional. Click on description, and a popup will open for the same in case you want to add description.
3. Choose a Severity level from Critical, Trouble, and Attention. This field will be Critical by default.
4. Rule Criteria
   Edit using Interactive Rule Builder
   - Action selection will be the same as Standard Rule creation, but multiple actions can be selected as per existing correlation rules. Read further to know how to Create Custom Action.
   - Filter and Threshold will also be the same as Standard Rule creation.
   - Link To Action: In the case where you have chosen multiple actions, you can link those actions to one another so that events involving those actions can be correlated and monitored for suspicious activity.

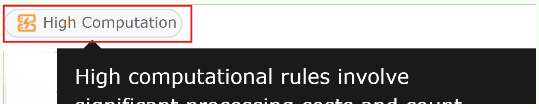
   Edit using Query Mode
   - Exclusive to advanced rule building, in this mode, you can configure the criteria and parameters by querying with the help of Query Syntax and Query Grammar for the same. Refer to Query Grammar to know more.
5. Define the Execution Configuration if you wish to schedule the rule.
6. Rule Message can also be given to provide a formatted message across the detection reports for the triggered rule.
   - Fields in the message will be defined from Macros.
7. Rule Insights: MITRE ATT&CK Mapping & more is optional and can also be configured for a rule.
8. After entering the required fields, click on Create.
9. Upon successful completion of the action, the below pop-up appears.



✓ The Custom- Registry Accessed rule has been created successfully ×

ⓘ What is a High Computation Rule?

If a threshold is applied to any rule, it will be calculated for licensing since it is highly intensive, and it will be marked as a High Computation Rule. The indicator will be visible in the rules list and also during the creation of the said rule.

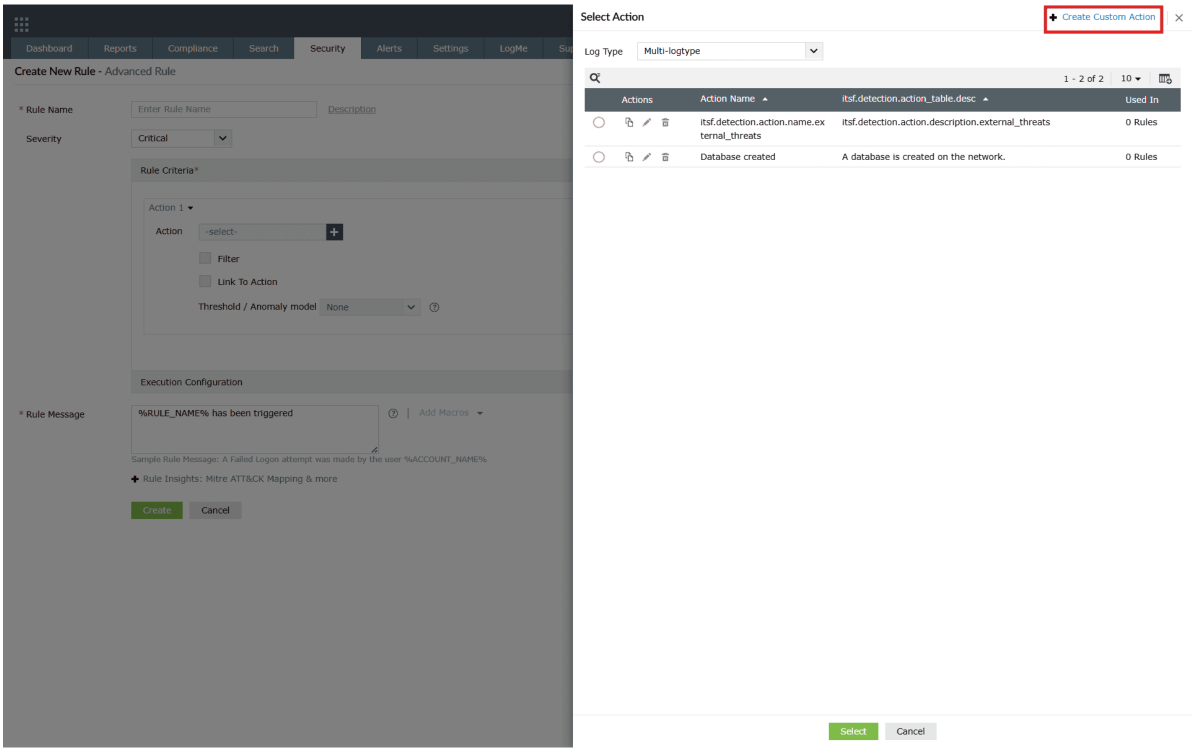


High computational rules involve significant processing costs and count

significant processing costs and count
towards your subscription. Know more

How to create Custom Action in advanced rules?

1. While choosing an Action during rule configuration, you can find an option to create a custom action as per your requirements. Click on Create Custom Action as highlighted in the below image.



Create New Rule - Advanced Rule

* Rule Name: Enter Rule Name · Description

Severity: Critical

Rule Criteria*

Action 1

Action: -select-

□ Filter

□ Link To Action

Threshold / Anomaly model: None

Execution Configuration

* Rule Message: %RULE_NAME% has been triggered · Add Macros

Sample Rule Message: A Failed Logon attempt was made by the user %ACCOUNT_NAME%

Rule Insights: Mitre ATT&CK Mapping & more

Select Action

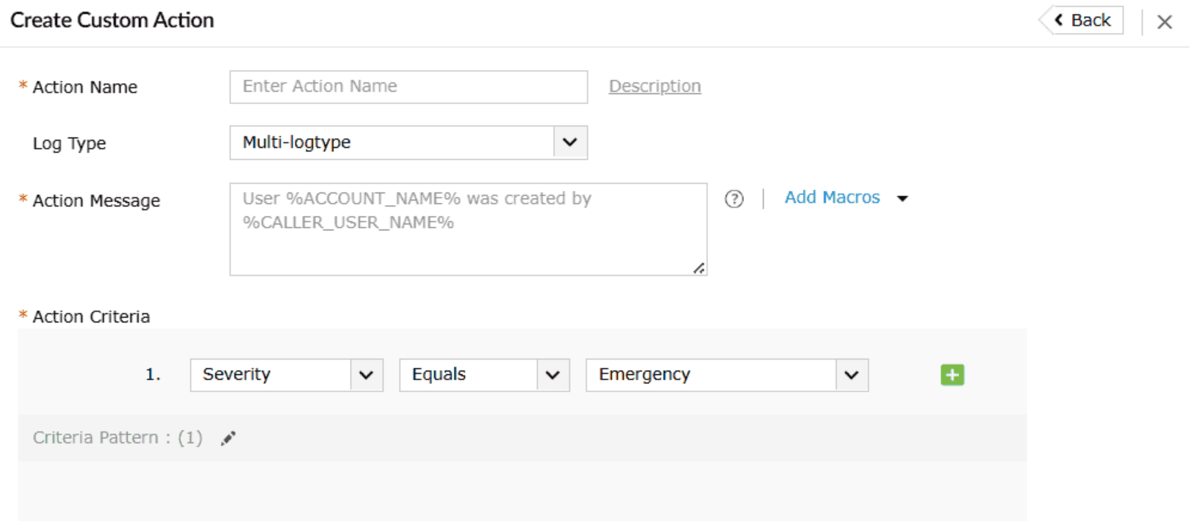
Log Type: Multi-logtype

1 - 2 of 2 · 10

	Actions	Action Name	itsf.detection.action_table.desc	Used In
○		itsf.detection.action.name.external_threats	itsf.detection.action.description.external_threats	0 Rules
○		Database created	A database is created on the network.	0 Rules

Image 7: Create custom action

2. The necessary fields to be defined will be shown as below.



Create Custom Action

* Action Name: Enter Action Name · Description

Log Type: Multi-logtype

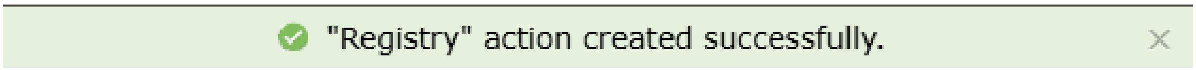
* Action Message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

* Action Criteria

1. Severity · Equals · Emergency

Criteria Pattern : (1)

3. Configure by setting the field values:
    - Action Name and Log Type are mandatory fields.
    - Description is an optional field. Click on it to view the description box.
    - Action Message is used for displaying a formatted message for the action used.
    - Macros can be added to the Action Message format.
    - Action Criteria will define the conditions which must be met for that specific action to be triggered.
    - Fields like Macros will be displayed with slight variations in the drop-down options depending upon the selected Log Type.
4. Once you have entered the required field values, click on Create.
5. Upon successful completion of the action, the below pop-up appears.



"Registry" action created successfully.

Read also

This document explained how to create new rules, configure standard, anomaly, and advanced rules, and set up custom actions for more flexible monitoring.

- Rule management overview
- Understanding rules
- Query grammar
- Managing rules
- Scheduled detection reports

4.1.2.4. Manage rules

Last updated on: September 12, 2025

In this page

Overview

This page explains how to use the Manage Rules module to oversee all detection rules in a centralized view. It covers actions such as enabling, disabling, cloning, editing, deleting, filtering, and importing/exporting rules. Each rule entry provides detailed information, including severity, MITRE ATT&CK mapping, tags, execution mode, alert profiles, and detection history. Additional features such as rule tuning, prerequisites, and mitigation steps help administrators refine detections, improve performance, and align rules with security frameworks.

Accessing the Manage Rules page

1. Navigate to the Security tab via the dashboard and click on Manage Rule as highlighted below.

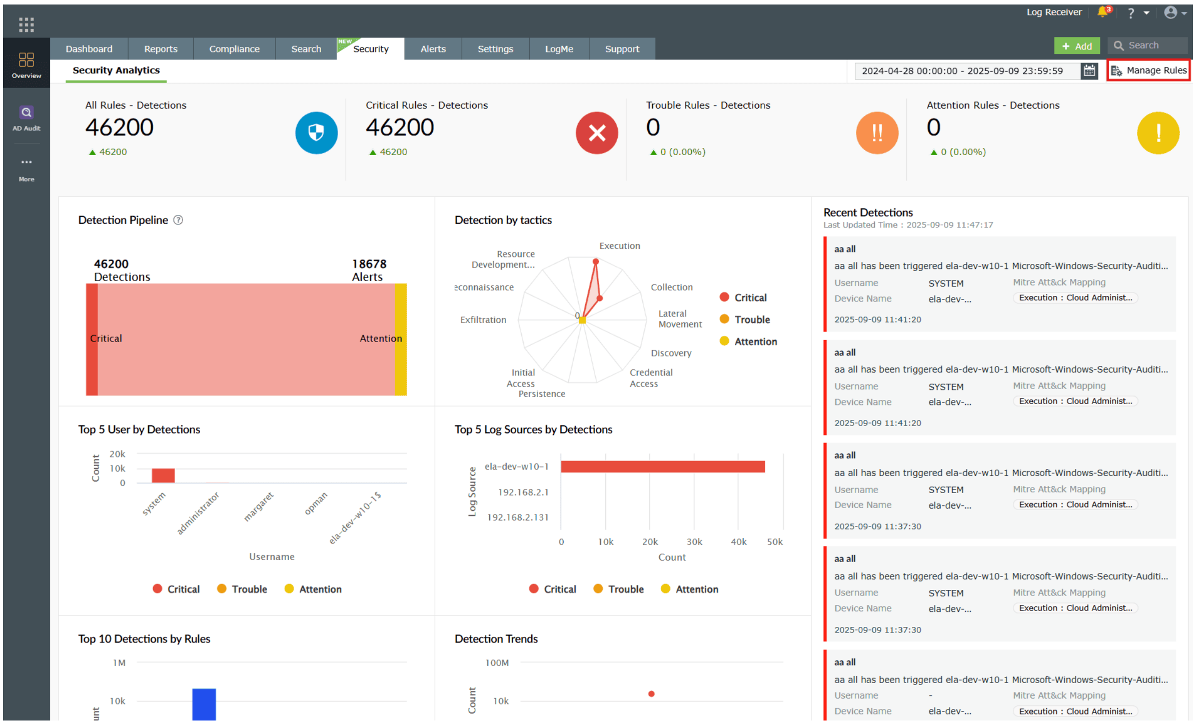
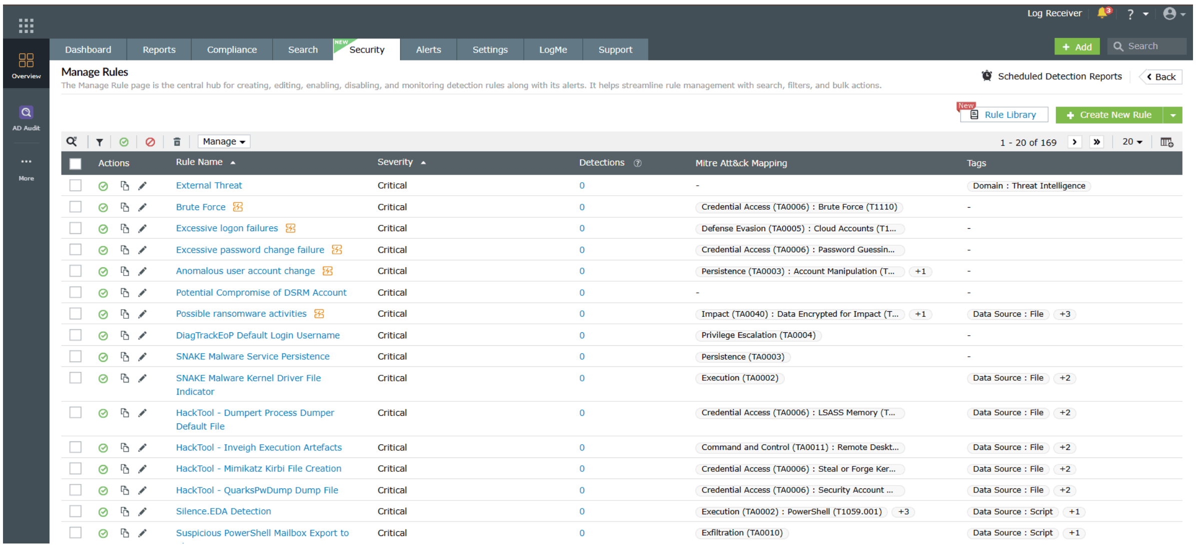


Image 1: Manage rules in security dashboard

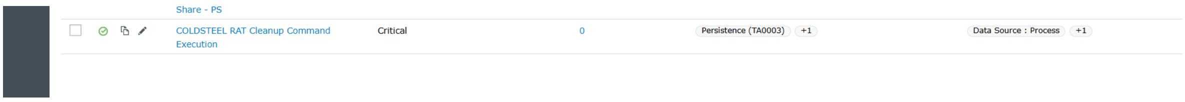
2. You will be taken to the Manage Rules page with the complete list of rules as shown in the below image. It is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.



Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

□	Actions	Rule Name ▲	Severity ▲	Detections	Mitre Att&ck Mapping	Tags
□	✓ ⎘ ✎	External Threat	Critical	0	-	Domain : Threat Intelligence
□	✓ ⎘ ✎	Brute Force	Critical	0	Credential Access (TA0006) : Brute Force (T1110)	-
□	✓ ⎘ ✎	Excessive logon failures	Critical	0	Defense Evasion (TA0005) : Cloud Accounts (T1...	-
□	✓ ⎘ ✎	Excessive password change failure	Critical	0	Credential Access (TA0006) : Password Guessin...	-
□	✓ ⎘ ✎	Anomalous user account change	Critical	0	Persistence (TA0003) : Account Manipulation (T... +1	-
□	✓ ⎘ ✎	Potential Compromise of DSRM Account	Critical	0	-	-
□	✓ ⎘ ✎	Possible ransomware activities	Critical	0	Impact (TA0040) : Data Encrypted for Impact (T... +1	Data Source : File +3
□	✓ ⎘ ✎	DiagTrackEoP Default Login Username	Critical	0	Privilege Escalation (TA0004)	-
□	✓ ⎘ ✎	SNAKE Malware Service Persistence	Critical	0	Persistence (TA0003)	-
□	✓ ⎘ ✎	SNAKE Malware Kernel Driver File Indicator	Critical	0	Execution (TA0002)	Data Source : File +2
□	✓ ⎘ ✎	HackTool - Dumpert Process Dumper Default File	Critical	0	Credential Access (TA0006) : LSASS Memory (T...	Data Source : File +2
□	✓ ⎘ ✎	HackTool - Inveigh Execution Artefacts	Critical	0	Command and Control (TA0011) : Remote Deskt...	Data Source : File +2
□	✓ ⎘ ✎	HackTool - Mimikatz Kirbi File Creation	Critical	0	Credential Access (TA0006) : Steal or Forge Ker...	Data Source : File +2
□	✓ ⎘ ✎	HackTool - QuarksPwDump Dump File	Critical	0	Credential Access (TA0006) : Security Account ...	Data Source : File +2
□	✓ ⎘ ✎	Silence.EDA Detection	Critical	0	Execution (TA0002) : PowerShell (T1059.001) +3	Data Source : Script +1
□	✓ ⎘ ✎	Suspicious PowerShell Mailbox Export to	Critical	0	Exfiltration (TA0010)	Data Source : Script +1



□	Actions	Rule Name	Severity	Detections	Mitre Att&ck Mapping	Tags
		Share - PS				
□	✓ ⎘ ✎	COLDSTEEL RAT Cleanup Command Execution	Critical	0	Persistence (TA0003) +1	Data Source : Process +1

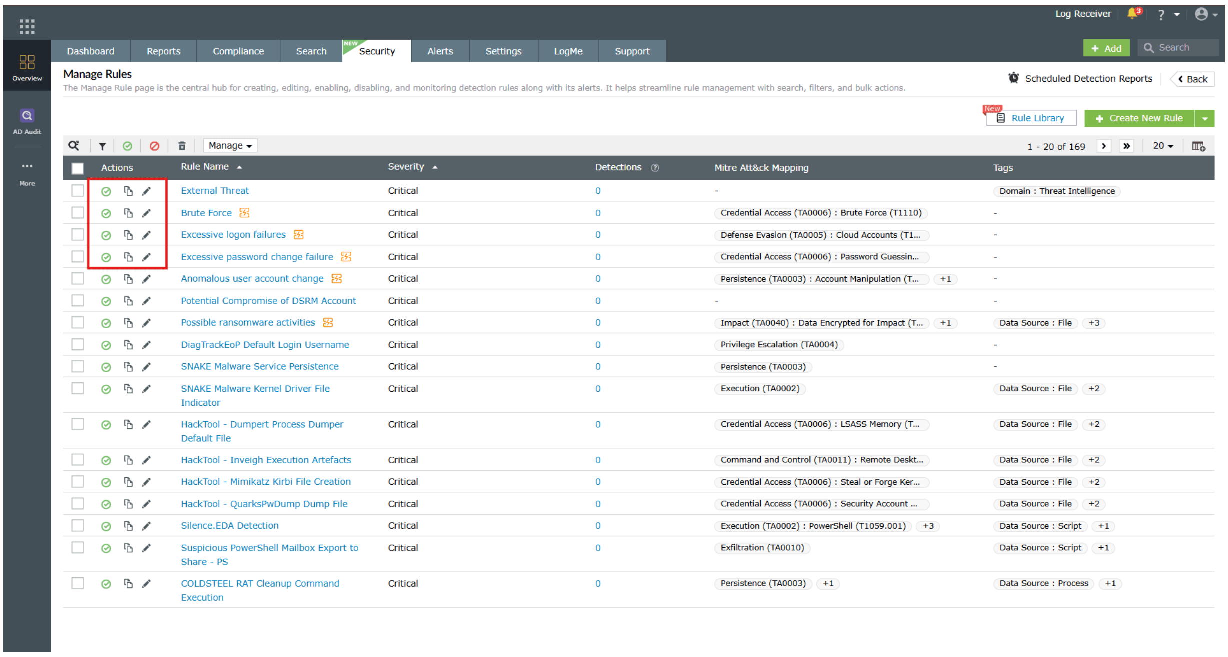
Image 2: Manage rules module via the security dashboard

Fields in the manage rules table

A. Actions column

The actions column acts as a medium for you to take required actions on the rule(s) as per your needs. Below are the available rule actions in the Manage Rules module.

- Enable/disable rules
- Clone rule
- Edit rule
- Delete rule(s)



The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

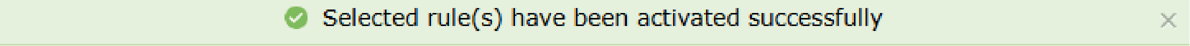
□	Actions	Rule Name	Severity	Detections	Mitre Att&ck Mapping	Tags
□	✓ ⎘ ✎	External Threat	Critical	0	-	Domain : Threat Intelligence
□	✓ ⎘ ✎	Brute Force	Critical	0	Credential Access (TA0006) : Brute Force (T1110)	-
□	✓ ⎘ ✎	Excessive logon failures	Critical	0	Defense Evasion (TA0005) : Cloud Accounts (T1...	-
□	✓ ⎘ ✎	Excessive password change failure	Critical	0	Credential Access (TA0006) : Password Guessin...	-
□	✓ ⎘ ✎	Anomalous user account change	Critical	0	Persistence (TA0003) : Account Manipulation (T... +1	-
□	✓ ⎘ ✎	Potential Compromise of DSRM Account	Critical	0	-	-
□	✓ ⎘ ✎	Possible ransomware activities	Critical	0	Impact (TA0040) : Data Encrypted for Impact (T... +1	Data Source : File +3
□	✓ ⎘ ✎	DiagTrackEoP Default Login Username	Critical	0	Privilege Escalation (TA0004)	-
□	✓ ⎘ ✎	SNAKE Malware Service Persistence	Critical	0	Persistence (TA0003)	-
□	✓ ⎘ ✎	SNAKE Malware Kernel Driver File Indicator	Critical	0	Execution (TA0002)	Data Source : File +2
□	✓ ⎘ ✎	HackTool - Dumpert Process Dumper Default File	Critical	0	Credential Access (TA0006) : LSASS Memory (T...	Data Source : File +2
□	✓ ⎘ ✎	HackTool - Inveigh Execution Artefacts	Critical	0	Command and Control (TA0011) : Remote Deskt...	Data Source : File +2
□	✓ ⎘ ✎	HackTool - Mimikatz Kirbi File Creation	Critical	0	Credential Access (TA0006) : Steal or Forge Ker...	Data Source : File +2
□	✓ ⎘ ✎	HackTool - QuarksPwDump Dump File	Critical	0	Credential Access (TA0006) : Security Account ...	Data Source : File +2
□	✓ ⎘ ✎	Silence.EDA Detection	Critical	0	Execution (TA0002) : PowerShell (T1059.001) +3	Data Source : Script +1
□	✓ ⎘ ✎	Suspicious PowerShell Mailbox Export to Share - PS	Critical	0	Exfiltration (TA0010)	Data Source : Script +1
□	✓ ⎘ ✎	COLDSTEEL RAT Cleanup Command Execution	Critical	0	Persistence (TA0003) +1	Data Source : Process +1

Image 3: Available actions in the manage rules module

Enable/Disable rules

Enabling a rule

1. Click on the disabled icon ⊘ under the Actions column to enable the rule.
2. As soon as you perform this action, the icon indicates that the rule is now enabled ✓ and the below pop-up message appears briefly.



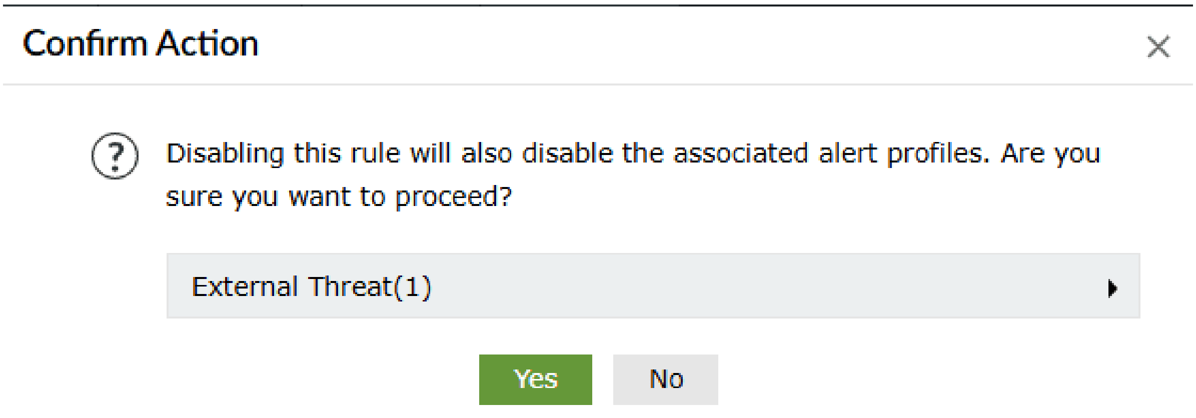
✓ Selected rule(s) have been activated successfully ×

Disabling a rule

1. Click on the enabled icon ✓ under the Actions column to disable the rule.

1. Click on the enabled icon ✓ under the Actions column to disable the rule.

2. A confirm action pop-up will appear if an alert profile is associated with the said rule. Click on Yes to proceed.

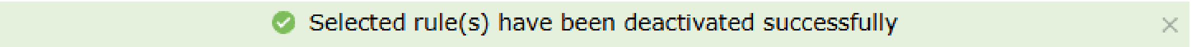


Confirm Action

Disabling this rule will also disable the associated alert profiles. Are you sure you want to proceed?

External Threat(1)

3. As soon as you perform this action, the icon indicates that the rule is now disabled ⊘ and the below pop-up message appears briefly.

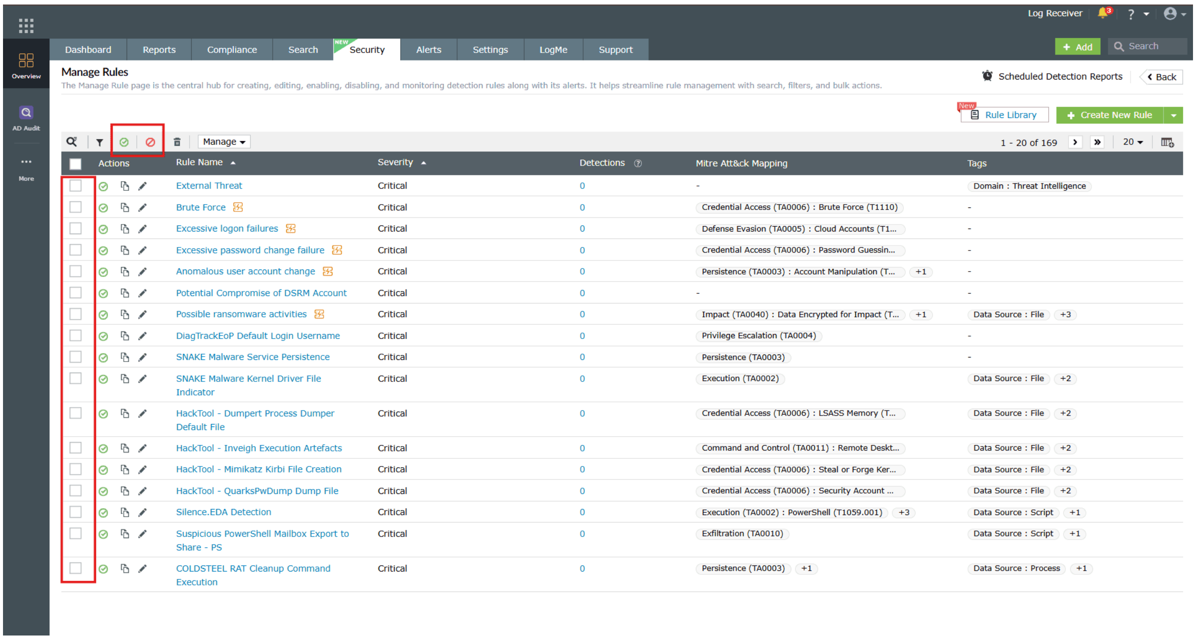


Selected rule(s) have been deactivated successfully

Enable/Disable multiple rules at once

1. Click on the empty checkbox(es) in the first column in order to select the respective rules.

2. Click on the Enable/Disable icons in the ribbon above the rules list.



Manage Rules

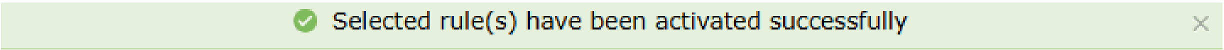
The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

□	Actions	Rule Name	Severity	Detections	Mitre Att&ck Mapping	Tags
□	✓	External Threat	Critical	0	-	Domain : Threat Intelligence
□	✓	Brute Force	Critical	0	Credential Access (TA0006) : Brute Force (T1110)	-
□	✓	Excessive logon failures	Critical	0	Defense Evasion (TA0005) : Cloud Accounts (T1...	-
□	✓	Excessive password change failure	Critical	0	Credential Access (TA0006) : Password Guessin...	-
□	✓	Anomalous user account change	Critical	0	Persistence (TA0003) : Account Manipulation (T... +1	-
□	✓	Potential Compromise of DSRM Account	Critical	0	-	-
□	✓	Possible ransomware activities	Critical	0	Impact (TA0040) : Data Encrypted for Impact (T... +1	Data Source : File +3
□	✓	DiagTrackEoP Default Login Username	Critical	0	Privilege Escalation (TA0004)	-
□	✓	SNAKE Malware Service Persistence	Critical	0	Persistence (TA0003)	-
□	✓	SNAKE Malware Kernel Driver File Indicator	Critical	0	Execution (TA0002)	Data Source : File +2
□	✓	HackTool - Dumpert Process Dumper Default File	Critical	0	Credential Access (TA0006) : LSASS Memory (T...	Data Source : File +2
□	✓	HackTool - Inveigh Execution Artefacts	Critical	0	Command and Control (TA0011) : Remote Deskt...	Data Source : File +2
□	✓	HackTool - Mimikatz Kirbi File Creation	Critical	0	Credential Access (TA0006) : Steal or Forge Ker...	Data Source : File +2
□	✓	HackTool - QuarksPwDump Dump File	Critical	0	Credential Access (TA0006) : Security Account ...	Data Source : File +2
□	✓	Silence.EDA Detection	Critical	0	Execution (TA0002) : PowerShell (T1059.001) +3	Data Source : Script +1
□	✓	Suspicious PowerShell Mailbox Export to Share - PS	Critical	0	Exfiltration (TA0010)	Data Source : Script +1
□	✓	COLDSTEEL RAT Cleanup Command Execution	Critical	0	Persistence (TA0003) +1	Data Source : Process +1

Image 4: Bulk actions in the manage rules module

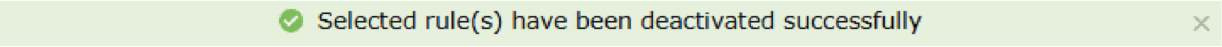
3. Upon successful completion of the action, the below pop-up appears.

When enabled:



Selected rule(s) have been activated successfully

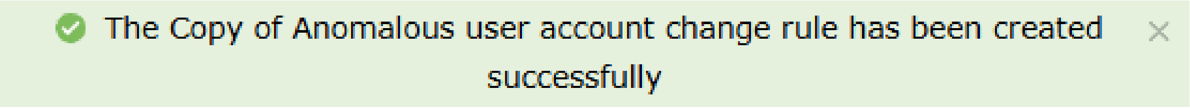
When disabled:



Selected rule(s) have been deactivated successfully

Clone a rule

1. Click on the Clone icon ⧉ under the Actions column to clone the respective rule.
2. Depending upon the rule type—Standard, Anomaly, or Advanced—you will be taken to the specific configuration page of that particular rule.
3. Make the necessary changes in the field values in order to customize the cloned rule and click on Create.
4. Upon successful completion of the action, the below pop-up appears.



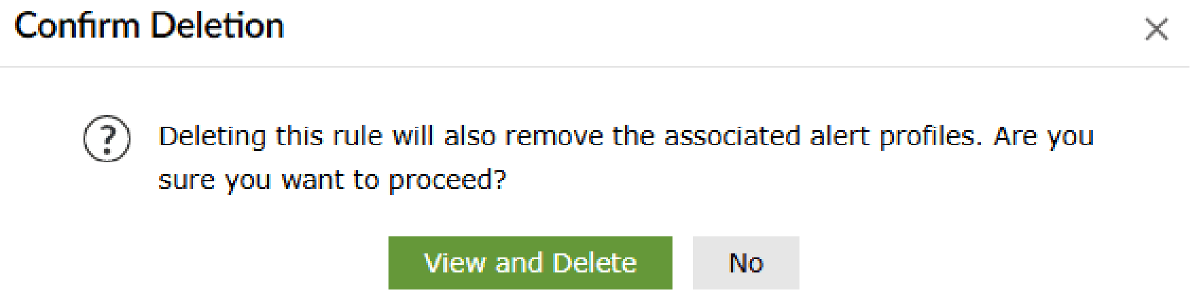
The Copy of Anomalous user account change rule has been created successfully

Edit a rule

1. Click on the Edit icon ✎ under the Actions column to edit the respective rule.
2. Depending upon the rule type—Standard, Anomaly, or Advanced—you will be taken to the specific configuration page of that particular rule.
3. Make the necessary edits in the field values and click on Update.
4. The rule will be updated instantly in the rules list.

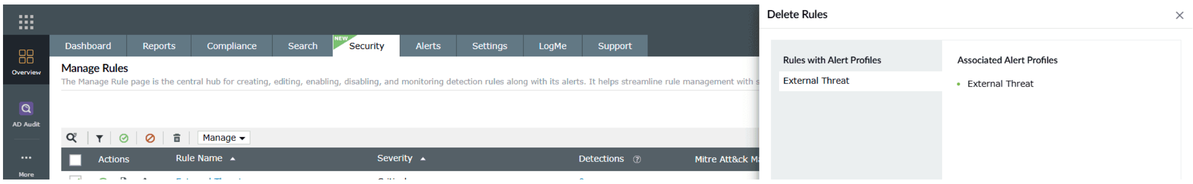
Delete rule(s)

1. Click on the empty checkbox(es) in the first column in order to select the respective rules.
2. Then click on the Delete icon 🗑 in the ribbon above the rules list.
3. A Confirm Action pop-up appears. Click on Delete.



Confirm Deletion

Deleting this rule will also remove the associated alert profiles. Are you sure you want to proceed?

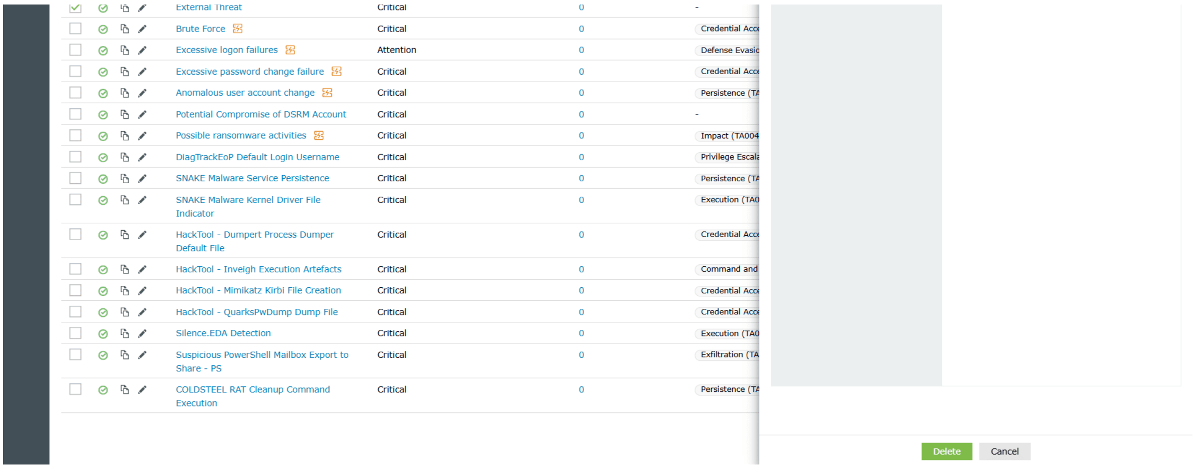


Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with s

Delete Rules

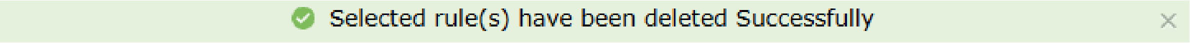
Rules with Alert Profiles	Associated Alert Profiles
External Threat	External Threat



☑	External Threat	Critical	0	-
□	Brute Force	Critical	0	Credential Acce
□	Excessive logon failures	Attention	0	Defense Evasic
□	Excessive password change failure	Critical	0	Credential Acce
□	Anomalous user account change	Critical	0	Persistence (TA
□	Potential Compromise of DSRM Account	Critical	0	-
□	Possible ransomware activities	Critical	0	Impact (TA004
□	DiagTrackEoP Default Login Username	Critical	0	Privilege Escala
□	SNAKE Malware Service Persistence	Critical	0	Persistence (TA
□	SNAKE Malware Kernel Driver File Indicator	Critical	0	Execution (TA0
□	HackTool - Dumpert Process Dumper Default File	Critical	0	Credential Acce
□	HackTool - Inveigh Execution Artefacts	Critical	0	Command and
□	HackTool - Mimikatz Kirbi File Creation	Critical	0	Credential Acce
□	HackTool - QuarksPwDump Dump File	Critical	0	Credential Acce
□	Silence.EDA Detection	Critical	0	Execution (TA0
□	Suspicious PowerShell Mailbox Export to Share - PS	Critical	0	Exfiltration (TA
□	COLDSTEEL RAT Cleanup Command Execution	Critical	0	Persistence (TA

Image 5: Deleting rule in the manage rules module

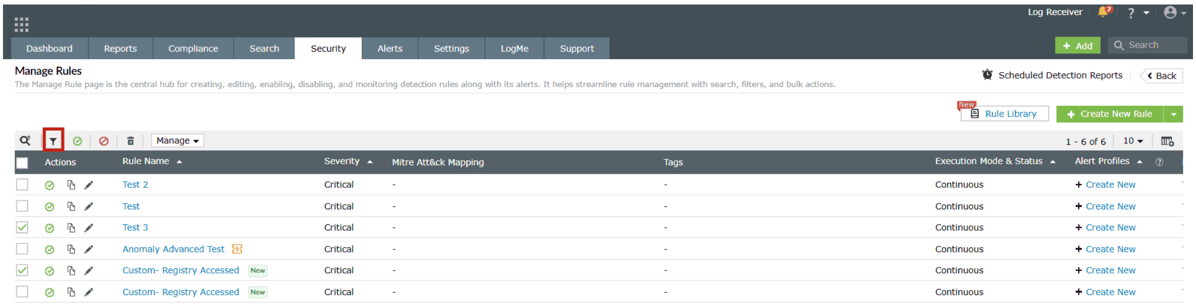
4. Upon successful completion of the action, the below pop-up appears.



Selected rule(s) have been deleted Successfully

Filter rule(s)

1. Click on the Filter icon in the ribbon above the rules list.



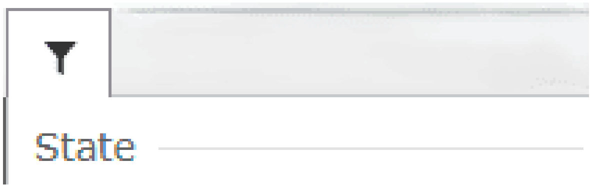
Manage Rules

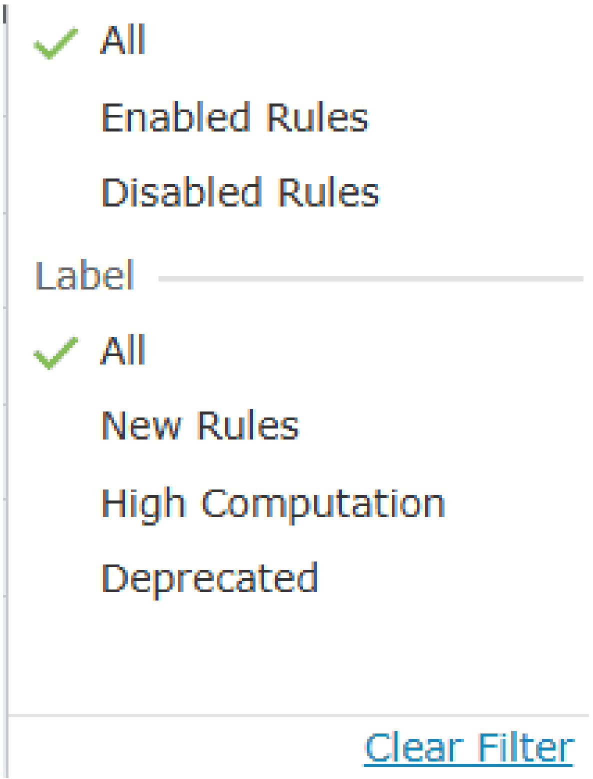
The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

	Actions	Rule Name	Severity	Mitre Att&ck Mapping	Tags	Execution Mode & Status	Alert Profiles
□		Test 2	Critical	-	-	Continuous	+ Create New
□		Test	Critical	-	-	Continuous	+ Create New
☑		Test 3	Critical	-	-	Continuous	+ Create New
□		Anomaly Advanced Test	Critical	-	-	Continuous	+ Create New
☑		Custom- Registry Accessed New	Critical	-	-	Continuous	+ Create New
□		Custom- Registry Accessed New	Critical	-	-	Continuous	+ Create New

Image 6: Filtering rules in the manage rules module

2. The following filter options appear.




✓ All

Enabled Rules

Disabled Rules

Label

✓ All

New Rules

High Computation

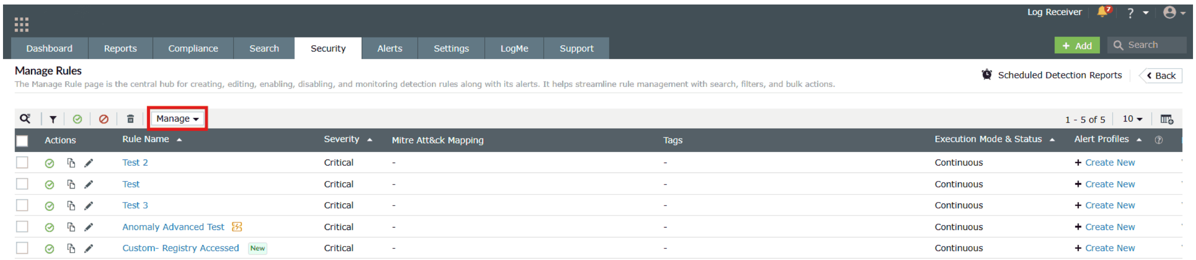
Deprecated

Clear Filter

3. You can choose multiple filters at once. Click on a filter to select it. Click on it again if you want to deselect it. The rules get filtered instantly as you click on any filter option.
4. Click on the Clear Filter option to undo all/any filtering that has been done to the rules.

Other configurations to manage rules

1. Click on the empty checkbox(es) in the first column in order to select the respective rules you wish to configure.
2. In the ribbon above the list of rules, an option to further Manage rules is available.



Manage Rules

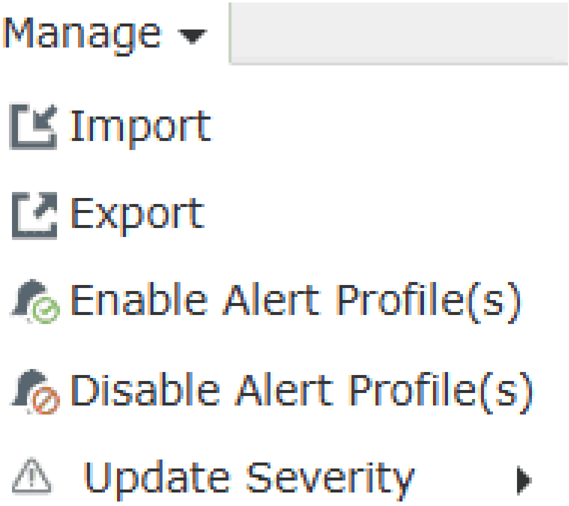
The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

□	Actions	Rule Name	Severity	Mitre Att&ck Mapping	Tags	Execution Mode & Status	Alert Profiles
□		Test 2	Critical	-	-	Continuous	+ Create New
□		Test	Critical	-	-	Continuous	+ Create New
□		Test 3	Critical	-	-	Continuous	+ Create New
□		Anomaly Advanced Test	Critical	-	-	Continuous	+ Create New
□		Custom- Registry Accessed New	Critical	-	-	Continuous	+ Create New

Image 7: Managing rules in the manage rules module

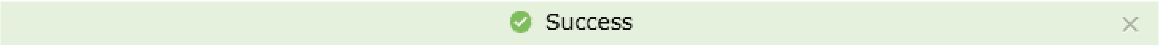
Image 7: Managing rules in the manage rules module

3. Click on it for the Manage tab to expand the configurations.



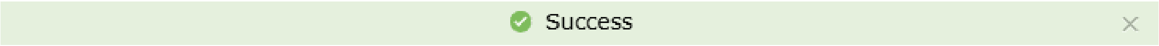
4. Configurations:

- Import: Import the desired rules by uploading a file containing the rules.
- Export: Instantly download the selected rules along with the configuration details. This option is applicable only for custom created rules.
- Enable Alert Profile(s): Click on it to Enable Alert Profile(s) for the selected rule(s) and the configuration is instantly updated displaying the below pop-up.



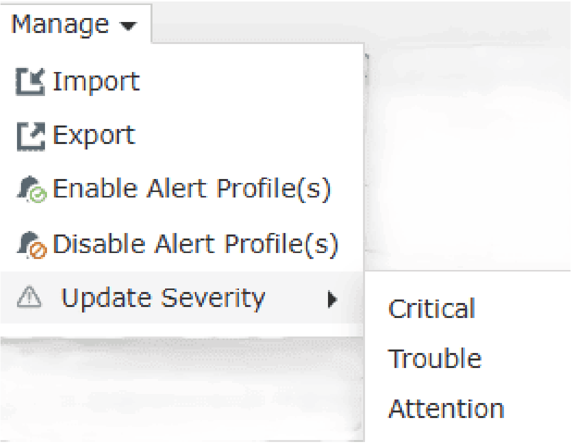
Success

- Disable Alert Profile(s): Click on it to Disable Alert Profile(s) for the selected rule(s) and the configuration is instantly updated displaying the below pop-up.

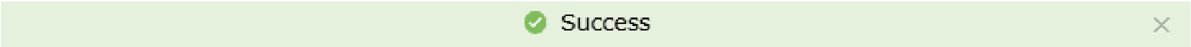


Success

- Update Severity: Click/Hover on it to view the three severity levels and choose the one you wish to apply.



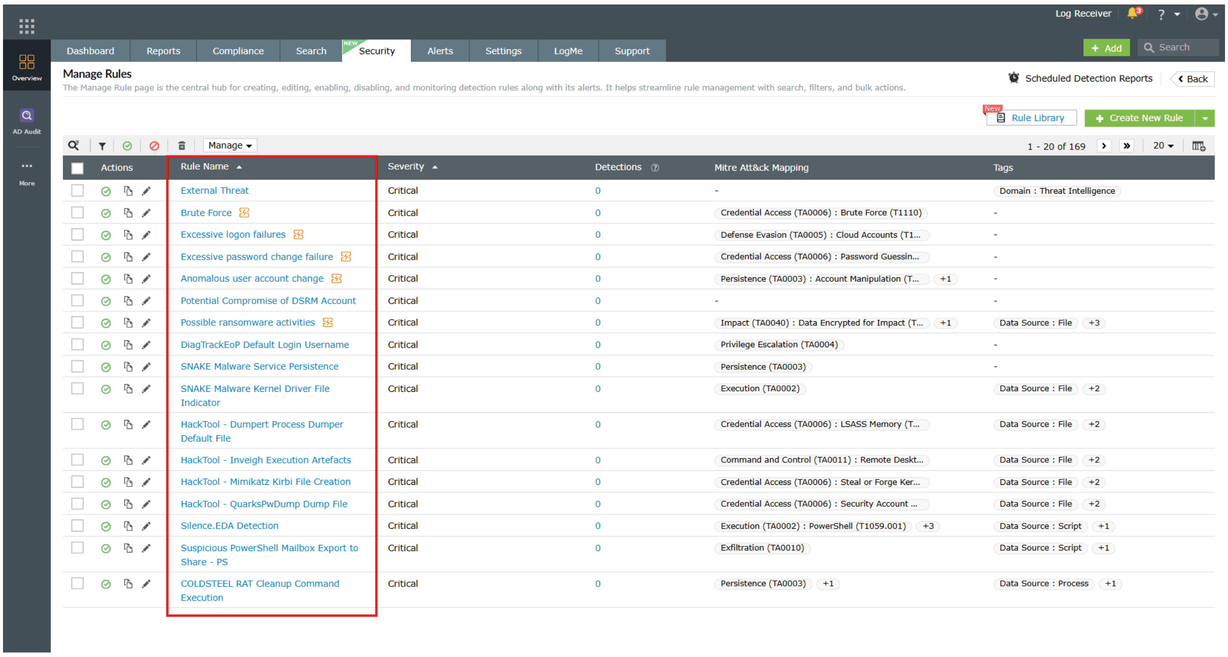
The configuration is instantly updated displaying the below pop-up.



Success

B. Rule Name column

The Rule Name column lists the names of all the configured rules till date.



Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

Actions	Rule Name	Severity	Detections	Mitre Att&ck Mapping	Tags
	External Threat	Critical	0	-	Domain : Threat Intelligence
	Brute Force	Critical	0	Credential Access (TA0006) : Brute Force (T1110)	-
	Excessive logon failures	Critical	0	Defense Evasion (TA0005) : Cloud Accounts (T1...	-
	Excessive password change failure	Critical	0	Credential Access (TA0006) : Password Guessin...	-
	Anomalous user account change	Critical	0	Persistence (TA0003) : Account Manipulation (T... +1	-
	Potential Compromise of DSRM Account	Critical	0	-	-
	Possible ransomware activities	Critical	0	Impact (TA0040) : Data Encrypted for Impact (T... +1	Data Source : File +3
	DiagTrackEoP Default Login Username	Critical	0	Privilege Escalation (TA0004)	-
	SNAKE Malware Service Persistence	Critical	0	Persistence (TA0003)	-
	SNAKE Malware Kernel Driver File Indicator	Critical	0	Execution (TA0002)	Data Source : File +2
	HackTool - Dumpert Process Dumper Default File	Critical	0	Credential Access (TA0006) : LSASS Memory (T...	Data Source : File +2
	HackTool - Inveigh Execution Artefacts	Critical	0	Command and Control (TA0011) : Remote Deskt...	Data Source : File +2
	HackTool - Mimikatz Kirbi File Creation	Critical	0	Credential Access (TA0006) : Steal or Forge Ker...	Data Source : File +2
	HackTool - QuarksPwDump Dump File	Critical	0	Credential Access (TA0006) : Security Account ...	Data Source : File +2
	Silence.EDA Detection	Critical	0	Execution (TA0002) : PowerShell (T1059.001) +3	Data Source : Script +1
	Suspicious PowerShell Mailbox Export to Share - PS	Critical	0	Exfiltration (TA0010)	Data Source : Script +1
	COLDSTEEL RAT Cleanup Command Execution	Critical	0	Persistence (TA0003) +1	Data Source : Process +1

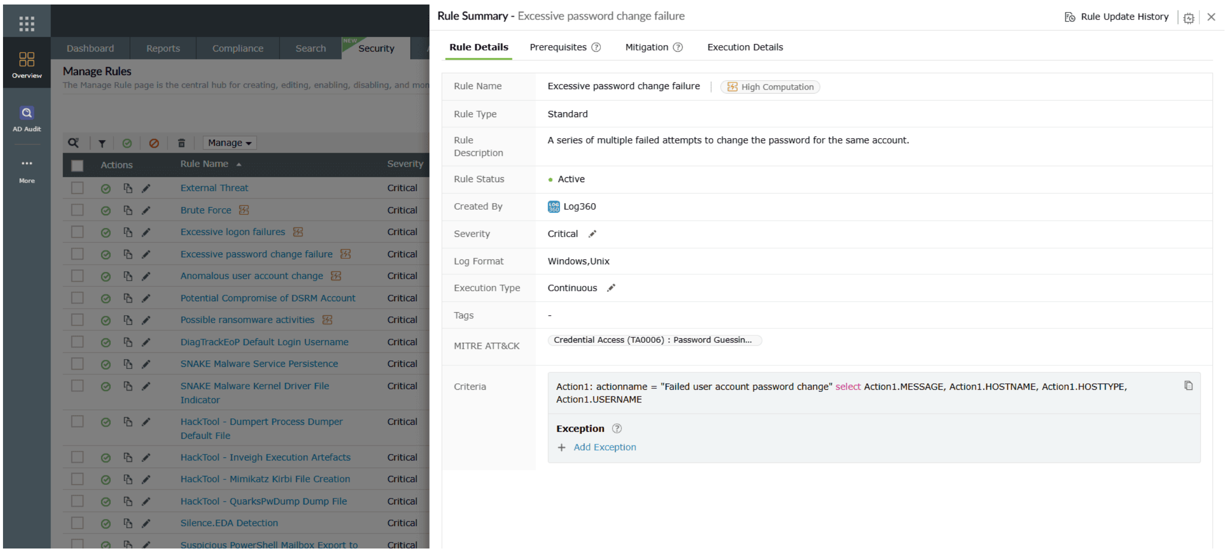
Image 8: Rule names in the manage rules module

Clicking on any rule name prompts the Rule Summary box to slide open. It includes 4 sub-tabs:

- Rule Details
- Prerequisites
- Mitigation
- Execution Details

Rule Details

Provides a summary of the rule along with the respective details and options to add exceptions for that particular rule.



Rule Summary - Excessive password change failure

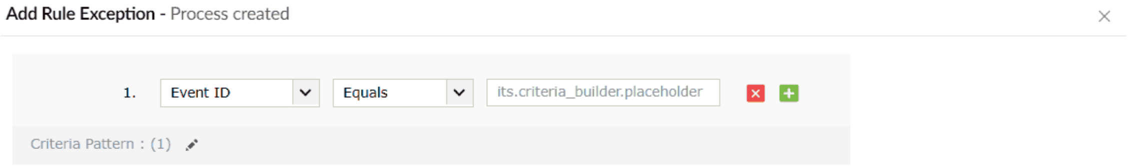
Rule Name	Excessive password change failure | High Computation
Rule Type	Standard
Rule Description	A series of multiple failed attempts to change the password for the same account.
Rule Status	● Active
Created By	Log360
Severity	Critical
Log Format	Windows,Unix
Execution Type	Continuous
Tags	-
MITRE ATT&CK	Credential Access (TA0006) : Password Guessin...
Criteria	Action1: actionname = "Failed user account password change" select Action1.MESSAGE, Action1.HOSTNAME, Action1.HOSTTYPE, Action1.USERNAME **Exception**

Share - PS

COLDSTEEL RAT Cleanup Command Execution Critical

Image 9: Rule details in the manage rules module

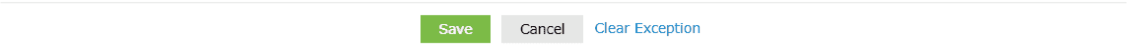
1. Rule Name: Displays the unique rule name assigned by you for this rule.
2. Rule Type: Displays which category of rules this rule comes under - Standard, Anomaly, or Advanced.
3. Rule Description: Displays whatever description you have added for this rule, if any.
4. Rule Status: Displays whether the rule is currently in an Active state or Inactive.
5. Created By: Displays the user (identified by their role in this network) who has created this rule.
6. Severity: Displays the Severity level set during the rule configuration - Critical, Trouble, or Attention.
7. Log Format: Shows the log type associated with the rule.
8. Execution Type: Displays the Execution Configuration mode set for this rule - Continuous; Schedule every 5 minutes, 10 minutes, 30 minutes, 1 hour; and Custom.
9. Tags: Categorizes the rule based on industry or type.
10. MITRE ATT&CK: Maps the rule to relevant MITRE tactics and techniques.
11. Criteria: Displays the rule conditions in query format.
    - Exception: The Exception defines the criteria for the detection engine to rule out cases from the detections and reports. A detection will not be created if the set conditions from the rule exception match.
        - When you click on the Add Exception button, the Add Rule Exception box slides open.



Add Rule Exception - Process created

1. Event ID Equals its.criteria_builder.placeholder

Criteria Pattern : (1)



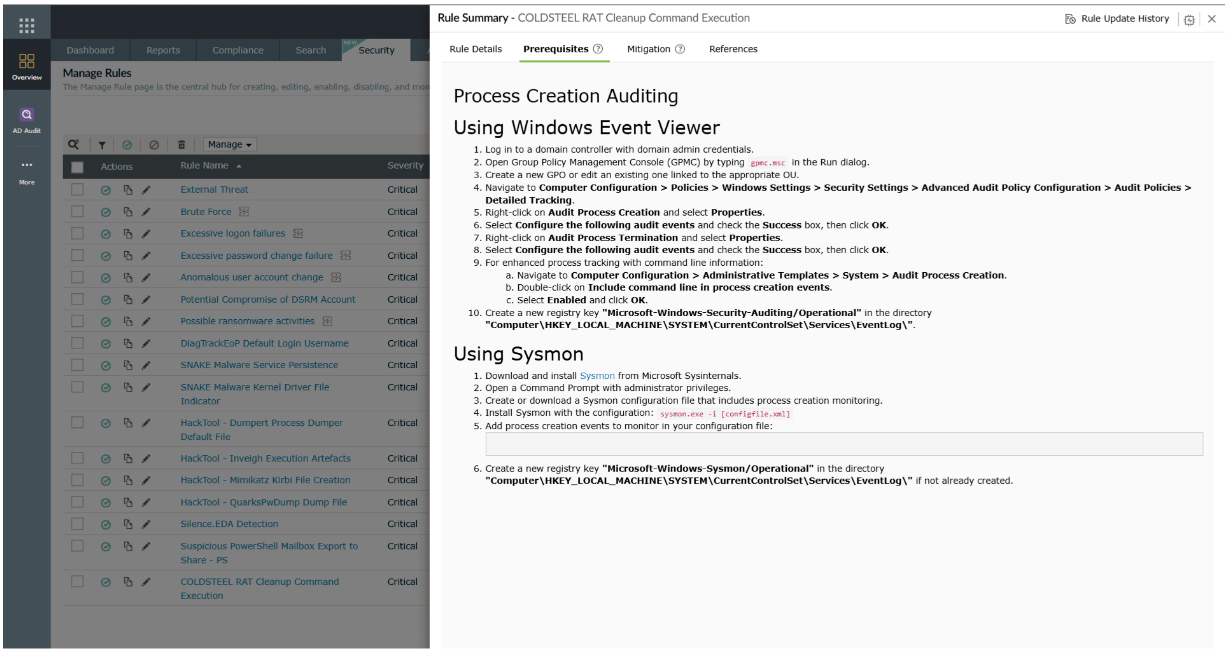
- You can configure the exceptions you wish to rule out from detections and reports.
- Click on the Save button to save the rule exception.
- Upon successful completion of the action, the below pop-up appears.

Rule Exception updated Successfully

- If you wish to reset and reconfigure that exception you can click on Clear Exception, and the configurations are reset.
- Click on Cancel if you wish to abort the process.

Prerequisites

This sub-tab provides an interface for you to check and ensure that the required dependencies of the rule are met for proper detection.



Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and mon

☐	Actions	Rule Name ▲	Severity
☐		External Threat	Critical
☐		Brute Force	Critical
☐		Excessive logon failures	Critical
☐		Excessive password change failure	Critical
☐		Anomalous user account change	Critical
☐		Potential Compromise of DSRM Account	Critical
☐		Possible ransomware activities	Critical
☐		DiagTrackEoP Default Login Username	Critical
☐		SNAKE Malware Service Persistence	Critical
☐		SNAKE Malware Kernel Driver File Indicator	Critical
☐		HackTool - Dumpert Process Dumper Default File	Critical
☐		HackTool - Inveigh Execution Artefacts	Critical
☐		HackTool - Mimikatz Kirbi File Creation	Critical
☐		HackTool - QuarksPwDump Dump File	Critical
☐		Silence.EDA Detection	Critical
☐		Suspicious PowerShell Mailbox Export to Share - PS	Critical
☐		COLDSTEEL RAT Cleanup Command Execution	Critical

Rule Summary - COLDSTEEL RAT Cleanup Command Execution

Process Creation Auditing

Using Windows Event Viewer

1. Log in to a domain controller with domain admin credentials.
2. Open Group Policy Management Console (GPMC) by typing `gpmc.msc` in the Run dialog.
3. Create a new GPO or edit an existing one linked to the appropriate OU.
4. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Detailed Tracking**.
5. Right-click on **Audit Process Creation** and select **Properties**.
6. Select **Configure the following audit events** and check the **Success** box, then click **OK**.
7. Right-click on **Audit Process Termination** and select **Properties**.
8. Select **Configure the following audit events** and check the **Success** box, then click **OK**.
9. For enhanced process tracking with command line information:
    a. Navigate to **Computer Configuration > Administrative Templates > System > Audit Process Creation**.
    b. Double-click on **Include command line in process creation events**.
    c. Select **Enabled** and click **OK**.
10. Create a new registry key **"Microsoft-Windows-Security-Auditing/Operational"** in the directory **"Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\"**.

Using Sysmon

1. Download and install Sysmon from Microsoft Sysinternals.
2. Open a Command Prompt with administrator privileges.
3. Create or download a Sysmon configuration file that includes process creation monitoring.
4. Install Sysmon with the configuration: `sysmon.exe -i [configfile.xml]`
5. Add process creation events to monitor in your configuration file:
6. Create a new registry key **"Microsoft-Windows-Sysmon/Operational"** in the directory **"Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\"** if not already created.

Image 10: Rule prerequisites in the manage rules module

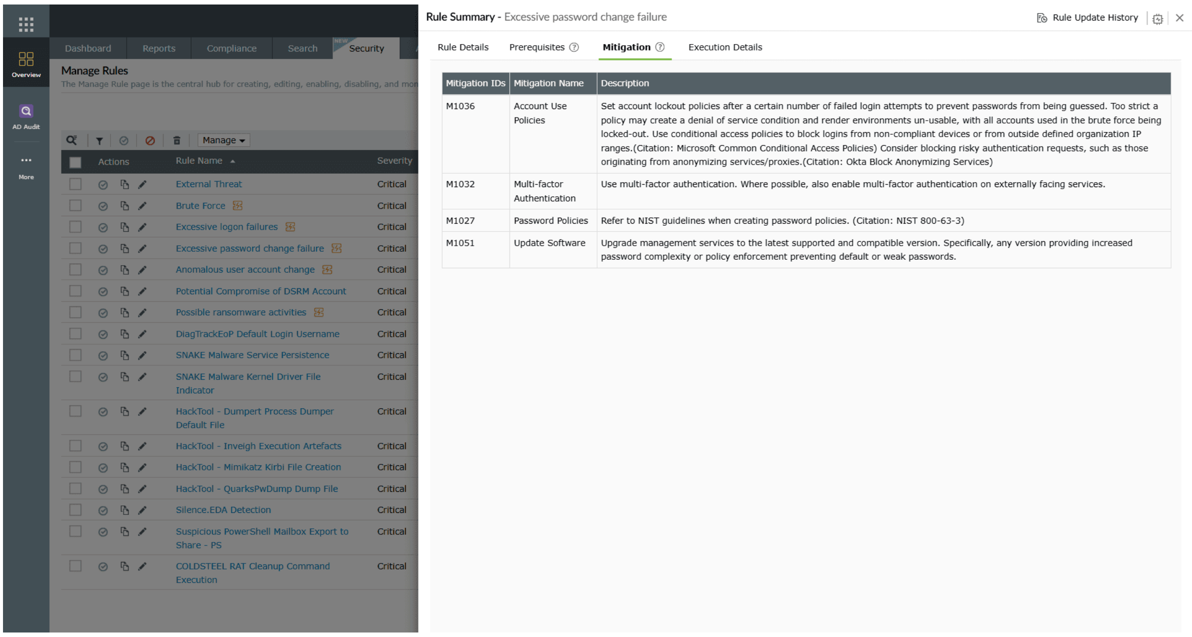
Mitigation

This sub-tab provides an interface for you to take recommended actions to minimize risks and prevent future threats. Mitigations are pre-added for predefined rules, whereas for custom rules they must be manually added by the user.

Case 1: Mitigation steps existing in the rule configuration.

- Mitigation IDs: Lists the MITRE ATT&CK mitigation techniques associated with the detected rule or threat.
- Description: Provides actionable guidance on how to mitigate or reduce the impact of the threat, such as

- Description: Provides actionable guidance on how to mitigate or reduce the impact of the threat, such as configuration changes, security policies, or best practices.
- False positives: Indicates the likelihood of false positives for the specific detection.


Dashboard
Reports
Compliance
Search
Security
Overview
AD Audit
More
Manage Rules
The Manage Rule page is the central hub for creating, editing, enabling, disabling, and mor
Manage
Actions
Rule Name
Severity
External Threat
Critical
Brute Force
Critical
Excessive logon failures
Critical
Excessive password change failure
Critical
Anomalous user account change
Critical
Potential Compromise of DSRM Account
Critical
Possible ransomware activities
Critical
DiagTrackEoP Default Login Username
Critical
SNAKE Malware Service Persistence
Critical
SNAKE Malware Kernel Driver File Indicator
Critical
HackTool - Dumpert Process Dumper Default File
Critical
HackTool - Inveigh Execution Artefacts
Critical
HackTool - Mimikatz Kirbi File Creation
Critical
HackTool - QuarksPwDump Dump File
Critical
Silence.EDA Detection
Critical
Suspicious PowerShell Mailbox Export to Share - PS
Critical
COLDSTEEL RAT Cleanup Command Execution
Critical
Rule Summary - Excessive password change failure
Rule Update History
Rule Details
Prerequisites
Mitigation
Execution Details

Mitigation IDs	Mitigation Name	Description
M1036	Account Use Policies	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges.(Citation: Microsoft Common Conditional Access Policies) Consider blocking risky authentication requests, such as those originating from anonymizing services/proxies.(Citation: Okta Block Anonymizing Services)
M1032	Multi-factor Authentication	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
M1027	Password Policies	Refer to NIST guidelines when creating password policies. (Citation: NIST 800-63-3)
M1051	Update Software	Upgrade management services to the latest supported and compatible version. Specifically, any version providing increased password complexity or policy enforcement preventing default or weak passwords.

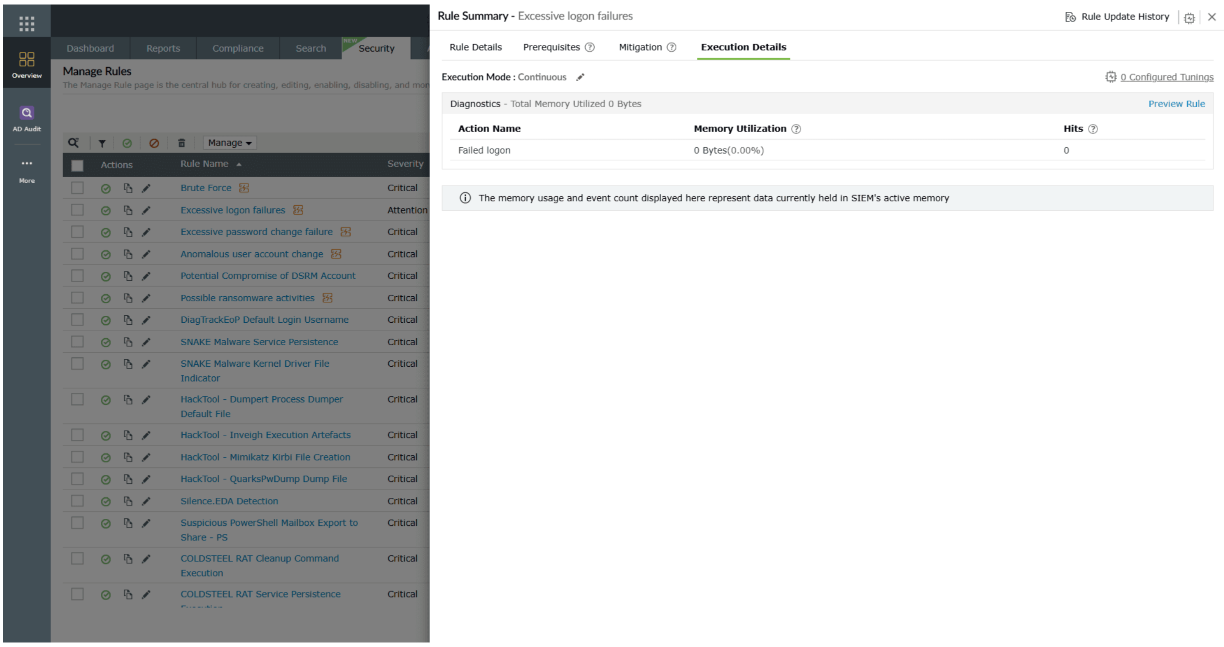
Image 11: Rule mitigation in the manage rules module

Case 2: No existing mitigation steps.

In such cases, it is implied that no mitigation is necessary for that particular rule.

Execution Details

Used to identify high-computation continuous rules in terms of memory usage. It also shows which of the currently collected logs fall under this rule's actions.


Dashboard
Reports
Compliance
Search
Security
Overview
AD Audit
More
Manage Rules
The Manage Rule page is the central hub for creating, editing, enabling, disabling, and mor
Manage
Actions
Rule Name
Severity
Brute Force
Critical
Excessive logon failures
Attention
Excessive password change failure
Critical
Anomalous user account change
Critical
Potential Compromise of DSRM Account
Critical
Possible ransomware activities
Critical
DiagTrackEoP Default Login Username
Critical
SNAKE Malware Service Persistence
Critical
SNAKE Malware Kernel Driver File Indicator
Critical
HackTool - Dumpert Process Dumper Default File
Critical
HackTool - Inveigh Execution Artefacts
Critical
HackTool - Mimikatz Kirbi File Creation
Critical
HackTool - QuarksPwDump Dump File
Critical
Silence.EDA Detection
Critical
Suspicious PowerShell Mailbox Export to Share - PS
Critical
COLDSTEEL RAT Cleanup Command Execution
Critical
COLDSTEEL RAT Service Persistence
Critical
Rule Summary - Excessive logon failures
Rule Update History
Rule Details
Prerequisites
Mitigation
Execution Details
0 Configured Tunings
Preview Rule

Execution Mode : Continuous

Diagnostics - Total Memory Utilized 0 Bytes

Action Name	Memory Utilization	Hits
Failed logon	0 Bytes(0.00%)	0

The memory usage and event count displayed here represent data currently held in SIEM's active memory

Image 12: Rule execution details in the manage rules module

Execution Mode:

Execution Mode:

1. Execution Mode: Displays the Execution Configuration mode set for this rule—Continuous; Schedule every 5 minutes, 10 minutes, 30 minutes, 1 hour; and Custom.
2. Diagnostics: Provides insights into the resource usage and activity generated by the rule. This helps you verify how the rule performs during execution.
   - Action Name: Displays the event/action associated with this particular detection. For example, Successful logon.
   - Memory Utilization: Track total memory used during action execution in near real time.
   - Hits: Track the total number of hits for the action in near real time.
3. Execution History: Displays a timeline of the rule’s past executions, including event counts and memory consumption recorded during each run. This helps you review the rule’s performance over time and troubleshoot any anomalies.
4. Refer to the understanding rules page to learn more about the differences in the execution mode for continuous and scheduled modes.

Rule tuning

The Rule Tuning option in helps administrators refine detection rules by optimizing query execution. It analyzes the way rules are processed and provides actionable insights to improve performance. By applying these recommendations, you can reduce execution load, improve query speed, and eliminate unnecessary noise.
Below are the enhancements rule tuning can help administrators with:

- Enhances rule performance by reducing unnecessary execution overhead.
- Prevents timeouts and delays during query runs.
- Minimizes false positives by excluding known or repetitive patterns.
- Helps scale detection efficiency as log volume grows.

> NOTE
>
> Tuning insights are generated from query response analysis. Applying them may affect result consistency. Review before applying.

1. Click the icon in the top-right corner of the Rule Summary box to view the rule tuning configurations box.
2. The Rule Tuning panel opens, displaying:
   - Rule conditions and actions.
   - Tuning insights and recommendations.
   - A preview of rule execution with graphical output.

Available actions:

1. Tuning insights
   - Provides action-based suggestions, such as:

    - Adding grouping fields to reduce the number of query executions.
    - Using the Limit operator to control cardinality.
    - Excluding specific usernames, devices, or fields to minimize load.
  - You can:
    - Apply individual tunings.
    - Use Apply All Tunings for bulk optimization.
2. Rule preview
   - Generates a sample output graph showing query execution trends.
   - Displays execution time and data results (e.g., usernames, devices).
   - Helps validate whether tuning improves efficiency without losing accuracy.
3. Handling query timeouts
   - If a scheduled task fails due to query timeout, you can:
     - Adjust the query timeout value.
     - Apply recommended tunings.
     - Configure exceptions manually to filter out known patterns.

Example use case: Brute Force detection
Consider the Brute Force rule, which detects failed and successful Windows logins within a specific timeframe.

- Without tuning, this rule may return large datasets causing execution delays.
- With tuning, you can:
  - Add grouping by username/device.
  - Limit the number of results analyzed.
  - Exclude repeated usernames or devices to reduce execution load.

Result: Faster query response, reduced noise, and more efficient detection of brute-force attempts.
Rule tuning best practices

- Always preview the rule before applying tunings.
- Avoid over-filtering, as it may suppress genuine alerts.
- Use manual exceptions for repetitive patterns instead of disabling rules.
- Periodically revisit tuning recommendations as log volume and attack patterns evolve.

C. Severity

Displays the severity level set for the rules- Critical, Trouble or Attention.

D. Mitre Att&ck Mapping

Tactic and technique classification aligned with the MITRE ATT&CK framework that are associated with the rules.

E. Tags

E. Tags

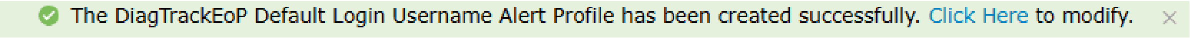
Additional contextual tags, such as threat actor, software, industry verticals that are associated with the rules.

F. Execution Mode & Status

Displays the Execution Configuration mode set for each rule.

G. Alert Profiles

- Provides the option to create an alert profile for all the rules listed here.
- When you click on the Create Alert Profile option, an alert profile for the corresponding rule is created instantly and the below pop-up appears.



The DiagTrackEoP Default Login Username Alert Profile has been created successfully. Click Here to modify.

- When you click on the Click Here option provided in the pop-up as shown above, you will be taken to the Edit Alert Profile module. Read the Alert Profile help page to learn more about editing and assigning alert profiles.

H. Created By

Displays the user (identified by their role in this network) who has created this rule.

I. Rule Type

Displays the rule category- Standard, Anomaly, or Advanced.

J. Installed Time

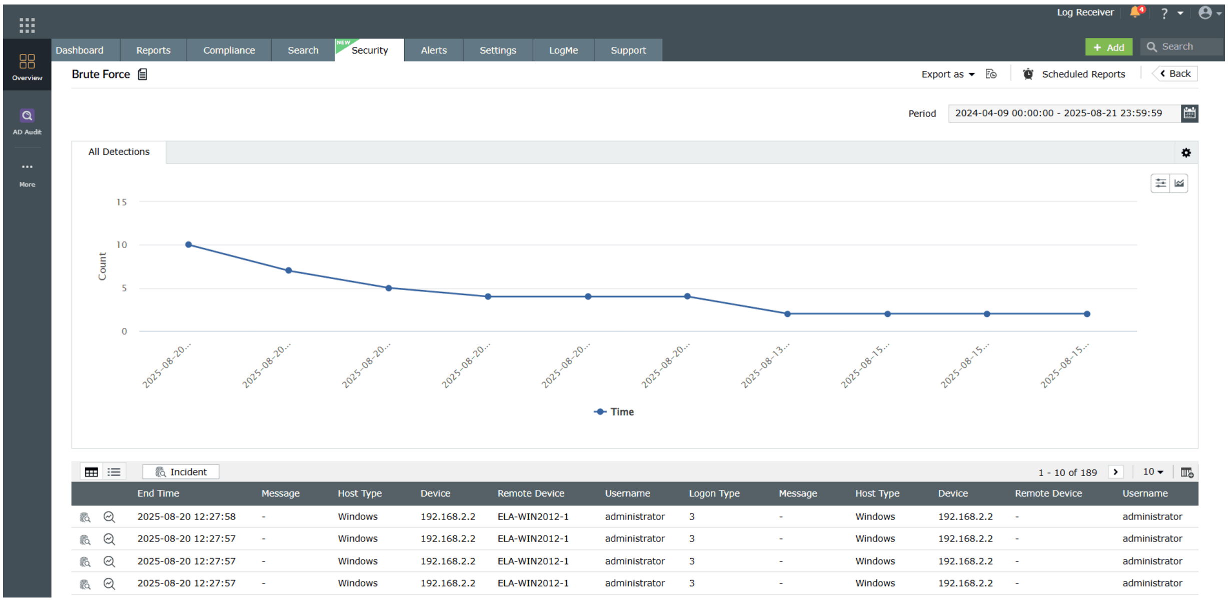
Displays the time of rule installation from the Rule Library.

K. Last Modified Time

Displays the time of the most recent modification done to the rule.

L. Detections

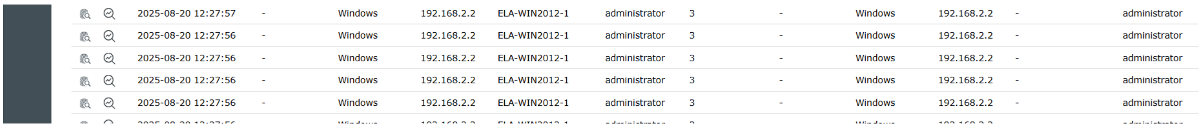
Click on the View Detections link to view all the detections that were triggered by that particular rule. A periodic graph of the detections will be shown to you for that particular rule as given below.



Brute Force

Period 2024-04-09 00:00:00 - 2025-08-21 23:59:59

	End Time	Message	Host Type	Device	Remote Device	Username	Logon Type	Message	Host Type	Device	Remote Device	Username
	2025-08-20 12:27:58	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-	Windows	192.168.2.2	-	administrator
	2025-08-20 12:27:57	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-	Windows	192.168.2.2	-	administrator
	2025-08-20 12:27:57	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-	Windows	192.168.2.2	-	administrator
	2025-08-20 12:27:57	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-	Windows	192.168.2.2	-	administrator

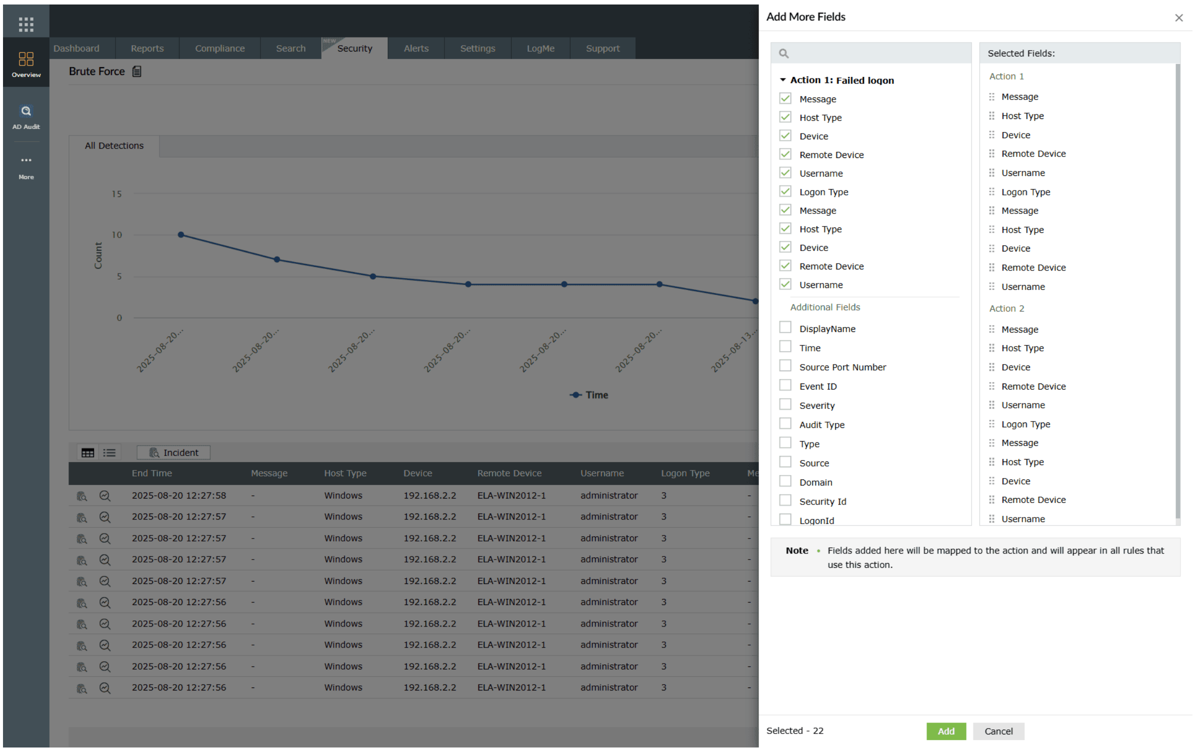


2025-08-20 12:27:57	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-	Windows	192.168.2.2	-	administrator
2025-08-20 12:27:56	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-	Windows	192.168.2.2	-	administrator
2025-08-20 12:27:56	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-	Windows	192.168.2.2	-	administrator
2025-08-20 12:27:56	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-	Windows	192.168.2.2	-	administrator
2025-08-20 12:27:56	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-	Windows	192.168.2.2	-	administrator

Image 13: Rule detection details in the manage rules module

The details displayed in the detection are as follows:

- Detection graph:
  - A visual depiction showing the event count over time that triggered the respective rule for quick anomaly spotting. Upon clicking the drop-down arrow available beside the graph, you will be shown the different types of graphs to choose from.
- Event Log Table: Displays details of each detected event that triggered the rule such as End Time, Event IDs, Log Source, Time, User Name, Domain, Message, etc. Clicking on the icon on the top-right corner of the data table allows you to select/deselect and Add what fields you wish to view separated by columns. You can choose fields from the many options provided.



End Time	Message	Host Type	Device	Remote Device	Username	Logon Type	Me
2025-08-20 12:27:58	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-
2025-08-20 12:27:57	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-
2025-08-20 12:27:57	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-
2025-08-20 12:27:57	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-
2025-08-20 12:27:57	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-
2025-08-20 12:27:56	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-
2025-08-20 12:27:56	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-
2025-08-20 12:27:56	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-
2025-08-20 12:27:56	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-
2025-08-20 12:27:56	-	Windows	192.168.2.2	ELA-WIN2012-1	administrator	3	-

Add More Fields ×

Action 1: Failed logon

☑ Message
☑ Host Type
☑ Device
☑ Remote Device
☑ Username
☑ Logon Type
☑ Message
☑ Host Type
☑ Device
☑ Remote Device
☑ Username

Additional Fields

□ DisplayName
□ Time
□ Source Port Number
□ Event ID
□ Severity
□ Audit Type
□ Type
□ Source
□ Domain
□ Security Id
□ LogonId

Selected Fields:

Action 1

Message
Host Type
Device
Remote Device
Username
Logon Type
Message
Host Type
Device
Remote Device
Username

Action 2

Message
Host Type
Device
Remote Device
Username
Logon Type
Message
Host Type
Device
Remote Device
Username

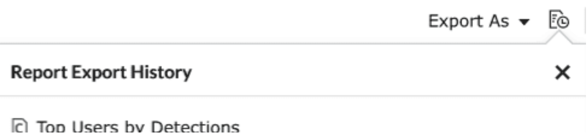
Note • Fields added here will be mapped to the action and will appear in all rules that use this action.

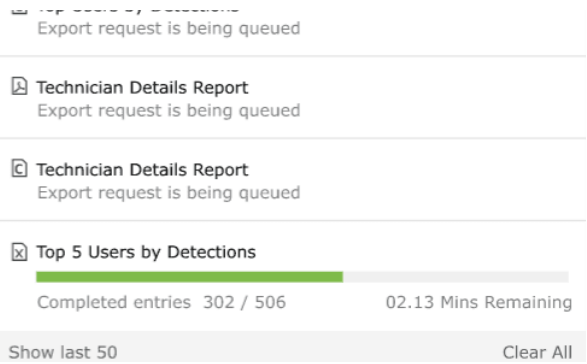
Selected - 22 Add Cancel

Image 14: Rule detection details columns in the manage rules module

Available actions in the detections module:

- Clicking on the button allows you to choose a format to export the said data either in a PDF format or a CSV file.
- Clicking on the Report export history icon allows you to view the complete history of the past data exports that have taken place for that particular report.





Export request is being queued

Technician Details Report
Export request is being queued

Technician Details Report
Export request is being queued

Top 5 Users by Detections
Completed entries 302 / 506 02.13 Mins Remaining

- You can also customize the time range for the detection by clicking on

Last 30 days

You can:

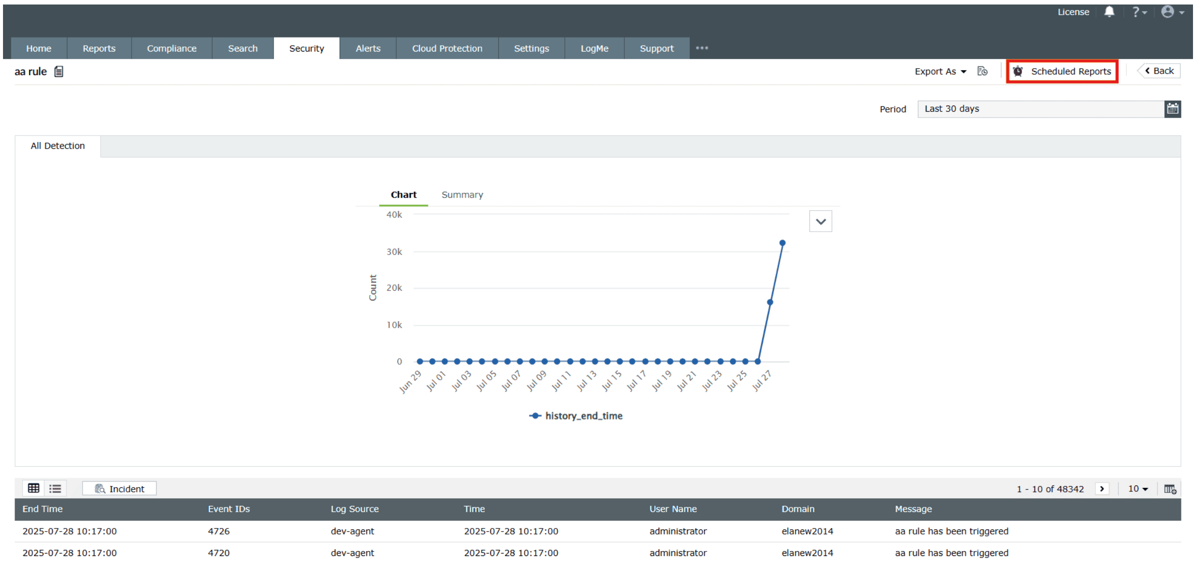
- Select the start date and end date for your desired time range.
- Click on any of the predefined time ranges available that suits your requirements.
- Click on Custom range and then proceed to enter a number in the box provided below that will represent the past number of days worth of data you wish to view.
- Click on Apply.

Scheduled Reports

NOTE

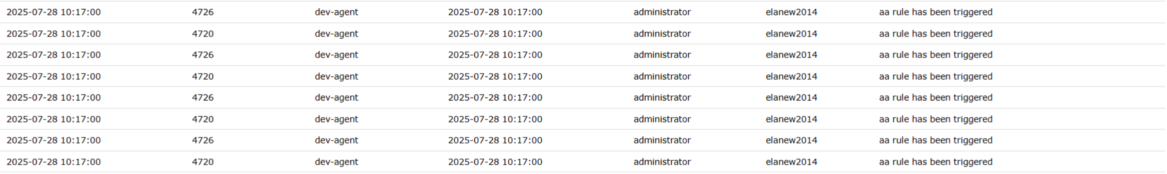
You can access the detection reports from the Manage Rules module directly. Read Scheduled Detection Reports to learn more.

1. Click on the Scheduled Reports option as highlighted below.



Period: Last 30 days

End Time	Event IDs	Log Source	Time	User Name	Domain	Message
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered



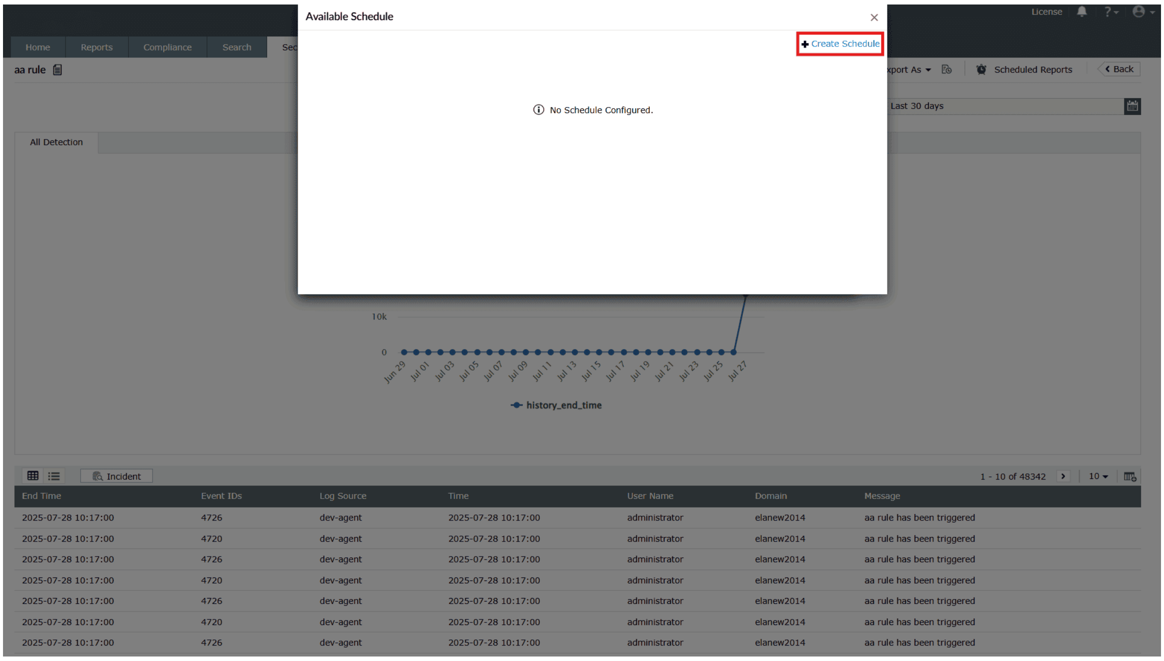
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered

Image 15: Rule scheduled reports in the manage rules module

2. The available schedules for those rule reports (if any) will be shown on the screen.

3. You can create a schedule for a particular rule by following the steps below:

- Click on Create Schedule as highlighted below.



Available Schedule

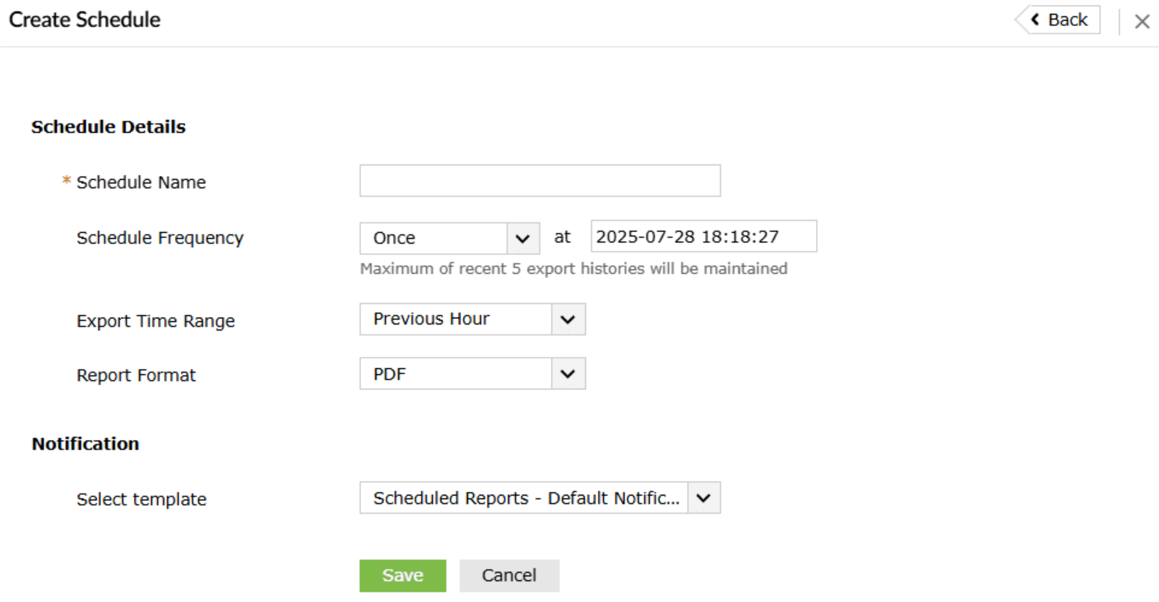
✚ Create Schedule

ⓘ No Schedule Configured.

End Time	Event IDs	Log Source	Time	User Name	Domain	Message
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4720	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered
2025-07-28 10:17:00	4726	dev-agent	2025-07-28 10:17:00	administrator	elanew2014	aa rule has been triggered

Image 16: Create scheduled reports in the manage rules module

- Upon clicking, the pop-up will display the fields to Create Schedule.



Create Schedule

Schedule Details

* Schedule Name:

Schedule Frequency: Once at 2025-07-28 18:18:27

Maximum of recent 5 export histories will be maintained

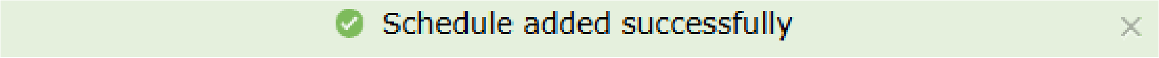
Export Time Range: Previous Hour

Report Format: PDF

Notification

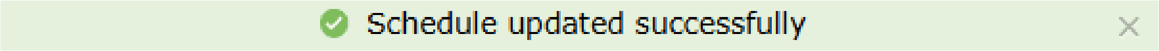
Select template: Scheduled Reports - Default Notific...

- Fill the necessary fields:
  - Schedule Details
    - Schedule Name: Assign a unique name to the schedule.
    - Schedule Frequency: Define how often the schedule should run (hourly, daily, weekly, or monthly).
    - Export Time Range: Specify the time range of data to include (e.g., last 24 hours, last 7 days, or custom).
    - Report Format: Choose the preferred format for the exported report (PDF, CSV, XLS).
  - Notification
    - Select Template: Pick a predefined report template or customize one.
- After configuring the schedule, click on Save. Upon successful completion, the schedule is updated in the pop-up box, along with a confirmation message.



✓ Schedule added successfully ✕

- You can also edit the schedule by clicking on the edit ✎ icon in the pop-up box. The same fields appear for editing.
- Edit and click on Update. Upon successful completion, the schedule is updated in the pop-up box, along with a confirmation message.



✓ Schedule updated successfully ✕

Read also
This document explained how to navigate the Manage Rules page, perform key actions on rules, view detailed rule summaries, tune performance, and generate detection reports for deeper analysis.

- Rule management overview
- Understanding rules
- Creating custom rules
- Query grammar
- Scheduled detection reports

4.1.2.5. Query grammar

Last updated on: September 12, 2025

In this page

Overview

Query Grammar is the language you can use while building the Query Syntax that the ML (Machine Learning) model understands and helps you build rule criteria and rule parameters during advanced rule creation.
This page contains the complete query grammar reference, including basic criteria, supported datatypes, relational and logical operators, advanced functions, aggregation constructs, correlation statements, and practical detection examples.

Basic Criteria

1. Data types

Type name	Description	Examples
String	A string value	"surname" "198.51.100.255" "Number of bytes"
Int	An integer value	23 -32 4000000244553
Float	A floating-point number.	3.14 -1.2e5
Timespan	A time interval represented by one or two digits followed by 's' for seconds, m'for minute. 'h' for hour, 'd' for days, 'w' for week, 'M'for month, 'q'for quarter, 'y'for year.	2s, 45m, 4h, 2d, 3w, 2M, 4q, 1y
Memory	A data size represented in 'B' for bytes, "KB' for kilobytes, 'MB' for megabytes, 'GB' for gigabytes 'TB' for terabytes, 'PB' for	2B, 3KB, 3 MB,

Type name	Description	Examples
Memory	for megabytes, GB for gigabytes, TB for terabytes, PB for petabytes	34GB, 9TB, 9PB
Date-time	A date-time format represented by "YYYY-MM-DD", "YYYY-MM-DD HH-MM-SS"	"2000-08-30" "2000-08-30 15:45:06"
IP	An IP value	"10.13.29.70" "127.0.0.1/16"

2. Numerical relational operators

Operators	Description	Supported data types	Examples
>	Greater than	Int, Float, Memory, IP	source_IP > 10.53.12.0
>=	Greater than or Equal to	Int, Float, Memory, IP	source_ip < 10.53.12.0
<	Less than	Int, Float, Memory, IP	source_IP < 10.53.12.0
<=	Less than or Equal to	Int, Float, Memory, IP	source_IP <= 10.53.12.0
=	Equal to	String, Int, Float, Memory, IP	EventID=4624
!=	Not Equal to	String, Int, Float, Memory, IP	EventID!=4624
in/IN	Equals to one of the elements	String, Int, Float, IP	EventID in (4624,4625)
notin/NOTIN	Not equals to any of the elements	String, Int, Float, IP	EventID notin (4624,4625)
isExist	Field isn't an empty string, and it isn't null.	For all fields	For all fields

Operators	Description	Supported data types	Examples
isNotExist	Field is an empty string, and it is null.	For all fields	isNotExist(source_ip)

3. String relational operators

Operators	Description	Examples
=	Equal to	username = "name"
!=	Not Equal to	username != "name"
contains/CONTAINS	Returns true if the field has a set of data	eventname contains "success"
notcontains/NOTCONTAINS	Returns true if the field hasn't set of data	eventname notcontains "success"
startswith/STARTSWITH	Returns true if the field value starts with data	username startswith "Ja"
endswith/ENDSWITH	Returns true if the field value ends with data	username endswith "kumar"
notstartswith/NOTSTARTSWITH	Returns true if the field value does not start with data	username notstartswith "Ja"
notendswith/NOTENDSWITH	Returns true if the field value does not end with data	username notendswith "kumar"
matches/MATCHES	Returns true if the field value matches the regex	username matches "pree*"
notmatches/NOTMATCHES	Returns true if the field value does not match the regex	username notmatches "pree*"
=	Equal to	username = "name"

4. Logical Operators

Operators	Description	Examples
Operators	Description	Examples
AND/and	Returns true only if both condition are true	username = "preethi" and eventid=4624
OR/or	Returns true if either of the condition is true, regardless of the other condition.	eventid = "4688" or eventid = "592"

Example

- Basic Criteria for Repeated failed SUDO commands:logtype="unix" and iename = "sudo command execution failed"
- Basic Criteria for Excessive password change failure:common_report_name = "user account password changes" and severity = "failure" or iename = "password update failure"
- Basic Criteria for Ryuk Wake on LAN Command:logtype in ("Windows", "Fortinet", "Sonic wall") and (eventid = "4688" or eventid = "592") and (commandline contains "8 lan" or commandline contains "9 rep")
- Basic criteria for window failed logon:logtype = "Windows" and actionname = "Failed logon"
- Basic criteria for success logon:actionname = "Success logon"

ⓘ NOTE:

- logtype will contain values such as *(include all logtype), Windows, Unix, Cisco, etc.
- Using actionname operator, we can use predefined actions in the query.

Query Syntax

The query language supports different operators and clauses. Below is the complete syntax reference.

1. Base syntax:

action_name:
logtype = (* | windows | syslog | ...) [logical_operator basic_criteria ...] with [aggregate_func(fieldname), ...]
Example: eventid = 4624

2. Sorting:

| sort fieldname (asc | desc)

3. Histogram:

| histo fieldname range(initial, initial to end) sort [aggregateField | count] (asc | desc)

4. Time window:

| timewindow value unit sort [aggregateField | count] (asc | desc) limit value having count operator value

5. Grouping:

| groupby fieldname with [aggregate_func(fieldname), ...] sort [aggregateExpr | count] (asc | desc) limit nums having [aggregateExpr | count] comparison_operator nums

ⓘ NOTE:

- Operators inside the brackets (groupby, histo, etc.) may appear in any order.
- The timeslice operator can occur only once.
- The groupby and histo operators can occur up to three times in any order.

6. Distinct:

| distinct fieldname sort (asc | desc) limit [1-200] having count operator value

7. Post-processing:

| having aggregateExpr operator value [logical_operator (aggregateExpr operator value)]
| isanomalous(field, model, field)

8. First and last:

| first [1-10] fieldname [, fieldname ...]
| last [1-10] fieldname [, fieldname ...]

9. Lookup:

| lookup <event-field> in <lookup-table.lookup-field> set <event-destfield> AS <lookup-table.lookup-destfield>

10. Definitions:

def: variable_name = <expression>
Supported types: int, string, float, time, boolean

11. Filtering:

filter: <condition>
This removes results that do not match the condition.

12. Event sequence:

follow: actionname1 followedby | notfollowedby actionname2 within [1-60] (millisecond | second | minute | hour | day)
Example: correlation-based detection of one event followed by another within 10 minutes.

13. Selection:

select action_name.field, action_name.fields, def_name

Advanced operator

1. isMalicious function
2. isVulnerable function
3. misConfiguredFor function

1. Is Malicious

- The 'isMalicious' condition is available only for IP address fields. It checks if the detected IP address is present in the predefined list of malicious IP addresses stored in the internal database.
- This function returns true or false.

Syntax: isMalicious(fieldname)
Example: External Remote Services
Failed Logon From Public IP:
logtype = "*" and eventid = 4625 and isExists(remoteip) and isMalicious(remoteip)

2. Is Vulnerable

- Available only after integration with Endpoint Central and can be used with device fields. Checks if a device is tagged as vulnerable in Endpoint Central and identifies devices vulnerable to specific attacks (e.g., CVE-2023-38831).
- This function returns true or false.

> NOTE:
>
> This operator is available only for EventLog Analyzer's continuous execution mode.

Syntax:
isVulnerable(fieldname)
isVulnerable(fieldname , matchvalue)
Examples:
A. Microsoft Outlook Vulnerability Exploitation
Outlook connecting to webDAV or SMB Share:
logtype = "windows" and eventid = 4656 and objectname contains "\REGISTRY\MACHINE\SYSTEM" or objectname contains "Services" or objectname contains "WebClient\NetworkProvider,LanmanWorkstation\NetworkProvider" and accesslist contains "ReadData (or ListDirectory)" and isVulnerable(Device Name, "CVE-2023-23397")
| groupby processname
Suspicious webDAV client execution via Rundll.exe:
logtype = "sysmon" and iename = "Sysmon Process Creation" and parentprocessname contains "svchost.exe" and parentprocesscommandline contains "-s WebClient" and processname contains "rundll.exe" and processname = Outlook connecting to webDAV or SMB Share.processname

B. AWS Failed logon

Error events:

logtype = "aws cloudtrail" and isVulnerable(errorcode)

3. MisconfiguredFor

Available only after integration with Endpoint Central and can be used with device fields. Detects devices with misconfigurations identified by Endpoint Central (e.g., Windows Credential Guard disabled).

> ⓘ NOTE:
>
> This operator is available only for EventLog Analyzer's continuous execution mode.

Syntax:

misConfiguredFor(fieldname , match_value)

Examples:

A. Built-in guest account privilege escalation

Successful Network Guest Logon:

logtype = "windows" and eventid = 4624 and username contains "Guest" and logontype = 3 and MisconfiguredFor(Devicename, "Built-in guest account is not disabled or properly restricted")

| groupby logonid

B. Privileged Operation Attempt:

logtype = "windows" and eventid = 4672 and logonid = Successful Network Guest Logon.logonid and MisconfiguredFor(Devicename, "Built-in guest account is not disabled or properly restricted")

C. User Account Local Group Membership change Attempt:

logtype = "windows" and eventid = 4732 and groupname contains "Administrators" and logonid = Successful Network Guest Logon.logonid and MisconfiguredFor(Devicename, "Built-in guest account is not disabled or properly restricted")

Query components

- Aggregation Function
- Sort Operator
- Timewindow Operator
- Groupby Operator
- Distinct Operator
- Having Operator
- First/Last Operator
- With Operator
- Order of Statements

1. Aggregation Function

Function	Description	Syntax	Example	Output
SUM	• Returns the sum of the selected values in the field. • Returns a single numerical value.	sum(field) or SUM(field)	sum(bytes_in)	3.27mb (3,432,605)
AVG	• Returns the average of the values in the field. • Returns a single numerical value.	avg(field) or AVG(field)	avg(_zl_timestamp)	1.36kb (1,393.156)
MAX	• Returns the maximum value in the field. • Returns a single numerical value.	max(field) or MAX(field)	max(received_bytes_i)	107.61kb (110,196)
MIN	• Returns the minimum value in the field. • Returns a single numerical value.	min(field) or MIN(field)	min(received_bytes_i)	107.61kb (110,196)
STDEV	• Returns the standard deviation of the given field. • Returns a single numerical value.	stdev(field) or STDEV(field)	stdev(_zl_timestamp)	2.46kb (2,521.297)
	• Returns the number of log messages that match the query. • With “with”			

Function	Description	Syntax	Example	Output
COUNT	• With "with" operator → returns a number. • With "having" operator → returns a boolean (true/false).	count	having count > 100	true/false
DCOUNT	Returns the count of distinct values. With "with" operator → returns a number. With "having" operator → returns a boolean (true/false).	dcount(field) or DCOUNT(field)	having dcount(_zl_host) > 2	true/false

2. Sort Operator

- Sorts all results by specified fields.
- By default results are sorted by count descending.
- After "sort", only non-aggregate fields are allowed.
- Syntax: sort fieldname1 (asc/desc) [, fieldname2 (asc/desc) ...]
- Example:
  - logtype="windows" and eventid = 4625 | sort username asc, hosttype desc

3. Timewindow Operator

- Groups logs into specified slices of time.
- After "sort", only aggregate fields are allowed.
- Max limit value for group by keyword is 1000.
- Possible timewindow units: y (year), M (month), w (week), d (day), h (hour), m (minute), s (second).
- Syntax: timewindow value unit sort [aggregateField, count] (asc/desc) limit value having count operator value
- Examples:
  - logtype="windows" | timewindow 5m
  - logtype="windows" | timewindow 5m sort count desc
  - logtype="windows" | timewindow 1h sort sum(bytes_in) as totalBytes asc
  - logtype="windows" | timewindow 1h sort timewindow desc
  - logtype="windows" | timewindow 5m limit 5
  - logtype="unix" and eventid = 4625 | timewindow 10m limit 10 having count > 100
  - logtype="windows" | timewindow 10m | groupby username

- logtype="windows" | timewindow 10m | groupby username

4. Groupby Operator

- Used to get unique values of a field.
- When multiple groupby fields are given, the first is primary and second is secondary.
- After "sort", only aggregate fields are allowed.
- Maximum limit for groupby is 1000.
- Syntax: groupby fieldname1 with aggregateField sort [aggregateField, count] [asc/desc] limit [1-1000] having aggregateExpr operator value
- Examples:
  - logtype="unix" | groupby username sort sum(sent_bytes_i) as total desc
  - logtype="unix" | groupby username sort sum(sent_bytes_i) as total desc limit 10 | groupby hostname
  - logtype="unix" | groupby username sort sum(sent_bytes_i) as total desc limit 10 | groupby hostname with sum(sent_bytes_i) as total
  - logtype="windows" and eventid = 4625 | groupby username having count > 100
  - logtype="windows" and eventid = 4625 | groupby username having avg(sent_bytes) as average > 10 MB
  - logtype="windows" | groupby username limit 20 | groupby hosttype having avg(sent_bytes_i) as average > 10MB | groupby hostname having sum(received_bytes_i) as total < 500 MB

5. Distinct Operator

- Fetches a table with only distinct values.
- Only one distinct field is allowed.
- Distinct field can only be sorted by count.
- Max limit for distinct = 200.
- Syntax: distinct fieldname sort (asc | desc) limit [1-200] having count operator value
- Examples:
  - logtype="windows" | distinct zuid
  - logtype="windows" | distinct zuid sort asc
  - logtype="windows" | distinct zuid limit 150
  - logtype="windows" | distinct location having count > 5

6. Having Operator

- Post-result operator. Used for outer aggregation conditions.
- Syntax: having aggregateExpr operator value [logical operator (aggregateExpr operator value)]
- Examples:
  - logtype="unix" and eventname contains "logon" | having count > 120
  - logtype="windows" and eventid = 4625 | having avg(sent_bytes) as average > 10 MB

- logtype="windows" and eventid = 4625 | having avg(sent_bytes) as average > 10 MB

7. First/Last Operator

- First operator returns the earliest logs, last operator returns the most recent logs.
- Either first or last can be used.
- Limit can be used with first/last.
- Maximum limit = 10.
- Syntax: first/last [1-10] fieldname1 (, fieldname2, ...)
- Examples:
  - logtype="windows" | groupby status | first 2 request_uri,remote_ip
  - logtype="windows" | groupby status | last 2 request_uri,remote_ip

8. With Operator

- Aggregate expression can be used in basic criteria and group operators.
- Syntax: with aggregateExpr (, aggregateExpr ...)
- Examples:
  - logtype="windows" and with sum(sent_bytes) as bytesSum, avg(received_bytes) as average | groupby srcip
  - logtype="windows" and | groupby srcip with sum(sent_bytes) as bytesSum, avg(received_bytes) as average

9. Order of Statements

| basic_criteria with field.aggregate_func [, field.aggregate_func, ...]
| sort field (asc/desc)
[| histo fieldname range(initial, initial to end) sort [aggregateField, count] [asc/desc]
| timewindow value limit value
| groupby field sort aggregate(field) (asc/desc) limit number]
| distinct field
| first/last [1-10] fieldname
| having (groupby_field.field / timewindow.count operator /
groupby_field.distinct_field.aggregate/aggregate_func.field) operator value
NOTE:

- Operators inside brackets may occur in any order.
- Timewindow can occur only once.
- Groupby and histo can occur up to three times in any order.

Lookup criteria

Lookup query

The lookup operator lets you fetch extra information from a lookup table.
It matches event field names and values with lookup table field names.

- If "set" is not used → it works like lookupcontains (checks if a key exists). It returns True/False.
- If "set" is used → it fetches values from the lookup table and stores them in fields you choose.

Syntax:

lookup event-field in lookup-table.lookup-field [and/or more conditions] (set lookup-table.lookup-destfield as newfield)

Examples:

- logtype = windows and eventid = 4625 → lookup username in user_details.user
- logtype = windows and eventid = 4625 → lookup username in user_details.user set user_details.ip_address as ip, user_details.port as port
- logtype = windows and eventid = 4625 → lookup username in user_details.user and device in user_details.hostname set user_details.ip_address as ip, user_details.port as port

Correlation criteria

1. Arithmetic operator
2. Correlation multi-action
3. Link statement
4. Sequence statement
5. Def and Filter statement
6. Select statement

1. Arithmetic operator

Operator	Description	Example
+	Add	timestamp + 3600000ms > 4800000
-	Subtract	timestamp - 3600000ms > 2400000
*	Multiply	ratio = (failure_event.count / access.count)
/	Divide	ratio = (failure_event.count / access.count) * 100

2. Correlation (Multi-Action)

- You can define multiple actions (e1, e2, etc.) with conditions.
- Each action must have basic criteria. Aggregate functions and lookups are optional.

- Syntax: actionname : basic_criteria | aggregate criteria | lookup_criteria | correlation_criteria
- Examples:
  - e1: logtype = cisco and common_report_name in (unix user added, firewall user added, user account created, computer account created)
  - e2: logtype = cisco and common_report_name in (computer account deleted, user account deleted, unix user deleted, firewall user deleted) and hosttype = e1.hosttype and targetuser = e1.targetuser and _zl_timestamp between e1._zl_timestamp and (e1._zl_timestamp + 3600000ms)

3. Link statement

- The link statement compares whether one action's field matches or does not match another action's field.
- You can combine it with other conditions using AND / OR / NOT.
- Syntax: fieldname (operator) actionname.fieldname [and/or more comparisons]
- Examples:
  - Brute force login
    - e1: logtype = windows and event_name = failed windows login | groupby username | groupby devicename
    - e2: logtype = windows and event_name = successful windows login and username = e1.username and devicename = e1.devicename
    - Sequence: e1 followedby e2 within 10m
    - Select e1.username, e2.devicename
  - Anomalous user account change
    - e1: logtype = windows and common_report_name in (unix user added, firewall user added, user account created, computer account created)
    - e2: logtype = windows and common_report_name in (computer account deleted, user account deleted, unix user deleted, firewall user deleted) and hosttype = e1.hosttype and targetuser = e1.targetuser and time >= e1.time
    - Select e1.hosttype, e1.targetuser

4. Sequence statement

- Defines whether one action follows or does not follow another within a specific time.
- You must always specify the time frame.
- Syntax: sequence : action1 (followedby / notfollowedby) action2 within time [and action2 followedby/notfollowedby action3 ...]
- Examples:
  - File Access Without Authorization
    - e1: logtype = windows and eventid = 4663 (object access attempt)
    - e2: logtype = windows and eventid = 4656 (handle requested)
    - Sequence: e1 notfollowedby e2 within 5m

        - Select e1.username, e1.devicename
    - Brute Force Login
        - e1: logtype = windows and event_name = failed windows login | groupby username | groupby devicename
        - e2: logtype = windows and event_name = successful windows login and username = e1.username and devicename = e1.devicename
        - Sequence: e1 followedby e2 within 10m
        - Select e1.username, e2.devicename
    - Ragnar Locker ransomware detection
        - e1: logtype = windows and processid = 4688 and processname = msiexec.exe
        - e2: logtype = windows and eventid = 4654 and objectname contains Program Files(X86) and endswith VirtualAppliances\va.exe and devicename = e1.devicename
        - e3: logtype = windows and processid = 4688 and processname = e2.objectname and devicename = e1.devicename
        - Sequence: e1 followedby e2 within 30m followedby e3 within 2m
    - Suspicious SQL Backup Activity
        - e1: logtype = windows and eventid = 4625 | distinct devicename
        - e2: logtype = windows and eventid = 4624 and devicename = e1.devicename and username = e1.username
        - e3: logtype = mssql and actionid = lgis
        - e4: logtype = * and action = ba
        - Sequence: e1 followedby e2 within 10m and e3 followedby e4 within 5m

5. Def and Filter statement

Def statement

- The def statement calculates an expression and puts the resulting value into a search results field.
- It is used to create a new field in your search results, and the values in that new field are the result of an expression.
- In a def statement, you can only get the overall count, average, or sum, such as action count or action-based field aggregation like 'e1.count' or 'e1.sent_bytes.sum'.
- Syntax: def: variable_name = actionname. (count / field.aggregate_function) operator actionname. (count | field.aggregate_function / value)

Filter statement

- The filter operator keeps only the records that match the filter criteria.
- The def statement field constraints will apply to the filter statement.
- Syntax: filter: (def_variable_name / actionname. (count / field.aggregate_function)) operator value

Example: Ratio of two events:

- access: logtype="windows" and
- failure_event: logtype="windows" and and
- def: ratio = count(failure_event) / count(access)
- def: percent = ratio * 100
- filter: percent > 50
- Select ratio, count(failure_event), count(access)

6. Select statement

- Select is used to display fields or aggregates you want to see in results.
- Syntax: select fields, aggregates
- Examples:
    - Excessive logon failures
        - e1: logtype = windows and common_report_name in (router logon failed, unix logon failed, firewall logon failed, logon failed, vpn logout, firewall logoff, failed cloud logon) | groupby username
        - Select e1._zl_timestamp, e1.hostname
    - Anomalous user account change
        - e1: logtype = windows and common_report_name in (unix user added, firewall user added, user account created, computer account created)
        - e2: logtype = * and common_report_name in (computer account deleted, user account deleted, unix user deleted, firewall user deleted) and hosttype = e1.hosttype and targetuser = e1.targetuser and _zl_timestamp between e1._zl_timestamp and (e1._zl_timestamp + 3600000ms)
        - Select e1._zl_timestamp, e1.log_uuid, e2._zl_timestamp, e2.log_uuid
    - Excessive VPN logon failure
        - failed_logon: logtype = * and eventtype = vpn_logon_failure | distinct username having count > 5
        - Select failed_logon.username, count(failed_logon)
    - Suspicious file access
        - file_access: logtype = windows and eventid = 4663 | groupby username | groupby objectname having count > 3
        - file_modified: logtype = windows and eventid = 4663 and type = modify and username = file_access.username and objectname = file_access.objectname
        - Sequence: file_access followedby file_modified within 5m
        - Select file_access.username, file_modified.objectname, count(file_access.objectname)

Use case specific examples

Below are practical examples of how query grammar can be applied to detect common security scenarios. Each example shows the query logic, supported operators, and output fields.

1. Successful Logon

Description: Detects successful logon events in Windows.

Query:

logtype = "Windows"

and eventid = 4624

and message contains "successful logon"

2. Excessive Failed Login attempts

Description: Flags usernames or devices with excessive failed login attempts.

Query:

logtype in ("windows", "unix")

and eventid = 4625

| groupby username

| groupby devicename having count > 10

3. Brute Force Login detection

Description: Detects brute-force attempts where multiple failed logins are followed by a successful login for the same user on the same device within a short time window.

Query:

Step 1 – Failed Logins (e1):

e1:

logtype = "windows"

and event_name = "Failed Windows Login"

| groupby username

| groupby devicename

Step 2 – Successful Login (e2):

e2:

logtype = "windows"

and event_name = "Successful Windows Login"

and username = e1.username

and devicename = e1.devicename

Sequence Logic:

e1 followedby e2 within 10m

Final output:

select e1.username, e2.devicename

4. Port Scanning attack

Description: Identifies devices or IPs scanning multiple ports within a short period.

Query:

e1:

logtype in ("unix", "windows", "sysmon")

and event_name = "allowed connection"

| groupby remoteip

```
| groupby host
| groupby port having count > 100
select e1.host, count(e1.host)
```

5. Data Exfiltration detection

Description: Detects unusually high outbound data transfer volumes.
Query:

```
netlog:
logtype = "unix"
and event_name = "allowed connection"
| groupby srcip
| groupby destip having sum(sentbytes) > 100MB
select netlog.srcip, netlog.destip, sum(netlog.sentbytes)
```

6. Ratio of Failed vs. Successful events

Description: Calculates the percentage of failed access events compared to total access events.
Query:
Step 1 – Total Access events:

```
access:
logtype = "*"
and type = "access"
```

Step 2 – Failed Access events:

```
failure_event:
logtype = "*"
and type = "access"
and status = "failure"
```

Define ratio:

```
def: ratio = (failure_event.count / access.count) * 100
```

Filter high failure rate:

```
filter: ratio > 50
```

Final output:

```
select ratio, access.count, failure_event.count
```

Detection rule limitation

Detection rule limitations specify the functional constraints and operator support across ELA and L3C correlation modes.
The below table details differences in supported operators, thresholds, aggregations, and query constructs between scheduled and continuous detection rules.

Feature	Description	EventLog Analyzer scheduled correlation	EventLog Analyzer continuous correlation	Log360 Cloud scheduled correlation	Log360 Cloud continuous correlation

Feature	Description	EventLog Analyzer scheduled correlation	EventLog Analyzer continuous correlation	Log360 Cloud scheduled correlation	Log360 Cloud continuous correlation
Numerical relational operator	Basic comparisons (>, <, =, !=, >=, <=, in, not in, exists, not exists, between, not between)	IP range not supported	All operators supported	IP range not supported	All operators supported
String relational operator	Text-based comparisons (contains, not contains, starts with, ends with, matches, not matches)	Matches and Not matches not supported	All operators supported	Matches and Not matches not supported	All operators supported
Logical operator	Logical conditions (and, or)	All supported	All supported	All supported	All supported
Advanced operator	Security checks (isMalicious, isVulnerable, misconfiguredFor)	Only isMalicious supported	All supported	None supported	Only isMalicious supported
Link to statement	Links actions in the criteria builder	Multiple + nested criteria supported	Multiple supported; nested not supported	Multiple + nested criteria supported	Up to 3 criteria supported; nested not supported
Threshold limits	Threshold count limit	No limit	Max limit 999	No limit	Default limit 10 (can be increased)
IN operator value limit	Max number of terms inside IN	25	25	25	25
Aggregation functions	Aggregates (sum, avg, max, min, stdev, percentile, count, distinct)	All supported	Only count and distinct supported	All supported	Only count and distinct supported
WITH operator	Use of aggregate functions in basic criteria	Up to 10 terms	Not supported	Up to 10 terms	Not supported
Sort	Sort results by fields	Supported (max 5	Not	Supported (max 5	Not

operator		fields)	supported	fields)	supported
Feature	Description	EventLog Analyzer scheduled correlation	EventLog Analyzer continuous correlation	Log360 Cloud scheduled correlation	Log360 Cloud continuous correlation
Time window operator	Sets time-based threshold	Up to 7 days; max 200	No limit (time window not supported)	Up to 1 day; max 200	Default 1 hour (extendable); time window not supported
Histo operator	Histogram functionality	Not supported	Not supported	Not supported	Not supported
GroupBy operator	Group fields in criteria	Max 3 fields	No limit	Max 3 fields (with restrictions)	Max 3 fields
Distinct operator	Distinct count in threshold/query	Only 1 distinct field (no sort/limit)	Only 1 distinct field (no sort/limit)	Only 1 distinct field (no sort/limit)	Only 1 distinct field (no sort/limit)
Max GroupBy + Distinct	Limit on combined use	Max 3 groupby + 1 distinct	Multiple groupby + 1 distinct	Either (max 2 groupby + 1 distinct) or (max 3 groupby + 0 distinct)	Max 3 groupby + 1 distinct
First/Last operator fields	Returns first or last record	Max 10 fields	Not supported	Max 10 fields	Not supported
isAnomalous operator	UEBA anomaly detection	–	–	–	–
Arithmetic operator	Arithmetic in queries	Supported	Not supported	Supported	Not supported
Maximum action limit	Number of actions allowed	Up to 10	Up to 10	Up to 3	Up to 3

Feature	Description	EventLog Analyzer scheduled correlation	EventLog Analyzer continuous correlation	Log360 Cloud scheduled correlation	Log360 Cloud continuous correlation
Sequence statement	Ordered event checks (followed by / not followed by)	Up to 7 days	Up to 30 days	Up to 1 day	Up to 1 hour
Def statement	Create new calculated fields	Max 10	Not supported	Max 10	Not supported
Filter statement	Keep records matching condition	Max 10	Not supported	Max 10	Not supported
Select statement	Choose fields (alias in scheduled rules only)	Max 20	Max 20	Max 20	Max 20
Query length	Maximum characters per query	10000	10000	10000	10000
Anomaly action in advanced rule	Cannot combine anomaly with threshold/groupby/distinct/link criteria	–	–	–	–

Read also

This document explained how query grammar supports advanced rule creation, from defining criteria with operators and functions to applying correlation logic and building practical detection use cases.

- Rule management overview
- Understanding rules
- Creating custom rules
- Managing rules
- Scheduled detection reports

4.1.2.6. Scheduled detection reports

Last updated on: September 12, 2025

In this page

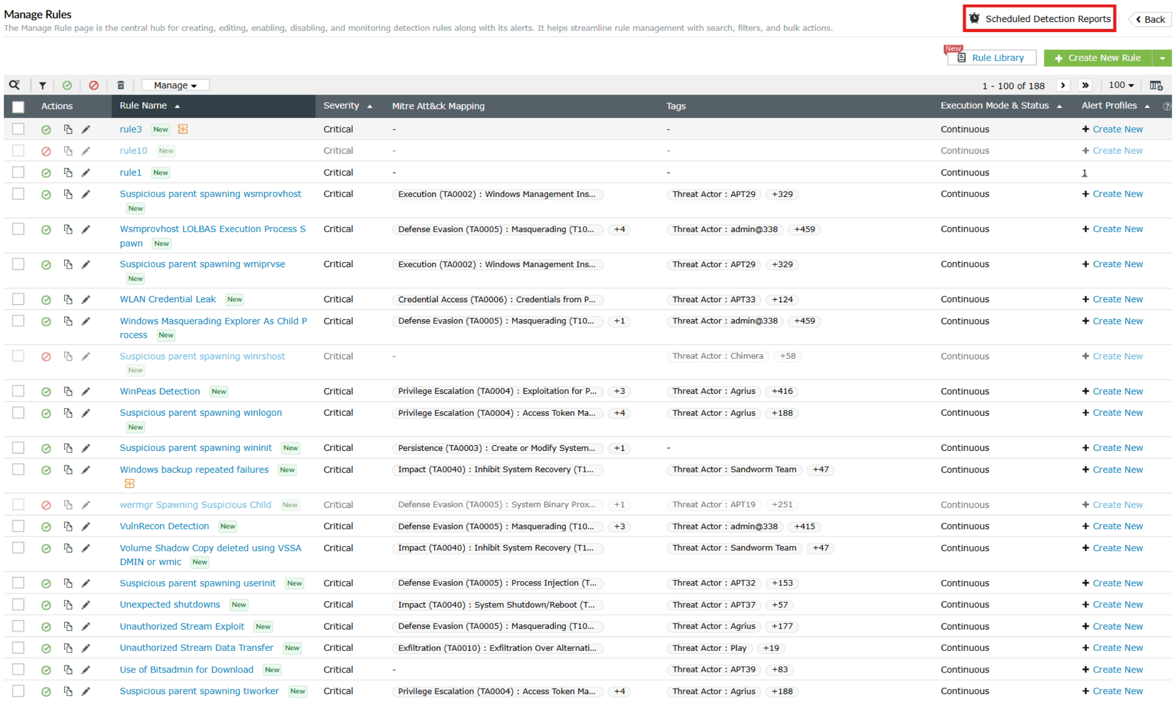
Overview

The Scheduled Detection Reports feature in the Manage Rules module provides a way to generate and export periodic reports for rule-based detections. Administrators can create new schedules, define frequency, select rules, configure export formats, and set notifications. These reports provide detailed visibility into detections over a specified time range, helping with trend analysis, compliance requirements, and continuous monitoring.

Scheduled detection reports (via the Manage Rules module)

Provides logs detected for a particular rule over a specified period of time.

1. You can access these reports by clicking on the Scheduled Detection Reports option in the Manage Rules module as highlighted below.



Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

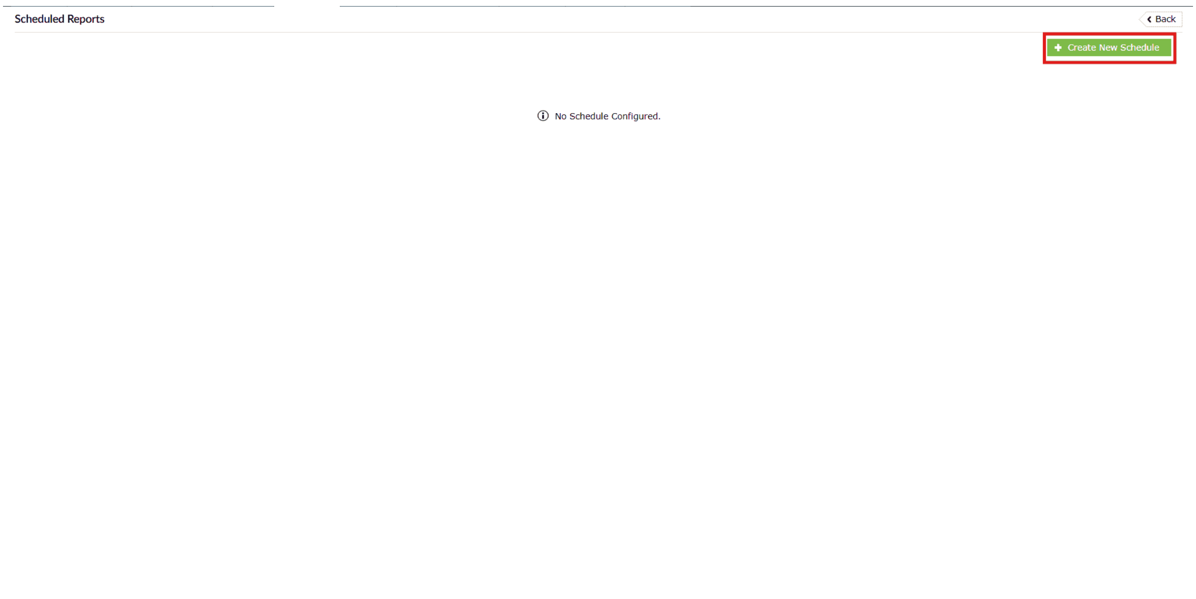
□	Actions	Rule Name	Severity	Mitre Att&ck Mapping	Tags	Execution Mode & Status	Alert Profiles
□	✓	rule3 New	Critical	-	-	Continuous	+ Create New
□	⊘	rule10 New	Critical	-	-	Continuous	+ Create New
□	✓	rule1 New	Critical	-	-	Continuous	1
□	✓	Suspicious parent spawning wsmprovhost New	Critical	Execution (TA0002) : Windows Management Ins...	Threat Actor : APT29 +329	Continuous	+ Create New
□	✓	Wsmprovhost LOLBAS Execution Process Spawn New	Critical	Defense Evasion (TA0005) : Masquerading (T10... +4	Threat Actor : admin@338 +459	Continuous	+ Create New
□	✓	Suspicious parent spawning wmiprvse New	Critical	Execution (TA0002) : Windows Management Ins...	Threat Actor : APT29 +329	Continuous	+ Create New
□	✓	WLAN Credential Leak New	Critical	Credential Access (TA0006) : Credentials from P...	Threat Actor : APT33 +124	Continuous	+ Create New
□	✓	Windows Masquerading Explorer As Child Process New	Critical	Defense Evasion (TA0005) : Masquerading (T10... +1	Threat Actor : admin@338 +459	Continuous	+ Create New
□	⊘	Suspicious parent spawning winrshost New	Critical	-	Threat Actor : Chimera +58	Continuous	+ Create New
□	✓	WinPeas Detection New	Critical	Privilege Escalation (TA0004) : Exploitation for P... +3	Threat Actor : Agrius +416	Continuous	+ Create New
□	✓	Suspicious parent spawning winlogon New	Critical	Privilege Escalation (TA0004) : Access Token Ma... +4	Threat Actor : Agrius +188	Continuous	+ Create New
□	✓	Suspicious parent spawning wininit New	Critical	Persistence (TA0003) : Create or Modify System... +1	-	Continuous	+ Create New
□	✓	Windows backup repeated failures New	Critical	Impact (TA0040) : Inhibit System Recovery (T1...	Threat Actor : Sandworm Team +47	Continuous	+ Create New
□	⊘	wermgr Spawning Suspicious Child New	Critical	Defense Evasion (TA0005) : System Binary Prox... +1	Threat Actor : APT19 +251	Continuous	+ Create New
□	✓	VulnRecon Detection New	Critical	Defense Evasion (TA0005) : Masquerading (T10... +3	Threat Actor : admin@338 +415	Continuous	+ Create New
□	✓	Volume Shadow Copy deleted using VSSADMIN or wmic New	Critical	Impact (TA0040) : Inhibit System Recovery (T1...	Threat Actor : Sandworm Team +47	Continuous	+ Create New
□	✓	Suspicious parent spawning userinit New	Critical	Defense Evasion (TA0005) : Process Injection (T...	Threat Actor : APT32 +153	Continuous	+ Create New
□	✓	Unexpected shutdowns New	Critical	Impact (TA0040) : System Shutdown/Reboot (T...	Threat Actor : APT37 +57	Continuous	+ Create New
□	✓	Unauthorized Stream Exploit New	Critical	Defense Evasion (TA0005) : Masquerading (T10...	Threat Actor : Agrius +177	Continuous	+ Create New
□	✓	Unauthorized Stream Data Transfer New	Critical	Exfiltration (TA0010) : Exfiltration Over Alternati...	Threat Actor : Play +19	Continuous	+ Create New
□	✓	Use of Bitsadmin for Download New	Critical	-	Threat Actor : APT39 +83	Continuous	+ Create New
□	✓	Suspicious parent spawning tiworker New	Critical	Privilege Escalation (TA0004) : Access Token Ma... +4	Threat Actor : Agrius +188	Continuous	+ Create New

Image 1: Scheduled reports in the manage rules module

2. You will be taken to the Scheduled Reports module.

To create a new schedule for the report(s)

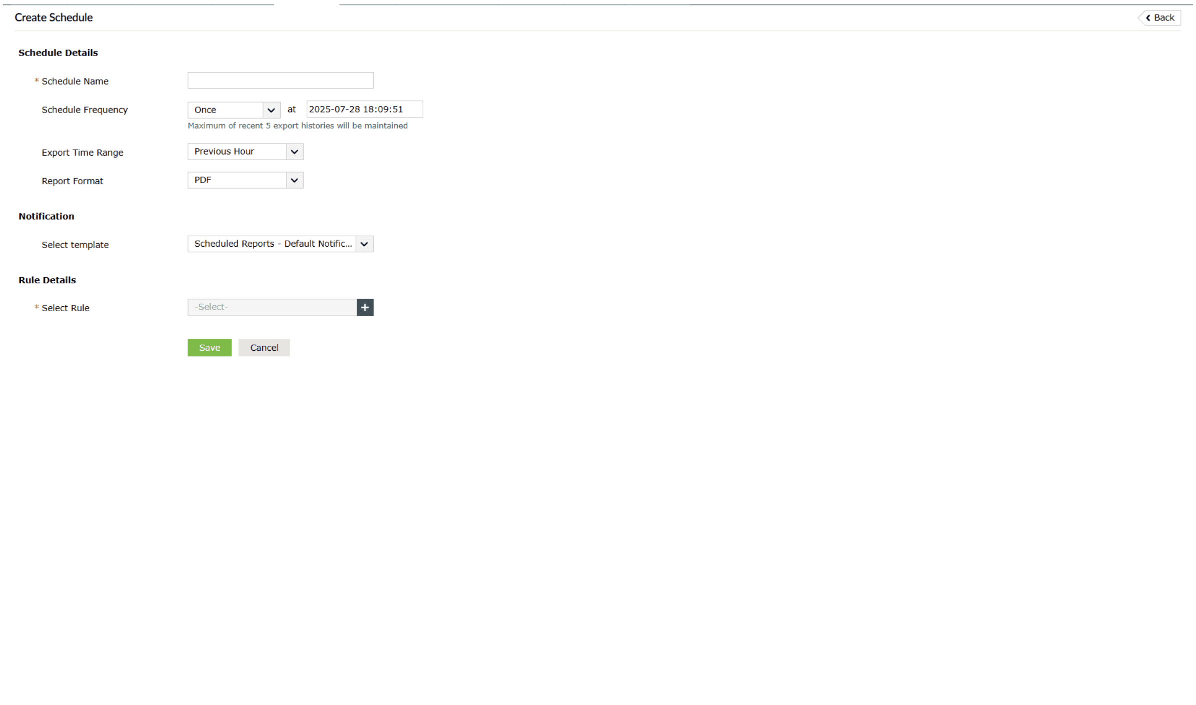
1. Click on the Create New Schedule button as highlighted below.


Scheduled Reports

No Schedule Configured.

Image 2: Create scheduled reports in the manage rules module

2. You will be taken to the Create Schedule module.


Create Schedule

Schedule Details

* Schedule Name

Schedule Frequency: Once at 2025-07-28 18:09:51

Maximum of recent 5 export histories will be maintained

Export Time Range: Previous Hour

Report Format: PDF

Notification

Select template: Scheduled Reports - Default Notific...

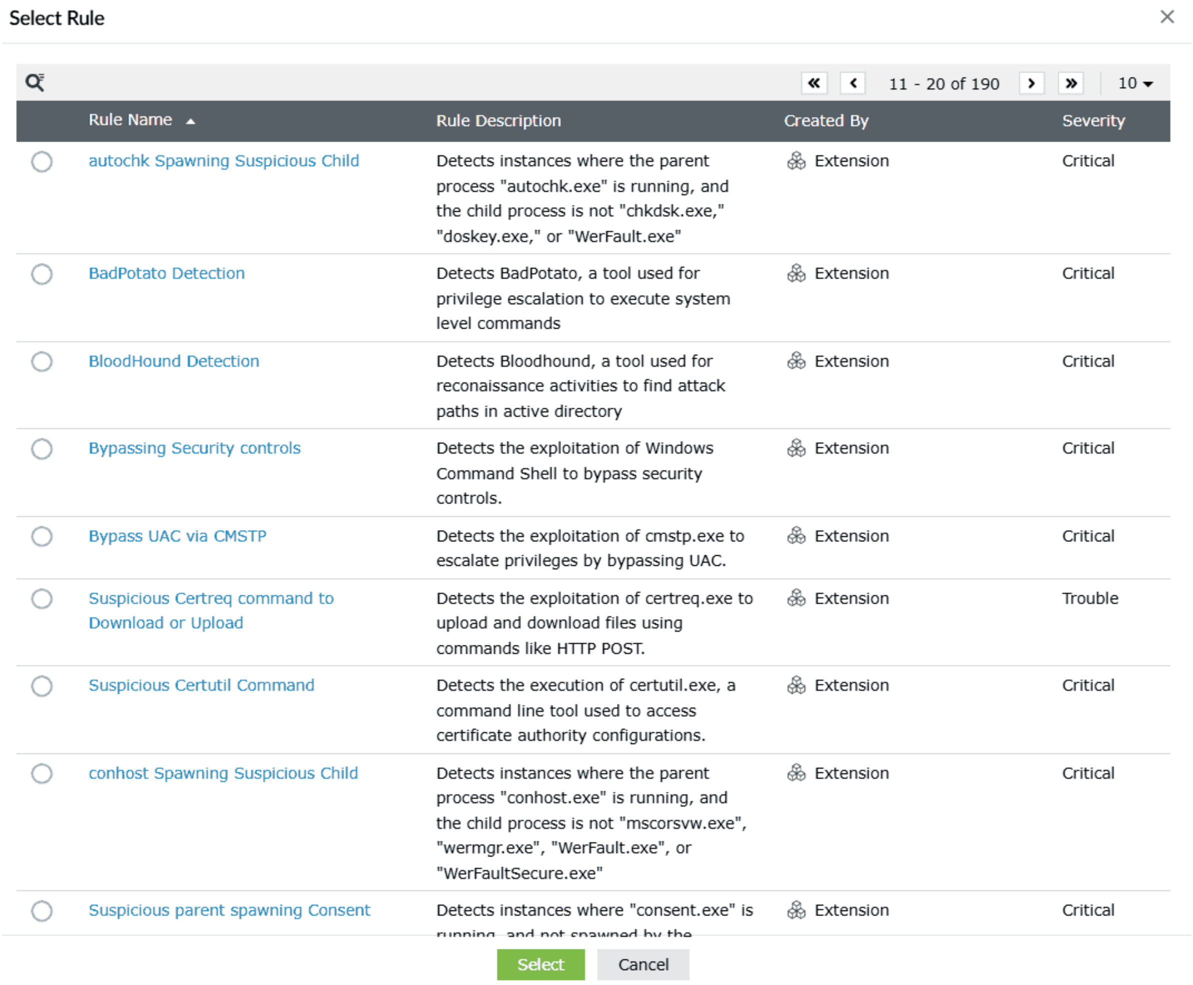
Rule Details

* Select Rule: -Select-

Image 3: Create scheduled reports in the manage rules module

- Schedule Details
    - Schedule Name: Assign a unique name to the schedule.
    - Schedule Frequency: Define how often the schedule should run (hourly, daily, weekly, or monthly).
    - Export Time Range: Specify the time range of data to include (e.g., last 24 hours, last 7 days, or custom).
    - Report Format: Choose the preferred format for the exported report (PDF, CSV, XLS).

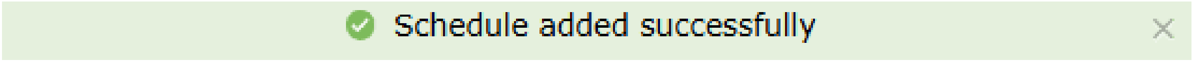
- Notification
  - Select Template: Pick a predefined report template or customize one.
- Rule Details
  - Select Rule: Choose the anomaly rule(s) you want to associate with the schedule. Reports and alerts generated will be based on the selected rules.



	Rule Name ▲	Rule Description	Created By	Severity
○	autochk Spawning Suspicious Child	Detects instances where the parent process "autochk.exe" is running, and the child process is not "chkdsk.exe," "doskey.exe," or "WerFault.exe"	Extension	Critical
○	BadPotato Detection	Detects BadPotato, a tool used for privilege escalation to execute system level commands	Extension	Critical
○	BloodHound Detection	Detects Bloodhound, a tool used for reconaissance activities to find attack paths in active directory	Extension	Critical
○	Bypassing Security controls	Detects the exploitation of Windows Command Shell to bypass security controls.	Extension	Critical
○	Bypass UAC via CMSTP	Detects the exploitation of cmstp.exe to escalate privileges by bypassing UAC.	Extension	Critical
○	Suspicious Certreq command to Download or Upload	Detects the exploitation of certreq.exe to upload and download files using commands like HTTP POST.	Extension	Trouble
○	Suspicious Certutil Command	Detects the execution of certutil.exe, a command line tool used to access certificate authority configurations.	Extension	Critical
○	conhost Spawning Suspicious Child	Detects instances where the parent process "conhost.exe" is running, and the child process is not "mscorsvw.exe", "wermgr.exe", "WerFault.exe", or "WerFaultSecure.exe"	Extension	Critical
○	Suspicious parent spawning Consent	Detects instances where "consent.exe" is running, and not spawned by the	Extension	Critical

Image 4: Create scheduled reports in the manage rules module

3. Click on Save after making all the required configurations. Upon successful completion of action, the below pop-up appears.



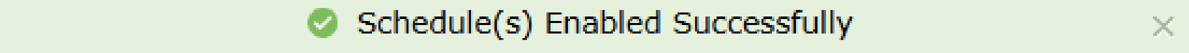
Schedule added successfully

To enable/disable a schedule for report(s)

To enable/disable a schedule for report(s)

Enabling a schedule

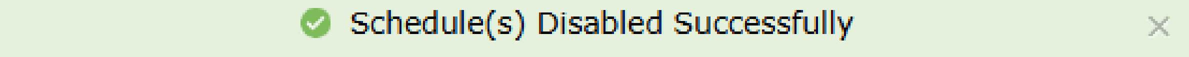
1. Click on the currently disabled icon ⊘ under the Actions column to enable the schedule.
2. As soon as you perform this action, the icon indicates that the schedule is now enabled ✓ and the below pop-up message appears briefly.



Schedule(s) Enabled Successfully

Disabling a schedule

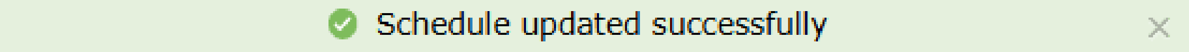
1. Click on the currently enabled icon ✓ under the Actions column to disable the schedule.
2. As soon as you perform this action, the icon indicates that the schedule is now disabled ⊘ and the below pop-up message appears briefly.



Schedule(s) Disabled Successfully

To edit a schedule for report(s)

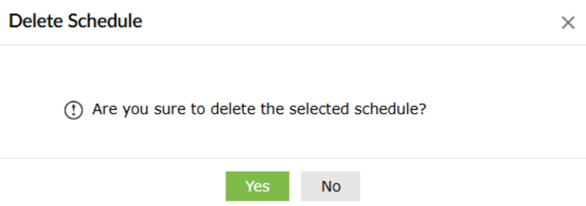
1. In the Scheduled Reports module, click on the edit ✎ icon under the Actions column.
2. The Edit Scheduled Reports module appears on the screen.
3. Make the necessary edits and click on the Update button. Upon successful completion of action, the below pop-up appears.



Schedule updated successfully

To delete a schedule for report(s)

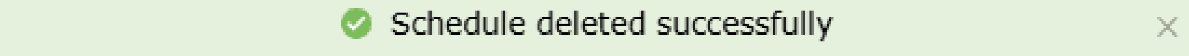
1. In the Scheduled Reports module, click on the delete 🗑 icon under the Actions column.
2. A Delete Schedule pop-up appears to confirm the action. Click on Yes.



Delete Schedule

Are you sure to delete the selected schedule?

3. Upon successful completion of action, the below pop-up appears.



Schedule deleted successfully

Read also

This document explained how to schedule detection reports, configure report details and notifications, and manage actions like enabling, disabling, editing, or deleting schedules.

- Rule management overview
- Understanding rules
- Creating custom rules
- Query grammar

- Managing rules

Chapter 4.1.3 **AD Object Filter**

4.1.3.1. Object filtering for Active Directory for rule fine tuning

Last updated on: September 12, 2025

In this page

Overview

The object-filter based rule fine-tuning for Active Directory enables you to optimize the detection rules by applying it specifically to certain AD objects to reduce false positives, alert fatigue and improve the rule accuracy. Using this intuitive object-filtering interface, the solution lets you to you can define users, groups or OUs (Organizational Units), interactive through GUI (Graphical User Interface). This ensures monitoring adapts automatically to directory changes, simplifies rule deployment, and improves alert relevance.
With re-engineered detection, object filters reduce alert fatigue for SOC teams by helping them fine-tune detections to specific users, groups, or OUs, reducing false positives and ensuring alerts stay actionable.

> NOTE
>
> Currently, the object filter capability is available only for pre-defined Windows and Active Directory rules.

Feature scope

The Object FIlter feature is accessible from the below modules:

- Rule library
- Rule management
- Alerts

Object selection and filtering

Object selection methods

1. Direct object selection

- You can select objects directly using Active DirectorySync data.
- The selection remains static for the chosen objects unless modified again.

2. Group or OU (Organizational Unit) based object selection

- Instead of selecting objects directly, you can assign specific OUs or groups.
- Membership objects within the OU or group are dynamically assigned based on the Active Directory sync data.

3. Manual values

- You can define manual values apart from value selection in the domain.
- The entered object name in manual values will be matched against criteria across all domains

Field specific object filters

Field	Available object filter options
User	User, Group based user, OU based user
Computer	• Computers, or • DCs (Domain Controllers), Member servers, Workstation
Group	Group, OU based group
OU	OU

Active Directory object filter behaviors

1. Domain object sync in the filter

Object syncing behavior varies based on the selected tabs in the object filter:

- Direct object selection
  - Sync is performed only for the selected object type.
- OU-based object selection
  - Sync includes both the OU and the associated object types within it.
  - For example, if it is OU-based user selection, both the OU and the user objects are synced accordingly

- For example, if it is OU-based user selection, both the OU and the user objects are synced accordingly.

- Group-based object selection
  - Membership sync is required to resolve group memberships accurately.
  - As per the framework design, this involves syncing User, Computer, OUs and Group objects as mandatory components to complete the membership resolution process.

2. Domain selection in the Filter

Domain behavior in the object filter depends on the feature usage context:

- In Alert Profiles
  - Domains listed in the object filter are based on the selected domains in the alert profile.
- In Rules
  - All available domains are listed in the object filter.

Selection behaviors

- Empty checkbox
  - If no objects are selected for a domain, No objects selected will be displayed with an empty checkbox.
- Partial selection
  - If some objects are selected, the domain checkbox appears partially selected.
  - The object count is displayed, and only those selected objects are used for object matching.
- Full selection
  - If the checkbox is fully selected, it indicates that all objects from the domain are included for matching.
  - All Users (or the applicable object type) is displayed.
- No domain configured
  - If no domains are configured, Add Domain Manually will be displayed.

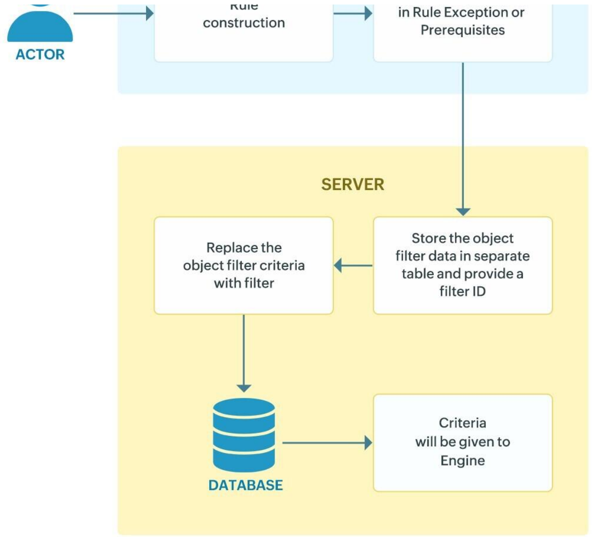
Prerequisites

License coverage details

- Direct object selection & manual values are accessible to those with Free and Basic plans.
- Group-based object selection and OU-based selection is accessible to those with a Standard plan subscription or higher tiers.

Workflow architecture

The following diagram illustrates the workflow of how the Object Filter operates. For clarity, the instance highlights its implementation within the Rule Management module.



ACTOR
Rule construction
in Rule Exception or Prerequisites
SERVER
Replace the object filter criteria with filter
Store the object filter data in separate table and provide a filter ID
DATABASE
Criteria will be given to Engine

Use cases

1. Automated alert customization with group & OU-based filters

Use case
Security teams and other key operational divisions often struggle with high alert noise because rules apply broadly across all users and devices, generating unnecessary signals from non-critical accounts.
With object filtering
Analysts can assign rules to specific OUs or security groups, ensuring only critical accounts and systems are monitored. Membership updates are synced dynamically via Active Directory, eliminating the need for manual rule edits. This allows the various operational teams to maintain focus on sensitive entities while cutting down false positives from routine operations.

2. Streamlined rule deployment across business units

Use case
Global organizations with distributed Active Directory environments face challenges when deploying uniform rules since objects vary across regions and business units.
With object filtering
Rules can be installed with OU-based user grouping, automatically pulling the correct set of objects per region. This enables region-specific monitoring without separate configurations, reduces administrative overhead, and ensures each division has accurate, localized detection coverage.

3. Exception handling for authorized administrative actions

Use case
Routine IT maintenance tasks (e.g., patching, group policy updates) frequently overlap with suspicious behavior patterns and trigger unnecessary alerts.
With object filtering
The Exceptions section lets teams exclude trusted accounts, devices, or OUs from rule conditions. By suppressing benign activity, SOCs can prioritize high-fidelity alerts without compromising visibility into sensitive changes elsewhere.

Limitations

- General
  - Object filter is available only for the Equals and NotEquals operators.
  - Object filter works on the latest synced domain data. If changes occur in Active Directory but are not yet synced, the filter processes data based on the last synced state.
- Alerts and rules
  - Object Selection: Maximum of 25 objects per domain for a field

Read also

This document explained how the Active Directory-based object filtering works, including selection methods, behaviors, prerequisites, and common use cases. You also learned how it helps cut alert noise, streamline deployments, and handle exceptions effectively.

- Accessing and applying object filtering in Log360

4.1.3.2. Accessing and applying object filtering

Last updated on: September 12, 2025

In this page

Overview

Object filtering capability lets you refine rules using intuitive GUI (Graphical User Interface), for optimized functionality by allowing you to apply the rules for specific users, groups, or OUs (Organizational Units) of Active Directory for improved results. This helps ensure that monitoring and exceptions target the right entities without unnecessary noise.

> NOTE
>
> The object filter capability is available only for pre-defined Windows and Active Directory rules.

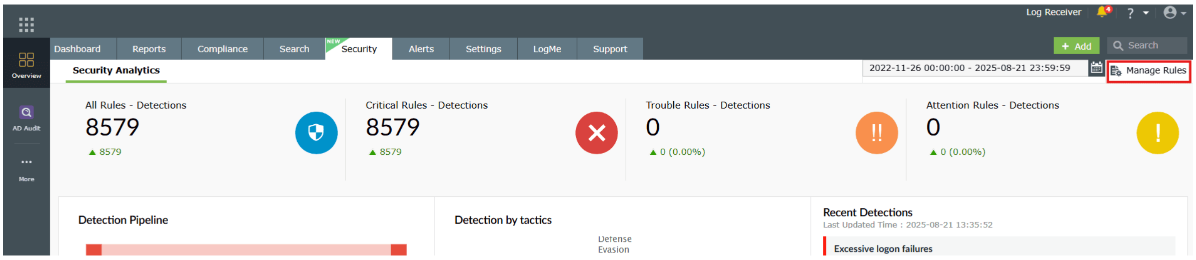
Implementing object-filtering

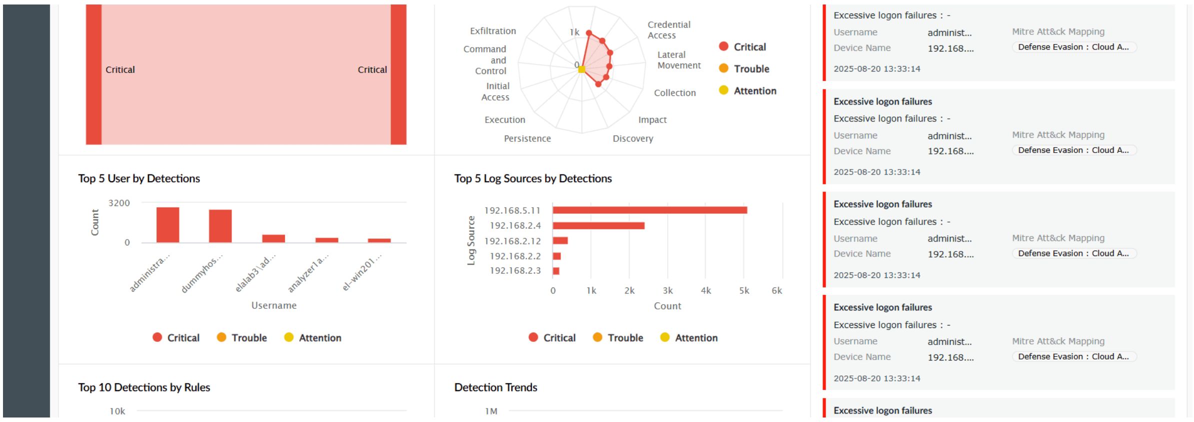
Object filtering can be applied at different points in the product to refine rule and alert configurations. You can set filters during rule installation via the Rule Library, adjust them in Rule Management by configuring Objects and Exceptions, apply them while enabling rules, and configure them within Alerts for precise monitoring.

Rule library

The solution lets you configure object filters for the rules even at the time of installation from the Rule Library. To do this,

1. Access the solution's web console, navigate to the Security tab to access the Security Analytics Dashboard and click on Manage Rules in the top-right corner.





Excessive logon failures : -

Username administ... Mitre Att&ck Mapping

Device Name 192.168.... Defense Evasion : Cloud A...

2025-08-20 13:33:14

Excessive logon failures

Excessive logon failures : -

Username administ... Mitre Att&ck Mapping

Device Name 192.168.... Defense Evasion : Cloud A...

2025-08-20 13:33:14

Excessive logon failures

Excessive logon failures : -

Username administ... Mitre Att&ck Mapping

Device Name 192.168.... Defense Evasion : Cloud A...

2025-08-20 13:33:14

Excessive logon failures

Excessive logon failures : -

Username administ... Mitre Att&ck Mapping

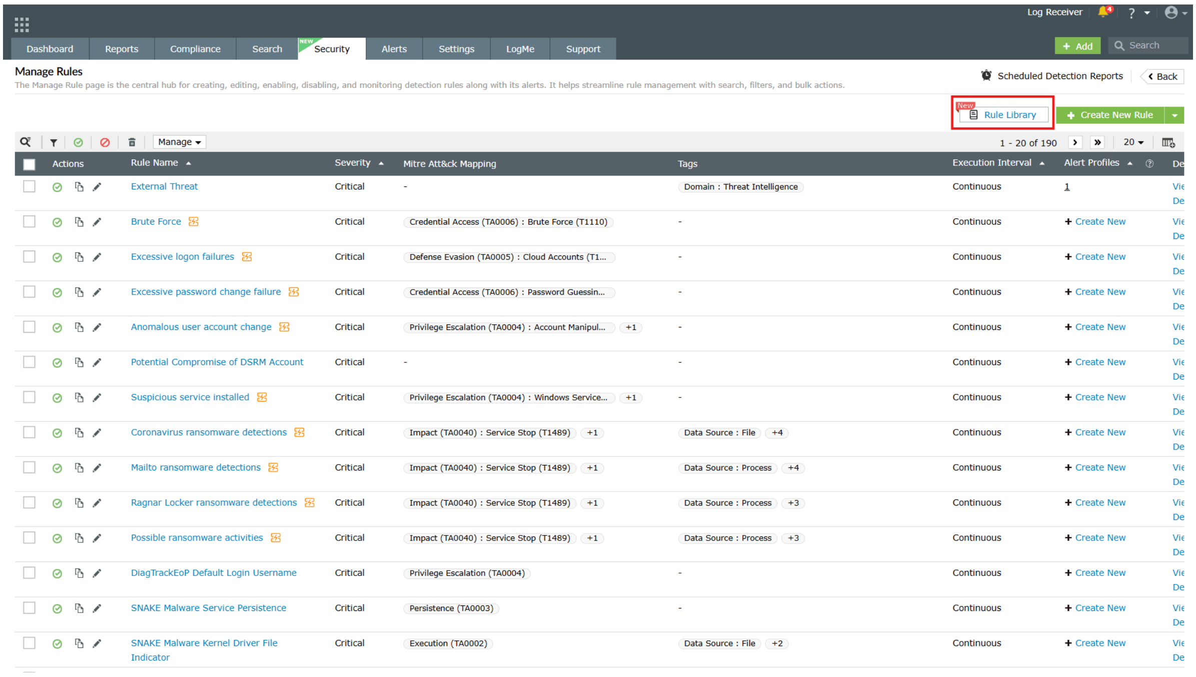
Device Name 192.168.... Defense Evasion : Cloud A...

2025-08-20 13:33:14

Excessive logon failures

Image 1: Security dashboard widgets

2. In the Manage Rules module, click on Rule Library.



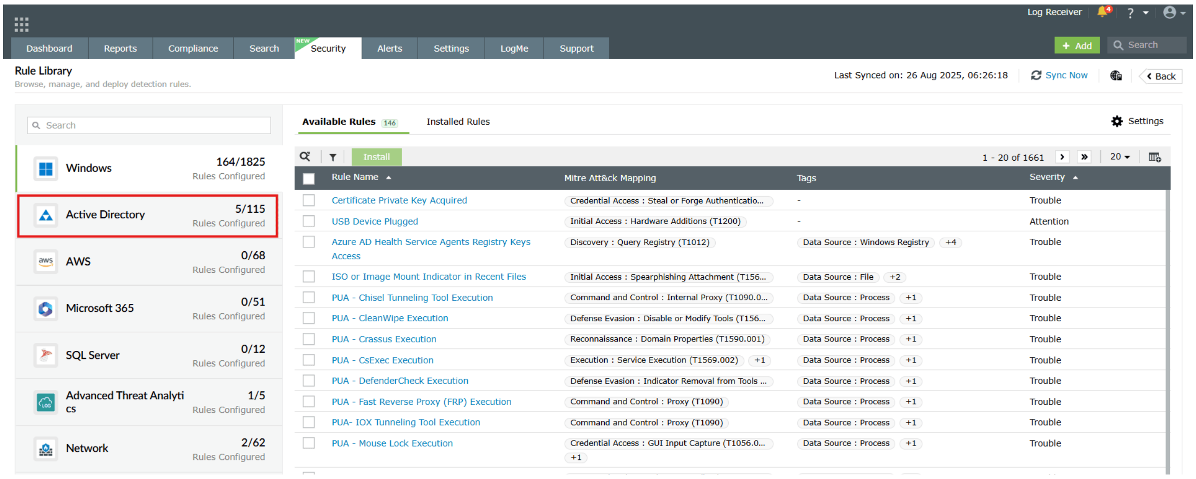
Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

Actions	Rule Name	Severity	Mitre Att&ck Mapping	Tags	Execution Interval	Alert Profiles	De
□	External Threat	Critical	-	Domain : Threat Intelligence	Continuous	1	Vie De
□	Brute Force	Critical	Credential Access (TA0006) : Brute Force (T1110)	-	Continuous	+ Create New	Vie De
□	Excessive logon failures	Critical	Defense Evasion (TA0005) : Cloud Accounts (T1...	-	Continuous	+ Create New	Vie De
□	Excessive password change failure	Critical	Credential Access (TA0006) : Password Guessin...	-	Continuous	+ Create New	Vie De
□	Anomalous user account change	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	-	Continuous	+ Create New	Vie De
□	Potential Compromise of DSRM Account	Critical	-	-	Continuous	+ Create New	Vie De
□	Suspicious service installed	Critical	Privilege Escalation (TA0004) : Windows Service... +1	-	Continuous	+ Create New	Vie De
□	Coronavirus ransomware detections	Critical	Impact (TA0040) : Service Stop (T1489) +1	Data Source : File +4	Continuous	+ Create New	Vie De
□	Mailto ransomware detections	Critical	Impact (TA0040) : Service Stop (T1489) +1	Data Source : Process +4	Continuous	+ Create New	Vie De
□	Ragnar Locker ransomware detections	Critical	Impact (TA0040) : Service Stop (T1489) +1	Data Source : Process +3	Continuous	+ Create New	Vie De
□	Possible ransomware activities	Critical	Impact (TA0040) : Service Stop (T1489) +1	Data Source : Process +3	Continuous	+ Create New	Vie De
□	DiagTrackEoP Default Login Username	Critical	Privilege Escalation (TA0004)	-	Continuous	+ Create New	Vie De
□	SNAKE Malware Service Persistence	Critical	Persistence (TA0003)	-	Continuous	+ Create New	Vie De
□	SNAKE Malware Kernel Driver File Indicator	Critical	Execution (TA0002)	Data Source : File +2	Continuous	+ Create New	Vie De

Image 2: Rule library in manage rules module

3. The object filter is available for both Windows and Active Directory rules. Click on the Active Directory category available in the left pane if you wish to apply the filter for these rules in specific.



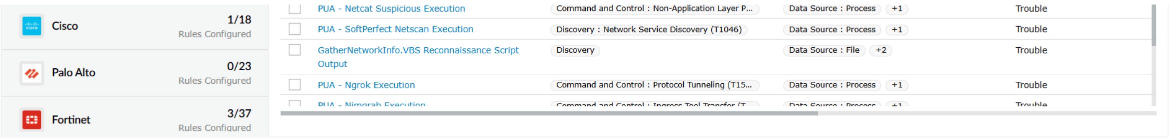
Rule Library

Browse, manage, and deploy detection rules.

Last Synced on: 26 Aug 2025, 06:26:18

Windows	164/1825	Rules Configured
Active Directory	5/115	Rules Configured
AWS	0/68	Rules Configured
Microsoft 365	0/51	Rules Configured
SQL Server	0/12	Rules Configured
Advanced Threat Analytics	1/5	Rules Configured
Network	2/62	Rules Configured

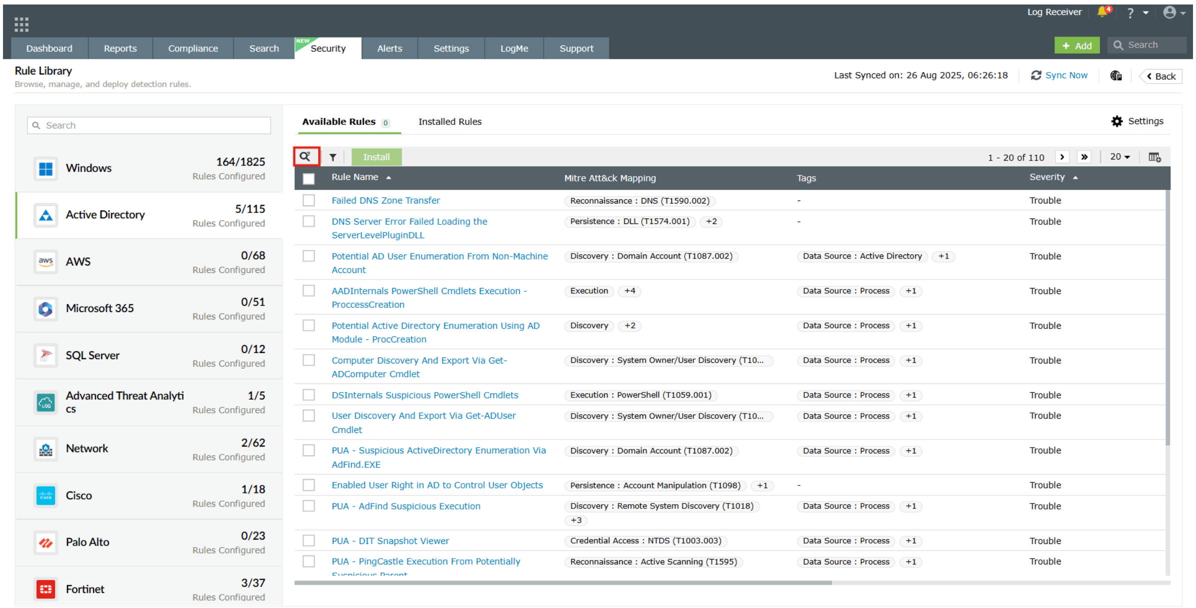
□	Rule Name	Mitre Att&ck Mapping	Tags	Severity
□	Certificate Private Key Acquired	Credential Access : Steal or Forge Authenticatio...	-	Trouble
□	USB Device Plugged	Initial Access : Hardware Additions (T1200)	-	Attention
□	Azure AD Health Service Agents Registry Keys Access	Discovery : Query Registry (T1012)	Data Source : Windows Registry +4	Trouble
□	ISO or Image Mount Indicator in Recent Files	Initial Access : Spearphishing Attachment (T156...	Data Source : File +2	Trouble
□	PUA - Chisel Tunneling Tool Execution	Command and Control : Internal Proxy (T1090.0...	Data Source : Process +1	Trouble
□	PUA - CleanWipe Execution	Defense Evasion : Disable or Modify Tools (T156...	Data Source : Process +1	Trouble
□	PUA - Crassus Execution	Reconnaissance : Domain Properties (T1590.001)	Data Source : Process +1	Trouble
□	PUA - CsExec Execution	Execution : Service Execution (T1569.002) +1	Data Source : Process +1	Trouble
□	PUA - DefenderCheck Execution	Defense Evasion : Indicator Removal from Tools ...	Data Source : Process +1	Trouble
□	PUA - Fast Reverse Proxy (FRP) Execution	Command and Control : Proxy (T1090)	Data Source : Process +1	Trouble
□	PUA- IOX Tunneling Tool Execution	Command and Control : Proxy (T1090)	Data Source : Process +1	Trouble
□	PUA - Mouse Lock Execution	Credential Access : GUI Input Capture (T1056.0... +1	Data Source : Process +1	Trouble


Cisco 1/18 Rules Configured
Palo Alto 0/23 Rules Configured
Fortinet 3/37 Rules Configured

□				
□	PUA - Netcat Suspicious Execution	Command and Control : Non-Application Layer P...	Data Source : Process +1	Trouble
□	PUA - SoftPerfect Netscan Execution	Discovery : Network Service Discovery (T1046)	Data Source : Process +1	Trouble
□	GatherNetworkInfo.VBS Reconnaissance Script Output	Discovery	Data Source : File +2	Trouble
□	PUA - Ngrok Execution	Command and Control : Protocol Tunneling (T15...	Data Source : Process +1	Trouble

Image 3: Rule library in manage rules module

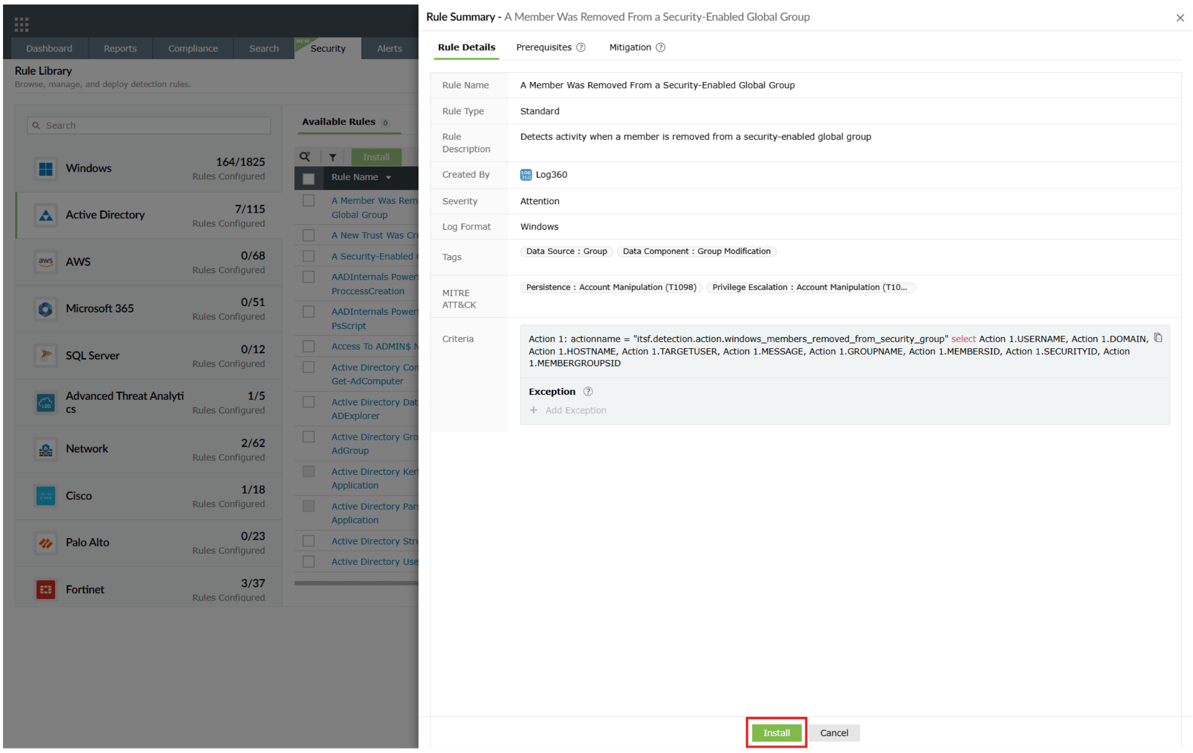
4. Click on the required rule name. You can use the search feature available to find the rule quickly.


Log Receiver
Dashboard
Reports
Compliance
Search
Security
Alerts
Settings
LogMe
Support
+ Add
Search
Rule Library
Browse, manage, and deploy detection rules.
Last Synced on: 26 Aug 2025, 06:26:18
Sync Now
Back
Search
Windows 164/1825 Rules Configured
Active Directory 5/115 Rules Configured
AWS 0/68 Rules Configured
Microsoft 365 0/51 Rules Configured
SQL Server 0/12 Rules Configured
Advanced Threat Analytics 1/5 Rules Configured
Network 2/62 Rules Configured
Cisco 1/18 Rules Configured
Palo Alto 0/23 Rules Configured
Fortinet 3/37 Rules Configured
Available Rules 0
Installed Rules
Settings
Install
1 - 20 of 110
20

□	Rule Name ▲	Mitre Att&ck Mapping	Tags	Severity ▲
□	Failed DNS Zone Transfer	Reconnaissance : DNS (T1590.002)	-	Trouble
□	DNS Server Error Failed Loading the ServerLevelPluginDLL	Persistence : DLL (T1574.001) +2	-	Trouble
□	Potential AD User Enumeration From Non-Machine Account	Discovery : Domain Account (T1087.002)	Data Source : Active Directory +1	Trouble
□	AADInternals PowerShell Cmdlets Execution - ProccessCreation	Execution +4	Data Source : Process +1	Trouble
□	Potential Active Directory Enumeration Using AD Module - ProcCreation	Discovery +2	Data Source : Process +1	Trouble
□	Computer Discovery And Export Via Get-ADComputer Cmdlet	Discovery : System Owner/User Discovery (T10...	Data Source : Process +1	Trouble
□	DSInternals Suspicious PowerShell Cmdlets	Execution : PowerShell (T1059.001)	Data Source : Process +1	Trouble
□	User Discovery And Export Via Get-ADUser Cmdlet	Discovery : System Owner/User Discovery (T10...	Data Source : Process +1	Trouble
□	PUA - Suspicious ActiveDirectory Enumeration Via AdFind.EXE	Discovery : Domain Account (T1087.002)	Data Source : Process +1	Trouble
□	Enabled User Right in AD to Control User Objects	Persistence : Account Manipulation (T1098) +1	-	Trouble
□	PUA - AdFind Suspicious Execution	Discovery : Remote System Discovery (T1018) +3	Data Source : Process +1	Trouble
□	PUA - DIT Snapshot Viewer	Credential Access : NTDS (T1003.003)	Data Source : Process +1	Trouble
□	PUA - PingCastle Execution From Potentially	Reconnaissance : Active Scanning (T1595)	Data Source : Process +1	Trouble

Image 4: Rule library in manage rules module

5. Clicking on the rule prompts open the Rule Summary box and the install button. Click on Install.

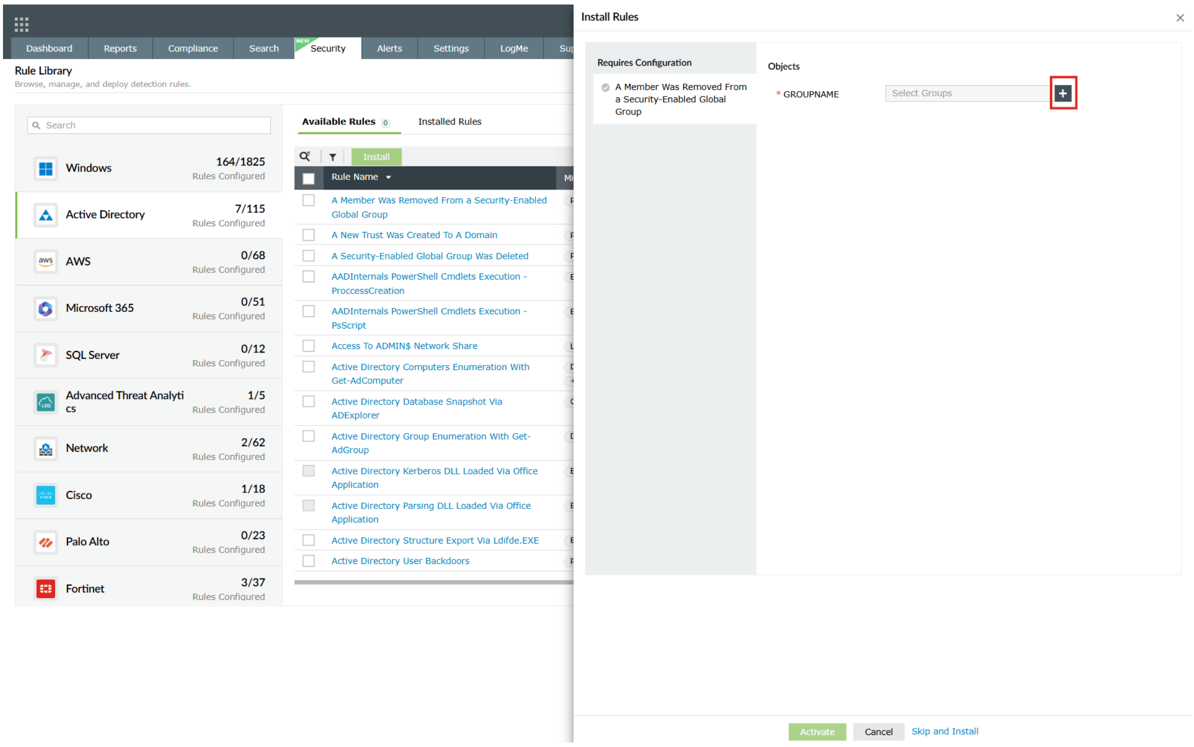

Dashboard
Reports
Compliance
Search
Security
Alerts
Rule Library
Browse, manage, and deploy detection rules.
Search
Windows 164/1825 Rules Configured
Active Directory 7/115 Rules Configured
AWS 0/68 Rules Configured
Microsoft 365 0/51 Rules Configured
SQL Server 0/12 Rules Configured
Advanced Threat Analytics 1/5 Rules Configured
Network 2/62 Rules Configured
Cisco 1/18 Rules Configured
Palo Alto 0/23 Rules Configured
Fortinet 3/37 Rules Configured
Available Rules 0
Install
Rule Name
Rule Details
Prerequisites
Mitigation
Install
Cancel

Rule Summary - A Member Was Removed From a Security-Enabled Global Group

Rule Name	A Member Was Removed From a Security-Enabled Global Group
Rule Type	Standard
Rule Description	Detects activity when a member is removed from a security-enabled global group
Created By	Log360
Severity	Attention
Log Format	Windows
Tags	Data Source : Group Data Component : Group Modification
MITRE ATT&CK	Persistence : Account Manipulation (T1098) Privilege Escalation : Account Manipulation (T10...
Criteria	Action 1: actionname = "itsf.detection.action.windows_members_removed_from_security_group" select Action 1.USERNAME, Action 1.DOMAIN, Action 1.HOSTNAME, Action 1.TARGETUSER, Action 1.MESSAGE, Action 1.GROUPNAME, Action 1.MEMBERSID, Action 1.SECURITYID, Action 1.MEMBERGROUPSID Exception + Add Exception

Image 5: Rule details in rule library

6. After clicking on Install, the Install Rules box slides open. Click on the add icon as highlighted below.



Dashboard | Reports | Compliance | Search | Security | Alerts | Settings | LogMe | Su

Rule Library
Browse, manage, and deploy detection rules.

Windows	164/1825 Rules Configured
Active Directory	7/115 Rules Configured
AWS	0/68 Rules Configured
Microsoft 365	0/51 Rules Configured
SQL Server	0/12 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	2/62 Rules Configured
Cisco	1/18 Rules Configured
Palo Alto	0/23 Rules Configured
Fortinet	3/37 Rules Configured

Available Rules 0 | Installed Rules

Install

Rule Name

- A Member Was Removed From a Security-Enabled Global Group
- A New Trust Was Created To A Domain
- A Security-Enabled Global Group Was Deleted
- AADInternals PowerShell Cmdlets Execution - ProccessCreation
- AADInternals PowerShell Cmdlets Execution - PsScript
- Access To ADMIN$ Network Share
- Active Directory Computers Enumeration With Get-AdComputer
- Active Directory Database Snapshot Via ADExplorer
- Active Directory Group Enumeration With Get-AdGroup
- Active Directory Kerberos DLL Loaded Via Office Application
- Active Directory Parsing DLL Loaded Via Office Application
- Active Directory Structure Export Via Ldifde.EXE
- Active Directory User Backdoors

Install Rules

Requires Configuration
A Member Was Removed From a Security-Enabled Global Group

Objects
* GROUPNAME | Select Groups | +

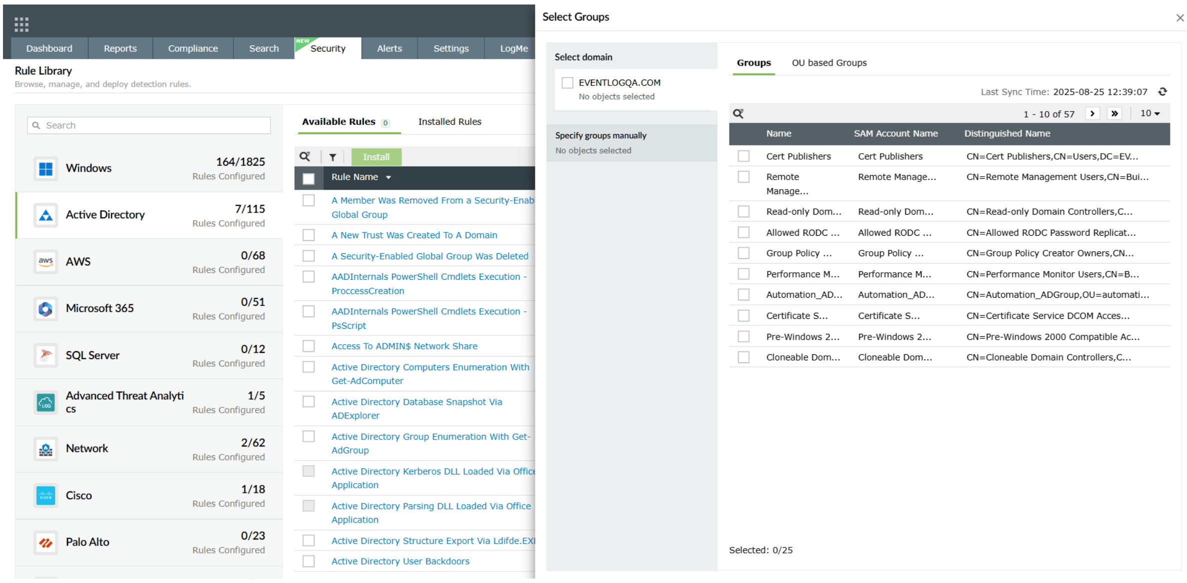
Activate | Cancel | Skip and Install

Image 6: Object filter in rule details in rule library

NOTE

You can choose to skip the below process by clicking on the Skip and Install option available in the Install Rules panel.

7. You will be taken to the Groups sub-tab displayed along with the object filter feature in order to be able to filter and choose what groups of users you wish to group under this rule before installation itself.



Dashboard | Reports | Compliance | Search | Security | Alerts | Settings | LogMe

Rule Library
Browse, manage, and deploy detection rules.

Windows	164/1825 Rules Configured
Active Directory	7/115 Rules Configured
AWS	0/68 Rules Configured
Microsoft 365	0/51 Rules Configured
SQL Server	0/12 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	2/62 Rules Configured
Cisco	1/18 Rules Configured
Palo Alto	0/23 Rules Configured

Available Rules 0 | Installed Rules

Install

Rule Name

- A Member Was Removed From a Security-Enab
- A New Trust Was Created To A Domain
- A Security-Enabled Global Group Was Deleted
- AADInternals PowerShell Cmdlets Execution - ProccessCreation
- AADInternals PowerShell Cmdlets Execution - PsScript
- Access To ADMIN$ Network Share
- Active Directory Computers Enumeration With Get-AdComputer
- Active Directory Database Snapshot Via ADExplorer
- Active Directory Group Enumeration With Get-AdGroup
- Active Directory Kerberos DLL Loaded Via Offic Application
- Active Directory Parsing DLL Loaded Via Office Application
- Active Directory Structure Export Via Ldifde.EX
- Active Directory User Backdoors

Select Groups

Select domain
□ EVENTLOGQA.COM
No objects selected

Specify groups manually
No objects selected

Groups | OU based Groups

Last Sync Time: 2025-08-25 12:39:07

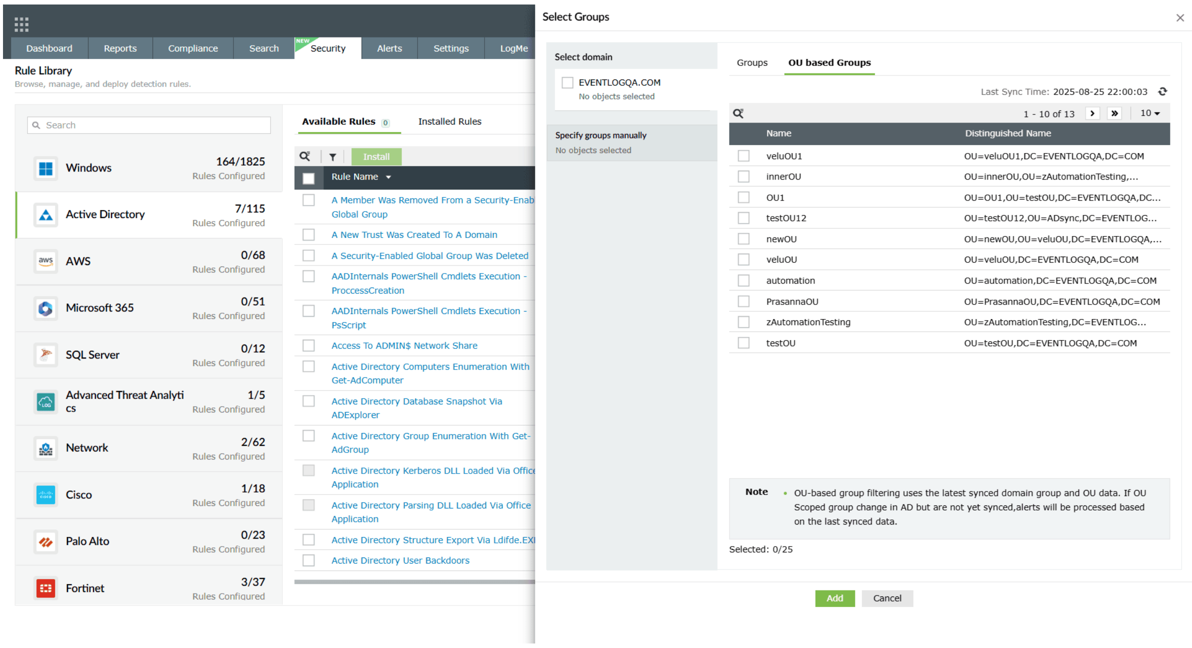
1 - 10 of 57 | 10

Name	SAM Account Name	Distinguished Name
Cert Publishers	Cert Publishers	CN=Cert Publishers,CN=Users,DC=EV...
Remote Manage...	Remote Manage...	CN=Remote Management Users,CN=Bui...
Read-only Dom...	Read-only Dom...	CN=Read-only Domain Controllers,C...
Allowed RODC ...	Allowed RODC ...	CN=Allowed RODC Password Replicat...
Group Policy ...	Group Policy ...	CN=Group Policy Creator Owners,CN...
Performance M...	Performance M...	CN=Performance Monitor Users,CN=B...
Automation_AD...	Automation_AD...	CN=Automation_ADGroup,OU=automati...
Certificate S...	Certificate S...	CN=Certificate Service DCOM Acces...
Pre-Windows 2...	Pre-Windows 2...	CN=Pre-Windows 2000 Compatible Ac...
Cloneable Dom...	Cloneable Dom...	CN=Cloneable Domain Controllers,C...

Selected: 0/25

Image 7: Applying object filter in rule details in rule library

8. Similarly, the OU based Groups sub-tab also includes the filter for user selection.


Dashboard
Reports
Compliance
Search
Security
Alerts
Settings
LogMe
Rule Library
Browse, manage, and deploy detection rules.
Search
Windows 164/1825 Rules Configured
Active Directory 7/115 Rules Configured
AWS 0/68 Rules Configured
Microsoft 365 0/51 Rules Configured
SQL Server 0/12 Rules Configured
Advanced Threat Analytics 1/5 Rules Configured
Network 2/62 Rules Configured
Cisco 1/18 Rules Configured
Palo Alto 0/23 Rules Configured
Fortinet 3/37 Rules Configured
Available Rules 0
Installed Rules
Install
Rule Name
A Member Was Removed From a Security-Enab Global Group
A New Trust Was Created To A Domain
A Security-Enabled Global Group Was Deleted
AADInternals PowerShell Cmdlets Execution - ProccessCreation
AADInternals PowerShell Cmdlets Execution - PsScript
Access To ADMIN$ Network Share
Active Directory Computers Enumeration With Get-AdComputer
Active Directory Database Snapshot Via ADExplorer
Active Directory Group Enumeration With Get-AdGroup
Active Directory Kerberos DLL Loaded Via Office Application
Active Directory Parsing DLL Loaded Via Office Application
Active Directory Structure Export Via Ldifde.EX
Active Directory User Backdoors
Select Groups
Select domain
EVENTLOGQA.COM
No objects selected
Specify groups manually
No objects selected
Groups
OU based Groups
Last Sync Time: 2025-08-25 22:00:03
1 - 10 of 13
10
Add
Cancel

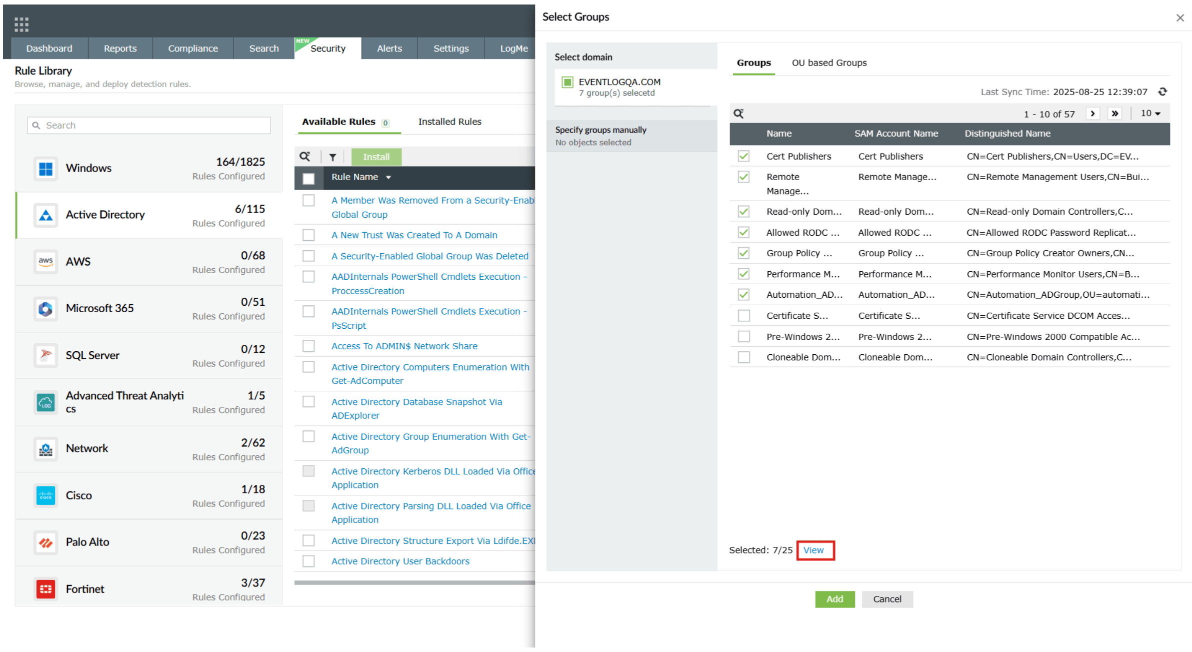
	Name	Distinguished Name
□	veluOU1	OU=veluOU1,DC=EVENTLOGQA,DC=COM
□	innerOU	OU=innerOU,OU=zAutomationTesting,...
□	OU1	OU=OU1,OU=testOU,DC=EVENTLOGQA,DC...
□	testOU12	OU=testOU12,OU=ADsync,DC=EVENTLOG...
□	newOU	OU=newOU,OU=veluOU,DC=EVENTLOGQA,...
□	veluOU	OU=veluOU,DC=EVENTLOGQA,DC=COM
□	automation	OU=automation,DC=EVENTLOGQA,DC=COM
□	PrasannaOU	OU=PrasannaOU,DC=EVENTLOGQA,DC=COM
□	zAutomationTesting	OU=zAutomationTesting,DC=EVENTLOG...
□	testOU	OU=testOU,DC=EVENTLOGQA,DC=COM

Note • OU-based group filtering uses the latest synced domain group and OU data. If OU Scoped group change in AD but are not yet synced,alerts will be processed based on the last synced data.

Selected: 0/25

Image 8: Applying object filter in rule details in rule library

9. After selecting the preferred groups, you can view your selection by clicking on the View option below.

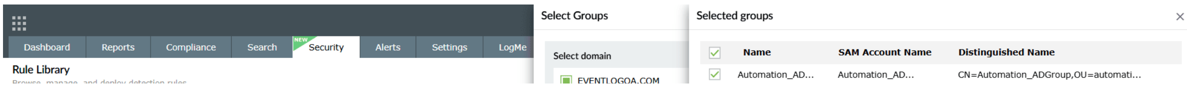

Dashboard
Reports
Compliance
Search
Security
Alerts
Settings
LogMe
Rule Library
Browse, manage, and deploy detection rules.
Search
Windows 164/1825 Rules Configured
Active Directory 6/115 Rules Configured
AWS 0/68 Rules Configured
Microsoft 365 0/51 Rules Configured
SQL Server 0/12 Rules Configured
Advanced Threat Analytics 1/5 Rules Configured
Network 2/62 Rules Configured
Cisco 1/18 Rules Configured
Palo Alto 0/23 Rules Configured
Fortinet 3/37 Rules Configured
Available Rules 0
Installed Rules
Install
Rule Name
A Member Was Removed From a Security-Enab Global Group
A New Trust Was Created To A Domain
A Security-Enabled Global Group Was Deleted
AADInternals PowerShell Cmdlets Execution - ProccessCreation
AADInternals PowerShell Cmdlets Execution - PsScript
Access To ADMIN$ Network Share
Active Directory Computers Enumeration With Get-AdComputer
Active Directory Database Snapshot Via ADExplorer
Active Directory Group Enumeration With Get-AdGroup
Active Directory Kerberos DLL Loaded Via Office Application
Active Directory Parsing DLL Loaded Via Office Application
Active Directory Structure Export Via Ldifde.EX
Active Directory User Backdoors
Select Groups
Select domain
EVENTLOGQA.COM
7 group(s) selecetd
Specify groups manually
No objects selected
Groups
OU based Groups
Last Sync Time: 2025-08-25 12:39:07
1 - 10 of 57
10
View
Add
Cancel

	Name	SAM Account Name	Distinguished Name
☑	Cert Publishers	Cert Publishers	CN=Cert Publishers,CN=Users,DC=EV...
☑	Remote Manage...	Remote Manage...	CN=Remote Management Users,CN=Bui...
☑	Read-only Dom...	Read-only Dom...	CN=Read-only Domain Controllers,C...
☑	Allowed RODC ...	Allowed RODC ...	CN=Allowed RODC Password Replicat...
☑	Group Policy ...	Group Policy ...	CN=Group Policy Creator Owners,CN...
☑	Performance M...	Performance M...	CN=Performance Monitor Users,CN=B...
☑	Automation_AD...	Automation_AD...	CN=Automation_ADGroup,OU=automati...
□	Certificate S...	Certificate S...	CN=Certificate Service DCOM Acces...
□	Pre-Windows 2...	Pre-Windows 2...	CN=Pre-Windows 2000 Compatible Ac...
□	Cloneable Dom...	Cloneable Dom...	CN=Cloneable Domain Controllers,C...

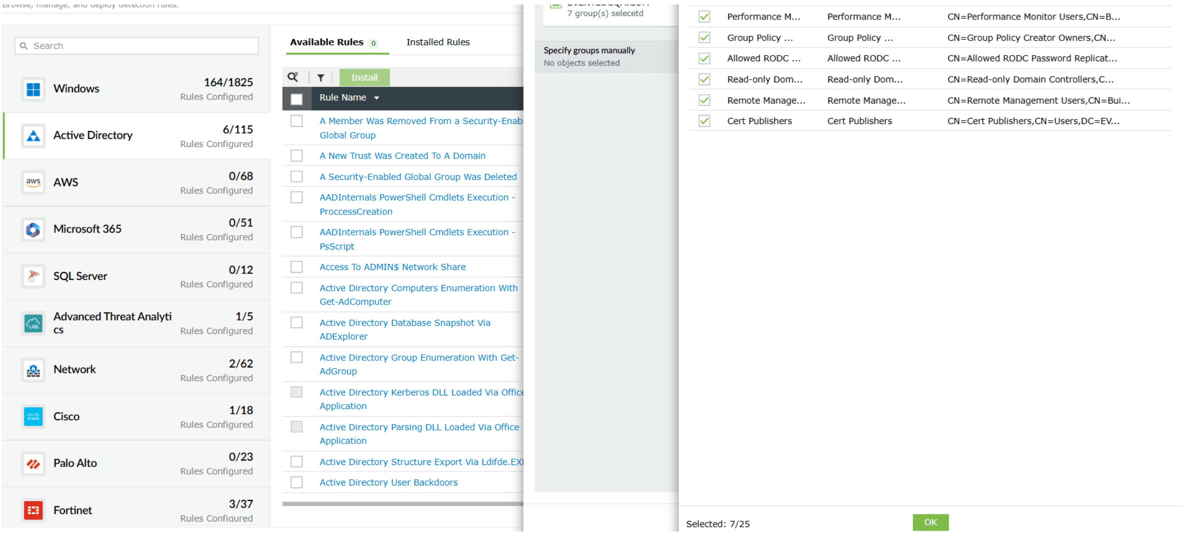
Selected: 7/25

Image 9: Viewing the object filtering list

10. The list of selected user groups will be displayed.



☑	Name	SAM Account Name	Distinguished Name
☑	Automation_AD...	Automation_AD...	CN=Automation_ADGroup,OU=automati...



Browse, manage, and deploy detection rules.

Search

Windows	164/1825 Rules Configured
Active Directory	6/115 Rules Configured
AWS	0/68 Rules Configured
Microsoft 365	0/51 Rules Configured
SQL Server	0/12 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	2/62 Rules Configured
Cisco	1/18 Rules Configured
Palo Alto	0/23 Rules Configured
Fortinet	3/37 Rules Configured

Available Rules 0 | Installed Rules

Install

□	Rule Name
□	A Member Was Removed From a Security-Enab Global Group
□	A New Trust Was Created To A Domain
□	A Security-Enabled Global Group Was Deleted
□	AADInternals PowerShell Cmdlets Execution - ProccessCreation
□	AADInternals PowerShell Cmdlets Execution - PsScript
□	Access To ADMIN$ Network Share
□	Active Directory Computers Enumeration With Get-AdComputer
□	Active Directory Database Snapshot Via ADExplorer
□	Active Directory Group Enumeration With Get-AdGroup
□	Active Directory Kerberos DLL Loaded Via Office Application
□	Active Directory Parsing DLL Loaded Via Office Application
□	Active Directory Structure Export Via Ldifde.EX
□	Active Directory User Backdoors

7 group(s) selecetd

Specify groups manually
No objects selected

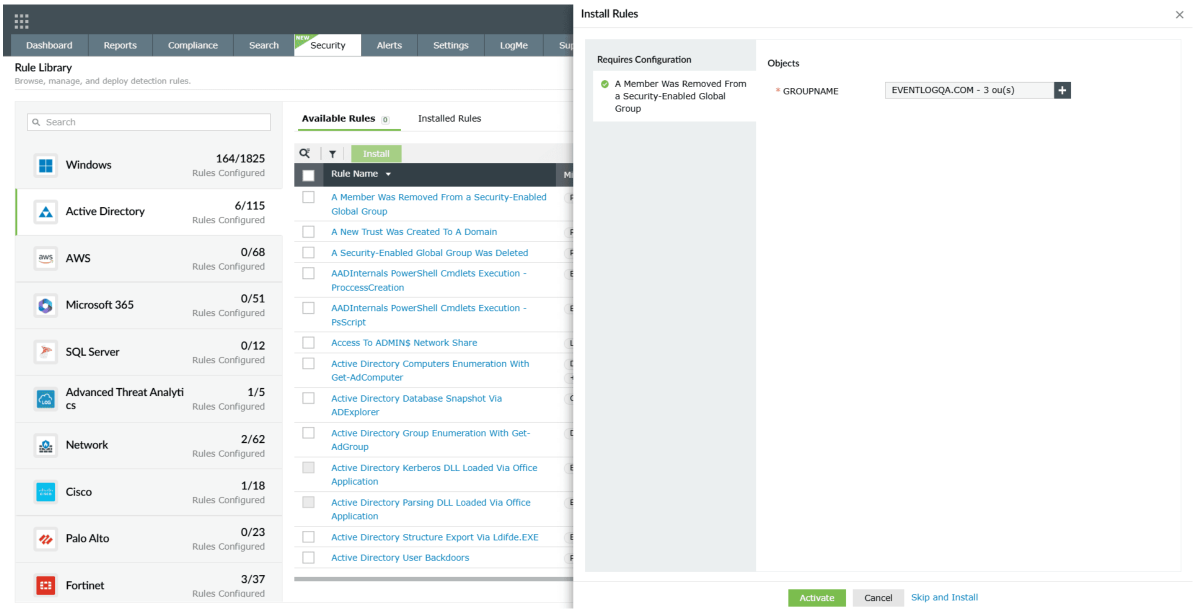
☑	Performance M...	Performance M...	CN=Performance Monitor Users,CN=B...
☑	Group Policy ...	Group Policy ...	CN=Group Policy Creator Owners,CN...
☑	Allowed RODC ...	Allowed RODC ...	CN=Allowed RODC Password Replicat...
☑	Read-only Dom...	Read-only Dom...	CN=Read-only Domain Controllers,C...
☑	Remote Manage...	Remote Manage...	CN=Remote Management Users,CN=Bui...
☑	Cert Publishers	Cert Publishers	CN=Cert Publishers,CN=Users,DC=EV...

Selected: 7/25

OK

Image 10: Viewing list of configured object filter users/groups

11. Once the selection is done, click on OK in the selection list and then click on Add in the Select Groups pane. The Install Rules pane will display the Requires Configuration section with a green check mark.



Rule Library
Browse, manage, and deploy detection rules.

Search

Windows	164/1825 Rules Configured
Active Directory	6/115 Rules Configured
AWS	0/68 Rules Configured
Microsoft 365	0/51 Rules Configured
SQL Server	0/12 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	2/62 Rules Configured
Cisco	1/18 Rules Configured
Palo Alto	0/23 Rules Configured
Fortinet	3/37 Rules Configured

Available Rules 0 | Installed Rules

Install

□	Rule Name
□	A Member Was Removed From a Security-Enabled Global Group
□	A New Trust Was Created To A Domain
□	A Security-Enabled Global Group Was Deleted
□	AADInternals PowerShell Cmdlets Execution - ProccessCreation
□	AADInternals PowerShell Cmdlets Execution - PsScript
□	Access To ADMIN$ Network Share
□	Active Directory Computers Enumeration With Get-AdComputer
□	Active Directory Database Snapshot Via ADExplorer
□	Active Directory Group Enumeration With Get-AdGroup
□	Active Directory Kerberos DLL Loaded Via Office Application
□	Active Directory Parsing DLL Loaded Via Office Application
□	Active Directory Structure Export Via Ldifde.EXE
□	Active Directory User Backdoors

Install Rules

Requires Configuration

✓ A Member Was Removed From a Security-Enabled Global Group

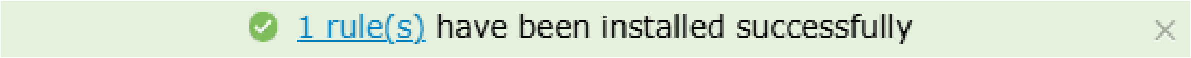
Objects

* GROUPNAME: EVENTLOGQA.COM - 3 ou(s) +

Activate | Cancel | Skip and Install

Image 11: Configuring object filter users/groups

12. Click on the Activate button. Upon successful completion of the action, the below pop-up appears.



✓ 1 rule(s) have been installed successfully ×

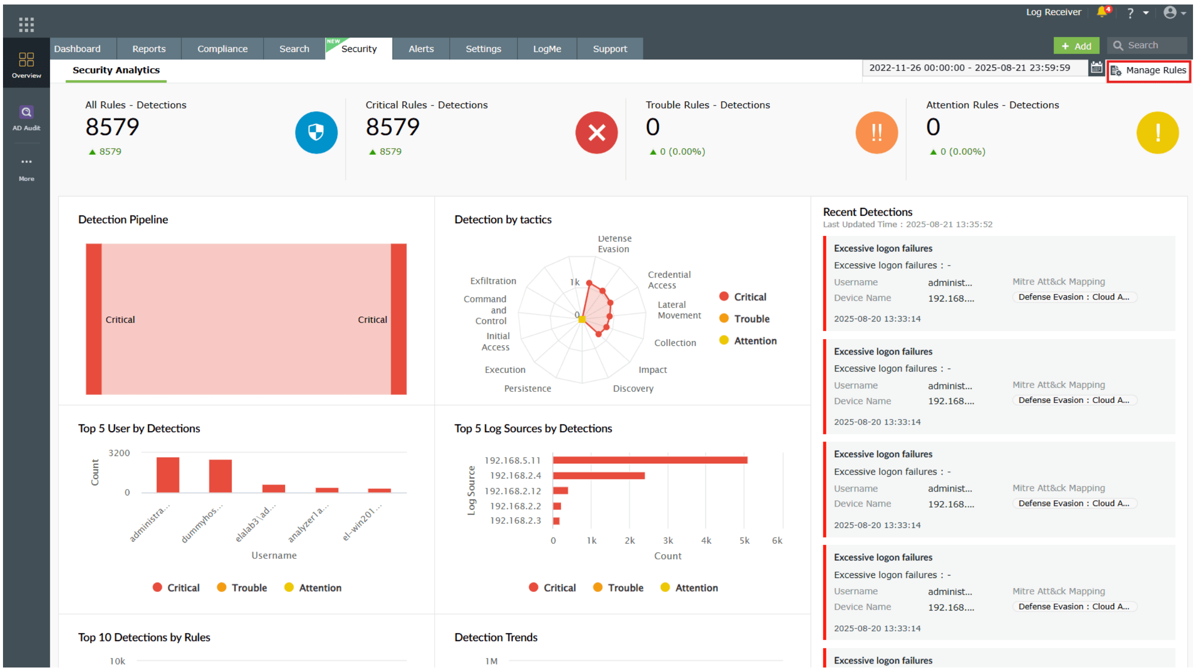
To learn more about the Rule Library, refer to the help document.

Rule management

The solution allows you to configure or update object filters for existing rules through the Rule Management module. The filters can be applied in both the Objects and Exception sections of a rule's summary. To do this, follow the steps below:

1. In your account, navigate to the Security tab to access the Security Analytics Dashboard and click on Manage Rules in the top right corner.

Rules in the top-right corner.



All Rules - Detections	Critical Rules - Detections	Trouble Rules - Detections	Attention Rules - Detections
8579	8579	0	0
▲ 8579	▲ 8579	▲ 0 (0.00%)	▲ 0 (0.00%)

Recent Detections
Last Updated Time : 2025-08-21 13:35:52

Excessive logon failures
Excessive logon failures : -
Username administ...
Device Name 192.168....
Mitre Att&ck Mapping
Defense Evasion : Cloud A...
2025-08-20 13:33:14

Excessive logon failures
Excessive logon failures : -
Username administ...
Device Name 192.168....
Mitre Att&ck Mapping
Defense Evasion : Cloud A...
2025-08-20 13:33:14

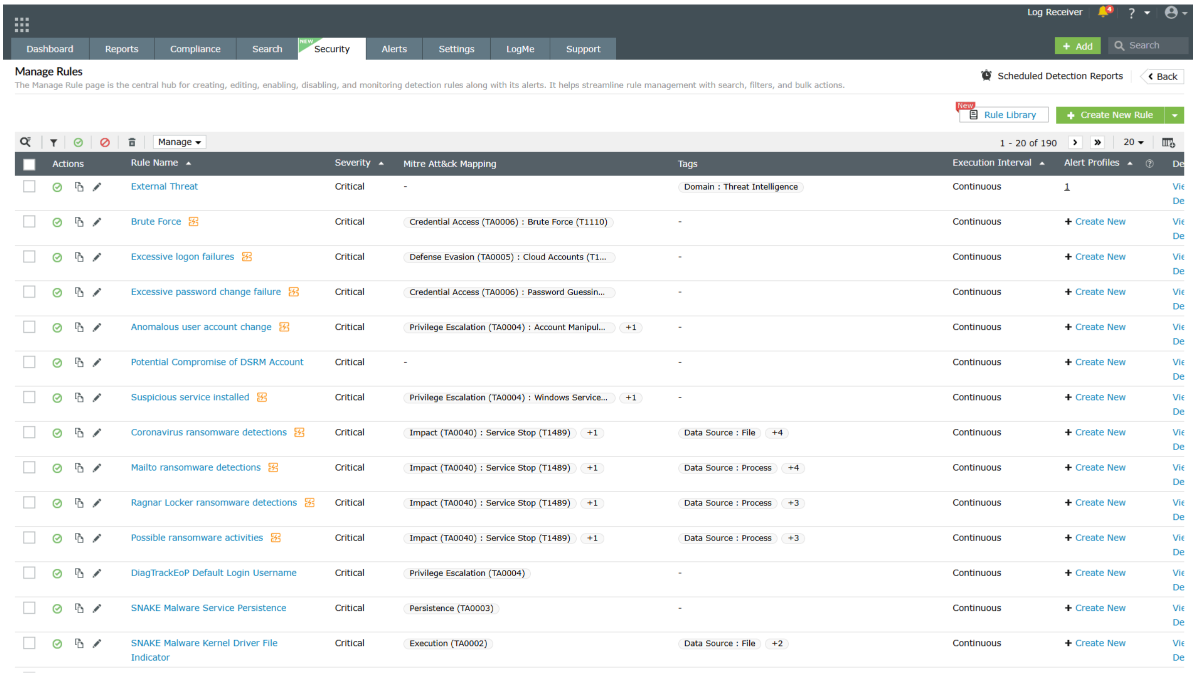
Excessive logon failures
Excessive logon failures : -
Username administ...
Device Name 192.168....
Mitre Att&ck Mapping
Defense Evasion : Cloud A...
2025-08-20 13:33:14

Excessive logon failures
Excessive logon failures : -
Username administ...
Device Name 192.168....
Mitre Att&ck Mapping
Defense Evasion : Cloud A...
2025-08-20 13:33:14

Excessive logon failures

Image 12: Manage rules in the security dashboard

2. You will be taken to the Manage Rules module.

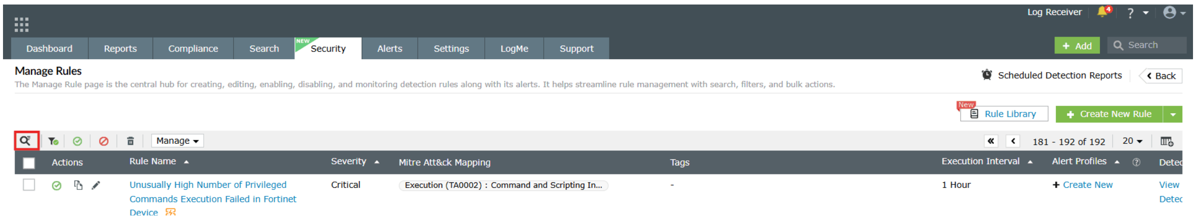


Manage Rules
The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

Actions	Rule Name	Severity	Mitre Att&ck Mapping	Tags	Execution Interval	Alert Profiles	De
	External Threat	Critical	-	Domain : Threat Intelligence	Continuous	1	Vie De
	Brute Force	Critical	Credential Access (TA0006) : Brute Force (T1110)	-	Continuous	+ Create New	Vie De
	Excessive logon failures	Critical	Defense Evasion (TA0005) : Cloud Accounts (T1...	-	Continuous	+ Create New	Vie De
	Excessive password change failure	Critical	Credential Access (TA0006) : Password Guessin...	-	Continuous	+ Create New	Vie De
	Anomalous user account change	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	-	Continuous	+ Create New	Vie De
	Potential Compromise of DSRM Account	Critical	-	-	Continuous	+ Create New	Vie De
	Suspicious service installed	Critical	Privilege Escalation (TA0004) : Windows Service... +1	-	Continuous	+ Create New	Vie De
	Coronavirus ransomware detections	Critical	Impact (TA0040) : Service Stop (T1489) +1	Data Source : File +4	Continuous	+ Create New	Vie De
	Mailto ransomware detections	Critical	Impact (TA0040) : Service Stop (T1489) +1	Data Source : Process +4	Continuous	+ Create New	Vie De
	Ragnar Locker ransomware detections	Critical	Impact (TA0040) : Service Stop (T1489) +1	Data Source : Process +3	Continuous	+ Create New	Vie De
	Possible ransomware activities	Critical	Impact (TA0040) : Service Stop (T1489) +1	Data Source : Process +3	Continuous	+ Create New	Vie De
	DiagTrackEoP Default Login Username	Critical	Privilege Escalation (TA0004)	-	Continuous	+ Create New	Vie De
	SNAKE Malware Service Persistence	Critical	Persistence (TA0003)	-	Continuous	+ Create New	Vie De
	SNAKE Malware Kernel Driver File Indicator	Critical	Execution (TA0002)	Data Source : File +2	Continuous	+ Create New	Vie De

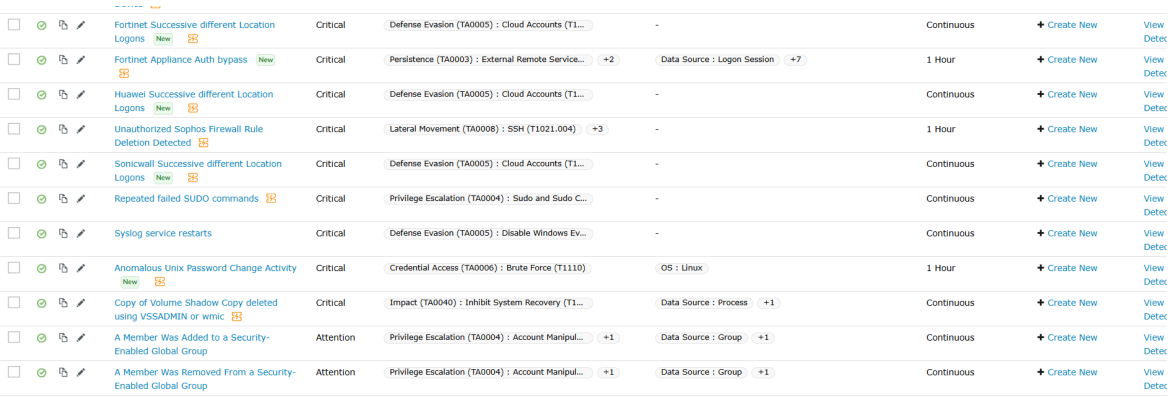
Image 13: Manage rules module

3. Click on the required rule name. You can use the search feature available to find the rule quickly.



Manage Rules
The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

Actions	Rule Name	Severity	Mitre Att&ck Mapping	Tags	Execution Interval	Alert Profiles	Detec
	Unusually High Number of Privileged Commands Execution Failed in Fortinet Device	Critical	Execution (TA0002) : Command and Scripting In...	-	1 Hour	+ Create New	View Detec



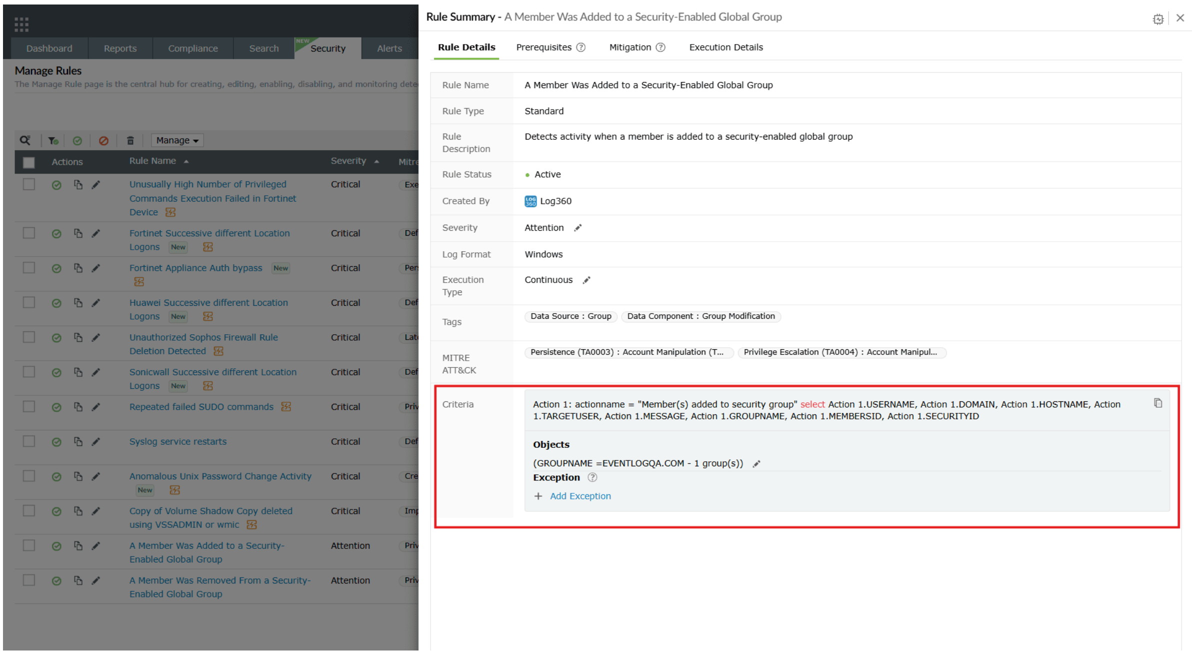
Rule Name	Severity	MITRE	Tags	Execution Type		
Fortinet Successive different Location Logons New	Critical	Defense Evasion (TA0005) : Cloud Accounts (T1...	-	Continuous	+ Create New	View Detec
Fortinet Appliance Auth bypass New	Critical	Persistence (TA0003) : External Remote Service... +2	Data Source : Logon Session +7	1 Hour	+ Create New	View Detec
Huawei Successive different Location Logons New	Critical	Defense Evasion (TA0005) : Cloud Accounts (T1...	-	Continuous	+ Create New	View Detec
Unauthorized Sophos Firewall Rule Deletion Detected	Critical	Lateral Movement (TA0008) : SSH (T1021.004) +3	-	1 Hour	+ Create New	View Detec
Sonicwall Successive different Location Logons New	Critical	Defense Evasion (TA0005) : Cloud Accounts (T1...	-	Continuous	+ Create New	View Detec
Repeated failed SUDO commands	Critical	Privilege Escalation (TA0004) : Sudo and Sudo C...	-	Continuous	+ Create New	View Detec
Syslog service restarts	Critical	Defense Evasion (TA0005) : Disable Windows Ev...	-	Continuous	+ Create New	View Detec
Anomalous Unix Password Change Activity New	Critical	Credential Access (TA0006) : Brute Force (T1110)	OS : Linux	1 Hour	+ Create New	View Detec
Copy of Volume Shadow Copy deleted using VSSADMIN or wmic	Critical	Impact (TA0040) : Inhibit System Recovery (T1...	Data Source : Process +1	Continuous	+ Create New	View Detec
A Member Was Added to a Security-Enabled Global Group	Attention	Privilege Escalation (TA0004) : Account Manipul... +1	Data Source : Group +1	Continuous	+ Create New	View Detec
A Member Was Removed From a Security-Enabled Global Group	Attention	Privilege Escalation (TA0004) : Account Manipul... +1	Data Source : Group +1	Continuous	+ Create New	View Detec

Image 14: Search option in manage rules module

4. Upon clicking on the rule name, the Rule Summary box slides open. The object filter feature is available for the below sections in the Rule Details sub-tab of Rule Summary.
   - Objects
   - Exception
   - Enabling rule

A. Objects section

1. Navigate to the Criteria section as highlighted below and click on the edit icon in Objects.



Dashboard
Reports
Compliance
Search
Security
Alerts
Manage Rules
The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring dete
Manage
Actions
Rule Name
Severity

Rule Summary - A Member Was Added to a Security-Enabled Global Group

Rule Details | Prerequisites | Mitigation | Execution Details

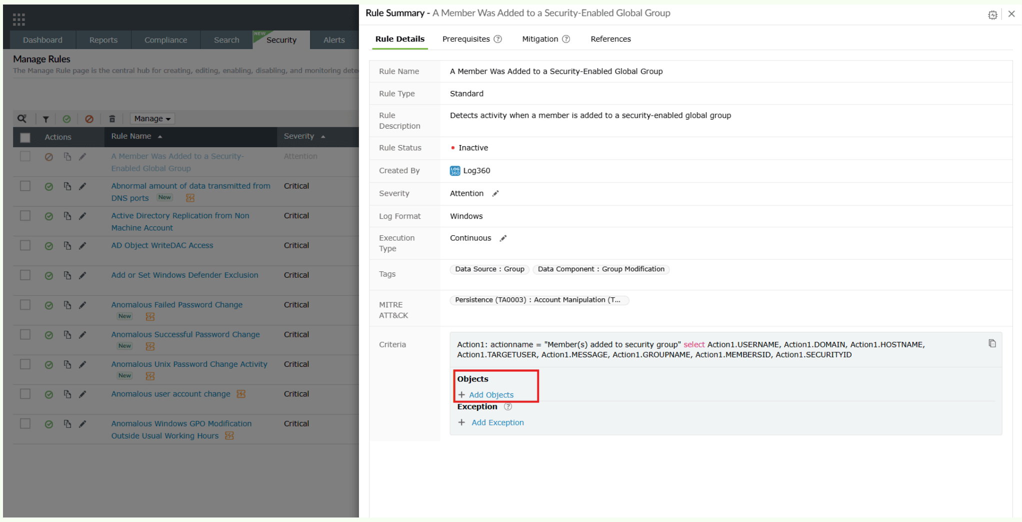
Rule Name	A Member Was Added to a Security-Enabled Global Group
Rule Type	Standard
Rule Description	Detects activity when a member is added to a security-enabled global group
Rule Status	● Active
Created By	Log360
Severity	Attention
Log Format	Windows
Execution Type	Continuous
Tags	Data Source : Group Data Component : Group Modification
MITRE ATT&CK	Persistence (TA0003) : Account Manipulation (T... Privilege Escalation (TA0004) : Account Manipul...
Criteria	Action 1: actionname = "Member(s) added to security group" select Action 1.USERNAME, Action 1.DOMAIN, Action 1.HOSTNAME, Action 1.TARGETUSER, Action 1.MESSAGE, Action 1.GROUPNAME, Action 1.MEMBERSID, Action 1.SECURITYID **Objects** (GROUPNAME =EVENTLOGQA.COM - 1 group(s)) **Exception** + Add Exception

Image 15: Object filtering in rule summary in manage rules module

NOTE

- The edit icon will be available only if you have previously selected user groups during rule installation from the Rule Library.
- In the case where you had chosen to Skip and Install rule, in the above mentioned Objects

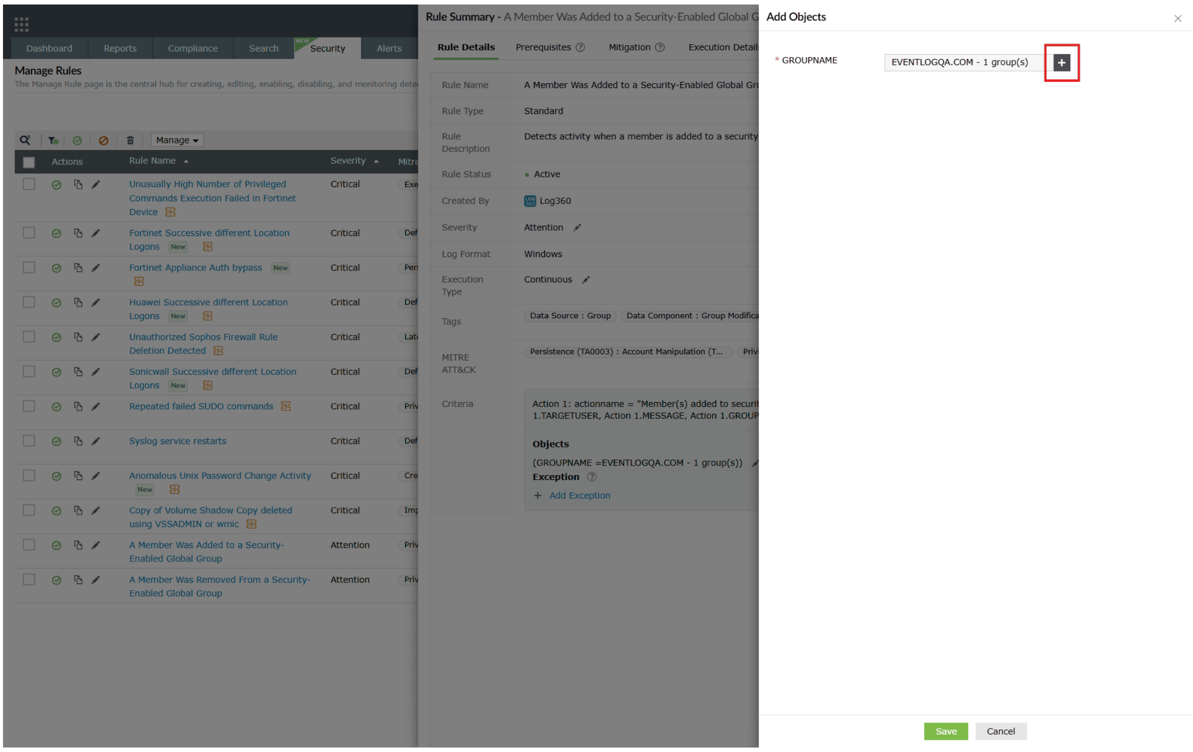
- In the case where you had chosen to Skip and install rule, in the above mentioned Objects field in the Criteria section, the option Add Objects will be visible. Click on it to access the object filter and follow the steps mentioned below to select user groups.


Rule Summary - A Member Was Added to a Security-Enabled Global Group

Rule Name	A Member Was Added to a Security-Enabled Global Group
Rule Type	Standard
Rule Description	Detects activity when a member is added to a security-enabled global group
Rule Status	Inactive
Created By	Log360
Severity	Attention
Log Format	Windows
Execution Type	Continuous
Tags	Data Source : Group Data Component : Group Modification
MITRE ATT&CK	Persistence (TA0003) : Account Manipulation (T...
Criteria	Action1: actionname = "Member(s) added to security group" select Action1.USERNAME, Action1.DOMAIN, Action1.HOSTNAME, Action1.TARGETUSER, Action1.MESSAGE, Action1.GROUPNAME, Action1.MEMBERSID, Action1.SECURITYID Objects + Add Objects Exception + Add Exception

Image 16: Adding objects in rule summary

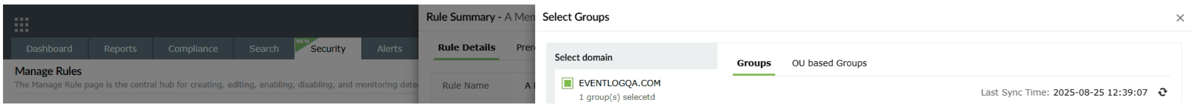
2. The Add Object pane slides open. Click on the add icon as highlighted below.


Add Objects

* GROUPNAME EVENTLOGQA.COM - 1 group(s)

Image 17: Object filtering in rule summary

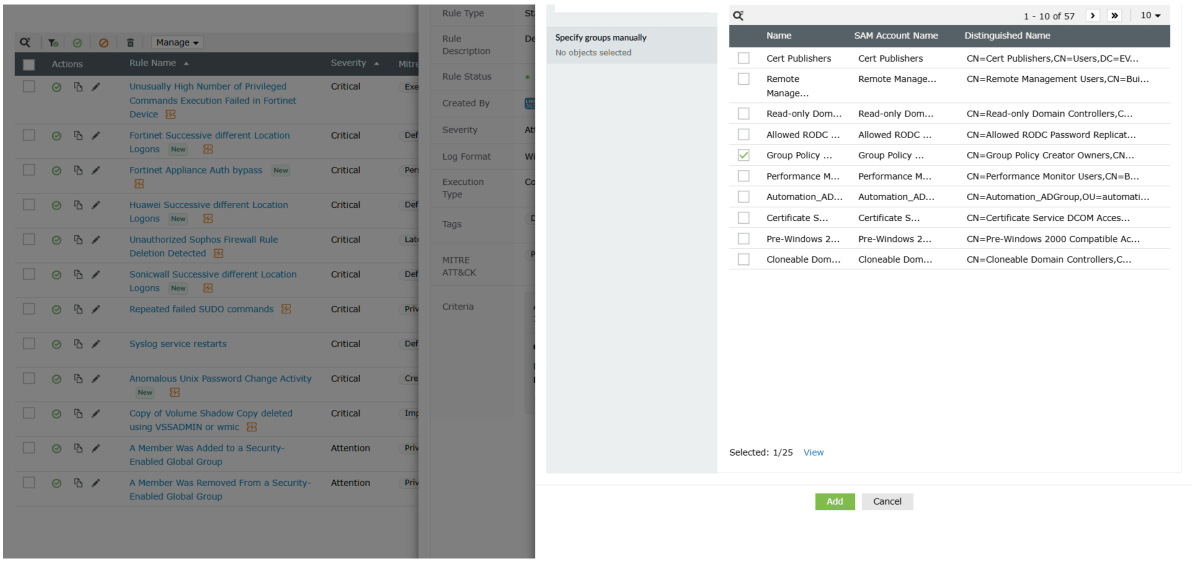
3. The Select Groups pane slides open. You will be taken to the Groups sub-tab displayed along with the object filter feature in order to be able to filter and choose what groups of users you wish to group under this rule.


Select Groups

Select domain

EVENTLOGQA.COM
1 group(s) selecetd

Last Sync Time: 2025-08-25 12:39:07



Specify groups manually
No objects selected

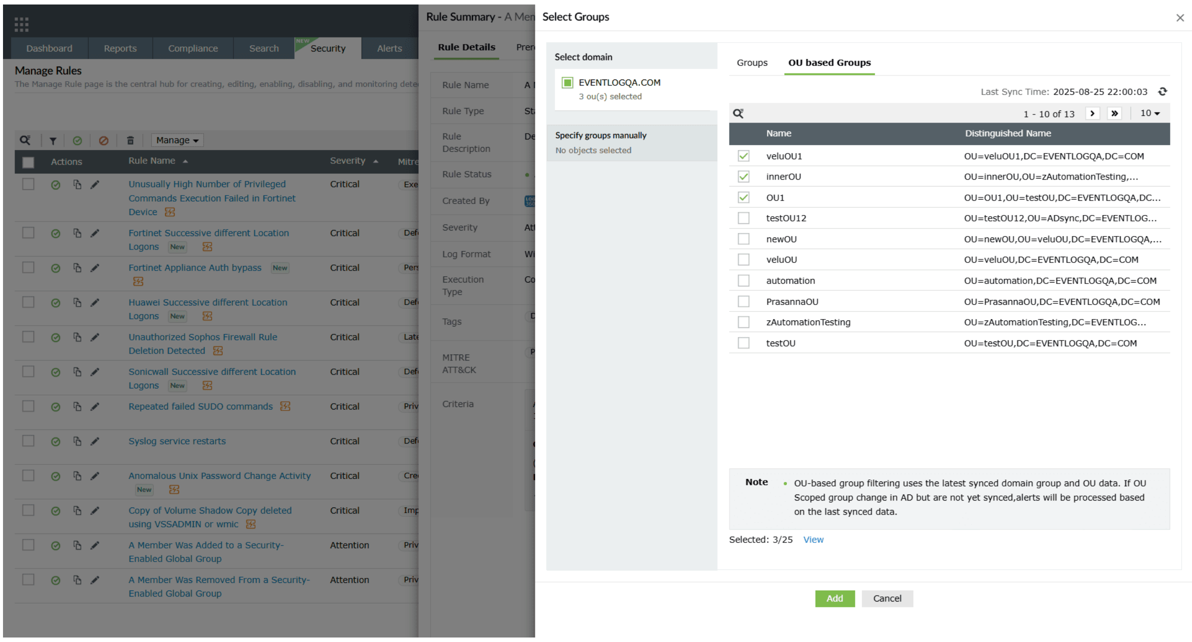
1 - 10 of 57

	Name	SAM Account Name	Distinguished Name
□	Cert Publishers	Cert Publishers	CN=Cert Publishers,CN=Users,DC=EV...
□	Remote Manage...	Remote Manage...	CN=Remote Management Users,CN=Bui...
□	Read-only Dom...	Read-only Dom...	CN=Read-only Domain Controllers,C...
□	Allowed RODC ...	Allowed RODC ...	CN=Allowed RODC Password Replicat...
☑	Group Policy ...	Group Policy ...	CN=Group Policy Creator Owners,CN...
□	Performance M...	Performance M...	CN=Performance Monitor Users,CN=B...
□	Automation_AD...	Automation_AD...	CN=Automation_ADGroup,OU=automati...
□	Certificate S...	Certificate S...	CN=Certificate Service DCOM Acces...
□	Pre-Windows 2...	Pre-Windows 2...	CN=Pre-Windows 2000 Compatible Ac...
□	Cloneable Dom...	Cloneable Dom...	CN=Cloneable Domain Controllers,C...

Selected: 1/25 View

Image 18: Object filtering in rule management

4. Similarly, the OU based Groups sub-tab also includes the filter for user selection.



Select Groups

Select domain
☑ EVENTLOGQA.COM
3 ou(s) selected

Specify groups manually
No objects selected

Groups | OU based Groups

Last Sync Time: 2025-08-25 22:00:03

1 - 10 of 13

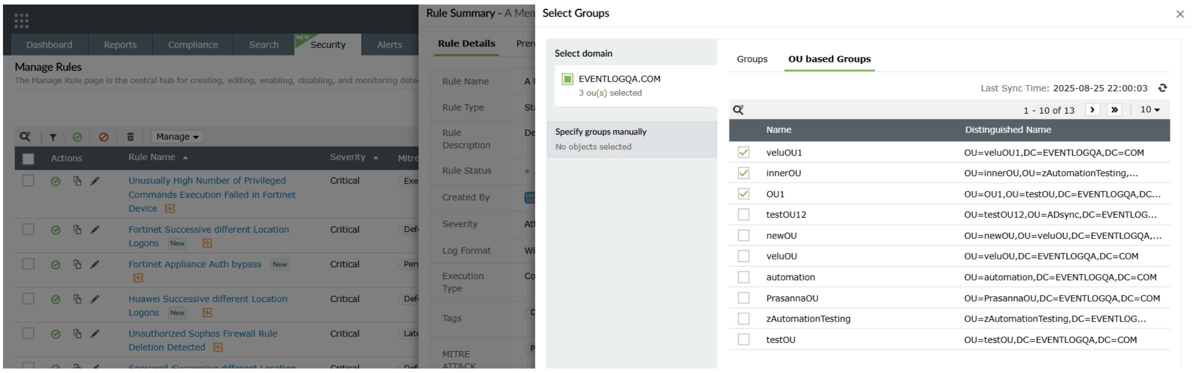
	Name	Distinguished Name
☑	veluOU1	OU=veluOU1,DC=EVENTLOGQA,DC=COM
☑	innerOU	OU=innerOU,OU=zAutomationTesting,...
☑	OU1	OU=OU1,OU=testOU,DC=EVENTLOGQA,DC...
□	testOU12	OU=testOU12,OU=ADsync,DC=EVENTLOG...
□	newOU	OU=newOU,OU=veluOU,DC=EVENTLOGQA,...
□	veluOU	OU=veluOU,DC=EVENTLOGQA,DC=COM
□	automation	OU=automation,DC=EVENTLOGQA,DC=COM
□	PrasannaOU	OU=PrasannaOU,DC=EVENTLOGQA,DC=COM
□	zAutomationTesting	OU=zAutomationTesting,DC=EVENTLOG...
□	testOU	OU=testOU,DC=EVENTLOGQA,DC=COM

Note • OU-based group filtering uses the latest synced domain group and OU data. If OU Scoped group change in AD but are not yet synced,alerts will be processed based on the last synced data.

Selected: 3/25 View

Image 19: Group selection in object filtering

5. After selecting the preferred groups, you can view your selection by clicking on the View option highlighted below.



Select Groups

Select domain
☑ EVENTLOGQA.COM
3 ou(s) selected

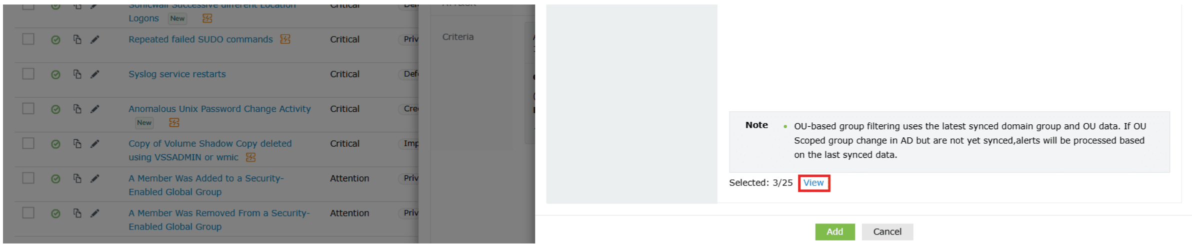
Specify groups manually
No objects selected

Groups | OU based Groups

Last Sync Time: 2025-08-25 22:00:03

1 - 10 of 13

	Name	Distinguished Name
☑	veluOU1	OU=veluOU1,DC=EVENTLOGQA,DC=COM
☑	innerOU	OU=innerOU,OU=zAutomationTesting,...
☑	OU1	OU=OU1,OU=testOU,DC=EVENTLOGQA,DC...
□	testOU12	OU=testOU12,OU=ADsync,DC=EVENTLOG...
□	newOU	OU=newOU,OU=veluOU,DC=EVENTLOGQA,...
□	veluOU	OU=veluOU,DC=EVENTLOGQA,DC=COM
□	automation	OU=automation,DC=EVENTLOGQA,DC=COM
□	PrasannaOU	OU=PrasannaOU,DC=EVENTLOGQA,DC=COM
□	zAutomationTesting	OU=zAutomationTesting,DC=EVENTLOG...
□	testOU	OU=testOU,DC=EVENTLOGQA,DC=COM



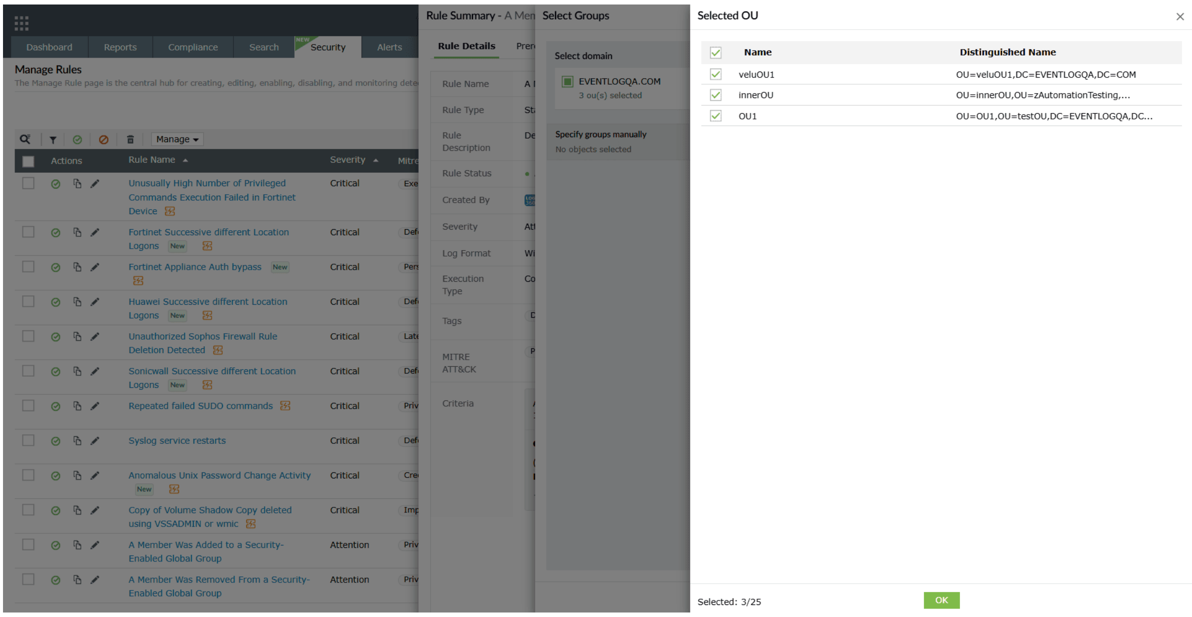
Note • OU-based group filtering uses the latest synced domain group and OU data. If OU Scoped group change in AD but are not yet synced,alerts will be processed based on the last synced data.

Selected: 3/25 View

Criteria
Repeated failed SUDO commands
Syslog service restarts
Anomalous Unix Password Change Activity
Copy of Volume Shadow Copy deleted using VSSADMIN or wmic
A Member Was Added to a Security-Enabled Global Group
A Member Was Removed From a Security-Enabled Global Group
Add
Cancel

Image 20: Viewing list of configured object filter users/groups

6. The list of selected user groups will be displayed.



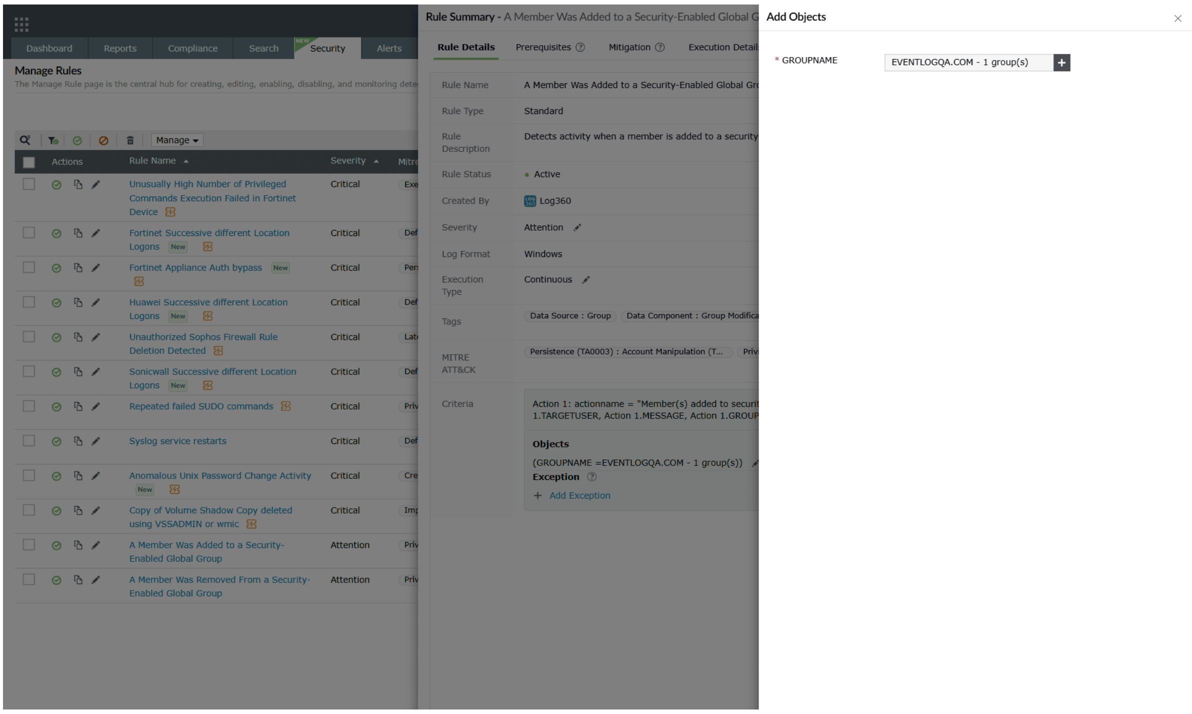
Selected OU

☑	Name	Distinguished Name
☑	veluOU1	OU=veluOU1,DC=EVENTLOGQA,DC=COM
☑	innerOU	OU=innerOU,OU=zAutomationTesting,...
☑	OU1	OU=OU1,OU=testOU,DC=EVENTLOGQA,DC...

Selected: 3/25

Image 21: Configuring object filter users/groups

7. Once the selection is done, click on OK in the selection list and then click on Add in the Select Groups pane. Click on the Save button in the Add Objects pane.



Rule Summary - A Member Was Added to a Security-Enabled Global G

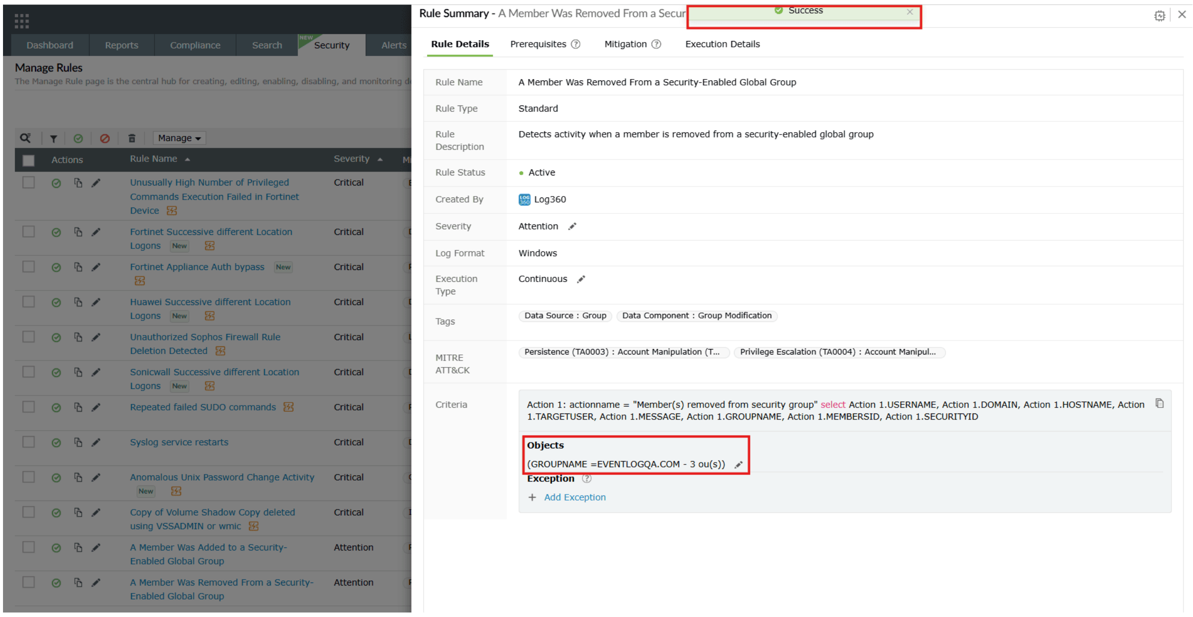
Rule Name	A Member Was Added to a Security-Enabled Global Gr
Rule Type	Standard
Rule Description	Detects activity when a member is added to a security
Rule Status	Active
Created By	Log360
Severity	Attention
Log Format	Windows
Execution Type	Continuous
Tags	Data Source : Group Data Component : Group Modifica
MITRE ATT&CK	Persistence (TA0003) : Account Manipulation (T... Priv
Criteria	Action 1: actionname = "Member(s) added to securi 1.TARGETUSER, Action 1.MESSAGE, Action 1.GROUP Objects (GROUPNAME =EVENTLOGQA.COM - 1 group(s)) Exception + Add Exception

Add Objects

* GROUPNAME EVENTLOGQA.COM - 1 group(s) +

Image 22: Configuring object filter users/groups in rule management

8. Upon successful completion of action, a Success pop-up appears briefly, and the selection changes are instantly updated and are visible in the Objects section.



Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring de

Actions	Rule Name	Severity
	Unusually High Number of Privileged Commands Execution Failed in Fortinet Device	Critical
	Fortinet Successive different Location Logons New	Critical
	Fortinet Appliance Auth bypass New	Critical
	Huawei Successive different Location Logons New	Critical
	Unauthorized Sophos Firewall Rule Deletion Detected	Critical
	Sonicwall Successive different Location Logons New	Critical
	Repeated failed SUDO commands	Critical
	Syslog service restarts	Critical
	Anomalous Unix Password Change Activity New	Critical
	Copy of Volume Shadow Copy deleted using VSSADMIN or wmic	Critical
	A Member Was Added to a Security-Enabled Global Group	Attention
	A Member Was Removed From a Security-Enabled Global Group	Attention

Rule Summary - A Member Was Removed From a Secur

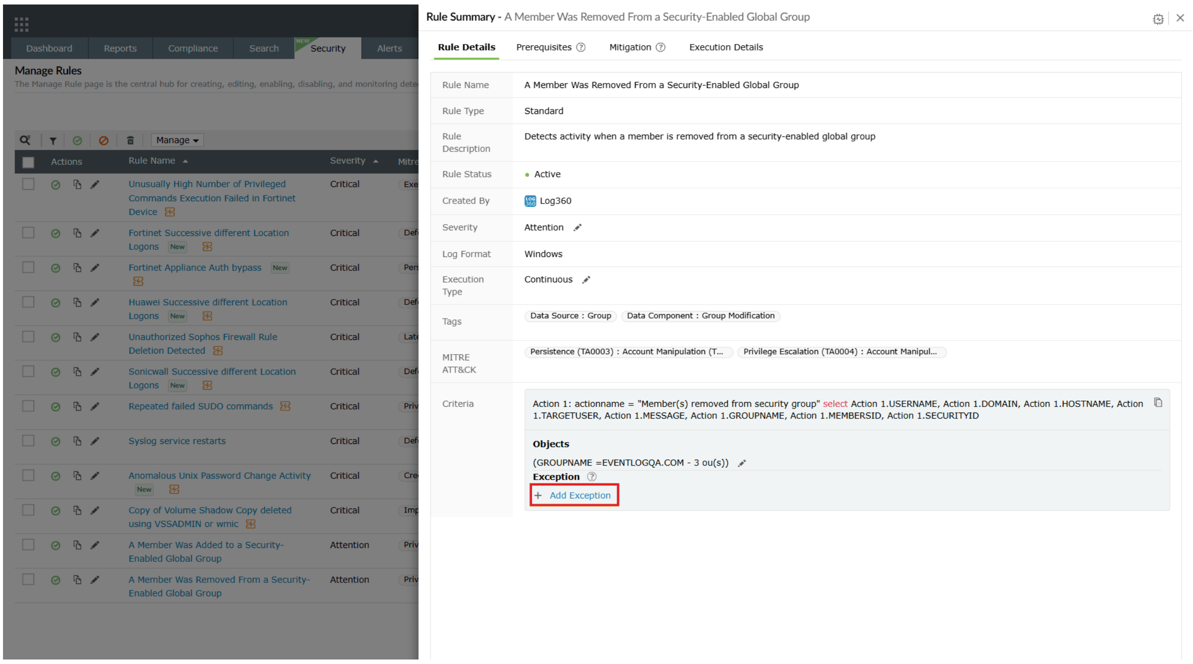
Rule Details | Prerequisites | Mitigation | Execution Details

Rule Name	A Member Was Removed From a Security-Enabled Global Group
Rule Type	Standard
Rule Description	Detects activity when a member is removed from a security-enabled global group
Rule Status	● Active
Created By	Log360
Severity	Attention
Log Format	Windows
Execution Type	Continuous
Tags	Data Source : Group Data Component : Group Modification
MITRE ATT&CK	Persistence (TA0003) : Account Manipulation (T... Privilege Escalation (TA0004) : Account Manipul...
Criteria	Action 1: actionname = "Member(s) removed from security group" select Action 1.USERNAME, Action 1.DOMAIN, Action 1.HOSTNAME, Action 1.TARGETUSER, Action 1.MESSAGE, Action 1.GROUPNAME, Action 1.MEMBERSID, Action 1.SECURITYID **Objects** (GROUPNAME =EVENTLOGQA.COM - 3 ou(s)) **Exception** + Add Exception

Image 23: Configuring object filter users/groups in rule management

B. Exception section

1. Navigate to the Criteria section as highlighted below and click on the Add Exception option as highlighted below.



Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring dete

Actions	Rule Name	Severity	Mitre
	Unusually High Number of Privileged Commands Execution Failed in Fortinet Device	Critical	Exe
	Fortinet Successive different Location Logons New	Critical	Def
	Fortinet Appliance Auth bypass New	Critical	Per
	Huawei Successive different Location Logons New	Critical	Def
	Unauthorized Sophos Firewall Rule Deletion Detected	Critical	Lat
	Sonicwall Successive different Location Logons New	Critical	Def
	Repeated failed SUDO commands	Critical	Priv
	Syslog service restarts	Critical	Def
	Anomalous Unix Password Change Activity New	Critical	Cre
	Copy of Volume Shadow Copy deleted using VSSADMIN or wmic	Critical	Imp
	A Member Was Added to a Security-Enabled Global Group	Attention	Priv
	A Member Was Removed From a Security-Enabled Global Group	Attention	Priv

Rule Summary - A Member Was Removed From a Security-Enabled Global Group

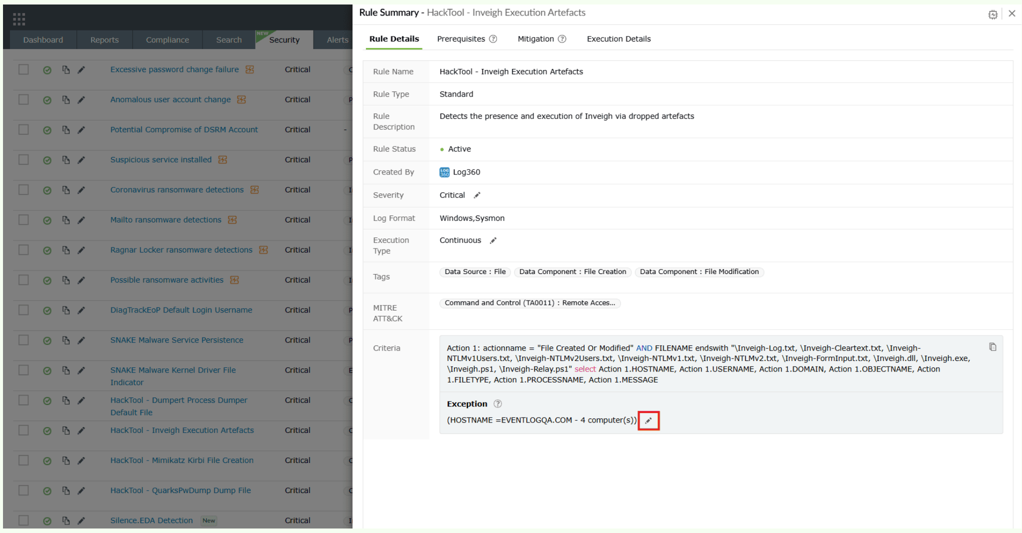
Rule Details | Prerequisites | Mitigation | Execution Details

Rule Name	A Member Was Removed From a Security-Enabled Global Group
Rule Type	Standard
Rule Description	Detects activity when a member is removed from a security-enabled global group
Rule Status	● Active
Created By	Log360
Severity	Attention
Log Format	Windows
Execution Type	Continuous
Tags	Data Source : Group Data Component : Group Modification
MITRE ATT&CK	Persistence (TA0003) : Account Manipulation (T... Privilege Escalation (TA0004) : Account Manipul...
Criteria	Action 1: actionname = "Member(s) removed from security group" select Action 1.USERNAME, Action 1.DOMAIN, Action 1.HOSTNAME, Action 1.TARGETUSER, Action 1.MESSAGE, Action 1.GROUPNAME, Action 1.MEMBERSID, Action 1.SECURITYID **Objects** (GROUPNAME =EVENTLOGQA.COM - 3 ou(s)) **Exception** + Add Exception

Image 24: Adding exceptions in rule summary

NOTE

- Rule exception can be configured only post installation.
- In case these configurations are made, you will be able to view the edit option to configure the exception instead of creating a new one.


Dashboard
Reports
Compliance
Search
NEW
Security
Alerts
Excessive password change failure
Critical
Anomalous user account change
Critical
Potential Compromise of DSRM Account
Critical
Suspicious service installed
Critical
Coronavirus ransomware detections
Critical
Mailto ransomware detections
Critical
Ragnar Locker ransomware detections
Critical
Possible ransomware activities
Critical
DiagTrackEoP Default Login Username
Critical
SNAKE Malware Service Persistence
Critical
SNAKE Malware Kernel Driver File Indicator
Critical
HackTool - Dumpert Process Dumper Default File
Critical
HackTool - Inveigh Execution Artefacts
Critical
HackTool - Mimikatz Kirbi File Creation
Critical
HackTool - QuarksPwDump Dump File
Critical
Silence.EDA Detection
New
Critical
Rule Details
Prerequisites
Mitigation
Execution Details

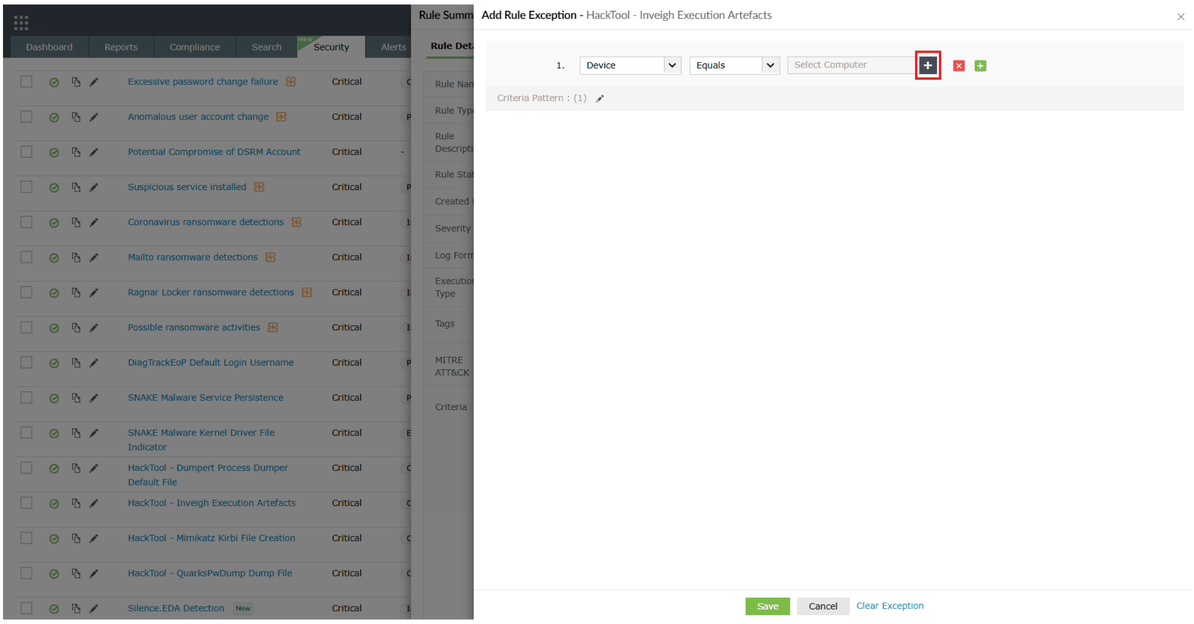
Rule Summary - HackTool - Inveigh Execution Artefacts

Rule Name	HackTool - Inveigh Execution Artefacts
Rule Type	Standard
Rule Description	Detects the presence and execution of Inveigh via dropped artefacts
Rule Status	● Active
Created By	Log360
Severity	Critical
Log Format	Windows,Sysmon
Execution Type	Continuous
Tags	Data Source : File Data Component : File Creation Data Component : File Modification
MITRE ATT&CK	Command and Control (TA0011) : Remote Acces...
Criteria	Action 1: actionname = "File Created Or Modified" AND FILENAME endswith "\Inveigh-Log.txt, \Inveigh-Cleartext.txt, \Inveigh-NTLMv1Users.txt, \Inveigh-NTLMv2Users.txt, \Inveigh-NTLMv1.txt, \Inveigh-NTLMv2.txt, \Inveigh-FormInput.txt, \Inveigh.dll, \Inveigh.exe, \Inveigh.ps1, \Inveigh-Relay.ps1" select Action 1.HOSTNAME, Action 1.USERNAME, Action 1.DOMAIN, Action 1.OBJECTNAME, Action 1.FILETYPE, Action 1.PROCESSNAME, Action 1.MESSAGE **Exception** (HOSTNAME =EVENTLOGQA.COM - 4 computer(s))

Image 25: Editing exceptions in rule summary

- Click on the edit icon as highlighted above and follow the steps given below.

2. The Add Rule Exception pane slides open. Make the necessary configurations with the preferred variables from the available drop-downs and then click on the add icon as highlighted below.
   This will allow you to filter through the devices and make selections as to which devices are to be configured for exceptions.


Dashboard
Reports
Compliance
Search
NEW
Security
Alerts
Excessive password change failure
Critical
Anomalous user account change
Critical
Potential Compromise of DSRM Account
Critical
Suspicious service installed
Critical
Coronavirus ransomware detections
Critical
Mailto ransomware detections
Critical
Ragnar Locker ransomware detections
Critical
Possible ransomware activities
Critical
DiagTrackEoP Default Login Username
Critical
SNAKE Malware Service Persistence
Critical
SNAKE Malware Kernel Driver File Indicator
Critical
HackTool - Dumpert Process Dumper Default File
Critical
HackTool - Inveigh Execution Artefacts
Critical
HackTool - Mimikatz Kirbi File Creation
Critical
HackTool - QuarksPwDump Dump File
Critical
Silence.EDA Detection
New
Critical
Select Computer
Save
Cancel
Clear Exception

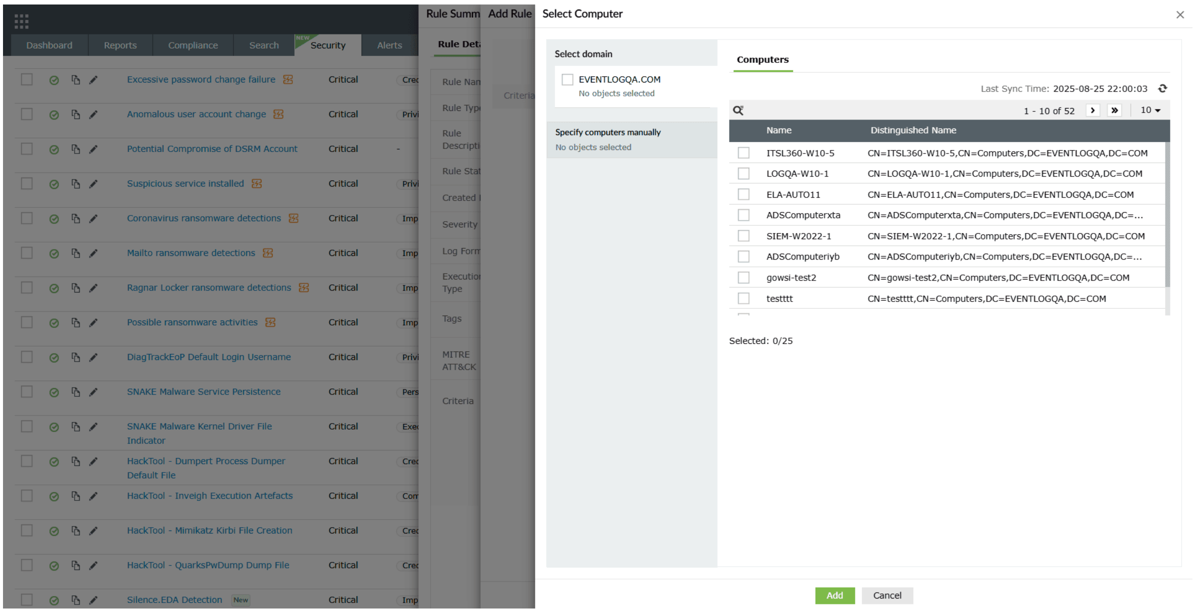
Add Rule Exception - HackTool - Inveigh Execution Artefacts

1. Device | Equals

Criteria Pattern : (1)

Image 26: Editing exceptions in rule summary with object filter

3. The Select Computer pane slides open. The device names will be displayed along with the object filter feature in order to be able to filter and choose what devices you wish to group under this rule.



Select Computer

Select domain

□ EVENTLOGQA.COM
No objects selected

Specify computers manually
No objects selected

Computers

Last Sync Time: 2025-08-25 22:00:03

1 - 10 of 52 › » 10

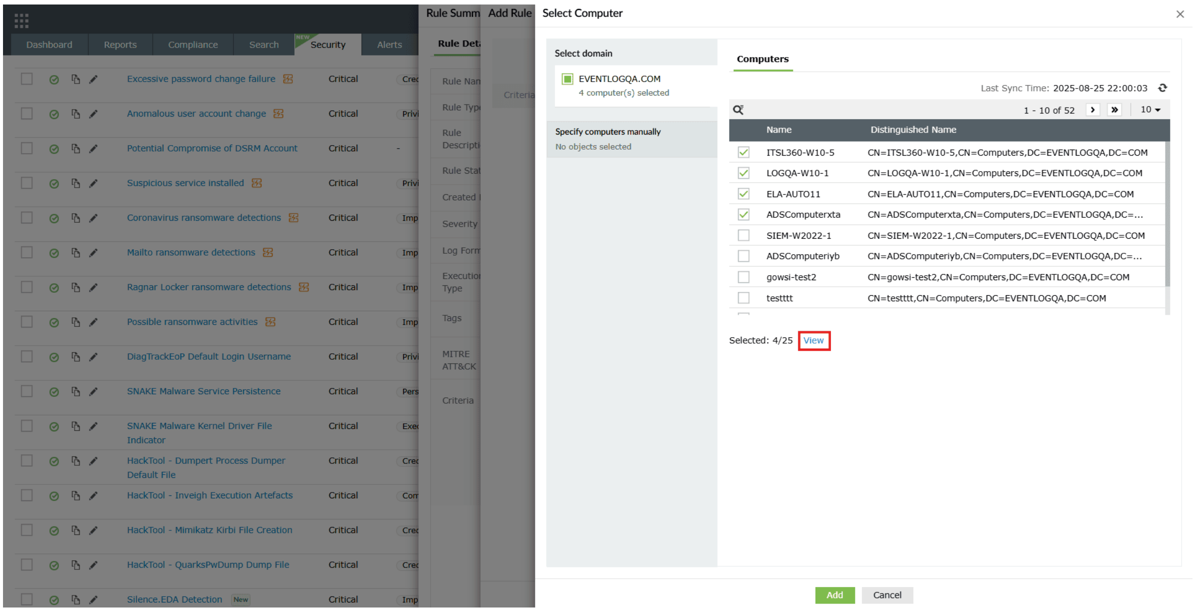
	Name	Distinguished Name
□	ITSL360-W10-5	CN=ITSL360-W10-5,CN=Computers,DC=EVENTLOGQA,DC=COM
□	LOGQA-W10-1	CN=LOGQA-W10-1,CN=Computers,DC=EVENTLOGQA,DC=COM
□	ELA-AUTO11	CN=ELA-AUTO11,CN=Computers,DC=EVENTLOGQA,DC=COM
□	ADSComputerxta	CN=ADSComputerxta,CN=Computers,DC=EVENTLOGQA,DC=...
□	SIEM-W2022-1	CN=SIEM-W2022-1,CN=Computers,DC=EVENTLOGQA,DC=COM
□	ADSComputeriyb	CN=ADSComputeriyb,CN=Computers,DC=EVENTLOGQA,DC=...
□	gowsi-test2	CN=gowsi-test2,CN=Computers,DC=EVENTLOGQA,DC=COM
□	testttt	CN=testttt,CN=Computers,DC=EVENTLOGQA,DC=COM

Selected: 0/25

Add Cancel

Image 27: Configuring object filter users/groups in exception

4. After selecting the preferred devices, you can view your selection by clicking on the View option as highlighted below.



Select Computer

Select domain

☑ EVENTLOGQA.COM
4 computer(s) selected

Specify computers manually
No objects selected

Computers

Last Sync Time: 2025-08-25 22:00:03

1 - 10 of 52 › » 10

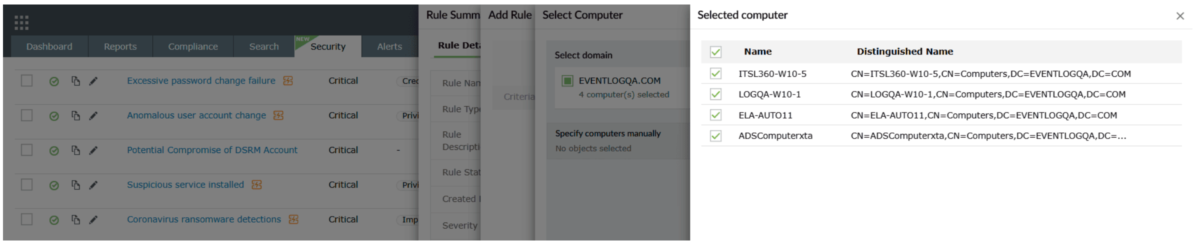
	Name	Distinguished Name
☑	ITSL360-W10-5	CN=ITSL360-W10-5,CN=Computers,DC=EVENTLOGQA,DC=COM
☑	LOGQA-W10-1	CN=LOGQA-W10-1,CN=Computers,DC=EVENTLOGQA,DC=COM
☑	ELA-AUTO11	CN=ELA-AUTO11,CN=Computers,DC=EVENTLOGQA,DC=COM
☑	ADSComputerxta	CN=ADSComputerxta,CN=Computers,DC=EVENTLOGQA,DC=...
□	SIEM-W2022-1	CN=SIEM-W2022-1,CN=Computers,DC=EVENTLOGQA,DC=COM
□	ADSComputeriyb	CN=ADSComputeriyb,CN=Computers,DC=EVENTLOGQA,DC=...
□	gowsi-test2	CN=gowsi-test2,CN=Computers,DC=EVENTLOGQA,DC=COM
□	testttt	CN=testttt,CN=Computers,DC=EVENTLOGQA,DC=COM

Selected: 4/25 View

Add Cancel

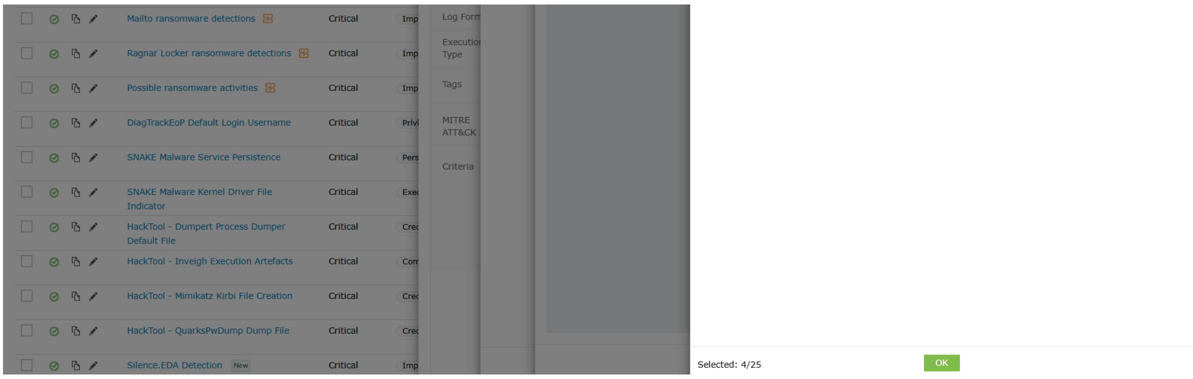
Image 28: Viewing list of configured object filter users/groups

5. The list of Selected computers will be displayed.



Selected computer

☑	Name	Distinguished Name
☑	ITSL360-W10-5	CN=ITSL360-W10-5,CN=Computers,DC=EVENTLOGQA,DC=COM
☑	LOGQA-W10-1	CN=LOGQA-W10-1,CN=Computers,DC=EVENTLOGQA,DC=COM
☑	ELA-AUTO11	CN=ELA-AUTO11,CN=Computers,DC=EVENTLOGQA,DC=COM
☑	ADSComputerxta	CN=ADSComputerxta,CN=Computers,DC=EVENTLOGQA,DC=...

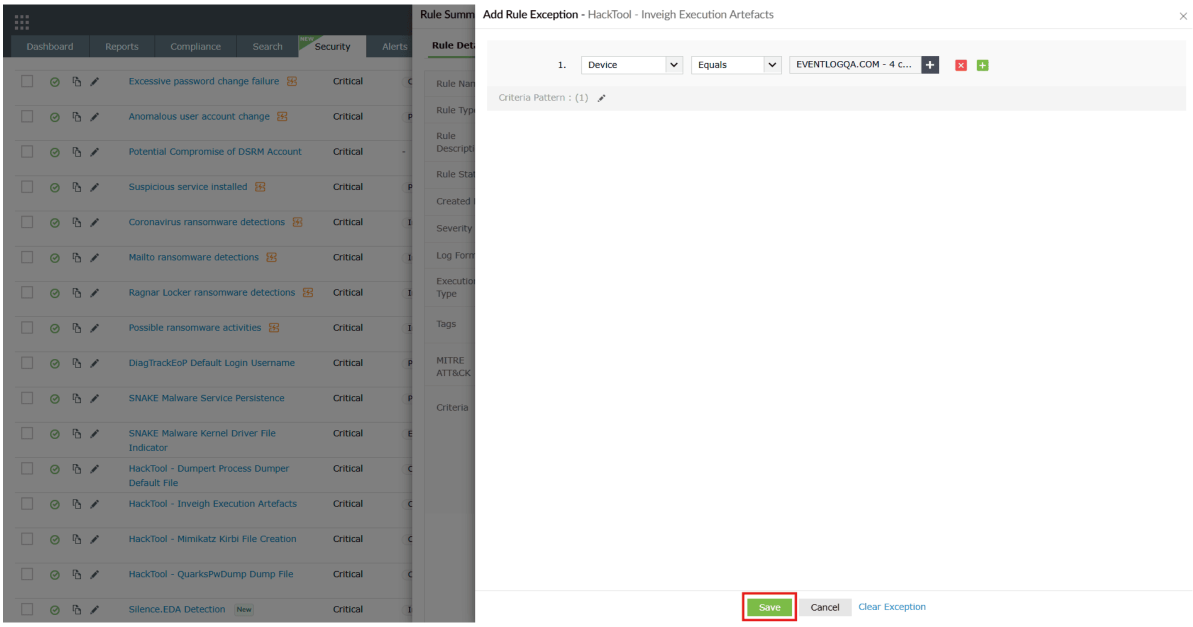


Rule	Severity
Mailto ransomware detections	Critical
Ragnar Locker ransomware detections	Critical
Possible ransomware activities	Critical
DiagTrackEoP Default Login Username	Critical
SNAKE Malware Service Persistence	Critical
SNAKE Malware Kernel Driver File Indicator	Critical
HackTool - Dumpert Process Dumper Default File	Critical
HackTool - Inveigh Execution Artefacts	Critical
HackTool - Mimikatz Kirbi File Creation	Critical
HackTool - QuarksPwDump Dump File	Critical
Silence.EDA Detection New	Critical

Selected: 4/25

Image 29: Configuring object filter users/groups

6. Once the selection is done, click on OK in the selection list and then click on Add in the Select Computer pane. Click on the Save button in the Add Rule Exception pane as highlighted below. In case you wish to reset the exception configurations and redo them, click on Clear Exception.



Rule	Severity
Excessive password change failure	Critical
Anomalous user account change	Critical
Potential Compromise of DSRM Account	Critical
Suspicious service installed	Critical
Coronavirus ransomware detections	Critical
Mailto ransomware detections	Critical
Ragnar Locker ransomware detections	Critical
Possible ransomware activities	Critical
DiagTrackEoP Default Login Username	Critical
SNAKE Malware Service Persistence	Critical
SNAKE Malware Kernel Driver File Indicator	Critical
HackTool - Dumpert Process Dumper Default File	Critical
HackTool - Inveigh Execution Artefacts	Critical
HackTool - Mimikatz Kirbi File Creation	Critical
HackTool - QuarksPwDump Dump File	Critical
Silence.EDA Detection New	Critical

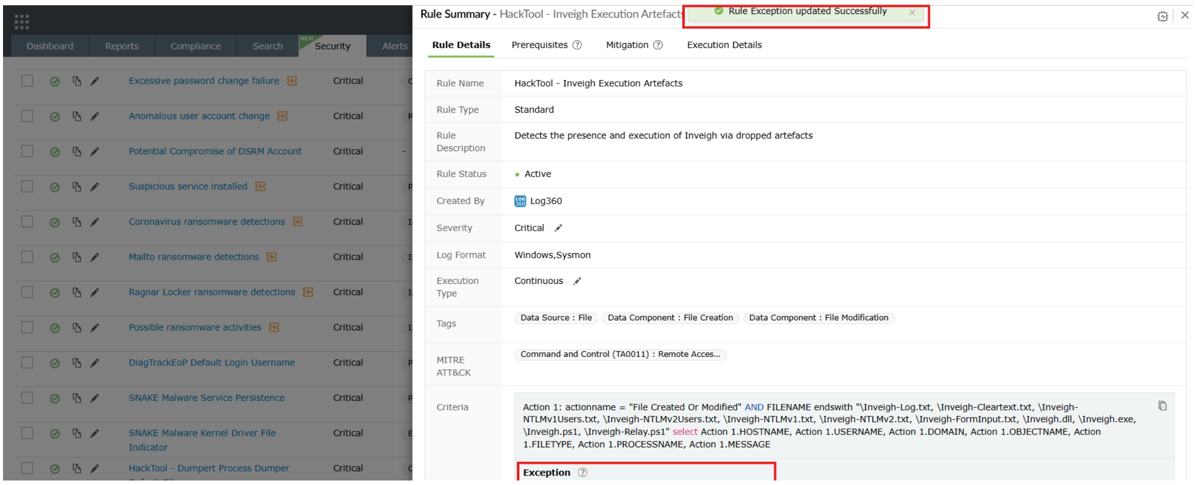
Add Rule Exception - HackTool - Inveigh Execution Artefacts

1. Device Equals EVENTLOGQA.COM - 4 c...

Criteria Pattern : (1)

Image 30: Configuring object filter users/groups in rule management

7. Upon successful completion of action, a Rule Exception saved Successfully pop-up appears briefly, and the selection changes are instantly updated and are visible in the Exception section.

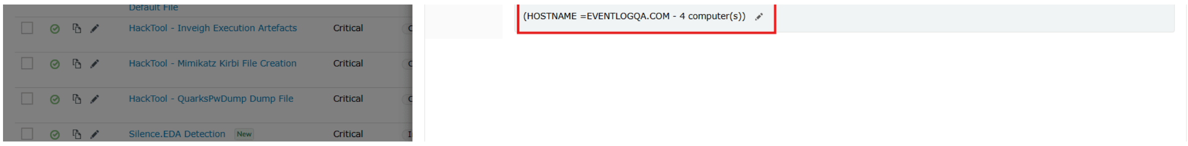


Rule Summary - HackTool - Inveigh Execution Artefacts

Rule Exception updated Successfully

Rule Name	HackTool - Inveigh Execution Artefacts
Rule Type	Standard
Rule Description	Detects the presence and execution of Inveigh via dropped artefacts
Rule Status	Active
Created By	Log360
Severity	Critical
Log Format	Windows,Sysmon
Execution Type	Continuous
Tags	Data Source : File Data Component : File Creation Data Component : File Modification
MITRE ATT&CK	Command and Control (TA0011) : Remote Acces...
Criteria	Action 1: actionname = "File Created Or Modified" AND FILENAME endswith "\Inveigh-Log.txt, \Inveigh-Cleartext.txt, \Inveigh-NTLMv1Users.txt, \Inveigh-NTLMv2Users.txt, \Inveigh-NTLMv1.txt, \Inveigh-NTLMv2.txt, \Inveigh-FormInput.txt, \Inveigh.dll, \Inveigh.exe, \Inveigh.ps1, \Inveigh-Relay.ps1" select Action 1.HOSTNAME, Action 1.USERNAME, Action 1.DOMAIN, Action 1.OBJECTNAME, Action 1.FILETYPE, Action 1.PROCESSNAME, Action 1.MESSAGE Exception

Rule	Severity
Excessive password change failure	Critical
Anomalous user account change	Critical
Potential Compromise of DSRM Account	Critical
Suspicious service installed	Critical
Coronavirus ransomware detections	Critical
Mailto ransomware detections	Critical
Ragnar Locker ransomware detections	Critical
Possible ransomware activities	Critical
DiagTrackEoP Default Login Username	Critical
SNAKE Malware Service Persistence	Critical
SNAKE Malware Kernel Driver File Indicator	Critical
HackTool - Dumpert Process Dumper	Critical



	Rule Name	Severity
	Default File	
□	HackTool - Inveigh Execution Artefacts	Critical
□	HackTool - Mimikatz Kirbi File Creation	Critical
□	HackTool - QuarksPwDump Dump File	Critical
□	Silence.EDA Detection New	Critical

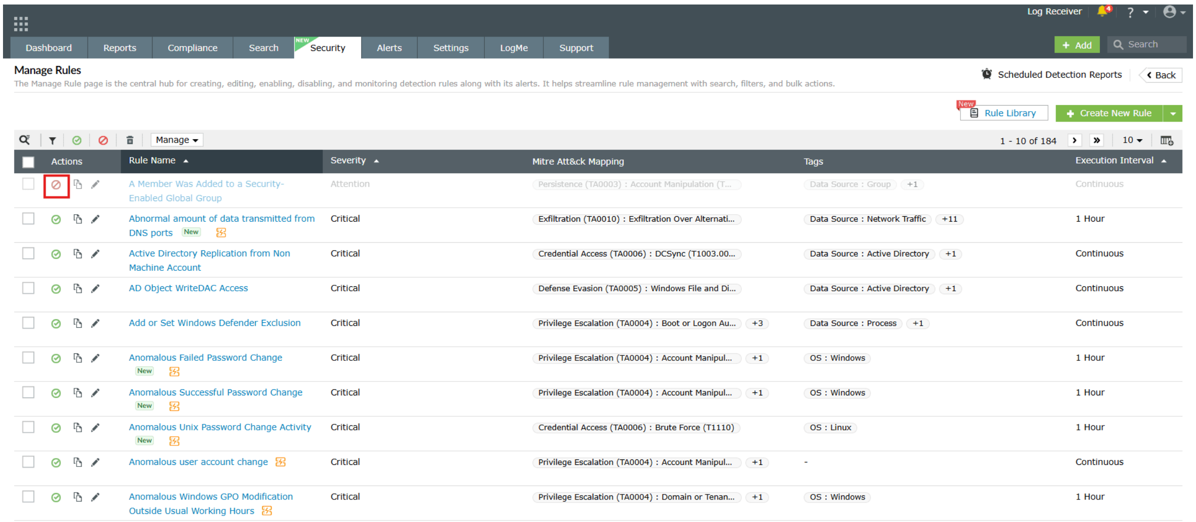
(HOSTNAME =EVENTLOGQA.COM - 4 computer(s))

Image 31: Configuring object filter users/groups in rule exceptions

C. Enabling rule

When activating a rule, the object filter automatically slides open for that particular rule.

1. Click on the currently disabled icon ⊘ under the Actions column to enable the rule.



Manage Rules

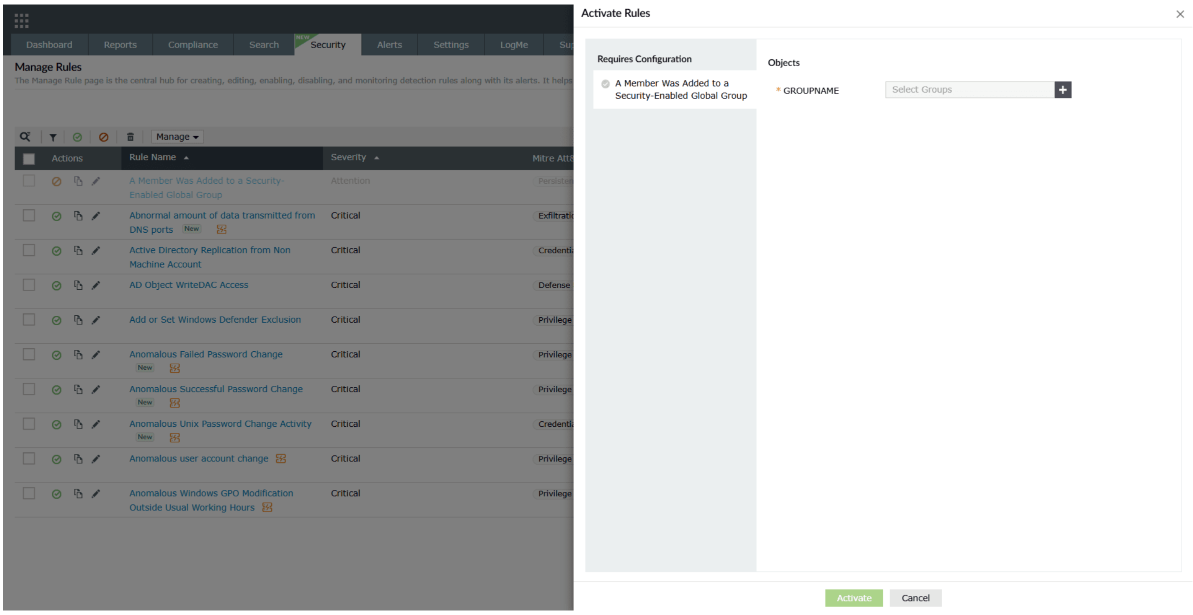
The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

1 - 10 of 184 | 10

Actions	Rule Name	Severity	Mitre Att&ck Mapping	Tags	Execution Interval
⊘	A Member Was Added to a Security-Enabled Global Group	Attention	Persistence (TA0003) : Account Manipulation (T...	Data Source : Group +1	Continuous
✓	Abnormal amount of data transmitted from DNS ports New	Critical	Exfiltration (TA0010) : Exfiltration Over Alternati...	Data Source : Network Traffic +11	1 Hour
✓	Active Directory Replication from Non Machine Account	Critical	Credential Access (TA0006) : DCSync (T1003.00...	Data Source : Active Directory +1	Continuous
✓	AD Object WriteDAC Access	Critical	Defense Evasion (TA0005) : Windows File and Di...	Data Source : Active Directory +1	Continuous
✓	Add or Set Windows Defender Exclusion	Critical	Privilege Escalation (TA0004) : Boot or Logon Au... +3	Data Source : Process +1	Continuous
✓	Anomalous Failed Password Change New	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows	1 Hour
✓	Anomalous Successful Password Change New	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows	1 Hour
✓	Anomalous Unix Password Change Activity New	Critical	Credential Access (TA0006) : Brute Force (T1110)	OS : Linux	1 Hour
✓	Anomalous user account change	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	-	Continuous
✓	Anomalous Windows GPO Modification Outside Usual Working Hours	Critical	Privilege Escalation (TA0004) : Domain or Tenan... +1	OS : Windows	1 Hour

Image 32: Enabling a rule

2. The object filter pane slides open upon clicking on the disabled icon.



Activate Rules

Requires Configuration

A Member Was Added to a Security-Enabled Global Group

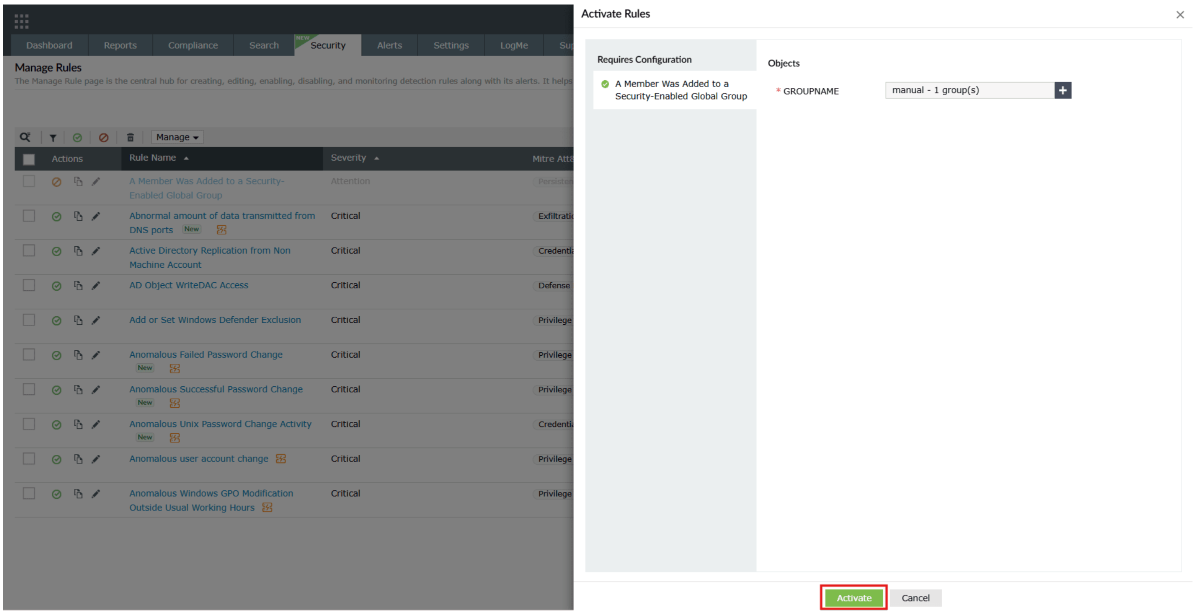
Objects

* GROUPNAME: Select Groups

Image 33: Object filtering while enabling a rule

3. Select preferred users/groups and click on the Activate button

3. Select preferred users/groups and click on the Activate button.



Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps

Rule Name	Severity	Mitre Att
A Member Was Added to a Security-Enabled Global Group	Attention	Persisten
Abnormal amount of data transmitted from DNS ports New	Critical	Exfiltratio
Active Directory Replication from Non Machine Account	Critical	Credenti
AD Object WriteDAC Access	Critical	Defense
Add or Set Windows Defender Exclusion	Critical	Privilege
Anomalous Failed Password Change New	Critical	Privilege
Anomalous Successful Password Change New	Critical	Privilege
Anomalous Unix Password Change Activity New	Critical	Credenti
Anomalous user account change	Critical	Privilege
Anomalous Windows GPO Modification Outside Usual Working Hours	Critical	Privilege

Requires Configuration

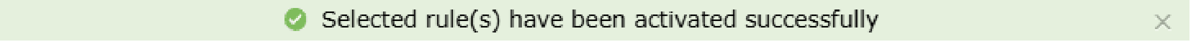
A Member Was Added to a Security-Enabled Global Group

Objects

* GROUPNAME: manual - 1 group(s)

Image 34: Object filtering while enabling a rule

4. Upon successful completion of action, the below pop-up appears.



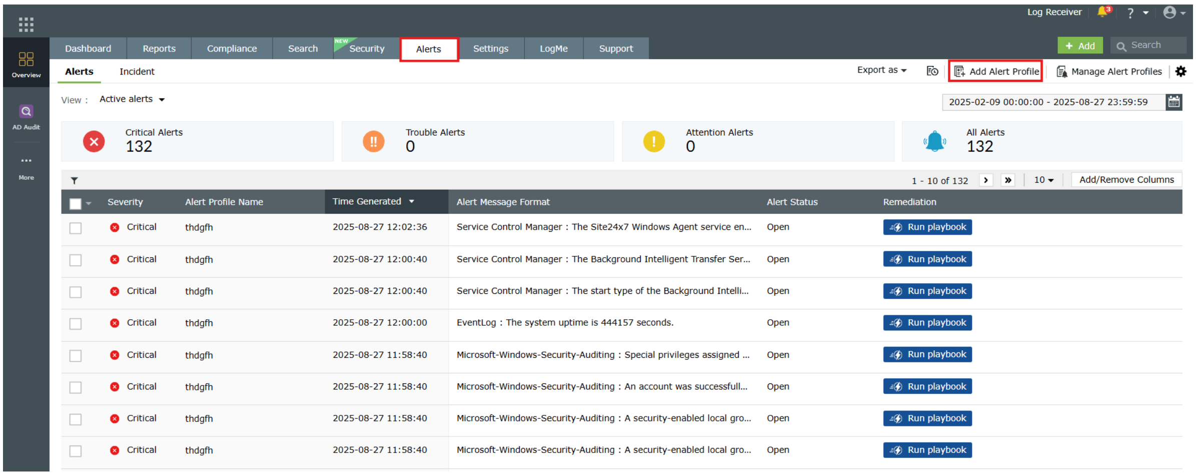
Selected rule(s) have been activated successfully

Alerts

The solution also supports object filters when creating or editing alert profiles, enabling you to refine Active Directory-based criteria with user, group, or OU selections. To do this, follow the steps below:

> NOTE
>
> The Active Directory object filter is accessible only for the rules and criteria under the Active Directory log type.

1. In the product console, navigate to the Alerts tab and click on Add Alert Profile.



View : Active alerts

2025-02-09 00:00:00 - 2025-08-27 23:59:59

Critical Alerts 132 | Trouble Alerts 0 | Attention Alerts 0 | All Alerts 132

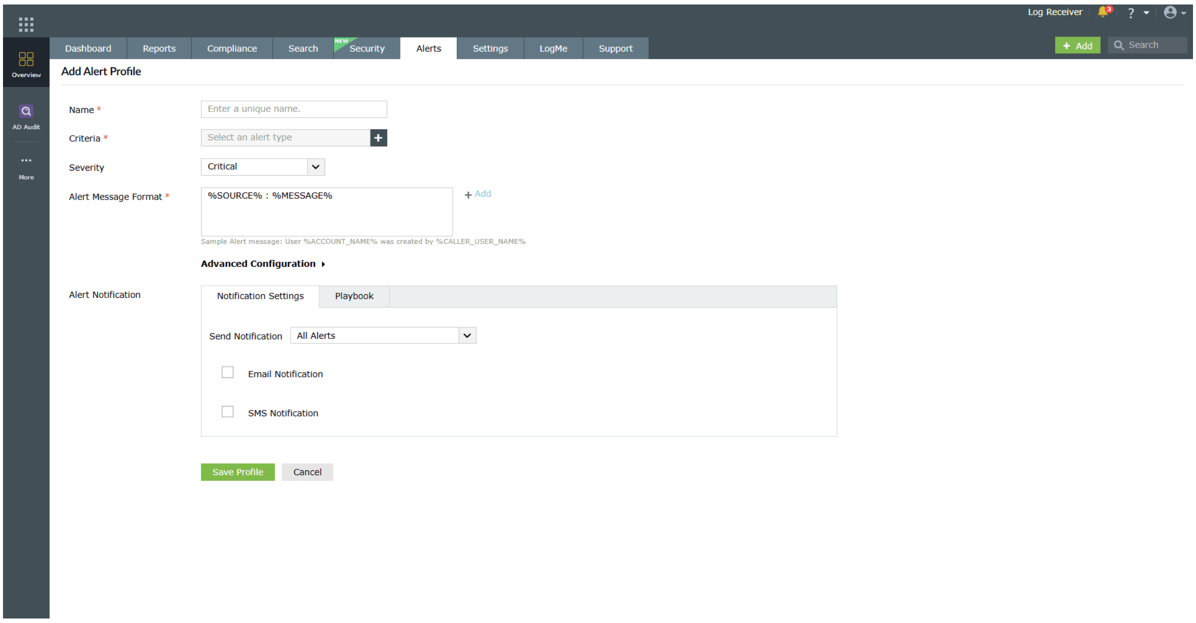
1 - 10 of 132 | 10

Severity	Alert Profile Name	Time Generated	Alert Message Format	Alert Status	Remediation
Critical	thdgfh	2025-08-27 12:02:36	Service Control Manager : The Site24x7 Windows Agent service en...	Open	Run playbook
Critical	thdgfh	2025-08-27 12:00:40	Service Control Manager : The Background Intelligent Transfer Ser...	Open	Run playbook
Critical	thdgfh	2025-08-27 12:00:40	Service Control Manager : The start type of the Background Intelli...	Open	Run playbook
Critical	thdgfh	2025-08-27 12:00:00	EventLog : The system uptime is 444157 seconds.	Open	Run playbook
Critical	thdgfh	2025-08-27 11:58:40	Microsoft-Windows-Security-Auditing : Special privileges assigned ...	Open	Run playbook
Critical	thdgfh	2025-08-27 11:58:40	Microsoft-Windows-Security-Auditing : An account was successfull...	Open	Run playbook
Critical	thdgfh	2025-08-27 11:58:40	Microsoft-Windows-Security-Auditing : A security-enabled local gro...	Open	Run playbook
Critical	thdgfh	2025-08-27 11:58:40	Microsoft-Windows-Security-Auditing : A security-enabled local gro...	Open	Run playbook

□	Critical	thdgfh	2025-08-27 11:58:40	Service Control Manager : The WMI Performance Adapter service ...	Open	Run playbook
□	Critical	thdgfh	2025-08-27 11:58:39	Microsoft-Windows-Security-Auditing : Special privileges assigned ...	Open	Run playbook

Image 35: Adding an alert profile

2. The Add Alert Profile module is displayed.



Add Alert Profile

Name * Enter a unique name.

Criteria * Select an alert type

Severity Critical

Alert Message Format * %SOURCE% : %MESSAGE% + Add

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Advanced Configuration

Alert Notification

Notification Settings | Playbook

Send Notification All Alerts

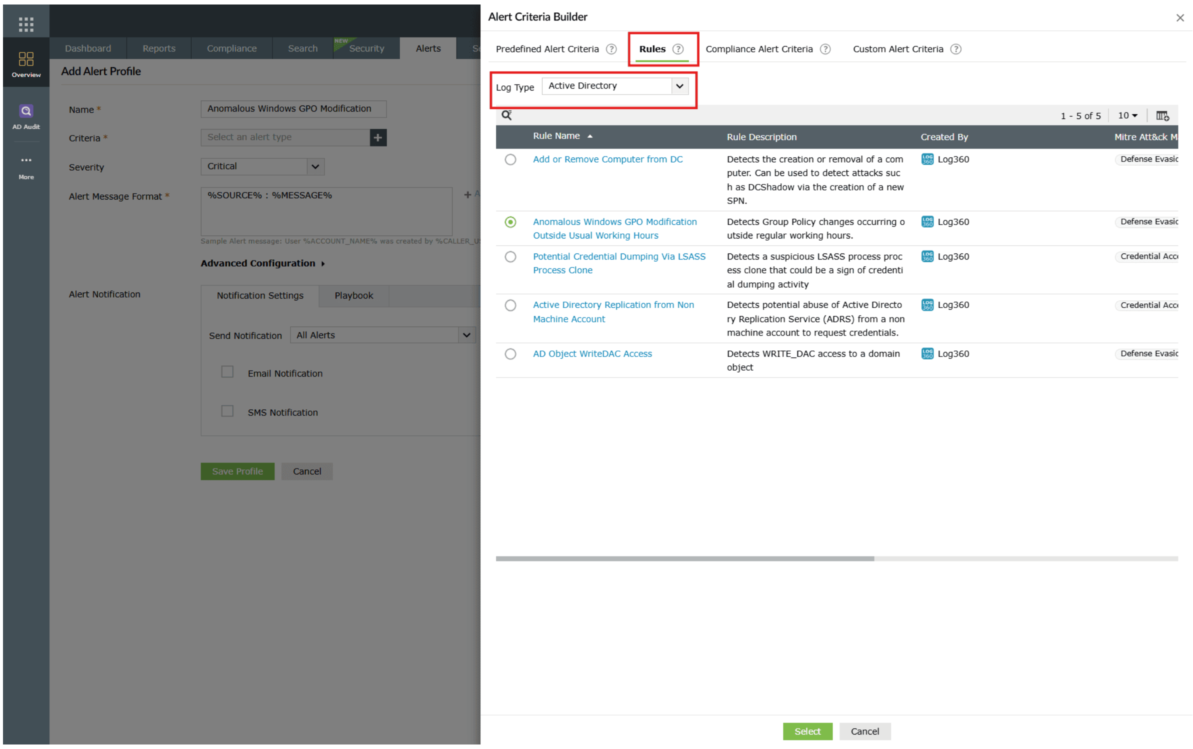
□ Email Notification

□ SMS Notification

Save Profile Cancel

Image 36: Add alert profile module

3. Provide the Name for the alert. Add Active Directory specific Criteria by choosing Active Directory as the Log Type in the Rules sub-tab of the Alert Criteria Builder. Click on the Select button.



Add Alert Profile

Name * Anomalous Windows GPO Modification

Criteria * Select an alert type

Severity Critical

Alert Message Format * %SOURCE% : %MESSAGE%

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_U

Advanced Configuration

Alert Notification

Notification Settings | Playbook

Send Notification All Alerts

□ Email Notification

□ SMS Notification

Save Profile Cancel

Alert Criteria Builder

Predefined Alert Criteria | Rules | Compliance Alert Criteria | Custom Alert Criteria

Log Type Active Directory

1 - 5 of 5 10

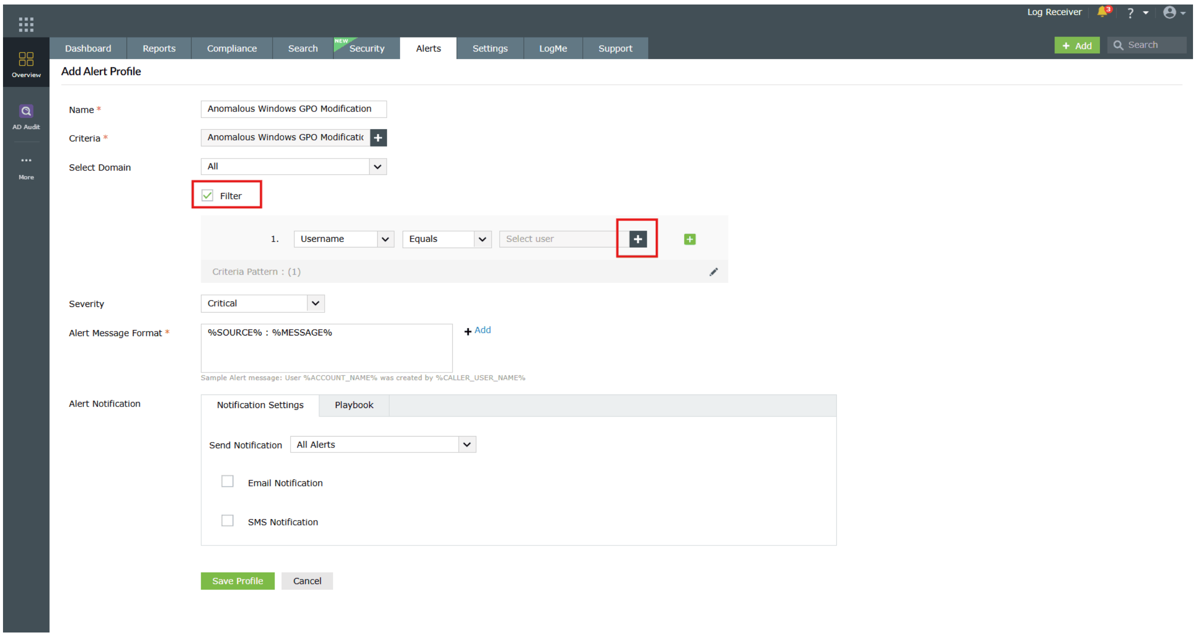
	Rule Name	Rule Description	Created By	Mitre Att&ck M
○	Add or Remove Computer from DC	Detects the creation or removal of a computer. Can be used to detect attacks such as DCShadow via the creation of a new SPN.	Log360	Defense Evasic
●	Anomalous Windows GPO Modification Outside Usual Working Hours	Detects Group Policy changes occurring outside regular working hours.	Log360	Defense Evasic
○	Potential Credential Dumping Via LSASS Process Clone	Detects a suspicious LSASS process process clone that could be a sign of credential dumping activity	Log360	Credential Acce
○	Active Directory Replication from Non Machine Account	Detects potential abuse of Active Directory Replication Service (ADRS) from a non machine account to request credentials.	Log360	Credential Acce
○	AD Object WriteDAC Access	Detects WRITE_DAC access to a domain object	Log360	Defense Evasic

Select Cancel

Image 37: Object filtering in the alerts module

Image 37: Object filtering in the alerts module

4. Choose the domain under the Select Domain drop-down. Tick the Filter checkbox and then configure the filter based on your requirements. Click on the add button of the object filter to select users to be grouped under this.



Add Alert Profile

Name * Anomalous Windows GPO Modification

Criteria * Anomalous Windows GPO Modificatic

Select Domain All

☑ Filter

1. Username Equals Select user

Criteria Pattern : (1)

Severity Critical

Alert Message Format * %SOURCE% : %MESSAGE%

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Alert Notification: Notification Settings | Playbook

Send Notification All Alerts

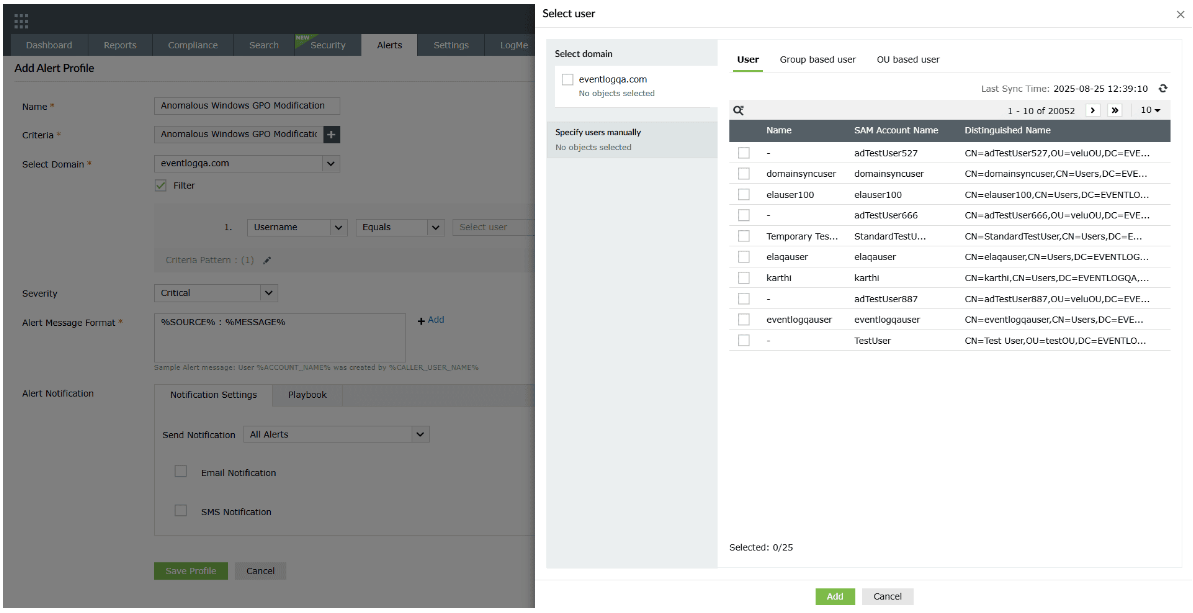
□ Email Notification

□ SMS Notification

Save Profile | Cancel

Image 38: Object filtering while adding an alerts profile

5. The Select user pane slides open. The user names will be displayed along with the object filter feature in order to be able to filter and choose which users you wish to group under this alert configuration.



Add Alert Profile

Name * Anomalous Windows GPO Modification

Criteria * Anomalous Windows GPO Modificatic

Select Domain * eventlogqa.com

☑ Filter

1. Username Equals Select user

Criteria Pattern : (1)

Severity Critical

Alert Message Format * %SOURCE% : %MESSAGE%

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Alert Notification: Notification Settings | Playbook

Send Notification All Alerts

□ Email Notification

□ SMS Notification

Save Profile | Cancel

Select user

Select domain

□ eventlogqa.com
No objects selected

Specify users manually
No objects selected

User | Group based user | OU based user

Last Sync Time: 2025-08-25 12:39:10

1 - 10 of 20052 | 10

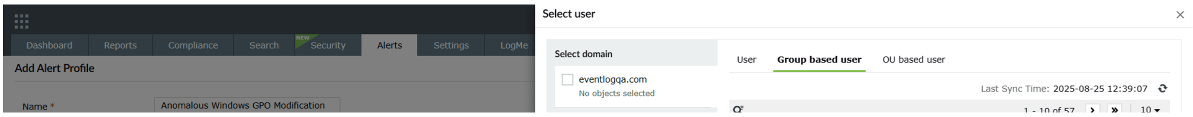
	Name	SAM Account Name	Distinguished Name
□	-	adTestUser527	CN=adTestUser527,OU=veluOU,DC=EVE...
□	domainsyncuser	domainsyncuser	CN=domainsyncuser,CN=Users,DC=EVE...
□	elauser100	elauser100	CN=elauser100,CN=Users,DC=EVENTLO...
□	-	adTestUser666	CN=adTestUser666,OU=veluOU,DC=EVE...
□	Temporary Tes...	StandardTestU...	CN=StandardTestUser,CN=Users,DC=E...
□	elaqauser	elaqauser	CN=elaqauser,CN=Users,DC=EVENTLOG...
□	karthi	karthi	CN=karthi,CN=Users,DC=EVENTLOGQA,...
□	-	adTestUser887	CN=adTestUser887,OU=veluOU,DC=EVE...
□	eventlogqauser	eventlogqauser	CN=eventlogqauser,CN=Users,DC=EVE...
□	-	TestUser	CN=Test User,OU=testOU,DC=EVENTLO...

Selected: 0/25

Add | Cancel

Image 39: Object filtering in the alerts module

6. Similarly, the Group based user sub-tab also includes the filter for user selection based on user groups.



Add Alert Profile

Name * Anomalous Windows GPO Modification

Select user

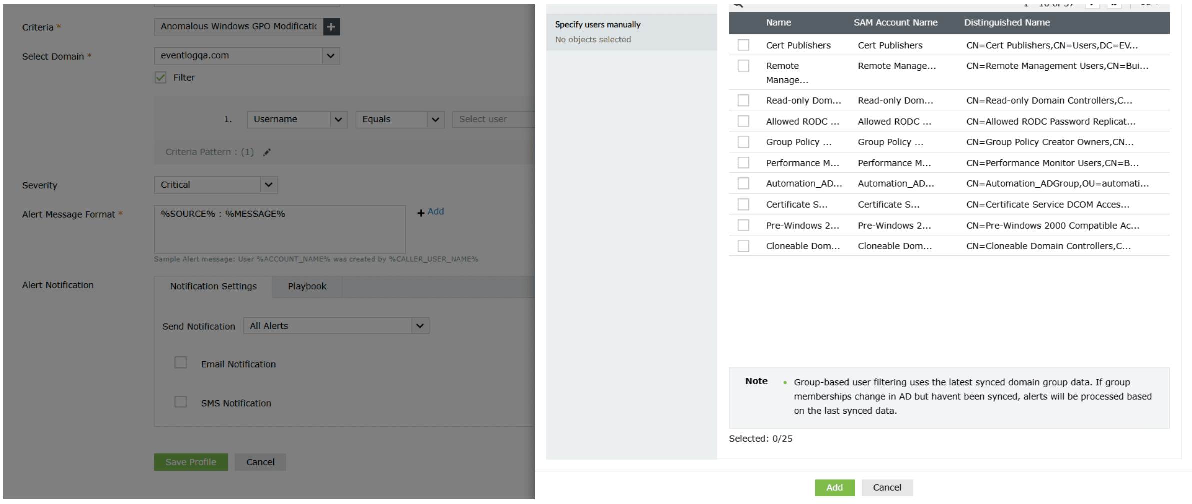
Select domain

□ eventlogqa.com
No objects selected

User | Group based user | OU based user

Last Sync Time: 2025-08-25 12:39:07

1 - 10 of 57 | 10



Criteria * Anomalous Windows GPO Modificatic

Select Domain * eventlogqa.com

☑ Filter

1. Username Equals Select user

Criteria Pattern : (1)

Severity Critical

Alert Message Format * %SOURCE% : %MESSAGE%

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Alert Notification

Send Notification All Alerts

□ Email Notification

□ SMS Notification

Specify users manually
No objects selected

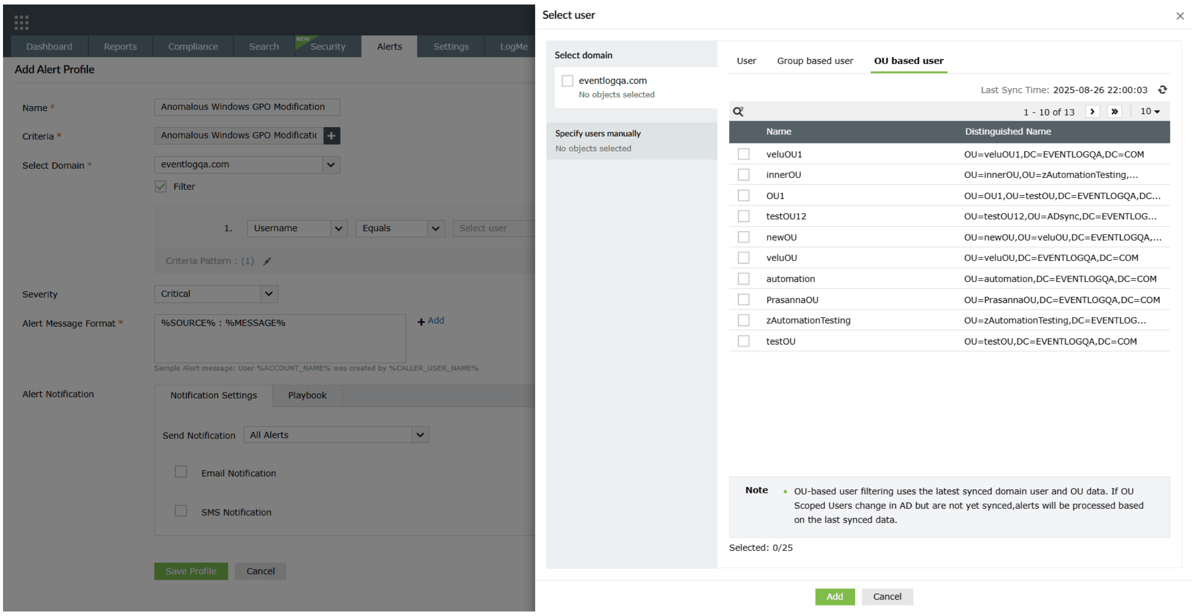
	Name	SAM Account Name	Distinguished Name
□	Cert Publishers	Cert Publishers	CN=Cert Publishers,CN=Users,DC=EV...
□	Remote Manage...	Remote Manage...	CN=Remote Management Users,CN=Bui...
□	Read-only Dom...	Read-only Dom...	CN=Read-only Domain Controllers,C...
□	Allowed RODC ...	Allowed RODC ...	CN=Allowed RODC Password Replicat...
□	Group Policy ...	Group Policy ...	CN=Group Policy Creator Owners,CN...
□	Performance M...	Performance M...	CN=Performance Monitor Users,CN=B...
□	Automation_AD...	Automation_AD...	CN=Automation_ADGroup,OU=automati...
□	Certificate S...	Certificate S...	CN=Certificate Service DCOM Acces...
□	Pre-Windows 2...	Pre-Windows 2...	CN=Pre-Windows 2000 Compatible Ac...
□	Cloneable Dom...	Cloneable Dom...	CN=Cloneable Domain Controllers,C...

Note • Group-based user filtering uses the latest synced domain group data. If group memberships change in AD but havent been synced, alerts will be processed based on the last synced data.

Selected: 0/25

Image 40: Configuring object filter users/groups

7. The OU based user sub-tab also includes the filter for user selection where the users are listed categorized by their OUs.



Add Alert Profile

Name * Anomalous Windows GPO Modification

Criteria * Anomalous Windows GPO Modificatic

Select Domain * eventlogqa.com

☑ Filter

1. Username Equals Select user

Criteria Pattern : (1)

Severity Critical

Alert Message Format * %SOURCE% : %MESSAGE%

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Alert Notification

Send Notification All Alerts

□ Email Notification

□ SMS Notification

Select user

Select domain

□ eventlogqa.com
No objects selected

Specify users manually
No objects selected

User | Group based user | OU based user

Last Sync Time: 2025-08-26 22:00:03

1 - 10 of 13 10

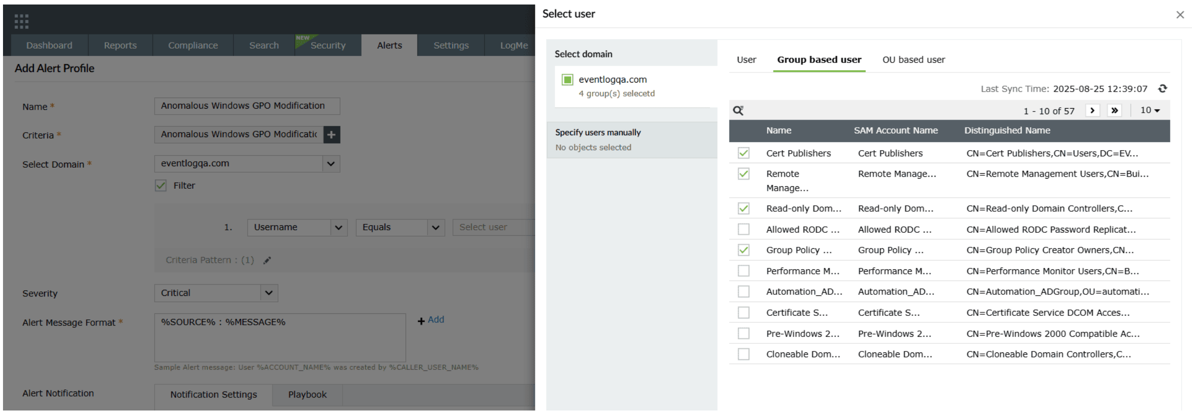
	Name	Distinguished Name
□	veluOU1	OU=veluOU1,DC=EVENTLOGQA,DC=COM
□	innerOU	OU=innerOU,OU=zAutomationTesting,...
□	OU1	OU=OU1,OU=testOU,DC=EVENTLOGQA,DC...
□	testOU12	OU=testOU12,OU=ADsync,DC=EVENTLOG...
□	newOU	OU=newOU,OU=veluOU,DC=EVENTLOGQA,...
□	veluOU	OU=veluOU,DC=EVENTLOGQA,DC=COM
□	automation	OU=automation,DC=EVENTLOGQA,DC=COM
□	PrasannaOU	OU=PrasannaOU,DC=EVENTLOGQA,DC=COM
□	zAutomationTesting	OU=zAutomationTesting,DC=EVENTLOG...
□	testOU	OU=testOU,DC=EVENTLOGQA,DC=COM

Note • OU-based user filtering uses the latest synced domain user and OU data. If OU Scoped Users change in AD but are not yet synced,alerts will be processed based on the last synced data.

Selected: 0/25

Image 41: Configuring object filter users/groups

8. After selecting the preferred users, you can view your selection by clicking on the View option as highlighted below.



Add Alert Profile

Name * Anomalous Windows GPO Modification

Criteria * Anomalous Windows GPO Modificatic

Select Domain * eventlogqa.com

☑ Filter

1. Username Equals Select user

Criteria Pattern : (1)

Severity Critical

Alert Message Format * %SOURCE% : %MESSAGE%

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Alert Notification

Select user

Select domain

☑ eventlogqa.com
4 group(s) selecetd

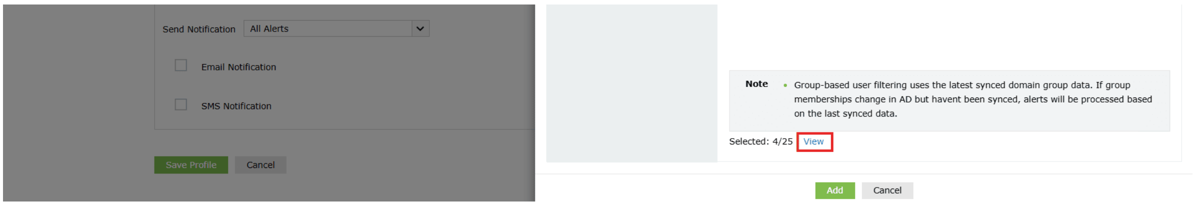
Specify users manually
No objects selected

User | Group based user | OU based user

Last Sync Time: 2025-08-25 12:39:07

1 - 10 of 57 10

	Name	SAM Account Name	Distinguished Name
☑	Cert Publishers	Cert Publishers	CN=Cert Publishers,CN=Users,DC=EV...
☑	Remote Manage...	Remote Manage...	CN=Remote Management Users,CN=Bui...
☑	Read-only Dom...	Read-only Dom...	CN=Read-only Domain Controllers,C...
□	Allowed RODC ...	Allowed RODC ...	CN=Allowed RODC Password Replicat...
☑	Group Policy ...	Group Policy ...	CN=Group Policy Creator Owners,CN...
□	Performance M...	Performance M...	CN=Performance Monitor Users,CN=B...
□	Automation_AD...	Automation_AD...	CN=Automation_ADGroup,OU=automati...
□	Certificate S...	Certificate S...	CN=Certificate Service DCOM Acces...
□	Pre-Windows 2...	Pre-Windows 2...	CN=Pre-Windows 2000 Compatible Ac...
□	Cloneable Dom...	Cloneable Dom...	CN=Cloneable Domain Controllers,C...



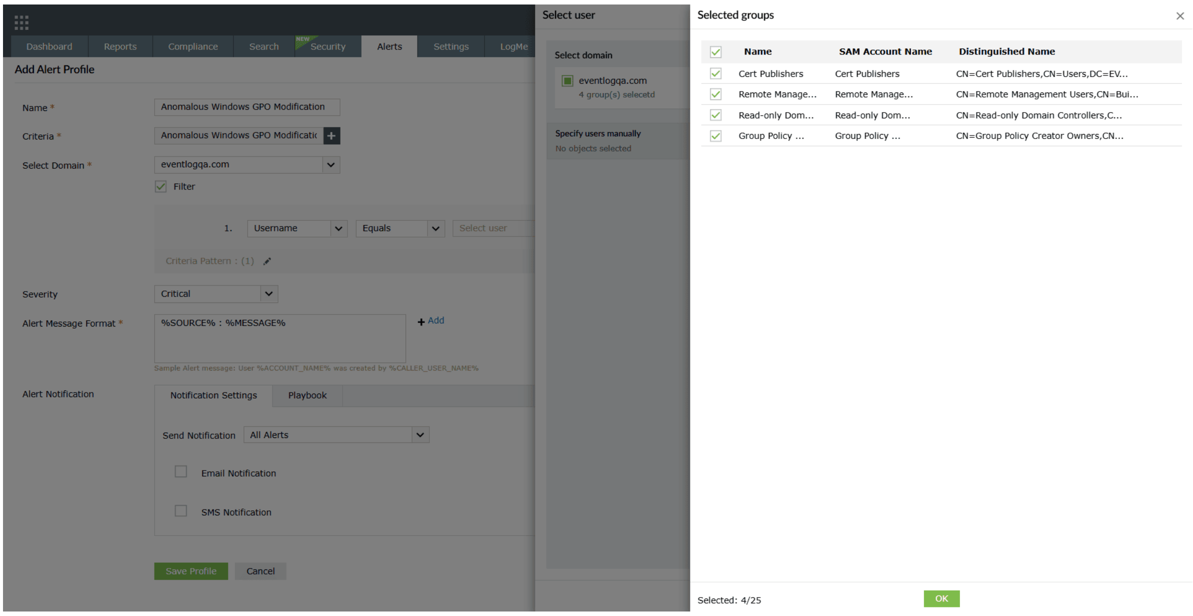
Send Notification: All Alerts

Note • Group-based user filtering uses the latest synced domain group data. If group memberships change in AD but havent been synced, alerts will be processed based on the last synced data.

Selected: 4/25 View

Image 42: Viewing list of configured object filter users/groups

9. The list of Selected users/groups will be displayed.



Name *: Anomalous Windows GPO Modification

Criteria *: Anomalous Windows GPO Modificatic

Select Domain *: eventlogqa.com

1. Username | Equals | Select user

Criteria Pattern : (1)

Severity: Critical

Alert Message Format *: %SOURCE% : %MESSAGE%

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Alert Notification

Send Notification: All Alerts

eventlogqa.com
4 group(s) selecetd

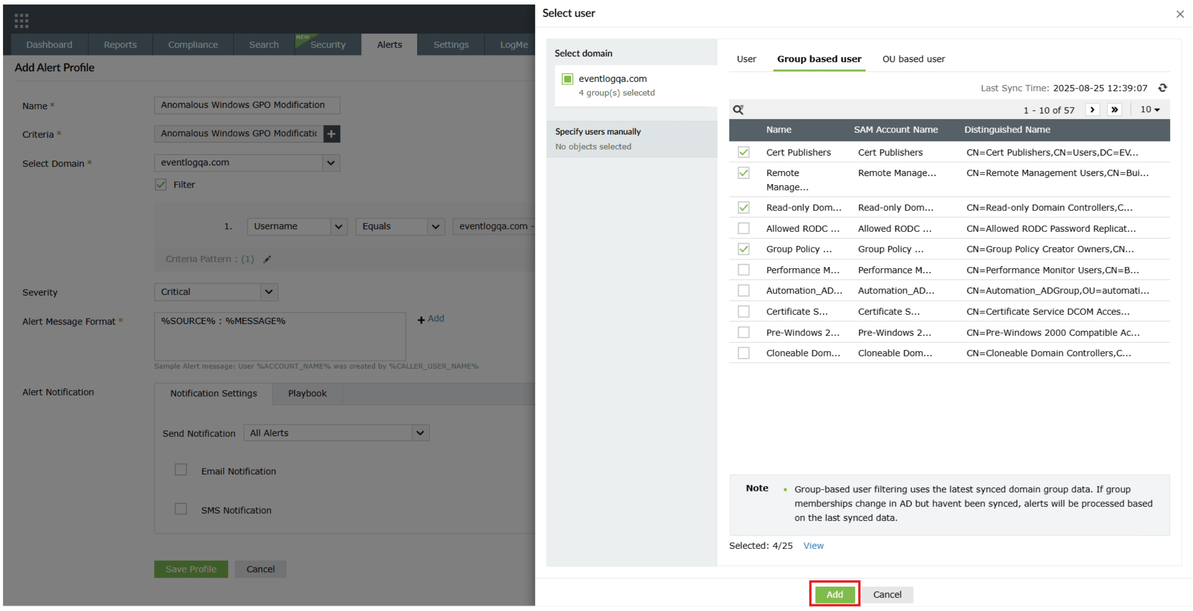
No objects selected

☑	Name	SAM Account Name	Distinguished Name
☑	Cert Publishers	Cert Publishers	CN=Cert Publishers,CN=Users,DC=EV...
☑	Remote Manage...	Remote Manage...	CN=Remote Management Users,CN=Bui...
☑	Read-only Dom...	Read-only Dom...	CN=Read-only Domain Controllers,C...
☑	Group Policy ...	Group Policy ...	CN=Group Policy Creator Owners,CN...

Selected: 4/25

Image 43: Configuring object filter users/groups

10. Once the selection is done, click on OK in the selection list and then click on Add in the Select user pane.



Name *: Anomalous Windows GPO Modification

Criteria *: Anomalous Windows GPO Modificatic

Select Domain *: eventlogqa.com

1. Username | Equals | eventlogqa.com -

Criteria Pattern : (1)

Severity: Critical

Alert Message Format *: %SOURCE% : %MESSAGE%

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Alert Notification

Send Notification: All Alerts

eventlogqa.com
4 group(s) selecetd

No objects selected

Last Sync Time: 2025-08-25 12:39:07

1 - 10 of 57 | 10

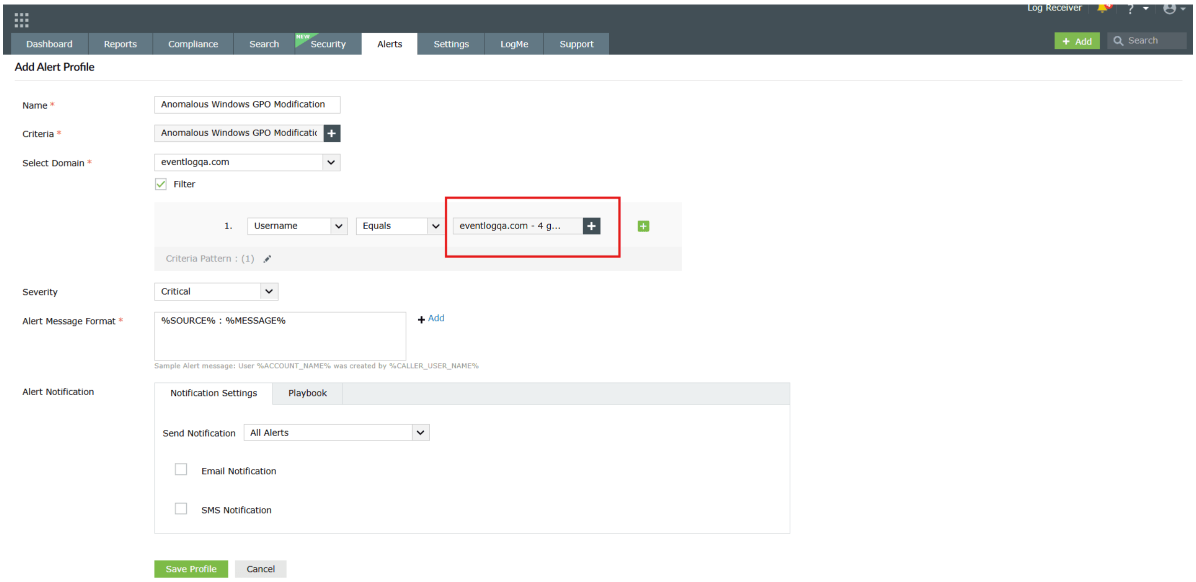
	Name	SAM Account Name	Distinguished Name
☑	Cert Publishers	Cert Publishers	CN=Cert Publishers,CN=Users,DC=EV...
☑	Remote Manage...	Remote Manage...	CN=Remote Management Users,CN=Bui...
☑	Read-only Dom...	Read-only Dom...	CN=Read-only Domain Controllers,C...
□	Allowed RODC ...	Allowed RODC ...	CN=Allowed RODC Password Replicat...
☑	Group Policy ...	Group Policy ...	CN=Group Policy Creator Owners,CN...
□	Performance M...	Performance M...	CN=Performance Monitor Users,CN=B...
□	Automation_AD...	Automation_AD...	CN=Automation_ADGroup,OU=automati...
□	Certificate S...	Certificate S...	CN=Certificate Service DCOM Acces...
□	Pre-Windows 2...	Pre-Windows 2...	CN=Pre-Windows 2000 Compatible Ac...
□	Cloneable Dom...	Cloneable Dom...	CN=Cloneable Domain Controllers,C...

Note • Group-based user filtering uses the latest synced domain group data. If group memberships change in AD but havent been synced, alerts will be processed based on the last synced data.

Selected: 4/25 View

Image 44: Configuring object filter users/groups

11. Upon successful completion of action, the selection changes are instantly updated.



Add Alert Profile

Name * Anomalous Windows GPO Modification

Criteria * Anomalous Windows GPO Modificatic

Select Domain * eventlogqa.com

☑ Filter

1. Username Equals eventlogqa.com - 4 g...

Criteria Pattern : (1)

Severity Critical

Alert Message Format * %SOURCE% : %MESSAGE% + Add

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Alert Notification

Send Notification All Alerts

□ Email Notification

□ SMS Notification

Image 45: Configuring object filter users/groups in alerts module

NOTE

The object filter can also be used in a existing alert profile by clicking on the edit icon ✎ of an alert profile and following the above mentioned steps. To learn more about creating and managing alert profiles, refer to the Alerts help document.

Read also

This document explained how to use the object filter during rule installation, rule management, and alert configuration. You also learned how it can be applied in the objects and exception sections, as well as in alert profiles, to improve accuracy in monitoring.

- Active Directory Object Filter Overview

Chapter 4.1.4 Rule library

4.1.4.1. About Rule Library

Last updated on: September 12, 2025

In this page

Log360's Rule Library is a centralized, cloud-delivered repository of security threat detection rules. It is designed to enhance Log360's ability to identify potential security threats. The rules within Log360's Rule Library are primarily based on two standards:

- MITRE ATT&CK® framework: The rules are directly mapped to tactics and techniques used by adversaries, allowing security teams to understand the context of an attack and anticipate the attacker's next move.
- Sigma rules: These are generic, open-source yet credible rules written in standardized format converted to Log360's query structure.

By leveraging a cloud-delivered rule library, security teams can receive up-to-date detection logic automatically without having to write or manually update every rule, thus staying ahead of emerging threats.

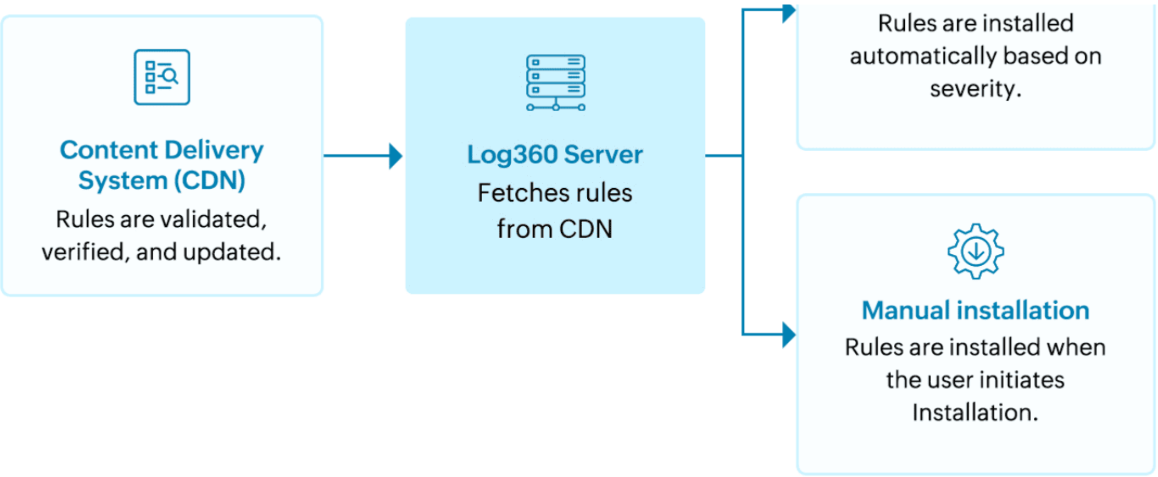
NOTE

Explore in depth the functionalities of Log360's rule library and its Security Intelligence Pack.

Highlights of Log360's Rule Library:

- Over 2,000 predefined threat detection rules to spot insider threat, external threats, malware, APTs and more.
- Rules are categorized based on the log sources they are associated with for easier implementation.
- Rules are also mapped to relevant MITRE ATT&CK® threat modelling framework.
- Option to automatically install new threat detection rules based on your security policies. This ensures your systems are immediately protected against the latest threats and attacks as soon as a new rule is released.

Workflow


Content Delivery System (CDN)
Rules are validated, verified, and updated.
Log360 Server
Fetches rules from CDN
Rules are installed automatically based on severity.
Manual installation
Rules are installed when the user initiates Installation.

The cloud delivered system of Log360, hosts the detection rules uploaded by ManageEngine. The rules are then delivered to the Log360 server.

Please note that the Log360 server should have an active internet connection for uninterrupted update of the detection rules. For offline or air-gapped environments, rule updates can be applied by downloading the latest Rule Library package and configuring the system to use it locally.

Once the rules are updated, the Available Rules tab in the solution's console lets you install and configure them. Our solution also provides auto-installation option which updates the rules in your environment as the rule gets pushed to the Rule Library by ManageEngine team.

This guide explores how you can selectively install rules or configure auto-updates of rules.

Understanding Rule Library

In the central view of the Rule Library, rule attributes are displayed in a table. Columns represent different fields, and additional columns can be added or removed to customize the view. The Rule Library is divided into two tabs: Available Rules and Installed Rules.

Key aspects of the Rule Library include:

- MITRE ATT&CK® Mapping: Each rule is aligned with tactics and techniques from the MITRE ATT&CK® framework, offering better visibility into adversarial behaviors.
- Severity classification: Rules are assigned severity levels to help users prioritize detections and response actions effectively.

Common components:

These components are present in both the Available Rules and Installed Rules tabs.

Component	Details
Rule Name	The name of the rule for identification.
Severity	Shows the rule's criticality level, such as Attention, Critical, or Trouble.

Component	Details
MITRE ATT&CK® Mapping	Displays the associated MITRE ATT&CK® tactic and techniques.
Tags	Lists related tags such as data source and data component associated with the rule.
Rule Type	Specifies whether the rule is Standard, Anomaly, or Advanced.
Created Time	The date and time when the rule was first added.
Last Modified Time	The date and time when the rule was last modified.
Description	Provides a detailed summary of what the rule detects, including its purpose and author information.

Components specific to the Installed Rules table

Field	Details
Execution Interval	Defines how criteria matching occurs. • Continuous: Matches incoming logs and raises detection directly if they match. • Intelligent: Runs the criteria on indexed logs and raises detection if matched from indexed logs.
Created By	Indicates the source of the rule. In this case, all rules are created by Log360.

Read also

This page introduced the Rule Library, its role in enhancing threat detection and architecture. To learn how to manage and configure these rules in your environment, refer to:

- Installing Rules
- Configuring Auto-Install Settings

4.1.4.2. Installing Rules

Last updated on: September 12, 2025

In this page

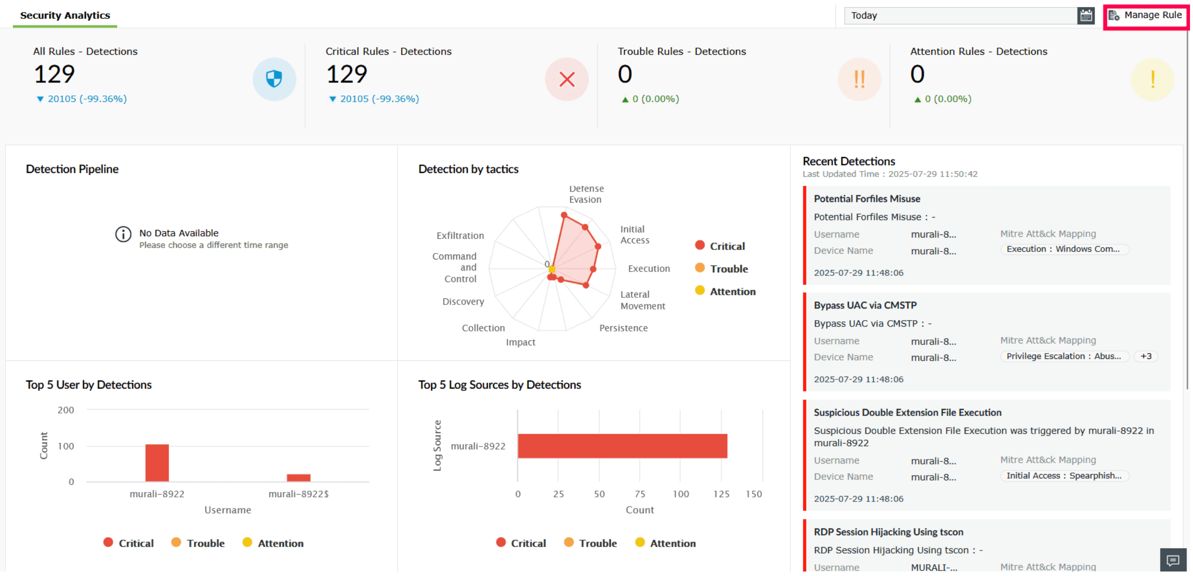
- Overview
- Steps to install Rules from the Rule Library

Overview

This page details how rules can be installed from the Rule Library. The rules can be installed automatically as ManageEngine develops and adds them to the cloud repository or can be browsed and installed manually. The below segment outlines the steps to install rules.

Steps to install Rules from the Rule Library

1. In your account, navigate to the Security tab to access the Security Analytics dashboard.
2. Click Manage Rule in the top-right corner.



Potential Forfiles Misuse
Potential Forfiles Misuse : -
Username murali-8... Mitre Att&ck Mapping
Device Name murali-8... Execution : Windows Com...
2025-07-29 11:48:06

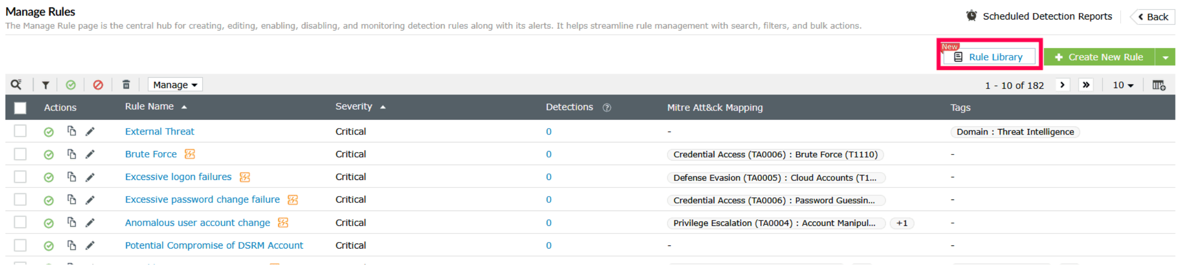
Bypass UAC via CMSTP
Bypass UAC via CMSTP : -
Username murali-8... Mitre Att&ck Mapping
Device Name murali-8... Privilege Escalation : Abus... +3
2025-07-29 11:48:06

Suspicious Double Extension File Execution
Suspicious Double Extension File Execution was triggered by murali-8922 in murali-8922
Username murali-8... Mitre Att&ck Mapping
Device Name murali-8... Initial Access : Spearphish...
2025-07-29 11:48:06

RDP Session Hijacking Using tscon
RDP Session Hijacking Using tscon : -
Username MURALI-... Mitre Att&ck Mapping

Figure 1: Navigating to the Rule Library

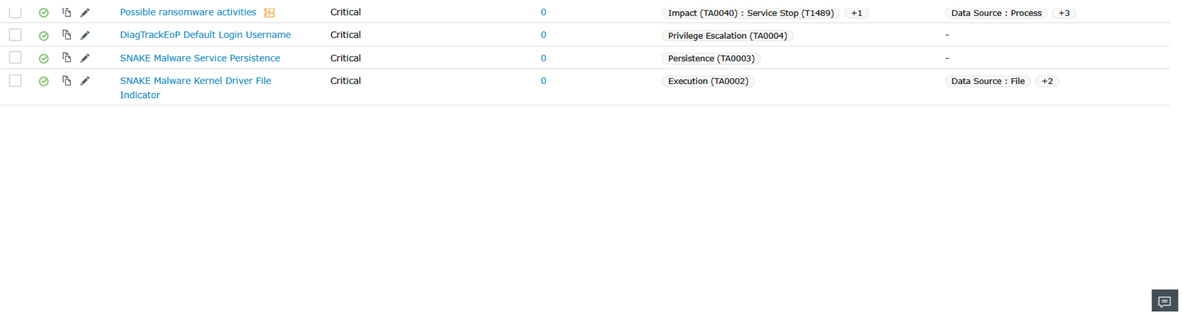
3. In the Manage Rules page, click Rule Library.



Manage Rules

The Manage Rule page is the central hub for creating, editing, enabling, disabling, and monitoring detection rules along with its alerts. It helps streamline rule management with search, filters, and bulk actions.

Actions	Rule Name	Severity	Detections	Mitre Att&ck Mapping	Tags
	External Threat	Critical	0	-	Domain : Threat Intelligence
	Brute Force	Critical	0	Credential Access (TA0006) : Brute Force (T1110)	-
	Excessive logon failures	Critical	0	Defense Evasion (TA0005) : Cloud Accounts (T1...	-
	Excessive password change failure	Critical	0	Credential Access (TA0006) : Password Guessin...	-
	Anomalous user account change	Critical	0	Privilege Escalation (TA0004) : Account Manipul... +1	-
	Potential Compromise of DSRM Account	Critical	0	-	-

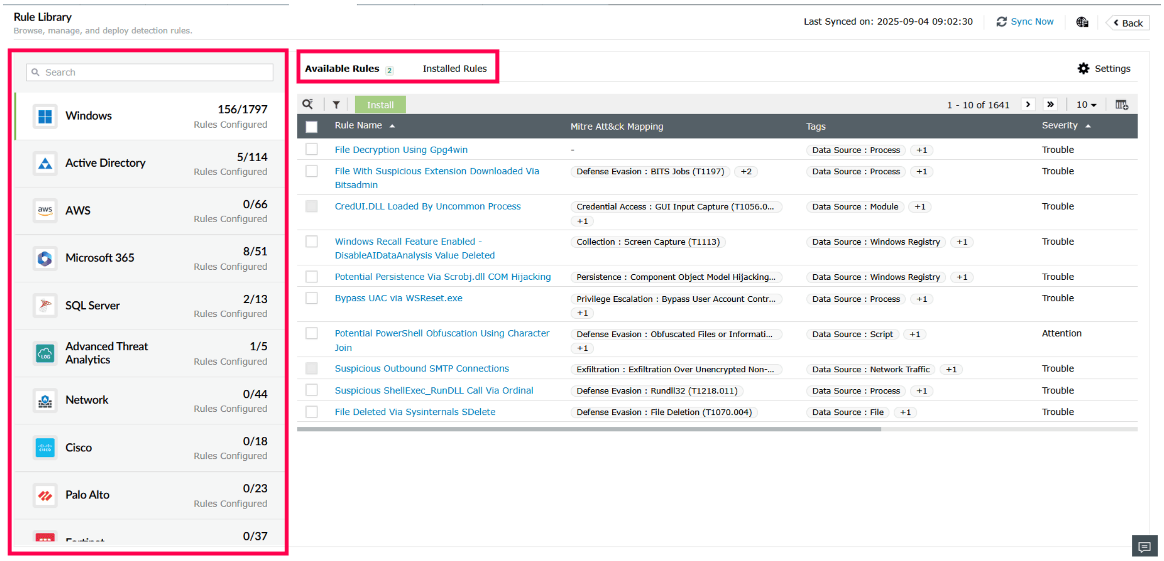


Possible ransomware activities	Critical	0	Impact (TA0040) : Service Stop (T1489) +1	Data Source : Process +3
DiagTrackEoP Default Login Username	Critical	0	Privilege Escalation (TA0004)	-
SNAKE Malware Service Persistence	Critical	0	Persistence (TA0003)	-
SNAKE Malware Kernel Driver File Indicator	Critical	0	Execution (TA0002)	Data Source : File +2

Figure 2: Navigating to the Rule Library

4. Select a category from the left panel to view its rules.

- Available Rules tab: Displays rules that are available in the central repository but not yet installed.
- Installed Rules tab: Displays already installed rules in your environment.



Rule Library
Browse, manage, and deploy detection rules.

Last Synced on: 2025-09-04 09:02:30

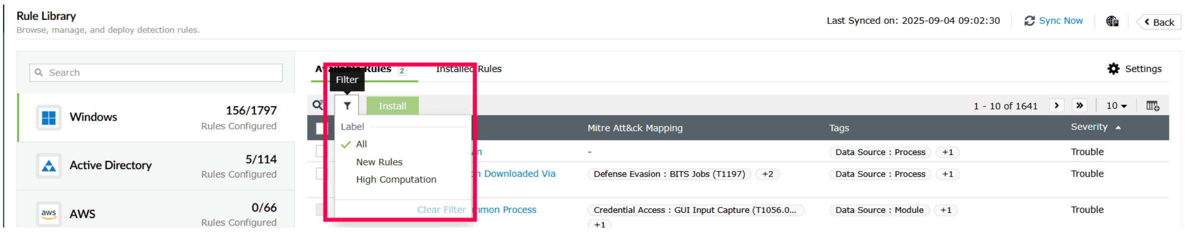
Category	Rules Configured
Windows	156/1797 Rules Configured
Active Directory	5/114 Rules Configured
AWS	0/66 Rules Configured
Microsoft 365	8/51 Rules Configured
SQL Server	2/13 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	0/44 Rules Configured
Cisco	0/18 Rules Configured
Palo Alto	0/23 Rules Configured
Fortinet	0/37

Rule Name	Mitre Att&ck Mapping	Tags	Severity
File Decryption Using Gpg4win	-	Data Source : Process +1	Trouble
File With Suspicious Extension Downloaded Via Bitsadmin	Defense Evasion : BITS Jobs (T1197) +2	Data Source : Process +1	Trouble
CredUI.DLL Loaded By Uncommon Process	Credential Access : GUI Input Capture (T1056.0... +1	Data Source : Module +1	Trouble
Windows Recall Feature Enabled - DisableAIDataAnalysis Value Deleted	Collection : Screen Capture (T1113)	Data Source : Windows Registry +1	Trouble
Potential Persistence Via Scrobj.dll COM Hijacking	Persistence : Component Object Model Hijacking...	Data Source : Windows Registry +1	Trouble
Bypass UAC via WSReset.exe	Privilege Escalation : Bypass User Account Contr... +1	Data Source : Process +1	Trouble
Potential PowerShell Obfuscation Using Character Join	Defense Evasion : Obfuscated Files or Informati... +1	Data Source : Script +1	Attention
Suspicious Outbound SMTP Connections	Exfiltration : Exfiltration Over Unencrypted Non-...	Data Source : Network Traffic +1	Trouble
Suspicious ShellExec_RunDLL Call Via Ordinal	Defense Evasion : Rundll32 (T1218.011)	Data Source : Process +1	Trouble
File Deleted Via Sysinternals SDelete	Defense Evasion : File Deletion (T1070.004)	Data Source : File +1	Trouble

Figure 3: Selecting Rule Library categories

5. In the Available Rules tab, click the ▼ icon to apply filters for rules. The filter works based on different criteria as outlined:

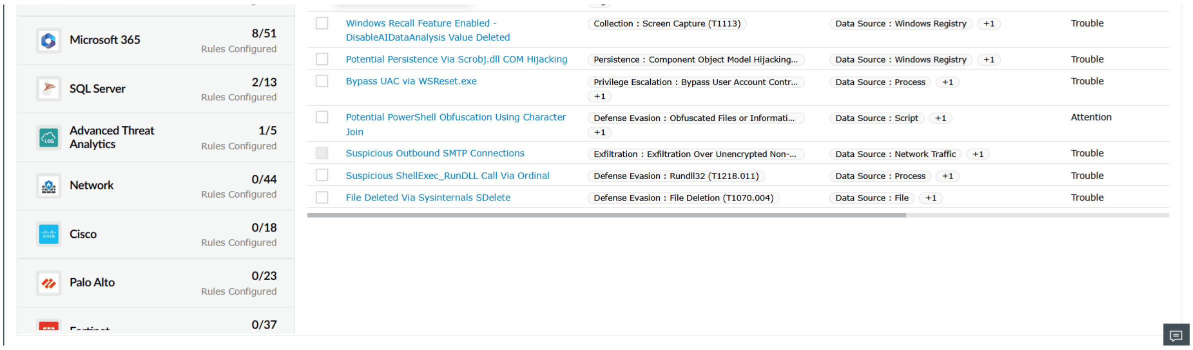
- All Rules: Displays all rules.
- New Rules: Recently added rules.
- High Computational: Resource-intensive rules, such as:
  - Threshold Logic: Triggers alerts only when an event crosses a defined limit.
  - Anomaly Models: Detects deviations from normal behavior patterns.
  - Multi-action Logic: Correlates two or more events



Rule Library
Browse, manage, and deploy detection rules.

Last Synced on: 2025-09-04 09:02:30

Sync Now
Back
Search
Windows 156/1797 Rules Configured
Active Directory 5/114 Rules Configured
AWS 0/66 Rules Configured
Available Rules 2
Installed Rules
Settings
Filter
Install
Label
✓ All
New Rules
High Computation
Clear Filter
1 - 10 of 1641
10
Mitre Att&ck Mapping
Tags
Severity
- Data Source : Process +1 Trouble
Downloaded Via Defense Evasion : BITS Jobs (T1197) +2 Data Source : Process +1 Trouble
mon Process Credential Access : GUI Input Capture (T1056.0... +1 Data Source : Module +1 Trouble

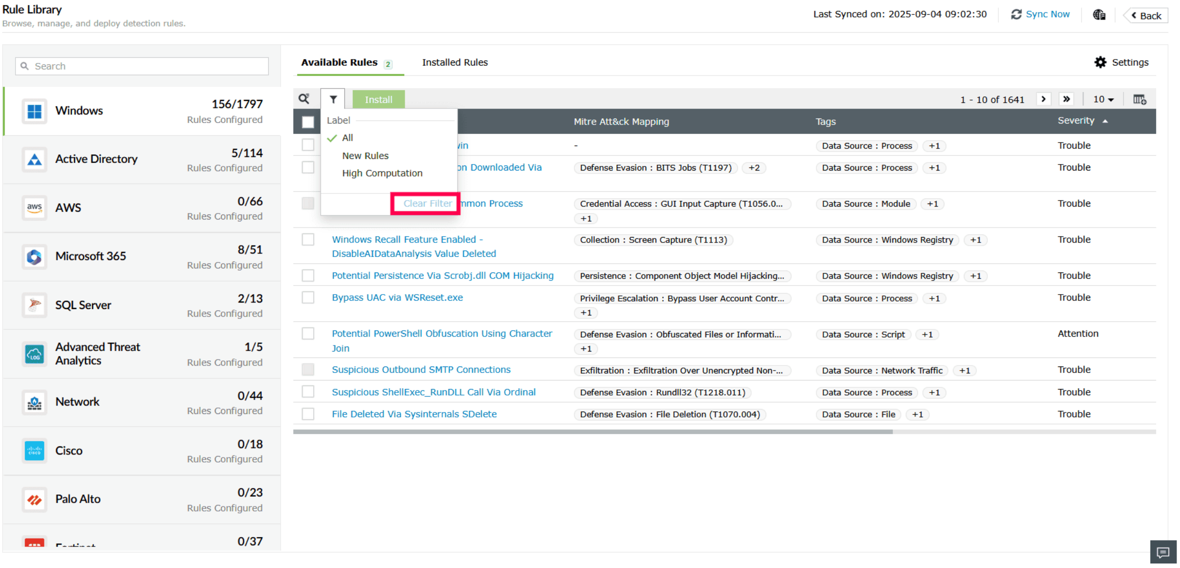


Microsoft 365	8/51 Rules Configured
SQL Server	2/13 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	0/44 Rules Configured
Cisco	0/18 Rules Configured
Palo Alto	0/23 Rules Configured
Fortinet	0/37

□	Windows Recall Feature Enabled - DisableAIDataAnalysis Value Deleted	Collection : Screen Capture (T1113)	Data Source : Windows Registry +1	Trouble
□	Potential Persistence Via Scrobj.dll COM Hijacking	Persistence : Component Object Model Hijacking...	Data Source : Windows Registry +1	Trouble
□	Bypass UAC via WSReset.exe	Privilege Escalation : Bypass User Account Contr... +1	Data Source : Process +1	Trouble
□	Potential PowerShell Obfuscation Using Character Join	Defense Evasion : Obfuscated Files or Informati... +1	Data Source : Script +1	Attention
□	Suspicious Outbound SMTP Connections	Exfiltration : Exfiltration Over Unencrypted Non-...	Data Source : Network Traffic +1	Trouble
□	Suspicious ShellExec_RunDLL Call Via Ordinal	Defense Evasion : Rundll32 (T1218.011)	Data Source : Process +1	Trouble
□	File Deleted Via Sysinternals SDelete	Defense Evasion : File Deletion (T1070.004)	Data Source : File +1	Trouble

Figure 4: Applying filters in the Available Rules tab

6. Click Clear Filters to remove all applied filters.



Rule Library

Browse, manage, and deploy detection rules.

Last Synced on: 2025-09-04 09:02:30 Sync Now Back

Available Rules 2 Installed Rules Settings

Search

Install 1 - 10 of 1641 10

Label

✓ All

New Rules

High Computation

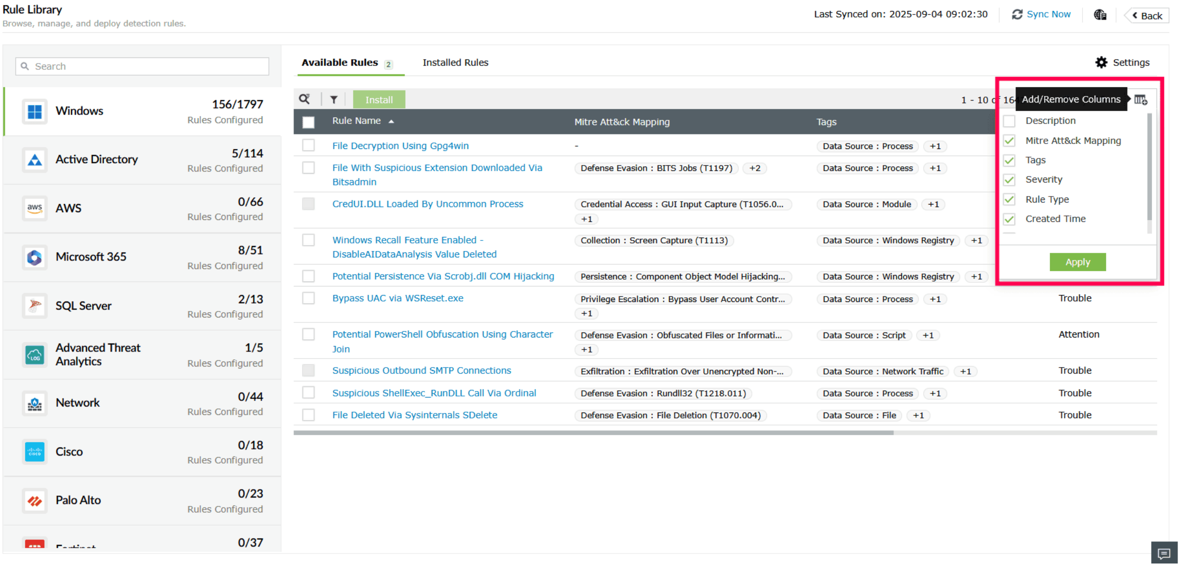
Clear Filter

Windows	156/1797 Rules Configured
Active Directory	5/114 Rules Configured
AWS	0/66 Rules Configured
Microsoft 365	8/51 Rules Configured
SQL Server	2/13 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	0/44 Rules Configured
Cisco	0/18 Rules Configured
Palo Alto	0/23 Rules Configured
Fortinet	0/37

□		Mitre Att&ck Mapping	Tags	Severity ▲
□	vin	-	Data Source : Process +1	Trouble
□	on Downloaded Via	Defense Evasion : BITS Jobs (T1197) +2	Data Source : Process +1	Trouble
□	mmon Process	Credential Access : GUI Input Capture (T1056.0... +1	Data Source : Module +1	Trouble
□	Windows Recall Feature Enabled - DisableAIDataAnalysis Value Deleted	Collection : Screen Capture (T1113)	Data Source : Windows Registry +1	Trouble
□	Potential Persistence Via Scrobj.dll COM Hijacking	Persistence : Component Object Model Hijacking...	Data Source : Windows Registry +1	Trouble
□	Bypass UAC via WSReset.exe	Privilege Escalation : Bypass User Account Contr... +1	Data Source : Process +1	Trouble
□	Potential PowerShell Obfuscation Using Character Join	Defense Evasion : Obfuscated Files or Informati... +1	Data Source : Script +1	Attention
□	Suspicious Outbound SMTP Connections	Exfiltration : Exfiltration Over Unencrypted Non-...	Data Source : Network Traffic +1	Trouble
□	Suspicious ShellExec_RunDLL Call Via Ordinal	Defense Evasion : Rundll32 (T1218.011)	Data Source : Process +1	Trouble
□	File Deleted Via Sysinternals SDelete	Defense Evasion : File Deletion (T1070.004)	Data Source : File +1	Trouble

Figure 5: Removing applied filters

7. Click the icon in the top-right corner to customize the rule table view. Select the checkbox next to the fields to add or remove them, and then click Apply.



Rule Library

Browse, manage, and deploy detection rules.

Last Synced on: 2025-09-04 09:02:30 Sync Now Back

Available Rules 2 Installed Rules Settings

Search

Install 1 - 10 of 164

Add/Remove Columns

□ Description

☑ Mitre Att&ck Mapping

☑ Tags

☑ Severity

☑ Rule Type

☑ Created Time

Apply

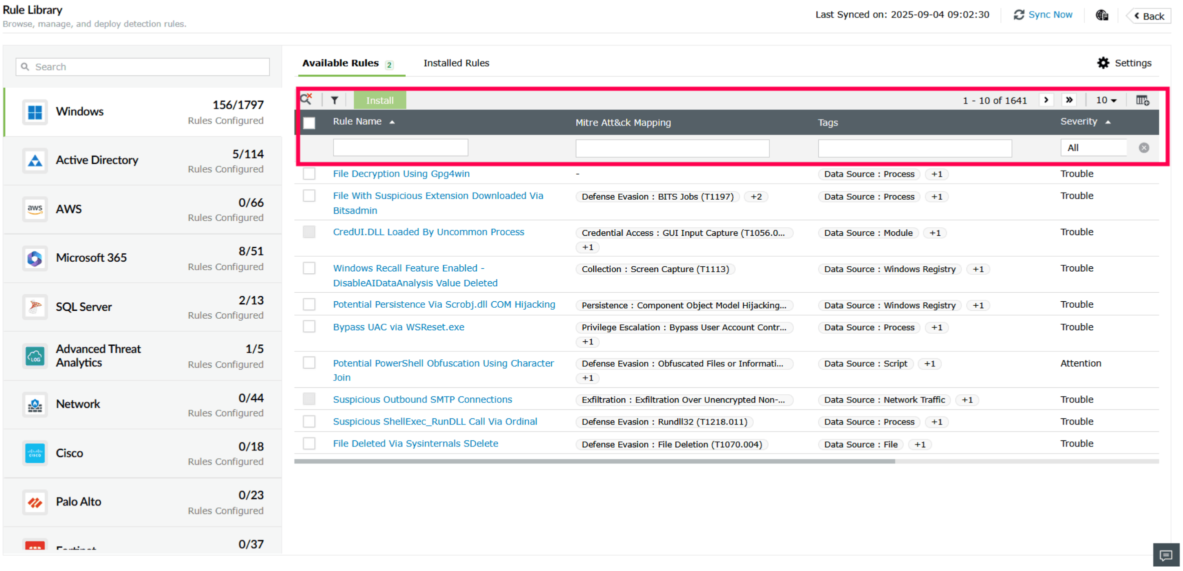
Windows	156/1797 Rules Configured
Active Directory	5/114 Rules Configured
AWS	0/66 Rules Configured
Microsoft 365	8/51 Rules Configured
SQL Server	2/13 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	0/44 Rules Configured
Cisco	0/18 Rules Configured
Palo Alto	0/23 Rules Configured
Fortinet	0/37

□	Rule Name ▲	Mitre Att&ck Mapping	Tags	
□	File Decryption Using Gpg4win	-	Data Source : Process +1	
□	File With Suspicious Extension Downloaded Via Bitsadmin	Defense Evasion : BITS Jobs (T1197) +2	Data Source : Process +1	
□	CredUI.DLL Loaded By Uncommon Process	Credential Access : GUI Input Capture (T1056.0... +1	Data Source : Module +1	
□	Windows Recall Feature Enabled - DisableAIDataAnalysis Value Deleted	Collection : Screen Capture (T1113)	Data Source : Windows Registry +1	
□	Potential Persistence Via Scrobj.dll COM Hijacking	Persistence : Component Object Model Hijacking...	Data Source : Windows Registry +1	
□	Bypass UAC via WSReset.exe	Privilege Escalation : Bypass User Account Contr... +1	Data Source : Process +1	Trouble
□	Potential PowerShell Obfuscation Using Character Join	Defense Evasion : Obfuscated Files or Informati... +1	Data Source : Script +1	Attention
□	Suspicious Outbound SMTP Connections	Exfiltration : Exfiltration Over Unencrypted Non-...	Data Source : Network Traffic +1	Trouble
□	Suspicious ShellExec_RunDLL Call Via Ordinal	Defense Evasion : Rundll32 (T1218.011)	Data Source : Process +1	Trouble
□	File Deleted Via Sysinternals SDelete	Defense Evasion : File Deletion (T1070.004)	Data Source : File +1	Trouble

Figure 6: Customizing columns in the Available Rules tab

8. Click the icon to access Advanced Search and locate rules by severity, rule type, MITRE tags, tags, or rule name.

9. To close the search, click the icon again.



Rule Library

Browse, manage, and deploy detection rules.

Last Synced on: 2025-09-04 09:02:30 | Sync Now | Back

Search

Windows	156/1797 Rules Configured
Active Directory	5/114 Rules Configured
AWS	0/66 Rules Configured
Microsoft 365	8/51 Rules Configured
SQL Server	2/13 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	0/44 Rules Configured
Cisco	0/18 Rules Configured
Palo Alto	0/23 Rules Configured
	0/37

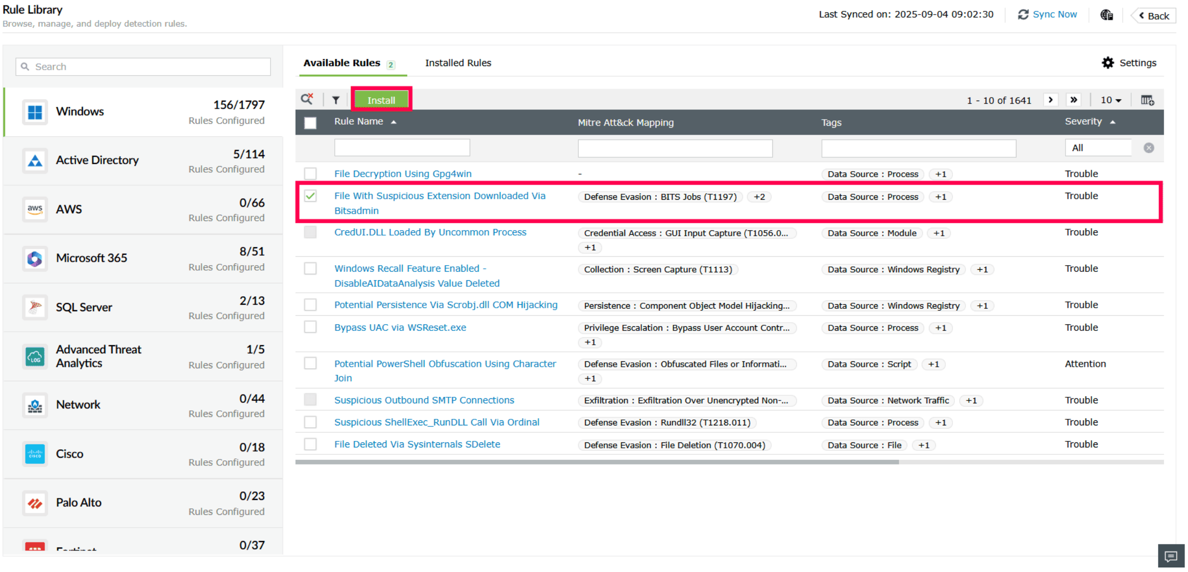
Available Rules 2 | Installed Rules | Settings

Install | 1 - 10 of 1641 | 10

□	Rule Name	Mitre Att&ck Mapping	Tags	Severity
				All
□	File Decryption Using Gpg4win	-	Data Source : Process +1	Trouble
□	File With Suspicious Extension Downloaded Via Bitsadmin	Defense Evasion : BITS Jobs (T1197) +2	Data Source : Process +1	Trouble
□	CredUI.DLL Loaded By Uncommon Process	Credential Access : GUI Input Capture (T1056.0... +1	Data Source : Module +1	Trouble
□	Windows Recall Feature Enabled - DisableAIDataAnalysis Value Deleted	Collection : Screen Capture (T1113)	Data Source : Windows Registry +1	Trouble
□	Potential Persistence Via Scrobj.dll COM Hijacking	Persistence : Component Object Model Hijacking...	Data Source : Windows Registry +1	Trouble
□	Bypass UAC via WSReset.exe	Privilege Escalation : Bypass User Account Contr... +1	Data Source : Process +1	Trouble
□	Potential PowerShell Obfuscation Using Character Join	Defense Evasion : Obfuscated Files or Informati... +1	Data Source : Script +1	Attention
□	Suspicious Outbound SMTP Connections	Exfiltration : Exfiltration Over Unencrypted Non-...	Data Source : Network Traffic +1	Trouble
□	Suspicious ShellExec_RunDLL Call Via Ordinal	Defense Evasion : Rundll32 (T1218.011)	Data Source : Process +1	Trouble
□	File Deleted Via Sysinternals SDelete	Defense Evasion : File Deletion (T1070.004)	Data Source : File +1	Trouble

Figure 7: Using Advanced Search

10. Select the checkbox next to the rules you want to install from the Available Rules tab, then click Install.



Rule Library

Browse, manage, and deploy detection rules.

Last Synced on: 2025-09-04 09:02:30 | Sync Now | Back

Search

Windows	156/1797 Rules Configured
Active Directory	5/114 Rules Configured
AWS	0/66 Rules Configured
Microsoft 365	8/51 Rules Configured
SQL Server	2/13 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	0/44 Rules Configured
Cisco	0/18 Rules Configured
Palo Alto	0/23 Rules Configured
	0/37

Available Rules 2 | Installed Rules | Settings

Install | 1 - 10 of 1641 | 10

□	Rule Name	Mitre Att&ck Mapping	Tags	Severity
				All
□	File Decryption Using Gpg4win	-	Data Source : Process +1	Trouble
☑	File With Suspicious Extension Downloaded Via Bitsadmin	Defense Evasion : BITS Jobs (T1197) +2	Data Source : Process +1	Trouble
□	CredUI.DLL Loaded By Uncommon Process	Credential Access : GUI Input Capture (T1056.0... +1	Data Source : Module +1	Trouble
□	Windows Recall Feature Enabled - DisableAIDataAnalysis Value Deleted	Collection : Screen Capture (T1113)	Data Source : Windows Registry +1	Trouble
□	Potential Persistence Via Scrobj.dll COM Hijacking	Persistence : Component Object Model Hijacking...	Data Source : Windows Registry +1	Trouble
□	Bypass UAC via WSReset.exe	Privilege Escalation : Bypass User Account Contr... +1	Data Source : Process +1	Trouble
□	Potential PowerShell Obfuscation Using Character Join	Defense Evasion : Obfuscated Files or Informati... +1	Data Source : Script +1	Attention
□	Suspicious Outbound SMTP Connections	Exfiltration : Exfiltration Over Unencrypted Non-...	Data Source : Network Traffic +1	Trouble
□	Suspicious ShellExec_RunDLL Call Via Ordinal	Defense Evasion : Rundll32 (T1218.011)	Data Source : Process +1	Trouble
□	File Deleted Via Sysinternals SDelete	Defense Evasion : File Deletion (T1070.004)	Data Source : File +1	Trouble

Figure 8: Installing rules from the Available Rules tab

NOTE

You can install multiple rules at once. Some rules require additional configuration during installation.

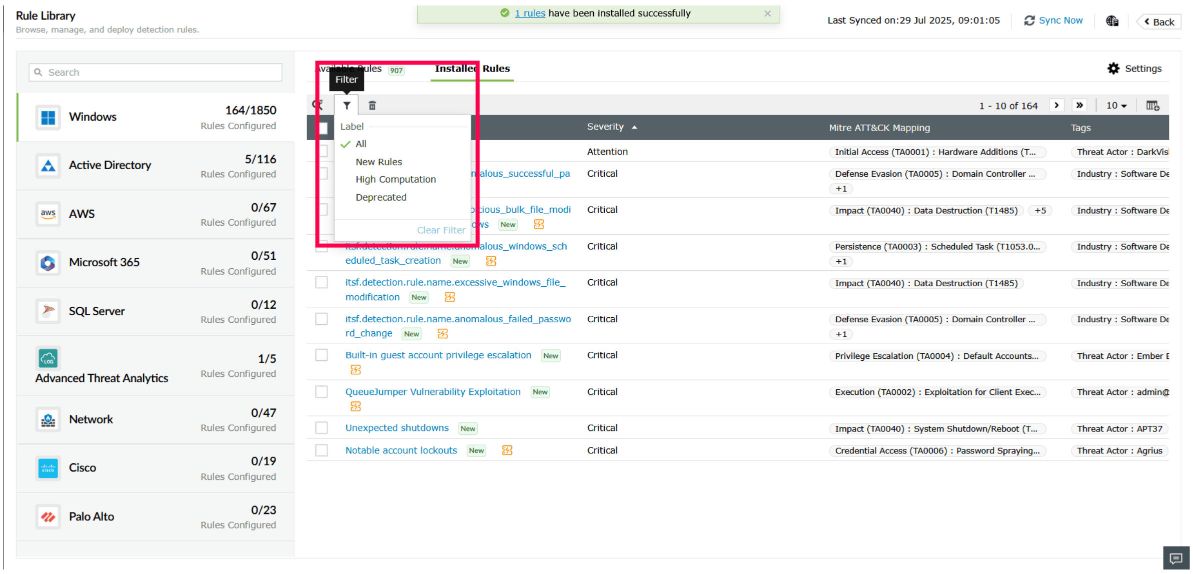
- If you install such a rule individually, a popup will prompt you to either complete the additional configuration and install the rule, or skip it and have the rule installed in a disabled state.

- If the same rule is installed as part of a bulk installation, it will be assumed that you chose to skip

the configuration, and the rule will be installed in a disabled state.
You can enable these rules later from the Manage Rule page after completing the necessary configurations.

11. In the Installed Rules tab, select the ▼ icon to apply the filters for rules, such as New Rules, High Computational, and Deprecated rules.

> NOTE
>
> Deprecated rules are rules that we no longer recommend for installation as they have been replaced, improved, or consolidated. If you have installed these rules, then they appear only in the Installed Rules tab.



Rule Library
Browse, manage, and deploy detection rules.

✓ 1 rules have been installed successfully ×

Last Synced on:29 Jul 2025, 09:01:05 | Sync Now | Back

Windows	164/1850 Rules Configured
Active Directory	5/116 Rules Configured
AWS	0/67 Rules Configured
Microsoft 365	0/51 Rules Configured
SQL Server	0/12 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	0/47 Rules Configured
Cisco	0/19 Rules Configured
Palo Alto	0/23 Rules Configured

Available Rules 907 | Installed Rules | Settings

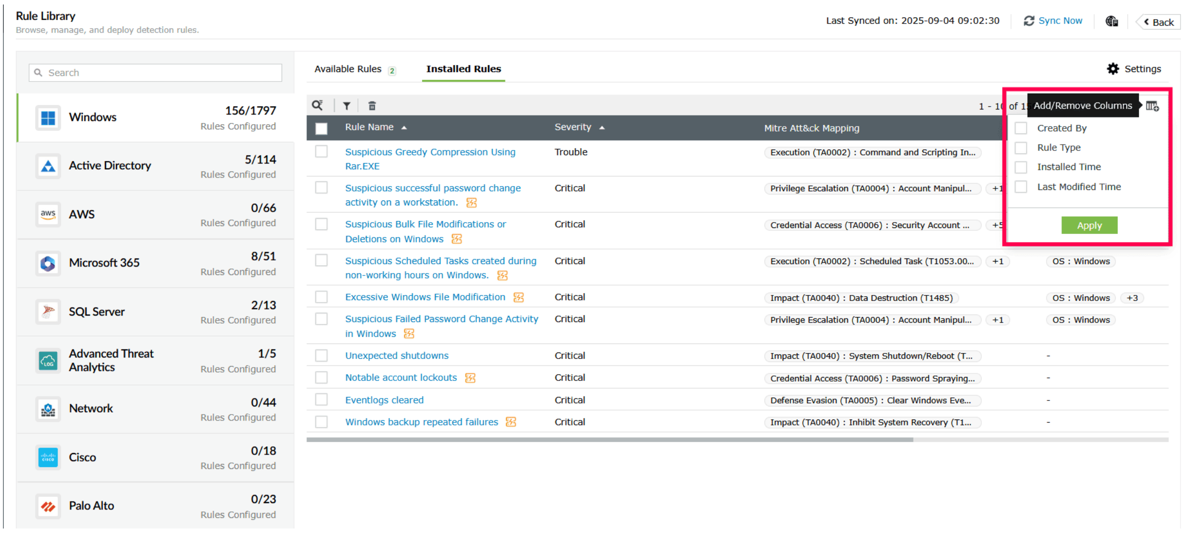
Filter
Label
✓ All
New Rules
High Computation
Deprecated
Clear Filter

1 - 10 of 164 | 10

	Severity	Mitre ATT&CK Mapping	Tags
	Attention	Initial Access (TA0001) : Hardware Additions (T...	Threat Actor : DarkVis
...alous_successful_pa	Critical	Defense Evasion (TA0005) : Domain Controller ... +1	Industry : Software De
...cious_bulk_file_modi ...ws New	Critical	Impact (TA0040) : Data Destruction (T1485) +5	Industry : Software De
itsf.detection.rule.name.anomalous_windows_scheduled_task_creation New	Critical	Persistence (TA0003) : Scheduled Task (T1053.0... +1	Industry : Software De
itsf.detection.rule.name.excessive_windows_file_modification New	Critical	Impact (TA0040) : Data Destruction (T1485)	Industry : Software De
itsf.detection.rule.name.anomalous_failed_password_change New	Critical	Defense Evasion (TA0005) : Domain Controller ... +1	Industry : Software De
Built-in guest account privilege escalation New	Critical	Privilege Escalation (TA0004) : Default Accounts...	Threat Actor : Ember E
QueueJumper Vulnerability Exploitation New	Critical	Execution (TA0002) : Exploitation for Client Exec...	Threat Actor : admin@
Unexpected shutdowns New	Critical	Impact (TA0040) : System Shutdown/Reboot (T...	Threat Actor : APT37
Notable account lockouts New	Critical	Credential Access (TA0006) : Password Spraying...	Threat Actor : Agrius

Figure 9: Applying filters in the Installed Rules tab

12. Click the icon to customize the table view. Select the checkboxes next to the fields you want to display, such as Created By, Installed Time, Last Updated Time, and then click Apply.



Rule Library
Browse, manage, and deploy detection rules.

Last Synced on: 2025-09-04 09:02:30 | Sync Now | Back

Windows	156/1797 Rules Configured
Active Directory	5/114 Rules Configured
AWS	0/66 Rules Configured
Microsoft 365	8/51 Rules Configured
SQL Server	2/13 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	0/44 Rules Configured
Cisco	0/18 Rules Configured
Palo Alto	0/23 Rules Configured

Available Rules 2 | Installed Rules | Settings

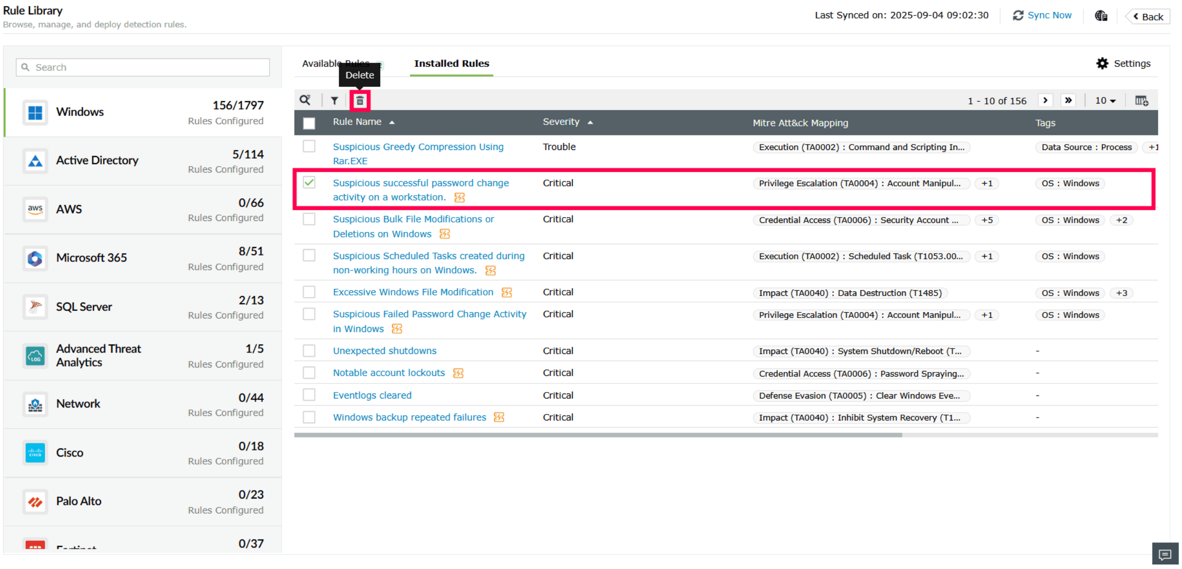
Add/Remove Columns
□ Created By
□ Rule Type
□ Installed Time
□ Last Modified Time
Apply

Rule Name	Severity	Mitre Att&ck Mapping	
Suspicious Greedy Compression Using Rar.EXE	Trouble	Execution (TA0002) : Command and Scripting In...	
Suspicious successful password change activity on a workstation.	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	
Suspicious Bulk File Modifications or Deletions on Windows	Critical	Credential Access (TA0006) : Security Account ... +5	
Suspicious Scheduled Tasks created during non-working hours on Windows.	Critical	Execution (TA0002) : Scheduled Task (T1053.00... +1	OS : Windows
Excessive Windows File Modification	Critical	Impact (TA0040) : Data Destruction (T1485)	OS : Windows +3
Suspicious Failed Password Change Activity in Windows	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows
Unexpected shutdowns	Critical	Impact (TA0040) : System Shutdown/Reboot (T...	-
Notable account lockouts	Critical	Credential Access (TA0006) : Password Spraying...	-
Eventlogs cleared	Critical	Defense Evasion (TA0005) : Clear Windows Eve...	-
Windows backup repeated failures	Critical	Impact (TA0040) : Inhibit System Recovery (T1...	-

Fortinet	0/37

Figure 10: Customizing columns in the Installed Rules tab

13. Select the checkboxes next to the rules you want to delete and click the 🗑 icon.



Rule Library
Browse, manage, and deploy detection rules.

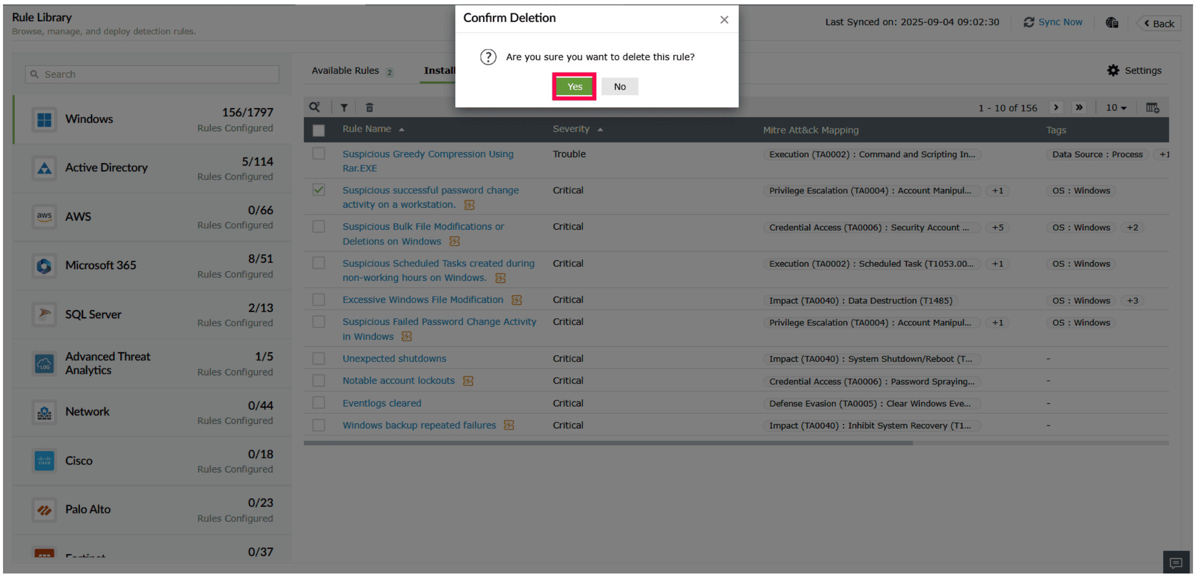
Last Synced on: 2025-09-04 09:02:30 | Sync Now | Back

Windows	156/1797	Rules Configured
Active Directory	5/114	Rules Configured
AWS	0/66	Rules Configured
Microsoft 365	8/51	Rules Configured
SQL Server	2/13	Rules Configured
Advanced Threat Analytics	1/5	Rules Configured
Network	0/44	Rules Configured
Cisco	0/18	Rules Configured
Palo Alto	0/23	Rules Configured
Fortinet	0/37	

□	Rule Name	Severity	Mitre Att&ck Mapping	Tags
□	Suspicious Greedy Compression Using Rar.EXE	Trouble	Execution (TA0002) : Command and Scripting In...	Data Source : Process +1
☑	Suspicious successful password change activity on a workstation.	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows
□	Suspicious Bulk File Modifications or Deletions on Windows	Critical	Credential Access (TA0006) : Security Account ... +5	OS : Windows +2
□	Suspicious Scheduled Tasks created during non-working hours on Windows.	Critical	Execution (TA0002) : Scheduled Task (T1053.00... +1	OS : Windows
□	Excessive Windows File Modification	Critical	Impact (TA0040) : Data Destruction (T1485)	OS : Windows +3
□	Suspicious Failed Password Change Activity in Windows	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows
□	Unexpected shutdowns	Critical	Impact (TA0040) : System Shutdown/Reboot (T...	-
□	Notable account lockouts	Critical	Credential Access (TA0006) : Password Spraying...	-
□	Eventlogs cleared	Critical	Defense Evasion (TA0005) : Clear Windows Eve...	-
□	Windows backup repeated failures	Critical	Impact (TA0040) : Inhibit System Recovery (T1...	-

Figure 11: Deleting rules from the Installed Rules tab

14. In the pop-up that appears, click Yes to confirm the deletion.



Confirm Deletion

Are you sure you want to delete this rule?

Rule Library
Browse, manage, and deploy detection rules.

Last Synced on: 2025-09-04 09:02:30 | Sync Now | Back

Windows	156/1797	Rules Configured
Active Directory	5/114	Rules Configured
AWS	0/66	Rules Configured
Microsoft 365	8/51	Rules Configured
SQL Server	2/13	Rules Configured
Advanced Threat Analytics	1/5	Rules Configured
Network	0/44	Rules Configured
Cisco	0/18	Rules Configured
Palo Alto	0/23	Rules Configured
Fortinet	0/37	

□	Rule Name	Severity	Mitre Att&ck Mapping	Tags
□	Suspicious Greedy Compression Using Rar.EXE	Trouble	Execution (TA0002) : Command and Scripting In...	Data Source : Process +1
☑	Suspicious successful password change activity on a workstation.	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows
□	Suspicious Bulk File Modifications or Deletions on Windows	Critical	Credential Access (TA0006) : Security Account ... +5	OS : Windows +2
□	Suspicious Scheduled Tasks created during non-working hours on Windows.	Critical	Execution (TA0002) : Scheduled Task (T1053.00... +1	OS : Windows
□	Excessive Windows File Modification	Critical	Impact (TA0040) : Data Destruction (T1485)	OS : Windows +3
□	Suspicious Failed Password Change Activity in Windows	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows
□	Unexpected shutdowns	Critical	Impact (TA0040) : System Shutdown/Reboot (T...	-
□	Notable account lockouts	Critical	Credential Access (TA0006) : Password Spraying...	-
□	Eventlogs cleared	Critical	Defense Evasion (TA0005) : Clear Windows Eve...	-
□	Windows backup repeated failures	Critical	Impact (TA0040) : Inhibit System Recovery (T1...	-

Figure 12: Deleting rules from the Installed Rules tab

Read also

This page detailed the steps to install rules from the Rule Library. To configure auto-install and rule update settings, refer to the following articles:

- Configuring auto-install settings
- Configuring Rule Update Settings

4.1.4.3. Configuring auto-install settings

Last updated on: September 12, 2025

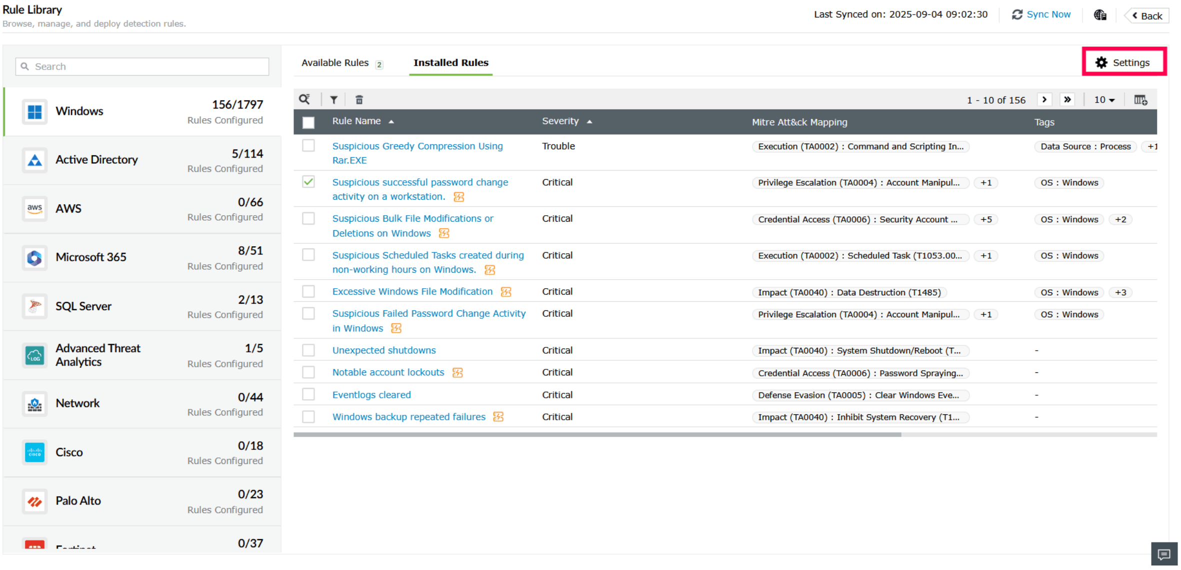
In this page

Overview

This page explains how to configure auto-install settings for rules in the Rule Library. This capability enables the automatic installation of rules based on their severity level.

Steps to configure auto-install settings

1. In the Rule Library page, navigate to Settings.

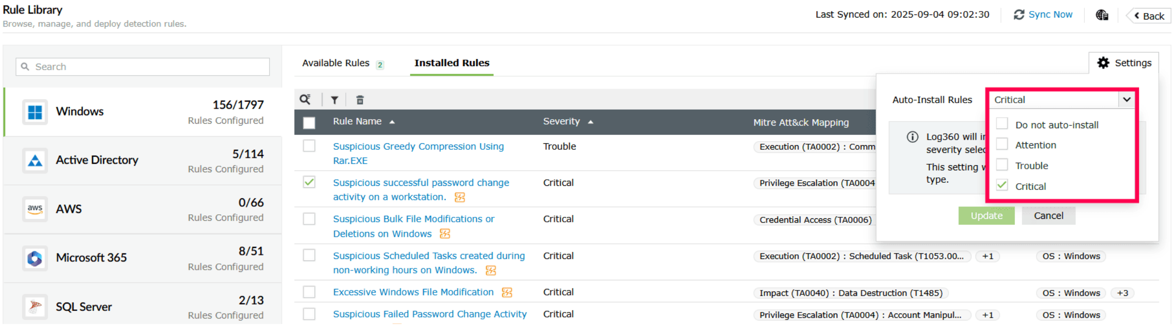


Rule Library
Browse, manage, and deploy detection rules.
Last Synced on: 2025-09-04 09:02:30
Sync Now
Back
Search
Windows 156/1797 Rules Configured
Active Directory 5/114 Rules Configured
AWS 0/66 Rules Configured
Microsoft 365 8/51 Rules Configured
SQL Server 2/13 Rules Configured
Advanced Threat Analytics 1/5 Rules Configured
Network 0/44 Rules Configured
Cisco 0/18 Rules Configured
Palo Alto 0/23 Rules Configured
Fortinet 0/37
Available Rules 2
Installed Rules
Settings
1 - 10 of 156
10

	Rule Name	Severity	Mitre Att&ck Mapping	Tags
□	Suspicious Greedy Compression Using Rar.EXE	Trouble	Execution (TA0002) : Command and Scripting In...	Data Source : Process +1
☑	Suspicious successful password change activity on a workstation.	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows
□	Suspicious Bulk File Modifications or Deletions on Windows	Critical	Credential Access (TA0006) : Security Account ... +5	OS : Windows +2
□	Suspicious Scheduled Tasks created during non-working hours on Windows.	Critical	Execution (TA0002) : Scheduled Task (T1053.00... +1	OS : Windows
□	Excessive Windows File Modification	Critical	Impact (TA0040) : Data Destruction (T1485)	OS : Windows +3
□	Suspicious Failed Password Change Activity in Windows	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows
□	Unexpected shutdowns	Critical	Impact (TA0040) : System Shutdown/Reboot (T...	-
□	Notable account lockouts	Critical	Credential Access (TA0006) : Password Spraying...	-
□	Eventlogs cleared	Critical	Defense Evasion (TA0005) : Clear Windows Eve...	-
□	Windows backup repeated failures	Critical	Impact (TA0040) : Inhibit System Recovery (T1...	-

Figure 1: Configuring auto-install settings

2. From the Auto-Install Rules dropdown, select the severity levels for which rules should be automatically installed, such as Critical, Trouble, or Attention.

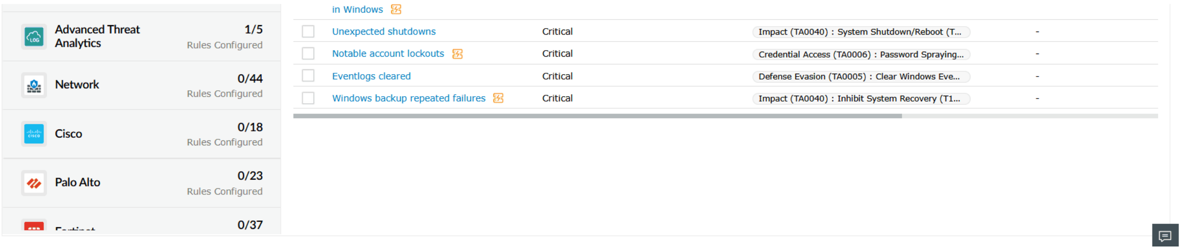


Rule Library
Browse, manage, and deploy detection rules.
Last Synced on: 2025-09-04 09:02:30
Sync Now
Back
Search
Windows 156/1797 Rules Configured
Active Directory 5/114 Rules Configured
AWS 0/66 Rules Configured
Microsoft 365 8/51 Rules Configured
SQL Server 2/13 Rules Configured
Available Rules 2
Installed Rules
Settings
Update
Cancel

Auto-Install Rules: Critical

□ Do not auto-install
□ Attention
□ Trouble
☑ Critical

Log360 will i severity selec
This setting w type.



Advanced Threat Analytics 1/5 Rules Configured

Network 0/44 Rules Configured

Cisco 0/18 Rules Configured

Palo Alto 0/23 Rules Configured

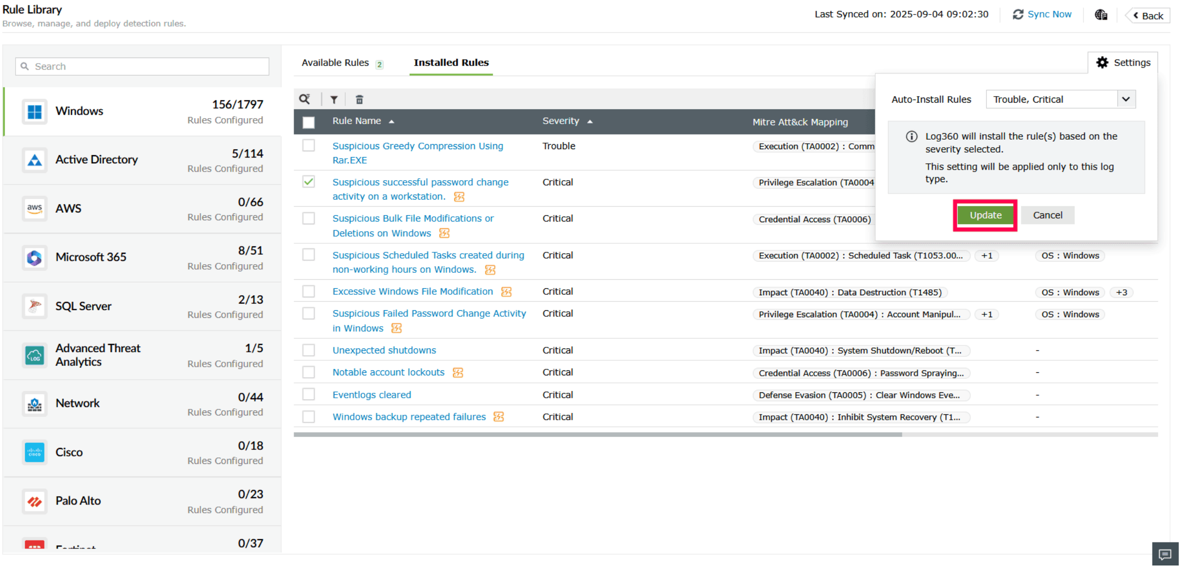
Fortinet 0/37

	in Windows			
□	Unexpected shutdowns	Critical	Impact (TA0040) : System Shutdown/Reboot (T...	-
□	Notable account lockouts	Critical	Credential Access (TA0006) : Password Spraying...	-
□	Eventlogs cleared	Critical	Defense Evasion (TA0005) : Clear Windows Eve...	-
□	Windows backup repeated failures	Critical	Impact (TA0040) : Inhibit System Recovery (T1...	-

Figure 2: Configuring Auto-Install Rules

3. To disable auto-install, select Do not auto-install.

4. Click Update to save your changes.



Rule Library

Browse, manage, and deploy detection rules.

Last Synced on: 2025-09-04 09:02:30 | Sync Now | Back

Search

Windows 156/1797 Rules Configured

Active Directory 5/114 Rules Configured

AWS 0/66 Rules Configured

Microsoft 365 8/51 Rules Configured

SQL Server 2/13 Rules Configured

Advanced Threat Analytics 1/5 Rules Configured

Network 0/44 Rules Configured

Cisco 0/18 Rules Configured

Palo Alto 0/23 Rules Configured

Fortinet 0/37

Available Rules 2 | Installed Rules | Settings

□	Rule Name ▲	Severity ▲	Mitre Att&ck Mapping	
□	Suspicious Greedy Compression Using Rar.EXE	Trouble	Execution (TA0002) : Comm	
☑	Suspicious successful password change activity on a workstation.	Critical	Privilege Escalation (TA0004	
□	Suspicious Bulk File Modifications or Deletions on Windows	Critical	Credential Access (TA0006)	
□	Suspicious Scheduled Tasks created during non-working hours on Windows.	Critical	Execution (TA0002) : Scheduled Task (T1053.00... +1	OS : Windows
□	Excessive Windows File Modification	Critical	Impact (TA0040) : Data Destruction (T1485)	OS : Windows +3
□	Suspicious Failed Password Change Activity in Windows	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows
□	Unexpected shutdowns	Critical	Impact (TA0040) : System Shutdown/Reboot (T...	-
□	Notable account lockouts	Critical	Credential Access (TA0006) : Password Spraying...	-
□	Eventlogs cleared	Critical	Defense Evasion (TA0005) : Clear Windows Eve...	-
□	Windows backup repeated failures	Critical	Impact (TA0040) : Inhibit System Recovery (T1...	-

Auto-Install Rules: Trouble, Critical

Log360 will install the rule(s) based on the severity selected.

This setting will be applied only to this log type.

Update | Cancel

Figure 3: Configuring Auto-Install Rules

NOTE

Rules that are highly computational will be installed in a disabled state by default.

5. Auto-install settings are applied per Rule Library category, so configure them individually for each category as needed.

6. Rules installed through auto-install are activated automatically, but you must manually enable any associated alert profiles if required.

NOTE

Severity of the pre-defined rules is provided by ManageEngine Log360 team at the time of creation.

Read also

This page explained how to enable automatic installation of rules based on severity levels. To learn how to manage and configure these rules in your environment, refer to:

- Configuring Rule Update Settings
- Installing Rules

4.1.4.4. Configuring Rule Update Settings

Last updated on: September 12, 2025

In this page

Overview

Rule Update Settings ensure that your system consistently receives the latest rule updates from Security Intelligence Pack, our cloud repository, enabling accurate and reliable threat detection. For environments with internet connectivity, you can configure automatic synchronization or perform manual updates from the cloud server. For offline or air-gapped environments, rule updates can be applied by downloading the latest Rule Library package and configuring the system to use it locally.

Pre-requisites

Before configuring Rule Update Settings, ensure the following:

- Whitelist the domain static.zohocdn.com in your firewall or network security settings to avoid any connection blocks.
- The user creating scheduled tasks must have the necessary permissions to:
    - Access the script file.
    - Access the directory specified by the -targetDir parameter.
- The user creating the cron job must have:
    - Read and execute permissions for the script file.
    - Write access to any directories the script interacts with, such as log or download folders.
- Ensure curl is installed and accessible for the user running the cron job, as it is required to download the ZIP files.

Steps to configure Rule Update Settings for:

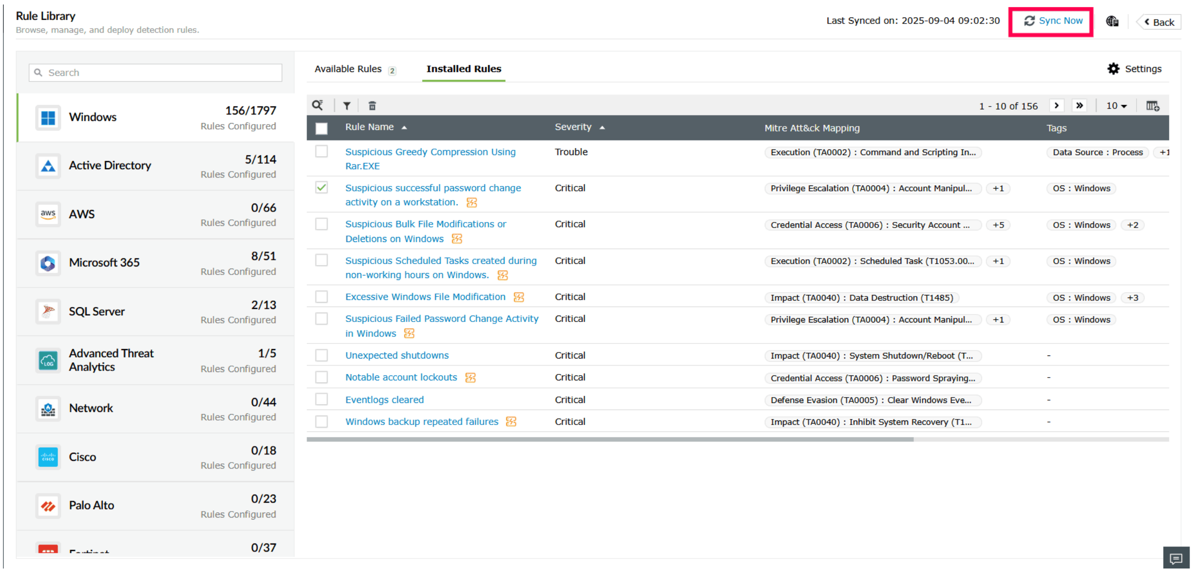
Environments connected to the internet

1. Navigate to the Rule Library page.

2. In the top-right corner, click the icon and select static.zohocdn.com from the drop-down.

3. Click Save to apply the changes.

4. Click Sync Now to fetch the latest rules immediately.



Rule Library
Browse, manage, and deploy detection rules.

Last Synced on: 2025-09-04 09:02:30

Windows	156/1797 Rules Configured
Active Directory	5/114 Rules Configured
AWS	0/66 Rules Configured
Microsoft 365	8/51 Rules Configured
SQL Server	2/13 Rules Configured
Advanced Threat Analytics	1/5 Rules Configured
Network	0/44 Rules Configured
Cisco	0/18 Rules Configured
Palo Alto	0/23 Rules Configured
	0/37

	Rule Name	Severity	Mitre Att&ck Mapping	Tags
□	Suspicious Greedy Compression Using Rar.EXE	Trouble	Execution (TA0002) : Command and Scripting In...	Data Source : Process +1
☑	Suspicious successful password change activity on a workstation.	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows
□	Suspicious Bulk File Modifications or Deletions on Windows	Critical	Credential Access (TA0006) : Security Account ... +5	OS : Windows +2
□	Suspicious Scheduled Tasks created during non-working hours on Windows.	Critical	Execution (TA0002) : Scheduled Task (T1053.00... +1	OS : Windows
□	Excessive Windows File Modification	Critical	Impact (TA0040) : Data Destruction (T1485)	OS : Windows +3
□	Suspicious Failed Password Change Activity in Windows	Critical	Privilege Escalation (TA0004) : Account Manipul... +1	OS : Windows
□	Unexpected shutdowns	Critical	Impact (TA0040) : System Shutdown/Reboot (T...	-
□	Notable account lockouts	Critical	Credential Access (TA0006) : Password Spraying...	-
□	Eventlogs cleared	Critical	Defense Evasion (TA0005) : Clear Windows Eve...	-
□	Windows backup repeated failures	Critical	Impact (TA0040) : Inhibit System Recovery (T1...	-

Figure 1: Syncing the Rule Library

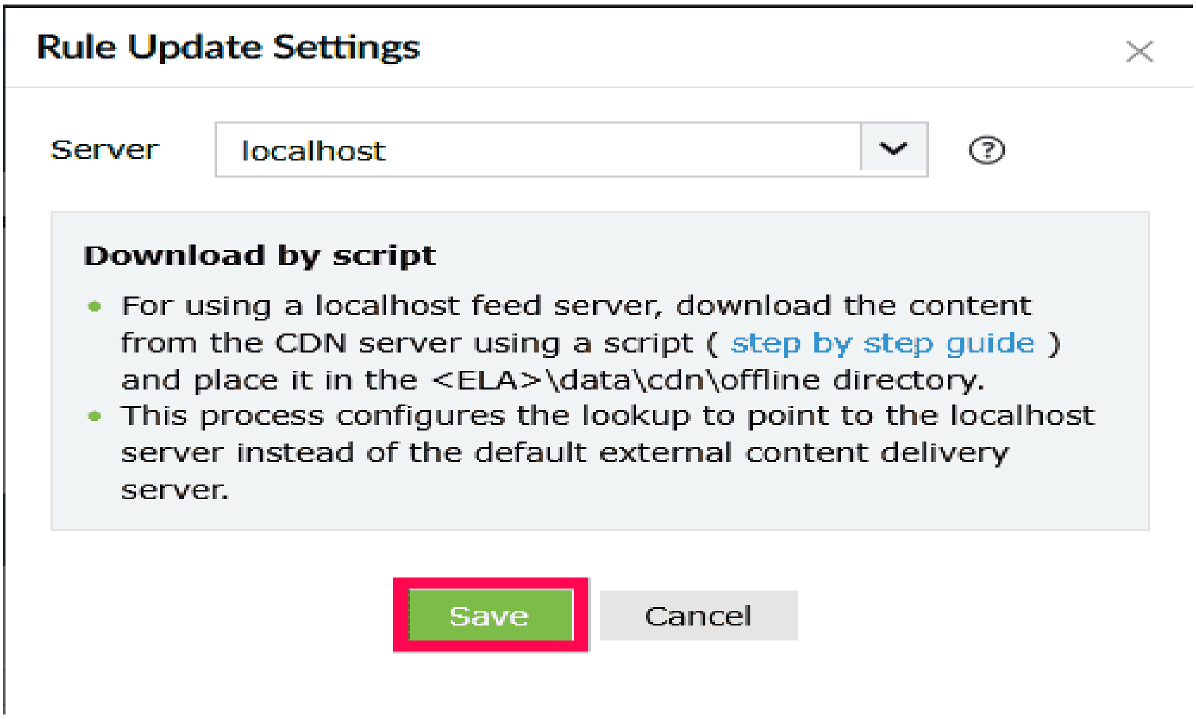
5. A scheduled synchronization job also runs every 6 hours to update rules automatically.

Offline or air-gapped environments

1. Go to the Rule Library page.

2. In the top-right corner, select the icon and select Localhost from the drop-down.

3. Click Save to apply the changes.



Rule Update Settings

Server: localhost

Download by script

- For using a localhost feed server, download the content from the CDN server using a script (step by step guide) and place it in the <ELA>\data\cdn\offline directory.
- This process configures the lookup to point to the localhost server instead of the default external content delivery server.

Figure 2: Configuring Rule Update Settings

4. Download the latest Rule Library ZIP file.
5. Place the downloaded log360library.lpm file in the following folder on the server: {server.home}\data\cdn\offline
6. The system extracts and applies the updated rules automatically.
7. If auto-install is enabled, rules matching the configured severity levels will be installed after syncing.

Downloading Rule Library ZIP files

1. Download the latest Rule Library file using the provided script:

> ⓘ NOTE
>
> The following scripts are located in the path <Installed Dir>\Log360\tools\

- Windows: download-log360library.bat
- Linux: download-log360library.sh

2. Run script file to download the latest log360Library ZIP file.

3. To automate the download process, you can schedule the script to run at regular intervals using:

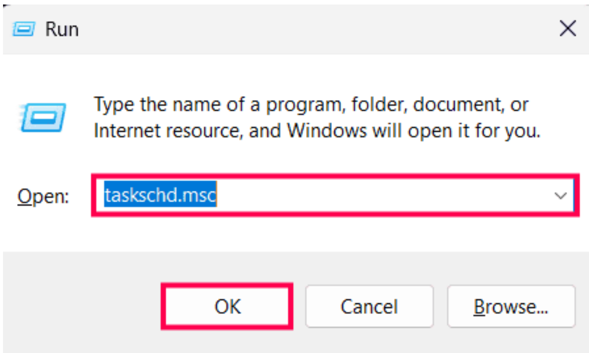
   - Task Scheduler on Windows

   - Cron Job on Linux

Steps to schedule a PowerShell script every 6 hours in Task Scheduler

1. Press Win + R to open the Run dialog box.

2. Type taskschd.msc, and click OK.

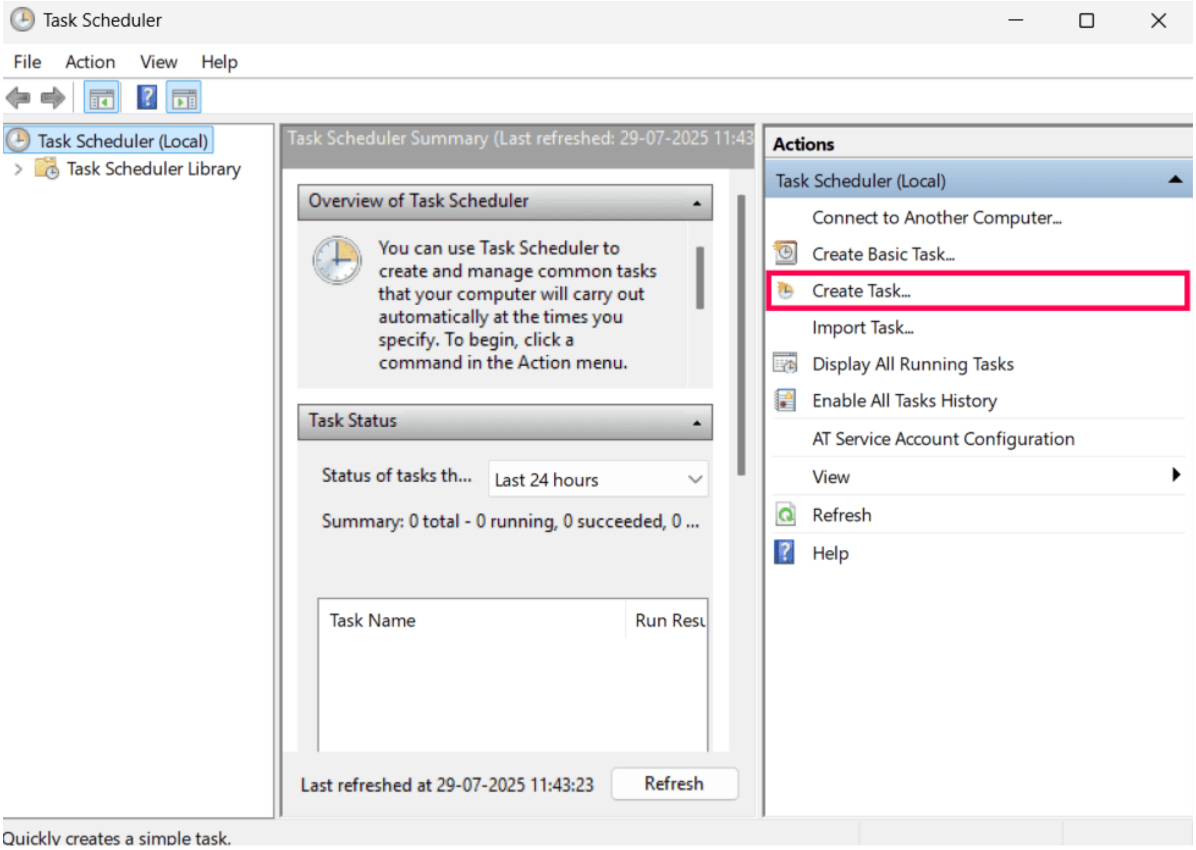


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: taskschd.msc

Figure 3: Opening the Task Scheduler

3. Click Create Task.



Task Scheduler Summary (Last refreshed: 29-07-2025 11:43

You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Status of tasks th... Last 24 hours

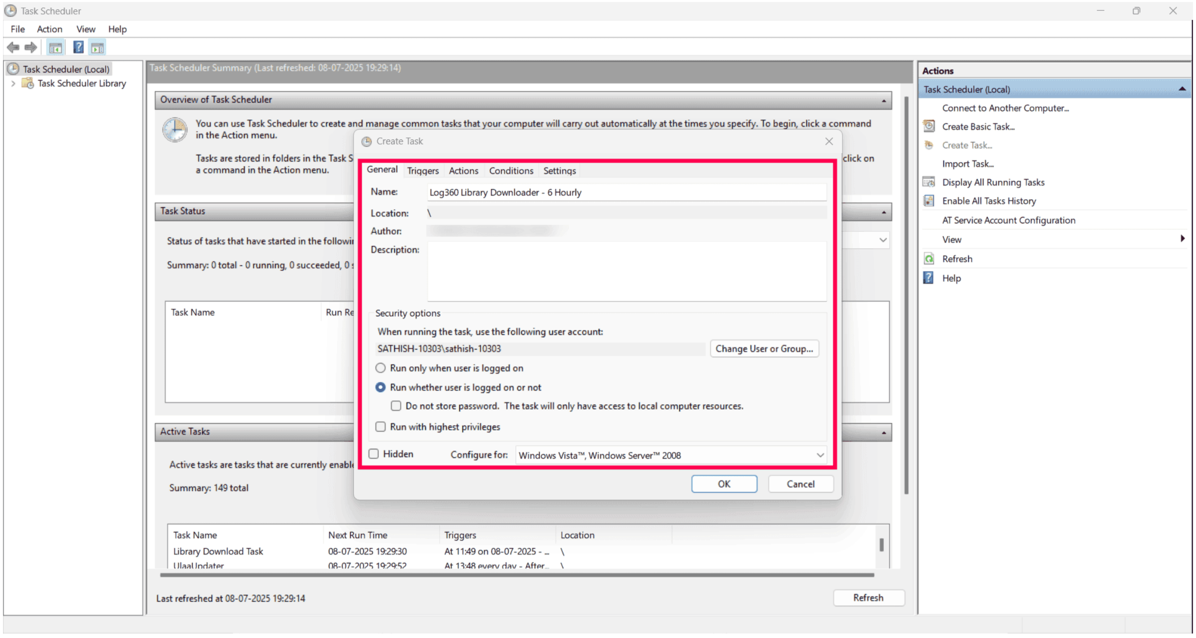
Summary: 0 total - 0 running, 0 succeeded, 0 ...

Last refreshed at 29-07-2025 11:43:23

Quickly creates a simple task.

Figure 4: Creating a new task in Task Scheduler

4. In the General tab:
   - Enter a name.
   - (Optional) Add a description.
   - Select Run whether user is logged on or not.



Create Task

General | Triggers | Actions | Conditions | Settings

Name: Log360 Library Downloader - 6 Hourly

Location: \

Author: [redacted]

Description:

Security options

When running the task, use the following user account:

SATHISH-10303\sathish-10303 [Change User or Group...]

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

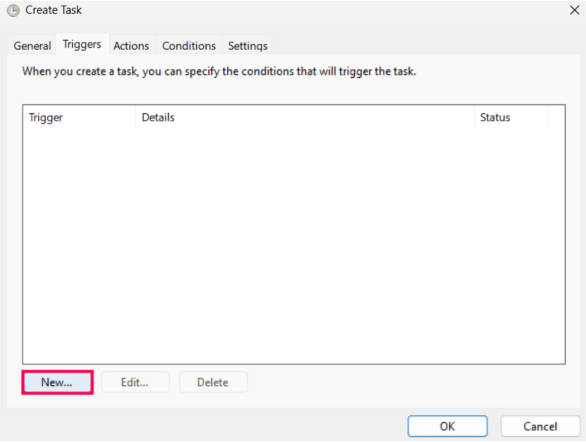
□ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008

[OK] [Cancel]

Figure 5: Configuring General settings

5. Go to the Triggers tab and click New.



Create Task

General | Triggers | Actions | Conditions | Settings

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status

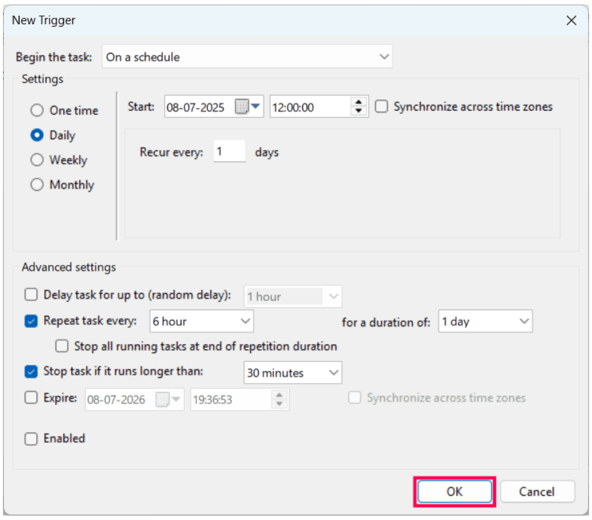
[New...] [Edit...] [Delete]

[OK] [Cancel]

Figure 6: Creating a new Trigger

6. In the New Trigger window:
   - From the Begin the task dropdown, select On a schedule.
   - Under Settings, choose Daily and set the Start date and time.
   - Under Advanced settings, check Repeat task every and set it to 6 hours.
   - In the For a duration of field, select 1 day.
   - Enable Stop task if it runs longer than and set it to 30 minutes.

- Ensure the Enabled checkbox is selected.
- Click OK to save the changes.



New Trigger

Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 08-07-2025 12:00:00 □ Synchronize across time zones

Recur every: 1 days

Advanced settings

□ Delay task for up to (random delay): 1 hour

☑ Repeat task every: 6 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

☑ Stop task if it runs longer than: 30 minutes

□ Expire: 08-07-2026 19:36:53 □ Synchronize across time zones

□ Enabled

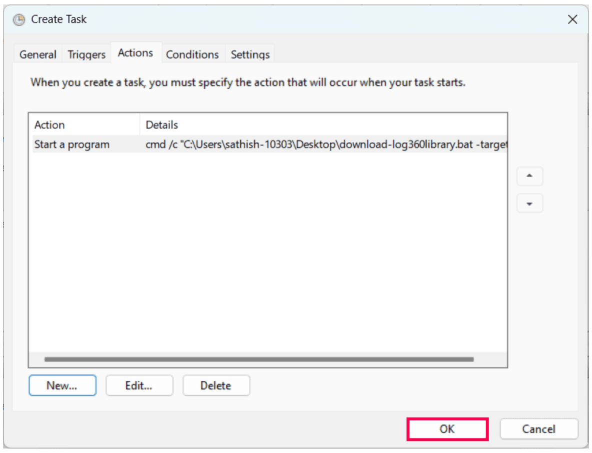
Figure 7: Configuring task triggers

7. Navigate to the Actions tab and click New.
8. In the Actions window:

- In the Action dropdown, select Start a program.
- In the Program/script field, enter cmd.
- In the Add arguments (optional) field, enter: /c "<download_path>\download-log360library.bat -targetDir <folder where files need to be downloaded>"

> ⓘ NOTE
>
> :If the -targetDir parameter is not provided, the files will be downloaded to the script file's parent directory by default.

- Click OK.



Create Task

When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	cmd /c "C:\Users\sathish-10303\Desktop\download-log360library.bat -target

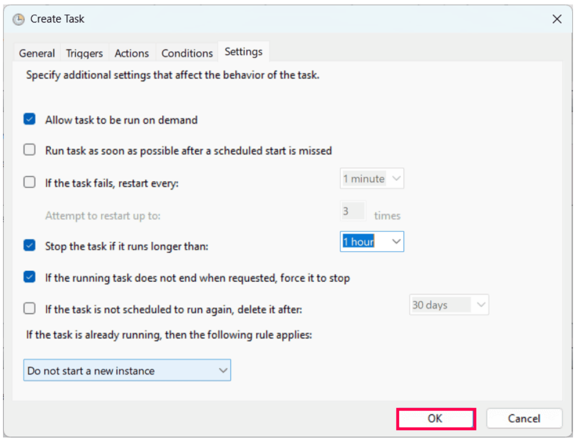
Figure 8: Configuring task actions

9. Navigate to the Conditions tab.

10. Go to the Settings tab.

11. In the Settings tab:

    - Select the checkbox next to Allow task to be run on demand.
    - Select the checkbox next to Stop the task if it runs longer than, and set the duration to 1 hour.
    - Select the checkbox next to If the running task does not end when requested, force it to stop.
    - In the If the task is already running, then the following rule is applied dropdown, choose Do not start a new instance.
    - Click OK to save the task.



Create Task

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

□ Run task as soon as possible after a scheduled start is missed

□ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 1 hour

☑ If the running task does not end when requested, force it to stop

□ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

Figure 9: Configuring additional settings

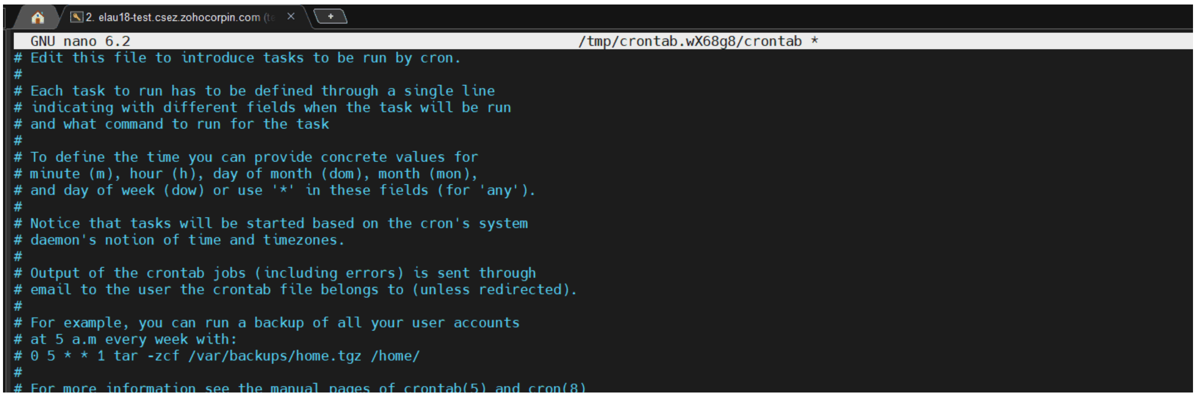
- When prompted, enter your Windows username and password.
- To verify the configuration, right-click the task in Task Scheduler and select Run.

Steps to schedule a shell script for every 6 hours in Cron Job

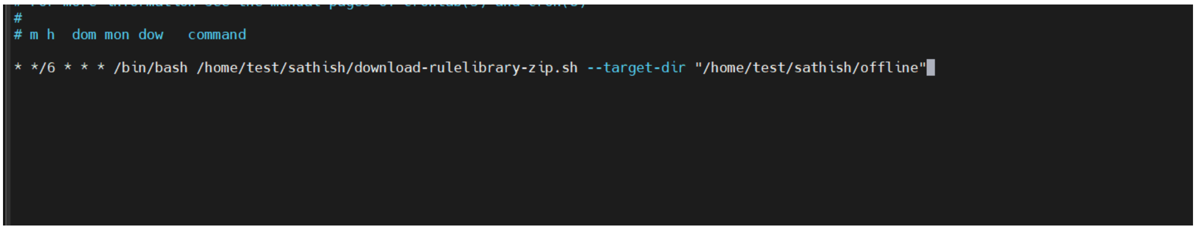
1. Set the script as executable before running it by using the following command: chmod +x <script_file_path>/download-log360library.sh

2. Run the crontab -e command to open the crontab editor.

3. Insert the following cron entry to run the script every 6 hours: 0 */6 * * * <script_file_path>/download-log360library.sh --target-dir "<download_path>



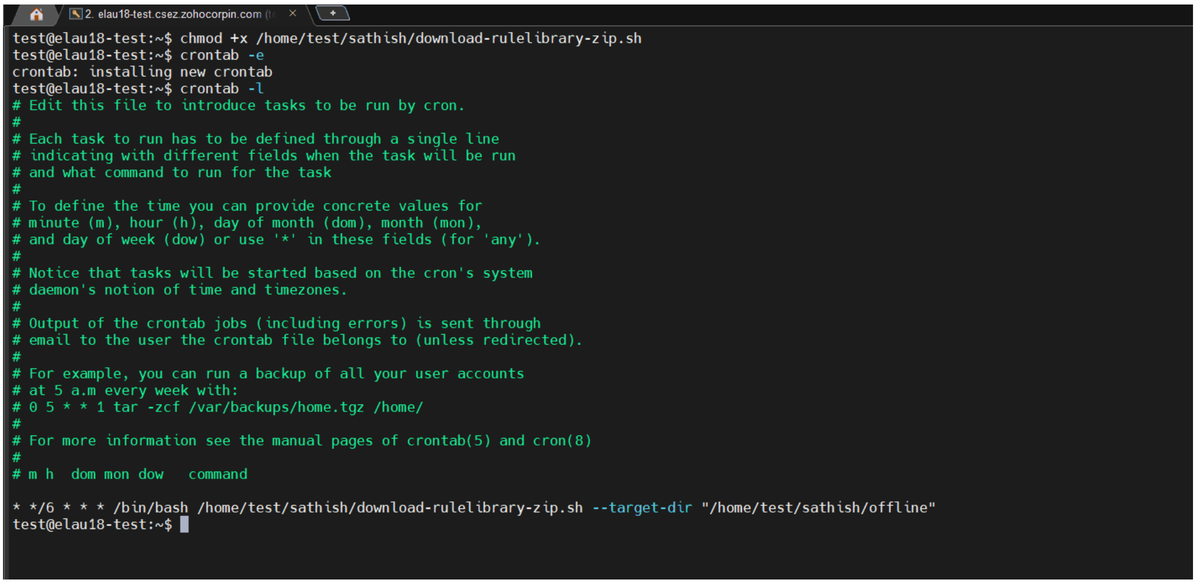
```
  GNU nano 6.2                                    /tmp/crontab.wX68g8/crontab *
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
```



```
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

* */6 * * * /bin/bash /home/test/sathish/download-rulelibrary-zip.sh --target-dir "/home/test/sathish/offline"
```

Figure 10: Adding the cron command

4. You can modify the path or time as required.
5. Save and exit the crontab editor:
    - Press Ctrl + O to save.
    - Press Ctrl + X to exit.
6. Verify the cron job installation by running the command: crontab -l



```
test@elau18-test:~$ chmod +x /home/test/sathish/download-rulelibrary-zip.sh
test@elau18-test:~$ crontab -e
crontab: installing new crontab
test@elau18-test:~$ crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

* */6 * * * /bin/bash /home/test/sathish/download-rulelibrary-zip.sh --target-dir "/home/test/sathish/offline"
test@elau18-test:~$
```

Figure 11: Saving and verifying the cron job

7. Check logs to confirm execution:
    - Review the script's log file: <download_path>/logs/download.log
    - Alternatively, review system logs such as var/log/cron.log depending on your operating system.

Read also

This page explained how to keep your Rule Library updated in online and offline environments. To learn more about the Rule Library and managing its capabilities, refer to:

- About Rule Library
- Installing Rules

4.1.5.1. Advanced Threat Analytics

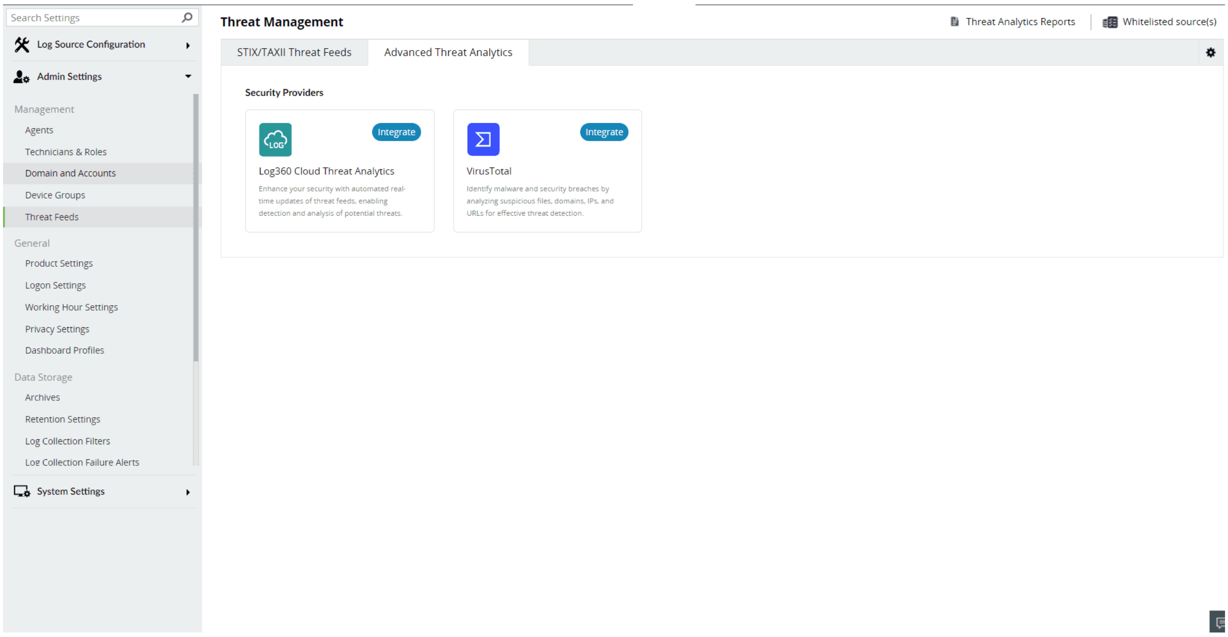
Last updated on: September 12, 2025

In this page

The Advanced Threat Analytics feature gives valuable insights into the severity of threats using the reputation score for potentially malicious URLs, domains, and IP addresses. To utilize the Advanced Threat Analytics feature in EventLog Analyzer, an add-on has to be purchased.

Advanced Threat Analytics add-on purchase:

- To purchase the Advanced Threat Analytics add-on, please click here.
- After purchasing and applying the add-on license, go to Settings → Admin Settings → Management→ Threat Feeds. The Advanced Threat Analytics tab will be present next to the STIX/TAXII Threat Feeds tab. Configure the respective feeds to access the threat analytics data.



Enhance your security with automated real-time updates of threat feeds, enabling detection and analysis of potential threats.

Identify malware and security breaches by analyzing suspicious files, domains, IPs, and URLs for effective threat detection.

Overview

1. Vendor support:

   EventLog Analyzer supports the following vendors for the Advanced Threat Analytics data:

   - Log360 Cloud Threat Analytics

     Default integration from Log360 Cloud suite. This can be accessed once the add-on is purchased.

   - VirusTotal

     Third-party threat feed integration. This follows the Bring Your Own Key(BYOK) model. If you have bought VirusTotal access separately, you can use your API key and get the threat analytics information in EventLog Analyzer.

2. Access

   Here's how users can access the Adavanced Threat Analytics information for different usecases:

   - For investigation: To investigate the external threat sources, the threat analytics information can be accessed through the External Threat report and the Incident Workbench.

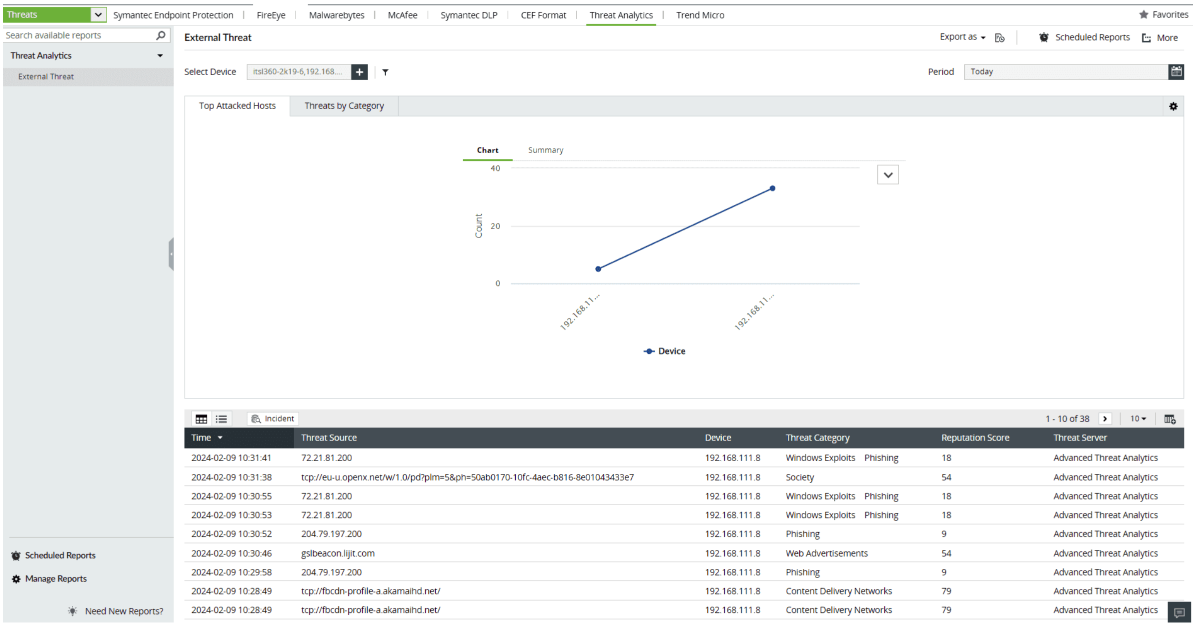
   - Detection: The Default Threat alert criteria detects interaction with external threat sources. Once the Advanced Threat Analytics add-on is applied, the alerts will be accurately fine tuned to reduce false positives.

External Threat report

Navigation: EventLog Analyzer home > Reports > Select Threats from the drop-down in the top left corner > Threat Analytics > External Threat

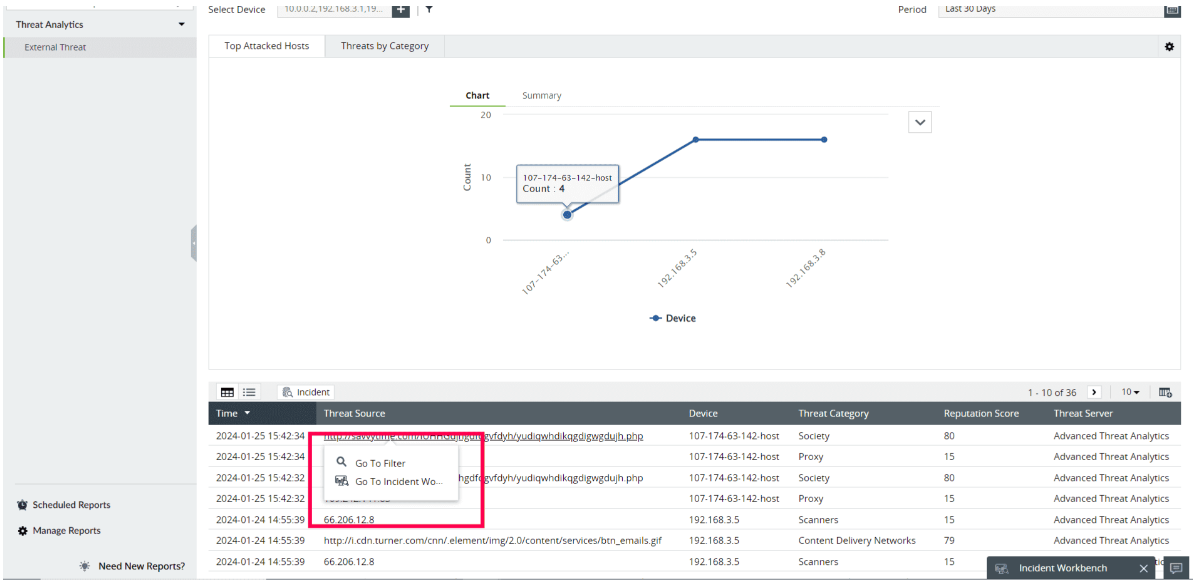
The External Threat report contains the information on the source of the threat, severity, reputation score, and more.

- View reports of Top Attacked Hosts and Threats by Category for the selected period.

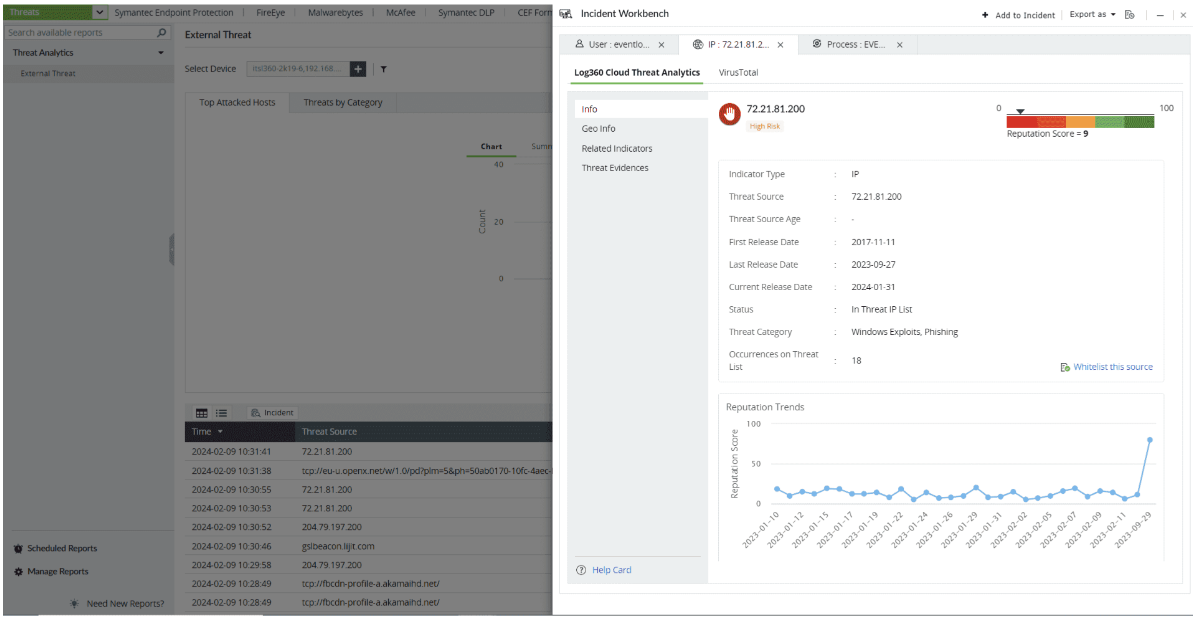


Time	Threat Source	Device	Threat Category	Reputation Score	Threat Server
2024-02-09 10:31:41	72.21.81.200	192.168.111.8	Windows Exploits Phishing	18	Advanced Threat Analytics
2024-02-09 10:31:38	tcp://eu-u.openx.net/w/1.0/pd?plm=5&ph=50ab0170-10fc-4aec-b816-8e01043433e7	192.168.111.8	Society	54	Advanced Threat Analytics
2024-02-09 10:30:55	72.21.81.200	192.168.111.8	Windows Exploits Phishing	18	Advanced Threat Analytics
2024-02-09 10:30:53	72.21.81.200	192.168.111.8	Windows Exploits Phishing	18	Advanced Threat Analytics
2024-02-09 10:30:52	204.79.197.200	192.168.111.8	Phishing	9	Advanced Threat Analytics
2024-02-09 10:30:46	gslbeacon.lijit.com	192.168.111.8	Web Advertisements	54	Advanced Threat Analytics
2024-02-09 10:29:58	204.79.197.200	192.168.111.8	Phishing	9	Advanced Threat Analytics
2024-02-09 10:28:49	tcp://fbcdn-profile-a.akamaihd.net/	192.168.111.8	Content Delivery Networks	79	Advanced Threat Analytics
2024-02-09 10:28:49	tcp://fbcdn-profile-a.akamaihd.net/	192.168.111.8	Content Delivery Networks	79	Advanced Threat Analytics

- 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



Time	Threat Source	Device	Threat Category	Reputation Score	Threat Server
2024-01-25 15:42:34	http://savvytime.com/IOHHGdjhgdf...gvfdyh/yudiqwhdikqgdigwgdujh.php	107-174-63-142-host	Society	80	Advanced Threat Analytics
2024-01-25 15:42:34		107-174-63-142-host	Proxy	15	Advanced Threat Analytics
2024-01-25 15:42:32	...hgdf...gvfdyh/yudiqwhdikqgdigwgdujh.php	107-174-63-142-host	Society	80	Advanced Threat Analytics
2024-01-25 15:42:32		107-174-63-142-host	Proxy	15	Advanced Threat Analytics
2024-01-24 14:55:39	66.206.12.8	192.168.3.5	Scanners	15	Advanced Threat Analytics
2024-01-24 14:55:39	http://i.cdn.turner.com/cnn/.element/img/2.0/content/services/btn_emails.gif	192.168.3.5	Content Delivery Networks	79	Advanced Threat Analytics
2024-01-24 14:55:39	66.206.12.8	192.168.3.5	Scanners	15	



External Threat

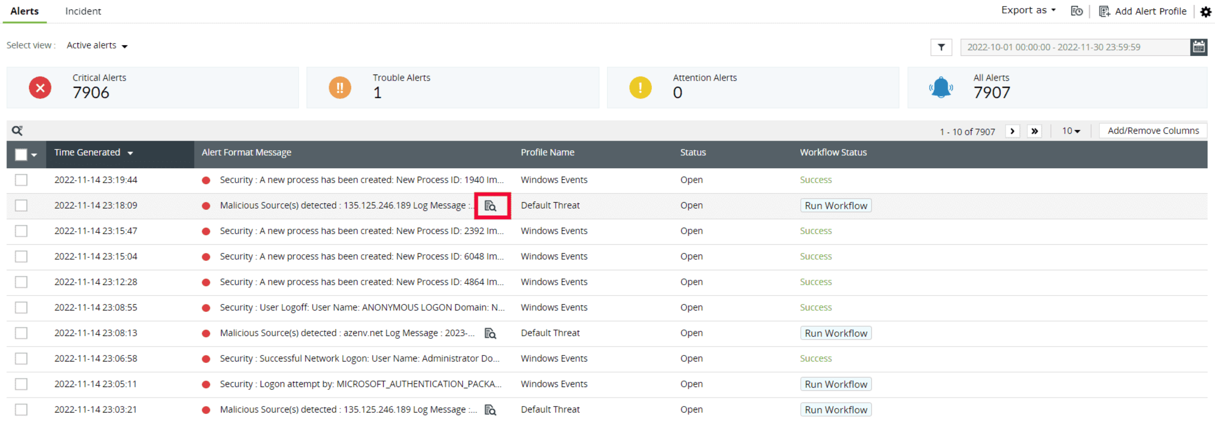
Time	Threat Source
2024-02-09 10:31:41	72.21.81.200
2024-02-09 10:31:38	tcp://eu-u.openx.net/w/1.0/pd?plm=5&ph=50ab0170-10fc-4aec-
2024-02-09 10:30:55	72.21.81.200
2024-02-09 10:30:53	72.21.81.200
2024-02-09 10:30:52	204.79.197.200
2024-02-09 10:30:46	gslbeacon.lijit.com
2024-02-09 10:29:58	204.79.197.200
2024-02-09 10:28:49	tcp://fbcdn-profile-a.akamaihd.net/
2024-02-09 10:28:49	tcp://fbcdn-profile-a.akamaihd.net/

72.21.81.200
High Risk
0 100
Reputation Score = **9**

Indicator Type : IP
Threat Source : 72.21.81.200
Threat Source Age : -
First Release Date : 2017-11-11
Last Release Date : 2023-09-27
Current Release Date : 2024-01-31
Status : In Threat IP List
Threat Category : Windows Exploits, Phishing
Occurrences on Threat List : 18

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.



Critical Alerts 7906
Trouble Alerts 1
Attention Alerts 0
All Alerts 7907

Time Generated	Alert Format Message	Profile Name	Status	Workflow Status
2022-11-14 23:19:44	Security : A new process has been created: New Process ID: 1940 Im...	Windows Events	Open	Success
2022-11-14 23:18:09	Malicious Source(s) detected : 135.125.246.189 Log Message :...	Default Threat	Open	Run Workflow
2022-11-14 23:15:47	Security : A new process has been created: New Process ID: 2392 Im...	Windows Events	Open	Success
2022-11-14 23:15:04	Security : A new process has been created: New Process ID: 6048 Im...	Windows Events	Open	Success
2022-11-14 23:12:28	Security : A new process has been created: New Process ID: 4864 Im...	Windows Events	Open	Success
2022-11-14 23:08:55	Security : User Logoff: User Name: ANONYMOUS LOGON Domain: N...	Windows Events	Open	Success
2022-11-14 23:08:13	Malicious Source(s) detected : azenv.net Log Message : 2023-...	Default Threat	Open	Run Workflow
2022-11-14 23:06:58	Security : Successful Network Logon: User Name: Administrator Do...	Windows Events	Open	Success
2022-11-14 23:05:11	Security : Logon attempt by: MICROSOFT_AUTHENTICATION_PACKA...	Windows Events	Open	Run Workflow
2022-11-14 23:03:21	Malicious Source(s) detected : 135.125.246.189 Log Message :...	Default Threat	Open	Run Workflow

4.1.5.2. Constella Intelligence

Last updated on: September 12, 2025

In this page

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

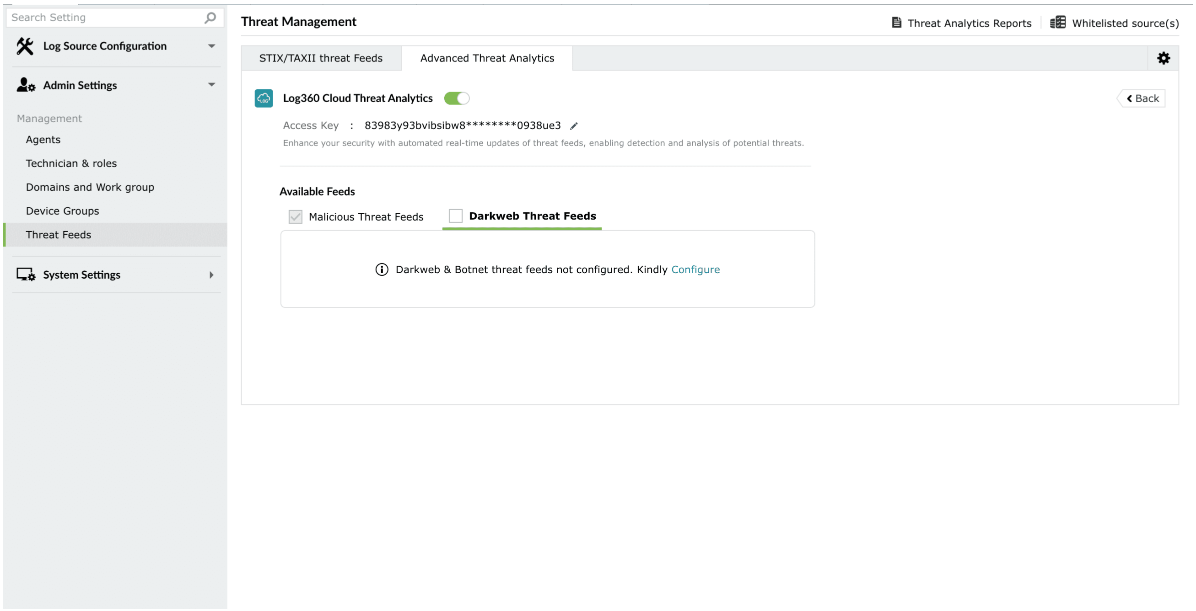
Configuring Dark Web threat feeds

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.



Access Key : 83983y93bvibsibw8********0938ue3

Enhance your security with automated real-time updates of threat feeds, enabling detection and analysis of potential threats.

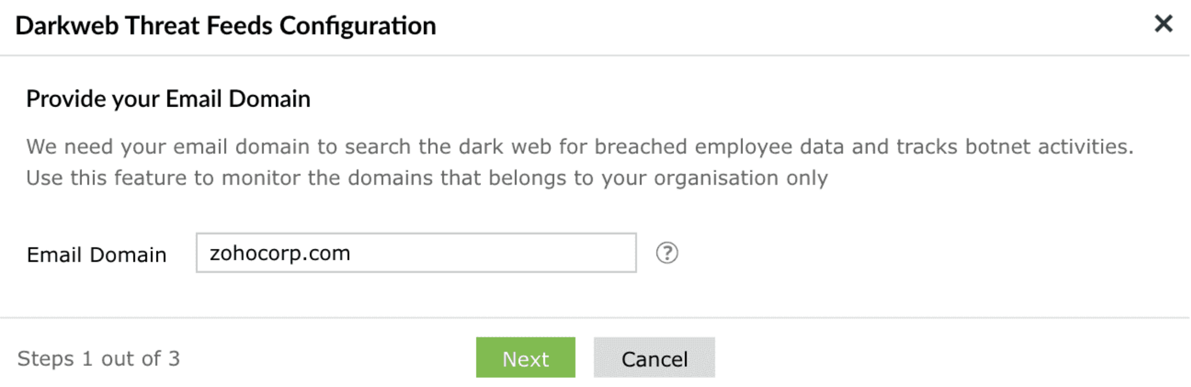
Available Feeds

☑ Malicious Threat Feeds □ Darkweb Threat Feeds

Darkweb & Botnet threat feeds not configured. Kindly Configure

- Upon clicking Configure, a pop-up requesting an email domain to monitor for dark web exposure will be

- Upon clicking Configure, a pop-up requesting an email domain to monitor for dark web exposure will be displayed. After entering the domain, you will be asked to provide a valid email address from that domain for verification.



Darkweb Threat Feeds Configuration

Provide your Email Domain

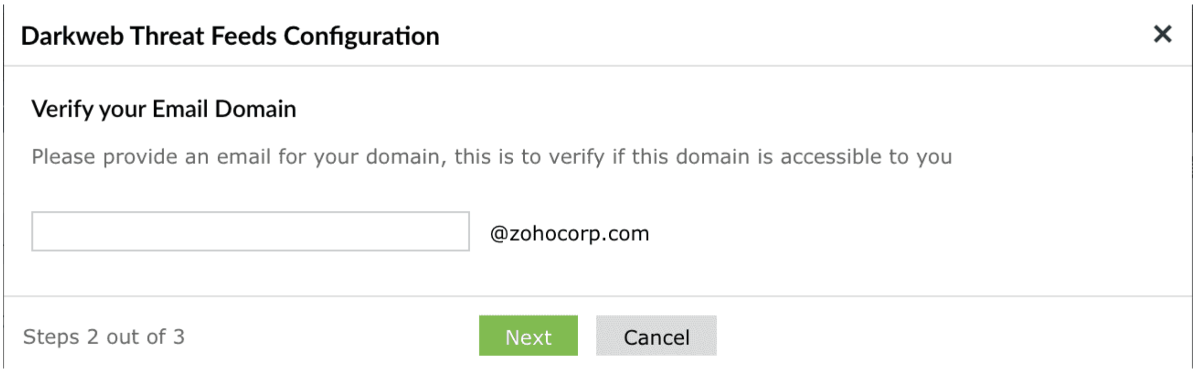
We need your email domain to search the dark web for breached employee data and tracks botnet activities. Use this feature to monitor the domains that belongs to your organisation only

Email Domain: zohocorp.com

Steps 1 out of 3

Note

Domain configuration for email is linked to licensing. You can only configure domains associated with licenses you have purchased.



Darkweb Threat Feeds Configuration

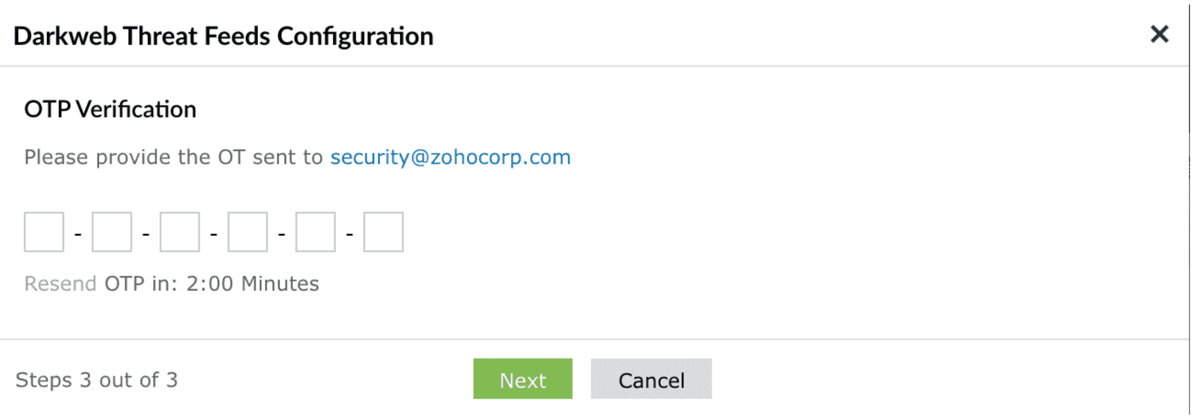
Verify your Email Domain

Please provide an email for your domain, this is to verify if this domain is accessible to you

@zohocorp.com

Steps 2 out of 3

- 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.



Darkweb Threat Feeds Configuration

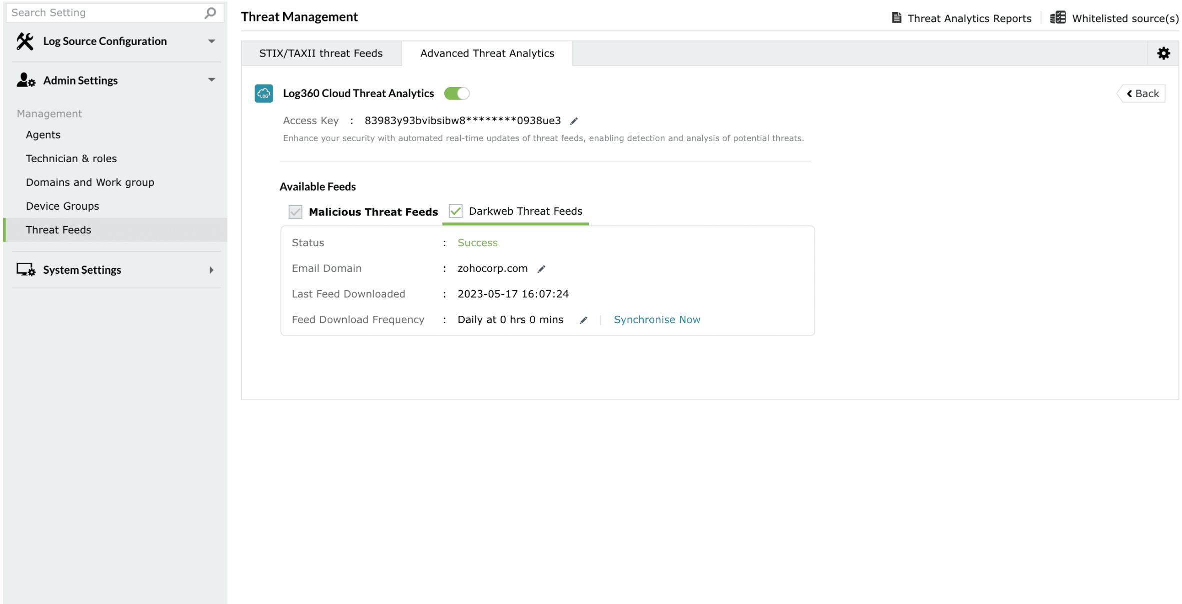
OTP Verification

Please provide the OT sent to security@zohocorp.com

Resend OTP in: 2:00 Minutes

Steps 3 out of 3

- You will see this page once your domain is successfully configured.



Threat Management

Log360 Cloud Threat Analytics

Access Key : 83983y93bvibsibw8********0938ue3

Enhance your security with automated real-time updates of threat feeds, enabling detection and analysis of potential threats.

Available Feeds

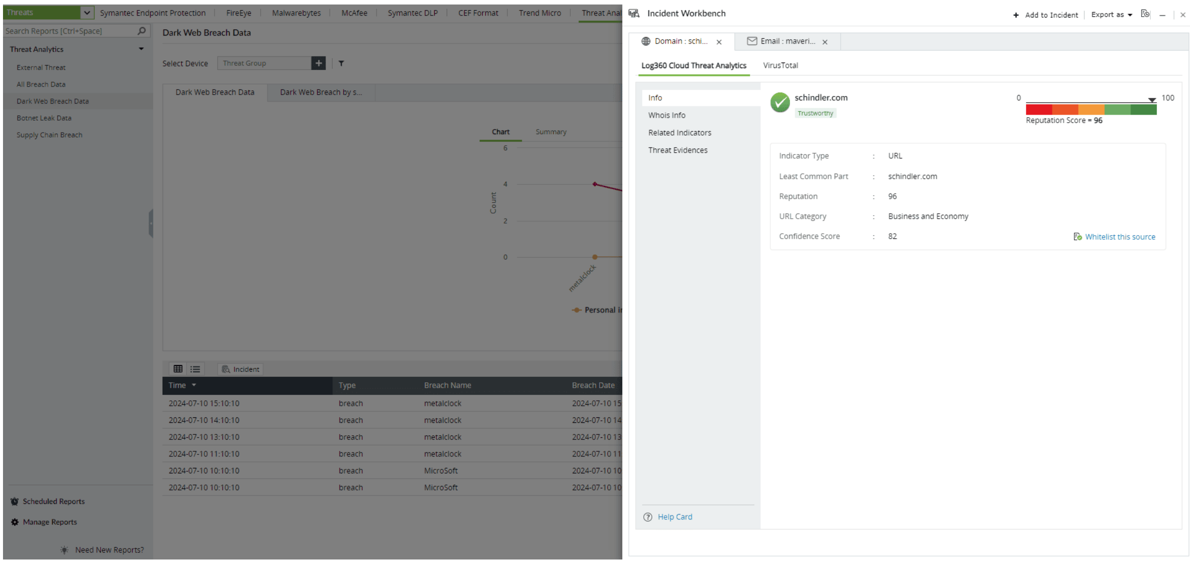
☐ **Malicious Threat Feeds** ☑ Darkweb Threat Feeds

Status	:	Success
Email Domain	:	zohocorp.com
Last Feed Downloaded	:	2023-05-17 16:07:24
Feed Download Frequency	:	Daily at 0 hrs 0 mins Synchronise Now

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



Dark Web Breach Data

Time	Type	Breach Name	Breach Date
2024-07-10 15:10:10	breach	metalclock	2024-07-10 15
2024-07-10 14:10:10	breach	metalclock	2024-07-10 14
2024-07-10 13:10:10	breach	metalclock	2024-07-10 13
2024-07-10 11:10:10	breach	metalclock	2024-07-10 11
2024-07-10 10:10:10	breach	MicroSoft	2024-07-10 10
2024-07-10 10:10:10	breach	MicroSoft	2024-07-10 10

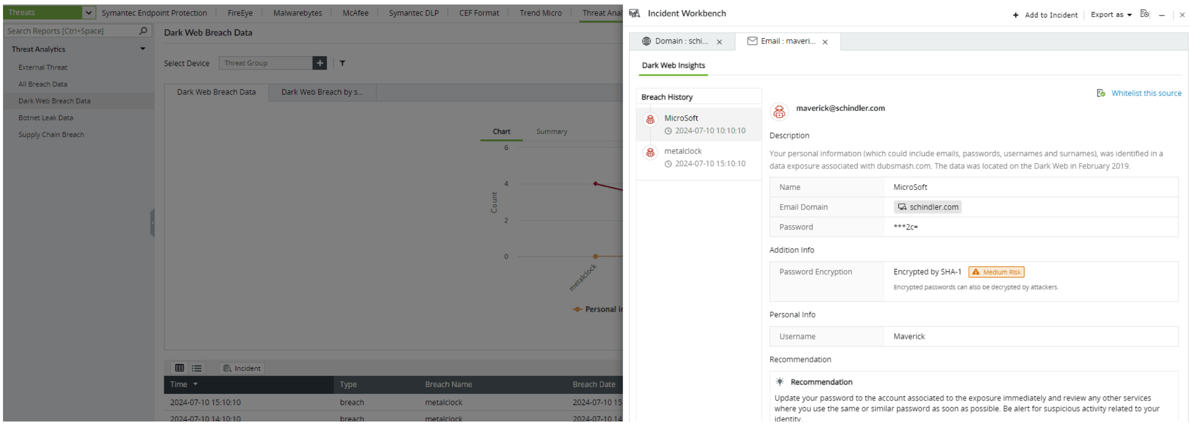
schindler.com

Trustworthy

Reputation Score = 96

Indicator Type	:	URL
Least Common Part	:	schindler.com
Reputation	:	96
URL Category	:	Business and Economy
Confidence Score	:	82

- Email analysis for the configured domain



Dark Web Breach Data

Time	Type	Breach Name	Breach Date
2024-07-10 15:10:10	breach	metalclock	2024-07-10 15
2024-07-10 14:10:10	breach	metalclock	2024-07-10 14

Breach History

MicroSoft
2024-07-10 10:10:10

metalclock
2024-07-10 15:10:10

maverick@schindler.com

Description

Your personal information (which could include emails, passwords, usernames and surnames), was identified in a data exposure associated with dubsmash.com. The data was located on the Dark Web in February 2019.

Name	MicroSoft
Email Domain	schindler.com
Password	***2c=

Addition Info

Password Encryption	Encrypted by SHA-1 ⚠ Medium Risk Encrypted passwords can also be decrypted by attackers.

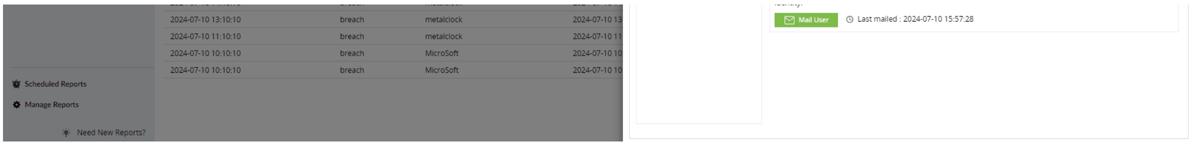
Personal Info

Username	Maverick

Recommendation

Recommendation

Update your password to the account associated to the exposure immediately and review any other services where you use the same or similar password as soon as possible. Be alert for suspicious activity related to your identity.



2024-07-10 13:10:10	breach	metalclock	2024-07-10 13
2024-07-10 11:10:10	breach	metalclock	2024-07-10 11
2024-07-10 10:10:10	breach	MicroSoft	2024-07-10 10
2024-07-10 10:10:10	breach	MicroSoft	2024-07-10 10

Last mailed : 2024-07-10 15:57:28

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

4.1.5.3. VirusTotal

Last updated on: September 12, 2025

In this page

Advanced threat analytics add-on in EventLog Analyzer

Note

VirusTotal is one of the largest live threat feeds that consolidates risk scores of IPs, URLs, Domains, and files from a wide range of security vendors. This integration in EventLog Analyzer follows the Bring Your Own Key(BYOK) model. If you have bought VirusTotal access separately, you can use your API key and analyze threat sources in EventLog Analyzer.

VirusTotal terms of service:

Users can access VirusTotal API in two ways:

1. Public API: Provides free access with specific limitations, including constraints on request frequency and access with lower priority.
2. Premium API: Provides exclusive access without limitations on request frequency and prioritized access, complemented by additional benefits.

Recommendation: For business workflows it is recommended to use Premium API for integration.
To learn more about VirusTotal, their terms of service, privacy policy, and API usage, please visit their website.

Configuration

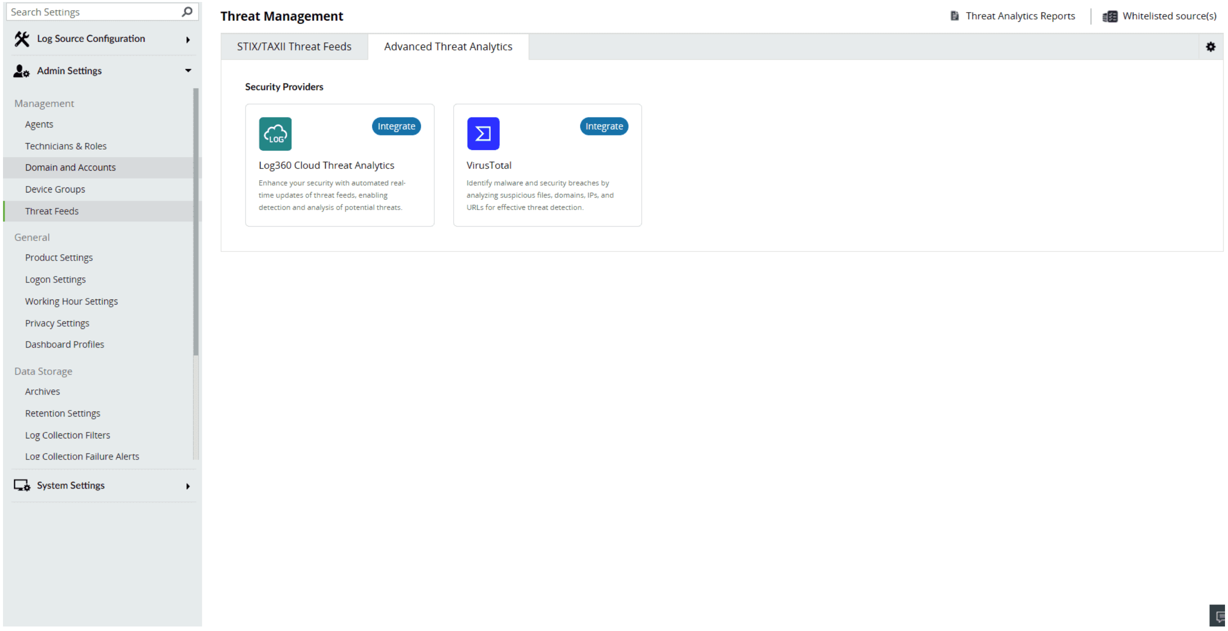
Note

Please refer to VirusTotal's privacy policy to understand how user-submitted data is utilized for analysis, as well as their policies on data processing, sharing, retention, and deletion.

Once you have purchased the Advanced Threat Analytics add-on and applied the license, head to the Advanced Threat Analytics page.

Navigation: Settings → Admin Settings → Management→ Threat Feeds→Advanced Threat

Analytics → VirusTotal → Integrate

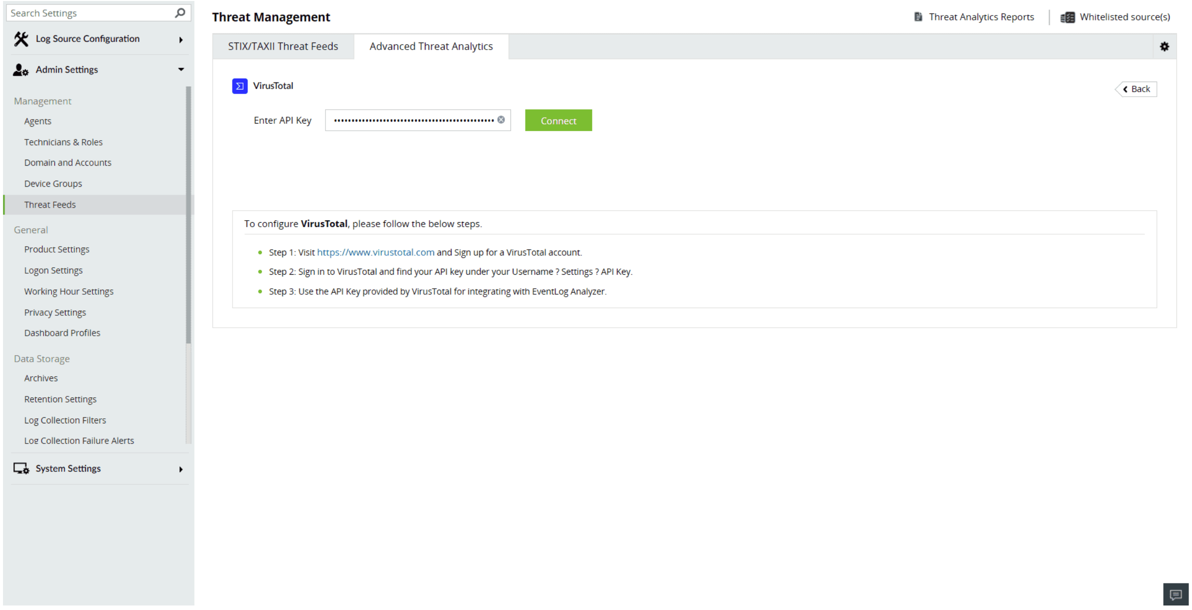


Enhance your security with automated real-time updates of threat feeds, enabling detection and analysis of potential threats.

Identify malware and security breaches by analyzing suspicious files, domains, IPs, and URLs for effective threat detection.

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.

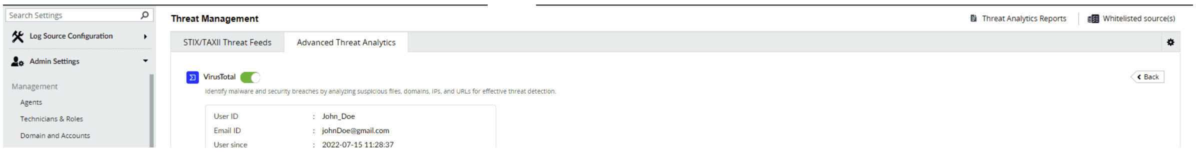


Enter API Key ••

To configure **VirusTotal**, please follow the below steps.

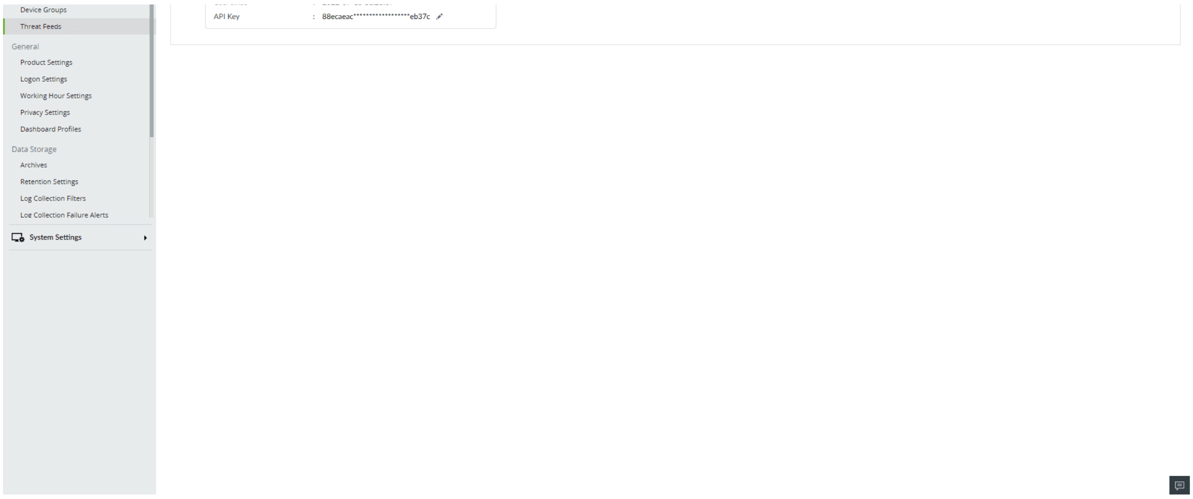
- Step 1: Visit https://www.virustotal.com and Sign up for a VirusTotal account.
- Step 2: Sign in to VirusTotal and find your API key under your Username ? Settings ? API Key.
- Step 3: Use the API Key provided by VirusTotal for integrating with EventLog Analyzer.

4. Paste the API key and click on Connect to finish configuring VirusTotal.



Identify malware and security breaches by analyzing suspicious files, domains, IPs, and URLs for effective threat detection.

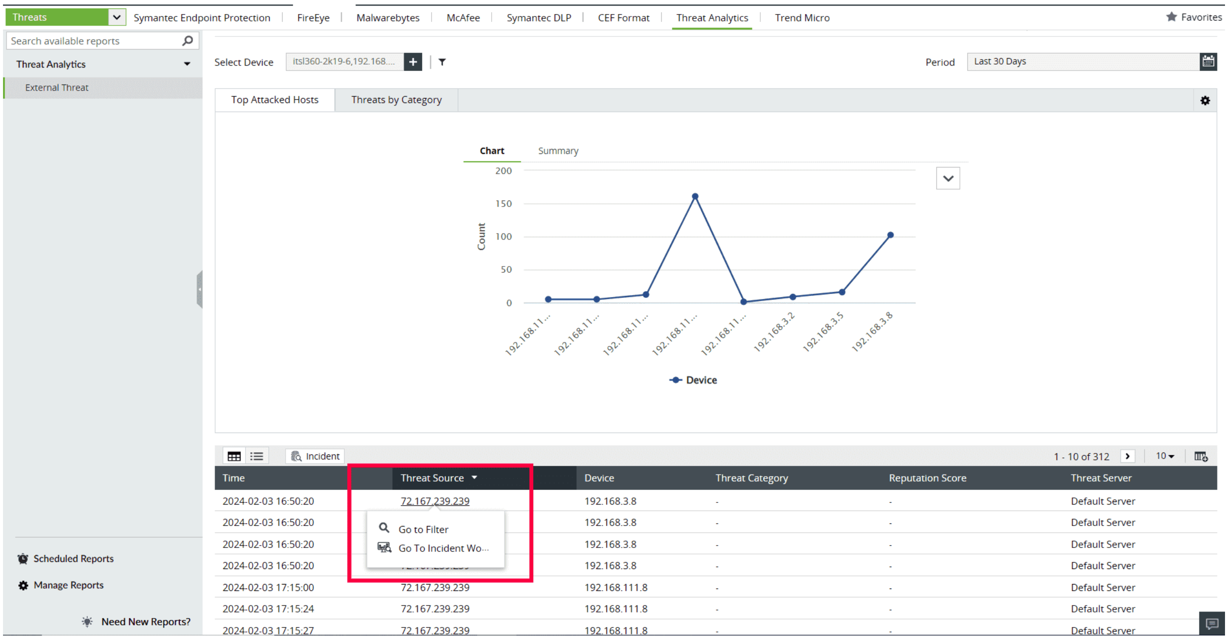
User ID : John_Doe
Email ID : johnDoe@gmail.com
User since : 2022-07-15 11:28:37



API Key : 88ecaeac******************eb37c

Analysis

In EventLog Analyzer, users can access the data from VirusTotal through the Incident Workbench. Learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer.



Select Device itsl360-2k19-6,192.168....

Period Last 30 Days

Time	Threat Source	Device	Threat Category	Reputation Score	Threat Server
2024-02-03 16:50:20	72.167.239.239	192.168.3.8	-	-	Default Server
2024-02-03 16:50:20		192.168.3.8	-	-	Default Server
2024-02-03 16:50:20		192.168.3.8	-	-	Default Server
2024-02-03 16:50:20	[illegible]	192.168.3.8	-	-	Default Server
2024-02-03 17:15:00	72.167.239.239	192.168.111.8	-	-	Default Server
2024-02-03 17:15:24	72.167.239.239	192.168.111.8	-	-	Default Server
2024-02-03 17:15:27	72.167.239.239	192.168.111.8	-	-	Default Server

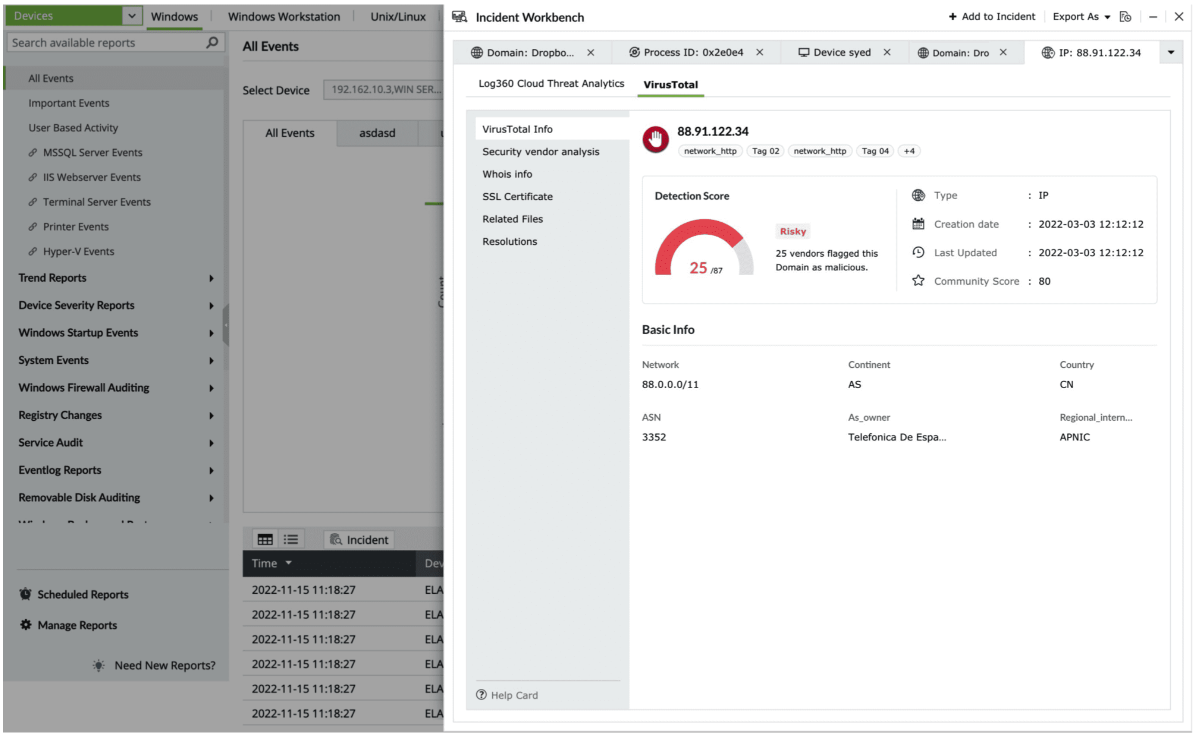
Note

To understand the different terminologies used in the VirusTotal reports, please use the Help Card in the bottom left corner.

Select any IP, URL, or Domain to analyze in the Workbench. You can access the following data:

- VirusTotal note-box
  This section contains the Detection Score of the Threat Source, which is the number of security vendors who have flagged the source as risky out of all the security vendors. Along with this, the basic details and the geo note-box of the Threat Source are also available

note-box of the Threat Source are also available.



88.91.122.34

network_http Tag 02 network_http Tag 04 +4

Detection Score

25 /87

Risky

25 vendors flagged this Domain as malicious.

Type : IP

Creation date : 2022-03-03 12:12:12

Last Updated : 2022-03-03 12:12:12

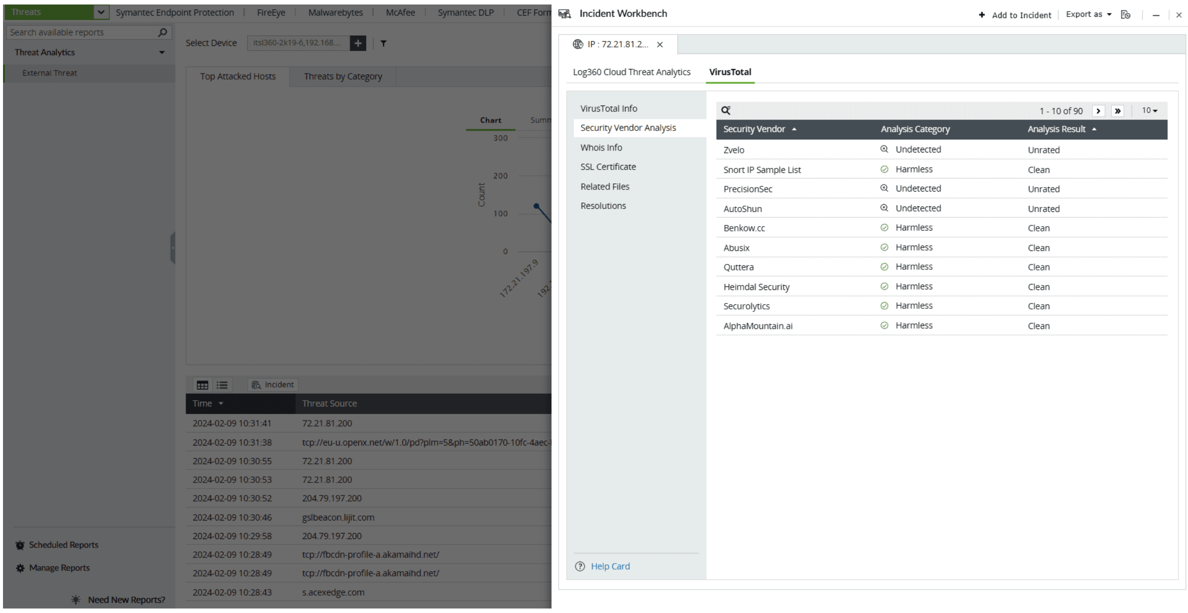
Community Score : 80

Basic Info

Network	Continent	Country
88.0.0.0/11	AS	CN
ASN	As_owner	Regional_intern...
3352	Telefonica De Espa...	APNIC

- Security Vendor analysis

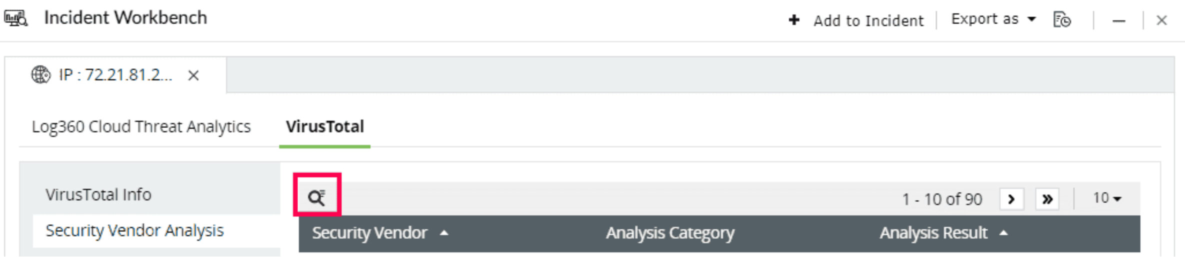
This section contains the individual analysis of 85+ security vendors such as SOCRadar, Fortinet, Forcepoint ThreatSeeker, and ArcSight Threat Intelligence.

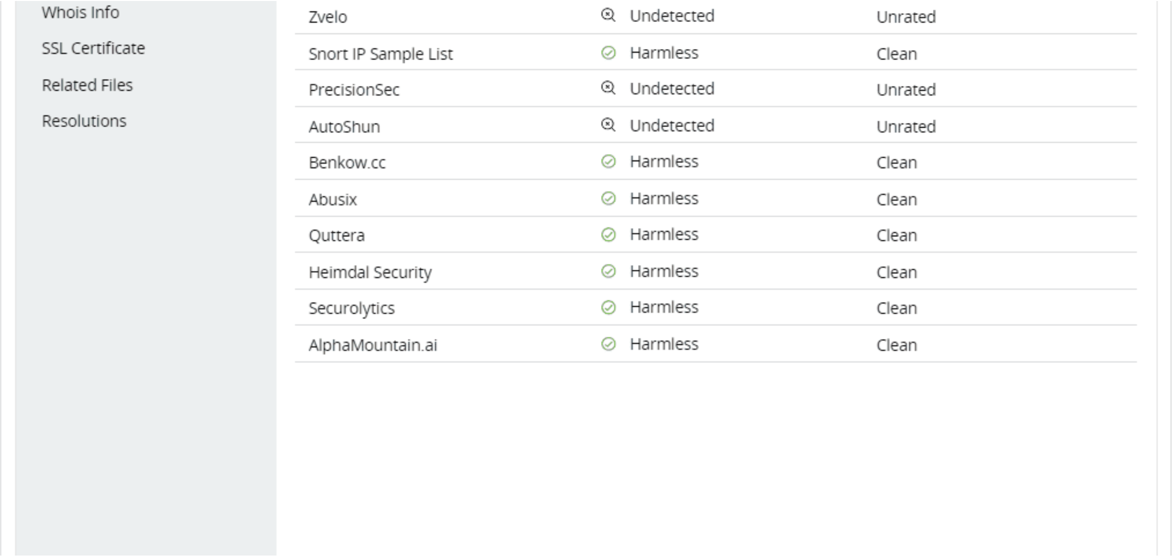


Time	Threat Source
2024-02-09 10:31:41	72.21.81.200
2024-02-09 10:31:38	tcp://eu-u.openx.net/w/1.0/pd?plm=5&ph=50ab0170-10fc-4aec-
2024-02-09 10:30:55	72.21.81.200
2024-02-09 10:30:53	72.21.81.200
2024-02-09 10:30:52	204.79.197.200
2024-02-09 10:30:46	gslbeacon.lijit.com
2024-02-09 10:29:58	204.79.197.200
2024-02-09 10:28:49	tcp://fbcdn-profile-a.akamaihd.net/
2024-02-09 10:28:49	tcp://fbcdn-profile-a.akamaihd.net/
2024-02-09 10:28:43	s.acexedge.com

Security Vendor	Analysis Category	Analysis Result
Zvelo	Undetected	Unrated
Snort IP Sample List	Harmless	Clean
PrecisionSec	Undetected	Unrated
AutoShun	Undetected	Unrated
Benkow.cc	Harmless	Clean
Abusix	Harmless	Clean
Quttera	Harmless	Clean
Heimdal Security	Harmless	Clean
Securolytics	Harmless	Clean
AlphaMountain.ai	Harmless	Clean

Click on the search icon in the top left corner to filter based on Security Vendor, Analysis Category, and Analysis Result.



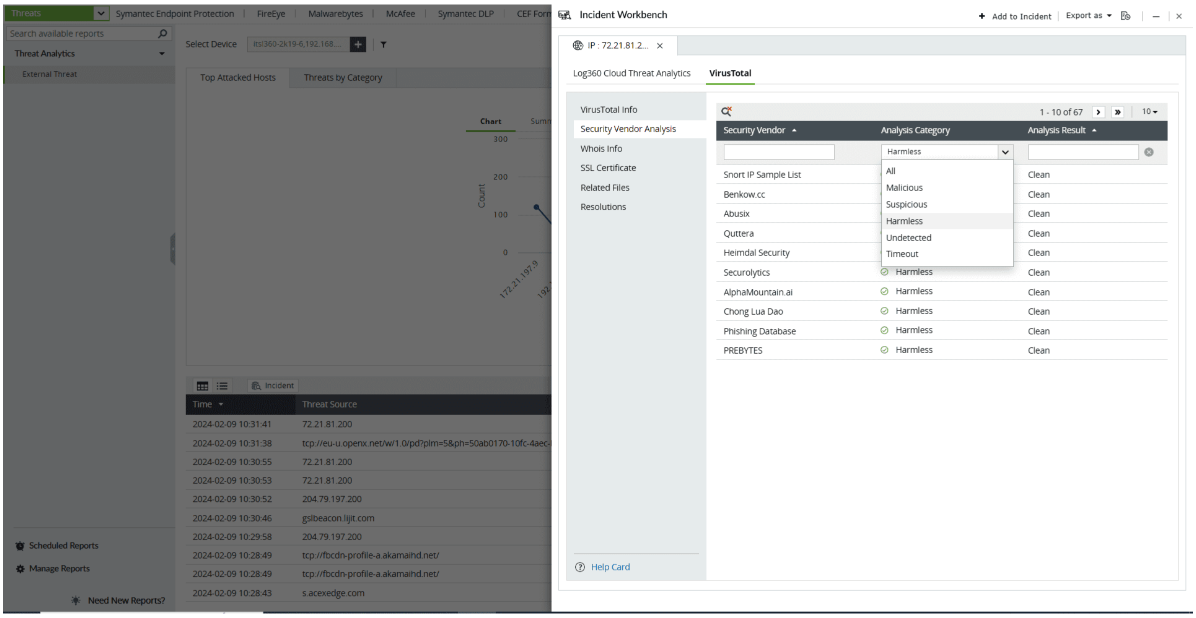


Whois Info
SSL Certificate
Related Files
Resolutions

Zvelo	Undetected	Unrated
Snort IP Sample List	✓ Harmless	Clean
PrecisionSec	Undetected	Unrated
AutoShun	Undetected	Unrated
Benkow.cc	✓ Harmless	Clean
Abusix	✓ Harmless	Clean
Quttera	✓ Harmless	Clean
Heimdal Security	✓ Harmless	Clean
Securolytics	✓ Harmless	Clean
AlphaMountain.ai	✓ Harmless	Clean

Here are the Analysis Categories:

- Malicious
- Suspicious
- Harmless
- Undetected
- Timeout

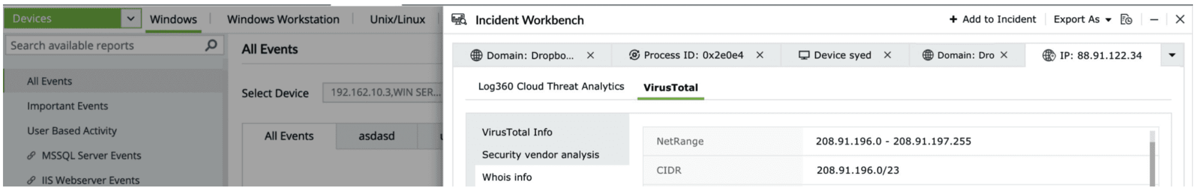


Time	Threat Source
2024-02-09 10:31:41	72.21.81.200
2024-02-09 10:31:38	tcp://eu-u.openx.net/w/1.0/pd?plm=5&ph=50ab0170-10fc-4aec-
2024-02-09 10:30:55	72.21.81.200
2024-02-09 10:30:53	72.21.81.200
2024-02-09 10:30:52	204.79.197.200
2024-02-09 10:30:46	gslbeacon.lijit.com
2024-02-09 10:29:58	204.79.197.200
2024-02-09 10:28:49	tcp://fbcdn-profile-a.akamaihd.net/
2024-02-09 10:28:49	tcp://fbcdn-profile-a.akamaihd.net/
2024-02-09 10:28:43	s.acexedge.com

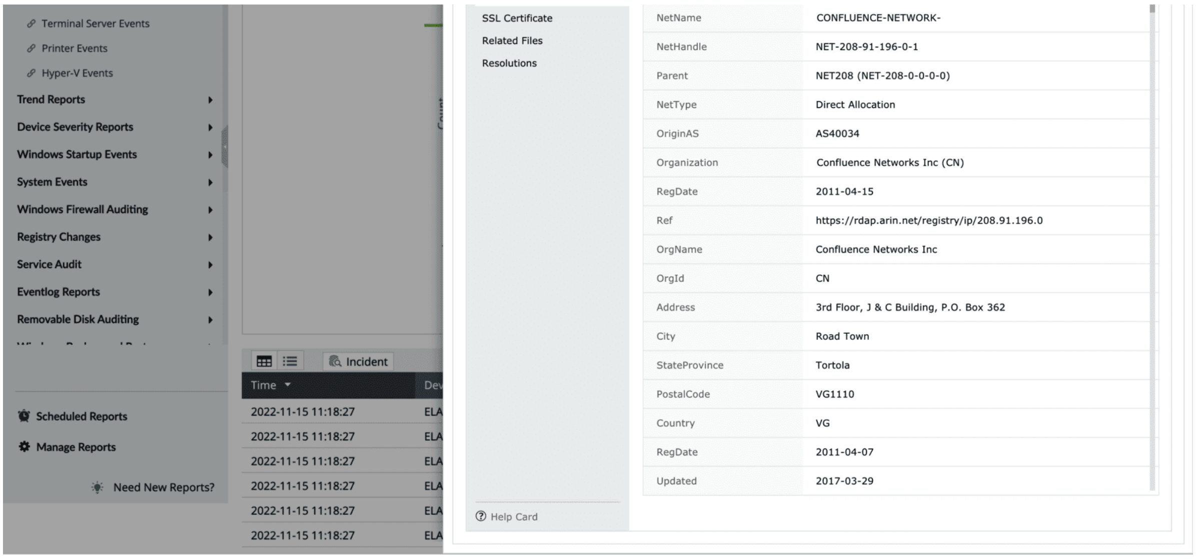
Security Vendor	Analysis Category	Analysis Result
	Harmless	
Snort IP Sample List		Clean
Benkow.cc		Clean
Abusix		Clean
Quttera		Clean
Heimdal Security		Clean
Securolytics	✓ Harmless	Clean
AlphaMountain.ai	✓ Harmless	Clean
Chong Lua Dao	✓ Harmless	Clean
Phishing Database	✓ Harmless	Clean
PREBYTES	✓ Harmless	Clean

- Whois note-box

This section contains the Whois note-boxrmation of the threat source domain.



NetRange	208.91.196.0 - 208.91.197.255
CIDR	208.91.196.0/23

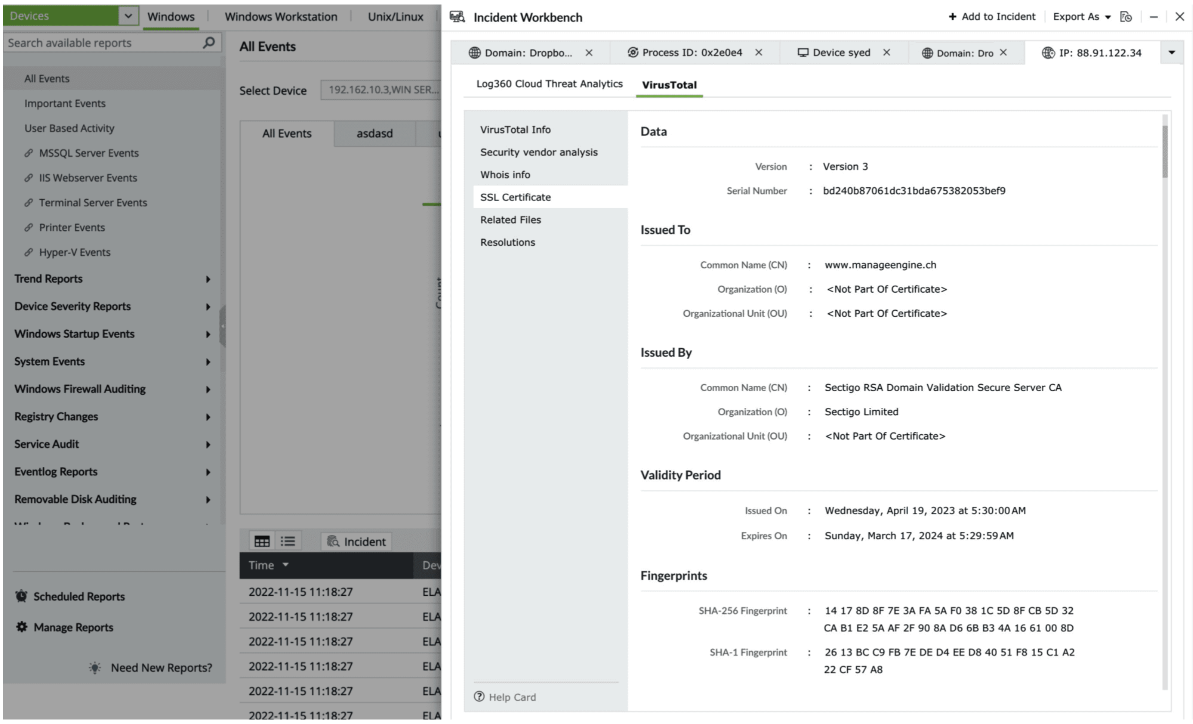


NetName	CONFLUENCE-NETWORK-
NetHandle	NET-208-91-196-0-1
Parent	NET208 (NET-208-0-0-0-0)
NetType	Direct Allocation
OriginAS	AS40034
Organization	Confluence Networks Inc (CN)
RegDate	2011-04-15
Ref	https://rdap.arin.net/registry/ip/208.91.196.0
OrgName	Confluence Networks Inc
OrgId	CN
Address	3rd Floor, J & C Building, P.O. Box 362
City	Road Town
StateProvince	Tortola
PostalCode	VG1110
Country	VG
RegDate	2011-04-07
Updated	2017-03-29

```
2022-11-15 11:18:27  ELA
2022-11-15 11:18:27  ELA
2022-11-15 11:18:27  ELA
2022-11-15 11:18:27  ELA
2022-11-15 11:18:27  ELA
2022-11-15 11:18:27  ELA
```

- SSL Certificate

  This section contains details of the SSL certificate issued to the Threat Source and who issued it.



Data

Version : Version 3
Serial Number : bd240b87061dc31bda675382053bef9

Issued To

Common Name (CN) : www.manageengine.ch
Organization (O) : <Not Part Of Certificate>
Organizational Unit (OU) : <Not Part Of Certificate>

Issued By

Common Name (CN) : Sectigo RSA Domain Validation Secure Server CA
Organization (O) : Sectigo Limited
Organizational Unit (OU) : <Not Part Of Certificate>

Validity Period

Issued On : Wednesday, April 19, 2023 at 5:30:00 AM
Expires On : Sunday, March 17, 2024 at 5:29:59 AM

Fingerprints

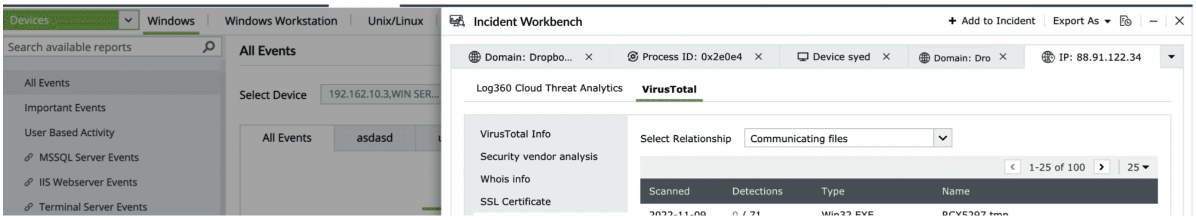
SHA-256 Fingerprint : 14 17 8D 8F 7E 3A FA 5A F0 38 1C 5D 8F CB 5D 32 CA B1 E2 5A AF 2F 90 8A D6 6B B3 4A 16 61 00 8D
SHA-1 Fingerprint : 26 13 BC C9 FB 7E DE D4 EE D8 40 51 F8 15 C1 A2 22 CF 57 A8

```
2022-11-15 11:18:27  ELA
2022-11-15 11:18:27  ELA
2022-11-15 11:18:27  ELA
2022-11-15 11:18:27  ELA
2022-11-15 11:18:27  ELA
2022-11-15 11:18:27  ELA
```

- Related Files

  This section maps the relationship of the files to the IP address in following ways:

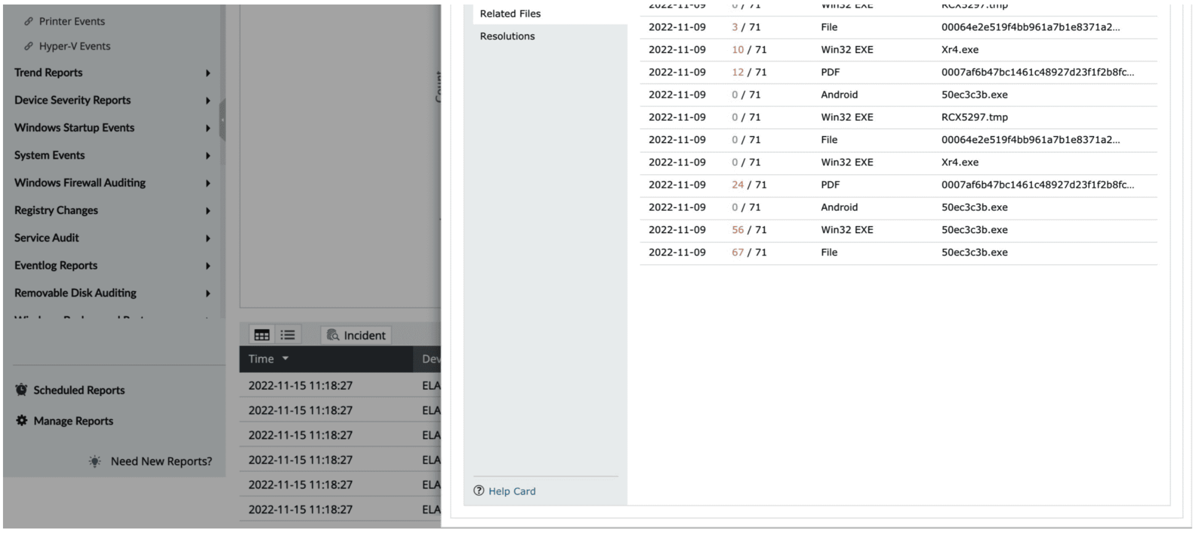
  - Files communicating with the IP address
  - Files downloaded from the IP address
  - Files containing the IP address



Select Relationship: Communicating files

1-25 of 100 | 25

Scanned	Detections	Type	Name
2022-11-09	0 / 71	Win32 EXE	RCX5297.tmp



- Printer Events
- Hyper-V Events
- Trend Reports
- Device Severity Reports
- Windows Startup Events
- System Events
- Windows Firewall Auditing
- Registry Changes
- Service Audit
- Eventlog Reports
- Removable Disk Auditing
- Scheduled Reports
- Manage Reports
- Need New Reports?

Incident

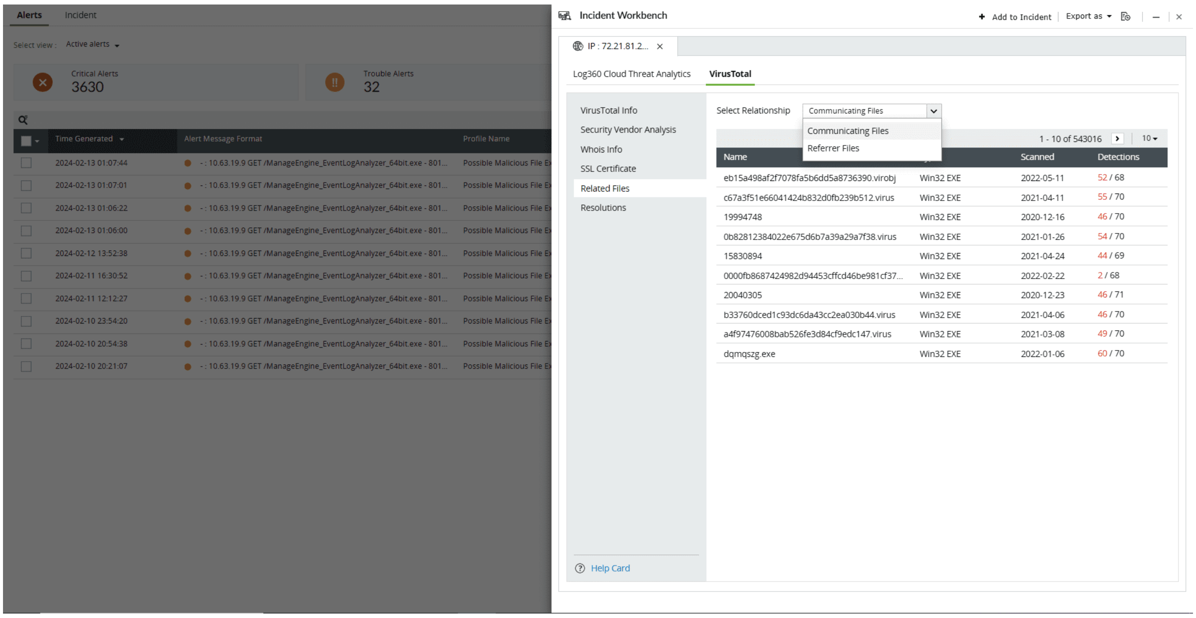
Time	Dev
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA

Related Files

Resolutions

2022-11-09	0 / 71	Win32 EXE	RCX5297.tmp
2022-11-09	3 / 71	File	00064e2e519f4bb961a7b1e8371a2...
2022-11-09	10 / 71	Win32 EXE	Xr4.exe
2022-11-09	12 / 71	PDF	0007af6b47bc1461c48927d23f1f2b8fc...
2022-11-09	0 / 71	Android	50ec3c3b.exe
2022-11-09	0 / 71	Win32 EXE	RCX5297.tmp
2022-11-09	0 / 71	File	00064e2e519f4bb961a7b1e8371a2...
2022-11-09	0 / 71	Win32 EXE	Xr4.exe
2022-11-09	24 / 71	PDF	0007af6b47bc1461c48927d23f1f2b8fc...
2022-11-09	0 / 71	Android	50ec3c3b.exe
2022-11-09	56 / 71	Win32 EXE	50ec3c3b.exe
2022-11-09	67 / 71	File	50ec3c3b.exe

Help Card



Alerts | Incident

Select view : Active alerts

Critical Alerts 3630

Trouble Alerts 32

	Time Generated	Alert Message Format	Profile Name
□	2024-02-13 01:07:44	- : 10.63.19.9 GET /ManageEngine_EventLogAnalyzer_64bit.exe - 801...	Possible Malicious File Ex
□	2024-02-13 01:07:01	- : 10.63.19.9 GET /ManageEngine_EventLogAnalyzer_64bit.exe - 801...	Possible Malicious File Ex
□	2024-02-13 01:06:22	- : 10.63.19.9 GET /ManageEngine_EventLogAnalyzer_64bit.exe - 801...	Possible Malicious File Ex
□	2024-02-13 01:06:00	- : 10.63.19.9 GET /ManageEngine_EventLogAnalyzer_64bit.exe - 801...	Possible Malicious File Ex
□	2024-02-12 13:52:38	- : 10.63.19.9 GET /ManageEngine_EventLogAnalyzer_64bit.exe - 801...	Possible Malicious File Ex
□	2024-02-11 16:30:52	- : 10.63.19.9 GET /ManageEngine_EventLogAnalyzer_64bit.exe - 801...	Possible Malicious File Ex
□	2024-02-11 12:12:27	- : 10.63.19.9 GET /ManageEngine_EventLogAnalyzer_64bit.exe - 801...	Possible Malicious File Ex
□	2024-02-10 23:54:20	- : 10.63.19.9 GET /ManageEngine_EventLogAnalyzer_64bit.exe - 801...	Possible Malicious File Ex
□	2024-02-10 20:54:38	- : 10.63.19.9 GET /ManageEngine_EventLogAnalyzer_64bit.exe - 801...	Possible Malicious File Ex
□	2024-02-10 20:21:07	- : 10.63.19.9 GET /ManageEngine_EventLogAnalyzer_64bit.exe - 801...	Possible Malicious File Ex

Incident Workbench

Add to Incident | Export as

IP : 72.21.81.2...

Log360 Cloud Threat Analytics | VirusTotal

- VirusTotal Info
- Security Vendor Analysis
- Whois Info
- SSL Certificate
- Related Files
- Resolutions

Select Relationship: Communicating Files

- Communicating Files
- Referrer Files

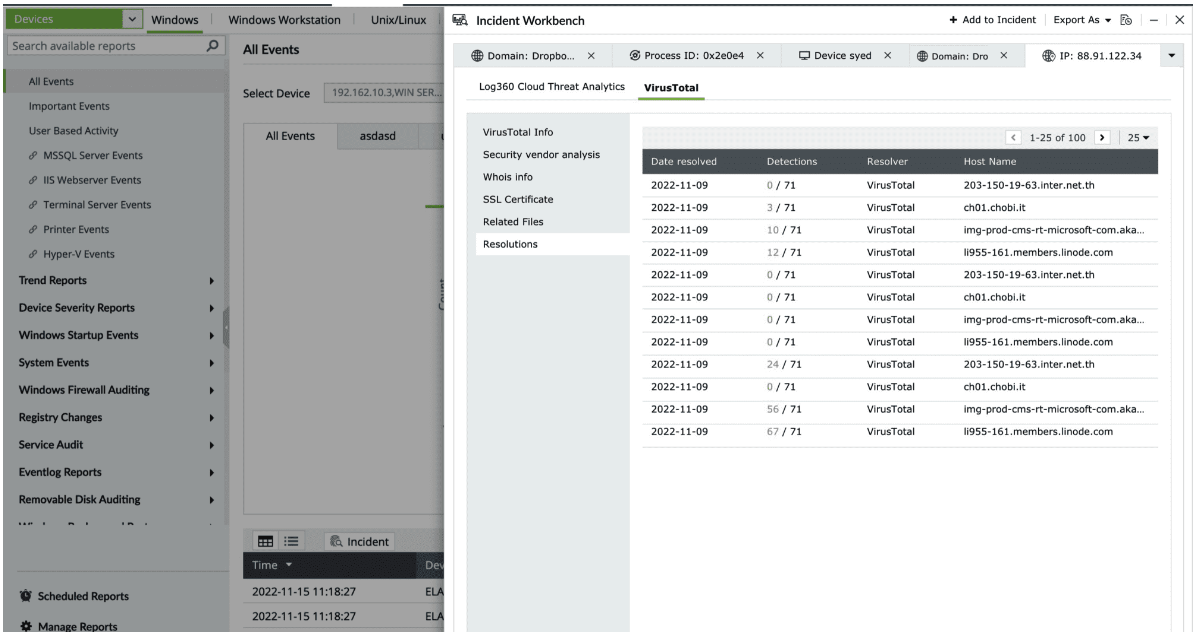
1 - 10 of 543016 | 10

Name		Scanned	Detections
eb15a498af2f7078fa5b6dd5a8736390.virobj	Win32 EXE	2022-05-11	52 / 68
c67a3f51e66041424b832d0fb239b512.virus	Win32 EXE	2021-04-11	55 / 70
19994748	Win32 EXE	2020-12-16	46 / 70
0b82812384022e675d6b7a39a29a7f38.virus	Win32 EXE	2021-01-26	54 / 70
15830894	Win32 EXE	2021-04-24	44 / 69
0000fb8687424982d94453cffcd46be981cf37...	Win32 EXE	2022-02-22	2 / 68
20040305	Win32 EXE	2020-12-23	46 / 71
b33760dced1c93dc6da43cc2ea030b44.virus	Win32 EXE	2021-04-06	46 / 70
a4f97476008bab526fe3d84cf9edc147.virus	Win32 EXE	2021-03-08	49 / 70
dqmqszg.exe	Win32 EXE	2022-01-06	60 / 70

Help Card

- Resolutions

  This section contains the past and current IP resolutions for a particular domain.



Devices | Windows | Windows Workstation | Unix/Linux

Search available reports

- All Events
- Important Events
- User Based Activity
- MSSQL Server Events
- IIS Webserver Events
- Terminal Server Events
- Printer Events
- Hyper-V Events
- Trend Reports
- Device Severity Reports
- Windows Startup Events
- System Events
- Windows Firewall Auditing
- Registry Changes
- Service Audit
- Eventlog Reports
- Removable Disk Auditing
- Scheduled Reports
- Manage Reports

All Events

Select Device: 192.162.10.3,WIN SER...

All Events | asdasd

Incident

Time	Dev
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA

Incident Workbench

Add to Incident | Export As

Domain: Dropbo... | Process ID: 0x2e0e4 | Device syed | Domain: Dro | IP: 88.91.122.34

Log360 Cloud Threat Analytics | VirusTotal

- VirusTotal Info
- Security vendor analysis
- Whois info
- SSL Certificate
- Related Files
- Resolutions

1-25 of 100 | 25

Date resolved	Detections	Resolver	Host Name
2022-11-09	0 / 71	VirusTotal	203-150-19-63.inter.net.th
2022-11-09	3 / 71	VirusTotal	ch01.chobi.it
2022-11-09	10 / 71	VirusTotal	img-prod-cms-rt-microsoft-com.aka...
2022-11-09	12 / 71	VirusTotal	li955-161.members.linode.com
2022-11-09	0 / 71	VirusTotal	203-150-19-63.inter.net.th
2022-11-09	0 / 71	VirusTotal	ch01.chobi.it
2022-11-09	0 / 71	VirusTotal	img-prod-cms-rt-microsoft-com.aka...
2022-11-09	0 / 71	VirusTotal	li955-161.members.linode.com
2022-11-09	24 / 71	VirusTotal	203-150-19-63.inter.net.th
2022-11-09	0 / 71	VirusTotal	ch01.chobi.it
2022-11-09	56 / 71	VirusTotal	img-prod-cms-rt-microsoft-com.aka...
2022-11-09	67 / 71	VirusTotal	li955-161.members.linode.com

Need New Reports?

2022-11-15 11:18:27 ELA
2022-11-15 11:18:27 ELA
2022-11-15 11:18:27 ELA
2022-11-15 11:18:27 ELA

4.1.5.4. Constella Intelligence

Last updated on: September 12, 2025

In this page

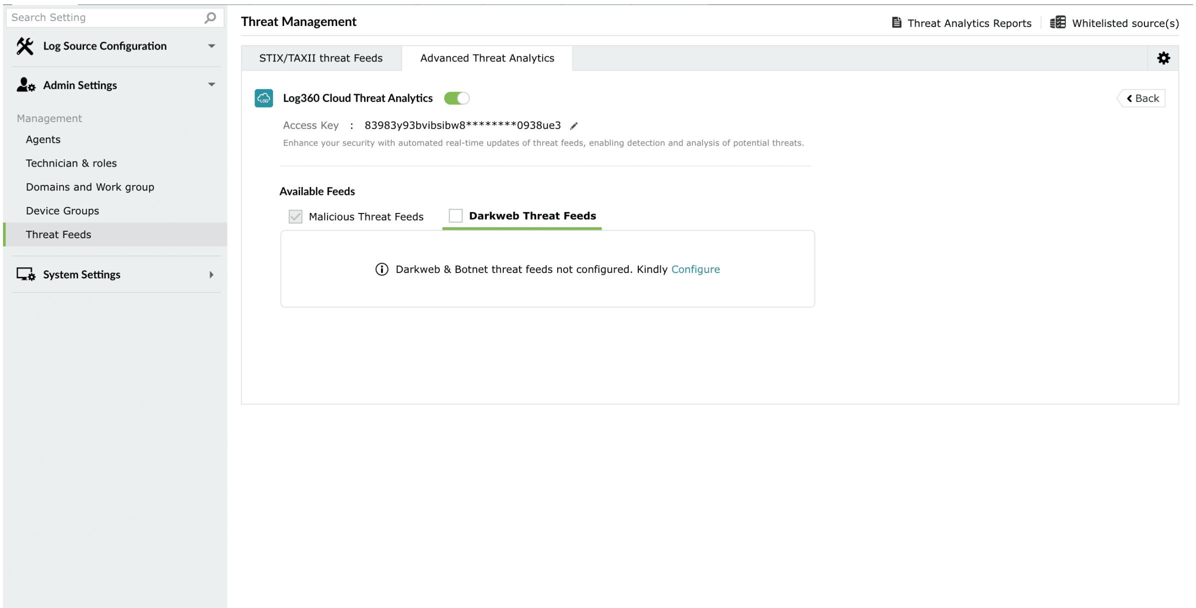
Constella Intelligence is a digital risk protection platform that provides dark web monitoring. This integration with EventLog Analyzer enables users to identify personal information such as credit card number, email information, usernames and credentials that are leaked in the dark web. Users can also

- 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.



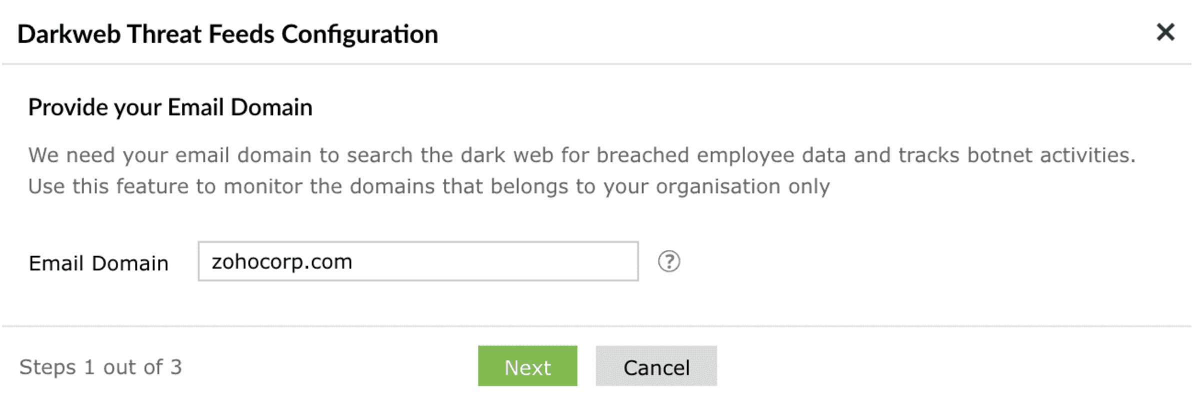
Access Key : 83983y93bvibsibw8********0938ue3

Enhance your security with automated real-time updates of threat feeds, enabling detection and analysis of potential threats.

☑ Malicious Threat Feeds ☐ Darkweb Threat Feeds

Darkweb & Botnet threat feeds not configured. Kindly Configure

- 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.



Darkweb Threat Feeds Configuration

Provide your Email Domain

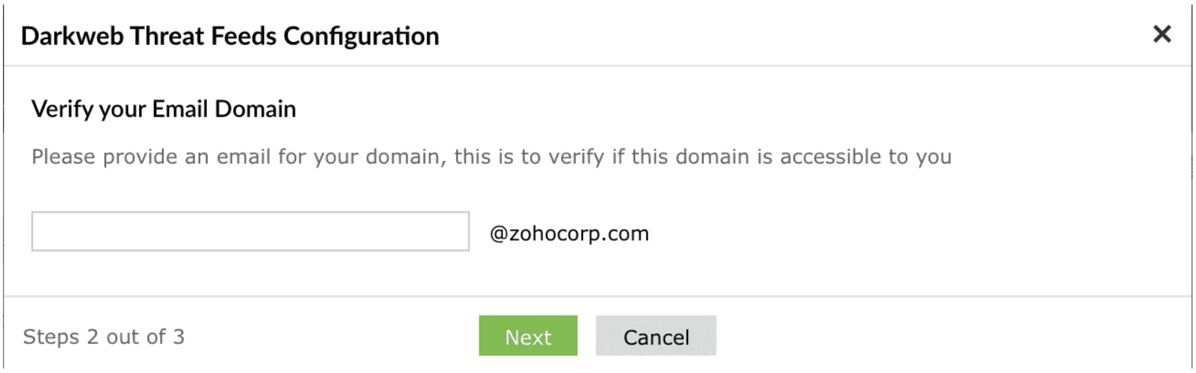
We need your email domain to search the dark web for breached employee data and tracks botnet activities. Use this feature to monitor the domains that belongs to your organisation only

Email Domain: zohocorp.com

Steps 1 out of 3

Note

Domain configuration for email is linked to licensing. You can only configure domains associated with licenses you have purchased.



Darkweb Threat Feeds Configuration

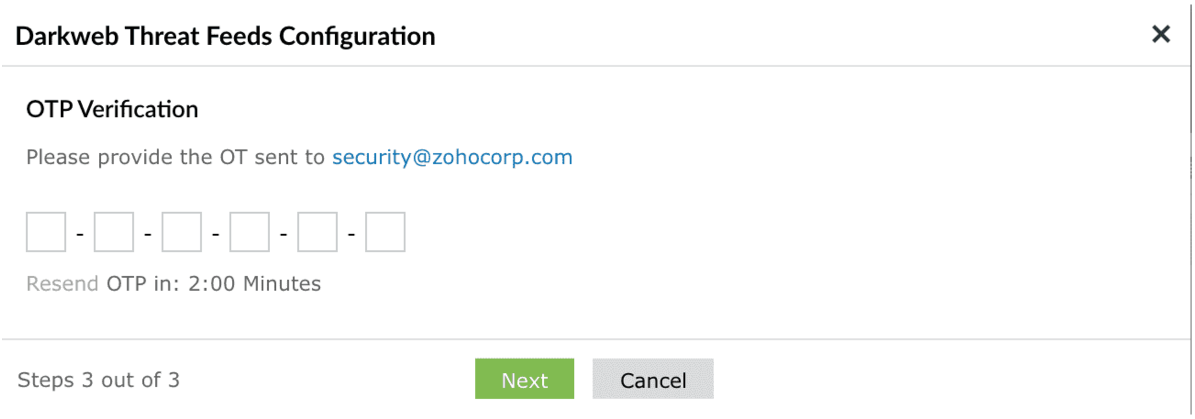
Verify your Email Domain

Please provide an email for your domain, this is to verify if this domain is accessible to you

@zohocorp.com

Steps 2 out of 3

- 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.



Darkweb Threat Feeds Configuration

OTP Verification

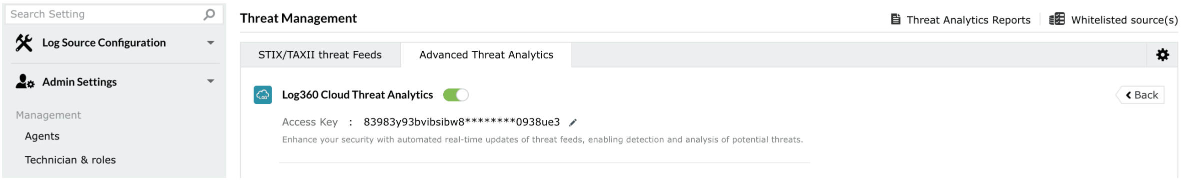
Please provide the OT sent to security@zohocorp.com

□ - □ - □ - □ - □ - □

Resend OTP in: 2:00 Minutes

Steps 3 out of 3

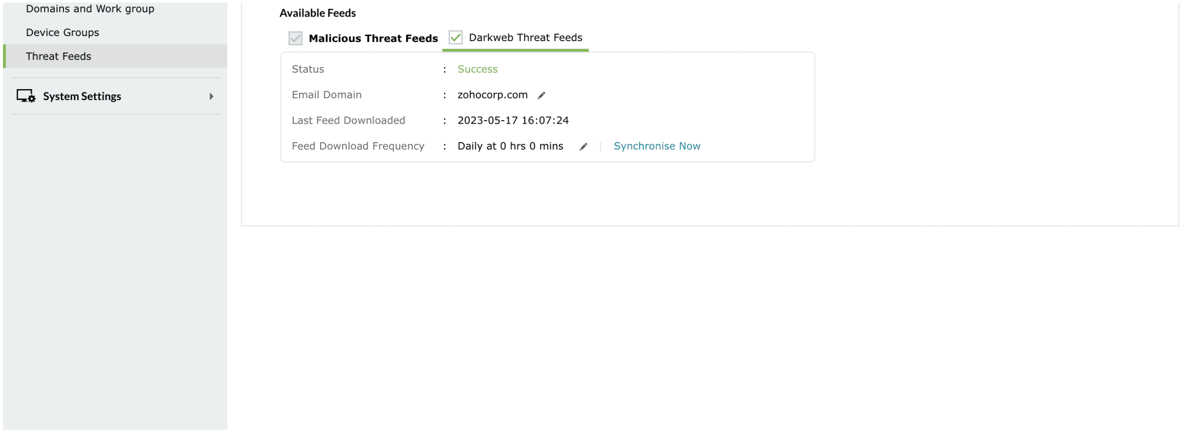
- You will see this page once your domain is successfully configured.



Log360 Cloud Threat Analytics

Access Key : 83983y93bvibsibw8********0938ue3

Enhance your security with automated real-time updates of threat feeds, enabling detection and analysis of potential threats.



Available Feeds

☐ Malicious Threat Feeds ☑ Darkweb Threat Feeds

Status : Success

Email Domain : zohocorp.com

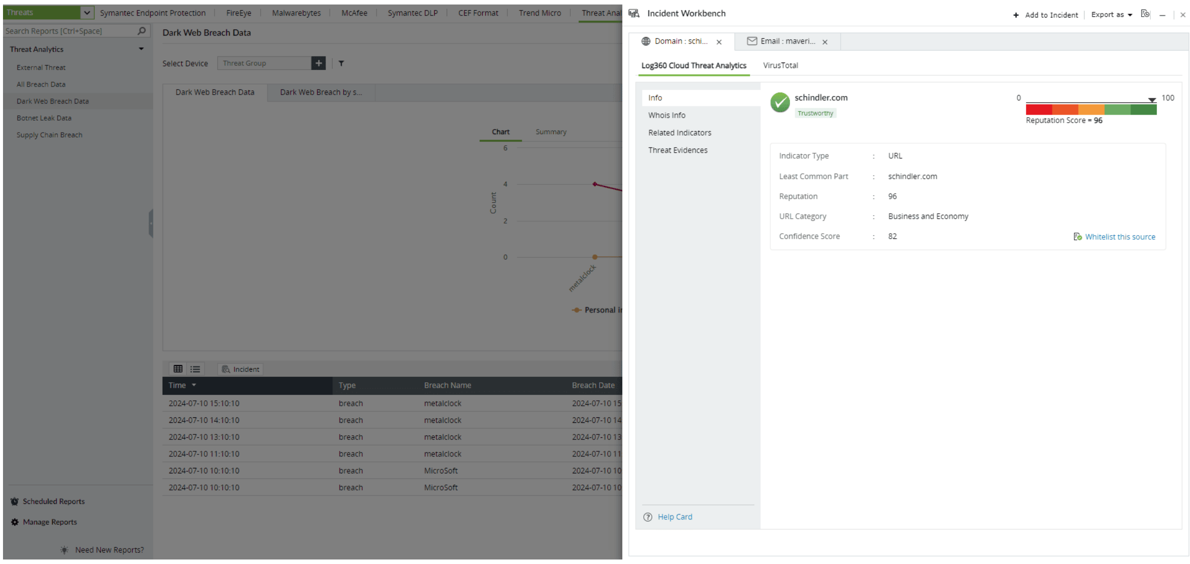
Last Feed Downloaded : 2023-05-17 16:07:24

Feed Download Frequency : Daily at 0 hrs 0 mins

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



Time	Type	Breach Name	Breach Date
2024-07-10 15:10:10	breach	metalclock	2024-07-10 15
2024-07-10 14:10:10	breach	metalclock	2024-07-10 14
2024-07-10 13:10:10	breach	metalclock	2024-07-10 13
2024-07-10 11:10:10	breach	metalclock	2024-07-10 11
2024-07-10 10:10:10	breach	MicroSoft	2024-07-10 10
2024-07-10 10:10:10	breach	MicroSoft	2024-07-10 10

schindler.com

Trustworthy

Reputation Score = 96

Indicator Type : URL

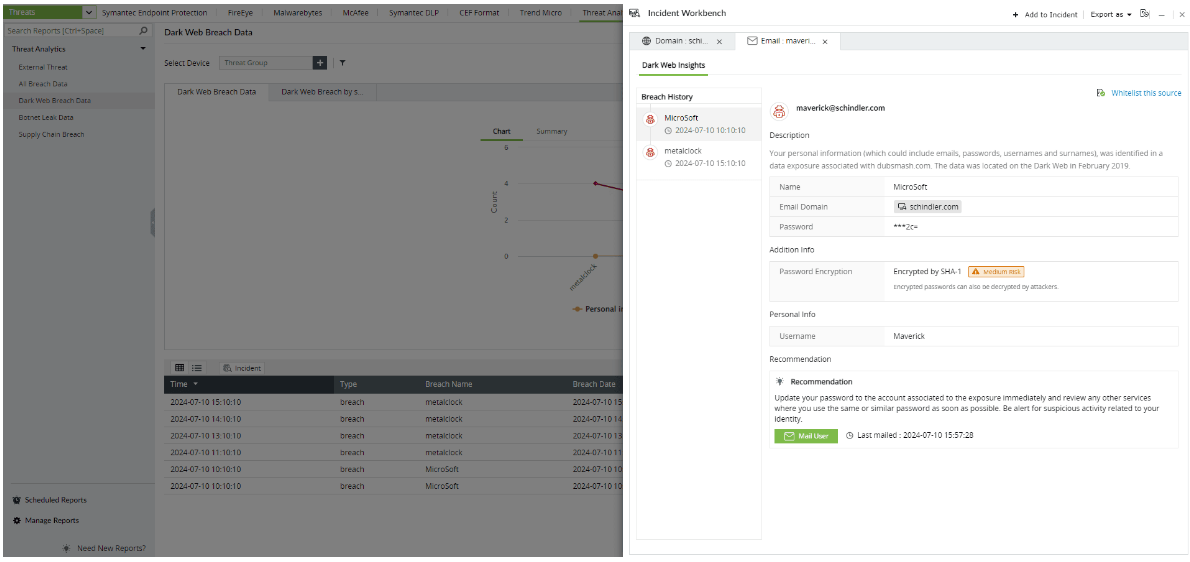
Least Common Part : schindler.com

Reputation : 96

URL Category : Business and Economy

Confidence Score : 82

- Email analysis for the configured domain



Time	Type	Breach Name	Breach Date
2024-07-10 15:10:10	breach	metalclock	2024-07-10 15
2024-07-10 14:10:10	breach	metalclock	2024-07-10 14
2024-07-10 13:10:10	breach	metalclock	2024-07-10 13
2024-07-10 11:10:10	breach	metalclock	2024-07-10 11
2024-07-10 10:10:10	breach	MicroSoft	2024-07-10 10
2024-07-10 10:10:10	breach	MicroSoft	2024-07-10 10

Breach History

MicroSoft 2024-07-10 10:10:10

metalclock 2024-07-10 15:10:10

maverick@schindler.com

Description

Your personal information (which could include emails, passwords, usernames and surnames), was identified in a data exposure associated with dubsmash.com. The data was located on the Dark Web in February 2019.

Name	MicroSoft
Email Domain	schindler.com
Password	***2c=

Addition Info

Password Encryption	Encrypted by SHA-1 ⚠ Medium Risk Encrypted passwords can also be decrypted by attackers.

Personal Info

Username	Maverick

Recommendation

Recommendation

Update your password to the account associated to the exposure immediately and review any other services where you use the same or similar password as soon as possible. Be alert for suspicious activity related to your identity.

Last mailed : 2024-07-10 15:57:28

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

4.1.5.5. Threat Whitelisting

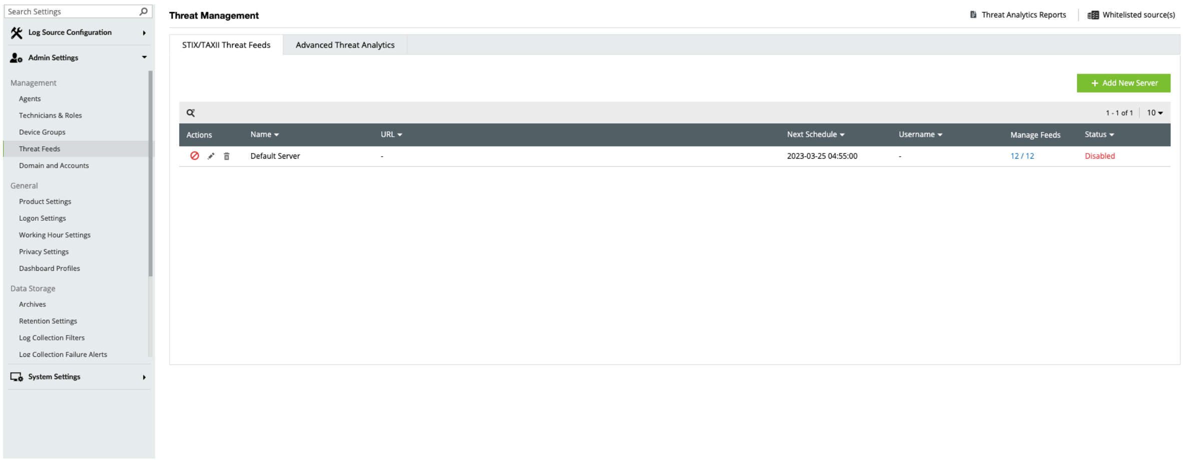
Last updated on: September 12, 2025

In this page

Threat whitelisting helps you to specify an index of approved IPs, URLs, and Domains.

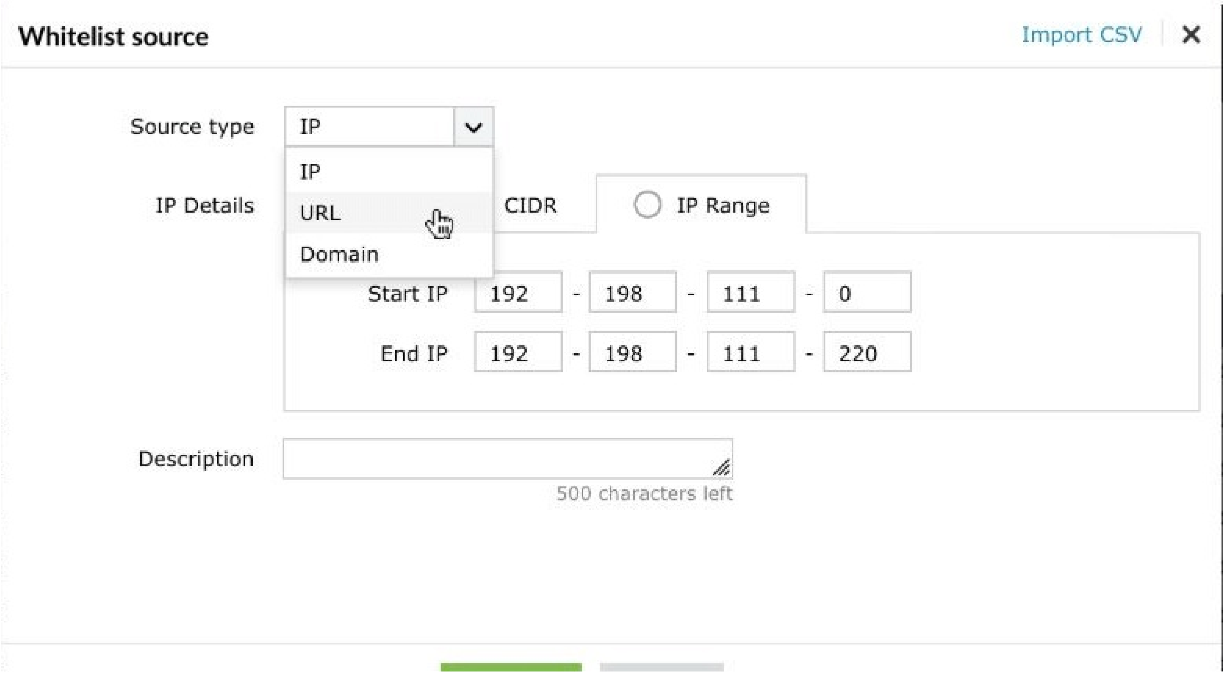
How to whitelist a new source?

- Navigate to Settings > Admin Settings > Threat Feeds > Whitelisted Sources.
- Click the Whitelist Source option. (top right corner of Threat Feeds page).



Actions	Name	URL	Next Schedule	Username	Manage Feeds	Status
	Default Server	-	2023-03-25 04:55:00	-	12 / 12	Disabled

- Select the source type from the drop-down list.



Source type: IP

IP Details: ○ IP Range

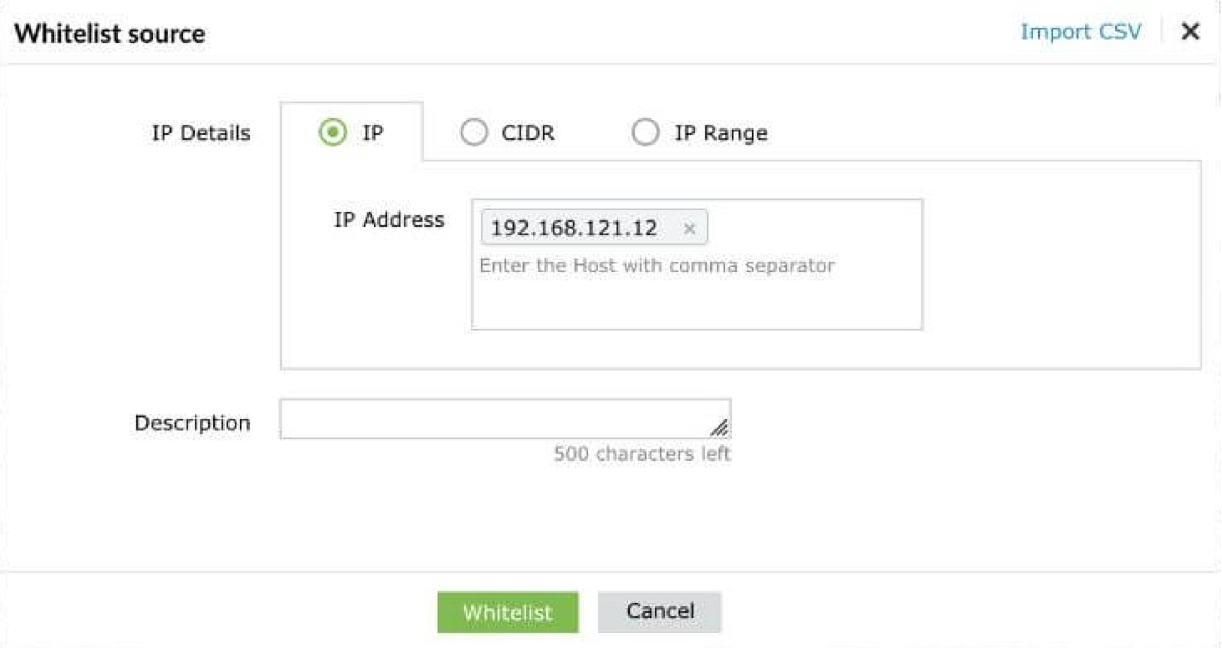
Start IP: 192 - 198 - 111 - 0

End IP: 192 - 198 - 111 - 220

Description:

IP Details

The value(s) entered should either be an IP address, CIDR, or an IP Range.

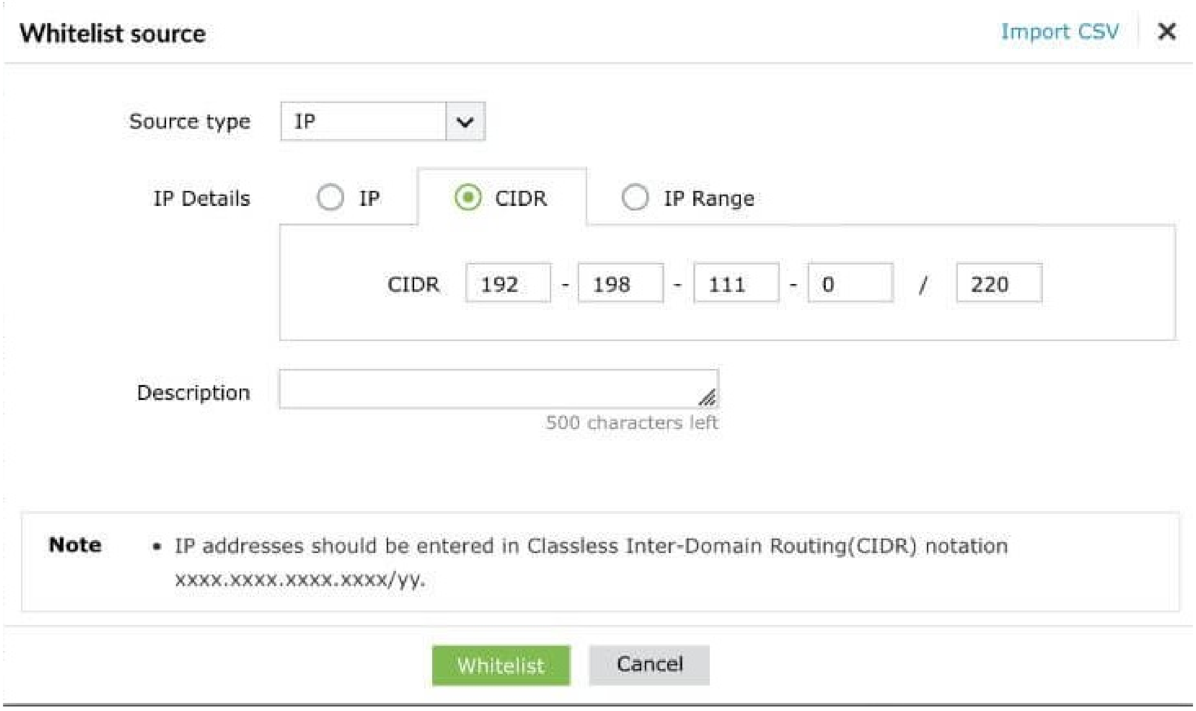


IP Details ● IP ○ CIDR ○ IP Range

IP Address: 192.168.121.12 ×

Description:

- The CIDR value can be entered using the '/' symbol. For instance, 192-198-111-0/220.



Source type: IP

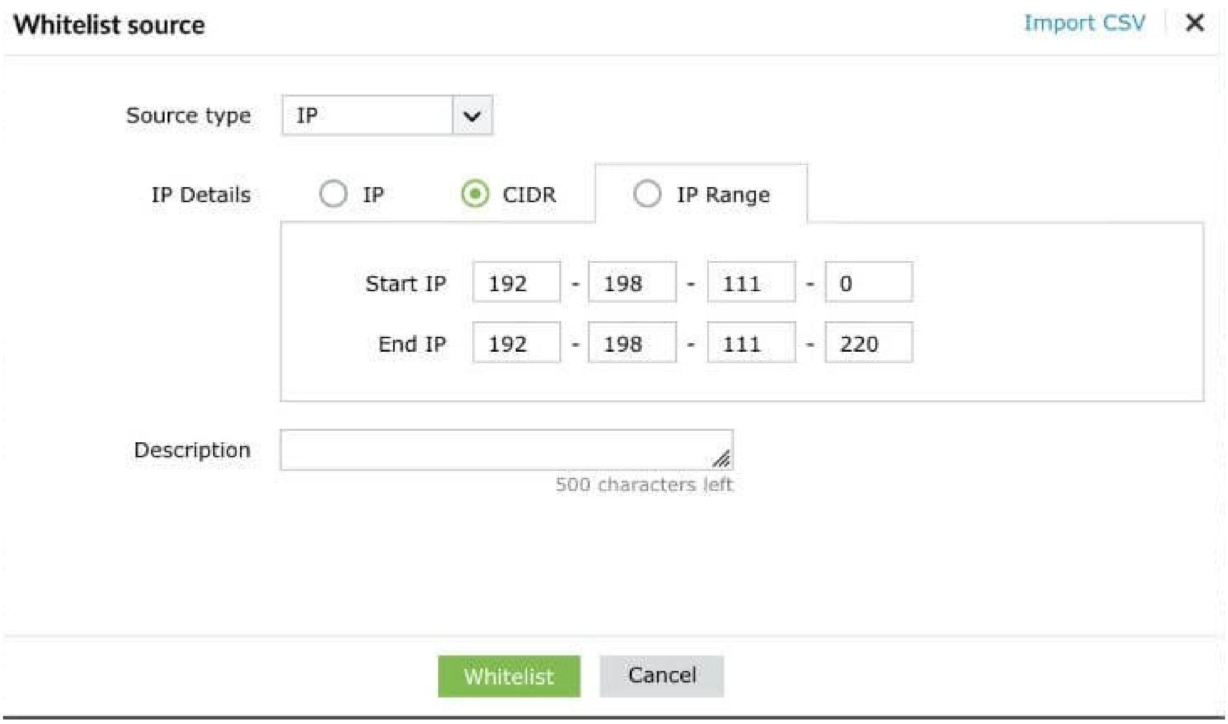
IP Details ○ IP ● CIDR ○ IP Range

CIDR 192 - 198 - 111 - 0 / 220

Description:

Note
- IP addresses should be entered in Classless Inter-Domain Routing(CIDR) notation xxxx.xxxx.xxxx.xxxx/yy.

- 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.



Whitelist source

Import CSV | ✕

Source type: IP

IP Details: ○ IP ● CIDR ○ IP Range

Start IP: 192 - 198 - 111 - 0

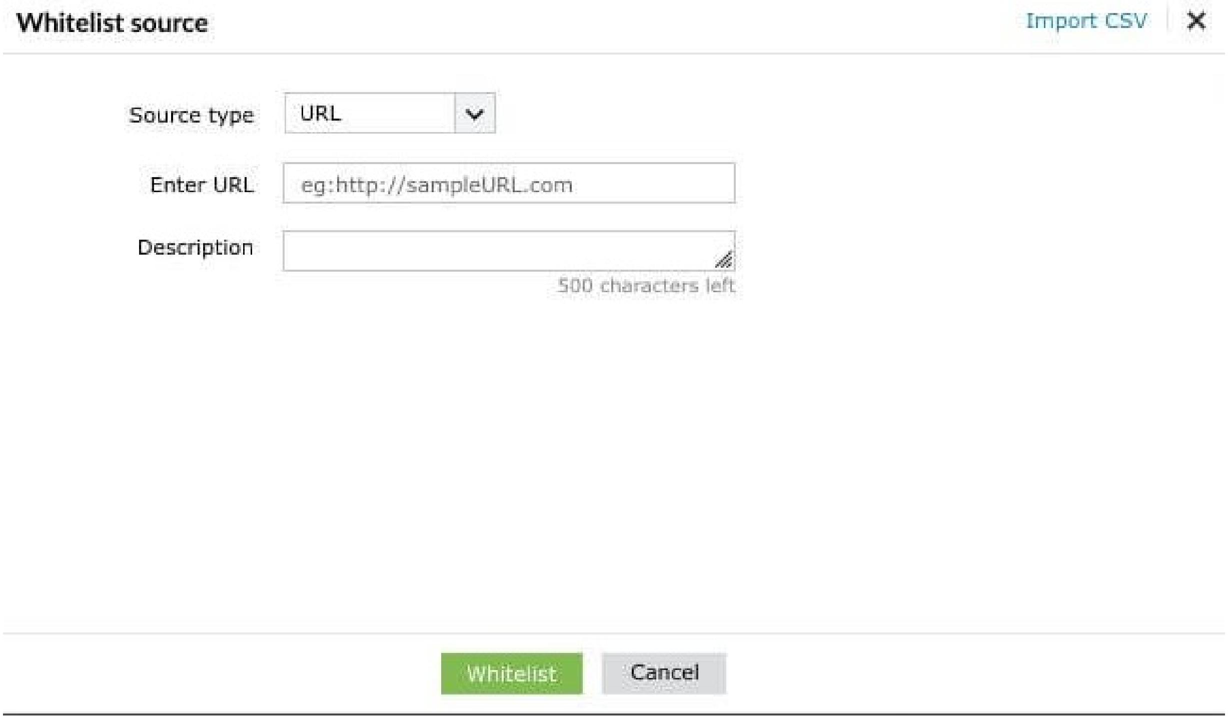
End IP: 192 - 198 - 111 - 220

Description:

500 characters left

URL

The URL can be whitelisted by mentioning the address in the text box. For instance, http://sampleURL.com



Whitelist source

Import CSV | ✕

Source type: URL

Enter URL: eg:http://sampleURL.com

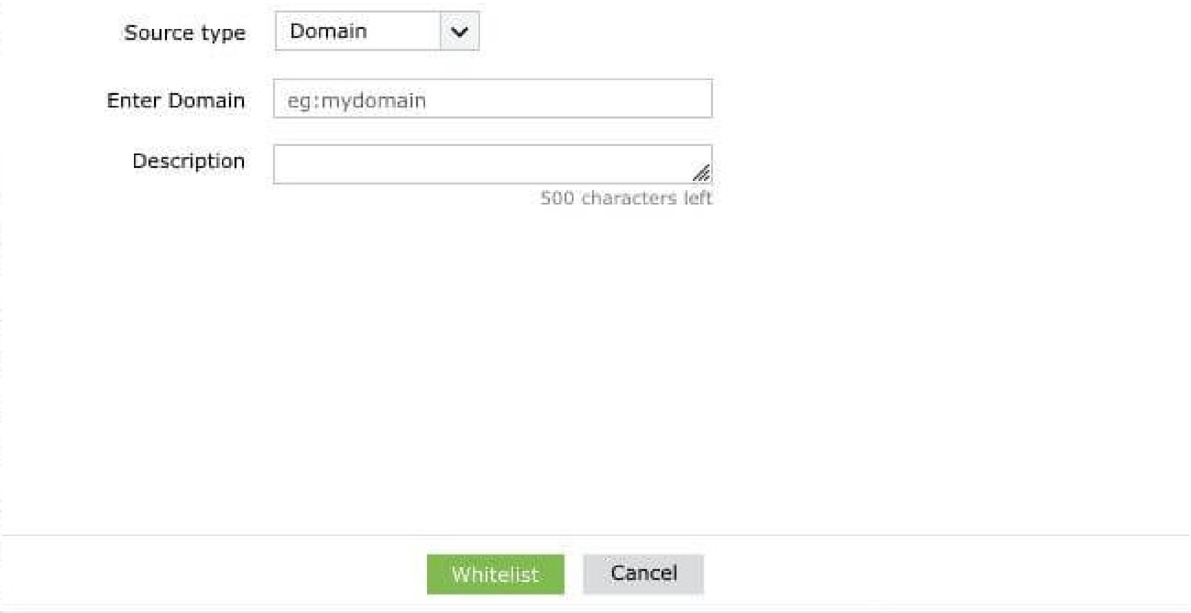
Description:

500 characters left

Domain

- A domain can be whitelisted by mentioning the domain address. For instance, 'mydomain'.

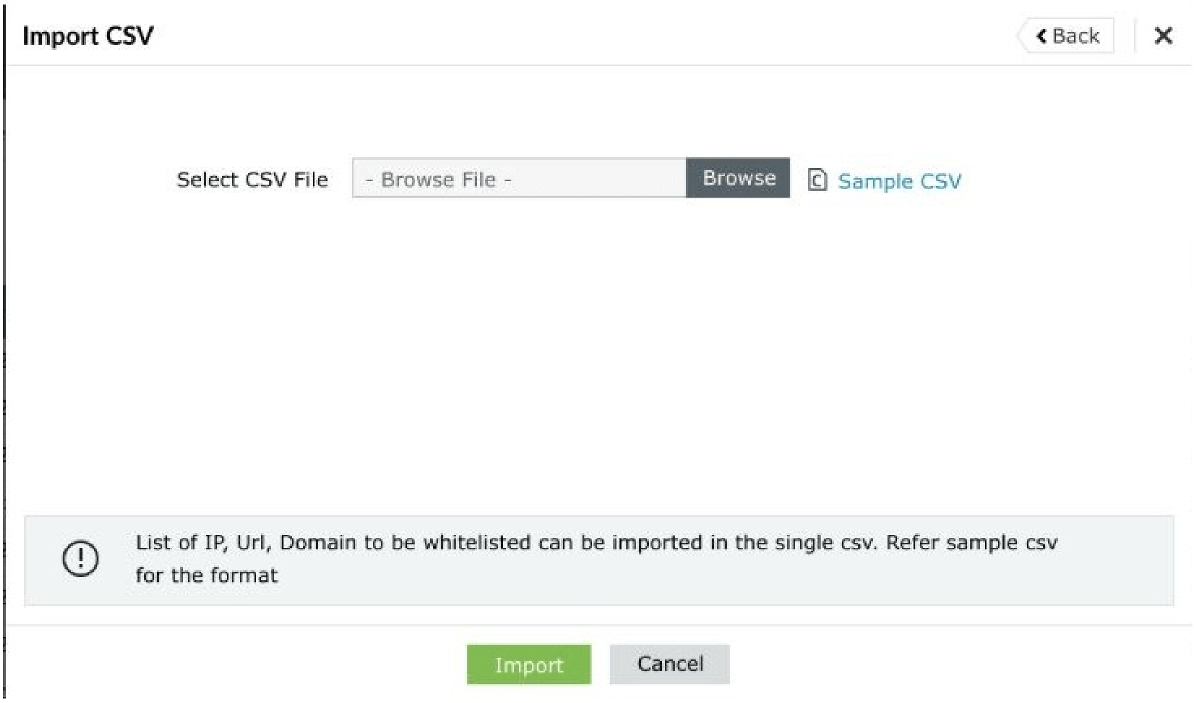
Whitelist source



- 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.



List of IP, Url, Domain to be whitelisted can be imported in the single csv. Refer sample csv for the format

- Refer the sample CSV for the file format.

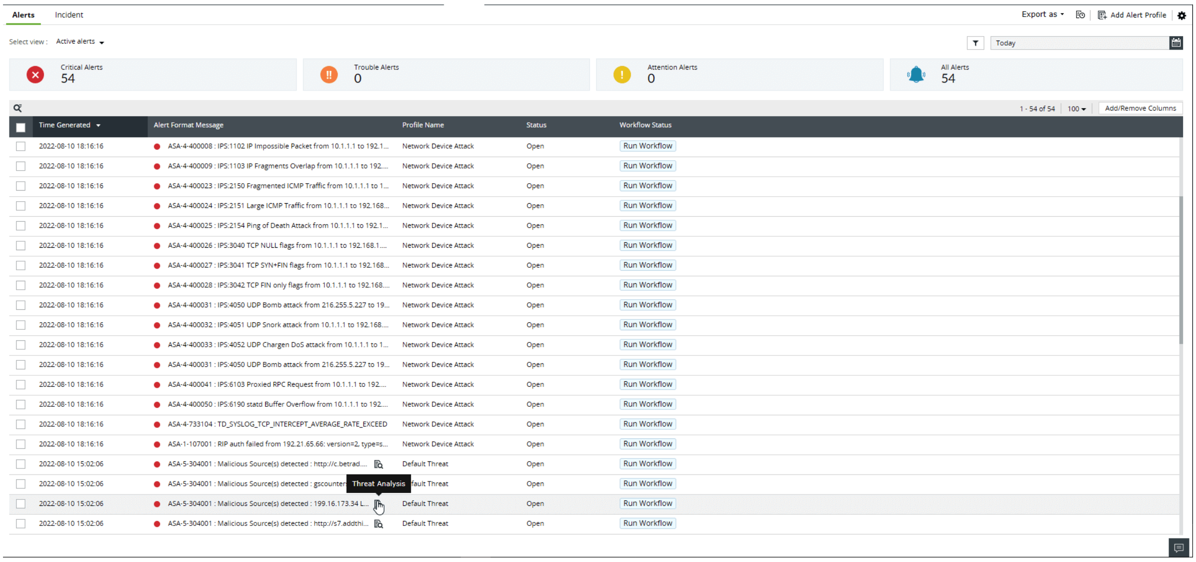
> Note
>
> Only CSV files are supported.

- 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

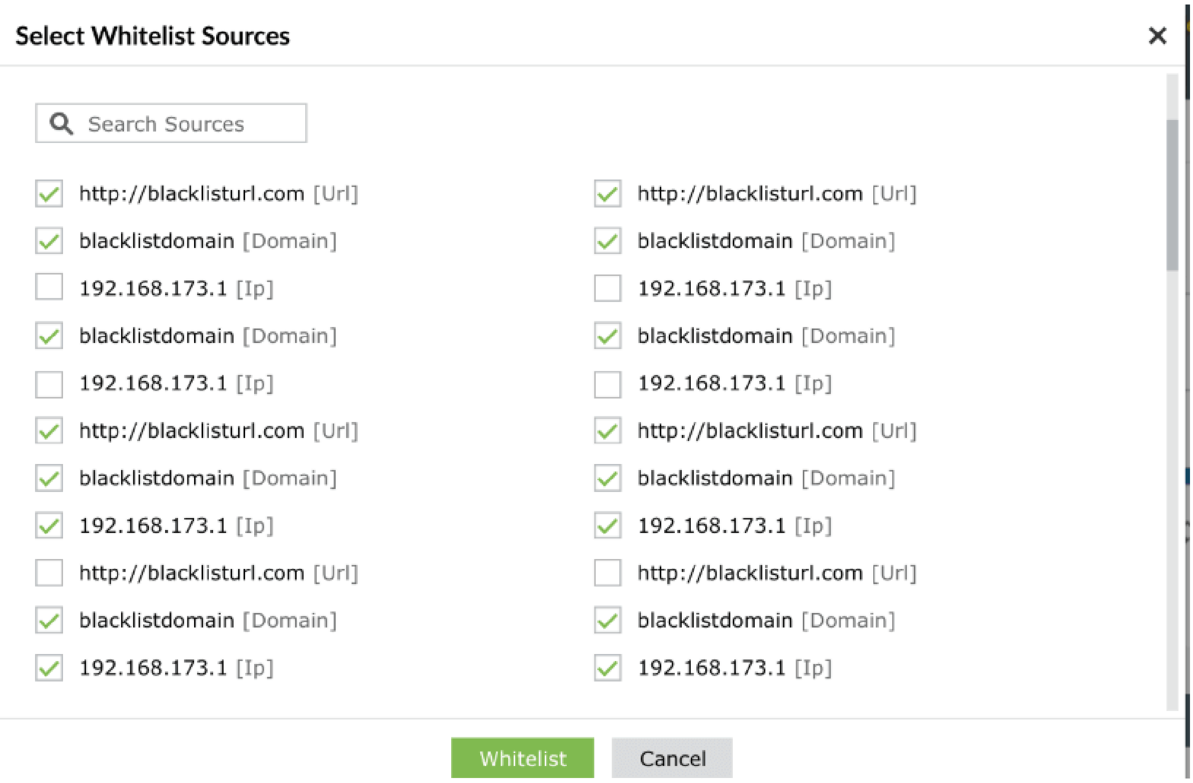
Threat Whitelisting has been integrated with Advanced Threat Analytics with the aim of reducing false positive alerts.

- Navigate to Alerts > Threat Alerts.



□	Time Generated	Alert Format Message	Profile Name	Status	Workflow Status
□	2022-08-10 18:16:16	● ASA-4-400008 : IPS:1102 IP Impossible Packet from 10.1.1.1 to 192.1...	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400009 : IPS:1103 IP Fragments Overlap from 10.1.1.1 to 192....	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400023 : IPS:2150 Fragmented ICMP Traffic from 10.1.1.1 to 1...	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400024 : IPS:2151 Large ICMP Traffic from 10.1.1.1 to 192.168...	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400025 : IPS:2154 Ping of Death Attack from 10.1.1.1 to 192.1...	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400026 : IPS:3040 TCP NULL flags from 10.1.1.1 to 192.168.1....	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400027 : IPS:3041 TCP SYN+FIN flags from 10.1.1.1 to 192.168...	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400028 : IPS:3042 TCP FIN only flags from 10.1.1.1 to 192.168....	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400031 : IPS:4050 UDP Bomb attack from 216.255.5.227 to 19...	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400032 : IPS:4051 UDP Snork attack from 10.1.1.1 to 192.168....	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400033 : IPS:4052 UDP Chargen DoS attack from 10.1.1.1 to 1...	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400031 : IPS:4050 UDP Bomb attack from 216.255.5.227 to 19...	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400041 : IPS:6103 Proxied RPC Request from 10.1.1.1 to 192....	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-400050 : IPS:6190 statd Buffer Overflow from 10.1.1.1 to 192....	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-4-733104 : TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED	Network Device Attack	Open	Run Workflow
□	2022-08-10 18:16:16	● ASA-1-107001 : RIP auth failed from 192.21.65.66: version=2, type=s...	Network Device Attack	Open	Run Workflow
□	2022-08-10 15:02:06	● ASA-5-304001 : Malicious Source(s) detected : http://c.betrad....	Default Threat	Open	Run Workflow
□	2022-08-10 15:02:06	● ASA-5-304001 : Malicious Source(s) detected : gscounter	fault Threat	Open	Run Workflow
□	2022-08-10 15:02:06	● ASA-5-304001 : Malicious Source(s) detected : 199.16.173.34 L...	Default Threat	Open	Run Workflow
□	2022-08-10 15:02:06	● ASA-5-304001 : Malicious Source(s) detected : http://s7.addthi...	Default Threat	Open	Run Workflow

- 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.



☑ http://blacklisturl.com [Url]
☑ blacklistdomain [Domain]
□ 192.168.173.1 [Ip]
☑ blacklistdomain [Domain]
□ 192.168.173.1 [Ip]
☑ http://blacklisturl.com [Url]
☑ blacklistdomain [Domain]
☑ 192.168.173.1 [Ip]
□ http://blacklisturl.com [Url]
☑ blacklistdomain [Domain]
☑ 192.168.173.1 [Ip]

☑ http://blacklisturl.com [Url]
☑ blacklistdomain [Domain]
□ 192.168.173.1 [Ip]
☑ blacklistdomain [Domain]
□ 192.168.173.1 [Ip]
☑ http://blacklisturl.com [Url]
☑ blacklistdomain [Domain]
☑ 192.168.173.1 [Ip]
□ http://blacklisturl.com [Url]
☑ blacklistdomain [Domain]
☑ 192.168.173.1 [Ip]

- 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.

4.1.5.6. Threat Import

Last updated on: September 12, 2025

In this page

Threat import lets you import threat feed data into EventLog Analyzer from CSV files. This will help users to add any third-party threat data easily, and EventLog Analyzer processes the threat feed data present in the files for threat alerting.

> Note
>
> The CSV files should contain the list of threat sources in the first column. Download sample CSV file.

How to add files for Threat Import

- If you need to add Threat Sources for threat alerting, place the files in the <Dir>\EventLog Analyzer\data\za\threatfeeds\ThreatImport\Import folder.
- Files in the ThreatImport directory will be deleted once it is processed. If any files are not deleted, this may indicate that an exception has occurred. Check the log file for details and contact support at eventloganalyzer-support@manageengine.com for further assistance.

> Note
>
> If you need to remove any Threat Sources from flagging threat alerts, place the file containing the Threat Feeds to be removed in <Dir>\EventLog Analyzer\data\za\threatfeeds\ThreatImport\Delete folder.

Scheduling Threat Import

- Scheduling helps users import Threat data from files at the specified location automatically on a daily basis. This ensures that threat feeds are consistently updated and stay current. A threat Import schedule can be enabled by changing the threat.import.schedule.enable property in <dir>\EventLog Analyzer\conf\EventLogAnalyzer\threat folder\threatstore.properties file from "false" to "true".
- A schedule will run everyday at 8:00 AM to process the files placed under respective ThreatImport folder.

- Users can disable the threat schedule by changing the value of threat.import.schedule.enable property key from <dir>\EventLog Analyzer\conf\EventLogAnalyzer\threat folder\threatstore.properties file back to "false".
- If the threat.import.schedule.enable property key value changes from "false" to "true", the product must be restarted.
- Restarting the product will trigger the threat import operation immediately instead of waiting for the 8.00 AM schedule.
- You can find entries related to the threat Import feature in the product log file by searching for ThreatImportHandler.

4.1.5.7. Switching threat stores

Last updated on: September 12, 2025

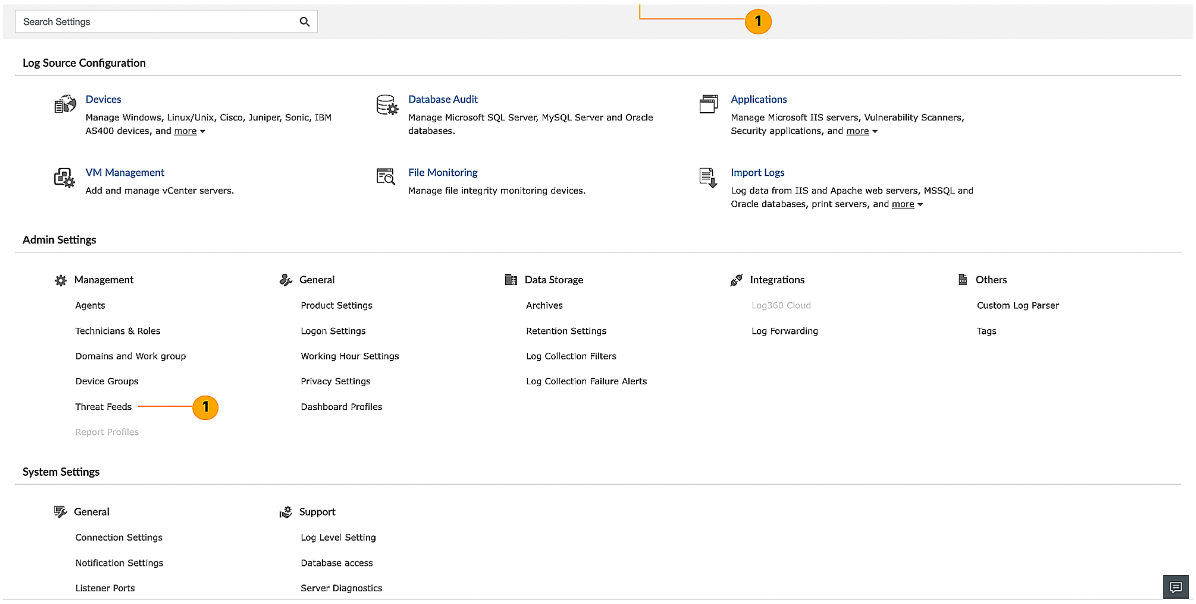
In this page

- How to whitelist a new source?
- Threat Alerting

To switch between the two threat storage (in-memory threat storage and disk-based threat storage) available in EventLog Analyzer, please follow the steps given below.

> Note
>
> - In-memory threat store requirements: The in-memory threat storage requires a minimum of 2 GB RAM to be allocated to EventLog Analyzer; of which at least 512 MB should be available for use.
> - Switching to in-memory threat storage is not possible in 32-bit systems.

1. Go to Settings → Admin Settings → Management → Threat Feeds.



Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more

Manage Microsoft SQL Server, MySQL Server and Oracle databases.

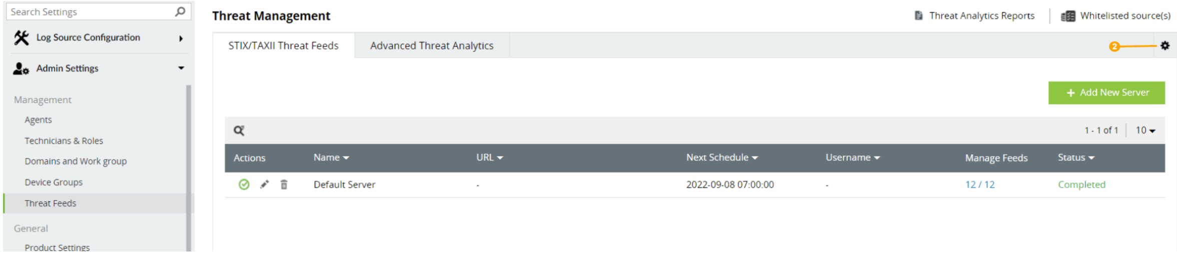
Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more

Add and manage vCenter servers.

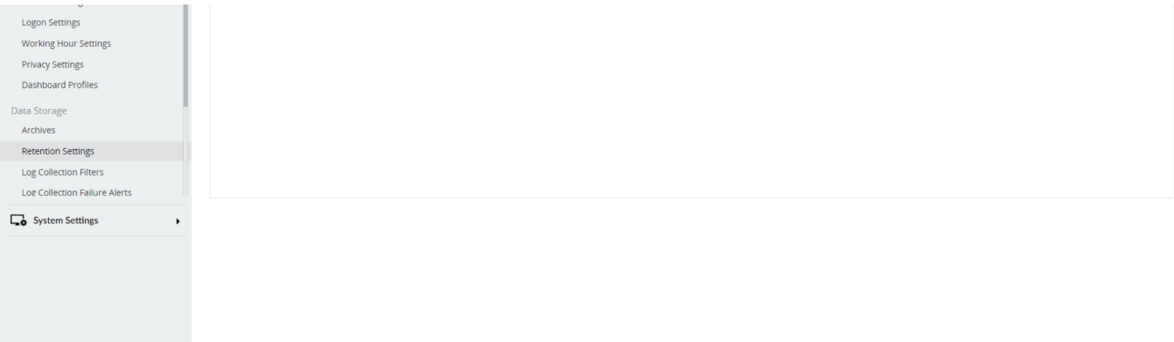
Manage file integrity monitoring devices.

Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more

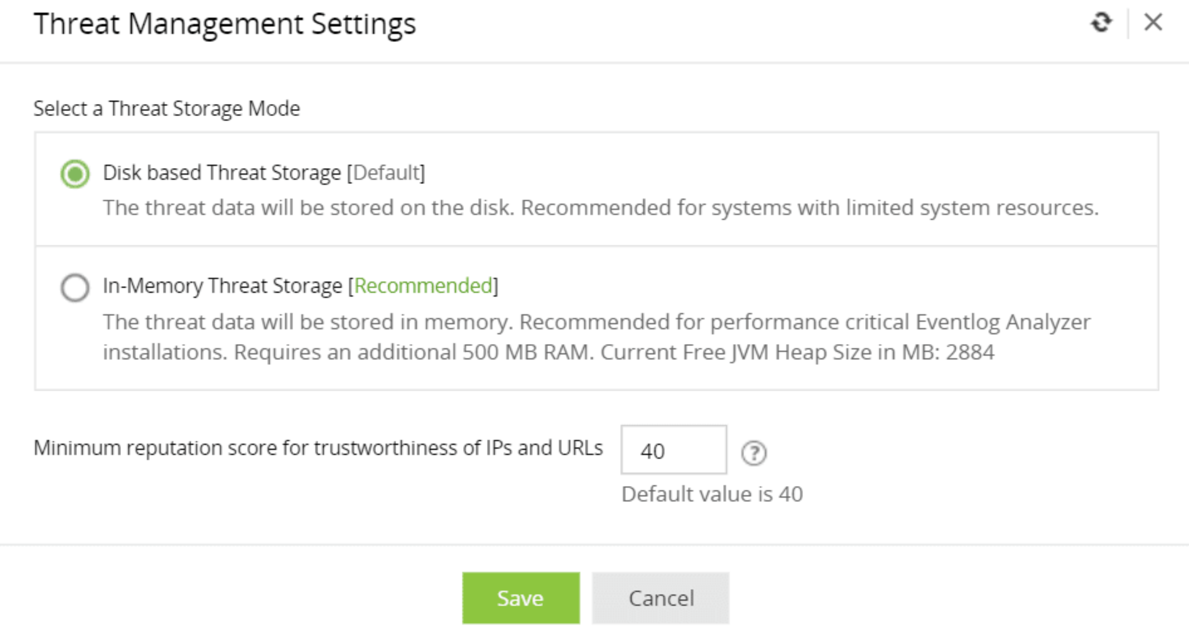
2. Under Threat Feeds sub section, click on Settings icon on the top right corner.



Actions	Name	URL	Next Schedule	Username	Manage Feeds	Status
✓	Default Server	-	2022-09-08 07:00:00	-	12 / 12	Completed



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.



Threat Management Settings

Select a Threat Storage Mode

● Disk based Threat Storage [Default]
The threat data will be stored on the disk. Recommended for systems with limited system resources.

○ In-Memory Threat Storage [Recommended]
The threat data will be stored in memory. Recommended for performance critical Eventlog Analyzer installations. Requires an additional 500 MB RAM. Current Free JVM Heap Size in MB: 2884

Minimum reputation score for trustworthiness of IPs and URLs: 40
Default value is 40

4.1.5.8. Integrating and using the MITRE ATT&CK framework with EventLog Analyzer

Last updated on: September 12, 2025

In this page

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

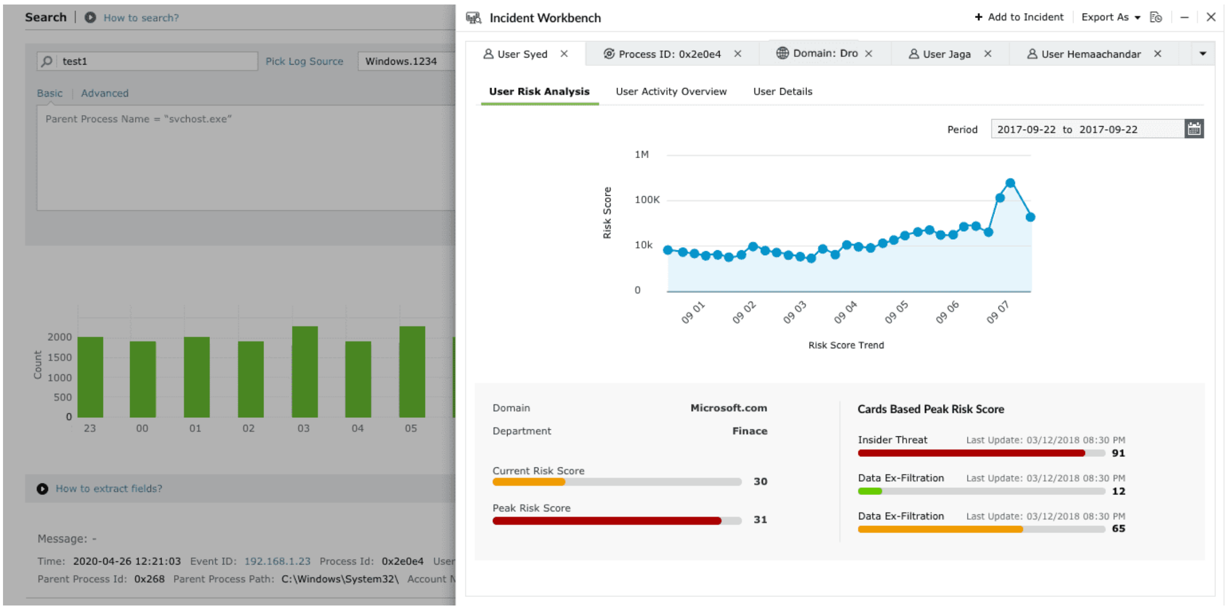
Threat investigation

4.2.1. Overview

Last updated on: September 12, 2025

In this page

- 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.



test1

Windows.1234

Parent Process Name = "svchost.exe"

Message: -

Time: 2020-04-26 12:21:03 Event ID: 192.168.1.23 Process Id: 0x2e0e4 User

Parent Process Id: 0x268 Parent Process Path: C:\Windows\System32\ Account N

Period 2017-09-22 to 2017-09-22

Domain Microsoft.com

Department Finace

Current Risk Score 30

Peak Risk Score 31

Cards Based Peak Risk Score

Insider Threat Last Update: 03/12/2018 08:30 PM 91

Data Ex-Filtration Last Update: 03/12/2018 08:30 PM 12

Data Ex-Filtration Last Update: 03/12/2018 08:30 PM 65

Features:

Here are the entities you can analyze using Incident Workbench:

- Users
  Analytics offered: ML-based user activity and risk score data compiled through UEBA integration from Log360's suite.
- Process
  Analytics offered: Process hunting tree with parent-child relationships and event timeline.
- Threat sources

Analytics offered: Risk analysis from security vendors using Advanced Threat Analytics integration.

Access and usability:

- Roles and restrictions:
    - Operator and guest role members have no access to the Incident Workbench.
    - Custom roles can be created to provide access to the Incident Workbench.
- Access: Incident workbench can be invoked from multiple dashboards of EventLog Analyzer such as reports, log search, compliance, alerts, and more.
- Users can add upto 20 tabs in a single instance of the Incident Workbench and save it to an existing incident or create a new incident.

Chapter 4.2.2 **Zia Insights**

4.2.2.1. About Zoho's Zia Insights

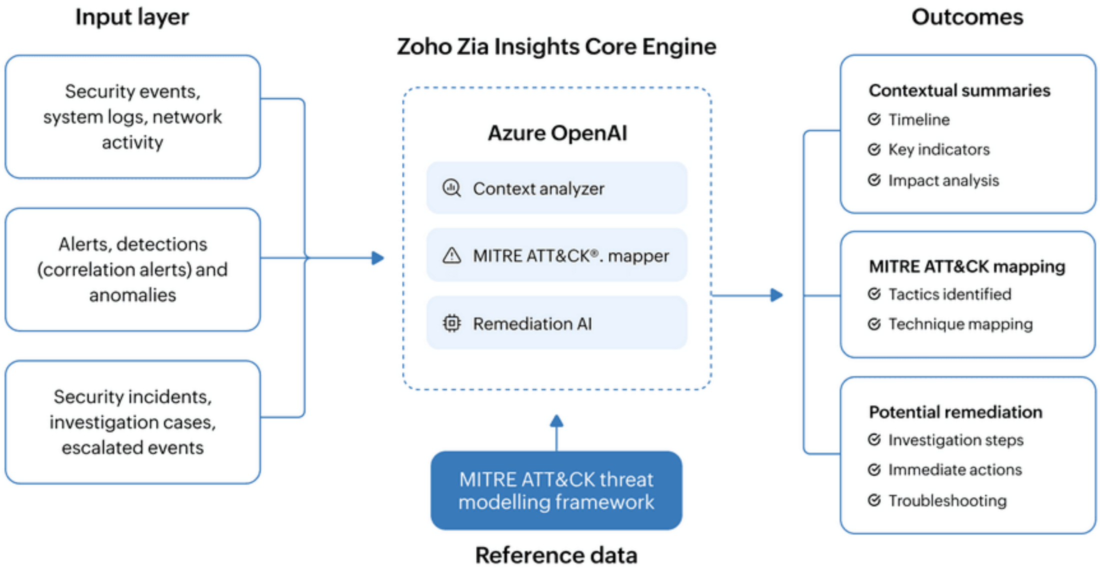
Last updated on: September 12, 2025

In this page

ManageEngine Log360 uses Zoho's Zia Insights, an AI-powered engine to enhance log analysis, threat detection, and incident response. By leveraging contextual AI, Zia Insights transforms raw logs, security events, audit trails, alerts, and incidents into actionable insights, enabling you to quickly identify risks, get context on an event, possible mitigation steps, and add value by mapping MITRE ATT&CK® techniques to the events wherever possible for effective analysis.

How Zia Insights work

This section elaborates the underlying architecture and functioning of Zia Insights. Zia Insights capability works with bring your own key (BYOK) model with Azure Open AI. By processing logs, alerts, and incidents, Zia Insights delivers contextual summaries, highlights potential risks, maps relevant activities to MITRE ATT&CK® techniques, and suggests possible remediation steps. These insights enable security teams to understand the event context better, accelerate investigations, and strengthen response strategies.



Zia Insights workflow

1. Invoking Zia Insights

The workflow begins when a user initiates a request for insight by selecting a specific log, alert, or incident. This action triggers the Zia Insights engine to begin its analysis.

Once invoked, the product console automatically retrieves all relevant data associated with the selected item. This includes raw logs, event metadata, alert context, or incident timelines, depending on the request initiated by the user. This collected information forms the input layer, which is critical to the insight generation process.

The input layer aggregates a wide range of security data sources, including:

- Security events, system logs, and network activity: Collected from endpoints, firewalls, cloud infrastructure, and other monitored systems
- Alerts and detections (correlation alerts): Triggered through rule-based correlation alerts.
- Security incidents, investigation cases, and escalated events: Data related to ongoing or historical threats under review by the SOC team

This comprehensive dataset ensures that Zia Insights has all the context it needs to generate actionable insights.

2. Insight generation

Once the relevant security data is collected, it is passed to the Zia Insights core engine, which leverages the capabilities of Azure OpenAI to transform raw data into contextual insights.

Zia Insights pairs the retrieved data with a predefined set of instructions known as a prompt. This prompt defines how Zia Insights should interpret the data and how the output should be structured.

Zia Insights then processes the data through several core components:

- Context analyzer
  Reconstructs the event timeline, identifies key actions, and potential threat classifications.
- MITRE ATT&CK® mapper
  Matches detected behaviors to known attacker tactics and techniques using the MITRE ATT&CK® framework, helping the SOC team understand potential threat stages.
- Remediation AI
  Suggests investigation steps, containment strategies, and recovery recommendations tailored to the specific scenario.

3. Outcomes from Zia Insights

After processing and analyzing the input data, Zia Insights produces a structured output that is both actionable and context-aware. The key components of the outcomesinclude:

Contextual summaries

Summarizes the event with a timeline, key indicators, and impact analysis

- Timeline: Reconstructs the sequence of related events to provide temporal clarity.
- Key indicators: Highlights important information such as source IPs, user accounts, and processes.
- Impact analysis: Evaluates the potential effect of the event on systems, users, or business operations, helping teams prioritize response.

MITRE ATT&CK® mapping

Based on the behaviors observed, Zia Insights maps the activity to corresponding MITRE ATT&CK® tactics and techniques. This enables standardized threat classification and aids in investigation and threat hunting.

Potential remediation

Zia Insights offers suggested investigation steps, immediate containment actions, and troubleshooting guidance to support timely and informed action.

Benefits of Zia Insights

Zia Insights empowers SOC team's investigation process and effectively mitigate or neutralize a threat with unprecedented speed. It allows SOC professionals to:

- Proactively hunt for subtle indicators: Leverage the Summary, Insights, and Timeline in Zia Insights to uncover subtle indicators of compromise proactively. These segments quickly highlight relevant events, actors, and entities.
- Accelerate Investigation: By automatically providing context, identifying actors, entities, and laying out the attack chain with MITRE ATT&CK® framework mapping.
- Enable Rapid Remediation: By offering specific, actionable steps tailored to the detected threat and log types.
- Enhance Threat Intelligence: By consistently mapping incidents to MITRE ATT&CK® , building institutional knowledge of adversary tactics.
- Optimize Analyst Productivity: By offloading initial analysis and information gathering to the AI, allowing human analysts to focus on critical decision-making and strategic defense.

Read also

This document detailed the working principles and key use cases of Zia Insights. For configuring and leveraging the capabilities of Zia Insights, refer to the articles below:

- Using Zia Insights
- Setting up Zia Insights

4.2.2.2. Using Zia Insights

Last updated on: September 12, 2025

In this page

Overview

Zoho Zia, the AI-engine, delivers contextual insights from logs, alerts, and incidents by leveraging advanced summarization, threat mapping, and possible remediations. Using Universally Unique Identifiers (UUIDs) for logs, Alert IDs for alert data, and Incident IDs for incident data, Zia Insights processes raw data to streamline threat detection, investigation, remediation, and compliance audit.
This page explains how Zia Insights categorizes events, generates insights, and guides response actions within the product console.

Key insights provided by Zia

Zia Insights provides six key information for effective security operations. They are:

- Log categorization
- Summary
- Insights
- Timeline
- Potential MITRE ATT&CK® Mapping
- Mitigation guidance

Log categorization

To accelerate log analysis and generate remediation steps, Zia Insights categorizes log data and provides tailored recommendations based on the log type. Refer the below table to learn how Zia Insights categorizes the logs, the detection indicator it uses for log categorization, and the modules it assigns to each category.

> NOTE
>
> All logs in the Search and Alerts modules are categorized, and remediation steps are provided if the log falls into one of the predefined categories.

Log type	Detection indicators	Insights provided

Log type	Detection indicators	Insights provided
Error and crash logs	Error codes, "failed" or "fatal" keywords, or stack traces. Application crashes, or service failures that disrupt normal operations.	Troubleshooting Steps For example, application crashes will include recommendations to analyze application logs at the time of the crash to identify any correlated events, and debug using tools like WinDbg to trace access violations.
Security logs	Failed authorizations, suspicious activities such as User Account Control (UAC) modifications, or triggered security alerts.	Potential Mitigation Steps For example, office process launching PowerShell will include recommendations to investigate the source document, restrict script execution using Powershell's Constrained Language Mode, and block macros from untrusted sources.
Audit logs	Unauthorized access attempts, audit policy violations, or configuration changes.	Recommendations For example, changes to audit policies will include recommendations to enforce strict access controls and alert mechanisms for critical audit events.

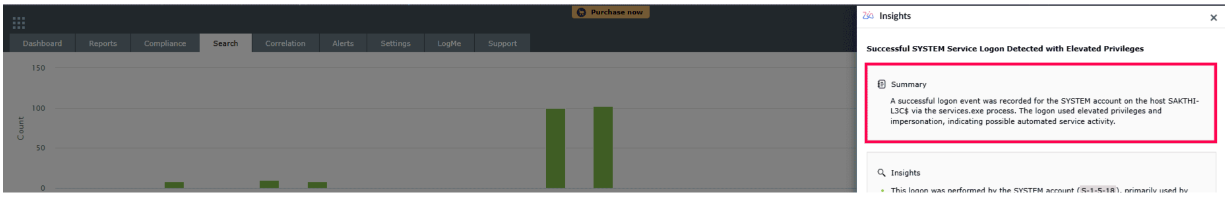
NOTE

If a log does not fall under one of the above mentioned categories, mitigation steps will not be available.

Summary

The Zia Insight's Summary segment provides a concise overview of logs, events, alerts, and incidents. It distils crucial information from logs and incidents by using structured inputs. For incidents, it gathers details like evidence, notes, activity logs, involved parties, and basic incident context to generate the summary.

NOTE Summary is generated for logs accessed via Search and Alerts consoles. While Zia provides a concise overview across both, the level of detail in the summary may depend on the context of the underlying data.



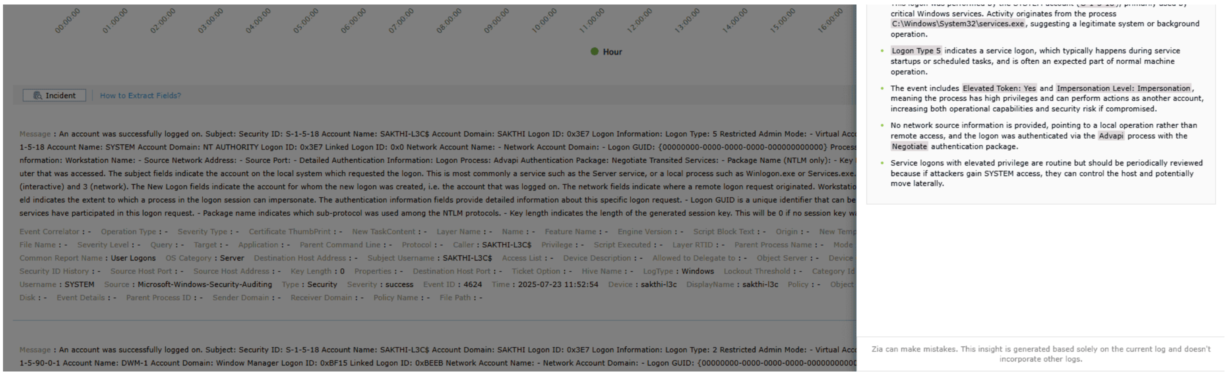
Successful SYSTEM Service Logon Detected with Elevated Privileges

Summary

A successful logon event was recorded for the SYSTEM account on the host SAKTHI-L3C$ via the services.exe process. The logon used elevated privileges and impersonation, indicating possible automated service activity.

Insights

- This logon was performed by the SYSTEM account (S-1-5-18), primarily used by



```
Message : An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: SAKTHI-L3C$ Account Domain: SAKTHI Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Virtual Acc
1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process
nformation: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key
uter that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.
(interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio
eld indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be
services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key wa
Event Correlator : -   Operation Type : -   Severity Type : -   Certificate ThumbPrint : -   New TaskContent : -   Layer Name : -   Name : -   Feature Name : -   Engine Version : -   Script Block Text : -   Origin : -   New Temp
File Name : -   Severity Level : -   Query : -   Target : -   Application : -   Parent Command Line : -   Protocol : -   Caller : SAKTHI-L3C$   Privilege : -   Script Executed : -   Layer RTID : -   Parent Process Name : -   Mode
Common Report Name : User Logons   OS Category : Server   Destination Host Address : -   Subject Username : SAKTHI-L3C$   Access List : -   Device Description : -   Allowed to Delegate to : -   Object Server : -   Device
Security ID History : -   Source Host Port : -   Source Host Address : -   Key Length : 0   Properties : -   Destination Host Port : -   Ticket Option : -   Hive Name : -   LogType : Windows   Lockout Threshold : -   Category Id
Username : SYSTEM   Source : Microsoft-Windows-Security-Auditing   Type : Security   Severity : success   Event ID : 4624   Time : 2025-07-23 11:52:54   Device : sakthi-l3c   DisplayName : sakthi-l3c   Policy : -   Object
Disk : -   Event Details : -   Parent Process ID : -   Sender Domain : -   Receiver Domain : -   Policy Name : -   File Path : -

Message : An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: SAKTHI-L3C$ Account Domain: SAKTHI Logon ID: 0x3E7 Logon Information: Logon Type: 2 Restricted Admin Mode: - Virtual Acc
1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xBF15 Linked Logon ID: 0xBEEB Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-00000000000
```

- This logon was performed by the SYSTEM account (S-1-5-18), primarily used by critical Windows services. Activity originates from the process C:\Windows\System32\services.exe, suggesting a legitimate system or background operation.
- Logon Type 5 indicates a service logon, which typically happens during service startups or scheduled tasks, and is often an expected part of normal machine operation.
- The event includes Elevated Token: Yes and Impersonation Level: Impersonation, meaning the process has high privileges and can perform actions as another account, increasing both operational capabilities and security risk if compromised.
- No network source information is provided, pointing to a local operation rather than remote access, and the logon was authenticated via the Advapi process with the Negotiate authentication package.
- Service logons with elevated privilege are routine but should be periodically reviewed because if attackers gain SYSTEM access, they can control the host and potentially move laterally.

Zia can make mistakes. This insight is generated based solely on the current log and doesn't incorporate other logs.

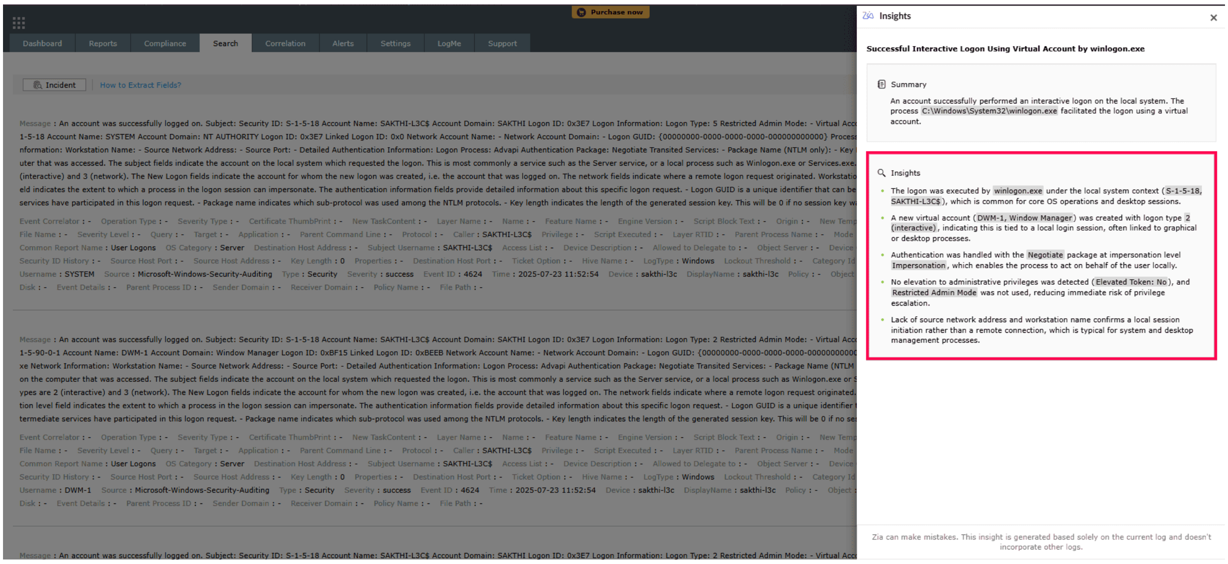
Figure 1: Zia Insights summary from Search

Insights

The Insights segment in Zia Insights provides actionable understanding derived from analyzing events leading to an alert, which enables the identification of key actors, source and destination IPs, user accounts, involved entities, example systems, and the detection of suspicious behaviors.

NOTE

Insights are generated only when you invoke Zia Insights from Search and Alerts consoles of the product. In the Incidents module, Insights are not available for workbench evidence.



```
Message : An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: SAKTHI-L3C$ Account Domain: SAKTHI Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Virtual Acc
1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process
nformation: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key
uter that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.
(interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstatio
eld indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be
services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key wa
Event Correlator : -   Operation Type : -   Severity Type : -   Certificate ThumbPrint : -   New TaskContent : -   Layer Name : -   Name : -   Feature Name : -   Engine Version : -   Script Block Text : -   Origin : -   New Temp
File Name : -   Severity Level : -   Query : -   Target : -   Application : -   Parent Command Line : -   Protocol : -   Caller : SAKTHI-L3C$   Privilege : -   Script Executed : -   Layer RTID : -   Parent Process Name : -   Mode
Common Report Name : User Logons   OS Category : Server   Destination Host Address : -   Subject Username : SAKTHI-L3C$   Access List : -   Device Description : -   Allowed to Delegate to : -   Object Server : -   Device
Security ID History : -   Source Host Port : -   Source Host Address : -   Key Length : 0   Properties : -   Destination Host Port : -   Ticket Option : -   Hive Name : -   LogType : Windows   Lockout Threshold : -   Category Id
Username : SYSTEM   Source : Microsoft-Windows-Security-Auditing   Type : Security   Severity : success   Event ID : 4624   Time : 2025-07-23 11:52:54   Device : sakthi-l3c   DisplayName : sakthi-l3c   Policy : -   Object
Disk : -   Event Details : -   Parent Process ID : -   Sender Domain : -   Receiver Domain : -   Policy Name : -   File Path : -

Message : An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: SAKTHI-L3C$ Account Domain: SAKTHI Logon ID: 0x3E7 Logon Information: Logon Type: 2 Restricted Admin Mode: - Virtual Acc
1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xBF15 Linked Logon ID: 0xBEEB Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-00000000000
xe Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM
on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or S
ypes are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated.
tion level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier t
termediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no ses
Event Correlator : -   Operation Type : -   Severity Type : -   Certificate ThumbPrint : -   New TaskContent : -   Layer Name : -   Name : -   Feature Name : -   Engine Version : -   Script Block Text : -   Origin : -   New Temp
File Name : -   Severity Level : -   Query : -   Target : -   Application : -   Parent Command Line : -   Protocol : -   Caller : SAKTHI-L3C$   Privilege : -   Script Executed : -   Layer RTID : -   Parent Process Name : -   Mode
Common Report Name : User Logons   OS Category : Server   Destination Host Address : -   Subject Username : SAKTHI-L3C$   Access List : -   Device Description : -   Allowed to Delegate to : -   Object Server : -   Device
Security ID History : -   Source Host Port : -   Source Host Address : -   Key Length : 0   Properties : -   Destination Host Port : -   Ticket Option : -   Hive Name : -   LogType : Windows   Lockout Threshold : -   Category Id
Username : DWM-1   Source : Microsoft-Windows-Security-Auditing   Type : Security   Severity : success   Event ID : 4624   Time : 2025-07-23 11:52:54   Device : sakthi-l3c   DisplayName : sakthi-l3c   Policy : -   Object
Disk : -   Event Details : -   Parent Process ID : -   Sender Domain : -   Receiver Domain : -   Policy Name : -   File Path : -

Message : An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: SAKTHI-L3C$ Account Domain: SAKTHI Logon ID: 0x3E7 Logon Information: Logon Type: 2 Restricted Admin Mode: - Virtual Acc
```

Successful Interactive Logon Using Virtual Account by winlogon.exe

Summary

An account successfully performed an interactive logon on the local system. The process C:\Windows\System32\winlogon.exe facilitated the logon using a virtual account.

Insights

- The logon was executed by winlogon.exe under the local system context (S-1-5-18, SAKTHI-L3C$), which is common for core OS operations and desktop sessions.
- A new virtual account (DWM-1, Window Manager) was created with logon type 2 (interactive), indicating this is tied to a local login session, often linked to graphical or desktop processes.
- Authentication was handled with the Negotiate package at impersonation level Impersonation, which enables the process to act on behalf of the user locally.
- No elevation to administrative privileges was detected (Elevated Token: No), and Restricted Admin Mode was not used, reducing immediate risk of privilege escalation.
- Lack of source network address and workstation name confirms a local session initiation rather than a remote connection, which is typical for system and desktop management processes.

Zia can make mistakes. This insight is generated based solely on the current log and doesn't incorporate other logs.

Figure 2: Insights generated by Zia based on Alert data

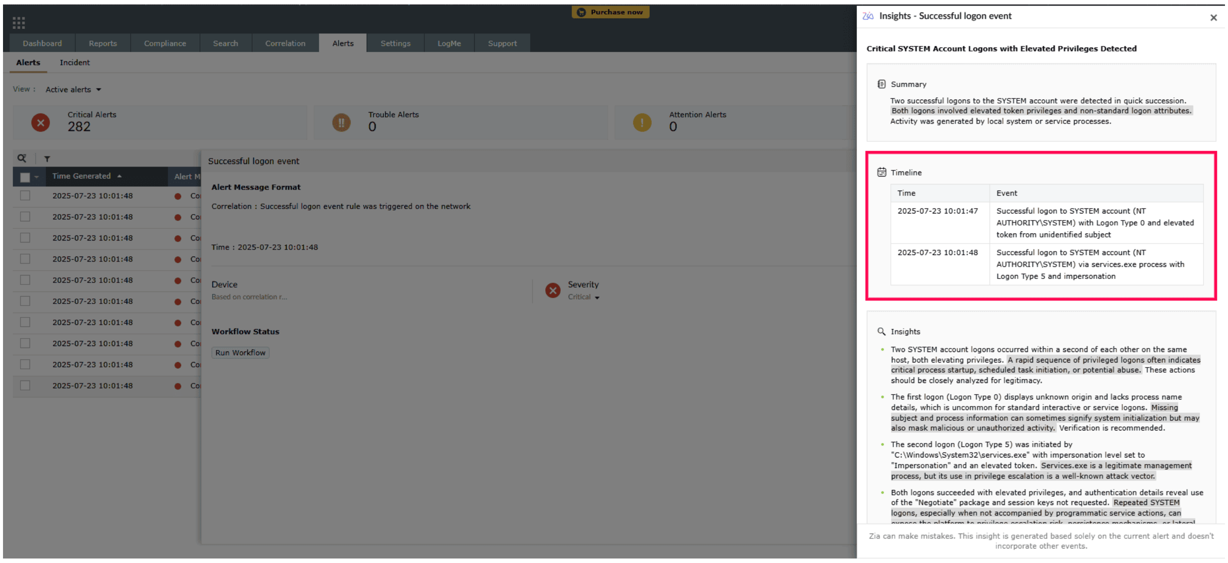
Timeline

Timeline segment of Zia Insights provides a chronological view of key events related to the alert or incident, including timestamps and specific actions or system behaviors that led up to or followed the incident. This helps reconstruct the attack chain, verify patterns, and correlate the activity with other events.

NOTE

The Timeline segment will be available in the following cases:
- In the Alerts module, when alerts are linked to correlation rules or alerts profiles that are defined based on thresholds.
- In the Incidents module.

1. Correlation rule-based alerts are alert profiles that get associated with specific detection rules. It results from the aggregation of multiple related events or alerts, which together reveal a broader and more significant security incident.
   Example: Events like login failures followed by successful logon and new services installed denote a sequence of activity by the same user. Timeline will be shown for these types of events.
2. Threshold-based alerts are triggered when a particular activity exceeds a predefined limit within a specified time frame, indicating potentially suspicious behavior.
   Example: An alert is generated when a login failure occurs 10 times within 5 minutes, which may suggest a brute-force attack. Timeline of the login failures will be graphically shown by Zia Insights.



Time Generated
2025-07-23 10:01:48
2025-07-23 10:01:48
2025-07-23 10:01:48
2025-07-23 10:01:48
2025-07-23 10:01:48
2025-07-23 10:01:48
2025-07-23 10:01:48
2025-07-23 10:01:48
2025-07-23 10:01:48
2025-07-23 10:01:48

Successful logon event

Alert Message Format

Correlation : Successful logon event rule was triggered on the network

Time : 2025-07-23 10:01:48

Device: Based on correlation r...

Severity: Critical

Workflow Status

Insights - Successful logon event

Critical SYSTEM Account Logons with Elevated Privileges Detected

Summary

Two successful logons to the SYSTEM account were detected in quick succession. Both logons involved elevated token privileges and non-standard logon attributes. Activity was generated by local system or service processes.

Timeline

Time	Event
2025-07-23 10:01:47	Successful logon to SYSTEM account (NT AUTHORITY\SYSTEM) with Logon Type 0 and elevated token from unidentified subject
2025-07-23 10:01:48	Successful logon to SYSTEM account (NT AUTHORITY\SYSTEM) via services.exe process with Logon Type 5 and impersonation

Insights

- Two SYSTEM account logons occurred within a second of each other on the same host, both elevating privileges. A rapid sequence of privileged logons often indicates critical process startup, scheduled task initiation, or potential abuse. These actions should be closely analyzed for legitimacy.
- The first logon (Logon Type 0) displays unknown origin and lacks process name details, which is uncommon for standard interactive or service logons. Missing subject and process information can sometimes signify system initialization but may also mask malicious or unauthorized activity. Verification is recommended.
- The second logon (Logon Type 5) was initiated by "C:\Windows\System32\services.exe" with impersonation level set to "Impersonation" and an elevated token. Services.exe is a legitimate management process, but its use in privilege escalation is a well-known attack vector.
- Both logons succeeded with elevated privileges, and authentication details reveal use of the "Negotiate" package and session keys not requested. Repeated SYSTEM logons, especially when not accompanied by programmatic service actions, can expose the platform to privilege escalation risk, persistence mechanisms, or lateral

Zia can make mistakes. This insight is generated based solely on the current alert and doesn't incorporate other events.

Figure 3: Overview of the event timeline by Zia Insights

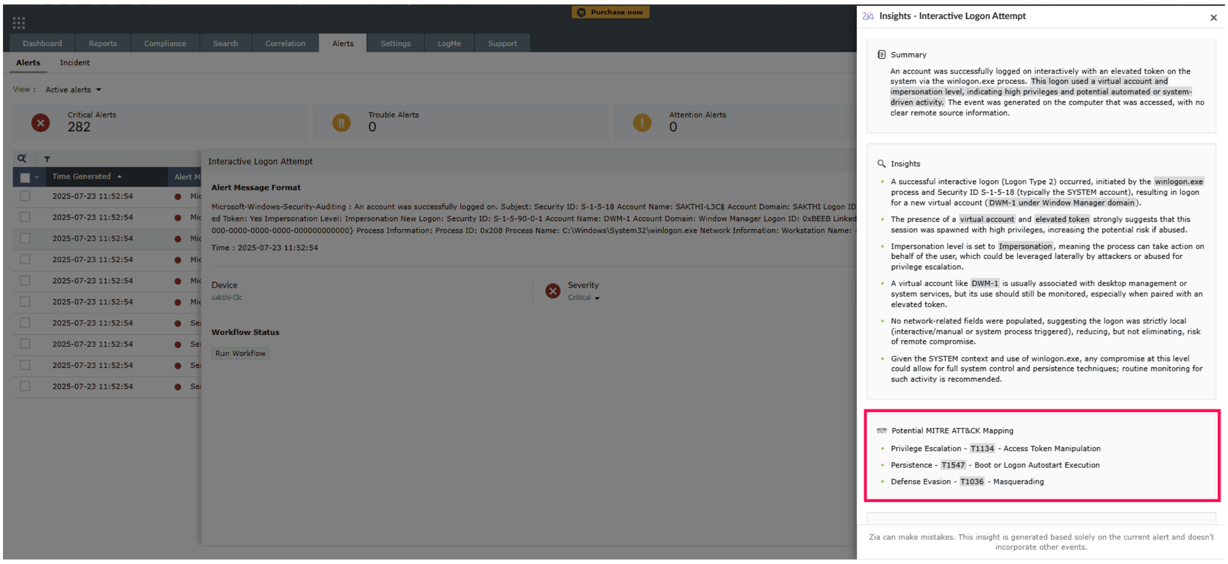
Potential MITRE ATT&CK® Mapping

Zia Insights maps events and alerts with known tactics, techniques, and procedures (TTPs) from the MITRE ATT&CK® framework. This includes mapping the activity to the corresponding Tactic Name, Technique ID, and Technique Name.

NOTE

Potential MITRE ATT&CK® Mapping is displayed only when the log indicate suspicious or

Potential MITRE ATT&CK® Mapping is displayed only when the log indicate suspicious or malicious activity.



2025-07-23 11:52:54

Interactive Logon Attempt

Alert Message Format

Microsoft-Windows-Security-Auditing : An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: SAKTHI-L3C$ Account Domain: SAKTHI Logon ID ed Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-90-0-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xBEEB Linked 000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name:

Time : 2025-07-23 11:52:54

Device: sakthi-l3c

Severity: Critical

Workflow Status

Insights - Interactive Logon Attempt

Summary

An account was successfully logged on interactively with an elevated token on the system via the winlogon.exe process. This logon used a virtual account and impersonation level, indicating high privileges and potential automated or system-driven activity. The event was generated on the computer that was accessed, with no clear remote source information.

Insights

- A successful interactive logon (Logon Type 2) occurred, initiated by the winlogon.exe process and Security ID S-1-5-18 (typically the SYSTEM account), resulting in logon for a new virtual account (DWM-1 under Window Manager domain).
- The presence of a virtual account and elevated token strongly suggests that this session was spawned with high privileges, increasing the potential risk if abused.
- Impersonation level is set to Impersonation, meaning the process can take action on behalf of the user, which could be leveraged laterally by attackers or abused for privilege escalation.
- A virtual account like DWM-1 is usually associated with desktop management or system services, but its use should still be monitored, especially when paired with an elevated token.
- No network-related fields were populated, suggesting the logon was strictly local (interactive/manual or system process triggered), reducing, but not eliminating, risk of remote compromise.
- Given the SYSTEM context and use of winlogon.exe, any compromise at this level could allow for full system control and persistence techniques; routine monitoring for such activity is recommended.

Potential MITRE ATT&CK Mapping

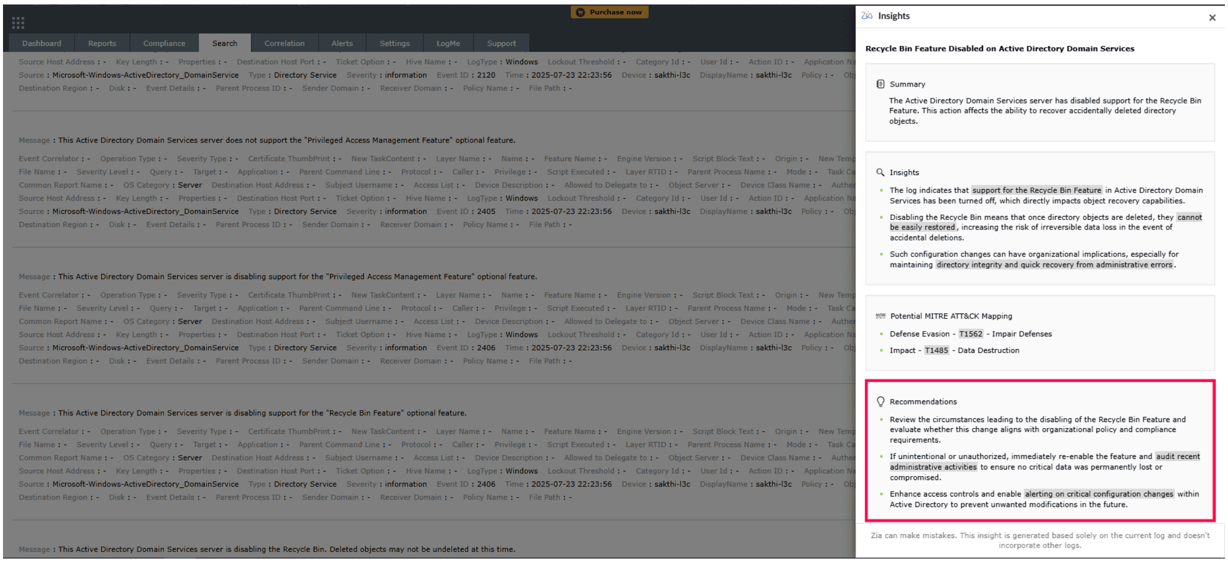
- Privilege Escalation - T1134 - Access Token Manipulation
- Persistence - T1547 - Boot or Logon Autostart Execution
- Defense Evasion - T1036 - Masquerading

Zia can make mistakes. This insight is generated based solely on the current alert and doesn't incorporate other events.

Figure 4: Mapped MITRE ATT&CK® techniques by Zia Insights

Mitigation guidance

Based on log categorization, Zia Insights provide actionable remediation steps that help contain the incident, restore normal operations, and reduce the risk of future occurrences. Recommendations are tailored to the type of log,such as crash, error, audit, and security.



Source : Microsoft-Windows-ActiveDirectory_DomainService Type : Directory Service Severity : information Event ID : 2120 Time : 2025-07-23 22:23:56 Device : sakthi-l3c DisplayName : sakthi-l3c

Message : This Active Directory Domain Services server does not support the "Privileged Access Management Feature" optional feature.

Source : Microsoft-Windows-ActiveDirectory_DomainService Type : Directory Service Severity : information Event ID : 2405 Time : 2025-07-23 22:23:56 Device : sakthi-l3c DisplayName : sakthi-l3c

Message : This Active Directory Domain Services server is disabling support for the "Privileged Access Management Feature" optional feature.

Source : Microsoft-Windows-ActiveDirectory_DomainService Type : Directory Service Severity : information Event ID : 2406 Time : 2025-07-23 22:23:56 Device : sakthi-l3c DisplayName : sakthi-l3c

Message : This Active Directory Domain Services server is disabling support for the "Recycle Bin Feature" optional feature.

Source : Microsoft-Windows-ActiveDirectory_DomainService Type : Directory Service Severity : information Event ID : 2406 Time : 2025-07-23 22:23:56 Device : sakthi-l3c DisplayName : sakthi-l3c

Message : This Active Directory Domain Services server is disabling the Recycle Bin. Deleted objects may not be undeleted at this time.

Insights

Recycle Bin Feature Disabled on Active Directory Domain Services

Summary

The Active Directory Domain Services server has disabled support for the Recycle Bin Feature. This action affects the ability to recover accidentally deleted directory objects.

Insights

- The log indicates that support for the Recycle Bin Feature in Active Directory Domain Services has been turned off, which directly impacts object recovery capabilities.
- Disabling the Recycle Bin means that once directory objects are deleted, they cannot be easily restored, increasing the risk of irreversible data loss in the event of accidental deletions.
- Such configuration changes can have organizational implications, especially for maintaining directory integrity and quick recovery from administrative errors.

Potential MITRE ATT&CK Mapping

- Defense Evasion - T1562 - Impair Defenses
- Impact - T1485 - Data Destruction

Recommendations

- Review the circumstances leading to the disabling of the Recycle Bin Feature and evaluate whether this change aligns with organizational policy and compliance requirements.
- If unintentional or unauthorized, immediately re-enable the feature and audit recent administrative activities to ensure no critical data was permanently lost or compromised.
- Enhance access controls and enable alerting on critical configuration changes within Active Directory to prevent unwanted modifications in the future.

Zia can make mistakes. This insight is generated based solely on the current log and doesn't incorporate other logs.

Figure 3: Overview of the event timeline by Zia Insights

Read also

This document elaborated on the overview, key insights, and use cases of Zia Insights. For configuring and leveraging the capabilities of Zia Insights, refer to the articles below:

- Setting up Zia Insights

- Invoking Zia Insights

4.2.2.3. Setting up Zia Insights

Last updated on: September 12, 2025

In this page

Overview

Zia Insights provides AI-powered actionable insights on incidents, alerts and logs using the Bring Your Own Key (BYOK) model, supporting integration with Azure OpenAI services.
This page elaborates on configurations that are essential to enable Zia Insights. It covers the creation of an Azure OpenAI resource, deployment of a compatible model, retrieval of necessary credentials such as the endpoint URL and API key, and integrating the AI service with the product console.

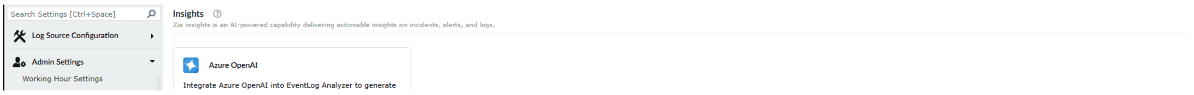
Pre-requisites

Before beginning the setup, ensure the following:

- You must have an active Azure subscription with access to the Azure OpenAI service.
- The following credentials are required from your Azure portal:
  - Endpoint URL
  - API key
  - Deployed model name

Accessing Zia Insights

1. Log in to your account.
2. Go to the Settings tab, and select Admin.
3. Navigate to Zia and select Insights.
4. To enable Zia Insights in, click Configure Now.

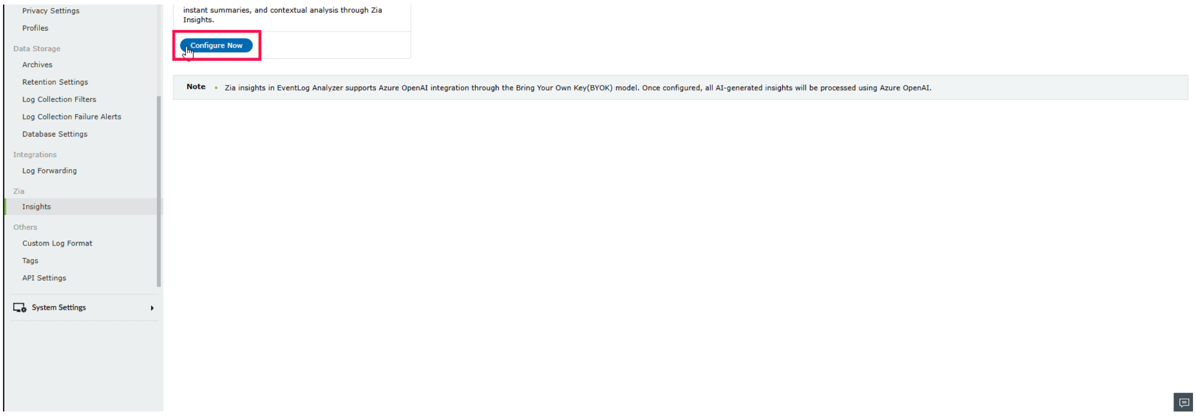


Insights

Zia insights is an AI-powered capability delivering actionable insights on incidents, alerts, and logs.

Azure OpenAI

Integrate Azure OpenAI into EventLog Analyzer to generate

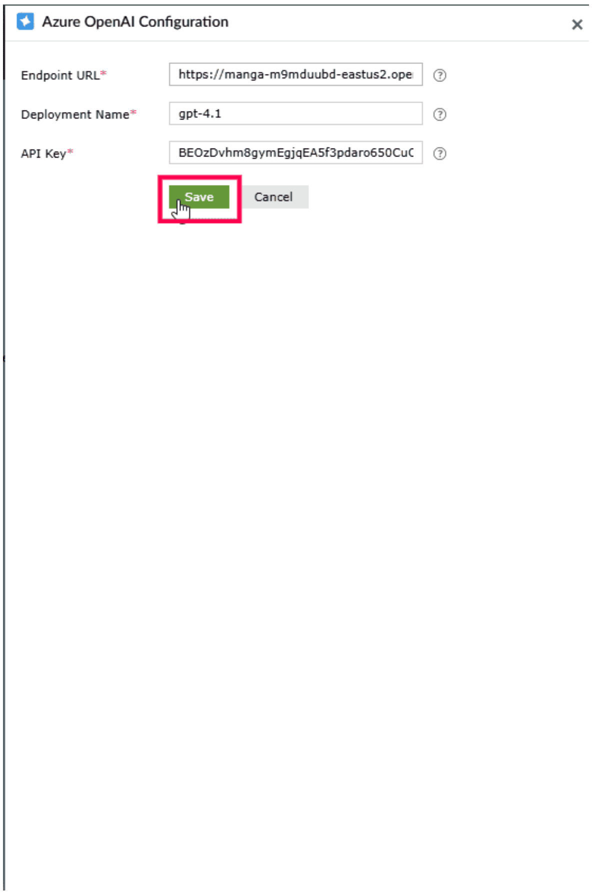


instant summaries, and contextual analysis through Zia Insights.

Note • Zia insights in EventLog Analyzer supports Azure OpenAI integration through the Bring Your Own Key(BYOK) model. Once configured, all AI-generated insights will be processed using Azure OpenAI.

Figure 1: Configuring Azure OpenAI

5. Enter the following details obtained from your Azure Portal:
   - Endpoint URL
   - DeploymentName
   - API Key
6. Click Save to complete the initial setup.



Endpoint URL* https://manga-m9mduubd-eastus2.ope

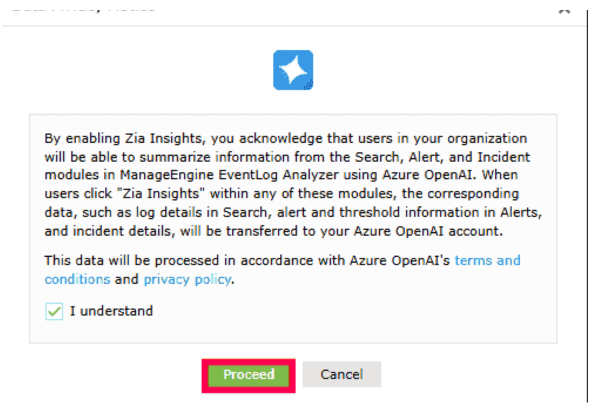
Deployment Name* gpt-4.1

API Key* BEOzDvhm8gymEgjqEA5f3pdaro650CuC

Figure 2: Configuring Azure OpenAI

7. In the pop-up window that appears, read the data privacy notice, select the I understand checkbox to acknowledge the terms, and then click Proceed to complete the OpenAI integration.

Data Privacy Notice



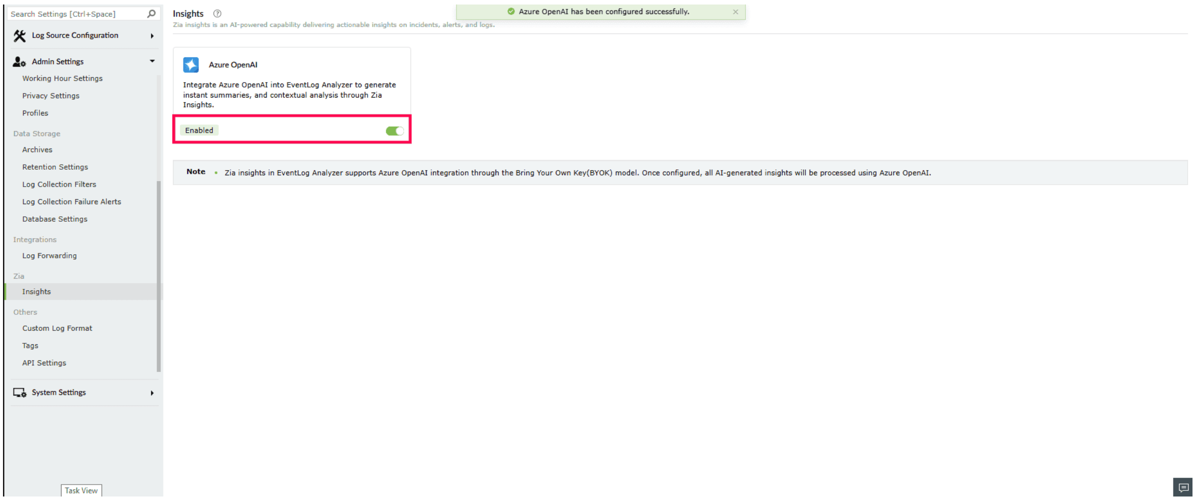
By enabling Zia Insights, you acknowledge that users in your organization will be able to summarize information from the Search, Alert, and Incident modules in ManageEngine EventLog Analyzer using Azure OpenAI. When users click "Zia Insights" within any of these modules, the corresponding data, such as log details in Search, alert and threshold information in Alerts, and incident details, will be transferred to your Azure OpenAI account.

This data will be processed in accordance with Azure OpenAI's terms and conditions and privacy policy.

☑ I understand

Figure 3: Azure OpenAI integration

8. Once the integration is complete, Zia Insights will be enabled.



Insights

Zia insights is an AI-powered capability delivering actionable insights on incidents, alerts, and logs.

Azure OpenAI has been configured successfully.

Azure OpenAI

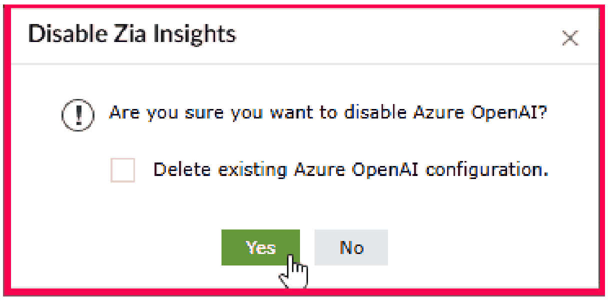
Integrate Azure OpenAI into EventLog Analyzer to generate instant summaries, and contextual analysis through Zia Insights.

Enabled

Note • Zia insights in EventLog Analyzer supports Azure OpenAI integration through the Bring Your Own Key(BYOK) model. Once configured, all AI-generated insights will be processed using Azure OpenAI.

Figure 4: Azure OpenAI integration

- To disable or re-enable Zia Insights, use the toggle switch beside the Azure OpenAI option.
- A confirmation pop-up will appear when disabling.
- Click Yes to disable Zia Insights.
- To delete the Azure OpenAI configuration, select the checkbox “Delete existing Azure OpenAI configuration” before clicking Yes.



Disable Zia Insights

Are you sure you want to disable Azure OpenAI?

□ Delete existing Azure OpenAI configuration.

Figure 5: Disabling and deleting Azure OpenAI configuration

Creating an Azure OpenAI resource

If you do not already have an Azure OpenAI resource, follow these steps:

NOTE If you already have an Azure OpenAI resource, refer to this to obtain the API key and Endpoint URL.

1. Log in to Azure portal and click Create a resource.

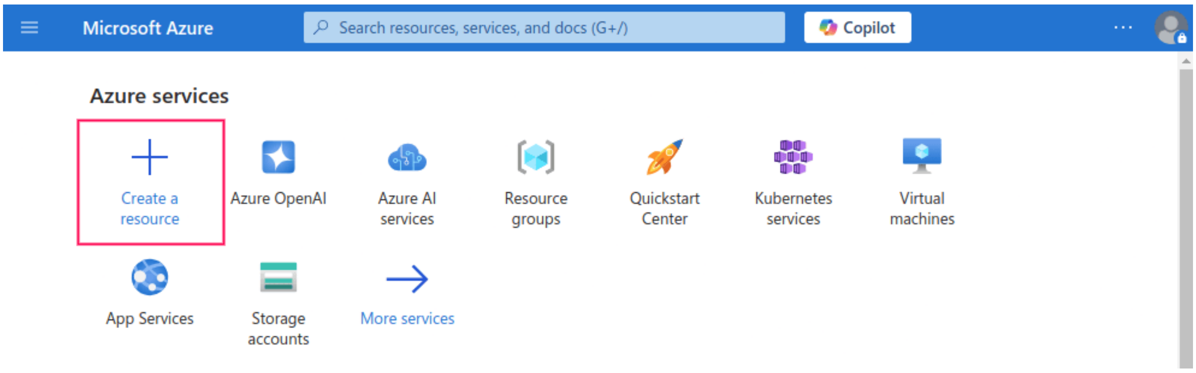
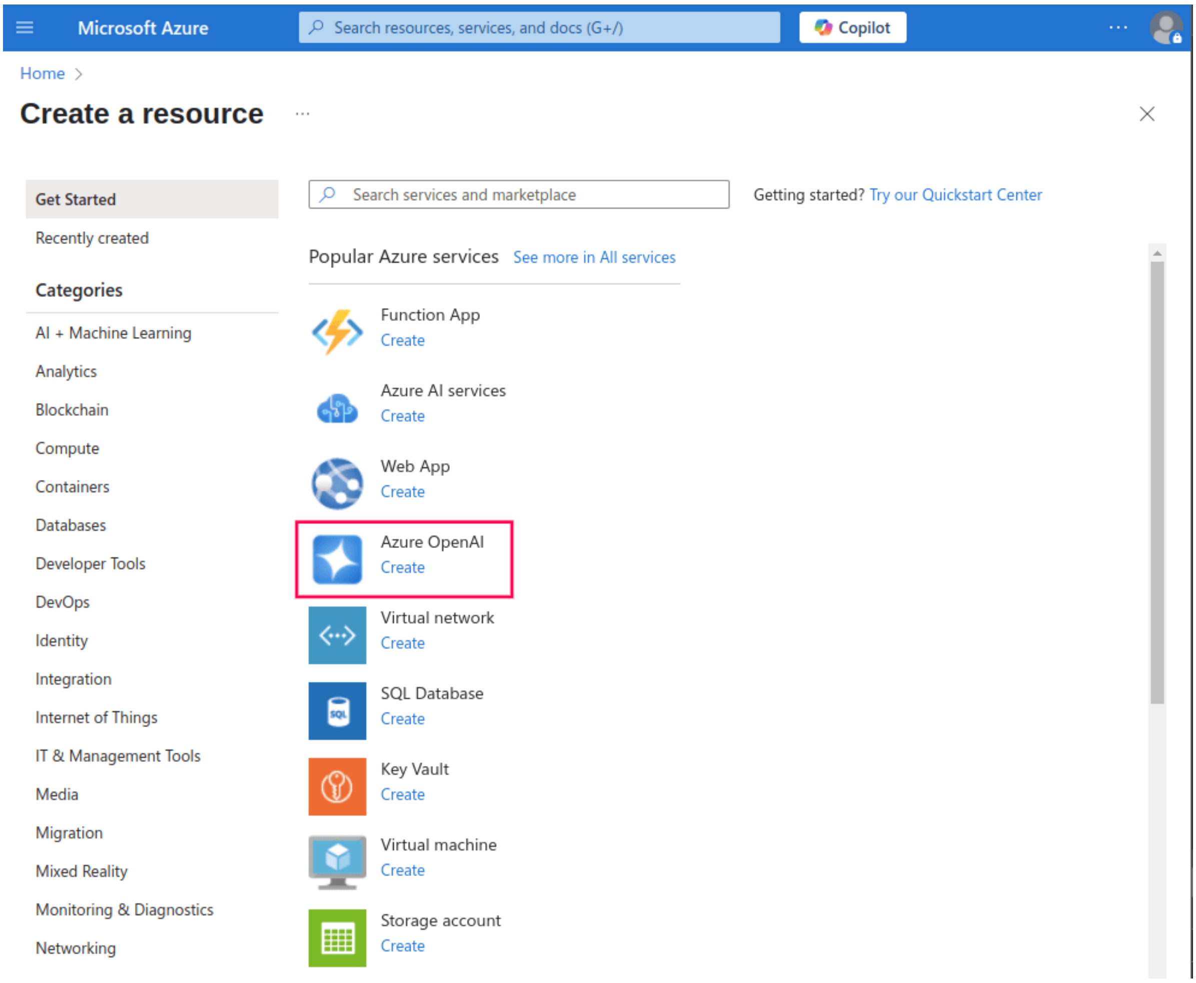


Figure 6: Creating a resource in Microsoft Azure

2. Select Azure OpenAI as the resource type.



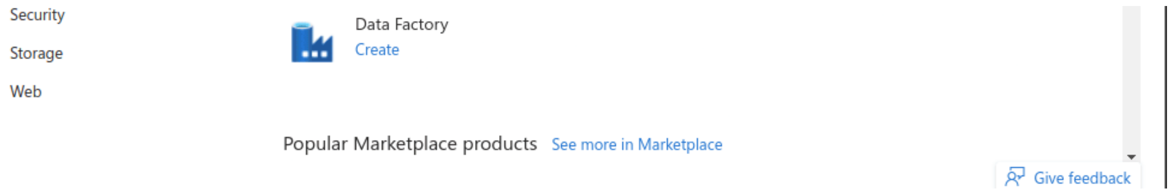
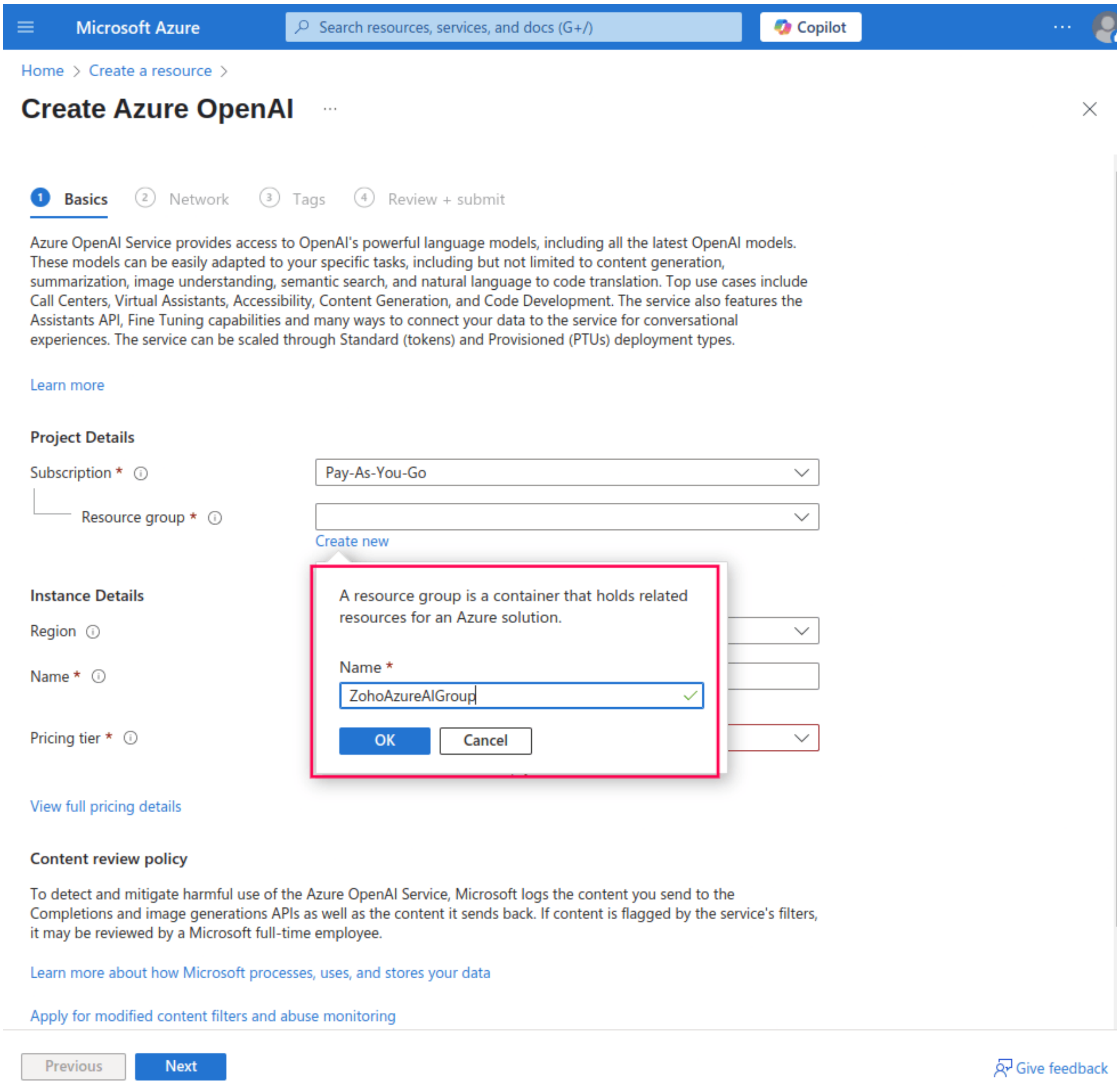


Figure 7: Creating an Azure OpenAI resource

3. Choose a Subscription of your choice.
4. Select an existing Resource group or create a new one.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Create a resource >

Create Azure OpenAI

1 Basics
2 Network
3 Tags
4 Review + submit

Azure OpenAI Service provides access to OpenAI's powerful language models, including all the latest OpenAI models. These models can be easily adapted to your specific tasks, including but not limited to content generation, summarization, image understanding, semantic search, and natural language to code translation. Top use cases include Call Centers, Virtual Assistants, Accessibility, Content Generation, and Code Development. The service also features the Assistants API, Fine Tuning capabilities and many ways to connect your data to the service for conversational experiences. The service can be scaled through Standard (tokens) and Provisioned (PTUs) deployment types.

Learn more

Project Details

Subscription * Pay-As-You-Go

Resource group *

Create new

A resource group is a container that holds related resources for an Azure solution.

Name * ZohoAzureAIGroup

Instance Details

Region

Name *

Pricing tier *

View full pricing details

Content review policy

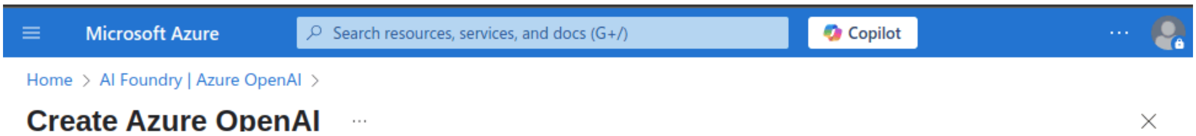
To detect and mitigate harmful use of the Azure OpenAI Service, Microsoft logs the content you send to the Completions and image generations APIs as well as the content it sends back. If content is flagged by the service's filters, it may be reviewed by a Microsoft full-time employee.

Learn more about how Microsoft processes, uses, and stores your data

Apply for modified content filters and abuse monitoring

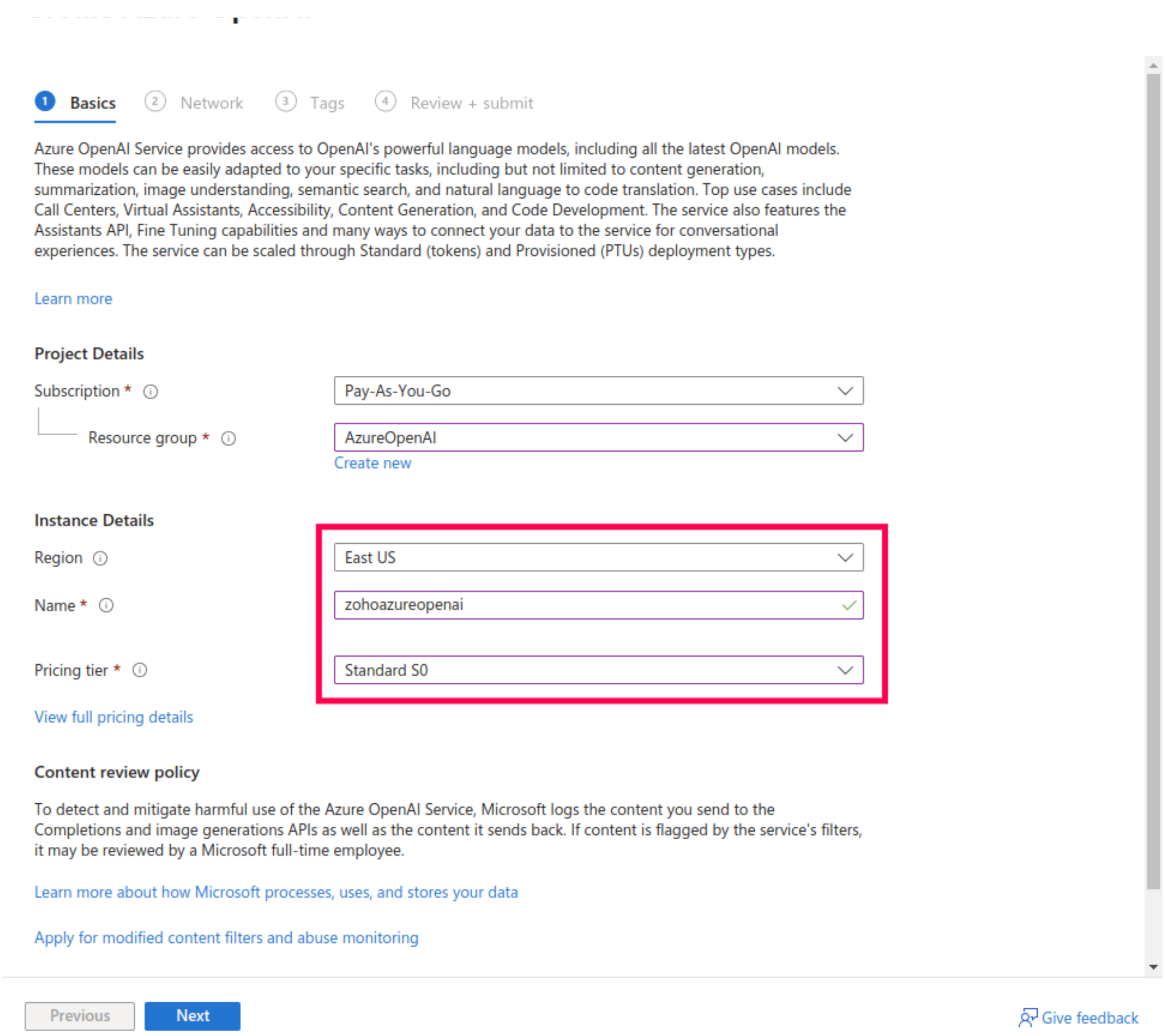
Figure 8: Creating a resource group in Microsoft Azure

5. Pick your desired Region and Pricing Tier.
6. Enter a suitable Name for the resource.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > AI Foundry | Azure OpenAI >

Create Azure OpenAI



Azure OpenAI Service provides access to OpenAI's powerful language models, including all the latest OpenAI models. These models can be easily adapted to your specific tasks, including but not limited to content generation, summarization, image understanding, semantic search, and natural language to code translation. Top use cases include Call Centers, Virtual Assistants, Accessibility, Content Generation, and Code Development. The service also features the Assistants API, Fine Tuning capabilities and many ways to connect your data to the service for conversational experiences. The service can be scaled through Standard (tokens) and Provisioned (PTUs) deployment types.

Learn more

Project Details

Subscription *: Pay-As-You-Go

Resource group *: AzureOpenAI

Create new

Instance Details

Region: East US

Name *: zohoazureopenai ✓

Pricing tier *: Standard S0

View full pricing details

Content review policy

To detect and mitigate harmful use of the Azure OpenAI Service, Microsoft logs the content you send to the Completions and image generations APIs as well as the content it sends back. If content is flagged by the service's filters, it may be reviewed by a Microsoft full-time employee.

Learn more about how Microsoft processes, uses, and stores your data

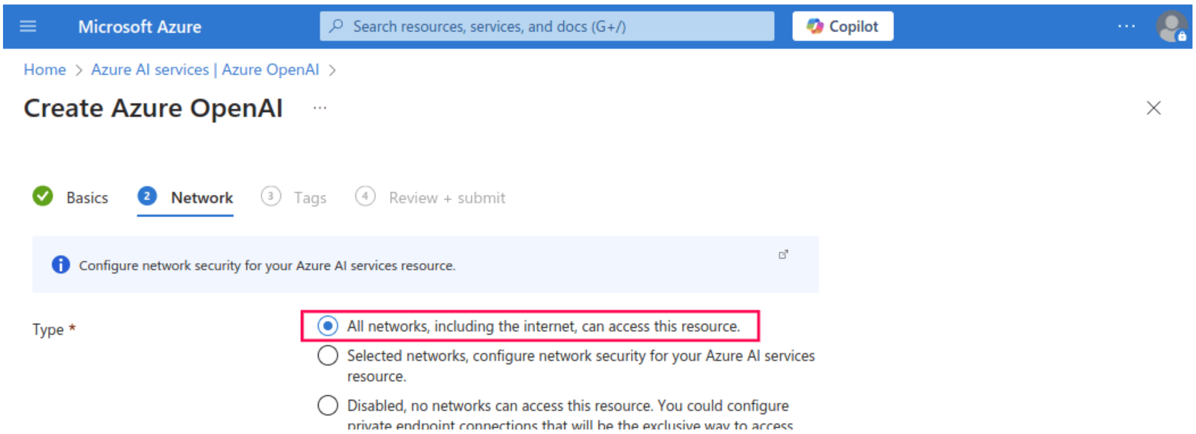
Apply for modified content filters and abuse monitoring

Figure 9: Instance details for Azure OpenAI service

7. Under Networking, select All networks, including the internet, can access this resource.

ⓘ NOTE

The Azure OpenAI resource must be publicly available on the internet so that the product console can access the endpoint.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Azure AI services | Azure OpenAI >

Create Azure OpenAI

✓ Basics ② Network ③ Tags ④ Review + submit

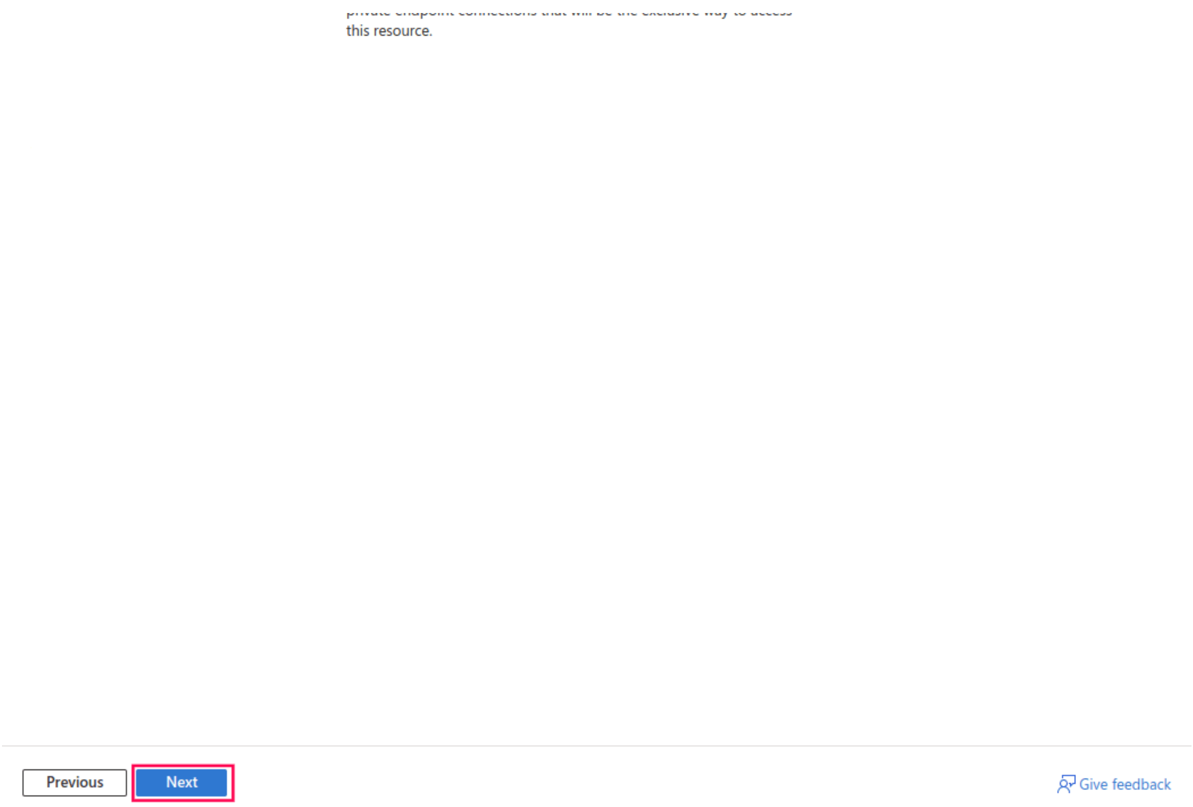
Configure network security for your Azure AI services resource.

Type *

● All networks, including the internet, can access this resource.

○ Selected networks, configure network security for your Azure AI services resource.

○ Disabled, no networks can access this resource. You could configure private endpoint connections that will be the exclusive way to access

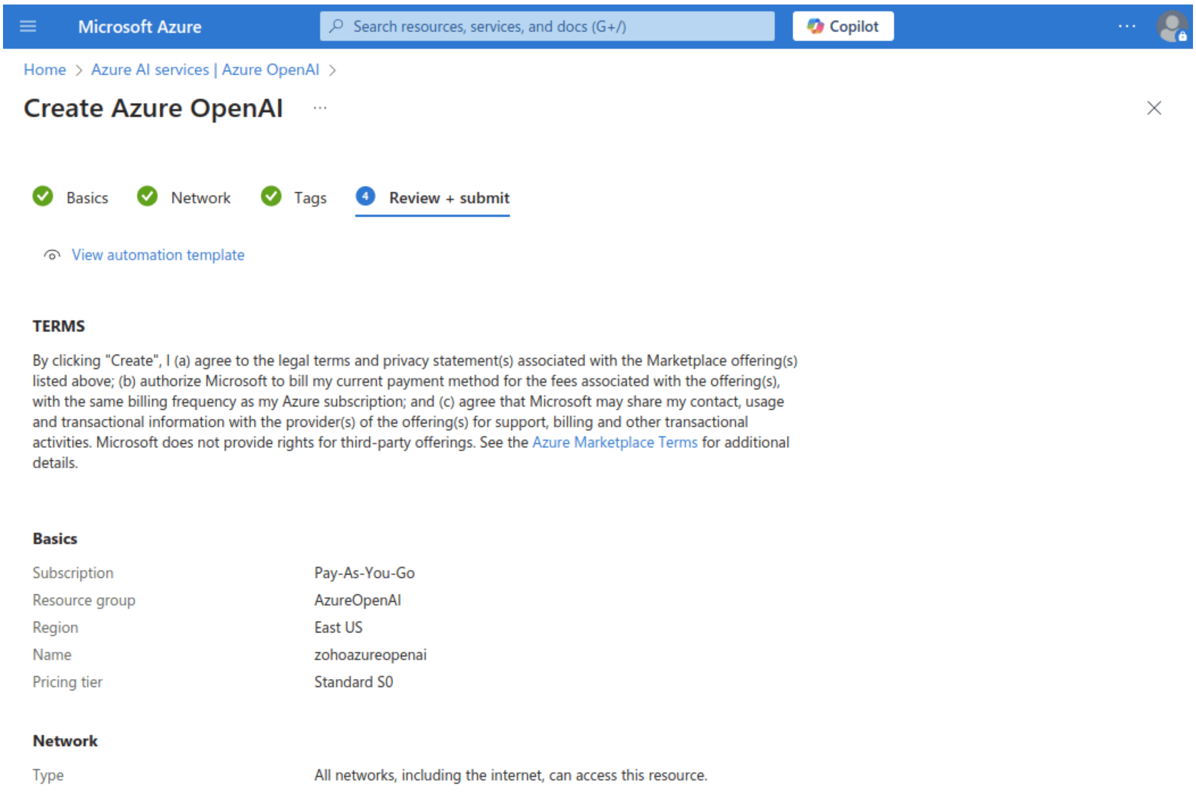


private endpoint connections that will be the exclusive way to access this resource.

Figure 10: Configuring network security for Azure AI services resource

8. Click Next to configure Tags (optional).

9. Click Next again to move to the Review + Submit page.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Azure AI services | Azure OpenAI >

Create Azure OpenAI

Basics
Network
Tags
4 Review + submit
View automation template

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

Basics

Subscription	Pay-As-You-Go
Resource group	AzureOpenAI
Region	East US
Name	zohoazureopenai
Pricing tier	Standard S0

Network

Type	All networks, including the internet, can access this resource.

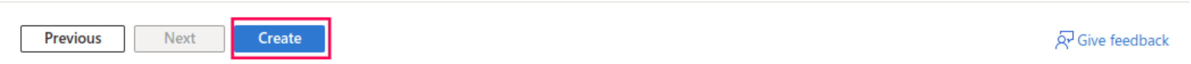


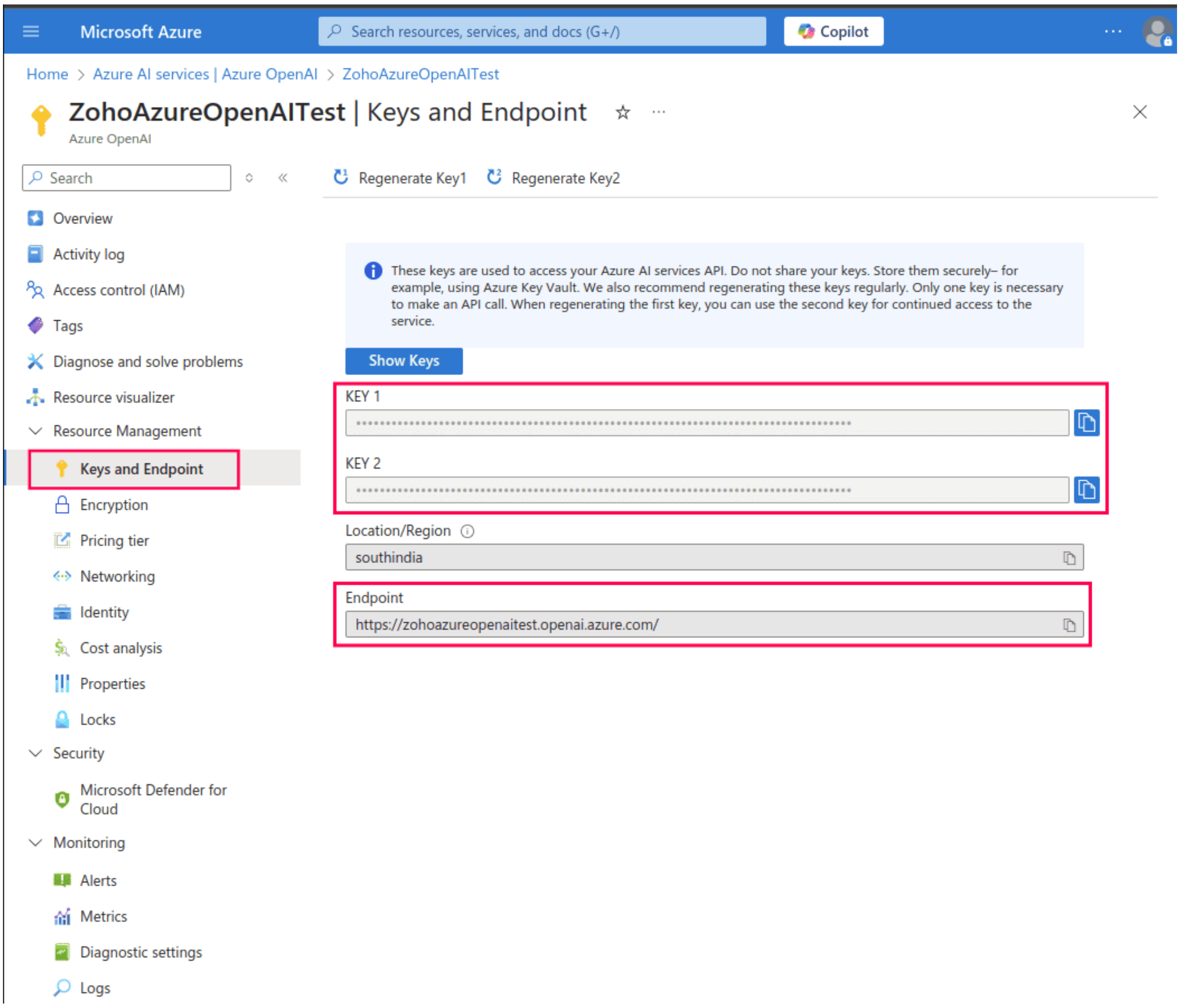
Figure 11: Final review to create resource

10. Review your settings and click Create to provision the resource.

Steps to obtain Endpoint URL and API key

If you already have an Endpoint URL and API key, skip to the next section. If not:

1. Log in to Azure portal and navigate to your Azure OpenAI resource.
2. In the left pane, under the Resource Management section, click on Keys and Endpoint. It will open Keys and Endpoint console.
3. In this window, you will find the Endpoint URL and API keys for your Azure OpenAI resource. Copy these details for use in the product.



These keys are used to access your Azure AI services API. Do not share your keys. Store them securely– for example, using Azure Key Vault. We also recommend regenerating these keys regularly. Only one key is necessary to make an API call. When regenerating the first key, you can use the second key for continued access to the service.

KEY 1: ••

KEY 2: ••

Location/Region: southindia

Endpoint: https://zohoazureopenaitest.openai.azure.com/

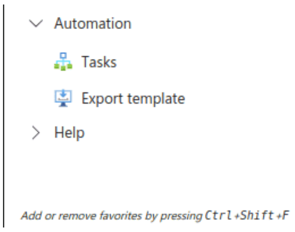


Figure 12: Obtaining API keys and Endpoint URL for Azure OpenAI resource

Deploying a model in Azure OpenAI

A deployed model is a version of an AI model (such as GPT-4o or GPT-4.1) that has been activated and made available for use within your Azure OpenAI resource. The product console will interact with the deployed model to generate AI-powered insights from your logs and alerts.

> NOTE
>
> If you already have a deployed model, you can directly use its deployment name when integrating with the product console. Ensure that the model is one of the following types:
>
> 1. The Chat Completion API model (models GPT-4o or newer). For better results, use latest available model such as GPT-4.1 or newer.
> 2. A non-reasoning model, excluding versions like o1-preview and o1-mini.

If you do not have a deployed model, follow the steps below.

Steps to deploy a model

1. Navigate to your Azure OpenAI resource and click Go to Azure AI Foundry portal.

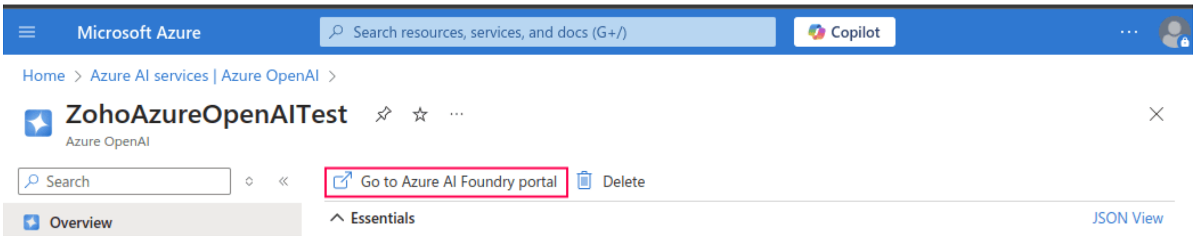
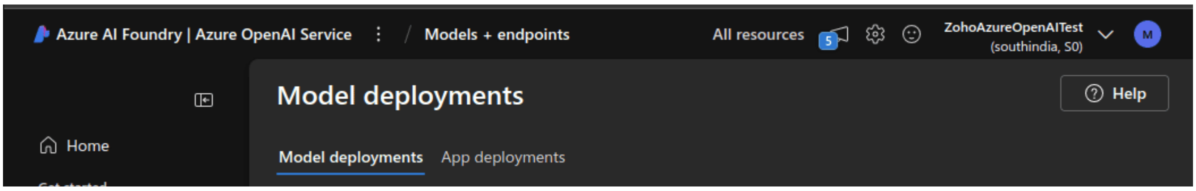
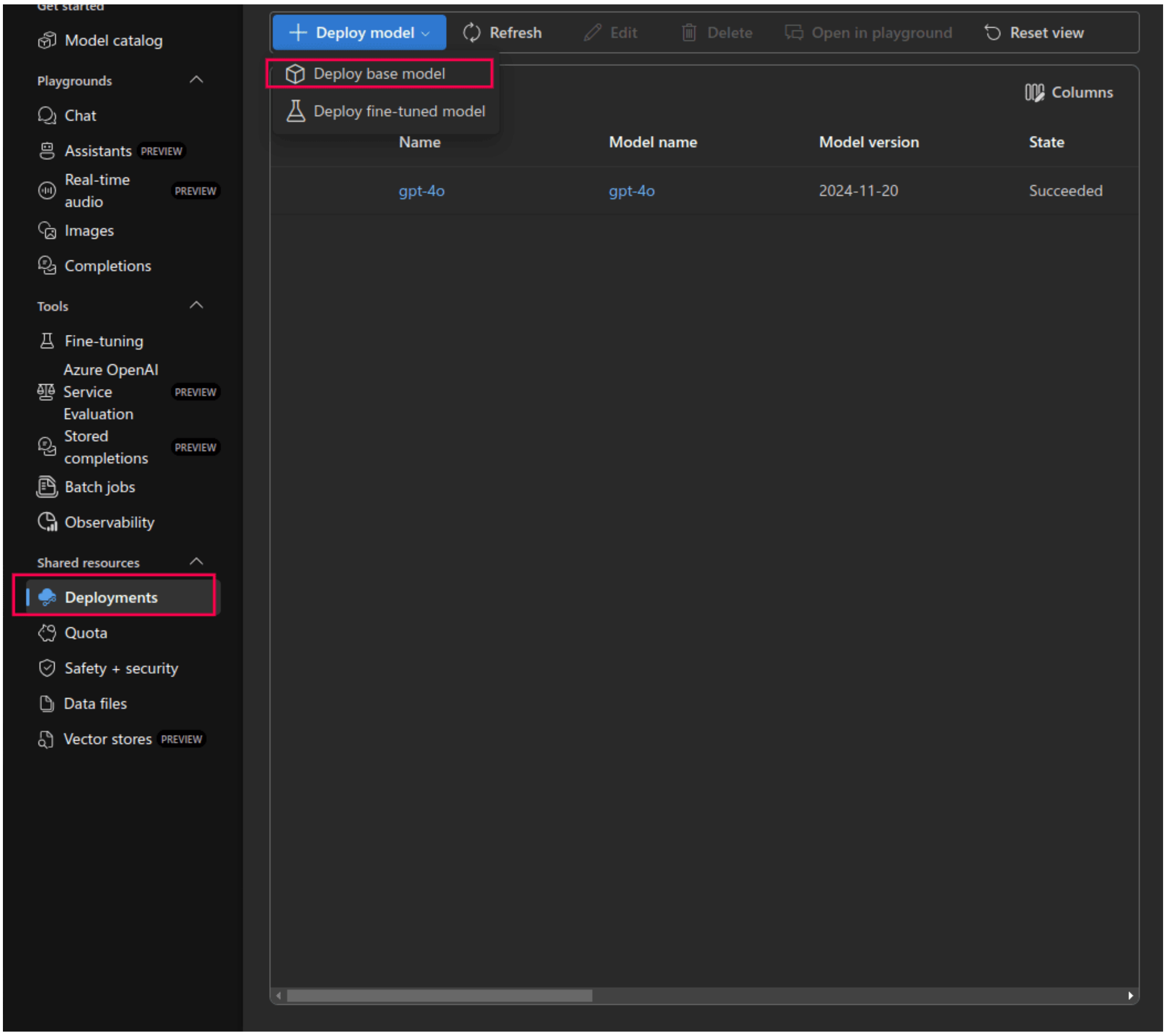

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Azure AI services | Azure OpenAI >
ZohoAzureOpenAITest
Azure OpenAI
Search
Go to Azure AI Foundry portal
Delete
Overview
Essentials
JSON View

Figure 13: Deploying a model in the Azure AI Foundry portal

2. On the Azure AI Foundry portal, navigate to the Deployments section, click Deploy model, and select Deploy base model.



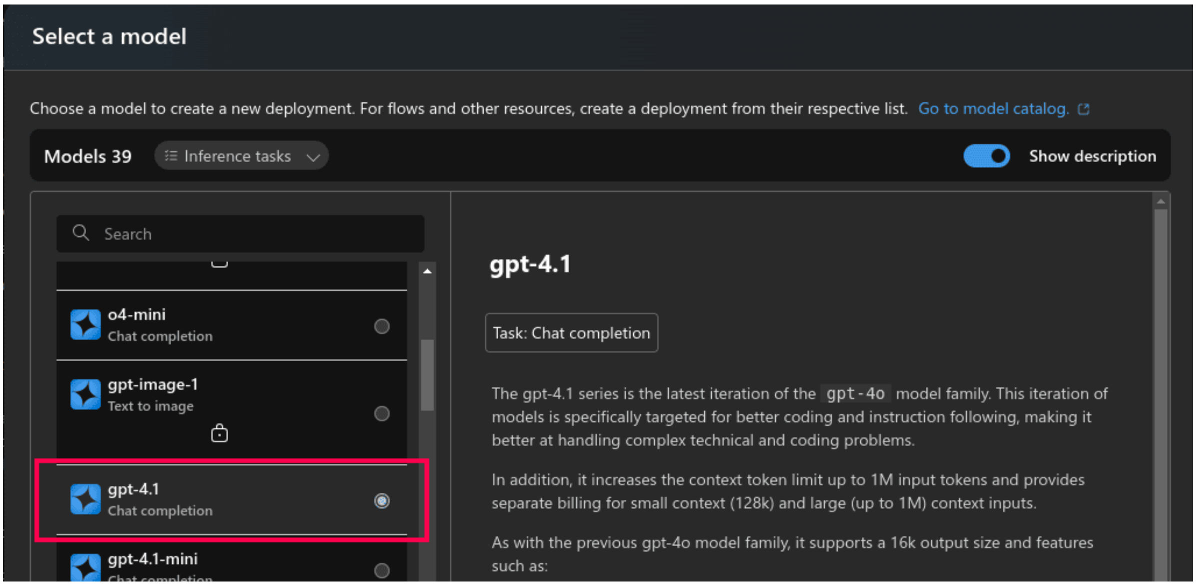


Name	Model name	Model version	State
gpt-4o	gpt-4o	2024-11-20	Succeeded

Figure 14: Deploying a model in Azure AI Foundry portal

3. Choose a model that meets the following constraints:

    - Must support the Chat Completion API (models GPT-4o or newer). For better results, use latest available model such as GPT-4.1 or newer. Avoid reasoning models like o1-preview and o1-mini because they do not support system prompts.

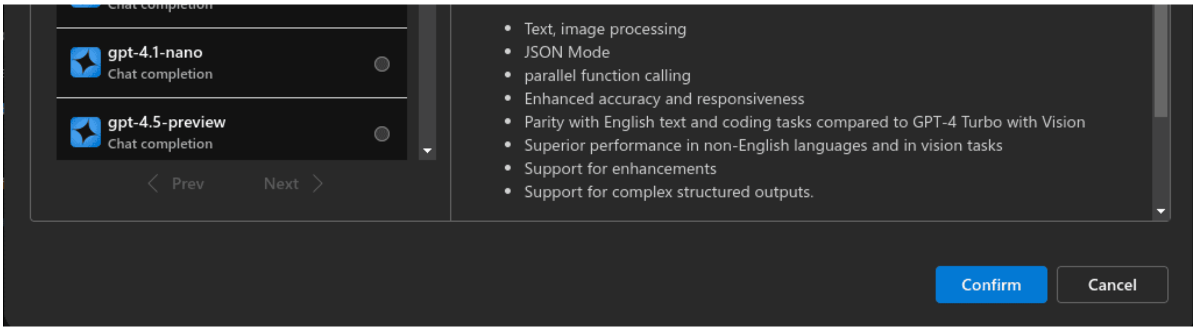


Choose a model to create a new deployment. For flows and other resources, create a deployment from their respective list. Go to model catalog.

The gpt-4.1 series is the latest iteration of the `gpt-4o` model family. This iteration of models is specifically targeted for better coding and instruction following, making it better at handling complex technical and coding problems.

In addition, it increases the context token limit up to 1M input tokens and provides separate billing for small context (128k) and large (up to 1M) context inputs.

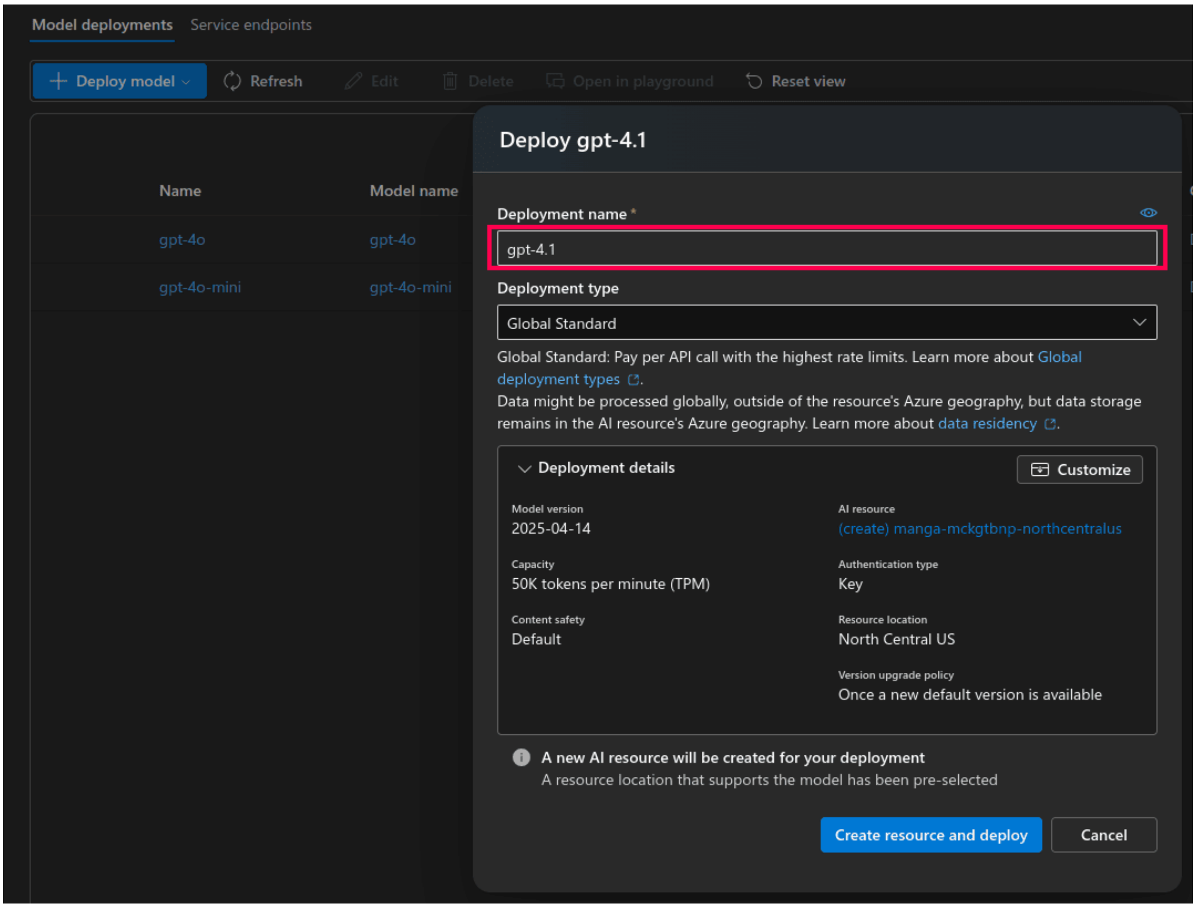
As with the previous gpt-4o model family, it supports a 16k output size and features such as:



- Text, image processing
- JSON Mode
- parallel function calling
- Enhanced accuracy and responsiveness
- Parity with English text and coding tasks compared to GPT-4 Turbo with Vision
- Superior performance in non-English languages and in vision tasks
- Support for enhancements
- Support for complex structured outputs.

Figure 15: Available models for deployment in Azure AI Foundry portal

4. Enter a deployment name of your choice (defaults to the model name).



Deploy gpt-4.1

Deployment name *
gpt-4.1

Deployment type
Global Standard

Global Standard: Pay per API call with the highest rate limits. Learn more about Global deployment types.
Data might be processed globally, outside of the resource's Azure geography, but data storage remains in the AI resource's Azure geography. Learn more about data residency.

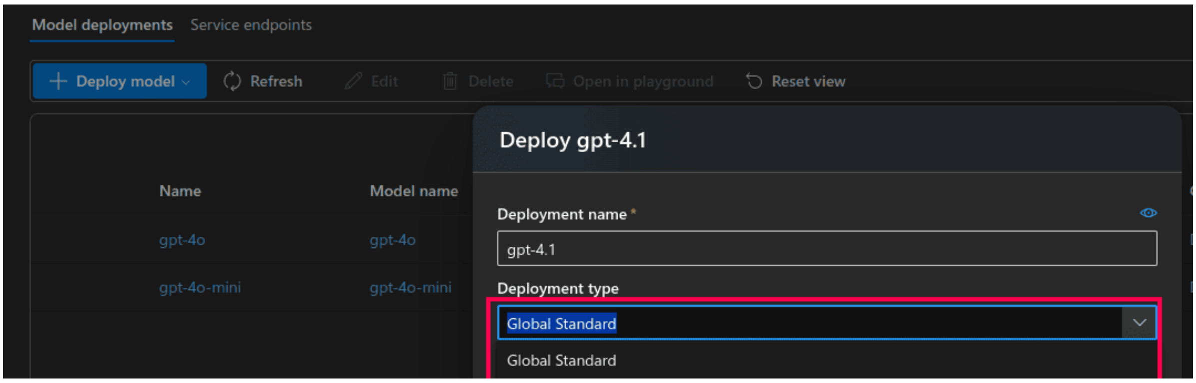
Deployment details

Model version: 2025-04-14
AI resource: (create) manga-mckgtbnp-northcentralus
Capacity: 50K tokens per minute (TPM)
Authentication type: Key
Content safety: Default
Resource location: North Central US
Version upgrade policy: Once a new default version is available

A new AI resource will be created for your deployment
A resource location that supports the model has been pre-selected

Figure 16: Deployment settings in Azure AI Foundry portal

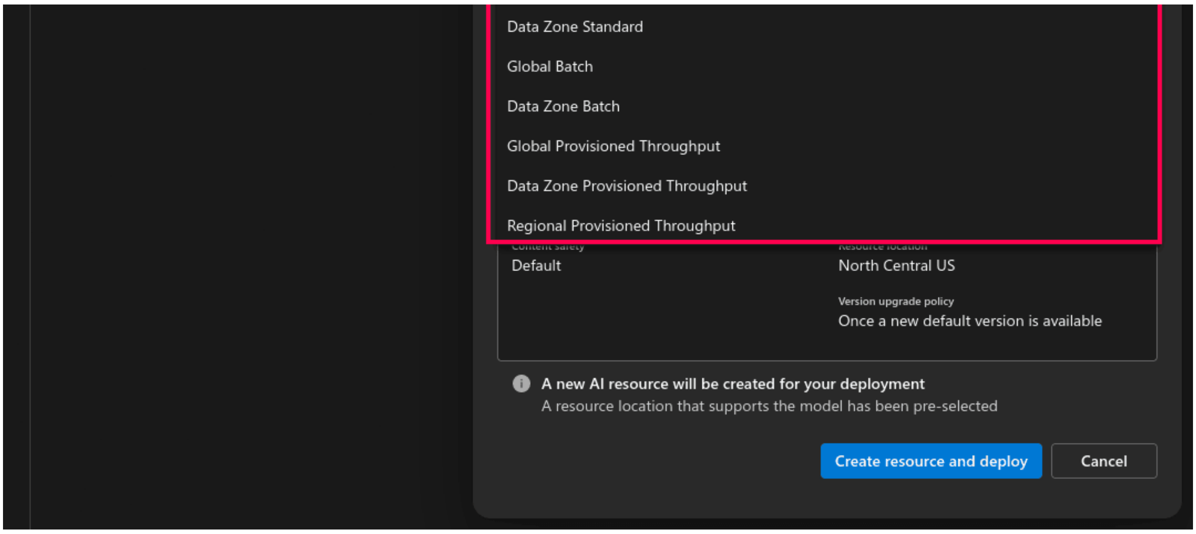
5. Select the deployment type based on your data processing needs. Learn more about deployment types.



Deploy gpt-4.1

Deployment name *
gpt-4.1

Deployment type
Global Standard
Global Standard



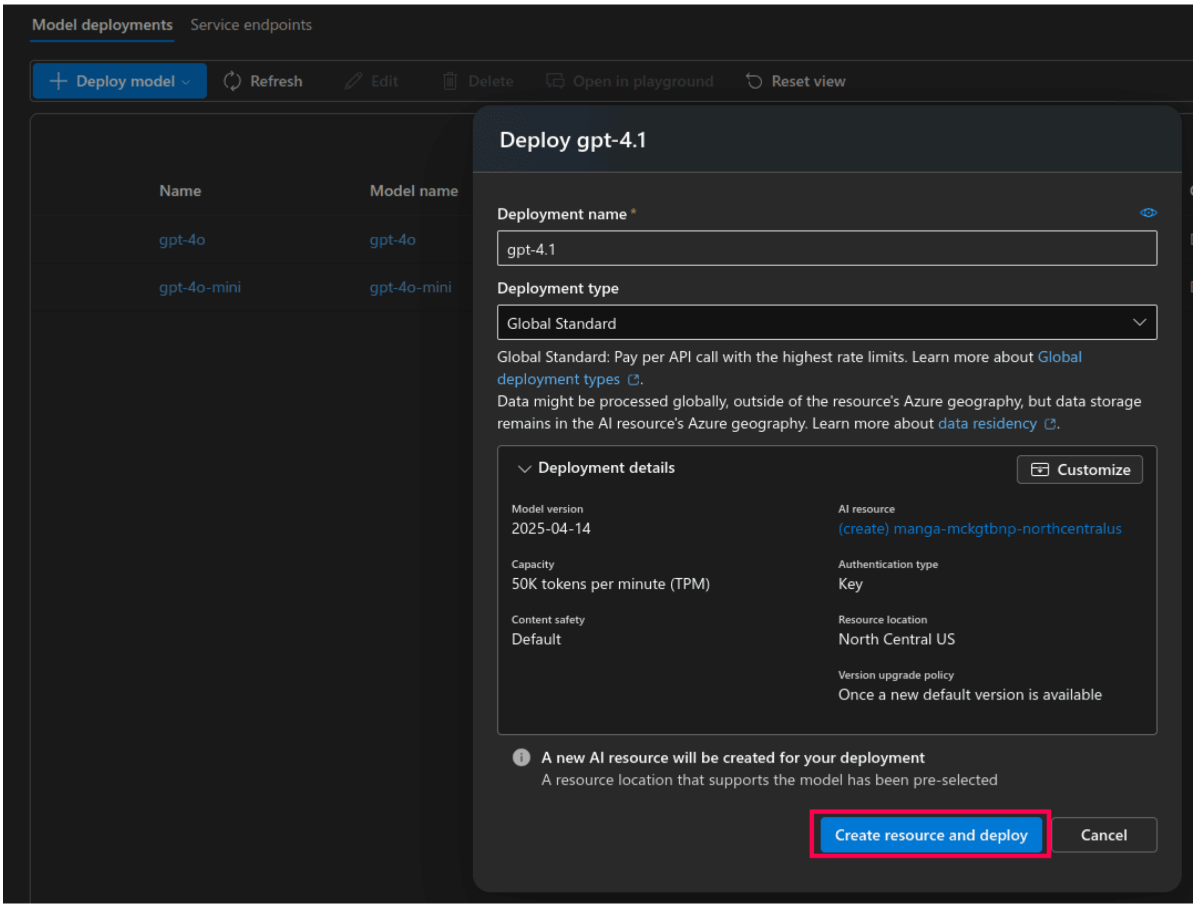
Data Zone Standard
Global Batch
Data Zone Batch
Global Provisioned Throughput
Data Zone Provisioned Throughput
Regional Provisioned Throughput

Content safety: Default
Resource location: North Central US
Version upgrade policy: Once a new default version is available

A new AI resource will be created for your deployment
A resource location that supports the model has been pre-selected

Figure 17: Deployment settings in Azure AI Foundry portal

6. Click Create resource and deploy to complete the model deployment.



Name	Model name
gpt-4o	gpt-4o
gpt-4o-mini	gpt-4o-mini

Deploy gpt-4.1

Deployment name *: gpt-4.1

Deployment type: Global Standard

Global Standard: Pay per API call with the highest rate limits. Learn more about Global deployment types.
Data might be processed globally, outside of the resource's Azure geography, but data storage remains in the AI resource's Azure geography. Learn more about data residency.

Deployment details

Model version: 2025-04-14
AI resource: (create) manga-mckgtbnp-northcentralus
Capacity: 50K tokens per minute (TPM)
Authentication type: Key
Content safety: Default
Resource location: North Central US
Version upgrade policy: Once a new default version is available

A new AI resource will be created for your deployment
A resource location that supports the model has been pre-selected

Figure 18: Model deployment in Azure AI Foundry portal

NOTE Once you've completed these steps and obtained your credentials, refer to this section to access Zia Insights.

Read also

This document detailed the configuration steps required to enable Zia Insights, including Azure OpenAI resource creation, model deployment, and integration setup. To leverage the capabilities of Zia Insights, refer to the following articles:

following articles:

- Using Zia Insights
- Invoking Zia Insights

4.2.2.4. Invoking Zia Insights

Last updated on: September 12, 2025

In this page

Overview

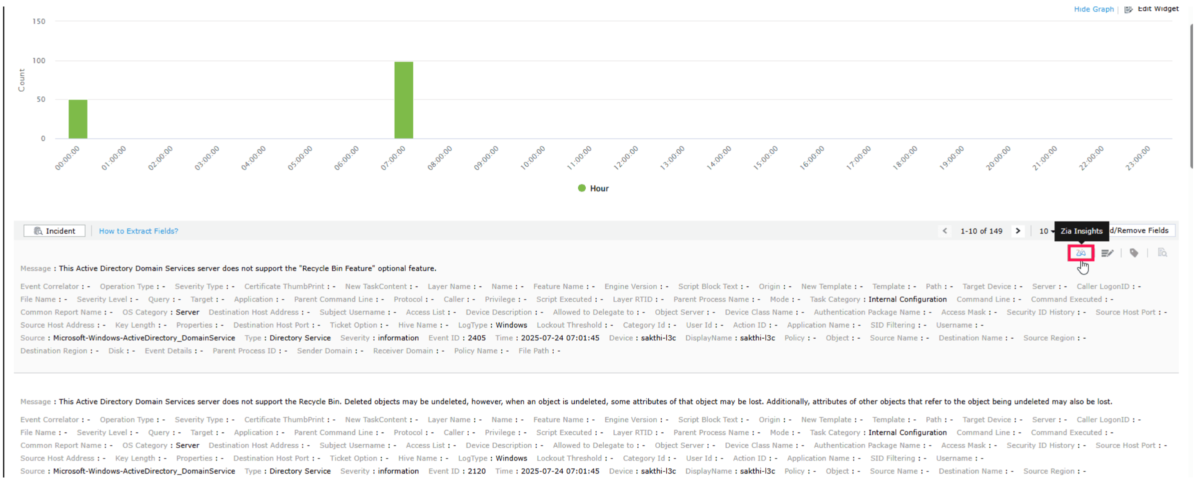
Zia Insights is an AI-powered capability that delivers contextual security insights by analyzing logs, alerts, and incidents. These insights help interpret security activity, identify impacted entities, map observed behavior to the MITRE ATT&CK® framework, and determine recommended response actions.
This page explains how to invoke Zia Insights from the Search, Alerts, and Incidents modules.

Invoking Zia Insights from Search

1. In your account, go to the Search tab.
2. Perform a search query using either the basic or advanced mode.

> NOTE
>
> Refer to this video to learn how to perform log searches.

3. In the search results, hover over a specific log entry.
4. Click on the zia icon on the top-right corner of the log entry to view insights generated by Zia.



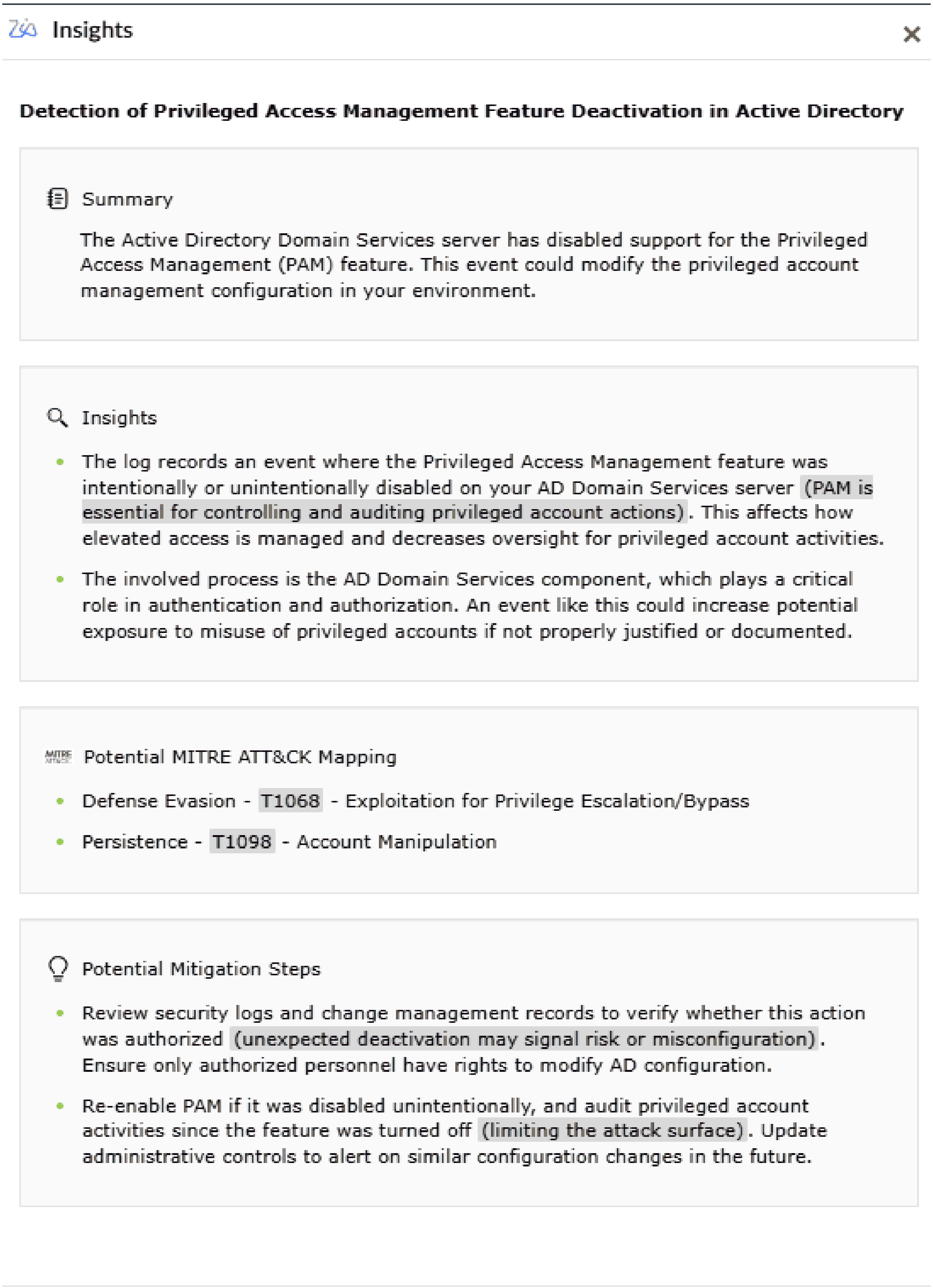
```
Message : This Active Directory Domain Services server does not support the "Recycle Bin Feature" optional feature.
Event Correlator : -   Operation Type : -   Severity Type : -   Certificate ThumbPrint : -   New TaskContent : -   Layer Name : -   Name : -   Feature Name : -   Engine Version : -   Script Block Text : -   Origin : -   New Template : -   Template : -   Path : -   Target Device : -   Server : -   Caller LogonID : -
File Name : -   Severity Level : -   Query : -   Target : -   Application : -   Parent Command Line : -   Protocol : -   Caller : -   Privilege : -   Script Executed : -   Layer RTID : -   Parent Process Name : -   Mode : -   Task Category : Internal Configuration   Command Line : -   Command Executed : -
Common Report Name : -   OS Category : Server   Destination Host Address : -   Subject Username : -   Access List : -   Device Description : -   Allowed to Delegate to : -   Object Server : -   Device Class Name : -   Authentication Package Name : -   Access Mask : -   Security ID History : -   Source Host Port : -
Source Host Address : -   Key Length : -   Properties : -   Destination Host Port : -   Ticket Option : -   Hive Name : -   LogType : Windows   Lockout Threshold : -   Category Id : -   User Id : -   Action ID : -   Application Name : -   SID Filtering : -   Username : -
Source : Microsoft-Windows-ActiveDirectory_DomainService   Type : Directory Service   Severity : information   Event ID : 2405   Time : 2025-07-24 07:01:45   Device : sakthi-l3c   DisplayName : sakthi-l3c   Policy : -   Object : -   Source Name : -   Destination Name : -   Source Region : -
Destination Region : -   Disk : -   Event Details : -   Parent Process ID : -   Sender Domain : -   Receiver Domain : -   Policy Name : -   File Path : -

Message : This Active Directory Domain Services server does not support the Recycle Bin. Deleted objects may be undeleted, however, when an object is undeleted, some attributes of that object may be lost. Additionally, attributes of other objects that refer to the object being undeleted may also be lost.
Event Correlator : -   Operation Type : -   Severity Type : -   Certificate ThumbPrint : -   New TaskContent : -   Layer Name : -   Name : -   Feature Name : -   Engine Version : -   Script Block Text : -   Origin : -   New Template : -   Template : -   Path : -   Target Device : -   Server : -   Caller LogonID : -
File Name : -   Severity Level : -   Query : -   Target : -   Application : -   Parent Command Line : -   Protocol : -   Caller : -   Privilege : -   Script Executed : -   Layer RTID : -   Parent Process Name : -   Mode : -   Task Category : Internal Configuration   Command Line : -   Command Executed : -
Common Report Name : -   OS Category : Server   Destination Host Address : -   Subject Username : -   Access List : -   Device Description : -   Allowed to Delegate to : -   Object Server : -   Device Class Name : -   Authentication Package Name : -   Access Mask : -   Security ID History : -   Source Host Port : -
Source Host Address : -   Key Length : -   Properties : -   Destination Host Port : -   Ticket Option : -   Hive Name : -   LogType : Windows   Lockout Threshold : -   Category Id : -   User Id : -   Action ID : -   Application Name : -   SID Filtering : -   Username : -
Source : Microsoft-Windows-ActiveDirectory_DomainService   Type : Directory Service   Severity : information   Event ID : 2120   Time : 2025-07-24 07:01:45   Device : sakthi-l3c   DisplayName : sakthi-l3c   Policy : -   Object : -   Source Name : -   Destination Name : -   Source Region : -
```

Figure 1: Invoking Zia Insights from Search

Figure 1: Invoking Zia Insights from Search

Insights provided by Zia Insights for Search

Zia will process the selected log and display contextual insights, including a summary, associated MITRE ATT&CK® techniques (if applicable), and suggested mitigation steps.



Insights

Detection of Privileged Access Management Feature Deactivation in Active Directory

Summary

The Active Directory Domain Services server has disabled support for the Privileged Access Management (PAM) feature. This event could modify the privileged account management configuration in your environment.

Insights

- The log records an event where the Privileged Access Management feature was intentionally or unintentionally disabled on your AD Domain Services server (PAM is essential for controlling and auditing privileged account actions). This affects how elevated access is managed and decreases oversight for privileged account activities.
- The involved process is the AD Domain Services component, which plays a critical role in authentication and authorization. An event like this could increase potential exposure to misuse of privileged accounts if not properly justified or documented.

Potential MITRE ATT&CK Mapping

- Defense Evasion - T1068 - Exploitation for Privilege Escalation/Bypass
- Persistence - T1098 - Account Manipulation

Potential Mitigation Steps

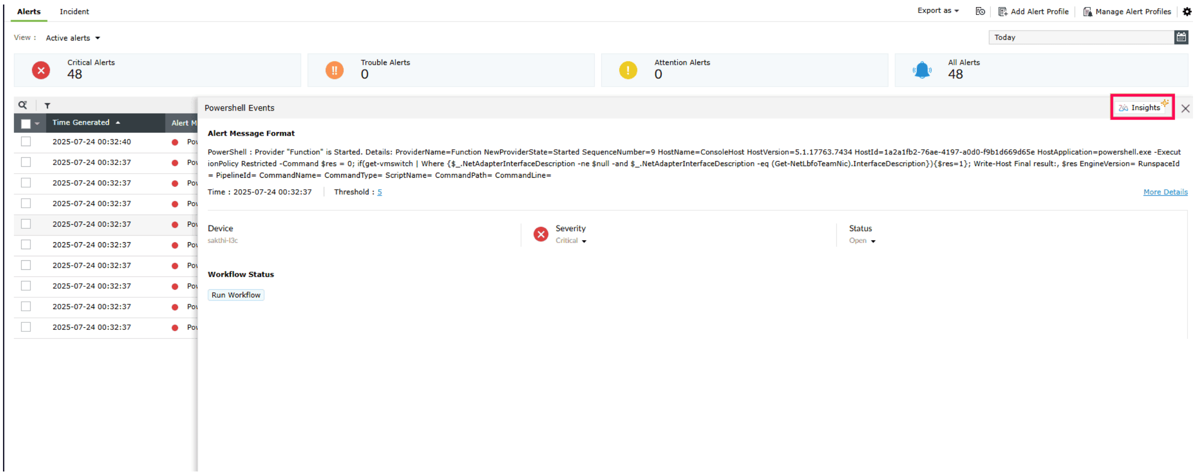
- Review security logs and change management records to verify whether this action was authorized (unexpected deactivation may signal risk or misconfiguration). Ensure only authorized personnel have rights to modify AD configuration.
- Re-enable PAM if it was disabled unintentionally, and audit privileged account activities since the feature was turned off (limiting the attack surface). Update administrative controls to alert on similar configuration changes in the future.

Zia can make mistakes. This insight is generated based solely on the current log and doesn't incorporate other logs.

Figure 2: Zia Insights generated for the selected log

Invoking Zia Insights from Alerts

1. In your account, go to the Alerts tab and select Alerts.
2. Select an alert from the list.
3. Click on the Zia insights icon displayed at the top-right corner to generate Zia Insights.



Time Generated	Alert M
2025-07-24 00:32:40	Po
2025-07-24 00:32:37	Po
2025-07-24 00:32:37	Po
2025-07-24 00:32:37	Po
2025-07-24 00:32:37	Po
2025-07-24 00:32:37	Po
2025-07-24 00:32:37	Po
2025-07-24 00:32:37	Po
2025-07-24 00:32:37	Po
2025-07-24 00:32:37	Po

Powershell Events

Alert Message Format

```
PowerShell : Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started SequenceNumber=9 HostName=ConsoleHost HostVersion=5.1.17763.7434 HostId=1a2a1fb2-76ae-4197-a0d0-f9b1d669d65e HostApplication=powershell.exe -ExecutionPolicy Restricted -Command $res = 0; if(get-vmswitch | Where {$_.NetAdapterInterfaceDescription -ne $null -and $_.NetAdapterInterfaceDescription -eq (Get-NetLbfoTeamNic).InterfaceDescription}){$res=1}; Write-Host Final result:, $res EngineVersion= RunspaceId = PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
```

Time : 2025-07-24 00:32:37 | Threshold : 5

More Details

Device: sakthi-l3c

Severity: Critical

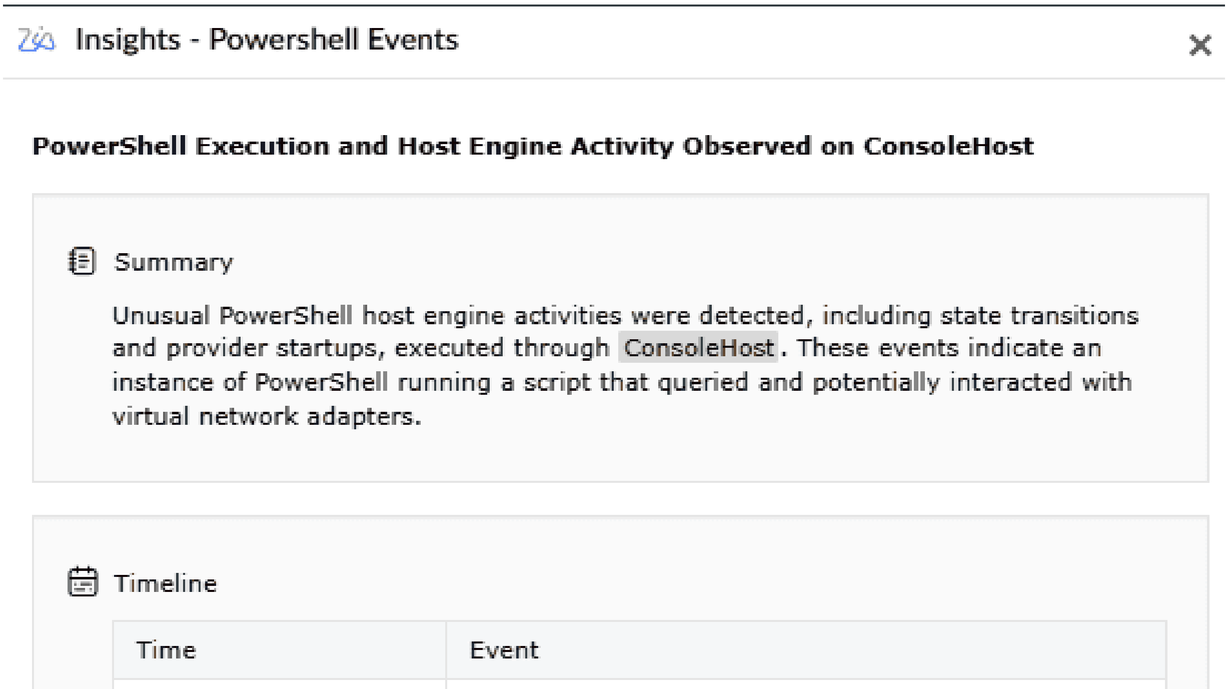
Status: Open

Workflow Status

Figure 3: Invoking Zia Insights from Alerts

Insights provided by Zia Insights for Alerts

For alerts, Zia Insights provides contextual summary, attack timeline, relevant MITRE ATT&CK® techniques (if applicable), and mitigation steps based on the alert data.



Insights - Powershell Events

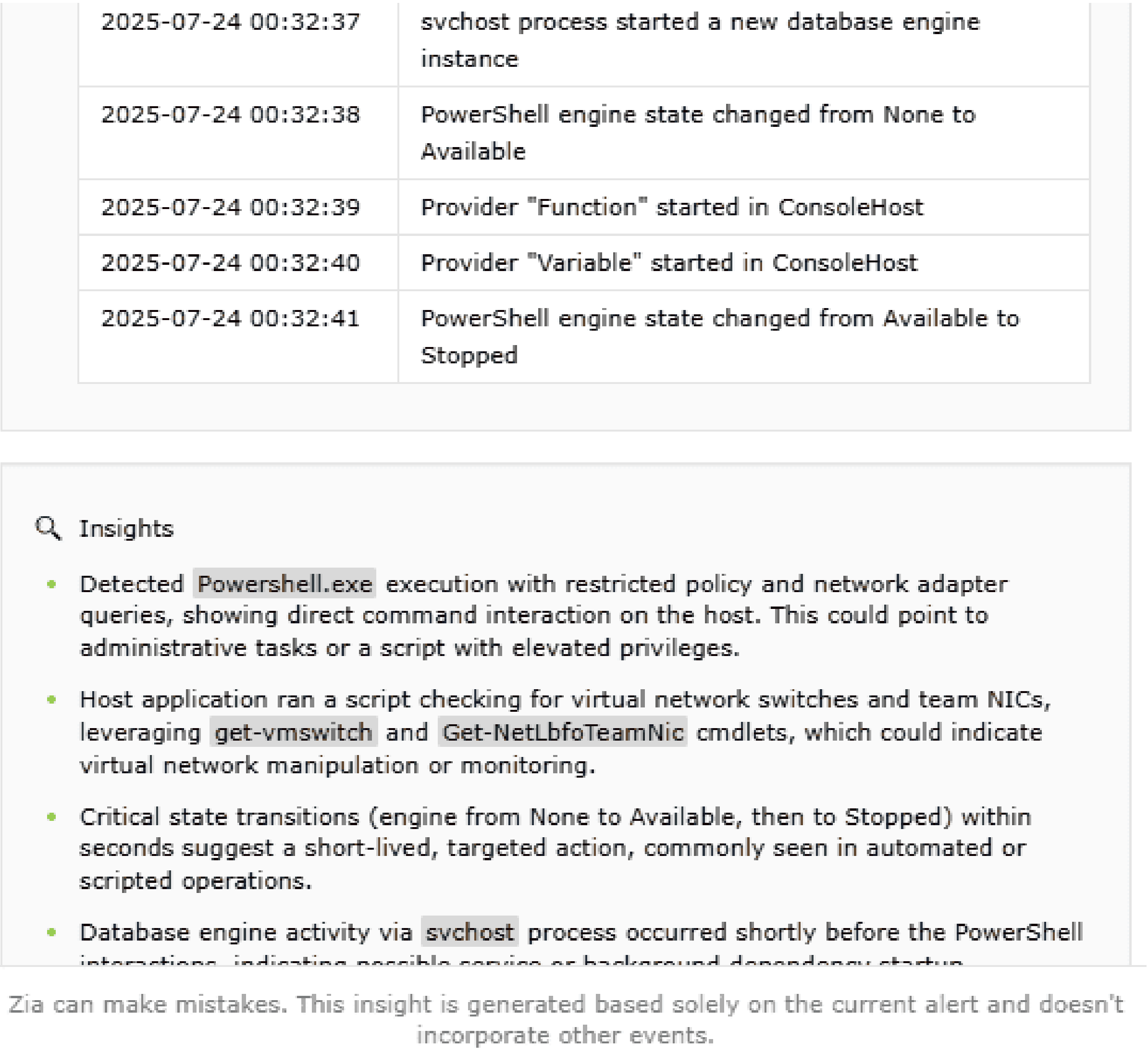
PowerShell Execution and Host Engine Activity Observed on ConsoleHost

Summary

Unusual PowerShell host engine activities were detected, including state transitions and provider startups, executed through ConsoleHost. These events indicate an instance of PowerShell running a script that queried and potentially interacted with virtual network adapters.

Timeline

Time	Event



2025-07-24 00:32:37	svchost process started a new database engine instance
2025-07-24 00:32:38	PowerShell engine state changed from None to Available
2025-07-24 00:32:39	Provider "Function" started in ConsoleHost
2025-07-24 00:32:40	Provider "Variable" started in ConsoleHost
2025-07-24 00:32:41	PowerShell engine state changed from Available to Stopped

Insights

- Detected Powershell.exe execution with restricted policy and network adapter queries, showing direct command interaction on the host. This could point to administrative tasks or a script with elevated privileges.
- Host application ran a script checking for virtual network switches and team NICs, leveraging get-vmswitch and Get-NetLbfoTeamNic cmdlets, which could indicate virtual network manipulation or monitoring.
- Critical state transitions (engine from None to Available, then to Stopped) within seconds suggest a short-lived, targeted action, commonly seen in automated or scripted operations.
- Database engine activity via svchost process occurred shortly before the PowerShell interactions, indicating possible service or background dependency startup

Zia can make mistakes. This insight is generated based solely on the current alert and doesn't incorporate other events.

Figure 4: Zia Insights generated for Alerts

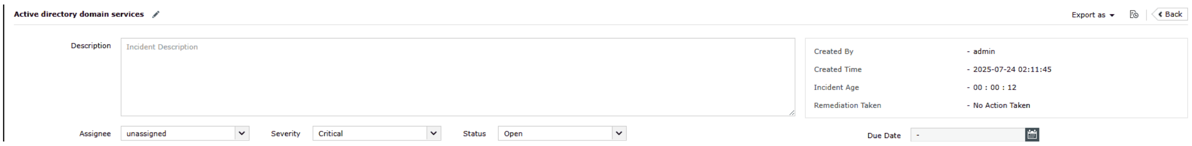
Invoking Zia Insights from Incidents

1. In your account, go to the Alerts tab and select Incident.

NOTE

Use the Select view dropdown to filter incidents. Select from All Incidents, Active Incidents, Critical Incidents, or create a new one using Add Custom View.

2. Select an incident from the list.
3. Click on the Zia insights icon to generate insights.



Active directory domain services

Description: Incident Description

Created By - admin

Created Time - 2025-07-24 02:11:45

Incident Age - 00 : 00 : 12

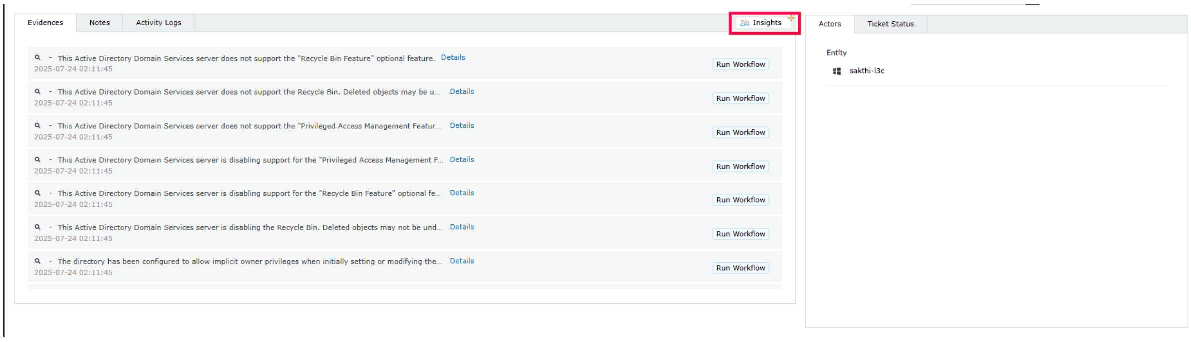
Remediation Taken - No Action Taken

Assignee: unassigned

Severity: Critical

Status: Open

Due Date: -



- This Active Directory Domain Services server does not support the "Recycle Bin Feature" optional feature. Details
2025-07-24 02:11:45 Run Workflow

- This Active Directory Domain Services server does not support the Recycle Bin. Deleted objects may be u... Details
2025-07-24 02:11:45 Run Workflow

- This Active Directory Domain Services server does not support the "Privileged Access Management Featur... Details
2025-07-24 02:11:45 Run Workflow

- This Active Directory Domain Services server is disabling support for the "Privileged Access Management F... Details
2025-07-24 02:11:45 Run Workflow

- This Active Directory Domain Services server is disabling support for the "Recycle Bin Feature" optional fe... Details
2025-07-24 02:11:45 Run Workflow

- This Active Directory Domain Services server is disabling the Recycle Bin. Deleted objects may not be und... Details
2025-07-24 02:11:45 Run Workflow

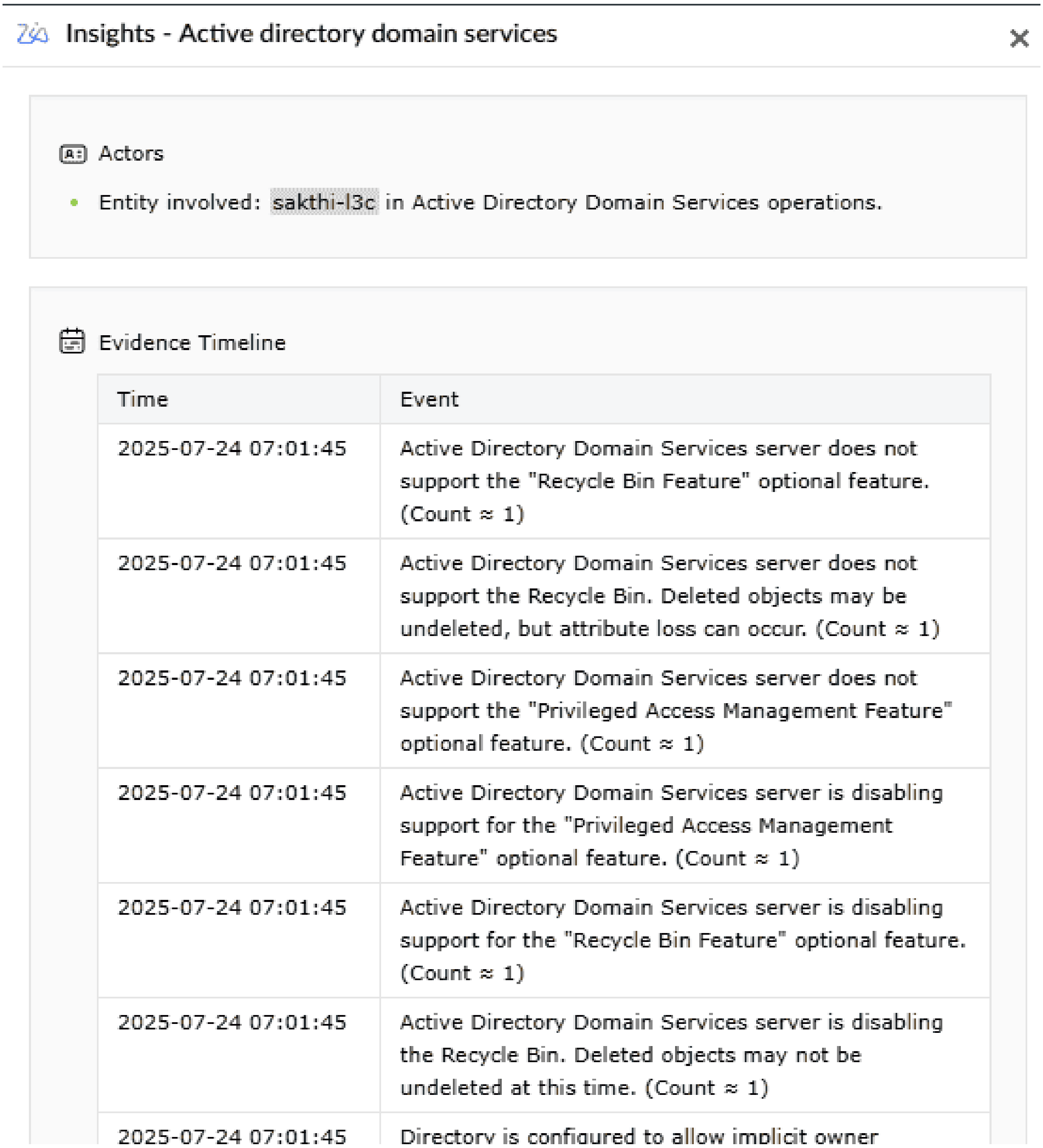
- The directory has been configured to allow implicit owner privileges when initially setting or modifying the... Details
2025-07-24 02:11:45 Run Workflow

Entity
sakthi-l3c

Figure 5: Invoking Zia Insights from Incidents

Insights provided by Zia Insights for Incidents

When invoked from the Incident console, Zia Insights provides details on involved actors, a chronological evidence timeline, evidence summary, and relevant MITRE ATT&CK® techniques based on the incident data.



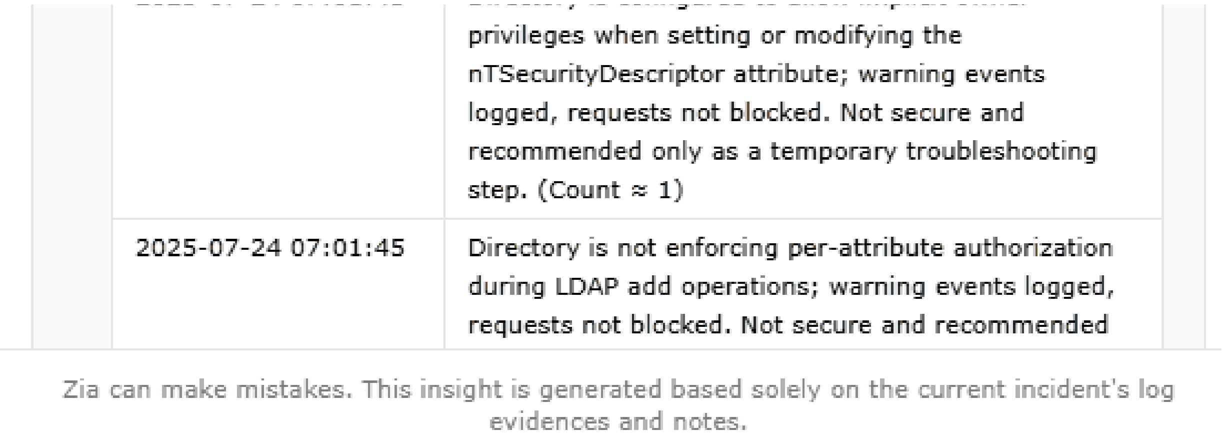
Insights - Active directory domain services

Actors

- Entity involved: sakthi-l3c in Active Directory Domain Services operations.

Evidence Timeline

Time	Event
2025-07-24 07:01:45	Active Directory Domain Services server does not support the "Recycle Bin Feature" optional feature. (Count ≈ 1)
2025-07-24 07:01:45	Active Directory Domain Services server does not support the Recycle Bin. Deleted objects may be undeleted, but attribute loss can occur. (Count ≈ 1)
2025-07-24 07:01:45	Active Directory Domain Services server does not support the "Privileged Access Management Feature" optional feature. (Count ≈ 1)
2025-07-24 07:01:45	Active Directory Domain Services server is disabling support for the "Privileged Access Management Feature" optional feature. (Count ≈ 1)
2025-07-24 07:01:45	Active Directory Domain Services server is disabling support for the "Recycle Bin Feature" optional feature. (Count ≈ 1)
2025-07-24 07:01:45	Active Directory Domain Services server is disabling the Recycle Bin. Deleted objects may not be undeleted at this time. (Count ≈ 1)
2025-07-24 07:01:45	Directory is configured to allow implicit owner



	privileges when setting or modifying the nTSecurityDescriptor attribute; warning events logged, requests not blocked. Not secure and recommended only as a temporary troubleshooting step. (Count ≈ 1)
2025-07-24 07:01:45	Directory is not enforcing per-attribute authorization during LDAP add operations; warning events logged, requests not blocked. Not secure and recommended

Zia can make mistakes. This insight is generated based solely on the current incident's log evidences and notes.

Figure 6: Zia Insights generated for Incidents

Read also

This document explained how to access Zia Insights from Search, Alerts, and Incidents within the product console to generate AI-powered security insights. For a comprehensive overview of Zia Insights and instructions on how to leverage its capabilities effectively, refer to the following articles:

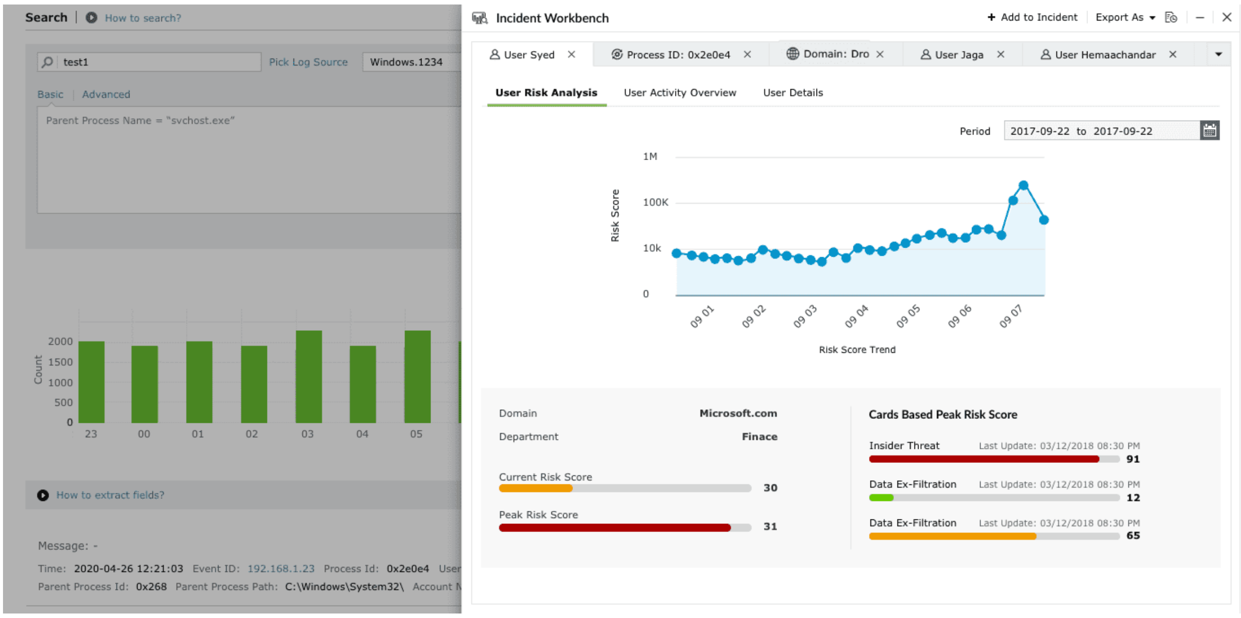
- Using Zia Insights
- Setting up Zia Insights

4.2.3.1. Overview

Last updated on: September 12, 2025

In this page

- 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.



Search | How to search?

test1 | Pick Log Source: Windows.1234

Basic | Advanced

Parent Process Name = "svchost.exe"

How to extract fields?

Message: -

Time: 2020-04-26 12:21:03 Event ID: 192.168.1.23 Process Id: 0x2e0e4 User

Parent Process Id: 0x268 Parent Process Path: C:\Windows\System32\ Account N

Incident Workbench

User Syed | Process ID: 0x2e0e4 | Domain: Dro | User Jaga | User Hemaachandar

User Risk Analysis | User Activity Overview | User Details

Period: 2017-09-22 to 2017-09-22

Domain: Microsoft.com

Department: Finace

Current Risk Score: 30

Peak Risk Score: 31

Cards Based Peak Risk Score

Insider Threat — Last Update: 03/12/2018 08:30 PM — 91

Data Ex-Filtration — Last Update: 03/12/2018 08:30 PM — 12

Data Ex-Filtration — Last Update: 03/12/2018 08:30 PM — 65

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

Analytics offered: Risk analysis from security vendors using Advanced Threat Analytics integration.

Access and usability:

- Roles and restrictions:
  - Operator and guest role members have no access to the Incident Workbench.
  - Custom roles can be created to provide access to the Incident Workbench.
- Access: Incident workbench can be invoked from multiple dashboards of EventLog Analyzer such as reports, log search, compliance, alerts, and more.
- Users can add upto 20 tabs in a single instance of the Incident Workbench and save it to an existing incident or create a new incident.

4.2.3.2. Incident Workbench Access

Last updated on: September 12, 2025

Note

Please refer to the Incident Workbench Overview page to learn about Incident Workbench. This page details on how to access the workbench in EventLog Analyzer.

- Log fields you can click on to invoke the Incident Workbench:

  Users:

  - Username
  - Target User
  - VPN UserName
  - User Principal Name
  - Destination User
  - Sourceuser
  - Subject Username

  Process:

  - Process Id
  - Parent Process ID
  - Process GUID
  - Parent Process GUID
  - Process Name
  - Parent Process Name

  Domain analysis:

  - Domain
  - URL Site

  IP Analysis:

  - Source IP
  - Client IP Address
  - Server IP Address
  - Address
  - Destination IP

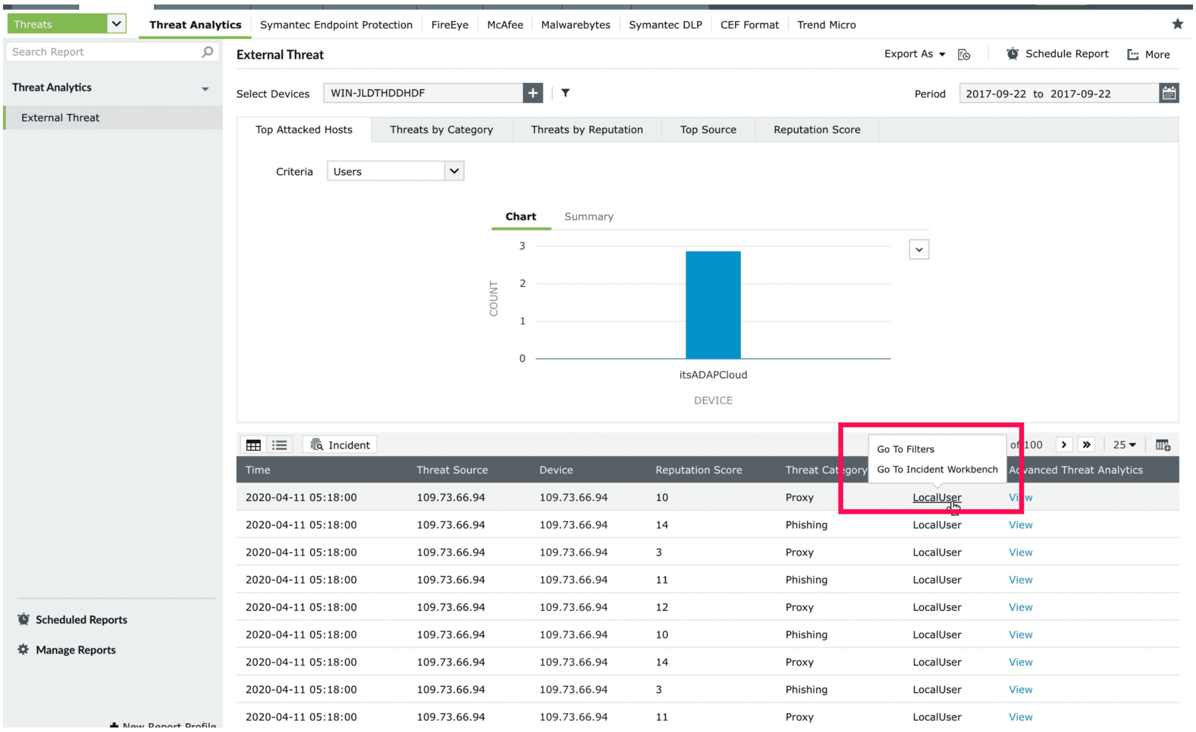
- Remote Ip
- Source Host Address
- NAT Source Address
- NAT Destination Address
- Destination IP
- Original Client IP
- IP Address
- Endpoint IP
- Private Ip
- Target Ip

URL Analysis:

- Payload URL
- Object URL
- URL

Invoking the Incident Workbench from different dashboards of EventLog Analyzer:

- From Reports



External Threat

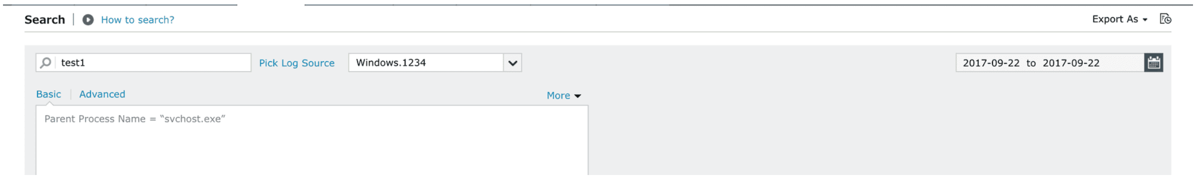
Select Devices: WIN-JLDTHDDHDF

Period: 2017-09-22 to 2017-09-22

Criteria: Users

Time	Threat Source	Device	Reputation Score	Threat Category		Advanced Threat Analytics
2020-04-11 05:18:00	109.73.66.94	109.73.66.94	10	Proxy	LocalUser	View
2020-04-11 05:18:00	109.73.66.94	109.73.66.94	14	Phishing	LocalUser	View
2020-04-11 05:18:00	109.73.66.94	109.73.66.94	3	Proxy	LocalUser	View
2020-04-11 05:18:00	109.73.66.94	109.73.66.94	11	Phishing	LocalUser	View
2020-04-11 05:18:00	109.73.66.94	109.73.66.94	12	Proxy	LocalUser	View
2020-04-11 05:18:00	109.73.66.94	109.73.66.94	10	Phishing	LocalUser	View
2020-04-11 05:18:00	109.73.66.94	109.73.66.94	14	Proxy	LocalUser	View
2020-04-11 05:18:00	109.73.66.94	109.73.66.94	3	Phishing	LocalUser	View
2020-04-11 05:18:00	109.73.66.94	109.73.66.94	11	Proxy	LocalUser	View

- From Log Search

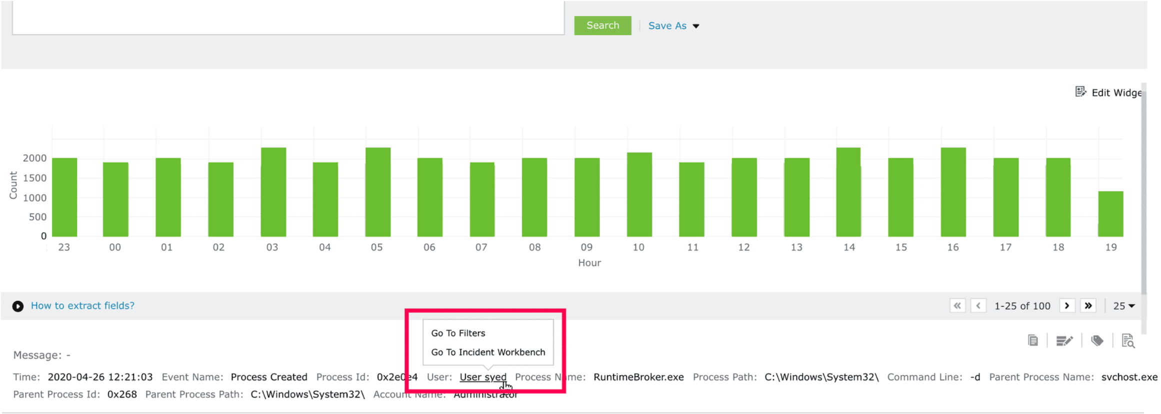


test1

Windows.1234

2017-09-22 to 2017-09-22

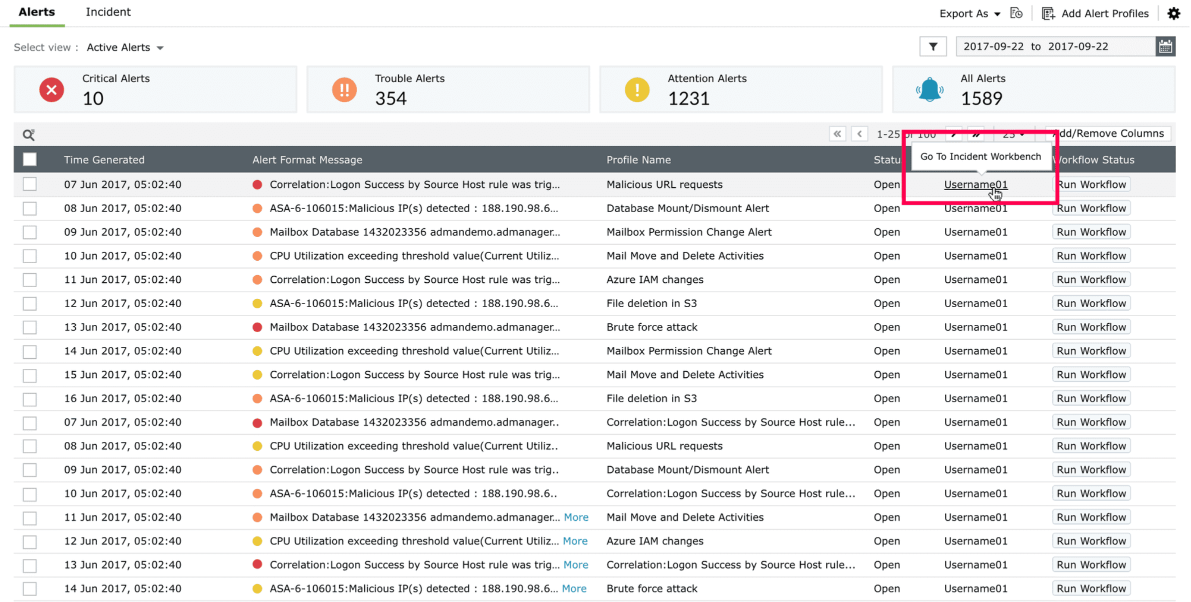
Parent Process Name = "svchost.exe"



Message: -

Time: 2020-04-26 12:21:03 Event Name: Process Created Process Id: 0x2e0e4 User: User syed Process Name: RuntimeBroker.exe Process Path: C:\Windows\System32\ Command Line: -d Parent Process Name: svchost.exe Parent Process Id: 0x268 Parent Process Path: C:\Windows\System32\ Account Name: Administrator

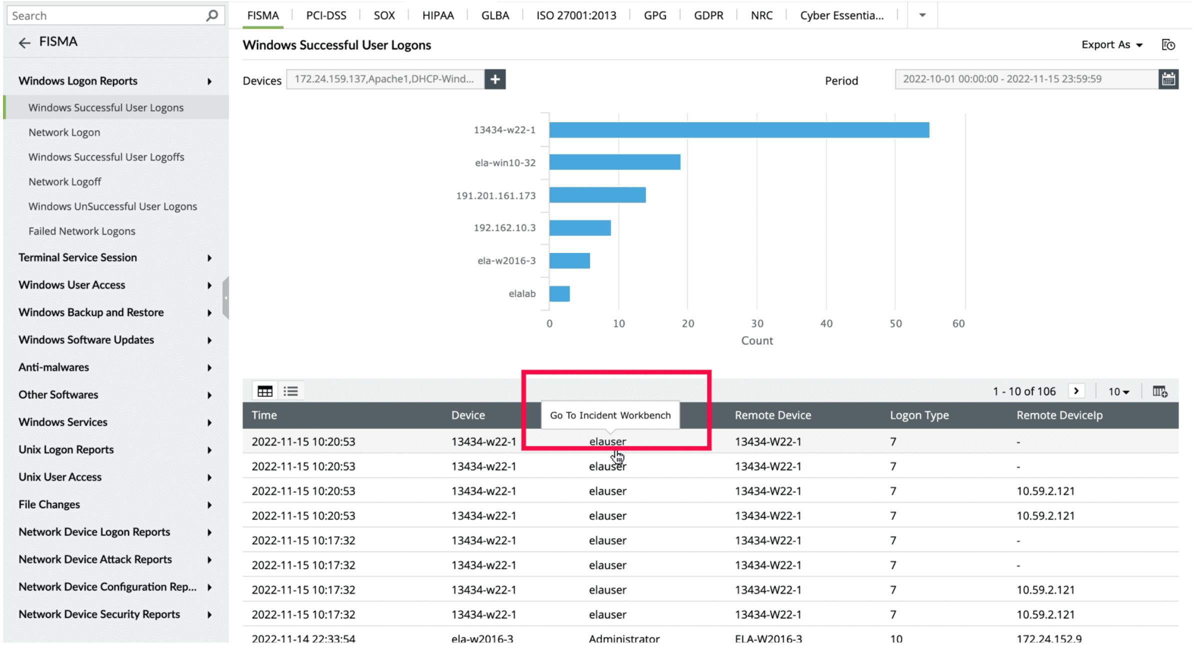
- From Alerts



Critical Alerts	Trouble Alerts	Attention Alerts	All Alerts
10	354	1231	1589

□	Time Generated	Alert Format Message	Profile Name	Statu		orkflow Status
□	07 Jun 2017, 05:02:40	● Correlation:Logon Success by Source Host rule was trig...	Malicious URL requests	Open	Username01	Run Workflow
□	08 Jun 2017, 05:02:40	● ASA-6-106015:Malicious IP(s) detected : 188.190.98.6...	Database Mount/Dismount Alert	Open	Username01	Run Workflow
□	09 Jun 2017, 05:02:40	● Mailbox Database 1432023356 admandemo.admanager...	Mailbox Permission Change Alert	Open	Username01	Run Workflow
□	10 Jun 2017, 05:02:40	● CPU Utilization exceeding threshold value(Current Utiliz...	Mail Move and Delete Activities	Open	Username01	Run Workflow
□	11 Jun 2017, 05:02:40	● Correlation:Logon Success by Source Host rule was trig...	Azure IAM changes	Open	Username01	Run Workflow
□	12 Jun 2017, 05:02:40	● ASA-6-106015:Malicious IP(s) detected : 188.190.98.6...	File deletion in S3	Open	Username01	Run Workflow
□	13 Jun 2017, 05:02:40	● Mailbox Database 1432023356 admandemo.admanager...	Brute force attack	Open	Username01	Run Workflow
□	14 Jun 2017, 05:02:40	● CPU Utilization exceeding threshold value(Current Utiliz...	Mailbox Permission Change Alert	Open	Username01	Run Workflow
□	15 Jun 2017, 05:02:40	● Correlation:Logon Success by Source Host rule was trig...	Mail Move and Delete Activities	Open	Username01	Run Workflow
□	16 Jun 2017, 05:02:40	● ASA-6-106015:Malicious IP(s) detected : 188.190.98.6...	File deletion in S3	Open	Username01	Run Workflow
□	07 Jun 2017, 05:02:40	● Mailbox Database 1432023356 admandemo.admanager..	Correlation:Logon Success by Source Host rule...	Open	Username01	Run Workflow
□	08 Jun 2017, 05:02:40	● CPU Utilization exceeding threshold value(Current Utiliz..	Malicious URL requests	Open	Username01	Run Workflow
□	09 Jun 2017, 05:02:40	● Correlation:Logon Success by Source Host rule was trig..	Database Mount/Dismount Alert	Open	Username01	Run Workflow
□	10 Jun 2017, 05:02:40	● ASA-6-106015:Malicious IP(s) detected : 188.190.98.6..	Correlation:Logon Success by Source Host rule...	Open	Username01	Run Workflow
□	11 Jun 2017, 05:02:40	● Mailbox Database 1432023356 admandemo.admanager... More	Mail Move and Delete Activities	Open	Username01	Run Workflow
□	12 Jun 2017, 05:02:40	● CPU Utilization exceeding threshold value(Current Utiliz... More	Azure IAM changes	Open	Username01	Run Workflow
□	13 Jun 2017, 05:02:40	● Correlation:Logon Success by Source Host rule was trig... More	Correlation:Logon Success by Source Host rule...	Open	Username01	Run Workflow
□	14 Jun 2017, 05:02:40	● ASA-6-106015:Malicious IP(s) detected : 188.190.98.6... More	Brute force attack	Open	Username01	Run Workflow

- From Compliance dashboard

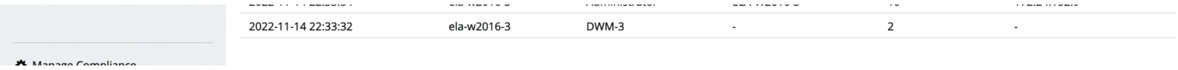


Windows Successful User Logons

Devices 172.24.159.137,Apache1,DHCP-Wind...

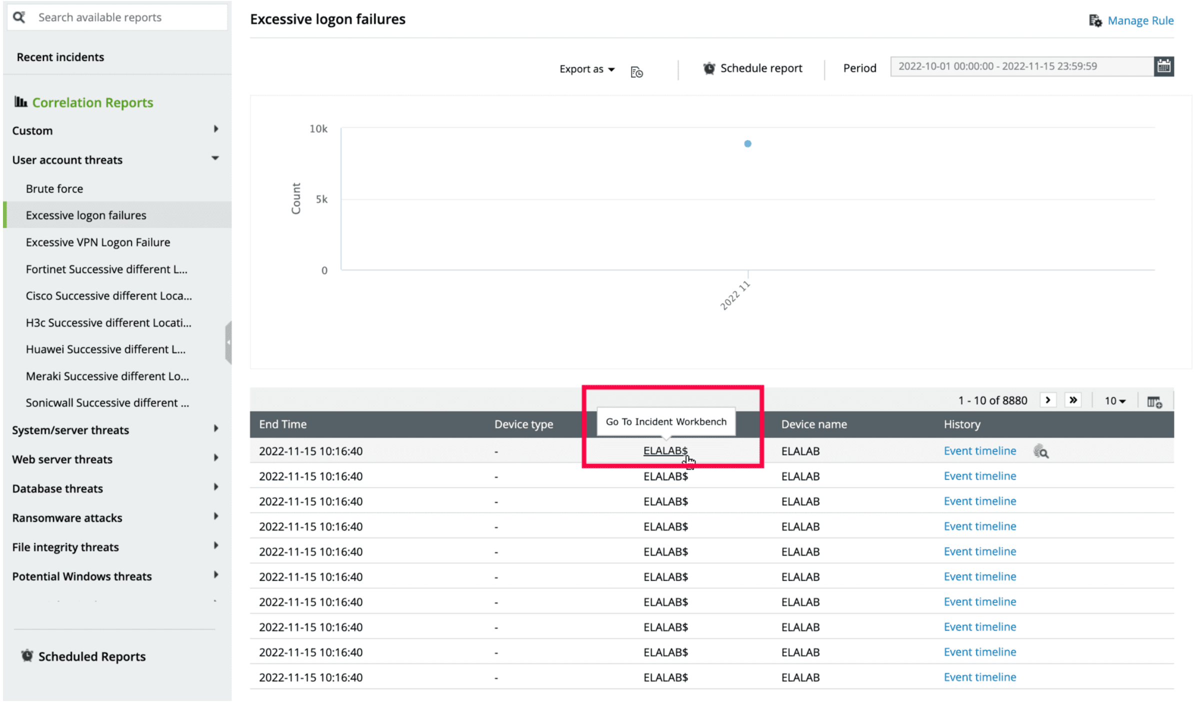
Period 2022-10-01 00:00:00 - 2022-11-15 23:59:59

Time	Device		Remote Device	Logon Type	Remote Devicelp
2022-11-15 10:20:53	13434-w22-1	elauser	13434-W22-1	7	-
2022-11-15 10:20:53	13434-w22-1	elauser	13434-W22-1	7	-
2022-11-15 10:20:53	13434-w22-1	elauser	13434-W22-1	7	10.59.2.121
2022-11-15 10:20:53	13434-w22-1	elauser	13434-W22-1	7	10.59.2.121
2022-11-15 10:17:32	13434-w22-1	elauser	13434-W22-1	7	-
2022-11-15 10:17:32	13434-w22-1	elauser	13434-W22-1	7	-
2022-11-15 10:17:32	13434-w22-1	elauser	13434-W22-1	7	10.59.2.121
2022-11-15 10:17:32	13434-w22-1	elauser	13434-W22-1	7	10.59.2.121
2022-11-14 22:33:54	ela-w2016-3	Administrator	ELA-W2016-3	10	172.24.152.9



2022-11-14 22:33:32	ela-w2016-3	DWM-3	-	2	-

- From Correlation

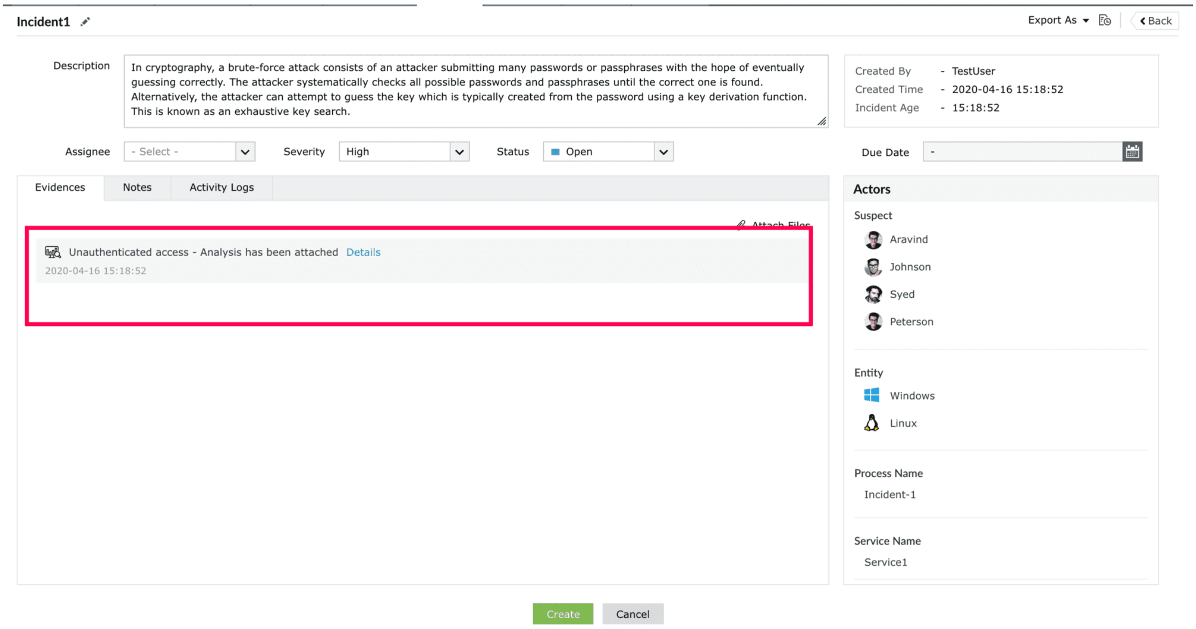


Excessive logon failures

Period 2022-10-01 00:00:00 - 2022-11-15 23:59:59

End Time	Device type		Device name	History
2022-11-15 10:16:40	-	ELALAB$	ELALAB	Event timeline
2022-11-15 10:16:40	-	ELALAB$	ELALAB	Event timeline
2022-11-15 10:16:40	-	ELALAB$	ELALAB	Event timeline
2022-11-15 10:16:40	-	ELALAB$	ELALAB	Event timeline
2022-11-15 10:16:40	-	ELALAB$	ELALAB	Event timeline
2022-11-15 10:16:40	-	ELALAB$	ELALAB	Event timeline
2022-11-15 10:16:40	-	ELALAB$	ELALAB	Event timeline
2022-11-15 10:16:40	-	ELALAB$	ELALAB	Event timeline
2022-11-15 10:16:40	-	ELALAB$	ELALAB	Event timeline
2022-11-15 10:16:40	-	ELALAB$	ELALAB	Event timeline

- From Incident management console



Incident1

Description: In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

Created By - TestUser
Created Time - 2020-04-16 15:18:52
Incident Age - 15:18:52

Assignee: - Select -
Severity: High
Status: Open
Due Date: -

Unauthenticated access - Analysis has been attached Details
2020-04-16 15:18:52

Suspect
Aravind
Johnson
Syed
Peterson

Entity
Windows
Linux

Process Name
Incident-1

Service Name
Service1

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.

4.2.3.3. User analytics in Incident Workbench

Last updated on: September 12, 2025

In this page

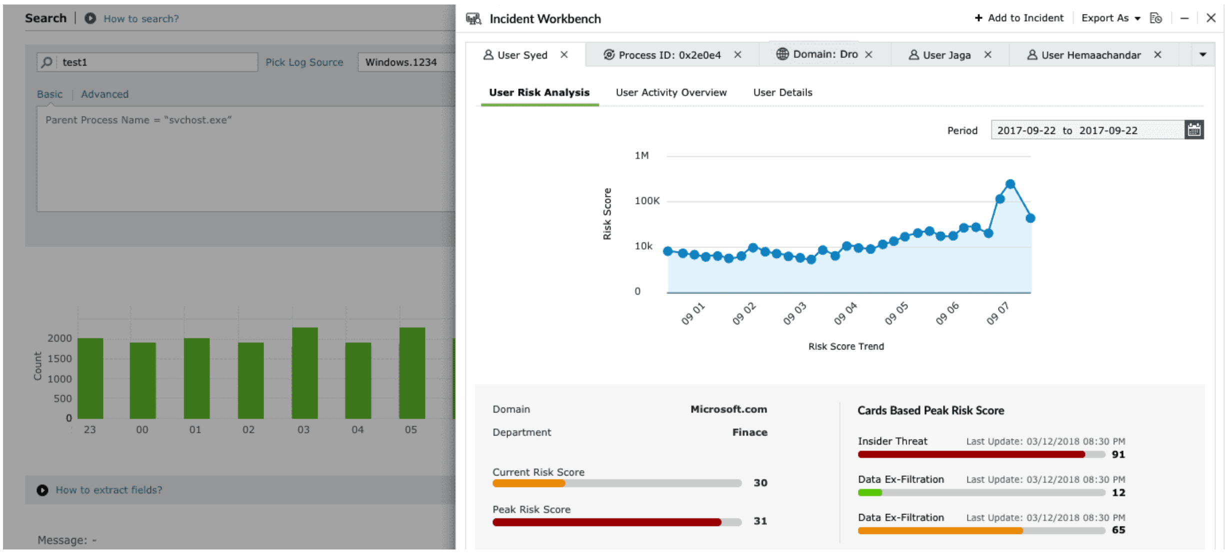
The user analytics data in Incident Workbench incorporates UEBA from the Log360 suite. It's necessary to purchase UEBA to get behaviour analytics and risk score trends of users.

1. Please refer to the Incident Workbench Overview page to learn about the feature, and check the Access page to learn how to invoke Incident Workbench from different dashboards of EventLog Analyzer.
2. To get user analytics, you can click on any of the following fields that uniquely identify a user:
   - Username
   - Target User
   - VPN UserName
   - User Principal Name
   - Destination User
   - Sourceuser
   - Subject Username

The following data will be available in the user analytics section of the Incident Workbench:

User Risk analysis

View the user's Risk Score Trend, Peak Risk Score and the Cards Based Peak Risk Score for possible insider threat and data exfiltration activities. Click on the Calendar icon and set the required period.



test1

Windows.1234

Parent Process Name = "svchost.exe"

Message: -

Period 2017-09-22 to 2017-09-22

Domain Microsoft.com

Department Finace

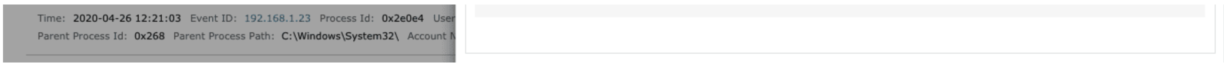
Current Risk Score 30

Peak Risk Score 31

Insider Threat Last Update: 03/12/2018 08:30 PM 91

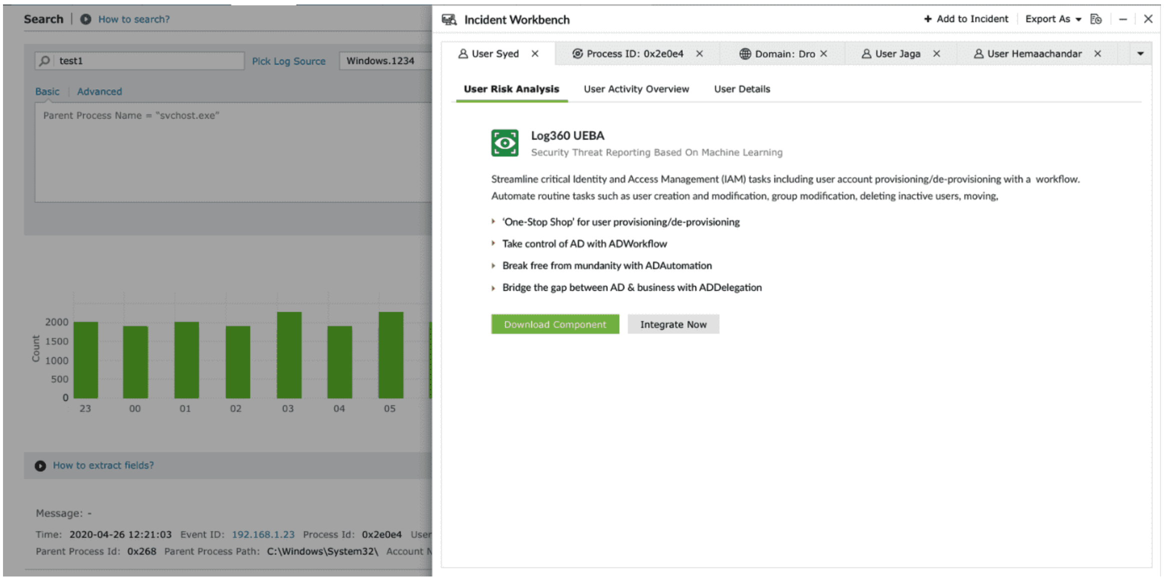
Data Ex-Filtration Last Update: 03/12/2018 08:30 PM 12

Data Ex-Filtration Last Update: 03/12/2018 08:30 PM 65



```
Time: 2020-04-26 12:21:03  Event ID: 192.168.1.23  Process Id: 0x2e0e4  User
Parent Process Id: 0x268  Parent Process Path: C:\Windows\System32\  Account N
```

- Here are the possible messages that will be displayed in the User Risk Analysis section and the causes
  - Case 1: UEBA not purchased



Log360 UEBA

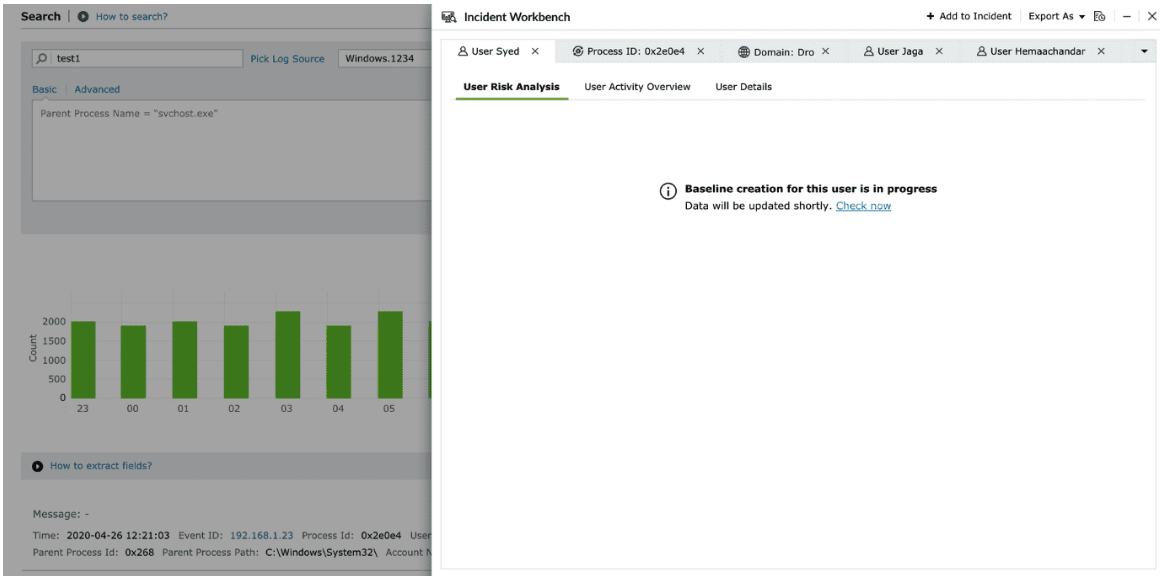
Security Threat Reporting Based On Machine Learning

Streamline critical Identity and Access Management (IAM) tasks including user account provisioning/de-provisioning with a workflow. Automate routine tasks such as user creation and modification, group modification, deleting inactive users, moving,

- 'One-Stop Shop' for user provisioning/de-provisioning
- Take control of AD with ADWorkflow
- Break free from mundanity with ADAutomation
- Bridge the gap between AD & business with ADDelegation

```
Message: -
Time: 2020-04-26 12:21:03  Event ID: 192.168.1.23  Process Id: 0x2e0e4  User
Parent Process Id: 0x268  Parent Process Path: C:\Windows\System32\  Account N
```

  - Case 2: Baseline creation is in progress as the model is training

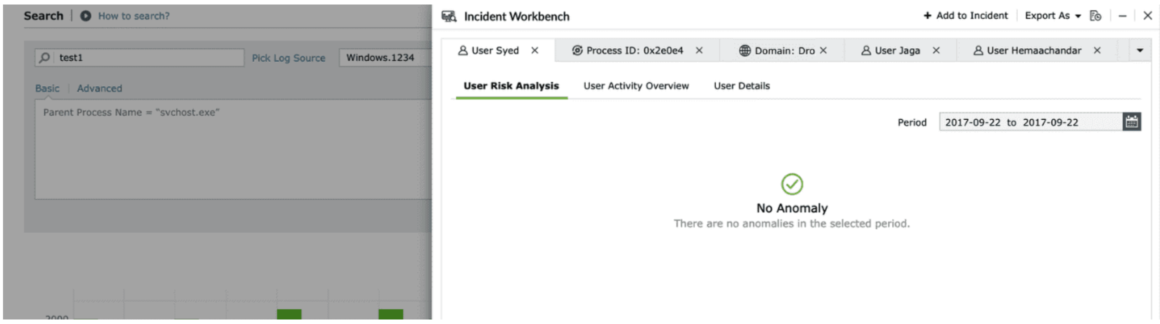


Baseline creation for this user is in progress

Data will be updated shortly. Check now

```
Message: -
Time: 2020-04-26 12:21:03  Event ID: 192.168.1.23  Process Id: 0x2e0e4  User
Parent Process Id: 0x268  Parent Process Path: C:\Windows\System32\  Account N
```

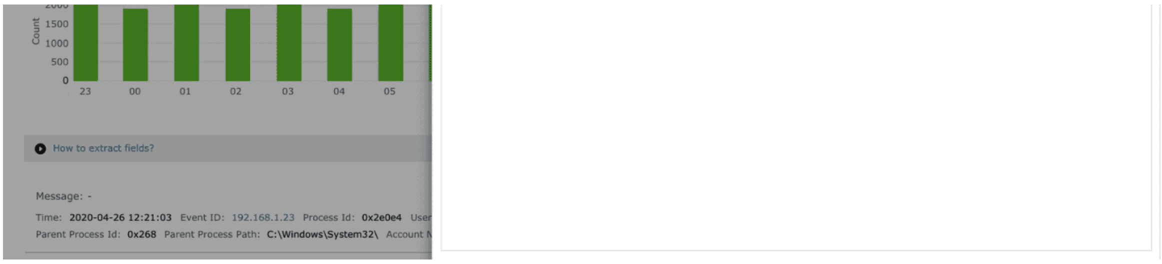
  - Case 3: The particular user has no anomalies



Period 2017-09-22 to 2017-09-22

No Anomaly

There are no anomalies in the selected period.



Message: -

Time: 2020-04-26 12:21:03 Event ID: 192.168.1.23 Process Id: 0x2e0e4 User

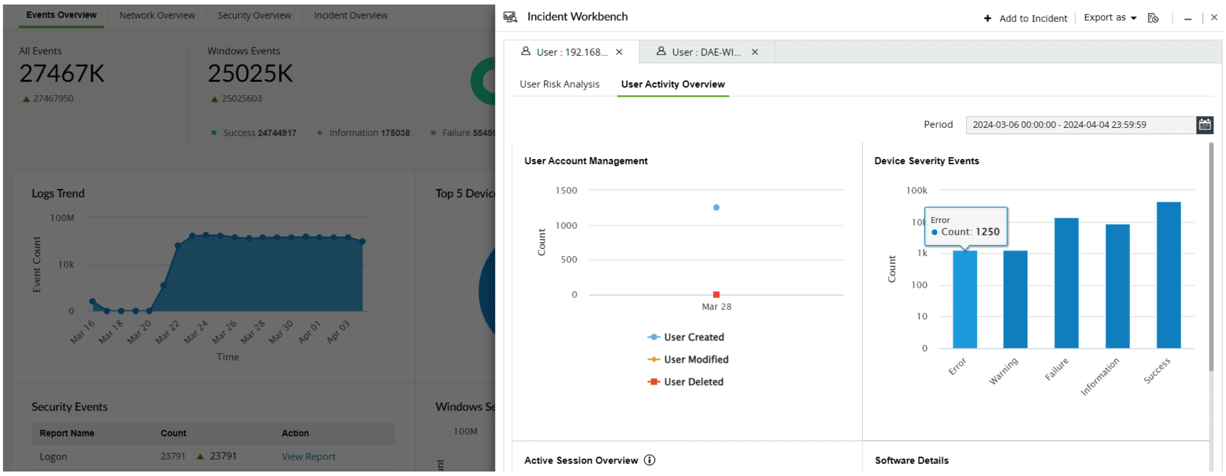
Parent Process Id: 0x268 Parent Process Path: C:\Windows\System32\ Account N

User Activity Overview

Note: The User Activity Overview section in the Incident Workbench does not require UEBA integration.

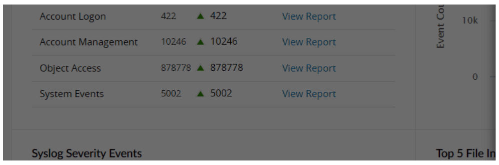
The User Activity Overview contains the following widgets:

User Account Management	Tracks create, modify, and delete actions related to the user account.
Device Severity Events	Consolidates the device severity events for the devices accessed by the user
Active Sessions Overview	Shows the list of active sessions on different devices and their duration
Software Installations and Updates	List of softwares installed, uninstalled and updated by the user during the selected period
Top 5 File Integrity Monitoring Events	Tracks events related to file creation, deletion, modification and access.
Process Tracking	Tracks process creation and termination activities

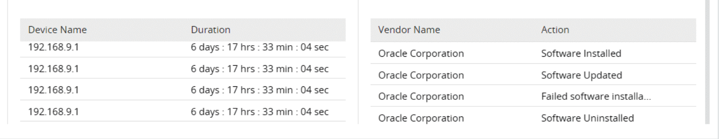


Period 2024-03-06 00:00:00 - 2024-04-04 23:59:59

Report Name	Count	Action
Logon	23791 ▲ 23791	View Report



Account Logon	422	▲ 422	View Report
Account Management	10246	▲ 10246	View Report
Object Access	878778	▲ 878778	View Report
System Events	5002	▲ 5002	View Report



Device Name	Duration
192.168.9.1	6 days : 17 hrs : 33 min : 04 sec
192.168.9.1	6 days : 17 hrs : 33 min : 04 sec
192.168.9.1	6 days : 17 hrs : 33 min : 04 sec
192.168.9.1	6 days : 17 hrs : 33 min : 04 sec

Vendor Name	Action
Oracle Corporation	Software Installed
Oracle Corporation	Software Updated
Oracle Corporation	Failed software installa...
Oracle Corporation	Software Uninstalled

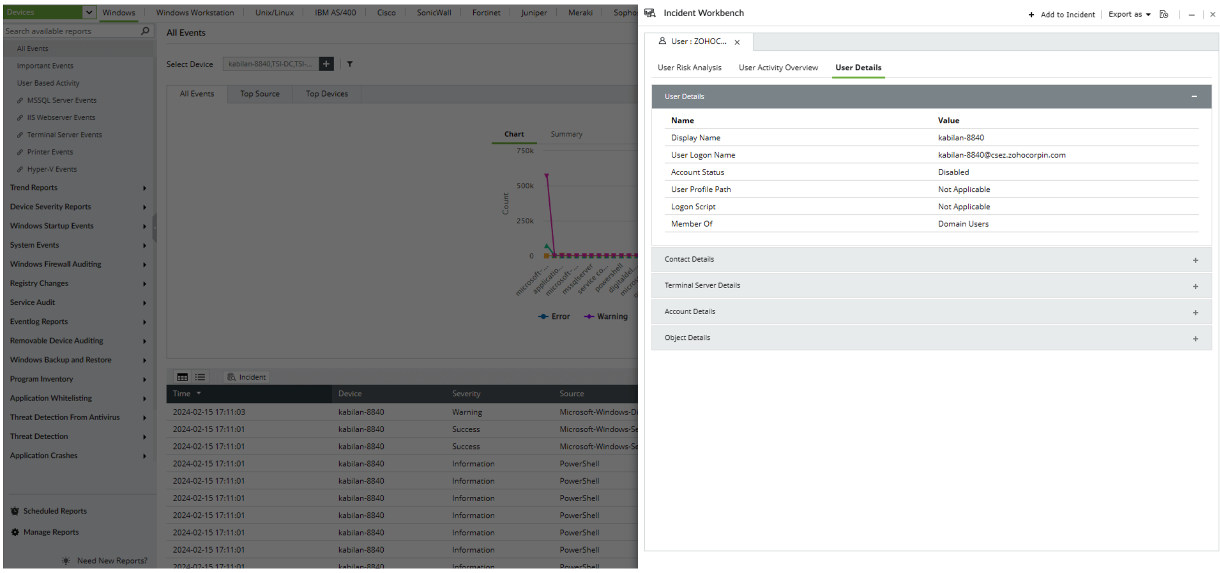
User Details

Note

The User Details section in the Incident Workbench doesn't require UEBA integration.

This sections fetches the Active Directory object details such as:

- User Details
- Contact Details
- Terminal Server Details
- Account Details and
- Object Details



Time	Device	Severity	Source
2024-02-15 17:11:03	kabilan-8840	Warning	Microsoft-Windows-Di
2024-02-15 17:11:01	kabilan-8840	Success	Microsoft-Windows-Se
2024-02-15 17:11:01	kabilan-8840	Success	Microsoft-Windows-Se
2024-02-15 17:11:01	kabilan-8840	Information	PowerShell
2024-02-15 17:11:01	kabilan-8840	Information	PowerShell
2024-02-15 17:11:01	kabilan-8840	Information	PowerShell
2024-02-15 17:11:01	kabilan-8840	Information	PowerShell
2024-02-15 17:11:01	kabilan-8840	Information	PowerShell
2024-02-15 17:11:01	kabilan-8840	Information	PowerShell
2024-02-15 17:11:01	kabilan-8840	Information	PowerShell

Name	Value
Display Name	kabilan-8840
User Logon Name	kabilan-8840@csez.zohocorpin.com
Account Status	Disabled
User Profile Path	Not Applicable
Logon Script	Not Applicable
Member Of	Domain Users

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.

4.2.3.4. Process analytics in Incident Workbench

Last updated on: September 12, 2025

In this page

The Process Analytics section of the Incident Workbench showcases process spawning with the parent child relationships and the process event details.

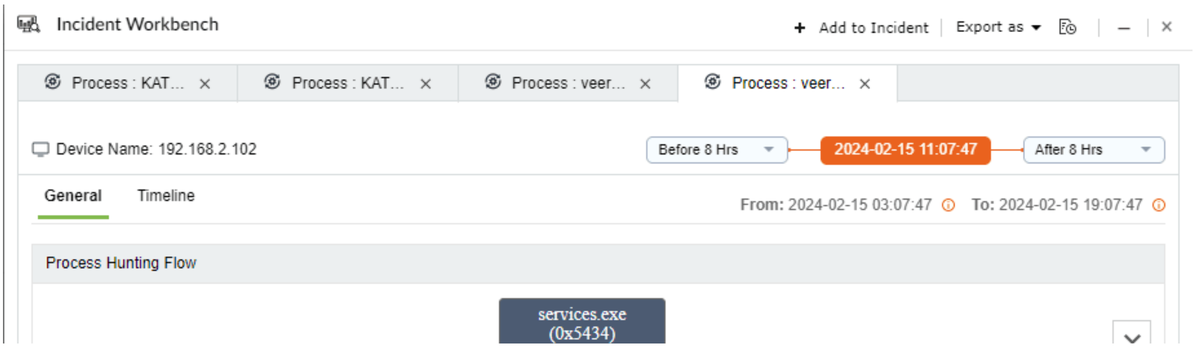
Note

1. Please refer to the Incident Workbench Overview page to learn about the feature, and check the Access page to learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer.
2. To access the process hunting tree, you can click on any of the following fields that uniquely identify a process:
   - Process Id
   - Parent Process ID
   - Process GUID
   - Parent Process GUID
   - Process Name
   - Parent Process Name
3. The process spawning will be available in graphical format for upto 50 child processes.

Process analytics views

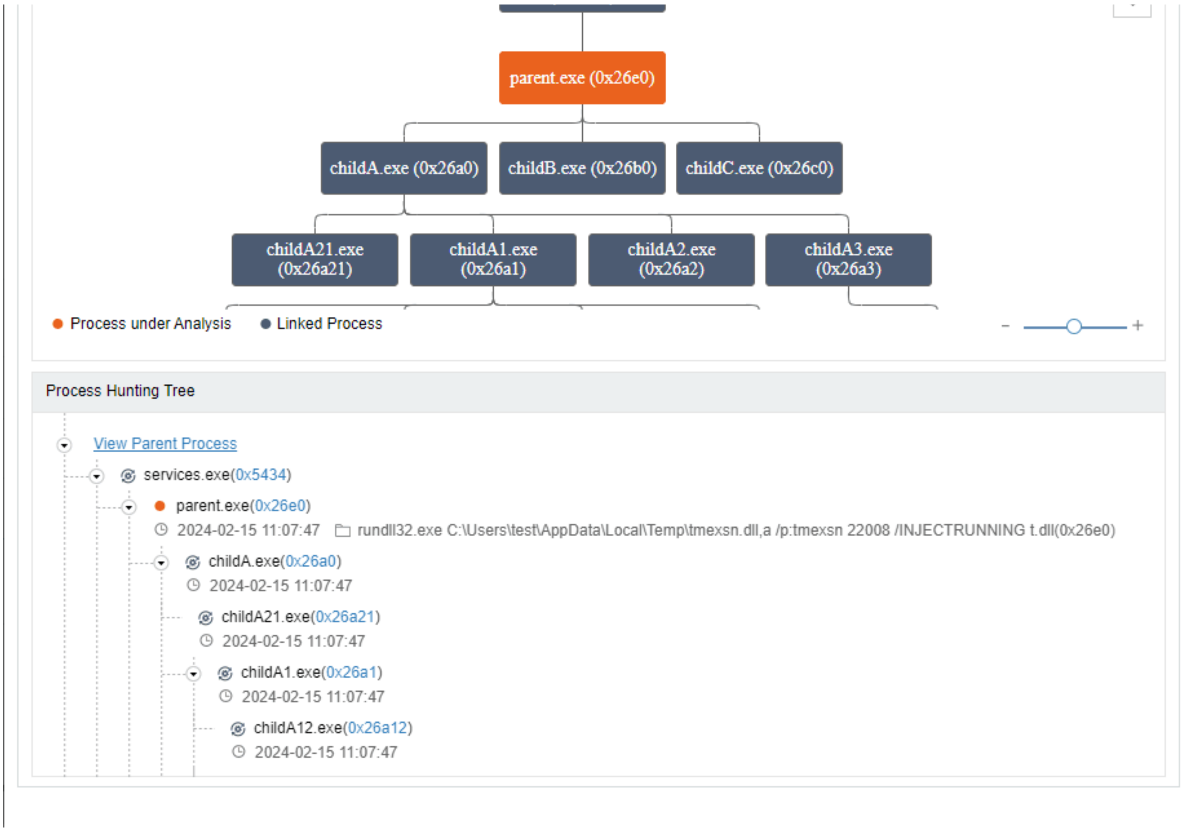
Here are the different graphical formats available in Incident Workbench to analyze process flow:

- Hierarchical tree with respective parent and children of the process



Device Name: 192.168.2.102

From: 2024-02-15 03:07:47 To: 2024-02-15 19:07:47



Process Hunting Tree

View Parent Process

services.exe(0x5434)

● parent.exe(0x26e0)

2024-02-15 11:07:47 rundll32.exe C:\Users\test\AppData\Local\Temp\tmexsn.dll,a /p:tmexsn 22008 /INJECTRUNNING t.dll(0x26e0)

childA.exe(0x26a0)

2024-02-15 11:07:47

childA21.exe(0x26a21)

2024-02-15 11:07:47

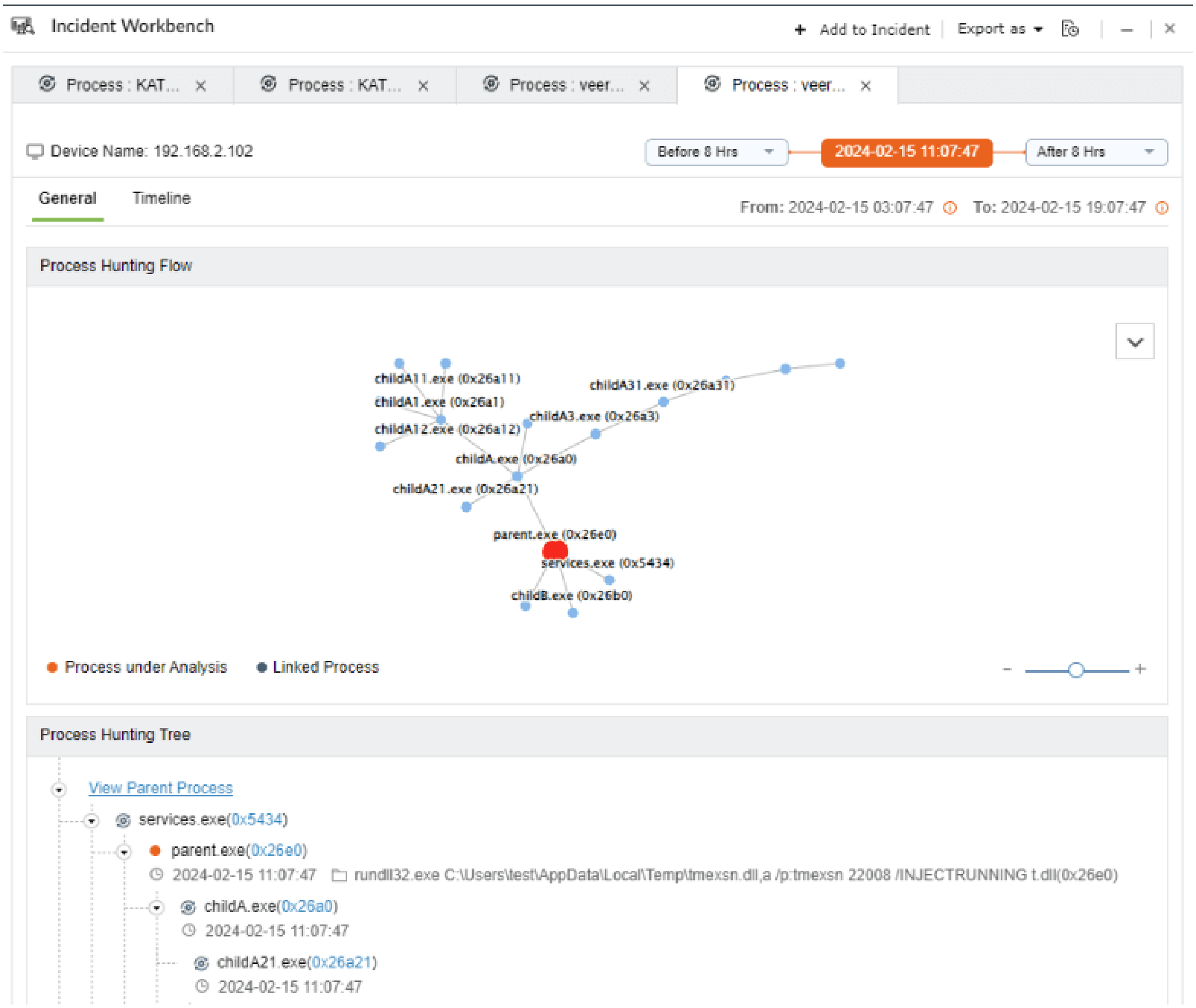
childA1.exe(0x26a1)

2024-02-15 11:07:47

childA12.exe(0x26a12)

2024-02-15 11:07:47

- Process cluster view



Device Name: 192.168.2.102

From: 2024-02-15 03:07:47 To: 2024-02-15 19:07:47

Process Hunting Flow

Process Hunting Tree

View Parent Process

services.exe(0x5434)

● parent.exe(0x26e0)

2024-02-15 11:07:47 rundll32.exe C:\Users\test\AppData\Local\Temp\tmexsn.dll,a /p:tmexsn 22008 /INJECTRUNNING t.dll(0x26e0)

childA.exe(0x26a0)

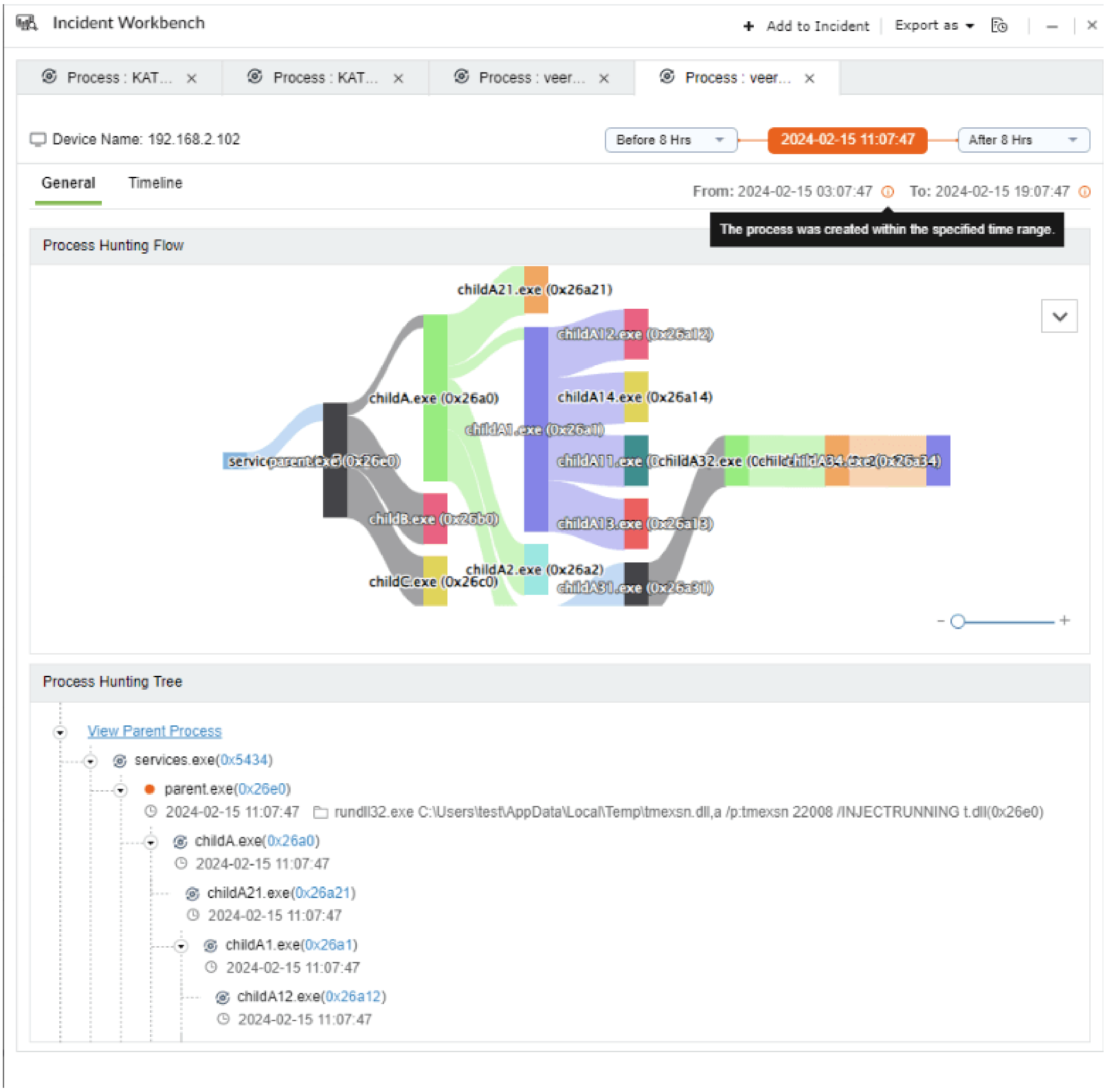
2024-02-15 11:07:47

childA21.exe(0x26a21)

2024-02-15 11:07:47

childA1.exe(0x26a1)
2024-02-15 11:07:47
childA12.exe(0x26a12)
2024-02-15 11:07:47

- Sankey Chart view with the process flow



Device Name: 192.168.2.102

2024-02-15 11:07:47

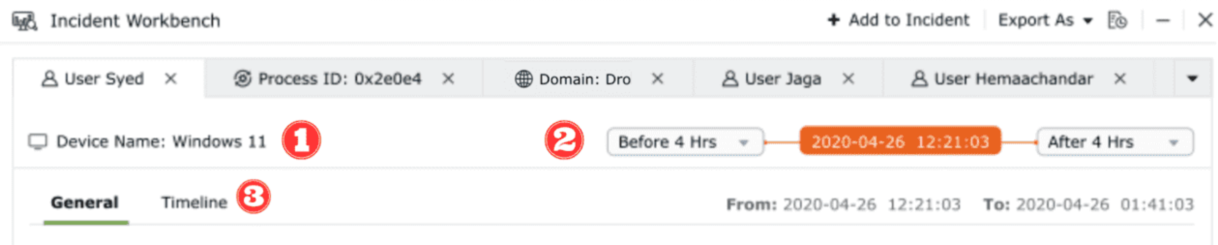
From: 2024-02-15 03:07:47 To: 2024-02-15 19:07:47

The process was created within the specified time range.

services.exe(0x5434)
parent.exe(0x26e0)
2024-02-15 11:07:47 rundll32.exe C:\Users\test\AppData\Local\Temp\tmexsn.dll,a /p:tmexsn 22008 /INJECTRUNNING t.dll(0x26e0)
childA.exe(0x26a0)
2024-02-15 11:07:47
childA21.exe(0x26a21)
2024-02-15 11:07:47
childA1.exe(0x26a1)
2024-02-15 11:07:47
childA12.exe(0x26a12)
2024-02-15 11:07:47

The process analytics tab explained.

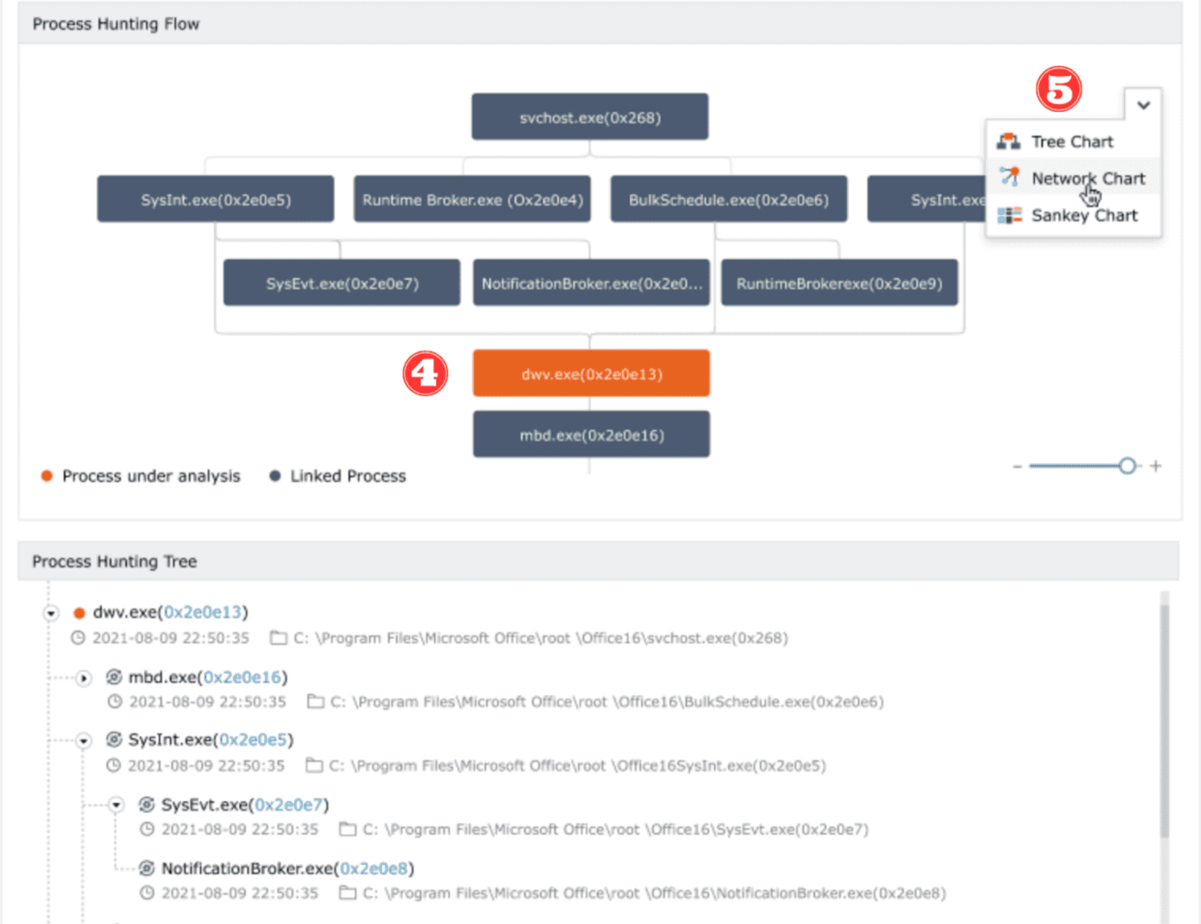
Process Analytics - Elements



Device Name: Windows 11

2020-04-26 12:21:03

From: 2020-04-26 12:21:03 To: 2020-04-26 01:41:03



dwv.exe(0x2e0e13)
2021-08-09 22:50:35 C: \Program Files\Microsoft Office\root \Office16\svchost.exe(0x268)

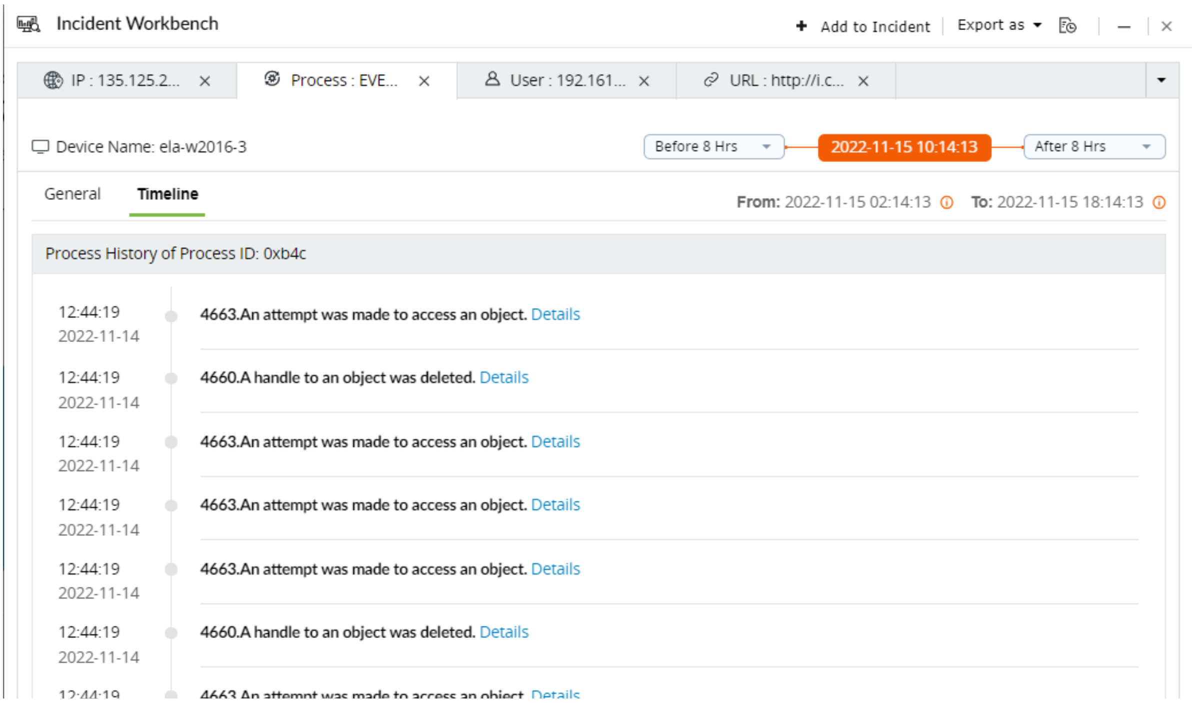
mbd.exe(0x2e0e16)
2021-08-09 22:50:35 C: \Program Files\Microsoft Office\root \Office16\BulkSchedule.exe(0x2e0e6)

SysInt.exe(0x2e0e5)
2021-08-09 22:50:35 C: \Program Files\Microsoft Office\root \Office16SysInt.exe(0x2e0e5)

SysEvt.exe(0x2e0e7)
2021-08-09 22:50:35 C: \Program Files\Microsoft Office\root \Office16\SysEvt.exe(0x2e0e7)

NotificationBroker.exe(0x2e0e8)
2021-08-09 22:50:35 C: \Program Files\Microsoft Office\root \Office16\NotificationBroker.exe(0x2e0e8)

1. Device Name: The device in which the process is active for the selected period.
2. Timeline adjuster: Use the timeline adjuster in the top right corner to view the process activities upto 8 hours prior to and after the selected event.
3. Views: Alternate between the General view and Timeline view. The General view has the graphical presentation of the process flow, and the Timeline view has the process history with list of events.



Device Name: ela-w2016-3

From: 2022-11-15 02:14:13 To: 2022-11-15 18:14:13

Process History of Process ID: 0xb4c

12:44:19 2022-11-14 4663.An attempt was made to access an object. Details

12:44:19 2022-11-14 4660.A handle to an object was deleted. Details

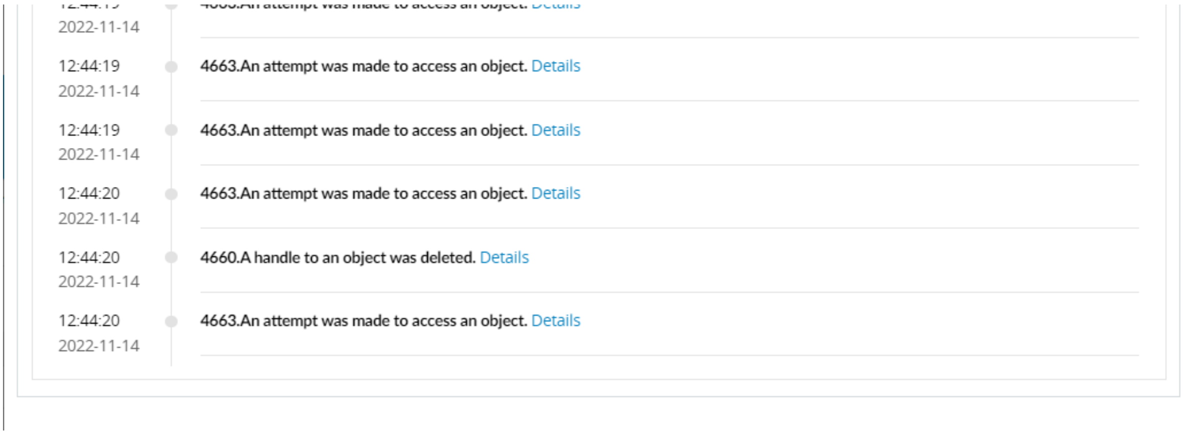
12:44:19 2022-11-14 4663.An attempt was made to access an object. Details

12:44:19 2022-11-14 4663.An attempt was made to access an object. Details

12:44:19 2022-11-14 4663.An attempt was made to access an object. Details

12:44:19 2022-11-14 4660.A handle to an object was deleted. Details

12:44:19 4663.An attempt was made to access an object. Details



```
12:44:19    4663.An attempt was made to access an object. Details
2022-11-14
12:44:19    4663.An attempt was made to access an object. Details
2022-11-14
12:44:19    4663.An attempt was made to access an object. Details
2022-11-14
12:44:20    4663.An attempt was made to access an object. Details
2022-11-14
12:44:20    4660.A handle to an object was deleted. Details
2022-11-14
12:44:20    4663.An attempt was made to access an object. Details
2022-11-14
```

4. Highlighted process: The Process being analyzed currently will be highlighted in orange and the rest of the linked processes will be in a different color.
5. Graphical formats: Select the dropdown button next to the process tree to alternate between different graphical formats

ⓘ Note

Minimize the tab to access the Incident Workbench while you traverse through different pages in EventLog Analyzer. As long as you don't close the workbench, the analysis will be available even if you log out of EventLog Analyzer and login again. You can also save it to an existing incident or create a new one.

4.2.3.5. Advanced Threat Analytics in Incident Workbench

Last updated on: September 12, 2025

In this page

Note

1. Please refer to the Incident Workbench Overview page to learn about the feature, and check the Access page to learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer.
2. To access Advanced Threat Analytics data, you can click on any of the following fields that uniquely identify the external sources:

Domain analysis:

- Domain
- Canonical Name
- Client Domain
- URL Site

IP Analysis:

- Remote DeviceIp
- Source IP
- Client IP Address
- Server IP Address
- Address
- Destination IP
- Device Ip
- Remote Ip
- Source Host Address
- NAT Source Address
- NAT Destination Address
- Destination IP
- Original Client IP
- IP Address

- Endpoint IP
- Private Ip
- Target Ip
- Source Device
- Target Machine
- Destination Host Address
- Target Device

URL Analysis:

- Payload URL
- Object Url
- URL

EventLog Analyzer supports the following vendors for the Advanced Threat Analytics in Incident Workbench:

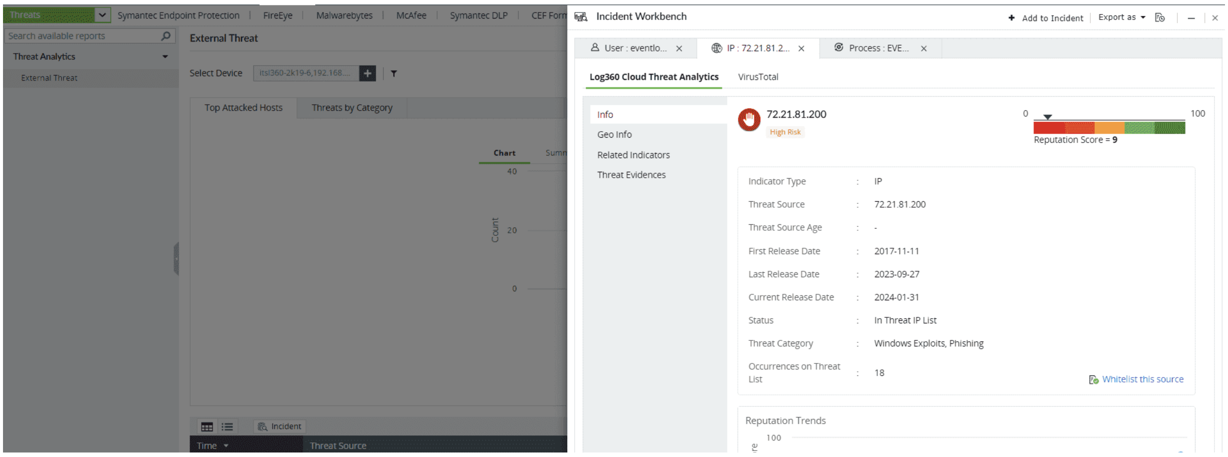
- Log360 Cloud Threat Analytics
- Dark Web Monitoring
- VirusTotal

Log360 Cloud Threat Analytics

This is the default integration from Log360Cloud suite, and can be accessed once the Advanced Threat Analytics add-on from EventLog Analyzer is purchased.

Note:

Check out the Advanced Threat Analytics page to learn about the configuration and analysis.



72.21.81.200

High Risk

Reputation Score = **9**

Indicator Type : IP

Threat Source : 72.21.81.200

Threat Source Age : -

First Release Date : 2017-11-11

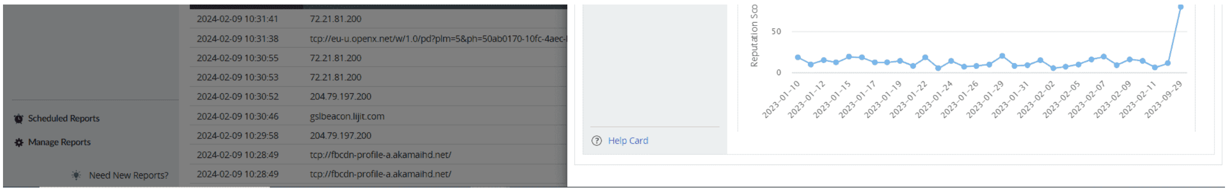
Last Release Date : 2023-09-27

Current Release Date : 2024-01-31

Status : In Threat IP List

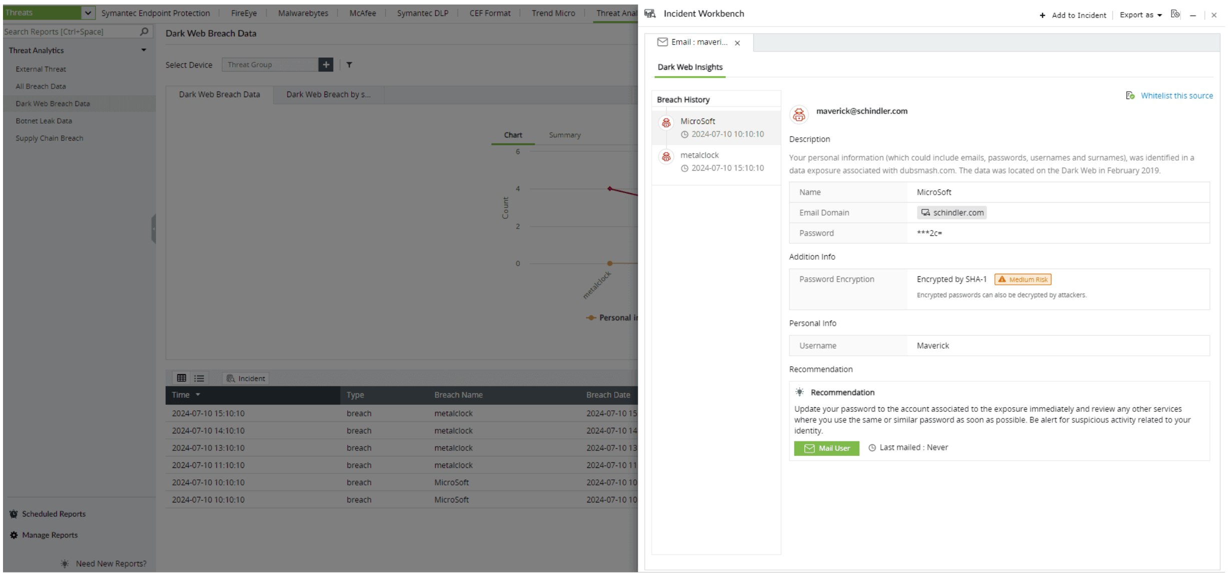
Threat Category : Windows Exploits, Phishing

Occurrences on Threat List : 18



2024-02-09 10:31:41	72.21.81.200
2024-02-09 10:31:38	tcp://eu-u.openx.net/w/1.0/pd?plm=5&ph=50ab0170-10fc-4aec-
2024-02-09 10:30:55	72.21.81.200
2024-02-09 10:30:53	72.21.81.200
2024-02-09 10:30:52	204.79.197.200
2024-02-09 10:30:46	gslbeacon.lijit.com
2024-02-09 10:29:58	204.79.197.200
2024-02-09 10:28:49	tcp://fbcdn-profile-a.akamaihd.net/
2024-02-09 10:28:49	tcp://fbcdn-profile-a.akamaihd.net/

Dark Web Monitoring



Time	Type	Breach Name	Breach Date
2024-07-10 15:10:10	breach	metalclock	2024-07-10 15
2024-07-10 14:10:10	breach	metalclock	2024-07-10 14
2024-07-10 13:10:10	breach	metalclock	2024-07-10 13
2024-07-10 11:10:10	breach	metalclock	2024-07-10 11
2024-07-10 10:10:10	breach	MicroSoft	2024-07-10 10
2024-07-10 10:10:10	breach	MicroSoft	2024-07-10 10

MicroSoft 2024-07-10 10:10:10

metalclock 2024-07-10 15:10:10

maverick@schindler.com

Description

Your personal information (which could include emails, passwords, usernames and surnames), was identified in a data exposure associated with dubsmash.com. The data was located on the Dark Web in February 2019.

Name	MicroSoft
Email Domain	schindler.com
Password	***2c=

Addition Info

Password Encryption	Encrypted by SHA-1 Medium Risk Encrypted passwords can also be decrypted by attackers.

Personal Info

Username	Maverick

Recommendation

Recommendation

Update your password to the account associated to the exposure immediately and review any other services where you use the same or similar password as soon as possible. Be alert for suspicious activity related to your identity.

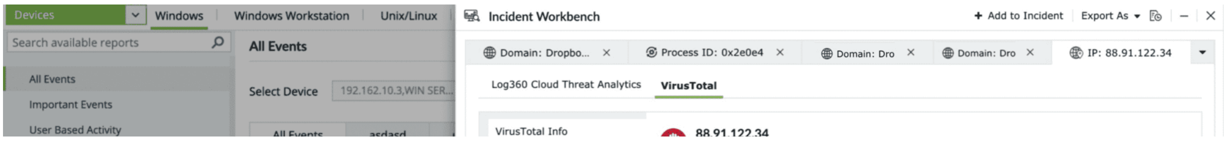
Last mailed : Never

When you purchase Advanced Threat Analytics, you also gain access to Dark Web monitoring. You can use your domain to enable Dark Web monitoring. This feature actively scans for any compromise of user data on the Dark Web and sends alerts. Compromised data can include credentials, credit card information, and more. With this information, the security analyst can gain insight into the depth of the breach and the type of information that has been breached.

VirusTotal

This is a third-party threat feed integration, and follows the Bring Your Own Key (BYOK) model. If you have purchased VirusTotal access separately or if you own a public API key for free, you can use your the key and get the threat analytics information in EventLog Analyzer.

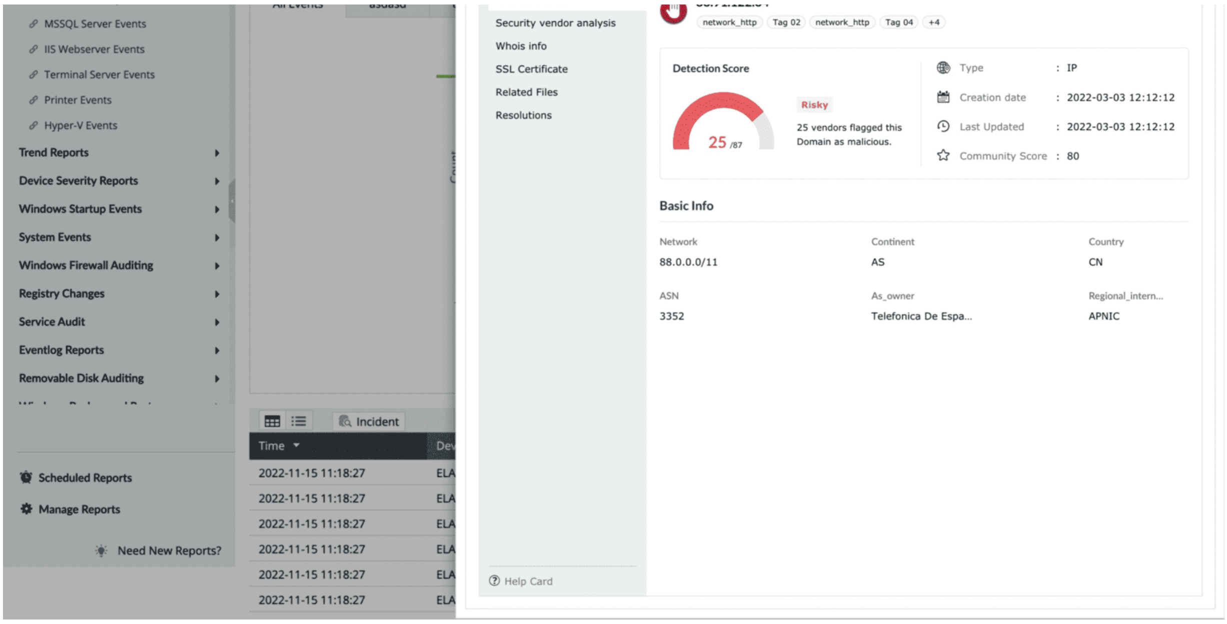
> Note:
>
> Check out the Advanced Threat Analytics page to learn about the configuration and analysis.



192.162.10.3,WIN SER...

Domain: Dropbo... | Process ID: 0x2e0e4 | Domain: Dro | Domain: Dro | IP: 88.91.122.34

88.91.122.34



Time	
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA
2022-11-15 11:18:27	ELA

Type : IP

Creation date : 2022-03-03 12:12:12

Last Updated : 2022-03-03 12:12:12

Community Score : 80

Basic Info

Network	Continent	Country
88.0.0.0/11	AS	CN
ASN	As_owner	Regional_intern...
3352	Telefonica De Espa...	APNIC

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.

4.2.3.6. Incident building using the Incident Workbench

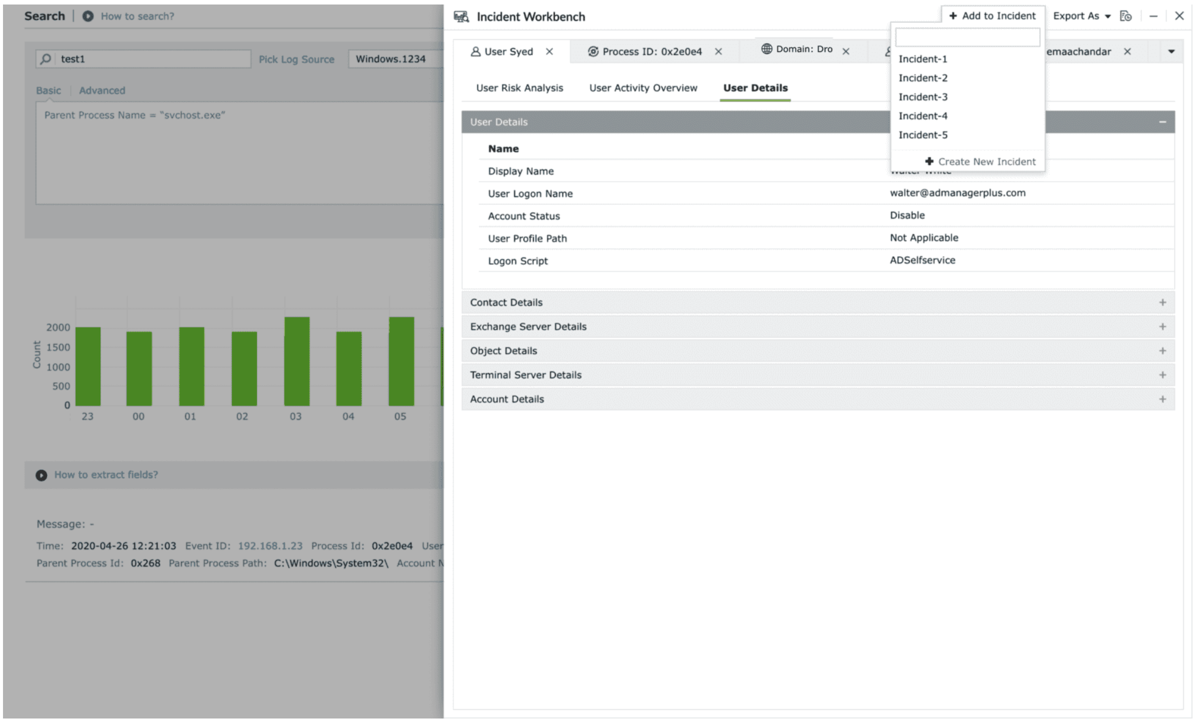
Last updated on: September 12, 2025

This page explains about building incidents using the instances of the Incident Workbench.

> Note
>
> 1. Please refer to the Incident Workbench Overview page to learn about the feature, and check the Access page to learn how to invoke the Incident Workbench from different dashboards of EventLog Analyzer
> 2. You can add upto 20 analysis tabs in a single instance of the Incident Workbench. If you want to analyze more entities you will have to close the current instance, and open a new one.

Steps to add the Incident Workbench instance to Incidents as evidence:

1. Click on Add to Incident in the top right corner of the Incident Workbench to save the instance.



test1 | Windows.1234

Parent Process Name = "svchost.exe"

Message: -

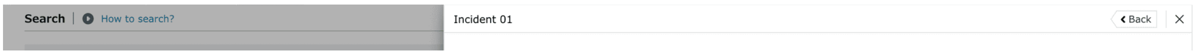
Time: 2020-04-26 12:21:03 Event ID: 192.168.1.23 Process Id: 0x2e0e4 User

Parent Process Id: 0x268 Parent Process Path: C:\Windows\System32\ Account N

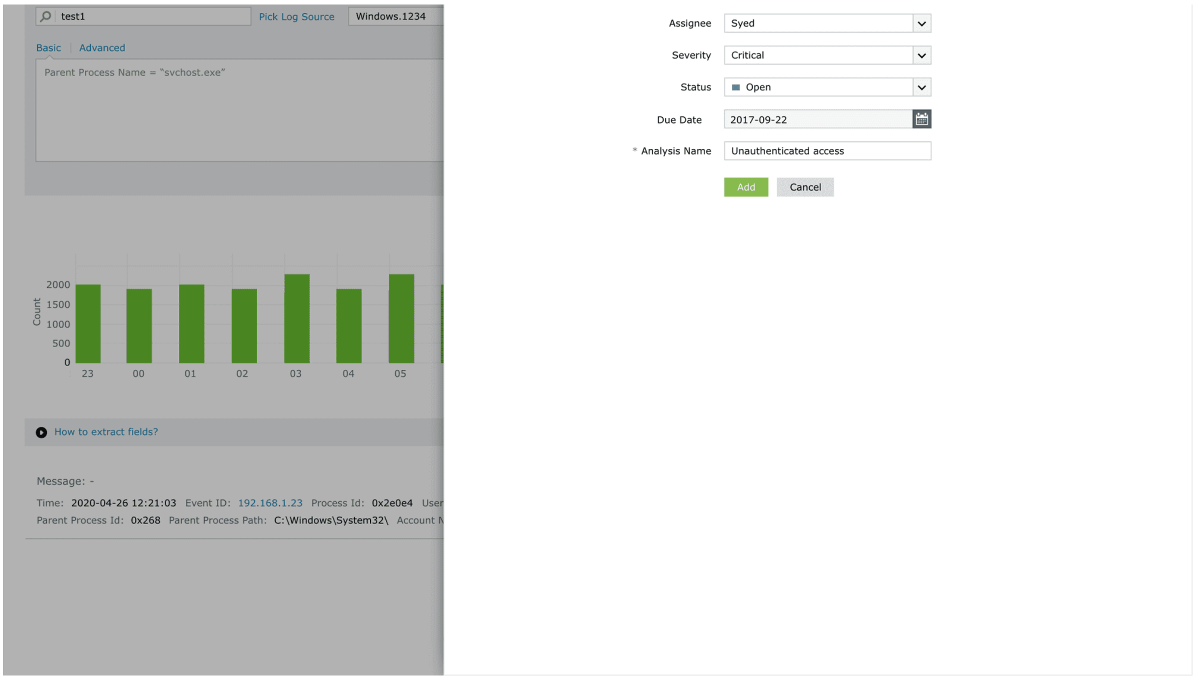
User Details

Name	
Display Name	
User Logon Name	walter@admanagerplus.com
Account Status	Disable
User Profile Path	Not Applicable
Logon Script	ADSelfservice

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.



Incident 01



test1 Pick Log Source Windows.1234

Basic | Advanced

Parent Process Name = "svchost.exe"

How to extract fields?

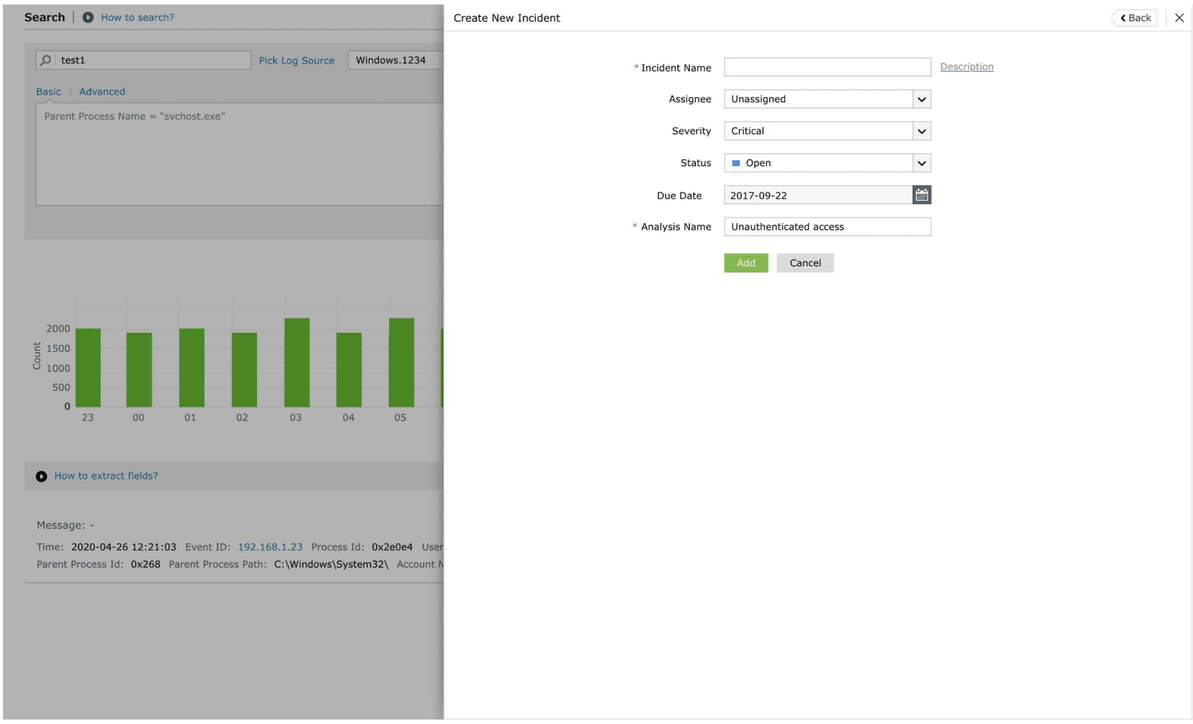
Message: -

Time: 2020-04-26 12:21:03 Event ID: 192.168.1.23 Process Id: 0x2e0e4 User

Parent Process Id: 0x268 Parent Process Path: C:\Windows\System32\ Account N

Assignee	Syed
Severity	Critical
Status	Open
Due Date	2017-09-22
* Analysis Name	Unauthenticated access

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.



Search | How to search?

test1 Pick Log Source Windows.1234

Basic | Advanced

Parent Process Name = "svchost.exe"

How to extract fields?

Message: -

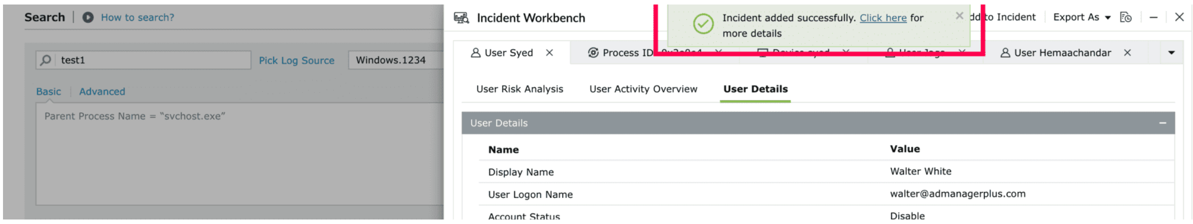
Time: 2020-04-26 12:21:03 Event ID: 192.168.1.23 Process Id: 0x2e0e4 User

Parent Process Id: 0x268 Parent Process Path: C:\Windows\System32\ Account N

Create New Incident

* Incident Name	
Assignee	Unassigned
Severity	Critical
Status	Open
Due Date	2017-09-22
* Analysis Name	Unauthenticated access

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.



Search | How to search?

test1 Pick Log Source Windows.1234

Basic | Advanced

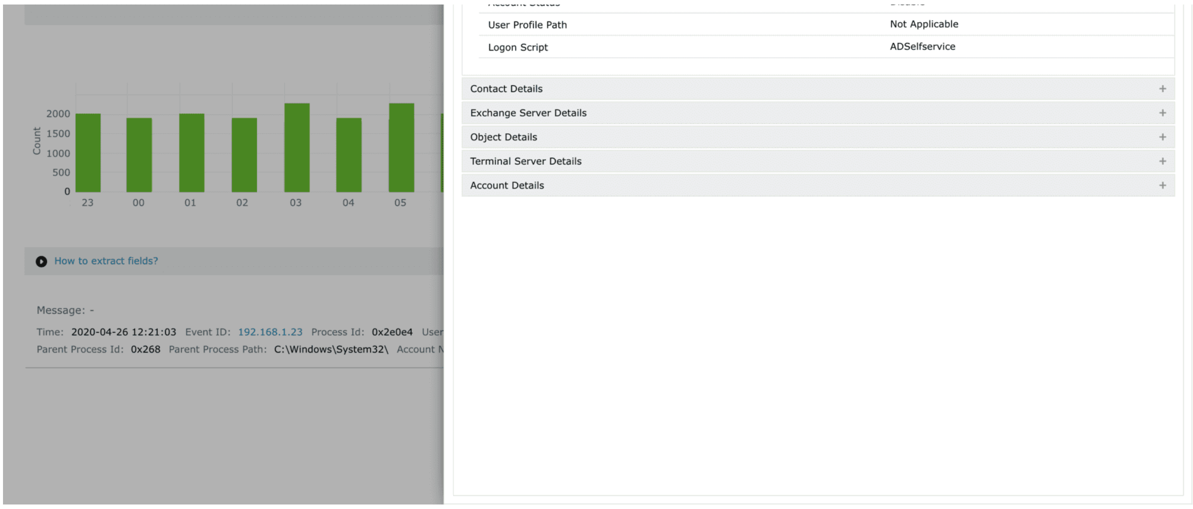
Parent Process Name = "svchost.exe"

Incident Workbench

Incident added successfully. Click here for more details

User Details

Name	Value
Display Name	Walter White
User Logon Name	walter@admanagerplus.com
Account Status	Disable



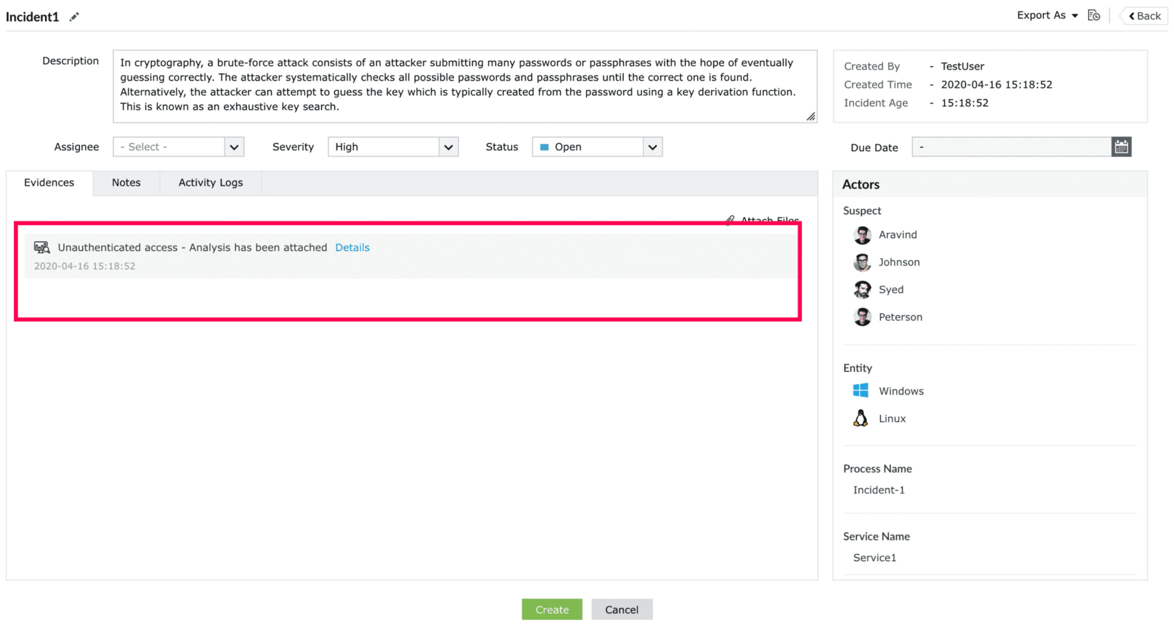
Message: -

Time: 2020-04-26 12:21:03 Event ID: 192.168.1.23 Process Id: 0x2e0e4 User

Parent Process Id: 0x268 Parent Process Path: C:\Windows\System32\ Account N

User Profile Path	Not Applicable
Logon Script	ADSelfservice

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.



Description: In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

Created By - TestUser
Created Time - 2020-04-16 15:18:52
Incident Age - 15:18:52

Assignee: - Select -
Severity: High
Status: Open
Due Date: -

Unauthenticated access - Analysis has been attached Details
2020-04-16 15:18:52

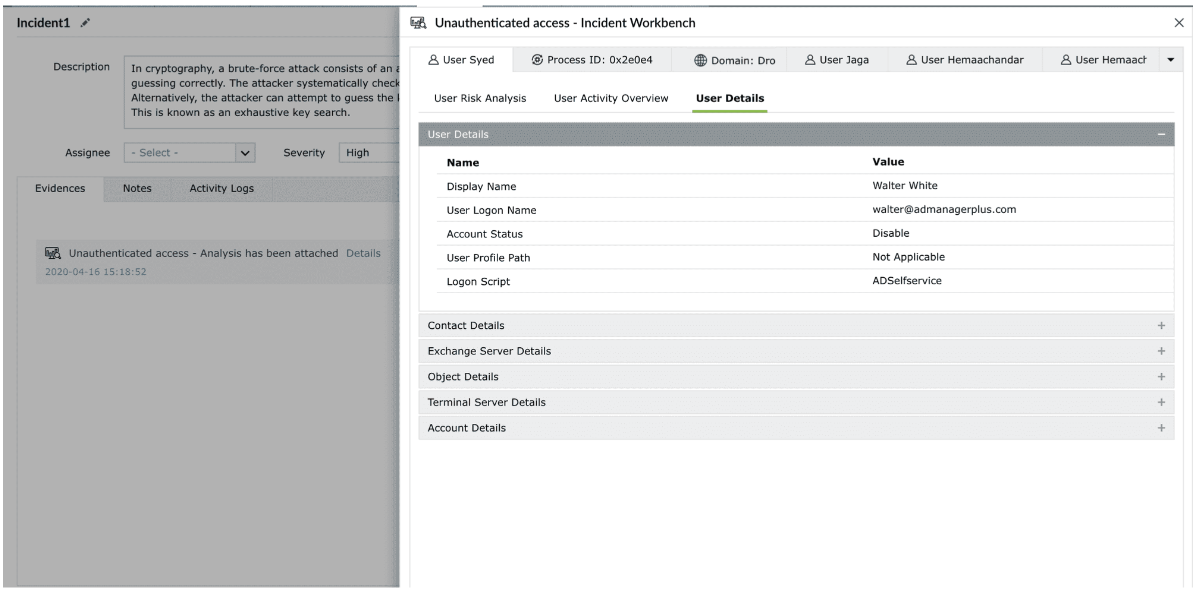
Actors

Suspect: Aravind, Johnson, Syed, Peterson

Entity: Windows, Linux

Process Name: Incident-1

Service Name: Service1



Incident1
Description
In cryptography, a brute-force attack consists of an a
guessing correctly. The attacker systematically check
Alternatively, the attacker can attempt to guess the l
This is known as an exhaustive key search.
Assignee
- Select -
Severity
High
Evidences
Notes
Activity Logs
Unauthenticated access - Analysis has been attached Details
2020-04-16 15:18:52

Unauthenticated access - Incident Workbench

User Syed
Process ID: 0x2e0e4
Domain: Dro
User Jaga
User Hemaachandar
User Hemaach
User Risk Analysis
User Activity Overview
User Details

User Details

Name	Value
Display Name	Walter White
User Logon Name	walter@admanagerplus.com
Account Status	Disable
User Profile Path	Not Applicable
Logon Script	ADSelfservice

Contact Details +
Exchange Server Details +
Object Details +
Terminal Server Details +
Account Details +

Use the Incident Management help document to learn more about creating, accessing and managing incidents.

Note

Minimize the tab to access the Incident Workbench while you traverse through different pages in EventLog Analyzer. As long as you don't close the workbench, the analysis will be available even if you log out of EventLog Analyzer and login again.

4.3.1.1. Incident management

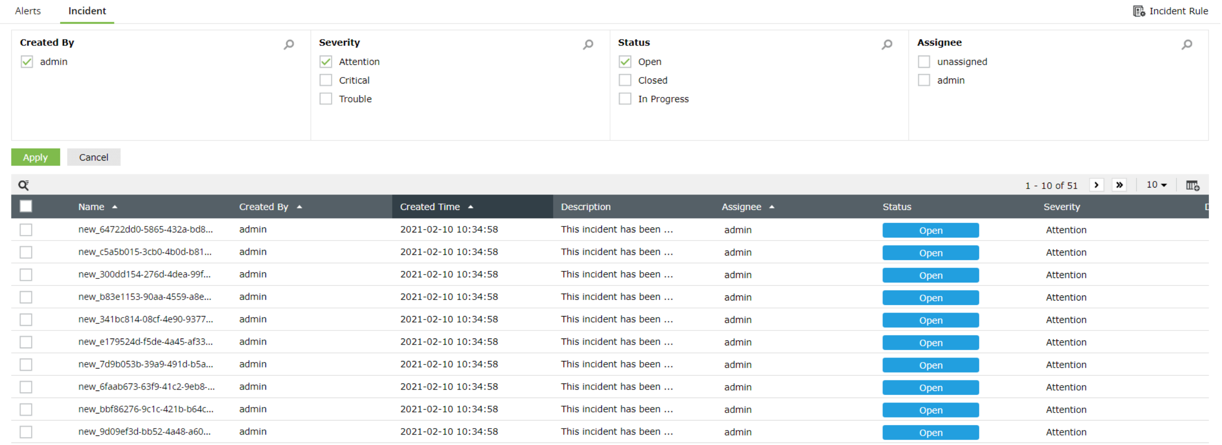
Last updated on: September 12, 2025

EventLog Analyzer helps you streamline the process of managing and investigating security incidents.. You can track the status of security incidents by navigating to the Alerts tab → Incident.

Viewing and editing incidents

In the Incident page, you can view the list of all incidents in your network along with crucial information such as the assignee, status, and severity. You can click on any incident to view and edit the incident's name, description, assignee, status, and severity. The Evidence and Notes tab display the list of evidence and notes attached to an incident. The Activity Logs page records and displays the events pertaining to the creation, modification, and deletion of incidents.

The incident page displays details such as the age of the incident, who created it, and when it was created. The Actors widget contains the list of users, entities, services, and processes responsible for the incident to help the assignee quickly investigate the incident and take remedial action.



Created By
☑ admin

Severity
☑ Attention
□ Critical
□ Trouble

Status
☑ Open
□ Closed
□ In Progress

Assignee
□ unassigned
□ admin

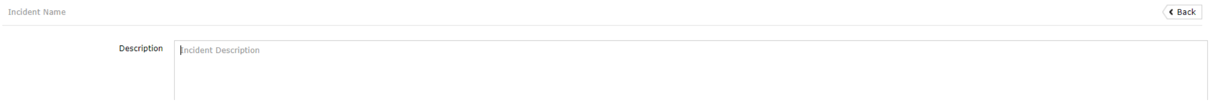
□	Name	Created By	Created Time	Description	Assignee	Status	Severity
□	new_64722dd0-5865-432a-bd8...	admin	2021-02-10 10:34:58	This incident has been ...	admin	Open	Attention
□	new_c5a5b015-3cb0-4b0d-b81...	admin	2021-02-10 10:34:58	This incident has been ...	admin	Open	Attention
□	new_300dd154-276d-4dea-99f...	admin	2021-02-10 10:34:58	This incident has been ...	admin	Open	Attention
□	new_b83e1153-90aa-4559-a8e...	admin	2021-02-10 10:34:58	This incident has been ...	admin	Open	Attention
□	new_341bc814-08cf-4e90-9377...	admin	2021-02-10 10:34:58	This incident has been ...	admin	Open	Attention
□	new_e179524d-f5de-4a45-af33...	admin	2021-02-10 10:34:58	This incident has been ...	admin	Open	Attention
□	new_7d9b053b-39a9-491d-b5a...	admin	2021-02-10 10:34:58	This incident has been ...	admin	Open	Attention
□	new_6faab673-63f9-41c2-9eb8-...	admin	2021-02-10 10:34:58	This incident has been ...	admin	Open	Attention
□	new_bbf86276-9c1c-421b-b64c...	admin	2021-02-10 10:34:58	This incident has been ...	admin	Open	Attention
□	new_9d09ef3d-bb52-4a48-a60...	admin	2021-02-10 10:34:58	This incident has been ...	admin	Open	Attention

Steps to create an incident

You can create an incident in EventLog Analyzer by navigating to the Alerts tab → Incident → +Add Incident.

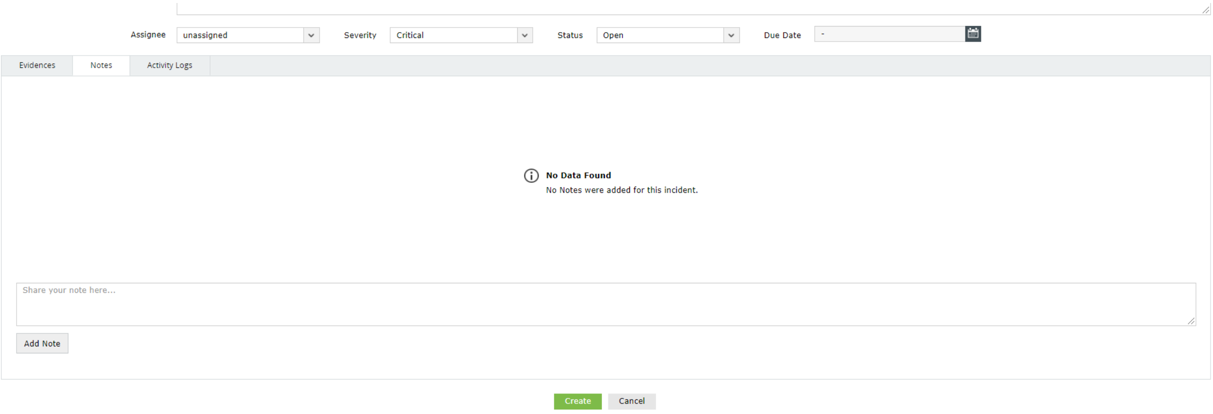
- In the Incident page, enter a name and description for your incident in the respective fields.
- Select the assignee, severity, and status of your incident from the respective drop-down menus.
- Click on Create.

You can view the incident creation event being logged in the Activity Logs pane.



Incident Name

Description: Incident Description



Assignee: unassigned

Severity: Critical

Status: Open

Due Date: -

No Data Found

No Notes were added for this incident.

Additionally, you can create incidents in EventLog Analyzer by:

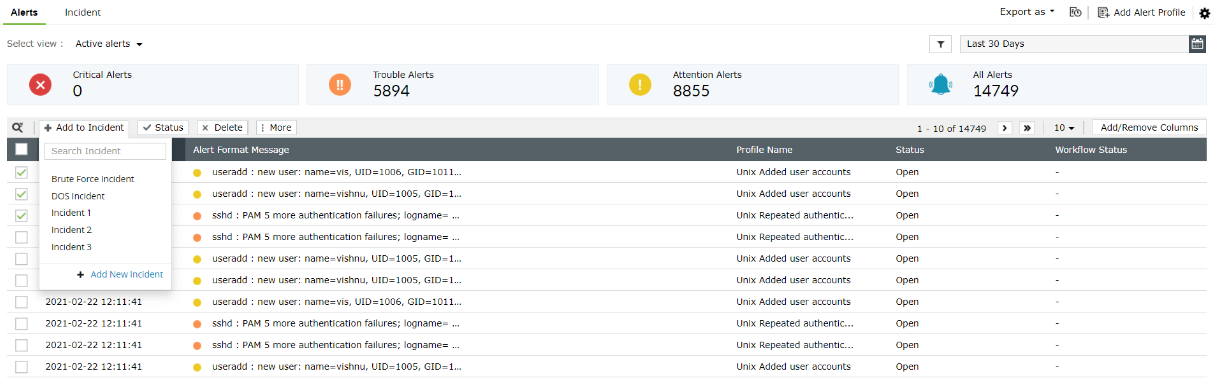
- Mapping alerts as incidents
- Mapping search results as incidents
- Mapping reports as incidents
- Automating incident creation by configuring incident rules

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.



Critical Alerts 0

Trouble Alerts 5894

Attention Alerts 8855

All Alerts 14749

1 - 10 of 14749

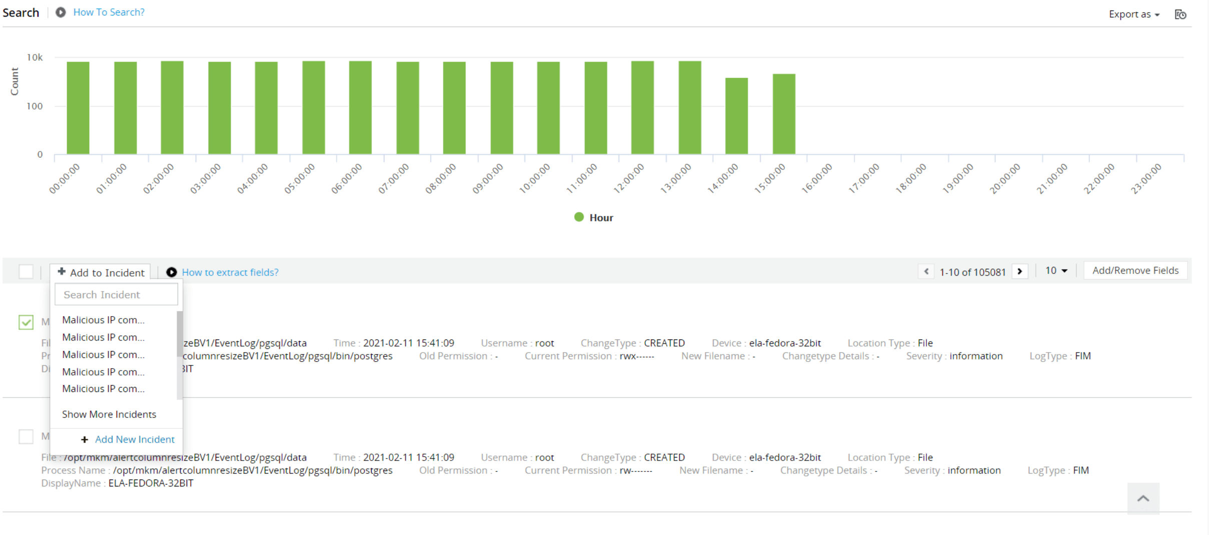
☐		Alert Format Message	Profile Name	Status	Workflow Status
☑		● useradd : new user: name=vis, UID=1006, GID=1011...	Unix Added user accounts	Open	-
☑		● useradd : new user: name=vishnu, UID=1005, GID=1...	Unix Added user accounts	Open	-
☑		● sshd : PAM 5 more authentication failures; logname= ...	Unix Repeated authentic...	Open	-
☐		● sshd : PAM 5 more authentication failures; logname= ...	Unix Repeated authentic...	Open	-
☐		● useradd : new user: name=vishnu, UID=1005, GID=1...	Unix Added user accounts	Open	-
☐		● useradd : new user: name=vishnu, UID=1005, GID=1...	Unix Added user accounts	Open	-
☐	2021-02-22 12:11:41	● useradd : new user: name=vis, UID=1006, GID=1011...	Unix Added user accounts	Open	-
☐	2021-02-22 12:11:41	● sshd : PAM 5 more authentication failures; logname= ...	Unix Repeated authentic...	Open	-
☐	2021-02-22 12:11:41	● sshd : PAM 5 more authentication failures; logname= ...	Unix Repeated authentic...	Open	-
☐	2021-02-22 12:11:41	● useradd : new user: name=vishnu, UID=1005, GID=1...	Unix Added user accounts	Open	-

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.



☑ M
Fi zeBV1/EventLog/pgsql/data Time : 2021-02-11 15:41:09 Username : root ChangeType : CREATED Device : ela-fedora-32bit Location Type : File
Pr columnresizeBV1/EventLog/pgsql/bin/postgres Old Permission : - Current Permission : rwx------ New Filename : - Changetype Details : - Severity : information LogType : FIM
Di 3IT

□ M
File : /opt/mkm/alertcolumnresizeBV1/EventLog/pgsql/data Time : 2021-02-11 15:41:09 Username : root ChangeType : CREATED Device : ela-fedora-32bit Location Type : File
Process Name : /opt/mkm/alertcolumnresizeBV1/EventLog/pgsql/bin/postgres Old Permission : - Current Permission : rw------- New Filename : - Changetype Details : - Severity : information LogType : FIM
DisplayName : ELA-FEDORA-32BIT

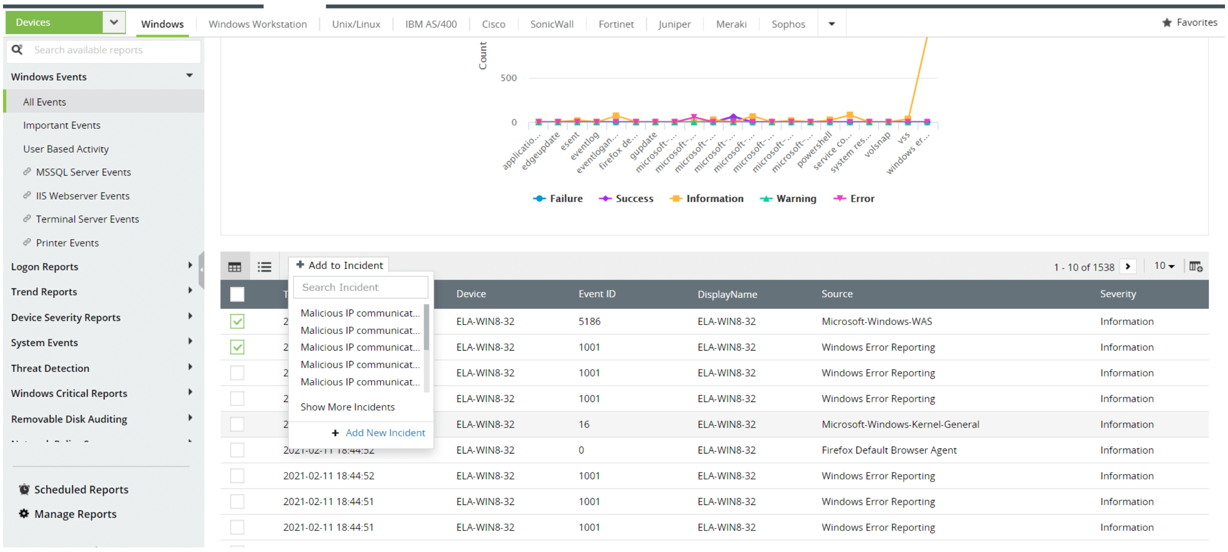
Steps to map reports as incidents

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.



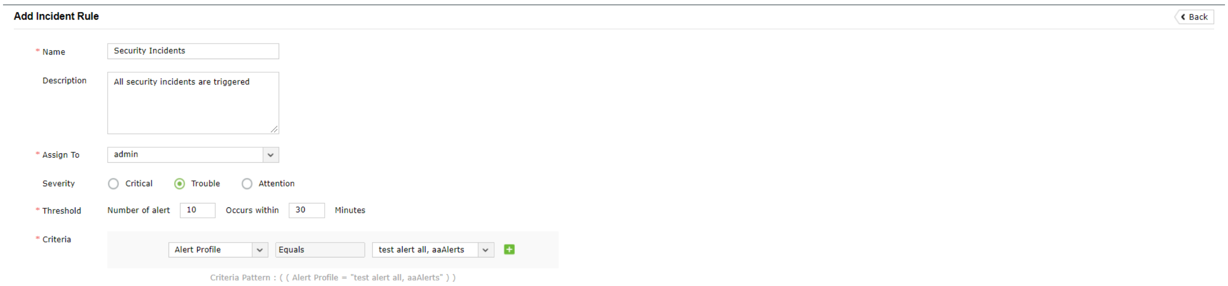
□	T	Device	Event ID	DisplayName	Source	Severity
☑	2	ELA-WIN8-32	5186	ELA-WIN8-32	Microsoft-Windows-WAS	Information
☑	2	ELA-WIN8-32	1001	ELA-WIN8-32	Windows Error Reporting	Information
□	2	ELA-WIN8-32	1001	ELA-WIN8-32	Windows Error Reporting	Information
□	2	ELA-WIN8-32	1001	ELA-WIN8-32	Windows Error Reporting	Information
□	2	ELA-WIN8-32	16	ELA-WIN8-32	Microsoft-Windows-Kernel-General	Information
□	2021-02-11 18:44:52	ELA-WIN8-32	0	ELA-WIN8-32	Firefox Default Browser Agent	Information
□	2021-02-11 18:44:52	ELA-WIN8-32	1001	ELA-WIN8-32	Windows Error Reporting	Information
□	2021-02-11 18:44:51	ELA-WIN8-32	1001	ELA-WIN8-32	Windows Error Reporting	Information
□	2021-02-11 18:44:51	ELA-WIN8-32	1001	ELA-WIN8-32	Windows Error Reporting	Information

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.



Add Incident Rule

* Name: Security Incidents

Description: All security incidents are triggered

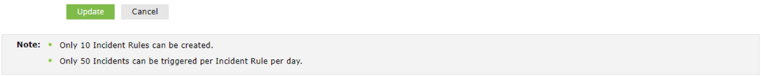
* Assign To: admin

Severity: ○ Critical ● Trouble ○ Attention

* Threshold: Number of alert 10 Occurs within 30 Minutes

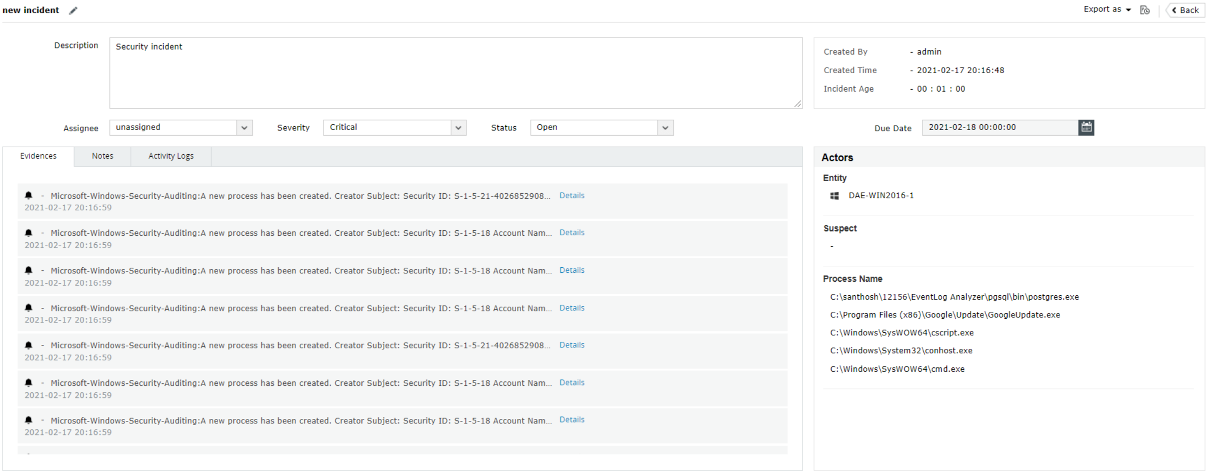
* Criteria: Alert Profile | Equals | test alert all, aaAlerts

Criteria Pattern : ((Alert Profile = "test alert all, aaAlerts"))



Note:
- Only 10 Incident Rules can be created.
- Only 50 Incidents can be triggered per Incident Rule per day.

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.



Description: Security incident

Created By - admin
Created Time - 2021-02-17 20:16:48
Incident Age - 00 : 01 : 00

Assignee: unassigned Severity: Critical Status: Open Due Date: 2021-02-18 00:00:00

```
- Microsoft-Windows-Security-Auditing:A new process has been created. Creator Subject: Security ID: S-1-5-21-4026852908...   Details
2021-02-17 20:16:59
- Microsoft-Windows-Security-Auditing:A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Nam...   Details
2021-02-17 20:16:59
- Microsoft-Windows-Security-Auditing:A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Nam...   Details
2021-02-17 20:16:59
- Microsoft-Windows-Security-Auditing:A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Nam...   Details
2021-02-17 20:16:59
- Microsoft-Windows-Security-Auditing:A new process has been created. Creator Subject: Security ID: S-1-5-21-4026852908...   Details
2021-02-17 20:16:59
- Microsoft-Windows-Security-Auditing:A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Nam...   Details
2021-02-17 20:16:59
- Microsoft-Windows-Security-Auditing:A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Nam...   Details
2021-02-17 20:16:59
```

Actors

Entity
DAE-WIN2016-1

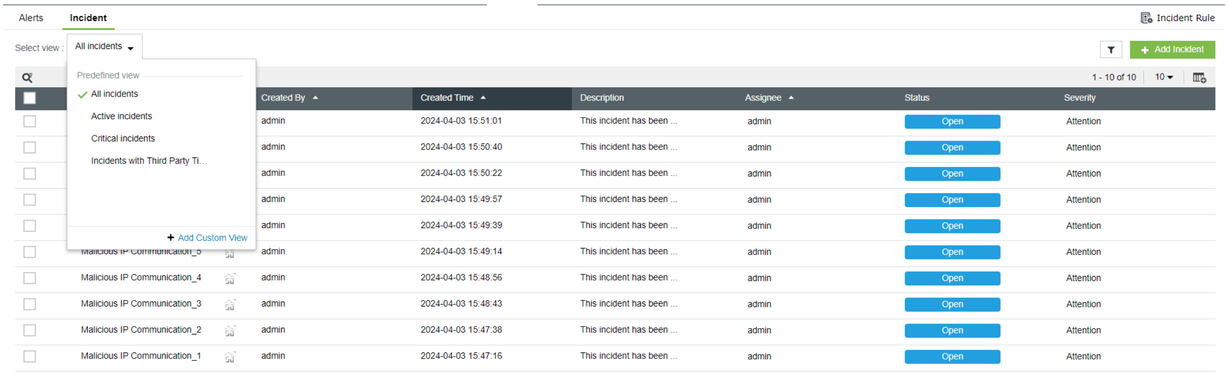
Suspect
-

Process Name
C:\santhosh\12156\EventLog Analyzer\pgsql\bin\postgres.exe
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
C:\Windows\SysWOW64\cscript.exe
C:\Windows\System32\conhost.exe
C:\Windows\SysWOW64\cmd.exe

> Note: You can create up to 10 incident rules in your EventLog Analyzer instance. The solution is capable of triggering up to fifty incidents per incident rule in a day.

Creating Incident views

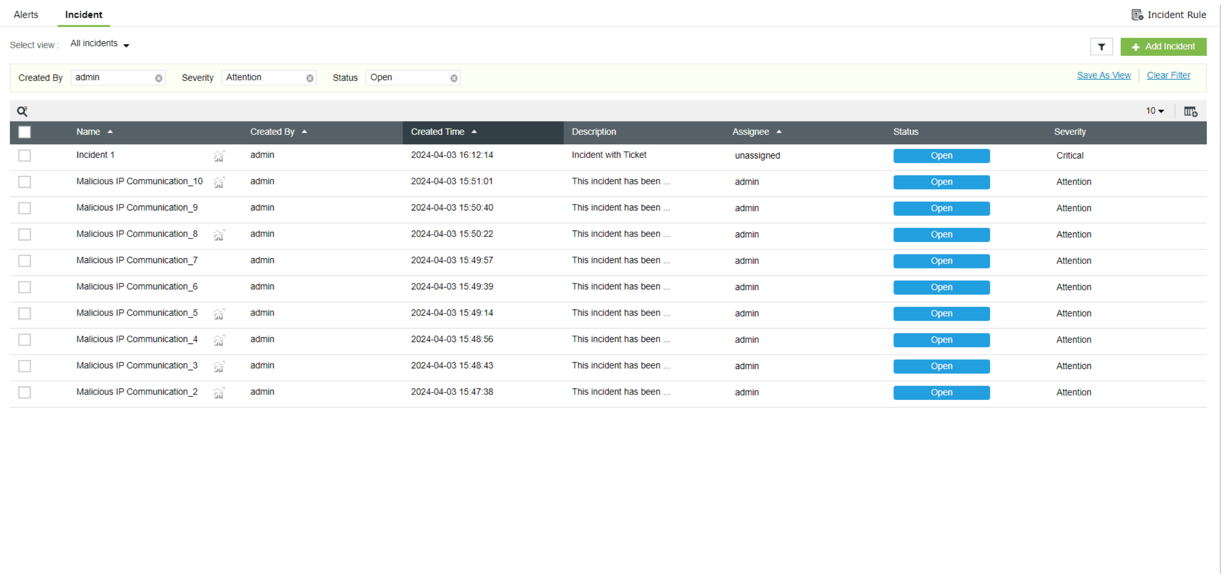
You can view the incidents under various categories, such as All incidents, Active incidents, Critical incidents, and Incident with third-party ticketing tool by selecting the required view from the Select View drop-down menu. You can also create custom views by configuring a filter for the type of incidents you want to view.



Select view : All incidents

□		Created By	Created Time	Description	Assignee	Status	Severity
□		admin	2024-04-03 15:51:01	This incident has been ...	admin	Open	Attention
□		admin	2024-04-03 15:50:40	This incident has been ...	admin	Open	Attention
□		admin	2024-04-03 15:50:22	This incident has been ...	admin	Open	Attention
□		admin	2024-04-03 15:49:57	This incident has been ...	admin	Open	Attention
□		admin	2024-04-03 15:49:39	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_5	admin	2024-04-03 15:49:14	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_4	admin	2024-04-03 15:48:56	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_3	admin	2024-04-03 15:48:43	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_2	admin	2024-04-03 15:47:38	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_1	admin	2024-04-03 15:47:16	This incident has been ...	admin	Open	Attention

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.

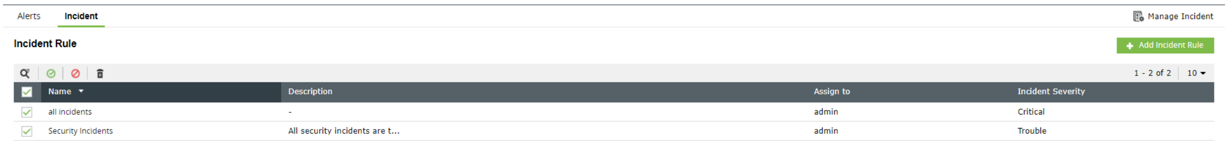


Created By: admin Severity: Attention Status: Open

□	Name	Created By	Created Time	Description	Assignee	Status	Severity
□	Incident 1	admin	2024-04-03 16:12:14	Incident with Ticket	unassigned	Open	Critical
□	Malicious IP Communication_10	admin	2024-04-03 15:51:01	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_9	admin	2024-04-03 15:50:40	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_8	admin	2024-04-03 15:50:22	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_7	admin	2024-04-03 15:49:57	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_6	admin	2024-04-03 15:49:39	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_5	admin	2024-04-03 15:49:14	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_4	admin	2024-04-03 15:48:56	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_3	admin	2024-04-03 15:48:43	This incident has been ...	admin	Open	Attention
□	Malicious IP Communication_2	admin	2024-04-03 15:47:38	This incident has been ...	admin	Open	Attention

Viewing and editing incident rules

In the Incident Rule page, you can select incidents to enable, disable, and delete them.



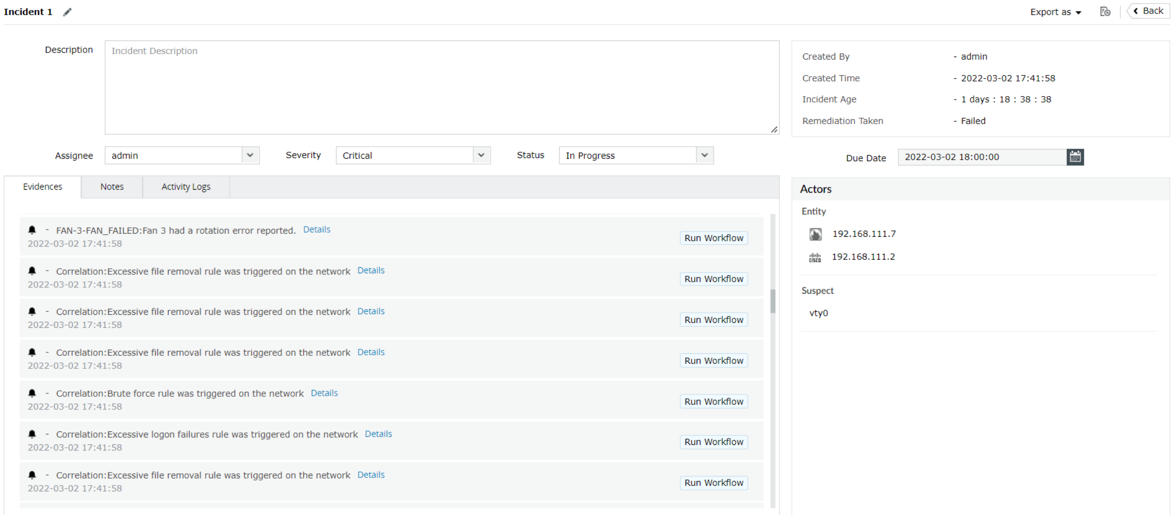
☑	Name	Description	Assign to	Incident Severity
☑	all incidents	-	admin	Critical
☑	Security Incidents	All security incidents are t...	admin	Trouble

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.



Incident 1

Description: Incident Description

Assignee: admin | Severity: Critical | Status: In Progress

Created By	- admin
Created Time	- 2022-03-02 17:41:58
Incident Age	- 1 days : 18 : 38 : 38
Remediation Taken	- Failed

Due Date: 2022-03-02 18:00:00

Evidences

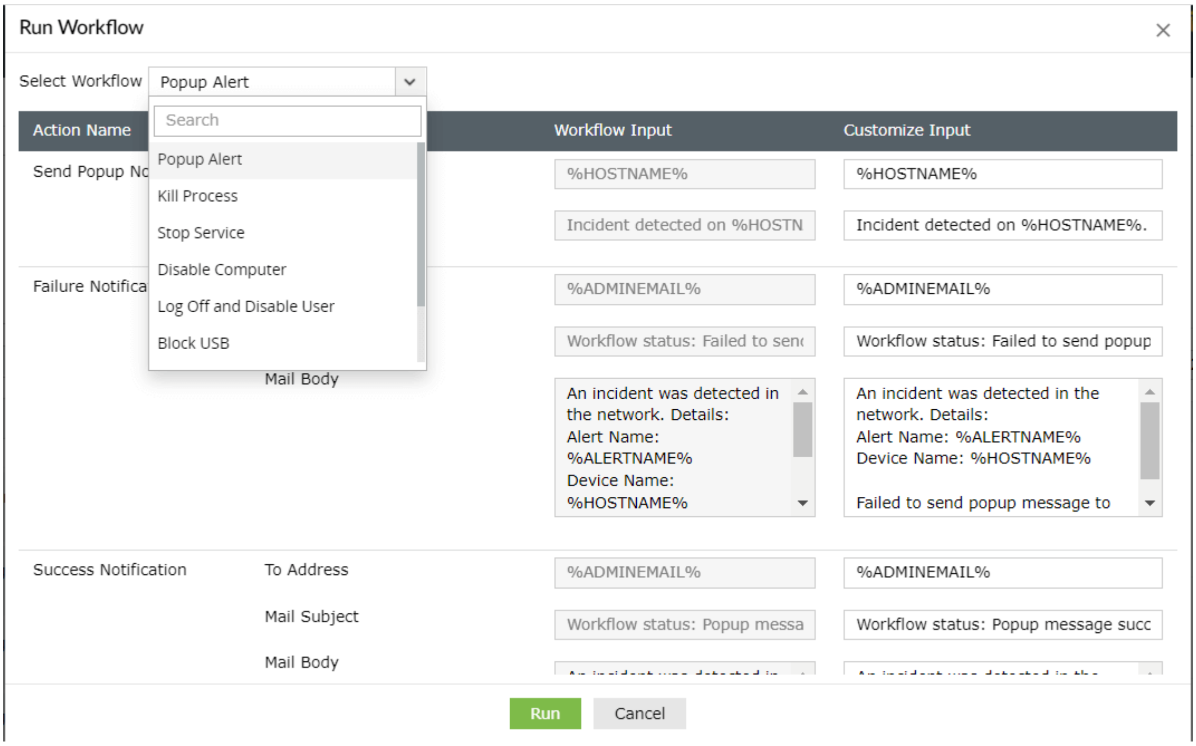
- FAN-3-FAN_FAILED:Fan 3 had a rotation error reported. Details 2022-03-02 17:41:58
- Correlation:Excessive file removal rule was triggered on the network Details 2022-03-02 17:41:58
- Correlation:Excessive file removal rule was triggered on the network Details 2022-03-02 17:41:58
- Correlation:Excessive file removal rule was triggered on the network Details 2022-03-02 17:41:58
- Correlation:Brute force rule was triggered on the network Details 2022-03-02 17:41:58
- Correlation:Excessive logon failures rule was triggered on the network Details 2022-03-02 17:41:58
- Correlation:Excessive file removal rule was triggered on the network Details 2022-03-02 17:41:58

Actors

Entity: 192.168.111.7, 192.168.111.2

Suspect: vty0

- Select a workflow from the drop down menu and click Run.



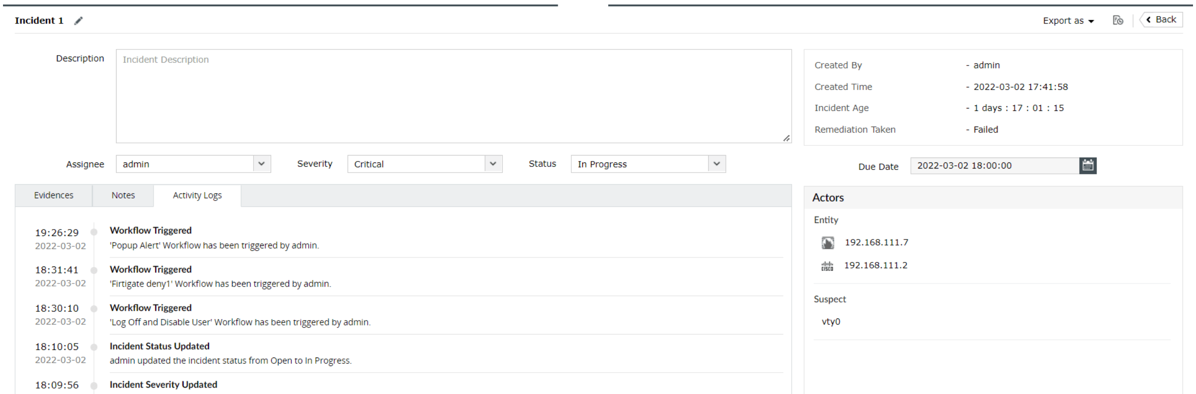
Run Workflow

Select Workflow: Popup Alert

Search
Popup Alert
Kill Process
Stop Service
Disable Computer
Log Off and Disable User
Block USB

Action Name		Workflow Input	Customize Input
Send Popup No		%HOSTNAME%	%HOSTNAME%
		Incident detected on %HOSTN	Incident detected on %HOSTNAME%.
Failure Notifica		%ADMINEMAIL%	%ADMINEMAIL%
		Workflow status: Failed to sen	Workflow status: Failed to send popup
	Mail Body	An incident was detected in the network. Details: Alert Name: %ALERTNAME% Device Name: %HOSTNAME%	An incident was detected in the network. Details: Alert Name: %ALERTNAME% Device Name: %HOSTNAME% Failed to send popup message to
Success Notification	To Address	%ADMINEMAIL%	%ADMINEMAIL%
	Mail Subject	Workflow status: Popup messa	Workflow status: Popup message succ
	Mail Body	An incident was detected in	An incident was detected in the

- Click Activity Logs to find the workflow history.



Incident 1

Description: Incident Description

Assignee: admin | Severity: Critical | Status: In Progress

Created By	- admin
Created Time	- 2022-03-02 17:41:58
Incident Age	- 1 days : 17 : 01 : 15
Remediation Taken	- Failed

Due Date: 2022-03-02 18:00:00

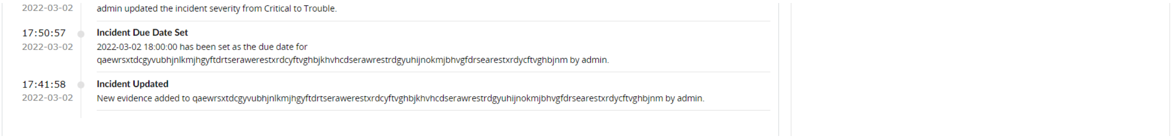
Activity Logs

19:26:29 2022-03-02	Workflow Triggered 'Popup Alert' Workflow has been triggered by admin.
18:31:41 2022-03-02	Workflow Triggered 'Firtigate deny1' Workflow has been triggered by admin.
18:30:10 2022-03-02	Workflow Triggered 'Log Off and Disable User' Workflow has been triggered by admin.
18:10:05 2022-03-02	Incident Status Updated admin updated the incident status from Open to In Progress.
18:09:56	Incident Severity Updated

Actors

Entity: 192.168.111.7, 192.168.111.2

Suspect: vty0



2022-03-02 admin updated the incident severity from Critical to Trouble.

17:50:57 2022-03-02 **Incident Due Date Set**
2022-03-02 18:00:00 has been set as the due date for qaewrsxtdcgyvubhjnlkmjhgyftdrtserawerestxrdcyftvghbjkhvhcdserawrestrdgyuhijnokmjbhvgfdrsearestxrdycftvghbjnm by admin.

17:41:58 2022-03-02 **Incident Updated**
New evidence added to qaewrsxtdcgyvubhjnlkmjhgyftdrtserawerestxrdcyftvghbjkhvhcdserawrestrdgyuhijnokmjbhvgfdrsearestxrdycftvghbjnm by admin.

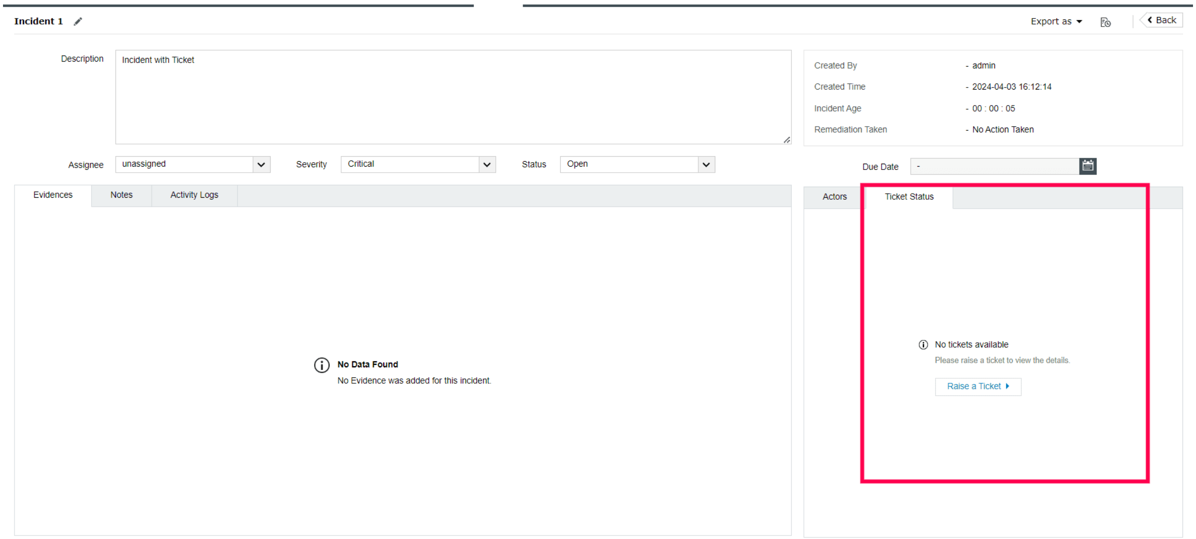
The status of the workflow will be displayed under Remediation Taken in the top-right corner. The same will be recorded in the exported report.

Note: Users can also run multiple workflows for a single alert or incident.

Creating Tickets for Incidents

To create a ticket for an incident,

- Navigate to the Incident section and select the required incident.
- Click the Raise a Ticket button under the Ticket Status tab to create a ticket in the configured ticketing tool; ticket details will be displayed immediately.



Description: Incident with Ticket

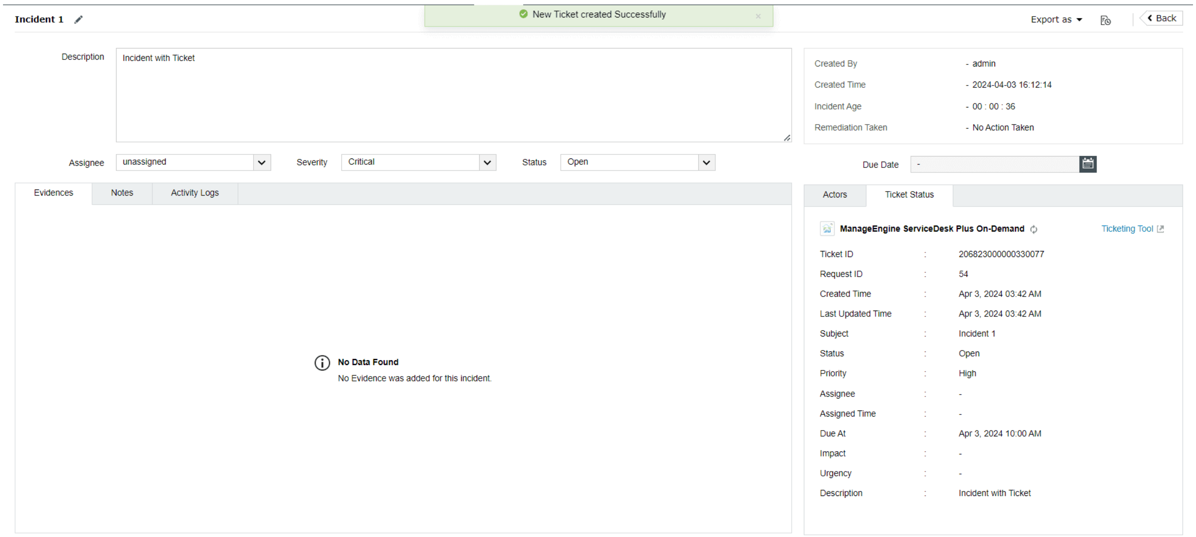
Created By - admin
Created Time - 2024-04-03 16:12:14
Incident Age - 00 : 00 : 05
Remediation Taken - No Action Taken

Assignee: unassigned
Severity: Critical
Status: Open
Due Date: -

No Data Found
No Evidence was added for this incident.

No tickets available
Please raise a ticket to view the details.

- The priority of the created ticket is set based on the current severity of the incident.



New Ticket created Successfully

Description: Incident with Ticket

Created By - admin
Created Time - 2024-04-03 16:12:14
Incident Age - 00 : 00 : 36
Remediation Taken - No Action Taken

Assignee: unassigned
Severity: Critical
Status: Open
Due Date: -

No Data Found
No Evidence was added for this incident.

ManageEngine ServiceDesk Plus On-Demand

Ticket ID	:	206823000000330077
Request ID	:	54
Created Time	:	Apr 3, 2024 03:42 AM
Last Updated Time	:	Apr 3, 2024 03:42 AM
Subject	:	Incident 1
Status	:	Open
Priority	:	High
Assignee	:	-
Assigned Time	:	-
Due At	:	Apr 3, 2024 10:00 AM
Impact	:	-
Urgency	:	-
Description	:	Incident with Ticket

- Any changes to the status or severity of the incident will automatically update the ticket's status and severity in the ticketing tool according to the mapped values.
- Refer to this link for status/severity mapping details.

ⓘ Note

Bidirectional synchronization is only available if the EventLog Analyzer app is installed in the ticketing tool. If not yet installed, follow the steps at this link to install the EventLog Analyzer app.

Incident Management Status/Severity Mapping with Ticketing Tool

Understanding how incident statuses and severities in EventLog Analyzer correspond to those in various ticketing tools is crucial for seamless integration and efficient incident management.

Default Status Mapping

The table below outlines the mapping between EventLog Analyzer incident statuses and the corresponding statuses in different ticketing tools:

Tool	EventLog Analyzer - Incident Status	Ticketing Tool - Ticket Status
Kayako	1. Open 2. In Progress 3. Closed	1. Open 2. Pending 3. Closed
Zendesk	1. Open 2. In Progress 3. Closed	1. Open 2. Pending 3. Solved
ServiceNow	1. Open 2. In Progress 1. Closed	1. New 2. In Progress / Active 3. Closed
Freshservice	1. Open 2. In Progress 3. Closed	1. Open 2. Pending 3. Closed

Jira Cloud	1. Open 2. In Progress 3. Closed	1. Open 2. Work in Progress 3. Done
Jira Service Desk	1. Open 2. In Progress 3. Closed	1. Open 2. Work in Progress 3. Done
ServiceDesk Plus Cloud	1. Open 2. In Progress 1. Closed	1. Open 2. Open 3. Closed
ServiceDesk Plus	1. Open 2. In Progress 3. Closed	1. Open 2. In Progress 3. Closed
ServiceDesk Plus MSP	1. Open 2. In Progress 3. Closed	1. Open 2. In Progress 3. Closed

Default Severity Mapping

The following table illustrates how incident severities are mapped between EventLog Analyzer and various ticketing tools:

Tool	EventLog Analyzer - Incident Severity	Ticketing Tool - Ticket Severity
Kayako	1. Critical 2. Trouble 3. Attention	Impact: 1. Urgent 2. High 3. Normal
Zendesk	1. Critical 2. Trouble 3. Attention	Priority: 1. Urgent 2. High 3. Normal

		3. Normal
ServiceNow	1. Critical 2. Trouble 3. Attention	Priority: 1. 1- Critical 2. 2 - High 3. 3 - Moderate
Jira Cloud	1. Critical 2. Trouble 3. Attention	Priority: 1. Highest 2. Medium 3. Low
Freshservice	1. Critical 2. Trouble 3. Attention	Priority: 1. Urgent 2. High 3. Low
Jira Service Desk	1. Critical 2. Trouble 3. Attention	Priority: 1. High 2. Medium 3. Low
ServiceDesk Plus Cloud	1. Critical 2. Trouble 3. Attention	Priority: 1. High 2. Medium 3. Normal
ServiceDesk Plus	1. Critical 2. Trouble 3. Attention	Priority: 1. High 2. Medium 3. Normal
ServiceDesk Plus MSP	1. Critical 2. Trouble	Priority: 1. High 2. Medium

	3. Attention	3. Normal
AlarmsOne	1. Critical 2. Trouble 3. Attention	Priority: 1. Critical 2. Major 3. Info

By aligning incident statuses and severities between EventLog Analyzer and your ticketing tools, you can ensure consistent communication and efficient incident resolution across platforms.

4.3.2.1. Playbook management overview

Last updated on: September 12, 2025

In this page

Overview

Playbooks are automated response workflows designed to help mitigate security incidents as soon as alerts are triggered. Whether it’s disabling compromised user accounts, blocking IPs, or enforcing USB policies, playbooks reduce response time and manual intervention through intelligent recommendations and predefined actions. This document explains how playbooks work, how to execute them, and how they align with real-world use cases mapped to the MITRE ATT&CK framework.

What is playbook?

You can mitigate security incidents in your network before they result in a breach by automating response workflows when alerts are triggered. The product allows you to create such workflows to automatically perform actions such as disabling USB ports, shutting down systems, and changing firewall rules when security incidents are detected. This automated capability that provides remediation suggestions is called Playbook.

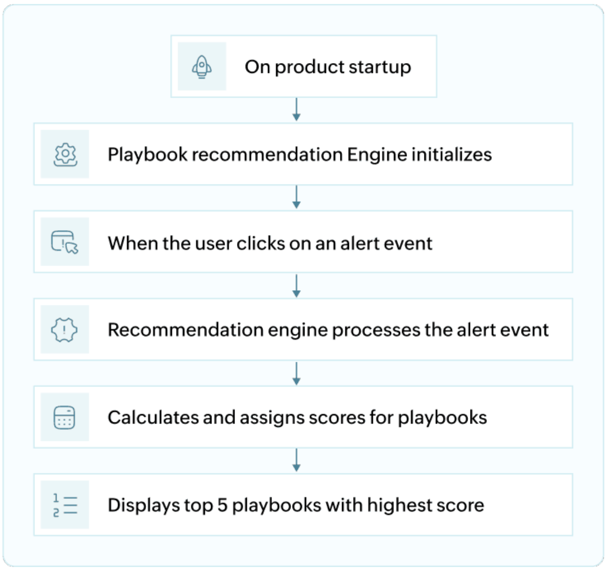
Playbook recommendations

Playbook recommendations are intelligent, context-aware response suggestions provided for every alert raised in the system. As soon as the product is launched, the playbook recommendation engine is initialized in the background. These recommendations are based on predefined logic that links specific alert types to optimal mitigation or investigation workflows, such as disabling a user account for suspicious login activity, or blocking an IP after detecting port scanning. This system ensures faster, guided incident response and minimizes manual decision-making during critical security events.

When you click on an alert, the engine processes the alert's event data and metadata including parameters like event type, source device, user behavior, and historical response patterns. Based on this context, it evaluates and maps the alert to the most relevant response workflows in the form of playbooks.

Each applicable playbook is assigned a relevance score that reflects how well it matches the characteristics of the alert. The top five scoring playbooks are then displayed under the Run Playbook section.

Workflow architecture


On product startup
Playbook recommendation Engine initializes
When the user clicks on an alert event
Recommendation engine processes the alert event
Calculates and assigns scores for playbooks
Displays top 5 playbooks with highest score

How is a playbook executed?

There are two ways in which a playbook can be executed:

- When a playbook is associated to an alert profile
- On-Demand playbook execution

A. When a playbook is associated to an alert profile

When an event triggers an alert, and the alert profile has a playbook linked to it, the playbook runs automatically. In short, the event causes an alert, and the alert triggers the assigned playbook.

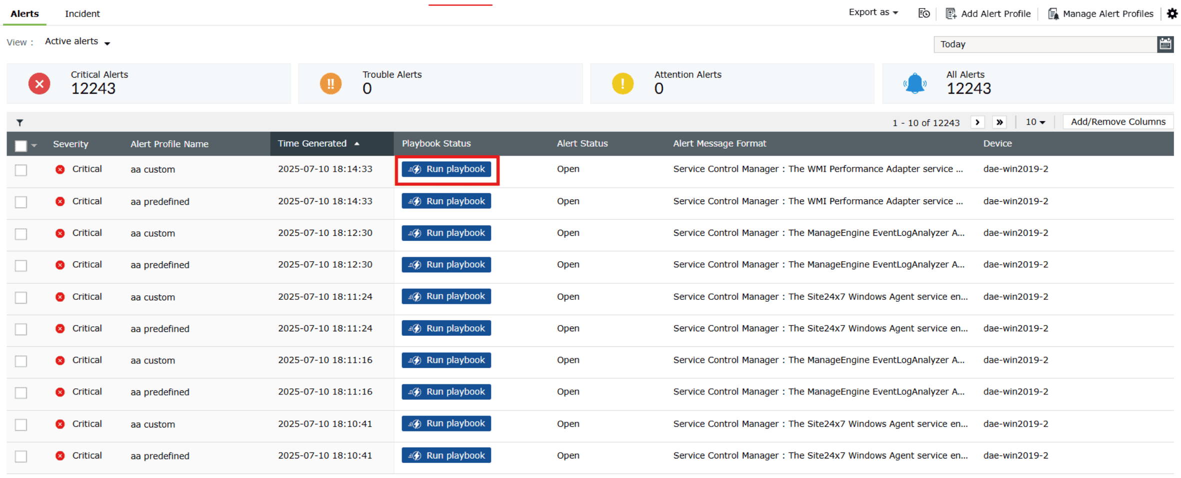
Refer to this document to learn how to associate a playbook to an alert profile.

B. On-Demand playbook execution

When an event occurrence is identified, you can manually execute a playbook- either from the list of Recommended Playbooks or Other Playbooks provided in the product console via the Alerts tab.

Below is the step-by-step guide on how to execute a playbook manually.

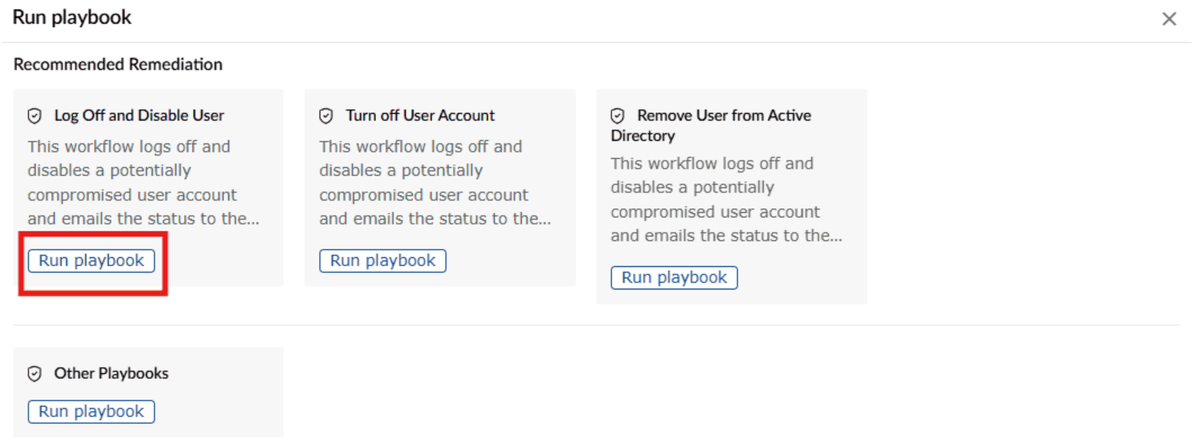
1. In the product console, navigate to the Alerts tab. The Run Playbook option is provided for each of the alerts generated. Click on the Run Playbook option associated with the alert you wish to execute the playbook for.



□	Severity	Alert Profile Name	Time Generated	Playbook Status	Alert Status	Alert Message Format	Device
□	Critical	aa custom	2025-07-10 18:14:33	Run playbook	Open	Service Control Manager : The WMI Performance Adapter service ...	dae-win2019-2
□	Critical	aa predefined	2025-07-10 18:14:33	Run playbook	Open	Service Control Manager : The WMI Performance Adapter service ...	dae-win2019-2
□	Critical	aa custom	2025-07-10 18:12:30	Run playbook	Open	Service Control Manager : The ManageEngine EventLogAnalyzer A...	dae-win2019-2
□	Critical	aa predefined	2025-07-10 18:12:30	Run playbook	Open	Service Control Manager : The ManageEngine EventLogAnalyzer A...	dae-win2019-2
□	Critical	aa custom	2025-07-10 18:11:24	Run playbook	Open	Service Control Manager : The Site24x7 Windows Agent service en...	dae-win2019-2
□	Critical	aa predefined	2025-07-10 18:11:24	Run playbook	Open	Service Control Manager : The Site24x7 Windows Agent service en...	dae-win2019-2
□	Critical	aa custom	2025-07-10 18:11:16	Run playbook	Open	Service Control Manager : The ManageEngine EventLogAnalyzer A...	dae-win2019-2
□	Critical	aa predefined	2025-07-10 18:11:16	Run playbook	Open	Service Control Manager : The ManageEngine EventLogAnalyzer A...	dae-win2019-2
□	Critical	aa custom	2025-07-10 18:10:41	Run playbook	Open	Service Control Manager : The Site24x7 Windows Agent service en...	dae-win2019-2
□	Critical	aa predefined	2025-07-10 18:10:41	Run playbook	Open	Service Control Manager : The Site24x7 Windows Agent service en...	dae-win2019-2

Image 1: Run playbook option for alerts in the alert profile

2. The Run playbook box with the available recommendations for that alert slides in. Click on the Run playbook button of any recommendation option you wish to execute as shown below.



Run playbook

Recommended Remediation

Log Off and Disable User

This workflow logs off and disables a potentially compromised user account and emails the status to the...

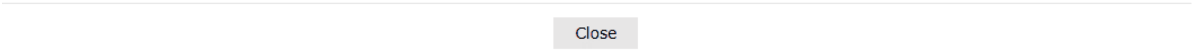
Turn off User Account

This workflow logs off and disables a potentially compromised user account and emails the status to the...

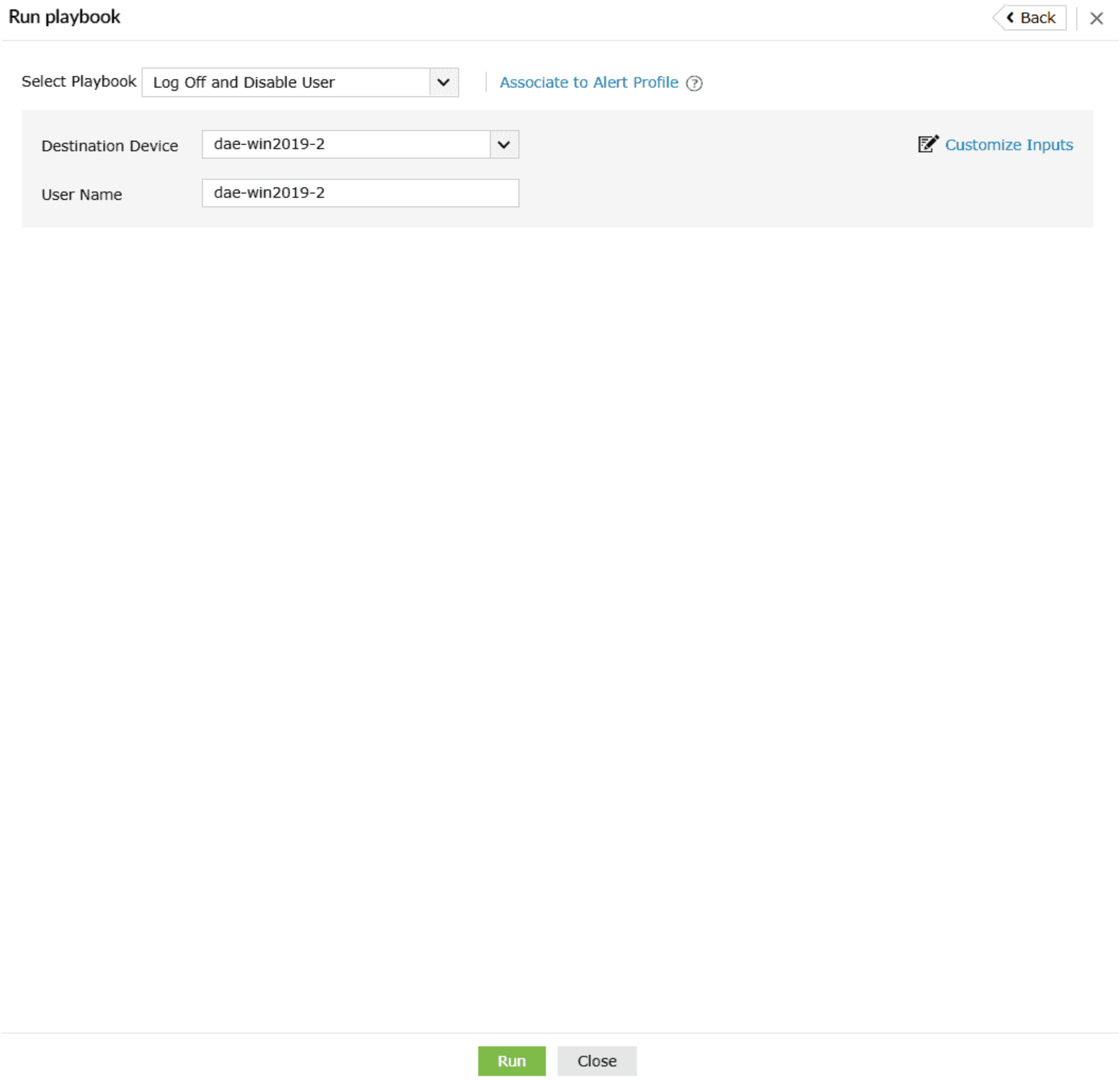
Remove User from Active Directory

This workflow logs off and disables a potentially compromised user account and emails the status to the...

Other Playbooks



3. The recommendations expand into fields as shown below.

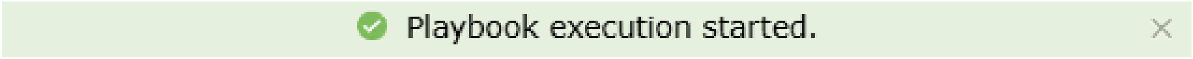


Select Playbook: Log Off and Disable User

Destination Device: dae-win2019-2

User Name: dae-win2019-2

4. The fields in each playbook recommendation vary from playbook to playbook. Click on Run after providing all the necessary inputs. The playbook is executed, and the below pop-up appears.

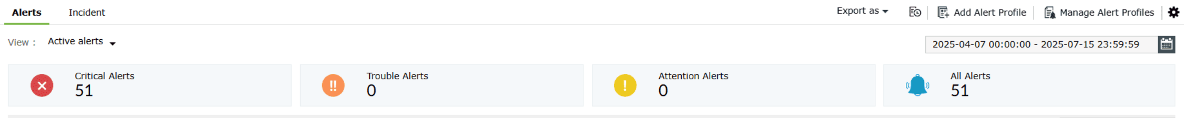


Playbook execution started.

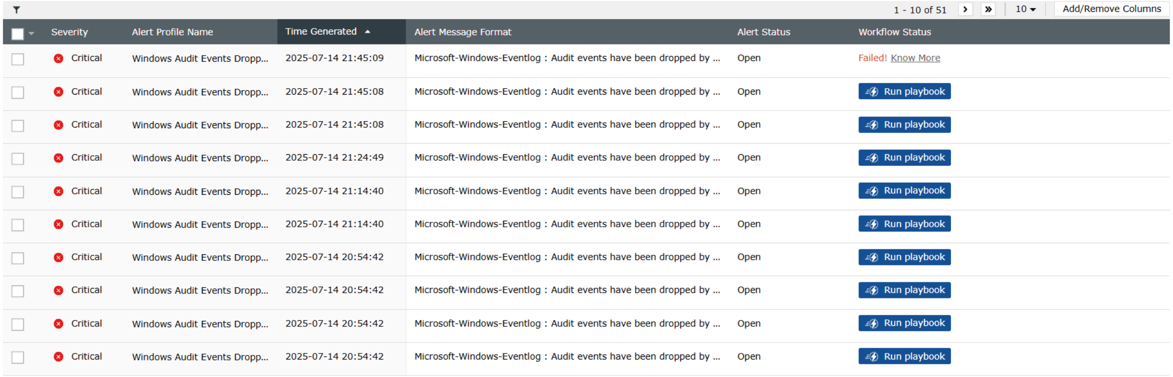
Playbook history

You can access and view the list of playbooks used until now from the playbook history as explained below:

1. Click anywhere on the row of the required alert profile in the Alerts tab.



Critical Alerts	Trouble Alerts	Attention Alerts	All Alerts
51	0	0	51

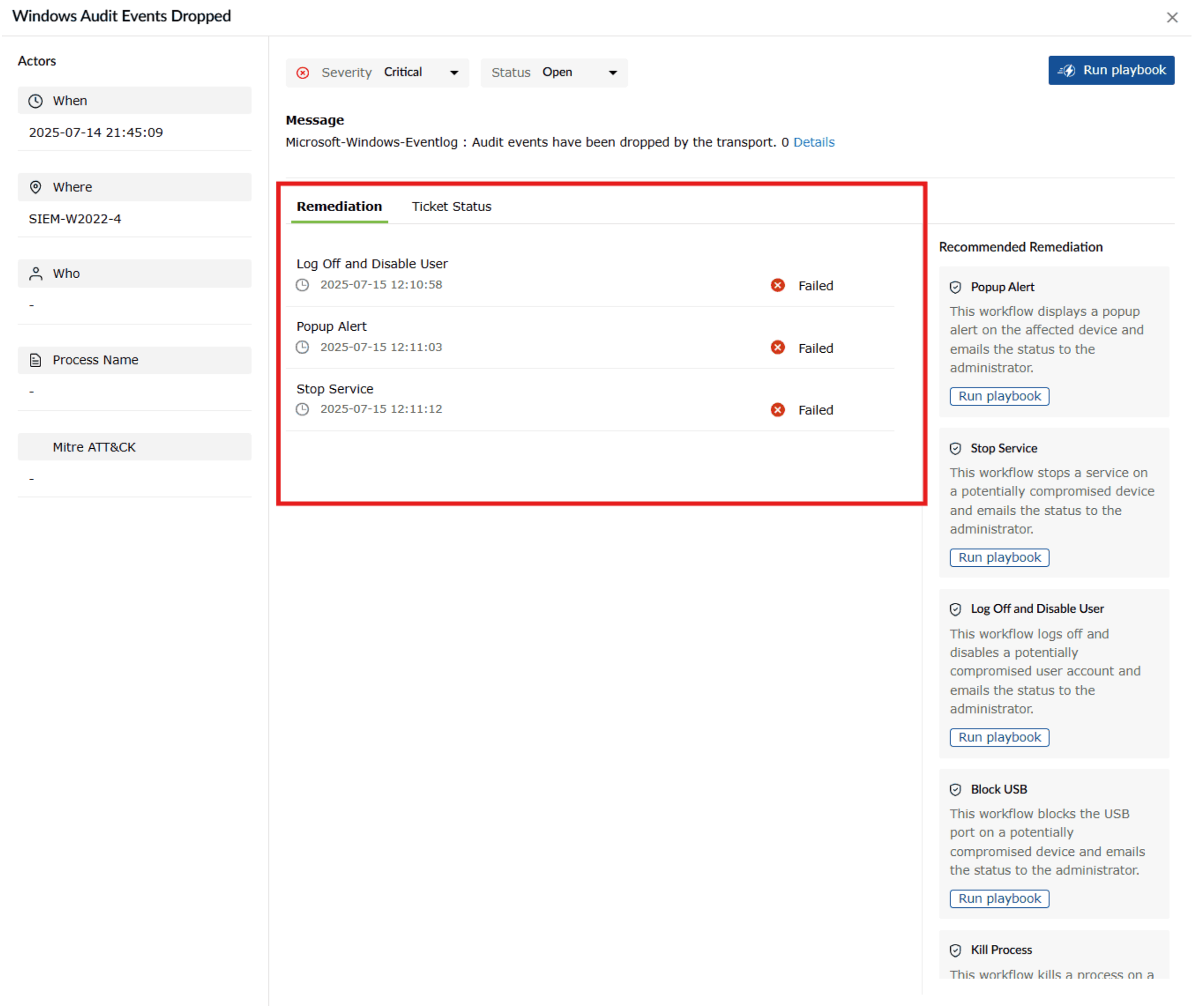


1 - 10 of 51 | 10 | Add/Remove Columns

□	Severity	Alert Profile Name	Time Generated	Alert Message Format	Alert Status	Workflow Status
□	Critical	Windows Audit Events Dropp...	2025-07-14 21:45:09	Microsoft-Windows-Eventlog : Audit events have been dropped by ...	Open	Failed! Know More
□	Critical	Windows Audit Events Dropp...	2025-07-14 21:45:08	Microsoft-Windows-Eventlog : Audit events have been dropped by ...	Open	Run playbook
□	Critical	Windows Audit Events Dropp...	2025-07-14 21:45:08	Microsoft-Windows-Eventlog : Audit events have been dropped by ...	Open	Run playbook
□	Critical	Windows Audit Events Dropp...	2025-07-14 21:24:49	Microsoft-Windows-Eventlog : Audit events have been dropped by ...	Open	Run playbook
□	Critical	Windows Audit Events Dropp...	2025-07-14 21:14:40	Microsoft-Windows-Eventlog : Audit events have been dropped by ...	Open	Run playbook
□	Critical	Windows Audit Events Dropp...	2025-07-14 21:14:40	Microsoft-Windows-Eventlog : Audit events have been dropped by ...	Open	Run playbook
□	Critical	Windows Audit Events Dropp...	2025-07-14 20:54:42	Microsoft-Windows-Eventlog : Audit events have been dropped by ...	Open	Run playbook
□	Critical	Windows Audit Events Dropp...	2025-07-14 20:54:42	Microsoft-Windows-Eventlog : Audit events have been dropped by ...	Open	Run playbook
□	Critical	Windows Audit Events Dropp...	2025-07-14 20:54:42	Microsoft-Windows-Eventlog : Audit events have been dropped by ...	Open	Run playbook
□	Critical	Windows Audit Events Dropp...	2025-07-14 20:54:42	Microsoft-Windows-Eventlog : Audit events have been dropped by ...	Open	Run playbook

Image 2: Playbook remediations for alerts via the Alerts tab

2. When you click on an alert name, the details of the alert and the related playbooks appear. Under Remediation, you can see the history of the playbooks used for the same alert up until now.



Windows Audit Events Dropped

Actors

When: 2025-07-14 21:45:09

Where: SIEM-W2022-4

Who: -

Process Name: -

Mitre ATT&CK: -

Severity: Critical

Status: Open

Run playbook

Message

Microsoft-Windows-Eventlog : Audit events have been dropped by the transport. 0 Details

Remediation | Ticket Status

Playbook	Time	Status
Log Off and Disable User	2025-07-15 12:10:58	Failed
Popup Alert	2025-07-15 12:11:03	Failed
Stop Service	2025-07-15 12:11:12	Failed

Recommended Remediation

Popup Alert
This workflow displays a popup alert on the affected device and emails the status to the administrator.
Run playbook

Stop Service
This workflow stops a service on a potentially compromised device and emails the status to the administrator.
Run playbook

Log Off and Disable User
This workflow logs off and disables a potentially compromised user account and emails the status to the administrator.
Run playbook

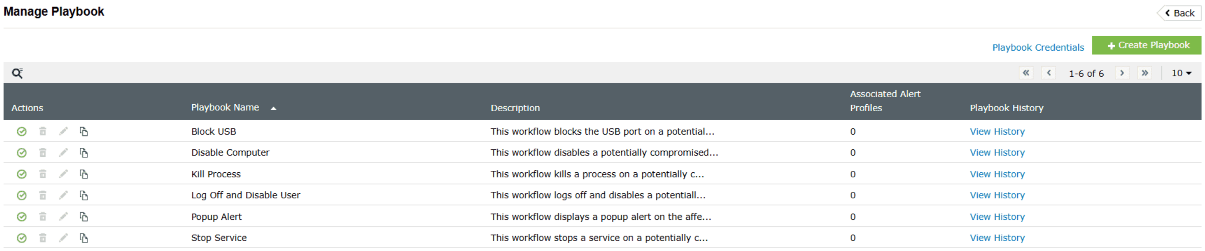
Block USB
This workflow blocks the USB port on a potentially compromised device and emails the status to the administrator.
Run playbook

Kill Process
This workflow kills a process on a

Image 3: Viewing playbooks history from the remediations

Pre-defined playbooks

The product offers 6 predefined playbooks for quick response to common security incidents. These ready-to-use playbooks perform actions like blocking USB ports, disabling computers, killing processes, or logging off users. Though they can’t be edited or deleted, you can run them on demand, link them to alert profiles, or use them as templates when creating custom playbooks. Below is the list of all 6 predefined playbooks and their description.



Actions	Playbook Name ▲	Description	Associated Alert Profiles	Playbook History
	Block USB	This workflow blocks the USB port on a potential...	0	View History
	Disable Computer	This workflow disables a potentially compromised...	0	View History
	Kill Process	This workflow kills a process on a potentially c...	0	View History
	Log Off and Disable User	This workflow logs off and disables a potentiall...	0	View History
	Popup Alert	This workflow displays a popup alert on the affe...	0	View History
	Stop Service	This workflow stops a service on a potentially c...	0	View History

Image 4: List of predefined playbooks available in the product

Playbook name	Description
Block USB	This playbook blocks the USB port on a potentially compromised device and emails the status to the administrator.
Disable Computer	This playbook disables a potentially compromised computer and emails the status to the administrator.
Kill Process	This playbook kills a process on a potentially compromised device and emails the status to the administrator.
Log Off and Disable User	This playbook logs off and disables a potentially compromised user account and emails the status to the administrator.
Popup Alert	This playbook displays a popup alert on the affected device and emails the status to the administrator.
Stop Service	This playbook stops a service on a potentially compromised device and emails the status to the administrator.

Playbook name	Description

Use cases

1. Real-time ransomware containment in endpoint environments

Use case
Ransomware attacks usually begin with suspicious file activity or an unauthorized encryption process on the endpoints.
With Playbooks
Playbooks aid in effective remediation strategies when a potential ransomware attack attempt is detected. You can auto-trigger a playbook to disable USB ports, shut down infected systems, block lateral movement via firewall rules, and also notify SOC teams—all within seconds of detection. This helps in reducing the attack blast radius while ensuring business continuity.

ⓘ MITRE Mapping

Tactic: Impact (TA0040), Execution (TA0002)
Technique: Data Encrypted for Impact (T1486), Command and Scripting Interpreter (T1059)

2. Adaptive firewall rule automation against emerging threats

Use case
A swift response is crucial after detection of Indicators of Compromise (IoCs) like malicious IPs or domains identified in threat intelligence feeds.
With Playbooks
The matching of alerts can trigger instant automated updates to firewall configurations like deny inbound/outbound rules for Cisco ASA, FortiGate, PaloAlto, SophosXG; etc and effectively blacklist malicious endpoints without the need for any manual rule entry thus, ensuring a rapid response across perimeter devices.

ⓘ MITRE Mapping

Tactic: Defense Evasion (TA0005), Command and Control (TA0011)
Technique: Ingress Tool Transfer (T1105), Application Layer Protocol: Web Protocols (T1071.001)

3. Automatic user account lockdown during Brute-force attacks

Use case
User accounts are targeted during malicious attempts like brute force login attempts and password spraying.
With Playbooks
When an alert for multiple failed login attempts is triggered, a well configured playbook can instantly disable the associated account, block the source IP in the firewall and also notify the admins via alert notifications. This ensures instantaneous mitigation before the attacker(s) successfully authenticate

MITRE Mapping

Tactic: Credential Access (TA0006)

Technique: Brute Force (T1110), Password Spraying (T1110.003)

4. Smart patching of vulnerabilities through Endpoint Central

Use case

Unpatched systems are highly advantageous as entry points for attackers. In large organizations, coordination with IT teams for patching is often delayed/time-consuming.

With Playbooks

When a vulnerability is detected, a playbook can approve the patch and also initiate its deployment via Endpoint Central without requiring any human intervention. This closes critical vulnerabilities faster than any of the manual processes.

MITRE Mapping

Tactic: Initial Access (TA0001), Persistence (TA0003)

Technique: Exploit Public-Facing Application (T1190), Exploitation for Privilege Escalation (T1068)

5. Rogue device detection and network quarantine

Use case

Unknown devices can suddenly appear on the network, often behaving anomalously or bypassing the critical asset inventories.

With Playbooks

When an alert is triggered for such suspicious device activities, a traceroute can be run along with a ping test to assess network path, then disable that device account in AD and create deny access rules in firewalls. This ensures that suspicious assets are isolated immediately while preserving evidence for forensics simultaneously.

MITRE Mapping

Tactic: Discovery (TA0007), Lateral Movement (TA0008)

Technique: Remote System Discovery (T1018), Exploitation of Remote Services (T1210)

6. Centralized enforcement of USB security policies

Use case

Unmanaged USB ports on high-risk systems can act as entry points for attacks pertaining to data leaks

With Playbooks

Optimized configurations could be made in the playbooks to automatically disable USB ports on systems detected for anomalous behavior or based on policy violation alerts. This also ensures zero-trust enforcement even in distributed endpoint environments.

ⓘ MITRE Mapping

Tactic: Collection (TA0009), Exfiltration (TA0010)

Technique: Data Staged (T1074), Exfiltration Over Physical Medium (T1052)

Read also

This document covered Playbook functionality, execution methods, and use cases. For related capabilities that enhance security orchestration and response, refer to

- Creating playbook
- Manage playbooks
- Update playbook credentials

4.3.2.2. Playbook management prerequisites

Last updated on: September 12, 2025

In this page

Overview

This document outlines the prerequisites for executing playbook actions, including supported OS platforms, necessary ports, protocols, and permission settings. It details the configurations required across Windows, Linux, AD, and firewall devices to ensure seamless response execution during security events.

Prerequisites

List of devices supported

- All types of Windows operating system.
- Linux operating systems:
  - Ubuntu
  - Debian
  - Fedora
  - CentOS
  - Red Hat Enterprise Linux (RHEL)
  - Arch Linux
  - SUSE Linux Enterprise Server (SLES)
  - openSUSE
  - Gentoo OS

Below are the necessary configurations to be made in order to access the playbook capability

Guide:
Port: Used for communication (this port should be open, free, and allowed in firewall)
Inbound: To which device/application the action is targeted towards.
Outbound: From where the action is raised.
Service: Which service/protocol will be used to execute this action.

NETWORK ACTIONS

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

WINDOWS ACTIONS

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

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

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and Permissions
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	Service should be running. • Full Control permission to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
ALL SERVICE BLOCK	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: • Distributed COM Users • Administrators User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	RPC randomly allocated high TCP ports	
START PROCESS	TCP/135	Audited Windows Device	EventLog Analyzer Server	RPC	UserGroups: Distributed COM Users User Permissions: For root\cim v2 In WMI Properties: • Execute Methods • Enable Account • Remote Enable • Read Security
	TCP/139	Audited Windows Device	EventLog Analyzer Server	NetBIOS session RPC/NP	
	TCP/445	Audited Windows Device	EventLog Analyzer Server	SMB RPC/NP	
	RPC ports -	Audited	EventLog	RPC randomly	

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

LINUX ACTIONS

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

AD ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Additional Rights and

BLOCK	PORT	INBOUND	OUTBOUND	SERVICE	Permissions
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
	TCP/135	Audited Windows Device	EventLog Analyzer Server	UserGroups: Distributed COM Users User Rights: • Act as part of the operating system • Log on as a batch job • Log on as a service • Replace a process level

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
WRITE TO FILE WINDOWS	RPC ports - TCP/1024 to 65,535	Audited Windows Device	EventLog Analyzer Server	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.
WRITE TO FILE LINUX	TCP/Specified port.	Audited Linux Device	EventLog Analyzer Server	Environment Permission: Sudo permission for user
HTTP WebHook	-	-	-	Environment Permission: A "connect" Socket Permission to the host/port combination of the destination URL or a "URL Permission" that permits this request.
FORWARD LOGS	TCP/Specified Port	Audited Windows / Linux Device	EventLog Analyzer Server	-
CSV LOOKUP	TCP/Specified Port	Audited Windows / Linux Device	EventLog Analyzer Server	User Permissions: Read permission to the specified CSV file.

FIREWALL ACTIONS

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
Cisco ASA deny inbound/Outbound rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: Refer to this page

BLOCK	PORT	INBOUND	OUTBOUND	Additional Rights and Permissions
Fortigate deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: Refer to this page
Palo Alto deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: Refer to this page
Sophos XG deny Access rules	https/443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: Refer to this page
Barracuda deny Access rules	https/8443	Firewall Device	EventLog Analyzer Server	Ports User Customizable Additional Rights: Refer to this page

Read also

This guide covers the groundwork for executing playbooks. For a deeper understanding of automation and orchestration in security response, refer to:

- Manage playbooks
- Update playbook credentials

4.3.2.3. Creating a playbook

Last updated on: September 12, 2025

In this page

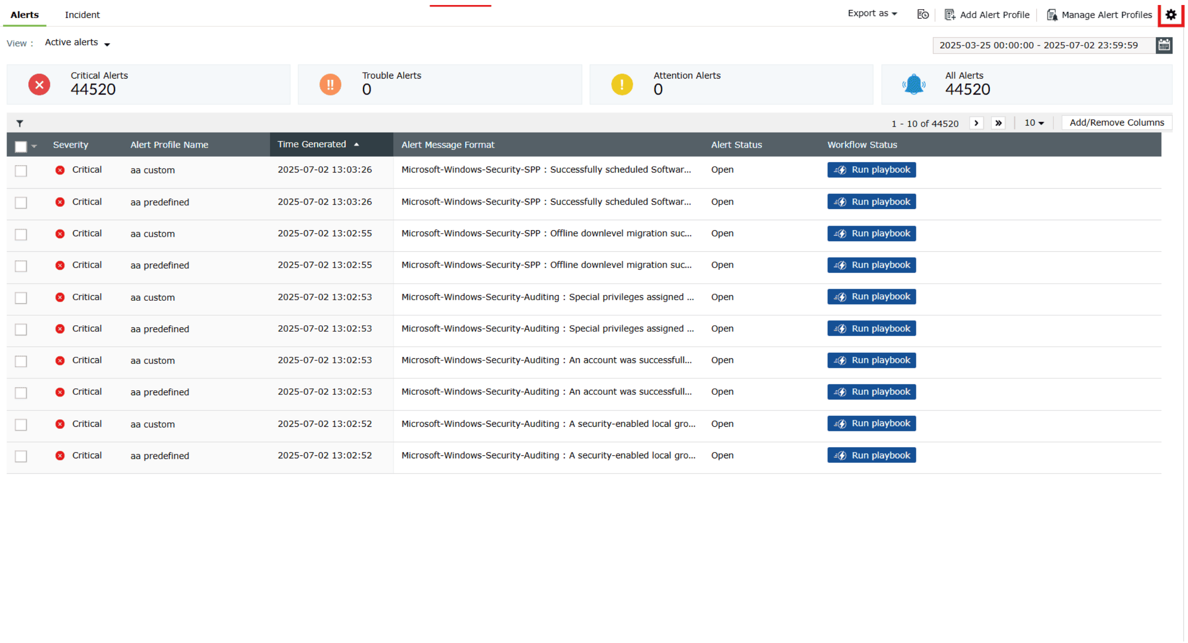
Overview

This document guides you through the steps to build custom playbooks using predefined logic blocks. These workflows automate security responses, ranging from system actions to AD user operations, helping you mitigate incidents more efficiently.

Creating a custom playbook

Steps to create a playbook

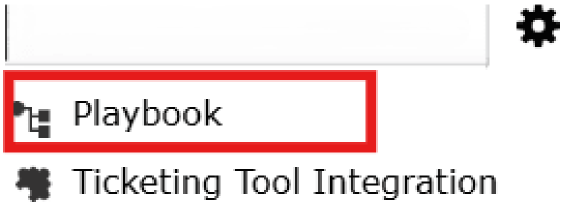
1. In the product console, navigate to the Alerts tab. Click on the More tools icon present at the top-right corner of the page as highlighted in the below image.



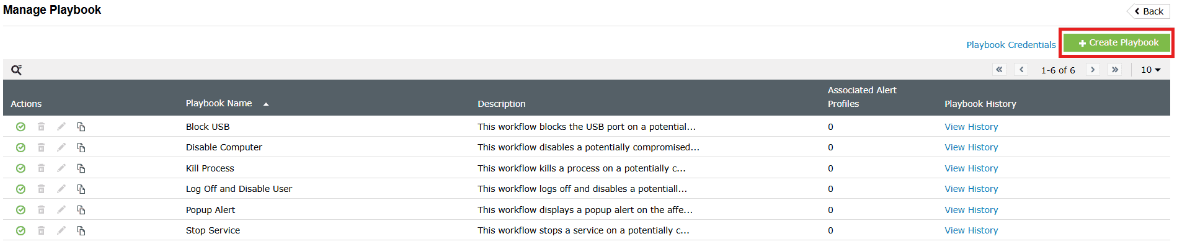
Severity	Alert Profile Name	Time Generated	Alert Message Format	Alert Status	Workflow Status
Critical	aa custom	2025-07-02 13:03:26	Microsoft-Windows-Security-SPP : Successfully scheduled Softwar...	Open	Run playbook
Critical	aa predefined	2025-07-02 13:03:26	Microsoft-Windows-Security-SPP : Successfully scheduled Softwar...	Open	Run playbook
Critical	aa custom	2025-07-02 13:02:55	Microsoft-Windows-Security-SPP : Offline downlevel migration suc...	Open	Run playbook
Critical	aa predefined	2025-07-02 13:02:55	Microsoft-Windows-Security-SPP : Offline downlevel migration suc...	Open	Run playbook
Critical	aa custom	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : Special privileges assigned ...	Open	Run playbook
Critical	aa predefined	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : Special privileges assigned ...	Open	Run playbook
Critical	aa custom	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : An account was successfull...	Open	Run playbook
Critical	aa predefined	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : An account was successfull...	Open	Run playbook
Critical	aa custom	2025-07-02 13:02:52	Microsoft-Windows-Security-Auditing : A security-enabled local gro...	Open	Run playbook
Critical	aa predefined	2025-07-02 13:02:52	Microsoft-Windows-Security-Auditing : A security-enabled local gro...	Open	Run playbook

Image 1: More tools icon in the Alerts tab

2. Click on Playbook to open the Manage Playbook page.



3. Click on the +Create Playbook button.



Manage Playbook

< Back

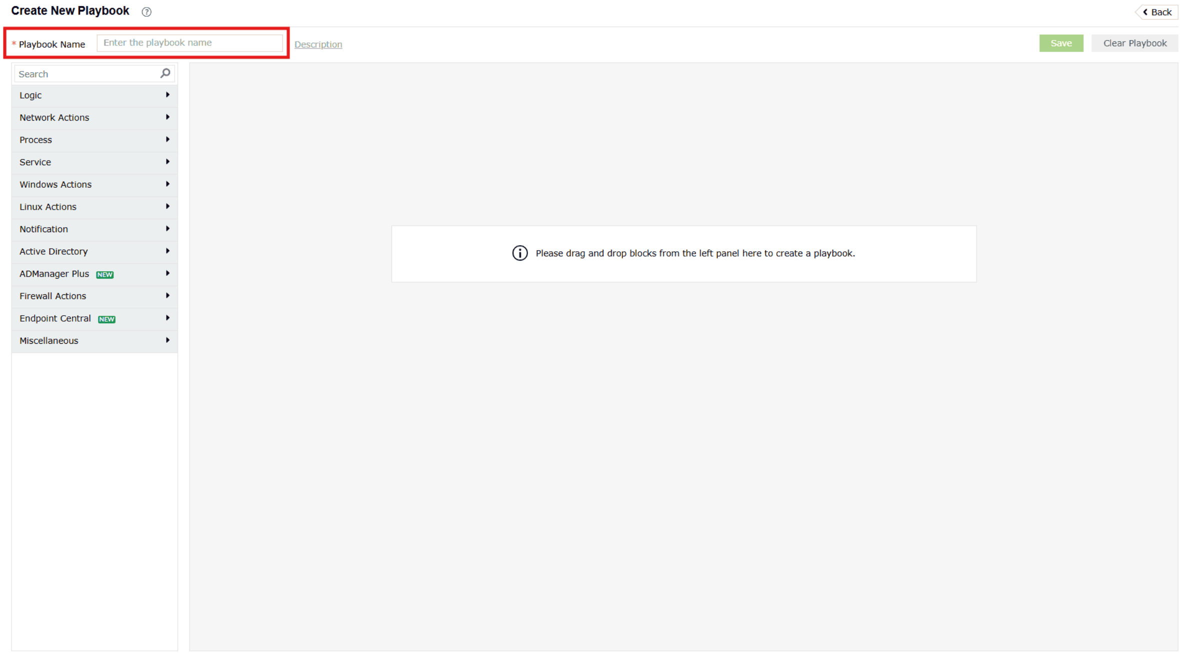
Playbook Credentials | + Create Playbook

« ‹ 1-6 of 6 › » 10 ▾

Actions	Playbook Name ▲	Description	Associated Alert Profiles	Playbook History
✓	Block USB	This workflow blocks the USB port on a potential...	0	View History
✓	Disable Computer	This workflow disables a potentially compromised...	0	View History
✓	Kill Process	This workflow kills a process on a potentially c...	0	View History
✓	Log Off and Disable User	This workflow logs off and disables a potentiall...	0	View History
✓	Popup Alert	This workflow displays a popup alert on the affe...	0	View History
✓	Stop Service	This workflow stops a service on a potentially c...	0	View History

Image 2: Create Playbook button via the Alerts tab

4. Enter a name for the playbook in the Playbook Name field.



Create New Playbook

< Back

* Playbook Name: Enter the playbook name | Description

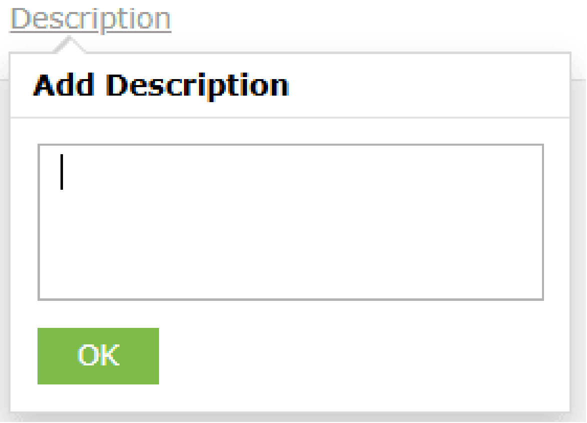
Save | Clear Playbook

Please drag and drop blocks from the left panel here to create a playbook.

Image 3: Playbook name field during playbook creation

5. Click on Description (optional) beside the Playbook Name field to enter an appropriate description for the playbook. Click on OK.

playbook. Click on OK.

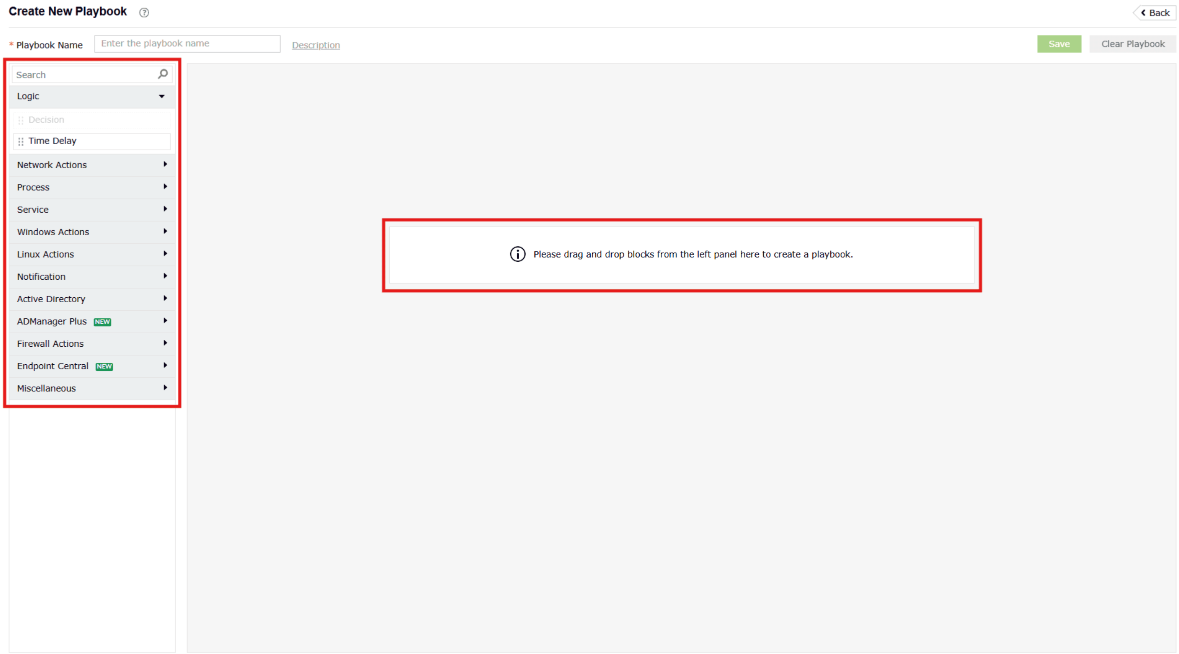


Description

Add Description

OK

6. On the left pane, there are components provided for different event categories. Click on the respective drop-down icons in order to expand the actions. Create a playbook by dragging and dropping the playbook blocks from the left pane into the space provided. Ensure that these blocks are logically arranged to execute an event in your infrastructure.



Create New Playbook

‹ Back

* Playbook Name: Enter the playbook name

Description

Save

Clear Playbook

Search

Logic

Decision

Time Delay

Network Actions

Process

Service

Windows Actions

Linux Actions

Notification

Active Directory

ADManager Plus NEW

Firewall Actions

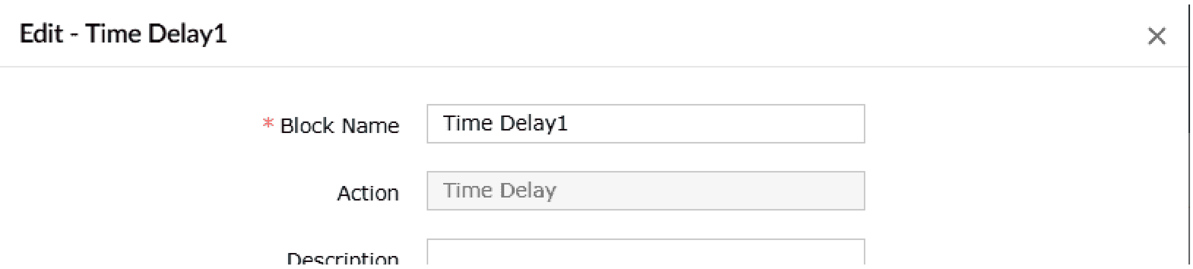
Endpoint Central NEW

Miscellaneous

ⓘ Please drag and drop blocks from the left panel here to create a playbook.

Image 4: Playbook blocks arrangement during playbook creation

7. The moment you finish the drag and drop action, an Edit pop-up appears with fields to configure that specific playbook block further. The fields to edit the playbook blocks vary from one block to another. After editing as per your requirements, click on OK. You can always come back and edit these blocks by clicking on the edit icon ✎ visible on the blocks in the drag and drop area.

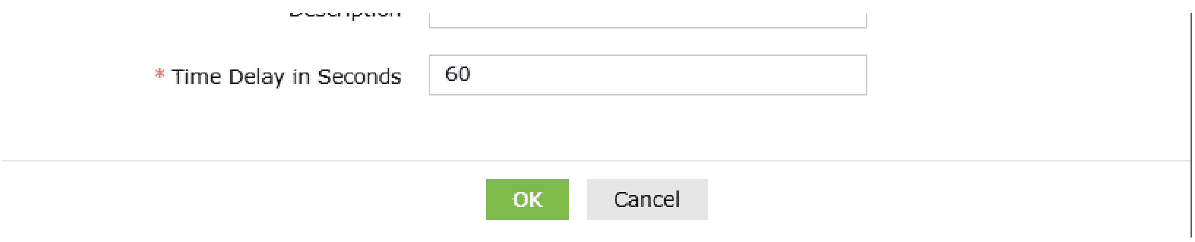


Edit - Time Delay1 ✕

* Block Name: Time Delay1

Action: Time Delay

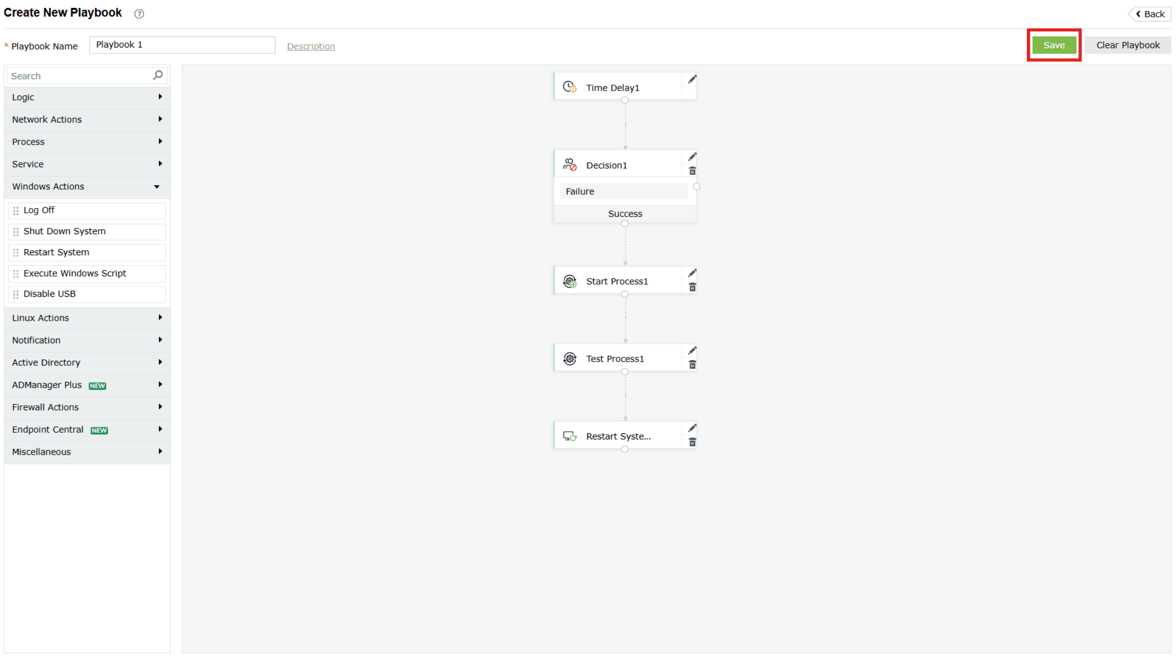
Description



* Time Delay in Seconds: 60

Image 5: Playbook blocks details during playbook creation

8. You can include multiple blocks in one playbook. Once you are done with the workflow design of your playbook, click on Save.



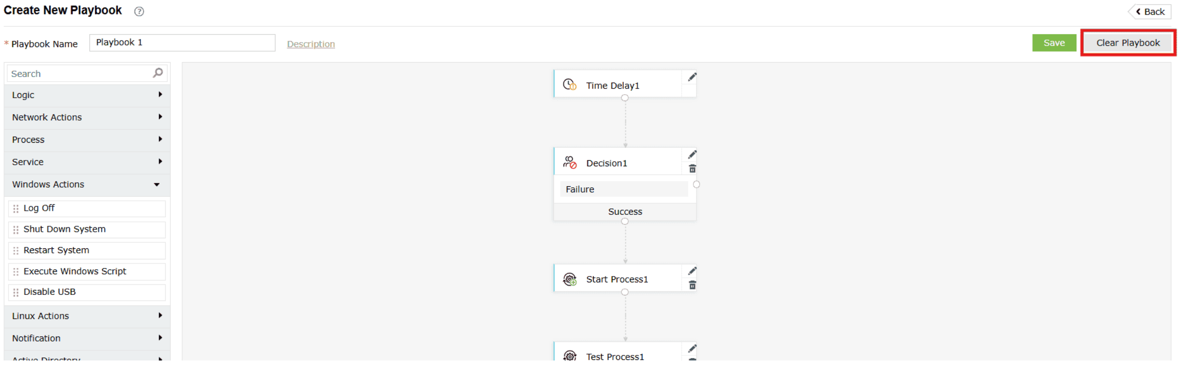
* Playbook Name: Playbook 1

Image 6: Save a playbook after playbook creation

9. The playbook is saved instantly, and you will be taken back to the Manage Playbook tab with your newly created playbook listed under the playbooks list.

Reset playbook

1. In case you wish to reset the configurations set in the playbook creation up until now, click on the Clear Playbook button as highlighted in the below image.



* Playbook Name: Playbook 1

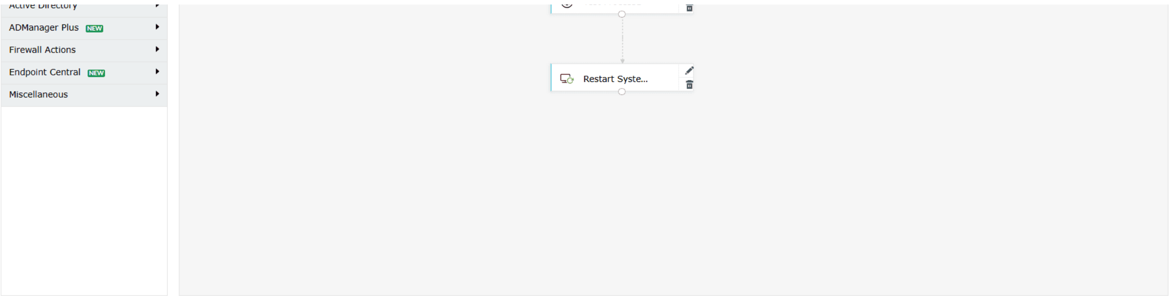
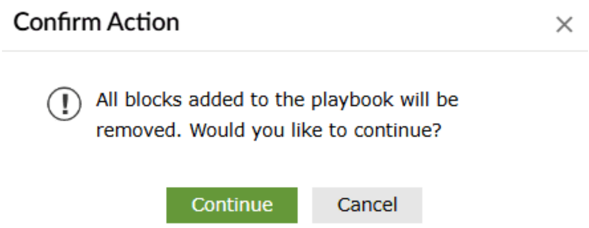


Image 7: Clear playbook option during playbook creation

2. A Confirm Action pop-up appears. Click on Continue.



Confirm Action

All blocks added to the playbook will be removed. Would you like to continue?

3. All the configurations set in the playbook until then are cleared instantly, and you can see that the workspace becomes empty again.

List of playbook blocks

The product contains multiple playbook blocks to help you configure the playbooks to perform the required actions. The logic blocks are categorized under different sections.

The list of playbook blocks and the details to be specified while configuring playbooks using them are given below:

Component	Logic blocks	Details to be specified
Logic Actions	Decision Allows you to branch the playbook based on the status of the previous action.	Optional description
	Time Delay Allows you to introduce a time delay in the execution of the playbook.	The time delay in seconds.
	Ping Device Allows	• The name of the device to be pinged. • Number of echo request messages to be sent.

Component	Logic blocks	Details to be specified
Network actions	you to ping a device within your network to check connectivity	• Size of the packet to be sent. • Timeout for the action. • Number of action retries within the specified time.
	Trace Route Allows you to run a trace route function to a device in your network to identify the path.	• The name of the device you wish to trace the route to. • The maximum number of Hops. • Timeout for the action.
Process actions	Test Process Allows you to test whether a process is running on a device.	• The name of the device on which you want to test the process. • The process you want to test. • ExecutablePath and CommandLine to execute the process.
	Start Process Allows you to start a process on a device	• The name of the device on which you want to start a process. • The process working directory. • The command to start the process.
	Stop Process Allows you to stop a process on a device.	• The name of the device on which you want to stop the process. • The process you want to stop. • ExecutablePath and CommandLine to execute the process.
Service actions	Test Service Allows you to test whether a service is running on a device.	• The name of the device on which you want to test the service. • The service you want to test
	Start Service Allows you to start a service on a device.	• The name of the device on which you wish to start a service. • The service to be started.

Component	Logic blocks	Details to be specified
	Stop Service Allows you to stop a service on a device.	• The name of the device on which you wish to stop a service. • The service to be stopped
Windows actions	Log Off Allows you to log off from the currently active session on a device.	• The name of the device you want to log off from. • Select whether you'd like to force this action.
	Shut Down System Allows you to shut down a Windows device.	• The name of the device to be shut down. • Select whether you'd like to force this action.
	Restart System Allows you to restart a Windows device.	• The name of the device to be restarted. • Select whether you'd like to force this action.
	Execute Windows Script Allows you to execute a specified script file on a Windows device.	• The name of the device on which you want to execute the script file. • The type of script file. • Upload the script file to be executed. • Arguments to the script, if any. • You can separate multiple arguments using commas. • Timeout for the action. • The working directory for the script's execution.
	Disable USB Allows you to disable the USB port on a device.	The name of the device on which you want to disable the USB port.
	Shut Down Linux Allows you to shut down a Linux device.	• The name of the device to be shut down. • Select whether you'd like to force this action.

Component	Logic blocks	Details to be specified
Linux actions	Restart Linux Allows you to restart a Linux device.	• The name of the device to be restarted. • Select whether you'd like to force this action.
	Execute Linux Script Allows you to execute a specified script file on a Linux device.	• The name of the device on which you want to execute the script file. • The type of script file. • Upload the script file to be executed. • Arguments to the script, if any. • You can separate multiple arguments using commas. • Timeout for the action. • The working directory for the script's execution.
Notification actions	Send Pop-Up Message Allows you to display a pop-up message on a device.	• The name of the device on which you want to display the message. • The message to be displayed.
	Send Email Allows you to send an email message.	• The recipient's email address. • The email subject and body.
	Send SMS Allows you to send an SMS message.	• The recipient's mobile number. • The SMS content.
	Send SNMP Trap Allows you to send SNMP traps to the required destination.	• Enterprise OID. • SNMP Manager. • Message content.
	Disable User Allows you to disable a user's account.	The name of the user account you want to disable.

Component	Logic blocks	Details to be specified
Active Directory actions	Delete User Allows you to delete a user account.	The name of the user account you want to delete.
	Disable Computer Allows you to disable a computer account.	The name of the computer account you want to disable
Firewall Actions	Cisco ASA Deny Inbound Rule Allows you to add an deny inbound rule.	• The name of the firewall device. • The Interface name. • Source address. • Destination address.
	Cisco ASA Deny Outbound Rule Allows you to add an deny outbound rule.	• The name of the firewall device. • The Interface name. • Source address. • Destination address.
	Fortigate Deny Access Rule Allows you to add an deny access rule.	• Name of the firewall device. Source address. • Destination address. • Name of the source interface. • Name of the destination interface.
	PaloAlto Deny Access Rule Allows you to add an deny access rule.	• Name of the firewall device. Source address. • Destination address. • Name of the source zone. • Name of the destination zone. • Type of Rule (Universal, Intrazone or Interzone).
	SophosXG Deny Access Rule Allows you to add an deny access rule.	• Name of the firewall device. • Source address. • Destination address.
		• The name of the firewall device.

Component	SophosXG Update Logic blocks Deny Access Rule	- The name of the firewall device. Details to be specified - The rule name.
	Allows you to update an deny access rule.	- Source address. - Destination address.
	Barracuda CloudGen Deny Access Rule Allows you to add an deny access rule.	- Name of the firewall device. - Source address. - Destination address. - Name of the source interface. - Name of the destination interface. - Type of Rule (Inbound or Outbound).
Miscellaneous actions	Write to File Allows you to write a message to a file	- The name of the device on which the file is located. - The file name. - The absolute file path. - The text to be written to the file. - Select whether you would like to append to or overwrite a file if it already exists.
	CSV Lookup Allows you to search for values within a CSV file.	- Upload the CSV file to perform by clicking on "Browse". - Specify the header or column number. - Select the field to be matched.
	Forward Logs Allows you to forward logs to the required destination.	- Name of the destination server. - The protocol to be used. - Port number and standard.
	HTTP Request Allows you to send an HTTP request to a URL.	- The URL to which you want to send an HTTP request to. - Specify the Method you want to use (Get or Post). - Add the required headers. - Add the required parameters.

Component	Logic blocks	Details to be specified
	Disable User Allows you to disable a user account	• The name of the block. • The action to be performed (here, Disable User). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to disable.
	Delete User Allows you to delete a user account	• The name of the block. • The action to be performed (here, Delete User). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to delete.
	Disable Computer Allows you to disable a computer account.	• The name of the block. • The action to be performed (here, Disable Computer). • A brief description for this block to record its purpose in the workflow. • The device name of the computer account you want to disable.
	Reset user password Allows the user to reset their password	• The name of the block. • The action to be performed (here, Reset user password). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to reset the password. • The type of password that you want: Random or Custom.
	Add user to group Allows you to add a user to a particular group	• The name of the block. • The action to be performed (here, Add user to group). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to add to

Component	Logic blocks	the group. Details to be specified • The name of the group you want to add the user.
ADManager Plus actions		
	Remove user from group Allows you to remove a user from a particular group	• The name of the block. • The action to be performed(here, Remove user from group). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to remove from the group. • The name of the group that you want to remove the user from, or remove the user from all the groups that are available.
	Enable user Allows you to enable a disabled user account	• The name of the block. • The action to be performed(here, Enable user). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to enable.
	Unlock user Allows you to unlock a locked user account	• The name of the block. • The action to be performed(here, Unlock user). • A brief description for logic block to record its purpose in the playbook. • The username of the user account you want to unlock.
	Update user Allows you to update an attribute of a user	• The name of the block. • The action to be performed(here, Update user). • A brief description for this block to record its purpose in the playbook. • The username of the user account you want to update. • The attribute that you want to update in the user account's data. • The value of the attribute that needs to be updated.

Component	Logic blocks	• The name of the block. Details to be specified • The action to be performed(here, Delete Computer).
	Delete Computer Allows you to delete a computer account	• A brief description for this block to record its purpose in the playbook. • The device name of the computer account you want to delete.
	Enable computer Allows you to enable a disabled computer account	• The name of the block. • The action to be performed(here, Enable Computer). • A brief description for this block to record its purpose in the playbook. • The device name of the computer account you want to enable.
Endpoint Central actions	Install Patch Allows you to install a patch on a specific device for a detected vulnerability.	• The name of the block. • Name/IP of the destination device to install patch. • Name of the deployment configuration. • Description for the deployment configuration. • Vulnerability identifier will be extracted from alert criteria. • Deployment policy to be applied.
	Approve Patch Allows you to approve patches for the detected vulnerability.	The name of the block Vulnerability identifier will be extracted from alert criteria.

Read also

This document covered how to create custom playbooks, including workflow components and supported actions. For related capabilities that enhance security orchestration and automation, refer to:

- Manage playbooks
- Update playbook credentials

4.3.2.4. Managing playbooks

Last updated on: September 12, 2025

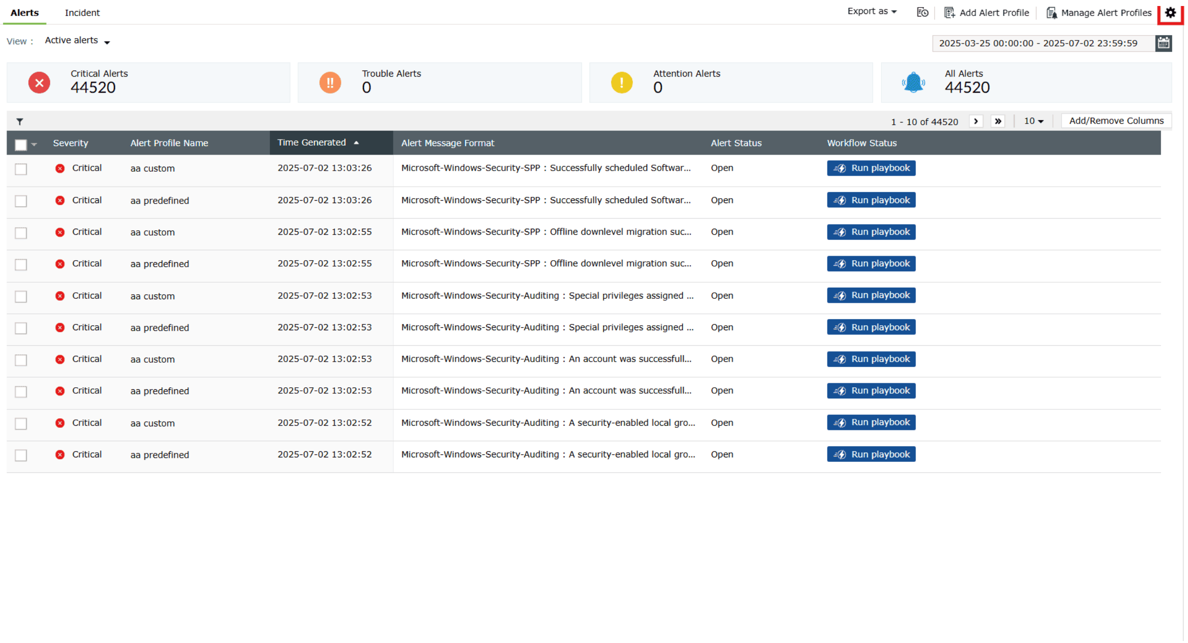
In this page

Overview

The manage playbook section provides an overview of all configured playbooks along with their status, associated alert profiles, and execution history. Custom playbooks can be edited, deleted, copied, or toggled on/off. Predefined playbooks, however, can only be enabled, disabled, or duplicated—not edited or deleted.

Managing playbooks

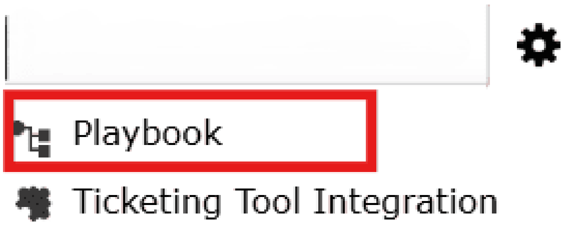
1. In the product console, navigate to the Alerts tab. Click on the More tools icon present at the top-right corner of the page as highlighted in the below image.



□	Severity	Alert Profile Name	Time Generated	Alert Message Format	Alert Status	Workflow Status
□	Critical	aa custom	2025-07-02 13:03:26	Microsoft-Windows-Security-SPP : Successfully scheduled Softwar...	Open	Run playbook
□	Critical	aa predefined	2025-07-02 13:03:26	Microsoft-Windows-Security-SPP : Successfully scheduled Softwar...	Open	Run playbook
□	Critical	aa custom	2025-07-02 13:02:55	Microsoft-Windows-Security-SPP : Offline downlevel migration suc...	Open	Run playbook
□	Critical	aa predefined	2025-07-02 13:02:55	Microsoft-Windows-Security-SPP : Offline downlevel migration suc...	Open	Run playbook
□	Critical	aa custom	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : Special privileges assigned ...	Open	Run playbook
□	Critical	aa predefined	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : Special privileges assigned ...	Open	Run playbook
□	Critical	aa custom	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : An account was successfull...	Open	Run playbook
□	Critical	aa predefined	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : An account was successfull...	Open	Run playbook
□	Critical	aa custom	2025-07-02 13:02:52	Microsoft-Windows-Security-Auditing : A security-enabled local gro...	Open	Run playbook
□	Critical	aa predefined	2025-07-02 13:02:52	Microsoft-Windows-Security-Auditing : A security-enabled local gro...	Open	Run playbook

Image 1: More tools option in the Alerts tab

2. Click on Playbook to open the Manage Playbook page.

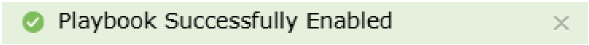


3. The Manage Playbook page displays the list of all playbooks, their descriptions, the number of alert profiles associated with each playbook, and their histories. You can:
   - Enable/disable
   - Delete
   - Edit
   - Copy a playbook

Enable/disable a playbook

Enabling a playbook

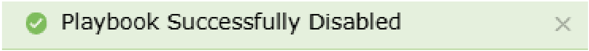
1. Click on the currently disabled icon ⊘ under the Actions column to enable the playbook.
2. As soon as you perform this action, the icon indicates that the playbook is now enabled ✓ and the below pop-up message appears briefly.



✓ Playbook Successfully Enabled ×

Disabling a playbook

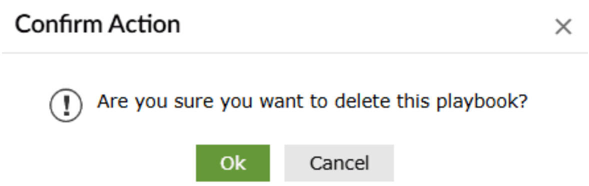
1. Click on the currently enabled icon ✓ under the Actions column to disable the playbook.
2. As soon as you perform this action, the icon indicates that the playbook is now disabled ⊘ and the below pop-up message appears briefly.



✓ Playbook Successfully Disabled ×

Delete a playbook

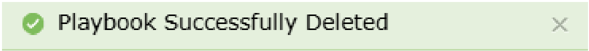
1. Click on the Delete icon 🗑 under the Actions column to delete the playbook.
2. A Confirm Action pop-up appears. Click on Ok.



Confirm Action ×

Are you sure you want to delete this playbook?

3. Upon successful completion of the action, the below pop-up appears.



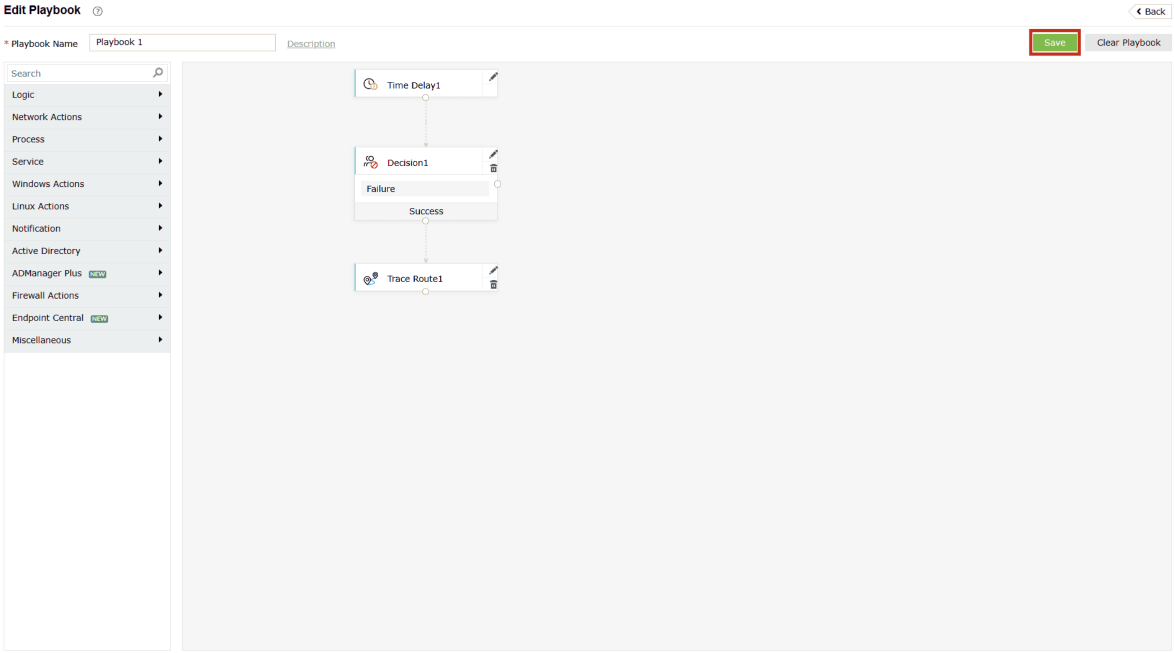
✓ Playbook Successfully Deleted ×

ⓘ NOTE

Only custom created playbooks can be deleted. Pre-defined playbooks can only be enabled/disabled or copied.

Edit a playbook

1. Click on the Edit icon ✎ under the Actions column to edit the respective playbook.
2. You will be taken to the Edit Playbook page. Make the necessary edits by changing the playbook blocks if needed and/or editing the playbook blocks' details, and click on Save.



Edit Playbook

* Playbook Name: Playbook 1

Image 2: Editing a playbook and saving the changes

3. The playbook is saved instantly, and you will be taken back to the Manage Playbook tab with your updated playbook listed under the playbooks list.

Copy a playbook

1. Click on the Copy icon ⧉ under the Actions column to duplicate the respective playbook.
2. That playbook is instantly duplicated, and you can see the cloned version with the Playbook Name "Copy of (name of the playbook you have cloned)".

Read also

To get the most out of Playbooks, learn how to create custom ones using drag-and-drop blocks and how to associate them with alert profiles for automated incident response. You may also want to explore supported playbook actions and prerequisite configurations.

- Update playbook credentials
- Creating playbook

- Creating playbook
- Prerequisites for playbook configuration

4.3.2.5. Updating playbook credentials

Last updated on: September 12, 2025

In this page

Overview

To ensure successful playbook execution across your infrastructure, credentials for supported devices must be securely configured within the product. You can set global or device-specific credentials for Windows, Linux, and major firewall vendors. Some integrations, like ADManager Plus and SNMP Traps, require additional setup to enable action-based responses.
Only users with admin privileges can manage playbook credentials.

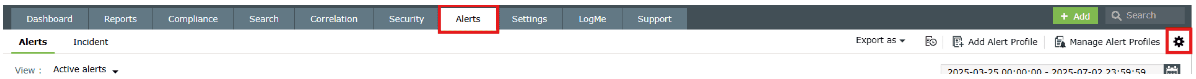
Updating playbook credentials

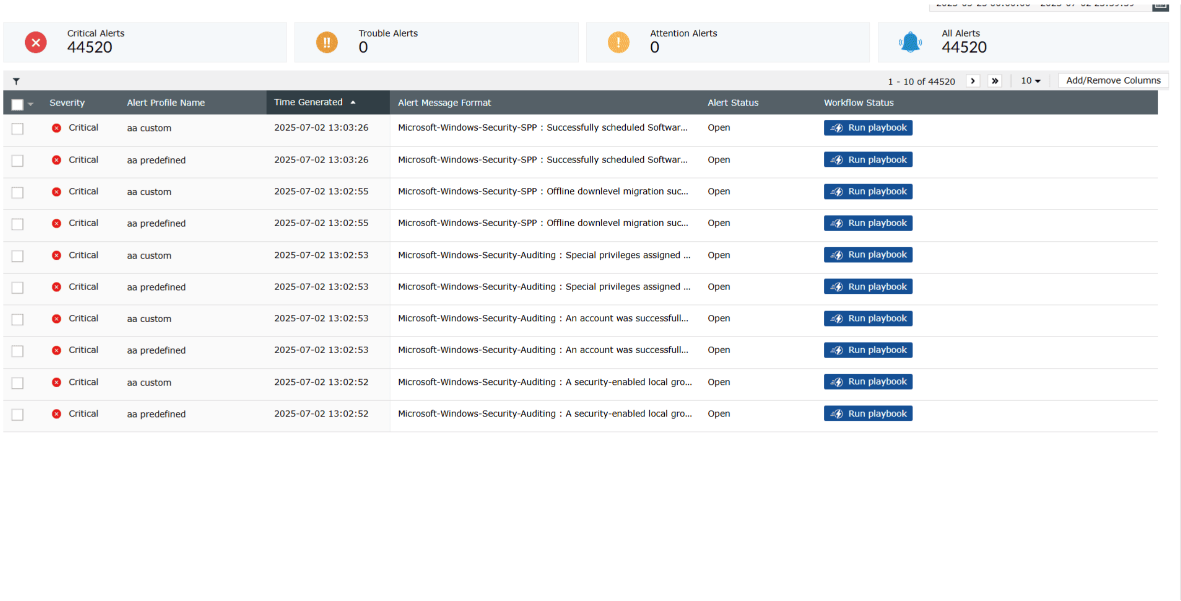
Pre-requisites to update playbook credentials:

- You can automate playbooks on Windows, Linux, and Cisco devices. But in order to perform this action, you must have administrative privileges.
- The credentials of these devices must also be updated in Log360 for seamless execution of the playbooks.

Accessing playbook credentials

1. In the product console, navigate to the Alerts tab. Click on the More tools icon present at the top-right corner of the page as highlighted in the below image.

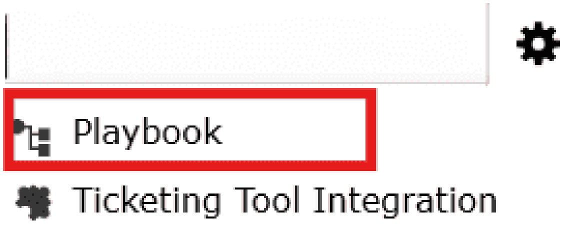




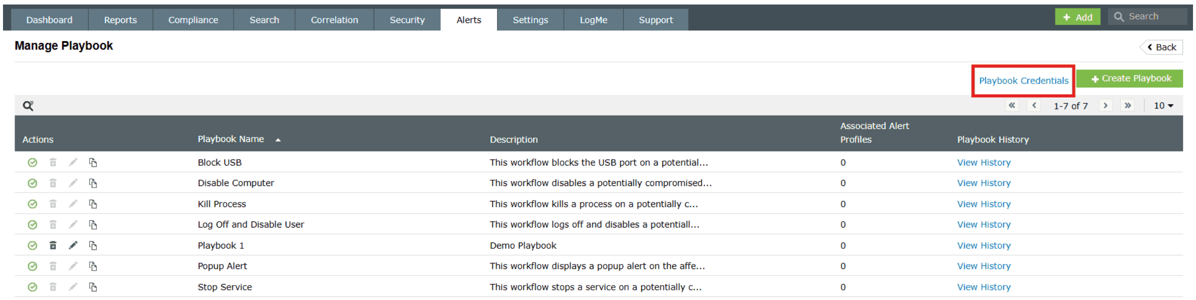
Severity	Alert Profile Name	Time Generated	Alert Message Format	Alert Status	Workflow Status
Critical	aa custom	2025-07-02 13:03:26	Microsoft-Windows-Security-SPP : Successfully scheduled Softwar...	Open	Run playbook
Critical	aa predefined	2025-07-02 13:03:26	Microsoft-Windows-Security-SPP : Successfully scheduled Softwar...	Open	Run playbook
Critical	aa custom	2025-07-02 13:02:55	Microsoft-Windows-Security-SPP : Offline downlevel migration suc...	Open	Run playbook
Critical	aa predefined	2025-07-02 13:02:55	Microsoft-Windows-Security-SPP : Offline downlevel migration suc...	Open	Run playbook
Critical	aa custom	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : Special privileges assigned ...	Open	Run playbook
Critical	aa predefined	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : Special privileges assigned ...	Open	Run playbook
Critical	aa custom	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : An account was successfull...	Open	Run playbook
Critical	aa predefined	2025-07-02 13:02:53	Microsoft-Windows-Security-Auditing : An account was successfull...	Open	Run playbook
Critical	aa custom	2025-07-02 13:02:52	Microsoft-Windows-Security-Auditing : A security-enabled local gro...	Open	Run playbook
Critical	aa predefined	2025-07-02 13:02:52	Microsoft-Windows-Security-Auditing : A security-enabled local gro...	Open	Run playbook

Image 1: More tools icon present in the Alerts tab

2. Click on Playbook to open the Manage Playbook page.



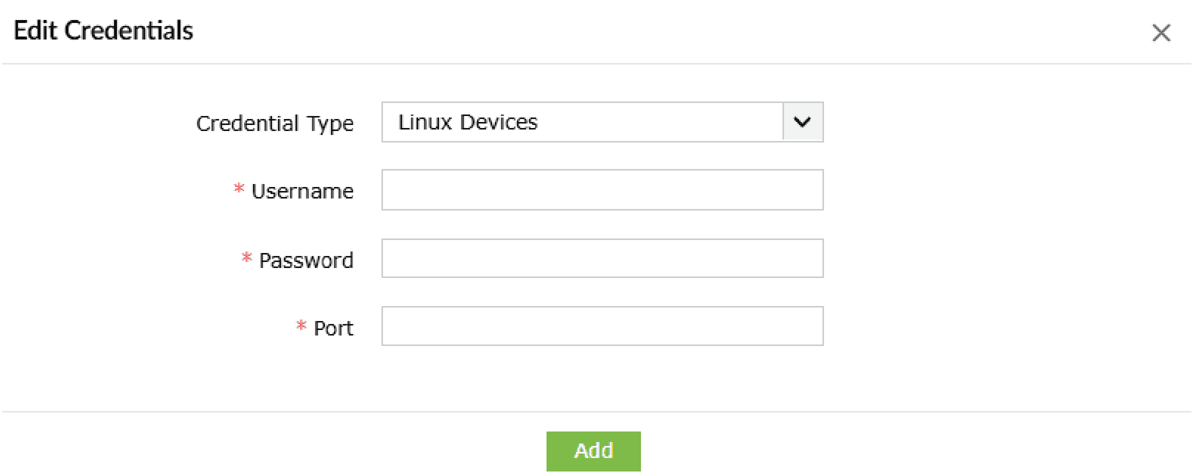
3. Click on the Playbook Credentials present in the Manage Playbook page.



Actions	Playbook Name	Description	Associated Alert Profiles	Playbook History
	Block USB	This workflow blocks the USB port on a potential...	0	View History
	Disable Computer	This workflow disables a potentially compromised...	0	View History
	Kill Process	This workflow kills a process on a potentially c...	0	View History
	Log Off and Disable User	This workflow logs off and disables a potentiall...	0	View History
	Playbook 1	Demo Playbook	0	View History
	Popup Alert	This workflow displays a popup alert on the affe...	0	View History
	Stop Service	This workflow stops a service on a potentially c...	0	View History

Image 2: Playbook credentials in the Alerts tab

4. When you click on Playbook Credentials, a pop-up appears to Edit Credentials.



Edit Credentials

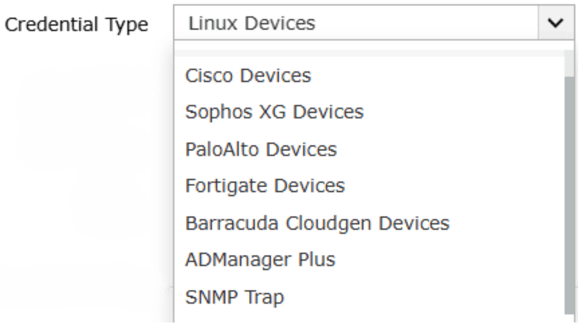
Credential Type: Linux Devices

* Username

* Password

* Port

5. Based on the device types, choose the Credential Type from the drop-down as shown below.



Credential Type: Linux Devices

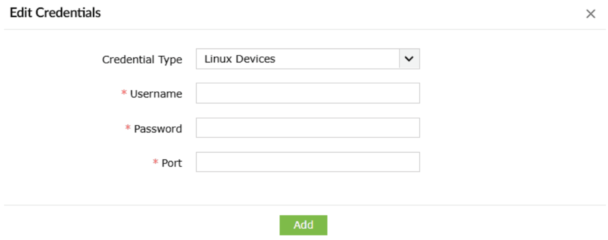
Continue reading to understand the step-by-step device specific guide to update playbook credentials.

To automate playbooks in Windows devices:

If the Windows devices have already been added to the product, playbooks can be executed by using the device credentials or the domain credentials of the devices. So, you need not manually update credentials for Windows devices.

To automate playbooks in Linux devices:

You can configure a set of common credentials for executing playbooks on all Linux devices.



Edit Credentials

Credential Type: Linux Devices

* Username

* Password

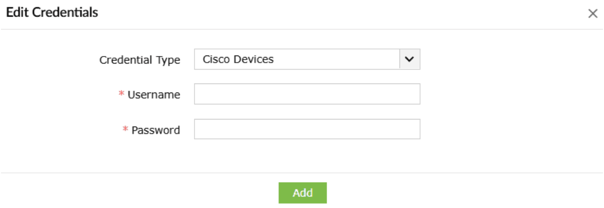
* Port

1. Enter the Username, Password, and Port number.
2. Click on Add to store and use these credentials to execute playbooks on all Linux devices.

To automate playbooks in Cisco devices

You must configure the REST API agent in the Cisco firewall to execute playbooks by following the steps given in this link. (The Cisco REST API supported versions are listed here).

You can configure a set of common credentials for executing playbooks in all Cisco devices as elaborated below:



Edit Credentials

Credential Type: Cisco Devices

* Username

* Password

Add

1. Enter the Username and Password.

2. Click on Add to store and use these credentials to execute playbooks on all Cisco devices.

If the common credentials do not work for certain Cisco Devices

You need to configure the credentials for those devices by following the steps given below:

1. In the product console, navigate to Settings → Devices.

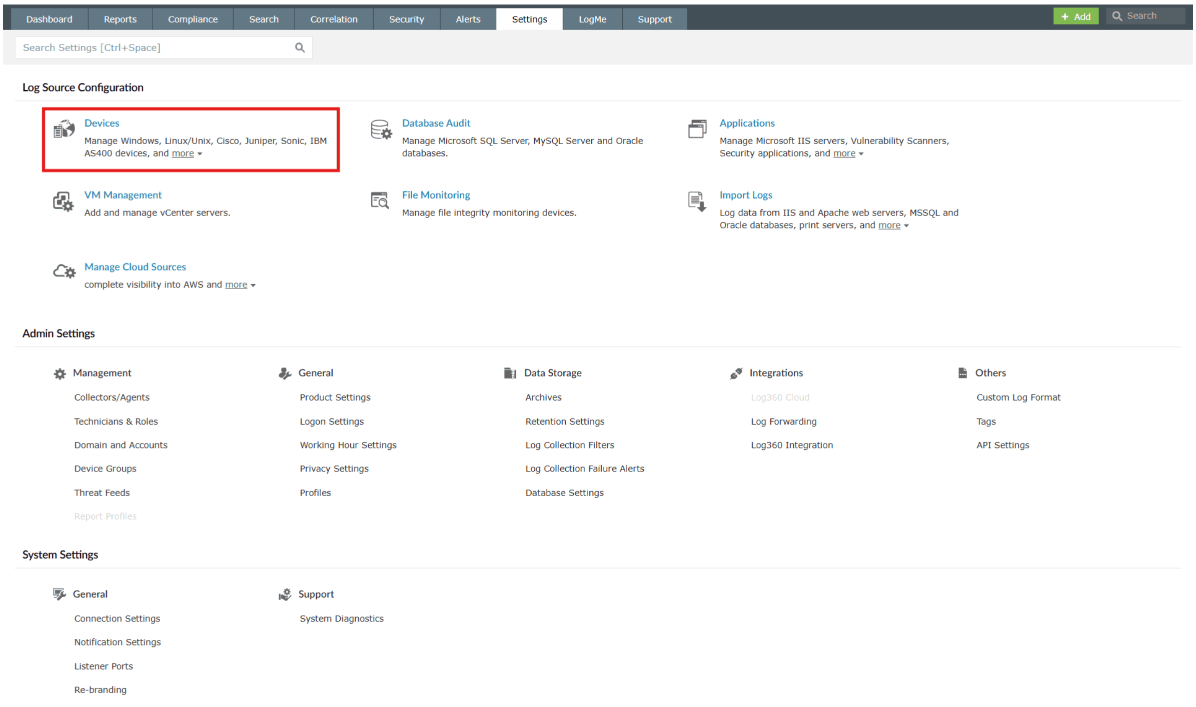
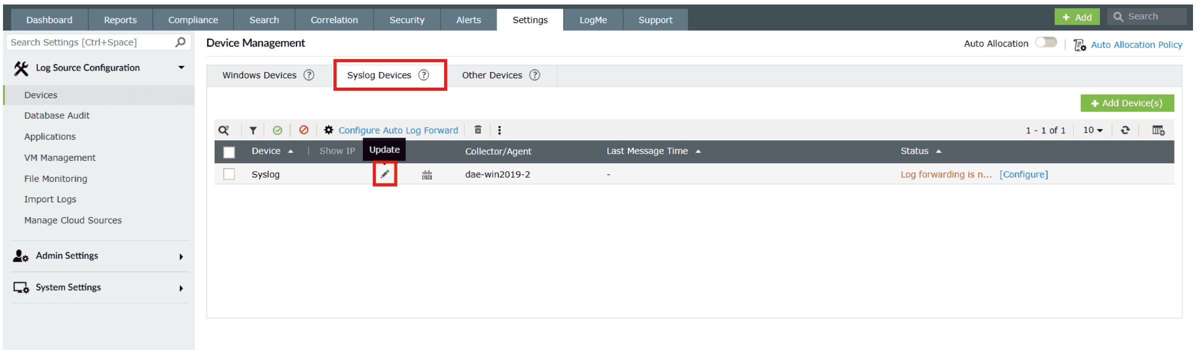


Image 3: Device settings via the Settings tab

2. Go to the Syslog Devices tab and hover your mouse pointer near the device on which you want to execute playbooks and click on the Edit icon.



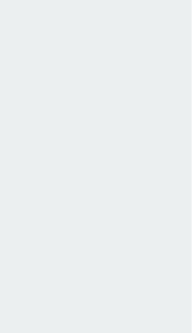
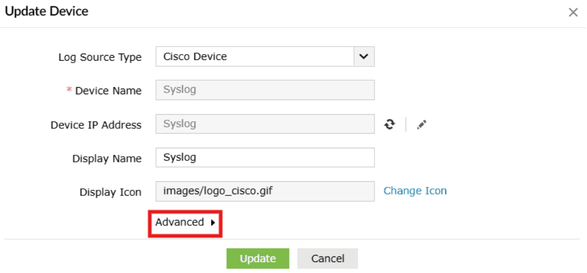


Image 4: Update Syslog device settings via the Settings tab

3. In the Update Device pop-up menu, click on Advanced.



Update Device ×

Log Source Type: Cisco Device

* Device Name: Syslog

Device IP Address: Syslog

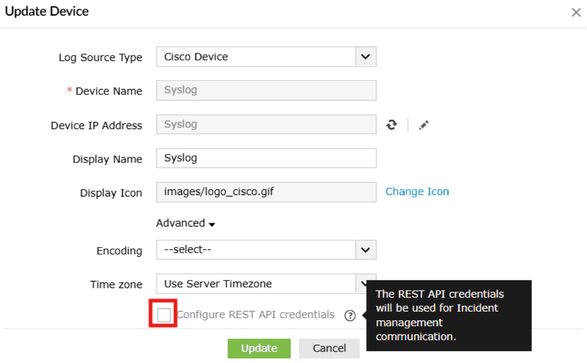
Display Name: Syslog

Display Icon: images/logo_cisco.gif Change Icon

Advanced ▸

Update Cancel

4. Select the Configure REST API Credentials check box.



Update Device ×

Log Source Type: Cisco Device

* Device Name: Syslog

Device IP Address: Syslog

Display Name: Syslog

Display Icon: images/logo_cisco.gif Change Icon

Advanced ▾

Encoding: --select--

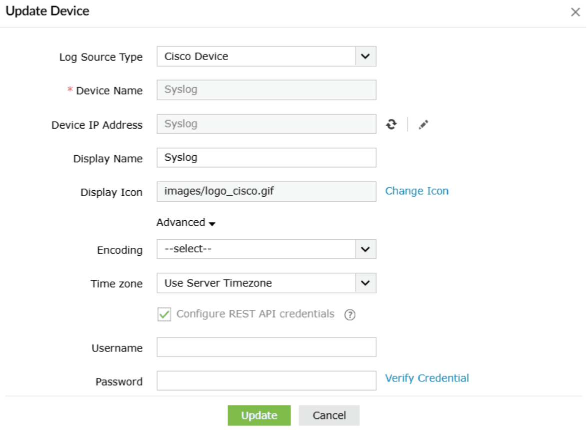
Time zone: Use Server Timezone

□ Configure REST API credentials ⓘ

The REST API credentials will be used for Incident management communication.

Update Cancel

5. Enter a Username and Password and click on Verify Credential to send a REST API call to the Cisco device to verify if the credentials are valid. Once the verification is complete, click on Update to store and use the specified credentials for executing playbooks.



Update Device ×

Log Source Type: Cisco Device

* Device Name: Syslog

Device IP Address: Syslog

Display Name: Syslog

Display Icon: images/logo_cisco.gif Change Icon

Advanced ▾

Encoding: --select--

Time zone: Use Server Timezone

☑ Configure REST API credentials ⓘ

Username:

Password: Verify Credential

Update Cancel

To automate workflows in Fortigate devices

In order to generate an API token to execute playbooks on Fortigate devices, you need to create a new REST API Admin on your device using the steps given below:

Phase 1: Create Administrator profile

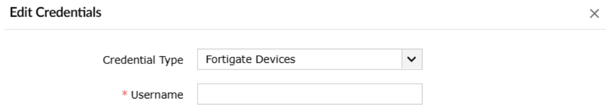
1. Navigate to System from the sections listed on the left in the dashboard.
2. Click on the Admin Profiles under the System section.
3. Click the Create icon to start creating a new admin profile.
4. You will see the New Admin Profile window open.
5. Enter an appropriate name for your admin profile.
6. Select access control permissions for different functionalities between None, Read, Read/Write or Custom.
7. Select Read/Write for both Policy and Address options under Firewall Option.
8. Click OK to create your new admin profile

Phase 2: Create a REST API Admin and generate an API key

1. Navigate to System from the sections listed on the left in the dashboard.
2. Select Administrators under the System section.
3. Click on the Create New icon.
4. Select the REST API Admin option.
5. You will see the New REST API Admin window open.
6. Enter an appropriate username for your REST API admin profile.
7. Select your previously created Administrator Profile from the drop-down menu.
8. Click on OK to confirm your New REST API Admin .
9. Once you are done with this process, the system will automatically generate a new API key, which will be displayed only once.
10. Copy the generated API key before shutting it down.

> ⓘ NOTE
>
> In case you lose your newly generated API key, you can go back to the Administrator section and click on the Regenerate icon.

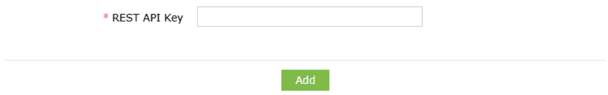
After this process, You can configure a set of common credentials for executing playbooks in all Fortigate devices by following the steps given below:



Edit Credentials

Credential Type: Fortigate Devices

* Username:



1. Enter the Username and the REST API Key.
2. Click on Add to store and use these credentials to execute playbooks on all Fortigate devices.

To automate playbooks in PaloAlto devices

Pre-requisites:
To execute playbooks successfully, API access should be enabled by following the steps given below.
Phase 1:

1. Choose an Admin Role profile.
2. Navigate to Device → Admin Roles and either pick an existing role or set up a new one.

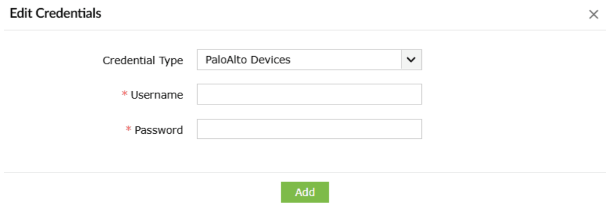
Phase 2:

1. Define the permissions available for the selected admin role.
2. Open the XML API section.
3. Turn on or off specific XML API capabilities like Report, Log, and Configuration.
4. Click OK to apply and save your changes.

Phase 3:
Assign the configured admin role to the desired administrator account.
Please note that the required permissions for the user under XML API are:

- Configuration
- Operational Requests
- Commit

You can configure a set of common credentials for executing playbooks in all PaloAlto devices by following the steps given below:

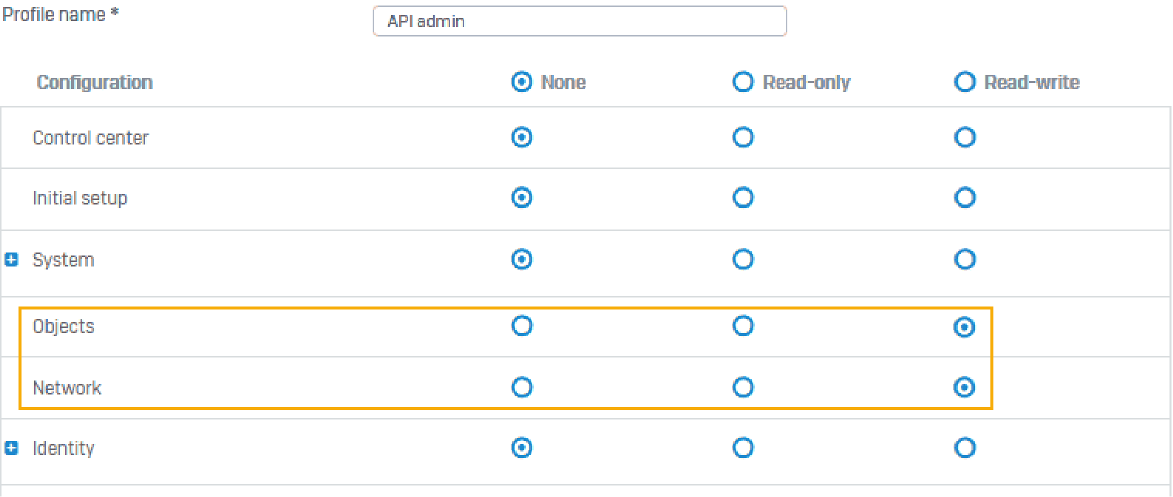

Credential Type: PaloAlto Devices

1. Enter the Username and Password.
2. Click on Add to store and use these credentials to execute playbooks on all PaloAlto devices.

To automate playbooks in SophosXG devices

You must configure the encrypted password to execute playbooks on SophosXG devices. You can generate the encrypted password using the steps given below:
Phase 1: Create an administrator profile
Log in to your Sophos application and create an administrator profile with read-write permission for objects and network

1. Go to Profiles > Device access and create an administrator profile with specific rights.
2. Click Save.

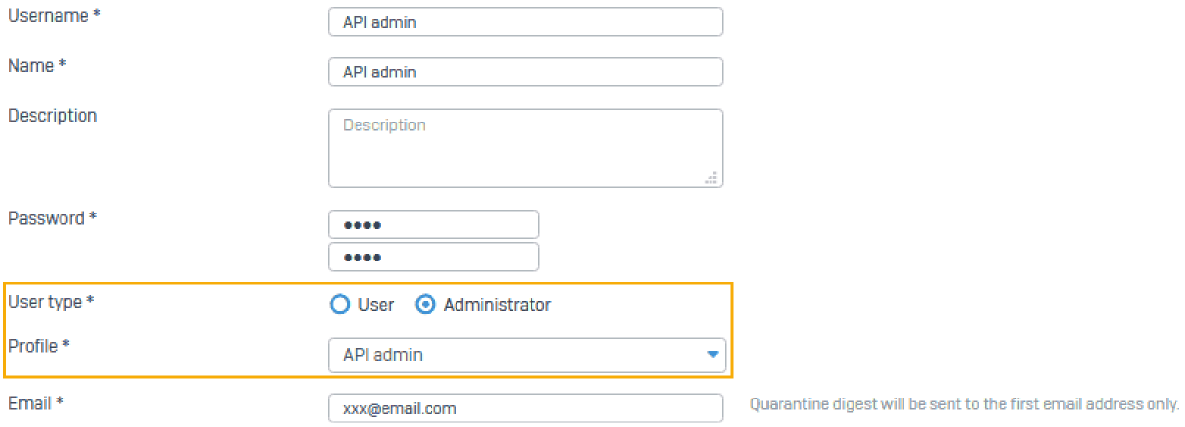


Profile name *	API admin

Configuration	● None	○ Read-only	○ Read-write
Control center	●	○	○
Initial setup	●	○	○
⊞ System	●	○	○
Objects	○	○	●
Network	○	○	●
⊞ Identity	●	○	○

Phase 2: Create an administrator

1. Create a user and add the administrator profile.
2. When you add a user with the API administrator profile, you can limit the administrator's rights based on the profile. Alternatively, you can use an existing administrator account.
3. Go to Authentication > Users and click Add.
4. Set User type to Administrator.
5. Select the API administrator profile created in step 1.
6. To allow access for a specific time, select the Access time.
7. To allow access only from specific IP addresses, select an option for Login restriction for device access.
8. Click Save.



Username *	API admin
Name *	API admin
Description	Description
Password *	•••• ••••
User type *	○ User ● Administrator
Profile *	API admin
Email *	xxx@email.com

Quarantine digest will be sent to the first email address only.

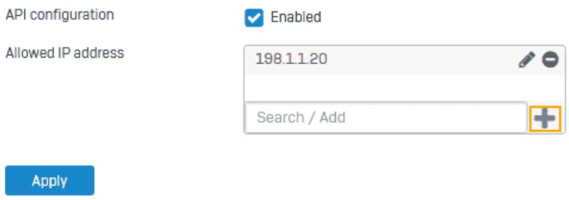
Phase 3: Allow API access

Turn on API configuration and allow API access from the administrator's IP address:

1. Go to Backup and firmware > API.
2. Select API configuration.

3. For Allowed IP address, enter the IP address from which you'll make the API request and click the add icon.

4. Click Apply.



API configuration ☑ Enabled

Allowed IP address: 198.1.1.20

Phase 4: To generate encrypted password

1. Log in to advanced shell in the firewall.

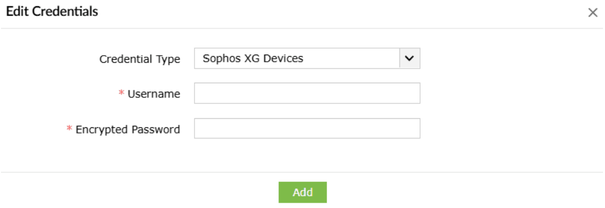
2. Execute the following command:

```
-aes-128-cbc-tool -k Th1s1Ss1mPlygR8API -t 1 -s <password>-
```

3. Copy the password and use it in the API configuration.

> NOTE
>
> The product will continue to support Sophos XG devices up to SFOS v19.0.
> If you wish to integrate with newer versions of Sophos XG, please contact us. We can make the necessary adjustments in the database to accommodate the new API credentials mechanism.
> All Sophos-related actions will continue to be supported.

After generating the encrypted password, you can configure a set of common credentials for executing playbooks in all SophosXG devices by following the steps given below:



Edit Credentials

Credential Type: Sophos XG Devices

* Username

* Encrypted Password

1. Enter the Username and Encrypted Password.

2. Click on Add to store and use these credentials to execute playbooks on all SophosXG devices.

To automate playbooks in Barracuda CloudGen devices

In order to execute playbooks in Barracuda CloudGen devices, you need to create an X-API Token using the steps given below:

Phase 1: Enable the REST API for HTTPS

1. Navigate to CONFIGURATION > Configuration Tree > Box > Infrastructure Services > REST API Service.

2. Click the Lock button to enable editing.

3. In the HTTP interface section, enable the HTTPS interface option.

4. Specify the port number you'd like to use for API requests in the HTTPS Port field.

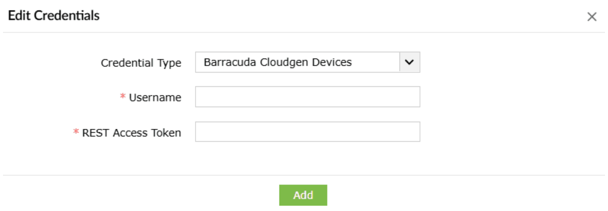
5. (Optional) To allow API requests through management IPs rather than the loopback address, enable the Bind to Management IPs setting.
6. Click New Key to generate a private key of your preferred key length, or import your existing key.
7. Click Ex/Import to either generate a self-signed certificate or upload an already existing one.

> NOTE
>
> Ensure that the certificate's common name matches the URI of your API request. For instance, if you're sending a request to https://CGF1.example:8443, the common name in the certificate should be CGF1.example.

Phase 2: Create an administrator profile for REST API authentication.
To authenticate with the REST API, a user account with the required privileges must exist, either in the Control Center for centrally managed firewalls or directly on the individual firewall for standalone setups. This user must hold the Manager role in both scenarios.
If you need a read-only user, you can duplicate the Observer role under the Control Center's Administrative Roles section, enable the Access to REST API option, and then create a new user under CC-Admin with this custom role assigned.
Phase 3: Create an X-API Token for authentication.

1. Navigate to CONFIGURATION > Configuration Tree > Box > Infrastructure Services > REST API Service.
2. Select Lock to begin editing.
3. From the left-hand panel, choose Access Tokens.
4. Click the + icon in the Access Tokens area.
5. Provide a name for the new token and click OK to proceed.
6. In the window that appears, click Generate New Token.
7. Specify the Admin username that will be used for authentication.
8. Set the validity period in days under the Time to live field.
9. Click OK to finalize and create the token.

After finishing the process, you can configure a set of common credentials for executing playbooks in all Barracuda CloudGen devices by following the steps given below:



Edit Credentials

Credential Type: Barracuda Cloudgen Devices

* Username:

* REST Access Token:

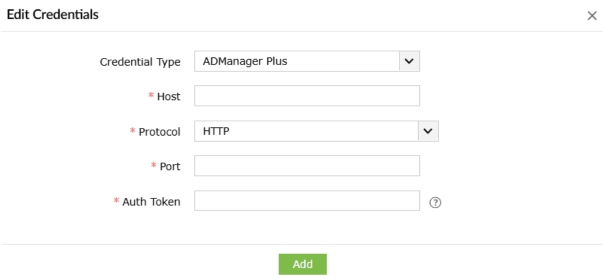
1. Enter the Username along with the generated REST Access Token.
2. Click on Add to store and use these credentials to execute playbooks in all Barracuda CloudGen devices.

Automating playbooks in ADManager Plus

ADManager Plus , an IGA solution with hybrid Active Directory management, reporting, and automation capabilities, must be integrated with Log360 for the successful execution of response playbooks. The list of actions that can be added to the playbook are called playbook blocks. These actions include:

- Enabling, disabling, updating, and deleting a user
- Enabling, disabling, and deleting a computer
- Resetting a user's password
- Adding to, and removing users from a group

Only after the integration is complete can any of these actions be carried out.
You can set up an integration in the product to execute actions via ADManager Plus. Here are the steps:



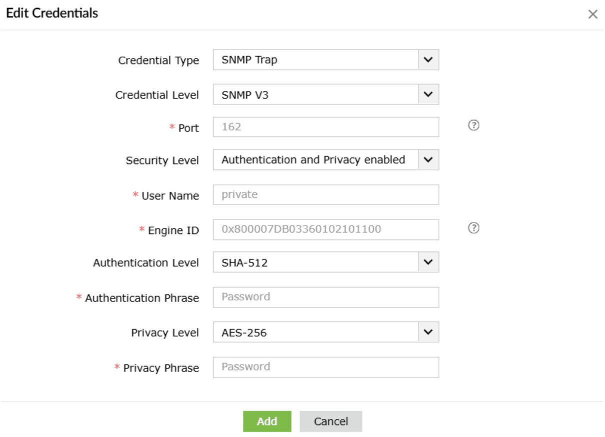
Edit Credentials

Credential Type	ADManager Plus
* Host	
* Protocol	HTTP
* Port	
* Auth Token	

1. After selecting the credential type as ADManager Plus, fill in the required details about the Host, Protocol, Port and Auth Token.
2. Click on Add, to integrate ADManager Plus with the product.

Automating playbooks in SNMP TRAP

To automate all SNMP Trap playbooks, you can configure a common credential by following these steps:



Edit Credentials

Credential Type	SNMP Trap
Credential Level	SNMP V3
* Port	162
Security Level	Authentication and Privacy enabled
* User Name	private
* Engine ID	0x800007DB03360102101100
Authentication Level	SHA-512
* Authentication Phrase	Password
Privacy Level	AES-256
* Privacy Phrase	Password

1. After choosing SNMP Trap as the credential type, enter the SNMP credential.
2. Click Add to save. This credential will now be used to execute all SNMP Trap playbooks.

ⓘ NOTE

Refer to the port management page for details on how to update credentials.

Read also

This document elaborated on a simple and step-by-step guide on how to update playbook credentials. If you're building workflows, explore how to create custom playbooks and assign device actions.

- Creating playbook
- Manage playbooks

4.3.3. Ticketing Tool configuration

Last updated on: September 12, 2025

With EventLog Analyzer, you can efficiently manage security incidents by raising tickets and assigning them to administrators for alerts that are generated. You can easily manage the incident within the EventLog Analyzer console itself or use an external help desk software for raising tickets. Under Alert Configurations, click on ticketing tool integration to configure an external help desk - ServiceNow, ManageEngine ServiceDesk Plus, ManageEngine ServiceDesk Plus On-Demand, ManageEngine ServiceDeskPlus MSP, ManageEngine AlarmsOne, Jira Service Desk, Jira Service Desk On-Demand, Zendesk, Freshservice, Kayako, or BMC Remedy Service Desk.

Manage Ticketing Tool Configuration

To configure incident management with ticketing tools, click on ticketing tool integration under Alert Configuration. From the Ticketing Tool drop-down list, select the ticketing tool that you want to configure EventLog Analyzer with. Then, follow the following steps based on the ticketing tool used.

For ManageEngine ServiceDesk Plus On-Demand:

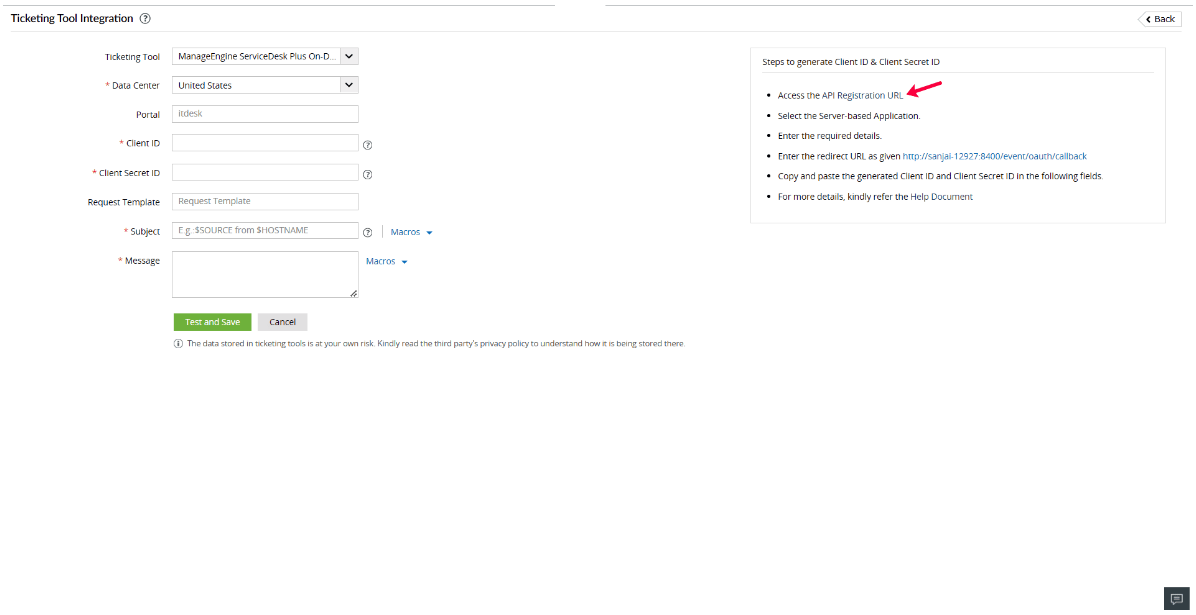
> Note
>
> Only users with permissions to view and edit requests can proceed with the configuration.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select ManageEngine ServiceDesk Plus On-Demand.

1. Choose the Data Center where your ServiceDesk Plus account is hosted. Kindly refer to the table below to find the corresponding Data Center for your ServiceDesk Plus account.

ServiceDesk Plus URL	Region	Data Center to be selected
https://sdpondemand.manageengine.com	United States	US
https://sdpondemand.manageengine.eu	Europe	EU
https://sdpondemand.manageengine.in	India	IN
https://servicedeskplus.cn	China	CN
https://servicedeskplus.net.au	Australia	AU

ServiceDesk Plus URL	Region	Data Center to be selected
https://servicedeskplus.jp	Japan	JP
https://servicedeskplus.ca	Canada	CA
https://servicedeskplus.uk	United Kingdom	UK
https://servicedeskplus.sa	Saudi Arabia	SA



Ticketing Tool Integration

Ticketing Tool	ManageEngine ServiceDesk Plus On-D...
* Data Center	United States
Portal	itdesk
* Client ID	
* Client Secret ID	
Request Template	Request Template
* Subject	E.g.:$SOURCE from $HOSTNAME
* Message	

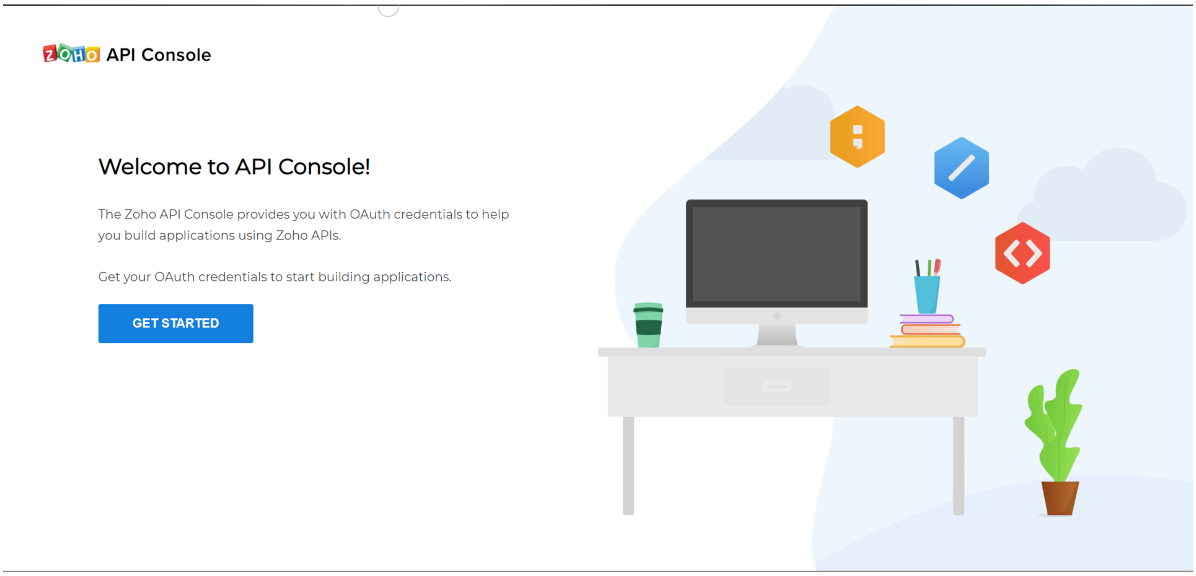
The data stored in ticketing tools is at your own risk. Kindly read the third party's privacy policy to understand how it is being stored there.

Steps to generate Client ID & Client Secret ID

- Access the API Registration URL
- Select the Server-based Application.
- Enter the required details.
- Enter the redirect URL as given http://sanjai-12927:8400/event/oauth/callback
- Copy and paste the generated Client ID and Client Secret ID in the following fields.
- For more details, kindly refer the Help Document

2. Click the API Registration URL to generate the Client ID and Client Secret ID.

3. Once the Zoho API Console is opened, click GET STARTED.

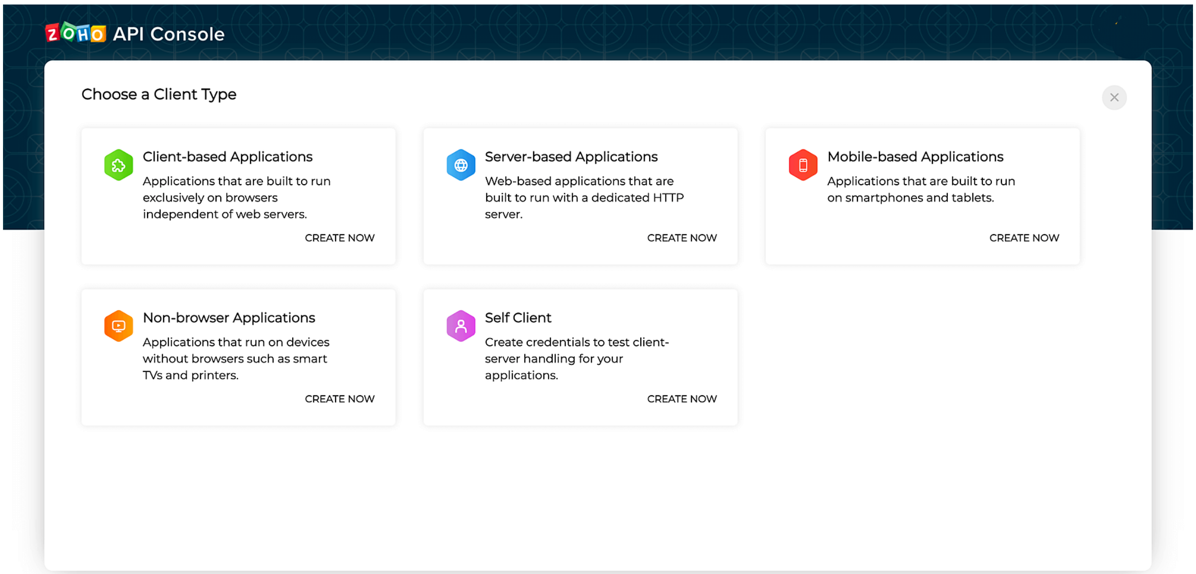


Welcome to API Console!

The Zoho API Console provides you with OAuth credentials to help you build applications using Zoho APIs.

Get your OAuth credentials to start building applications.

4. Select the Server-based Applications tile.



Choose a Client Type

Client-based Applications
Applications that are built to run exclusively on browsers independent of web servers.
CREATE NOW

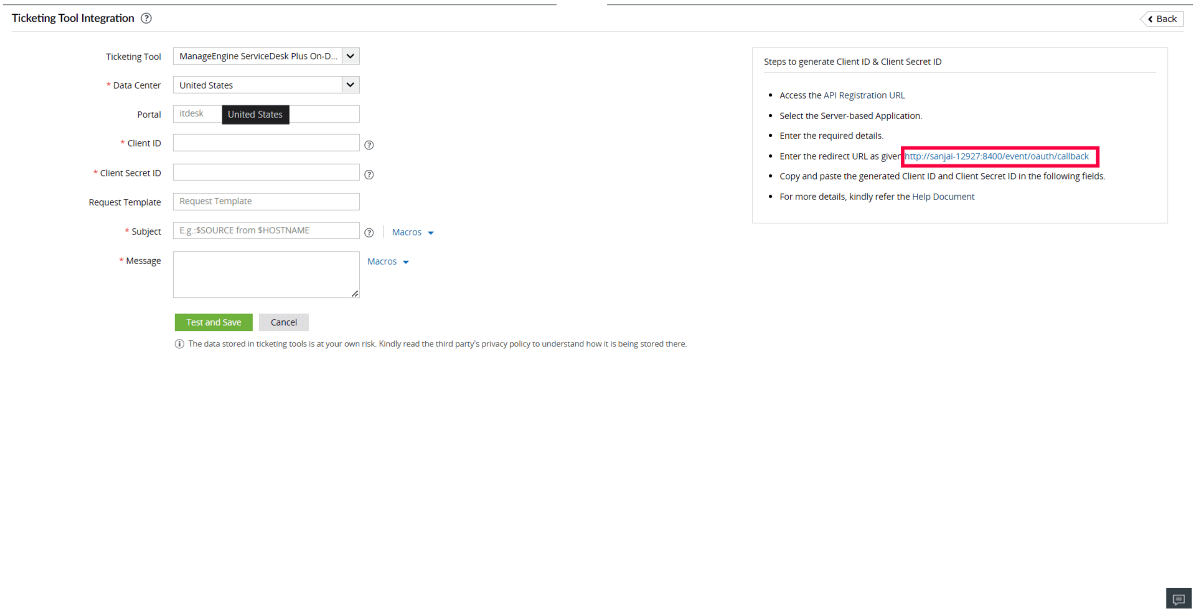
Server-based Applications
Web-based applications that are built to run with a dedicated HTTP server.
CREATE NOW

Mobile-based Applications
Applications that are built to run on smartphones and tablets.
CREATE NOW

Non-browser Applications
Applications that run on devices without browsers such as smart TVs and printers.
CREATE NOW

Self Client
Create credentials to test client-server handling for your applications.
CREATE NOW

5. To create a new client, enter the required details. Enter the redirect URL as given in the EventLog Analyzer console and click Create.



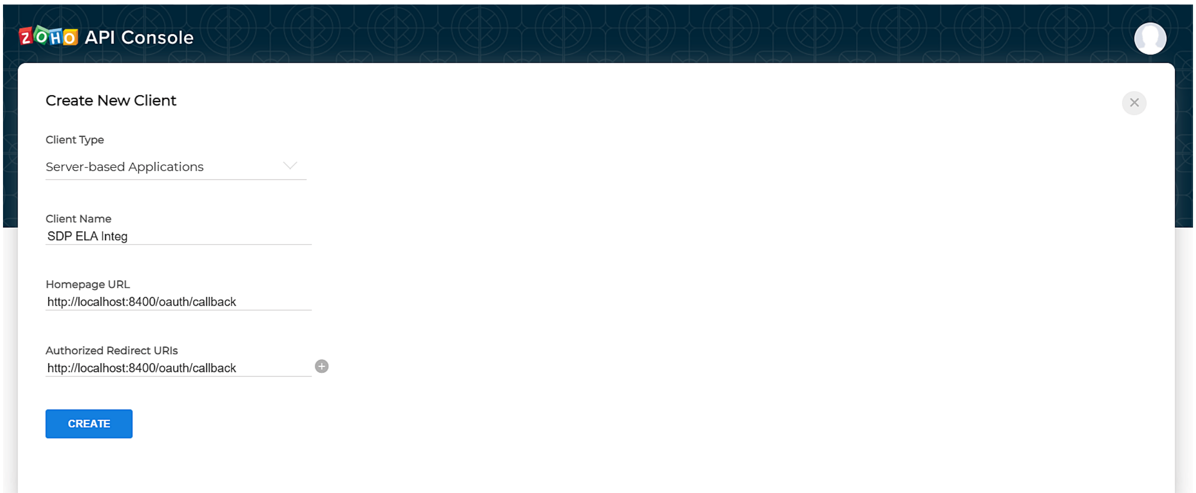
Ticketing Tool Integration ⓘ

Ticketing Tool	ManageEngine ServiceDesk Plus On-D...
* Data Center	United States
Portal	itdesk United States
* Client ID	
* Client Secret ID	
Request Template	Request Template
* Subject	E.g.:$SOURCE from $HOSTNAME
* Message	

ⓘ The data stored in ticketing tools is at your own risk. Kindly read the third party's privacy policy to understand how it is being stored there.

Steps to generate Client ID & Client Secret ID

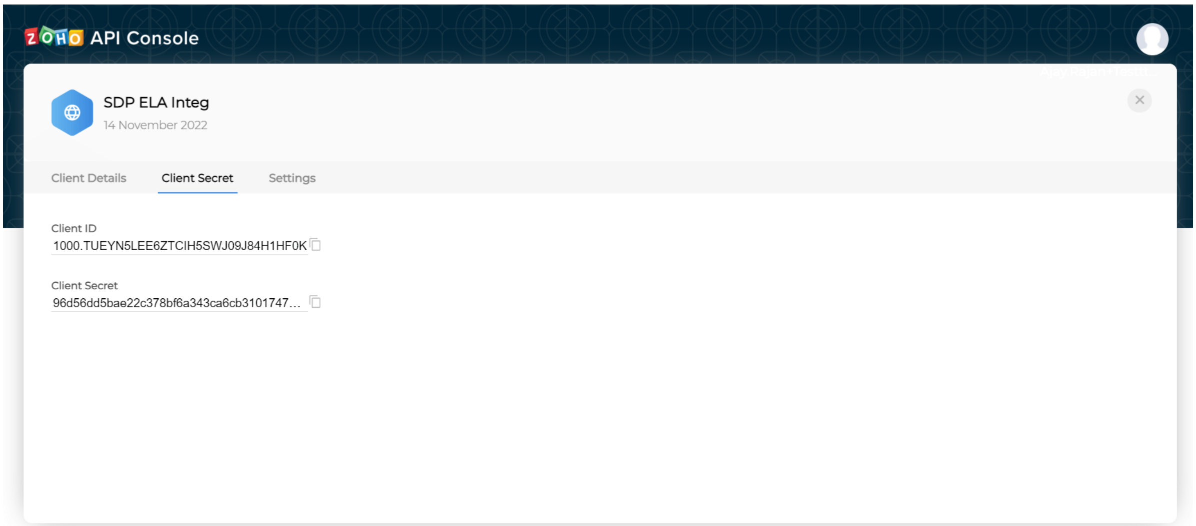
- Access the API Registration URL
- Select the Server-based Application.
- Enter the required details.
- Enter the redirect URL as given http://sanjai-12927:8400/event/oauth/callback
- Copy and paste the generated Client ID and Client Secret ID in the following fields.
- For more details, kindly refer the Help Document



Create New Client

Client Type	Server-based Applications
Client Name	SDP ELA Integ
Homepage URL	http://localhost:8400/oauth/callback
Authorized Redirect URIs	http://localhost:8400/oauth/callback

6. Copy the generated Client ID and Client Secret ID.



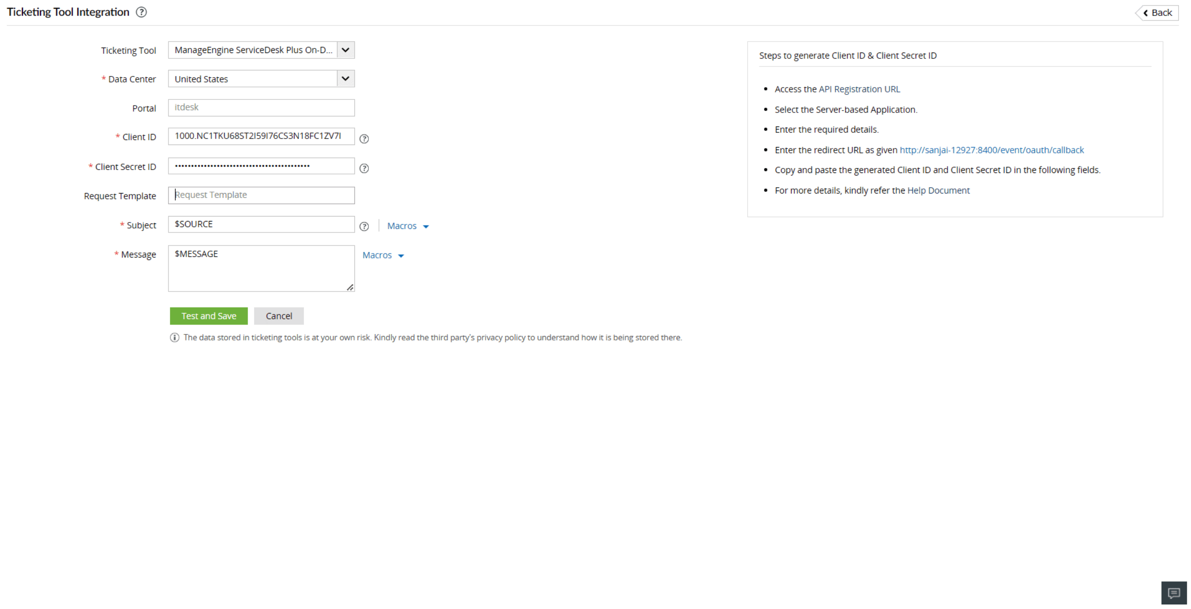
SDP ELA Integ

14 November 2022

Client ID
1000.TUEYN5LEE6ZTCIH5SWJ09J84H1HF0K

Client Secret
96d56dd5bae22c378bf6a343ca6cb3101747...

7. Back in the ELA console, paste the Client ID and Client Secret ID in the corresponding fields.



Ticketing Tool Integration

Ticketing Tool	ManageEngine ServiceDesk Plus On-D...
* Data Center	United States
Portal	itdesk
* Client ID	1000.NC1TKU68ST2I59I76CS3N18FC1ZV7I
* Client Secret ID	••
Request Template	Request Template
* Subject	$SOURCE
* Message	$MESSAGE

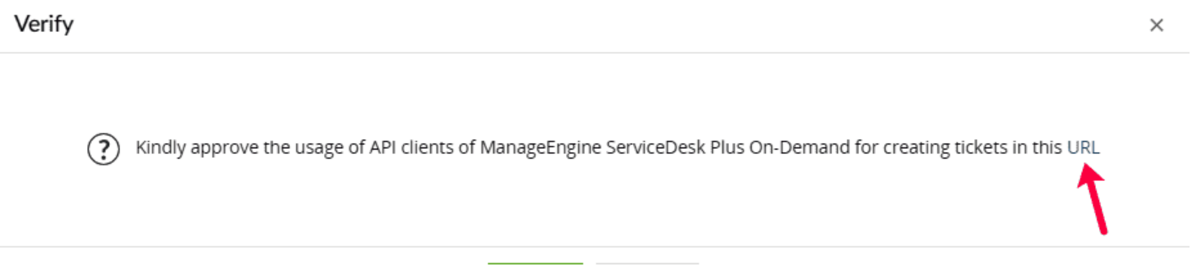
The data stored in ticketing tools is at your own risk. Kindly read the third party's privacy policy to understand how it is being stored there.

Steps to generate Client ID & Client Secret ID

- Access the API Registration URL
- Select the Server-based Application.
- Enter the required details.
- Enter the redirect URL as given http://sanjai-12927:8400/event/oauth/callback
- Copy and paste the generated Client ID and Client Secret ID in the following fields.
- For more details, kindly refer the Help Document

8. Please specify the Request Template you want to use for creating tickets in ServiceDeskPlus OnDemand. Leaving it empty would raise tickets using the Default Template.

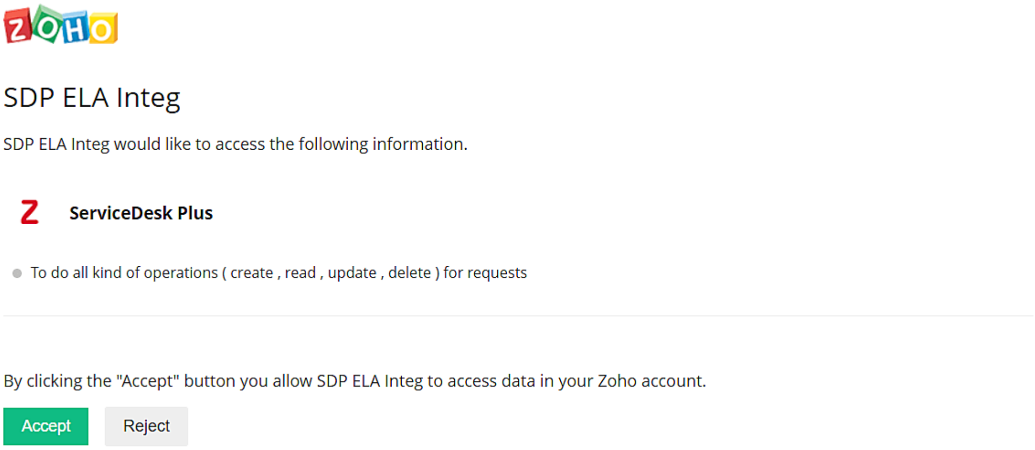
9. Provide the Subject and Message for the alert—these can be selected from a predefined list under Macros or entered manually as per your requirements. Click the Test and Save button to proceed. Upon clicking, a verification popup will appear—click the URL provided to approve the integration with ServiceDesk Plus On-Demand clients.



Verify

Kindly approve the usage of API clients of ManageEngine ServiceDesk Plus On-Demand for creating tickets in this URL

10. Click Accept for API approval.



SDP ELA Integ

SDP ELA Integ would like to access the following information.

ServiceDesk Plus

- To do all kind of operations (create , read , update , delete) for requests

By clicking the "Accept" button you allow SDP ELA Integ to access data in your Zoho account.

11. Click the Verify button in ELA console. The ticketing tool will now be configured successfully.

> ⓘ Note
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For ManageEngine AlarmsOne

> ⓘ Note
>
> Only users with the super admin or the alarm admin role can proceed with the configuration.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select ManageEngine AlarmsOne.

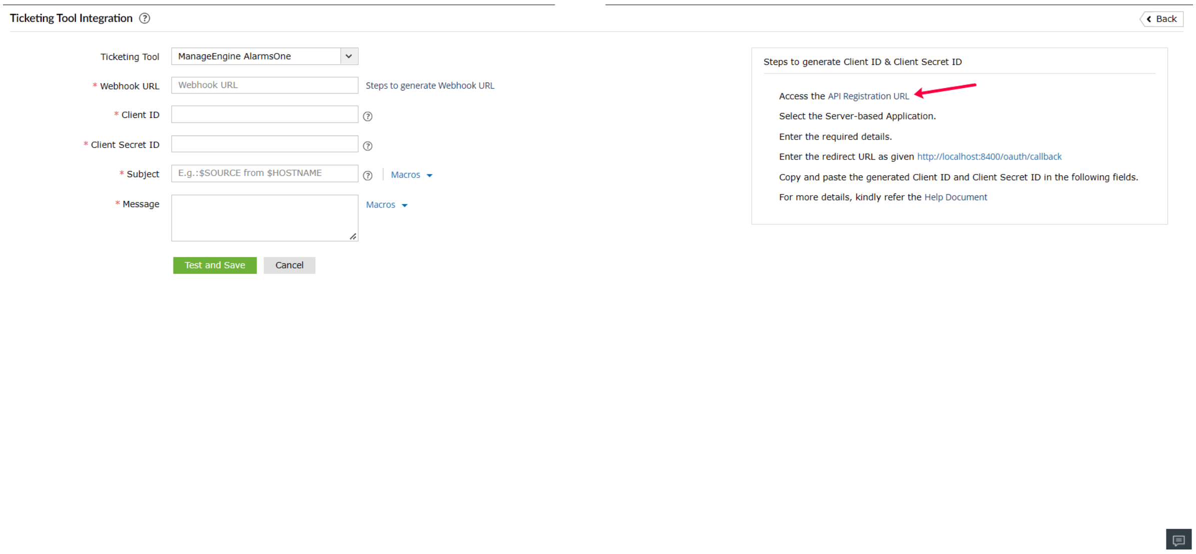
1. Open ManageEngine AlarmsOne and click the Applications icon, then click Applications(+) button in the left panel. From the list displayed, select Custom API Integration.

2. Enter an Application Label and Application Name. If a notification profile is already configured, select it. Click Add. You can also associate a notification profile later.

3. A Webhook URL specific to your custom app is generated.

4. Click API Registration URL in EventLog Analyzer to generate a Client ID and Client Secret ID

4. Click API Registration URL in EventLog Analyzer, to generate a Client ID and Client Secret ID.



Ticketing Tool Integration

Ticketing Tool: ManageEngine AlarmsOne

* Webhook URL: Webhook URL — Steps to generate Webhook URL

* Client ID

* Client Secret ID

* Subject: E.g.:$SOURCE from $HOSTNAME — Macros

* Message — Macros

Test and Save | Cancel

Steps to generate Client ID & Client Secret ID

Access the API Registration URL

Select the Server-based Application.

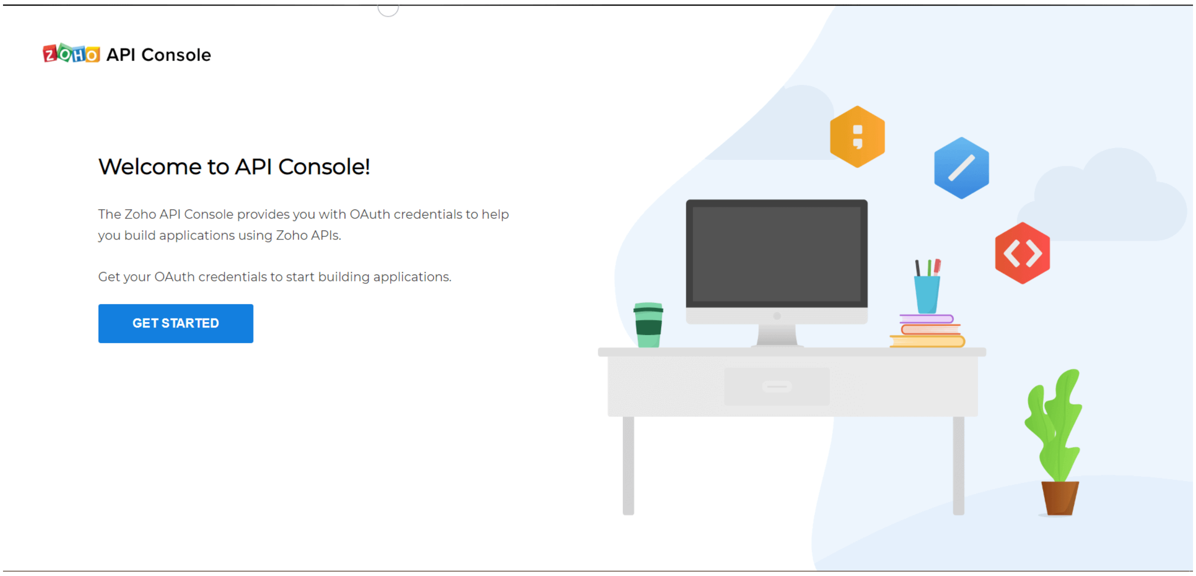
Enter the required details.

Enter the redirect URL as given http://localhost:8400/oauth/callback

Copy and paste the generated Client ID and Client Secret ID in the following fields.

For more details, kindly refer the Help Document

5. Once the Zoho API Console is opened, click GET STARTED.



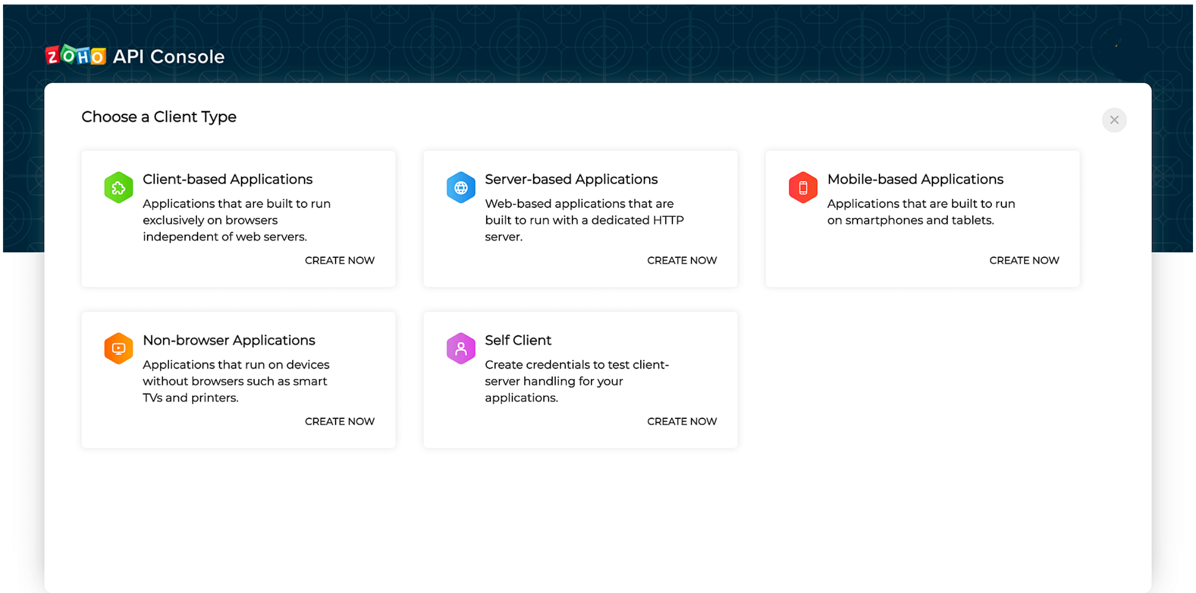
API Console

Welcome to API Console!

The Zoho API Console provides you with OAuth credentials to help you build applications using Zoho APIs.

Get your OAuth credentials to start building applications.

6. Select the Server-based Applications tile.



API Console

Choose a Client Type

Client-based Applications
Applications that are built to run exclusively on browsers independent of web servers.
CREATE NOW

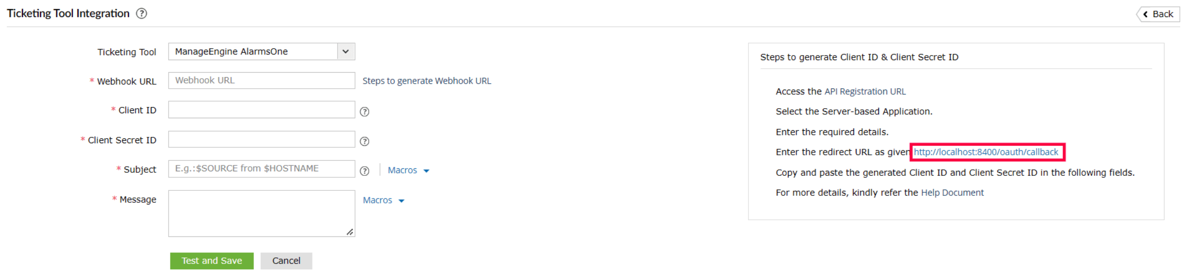
Server-based Applications
Web-based applications that are built to run with a dedicated HTTP server.
CREATE NOW

Mobile-based Applications
Applications that are built to run on smartphones and tablets.
CREATE NOW

Non-browser Applications
Applications that run on devices without browsers such as smart TVs and printers.
CREATE NOW

Self Client
Create credentials to test client-server handling for your applications.
CREATE NOW

7. To create a new client, enter the required details. Enter the redirect URL as given in the EventLog Analyzer console and click Create.



Ticketing Tool Integration

Ticketing Tool: ManageEngine AlarmsOne

* Webhook URL: Webhook URL — Steps to generate Webhook URL

* Client ID:

* Client Secret ID:

* Subject: E.g.:$SOURCE from $HOSTNAME

* Message:

Steps to generate Client ID & Client Secret ID

Access the API Registration URL

Select the Server-based Application.

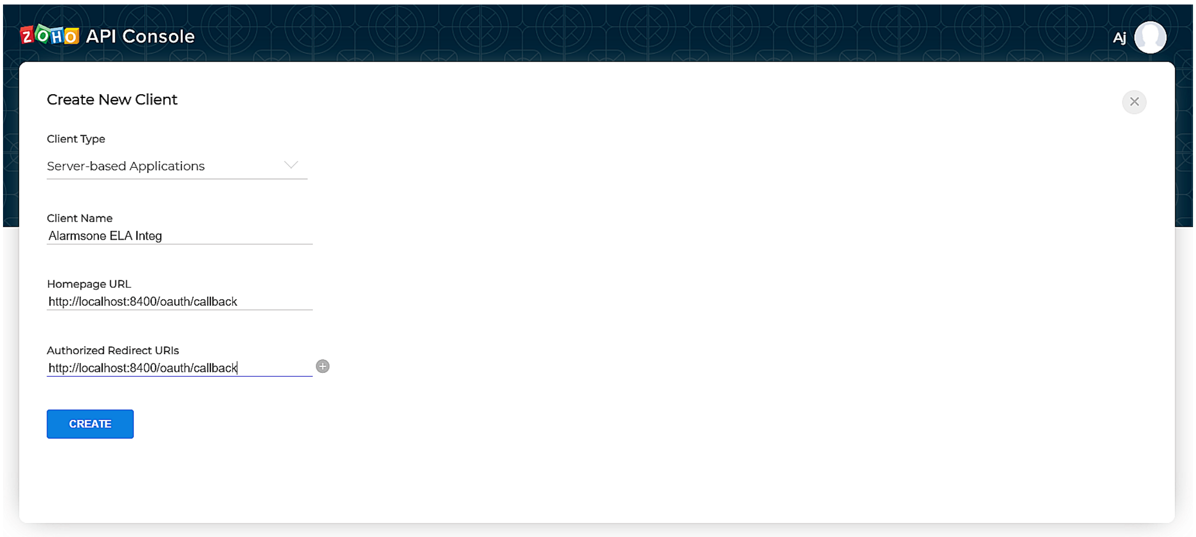
Enter the required details.

Enter the redirect URL as given http://localhost:8400/oauth/callback

Copy and paste the generated Client ID and Client Secret ID in the following fields.

For more details, kindly refer the Help Document

8. Copy the generated Client ID and Client Secret ID.



API Console

Create New Client

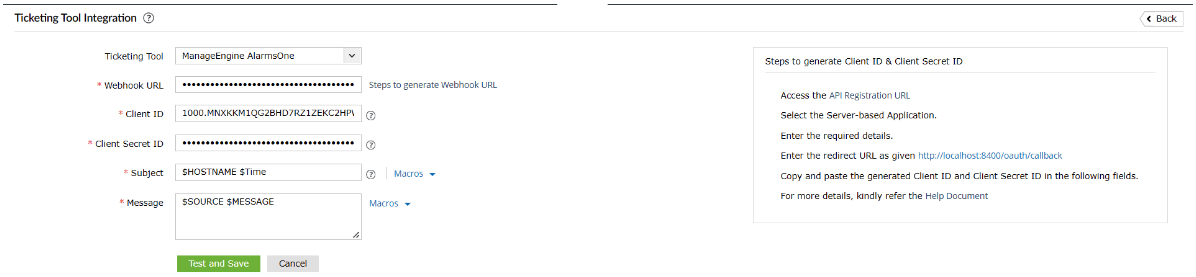
Client Type: Server-based Applications

Client Name: Alarmsone ELA Integ

Homepage URL: http://localhost:8400/oauth/callback

Authorized Redirect URIs: http://localhost:8400/oauth/callback

9. Back in the ELA console, paste the Webhooks URL, Client ID, and Client Secret ID in the required fields.



Ticketing Tool Integration

Ticketing Tool: ManageEngine AlarmsOne

* Webhook URL: •••••••••••••••••••••••••••••••••••••• — Steps to generate Webhook URL

* Client ID: 1000.MNXKKM1QG2BHD7RZ1ZEKC2HP\

* Client Secret ID: ••••••••••••••••••••••••••••••••••••••

* Subject: $HOSTNAME $Time

* Message: $SOURCE $MESSAGE

Steps to generate Client ID & Client Secret ID

Access the API Registration URL

Select the Server-based Application.

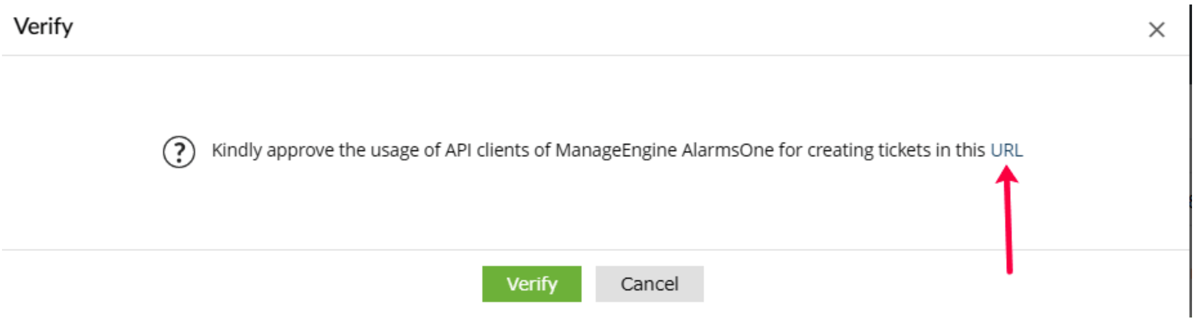
Enter the required details.

Enter the redirect URL as given http://localhost:8400/oauth/callback

Copy and paste the generated Client ID and Client Secret ID in the following fields.

For more details, kindly refer the Help Document

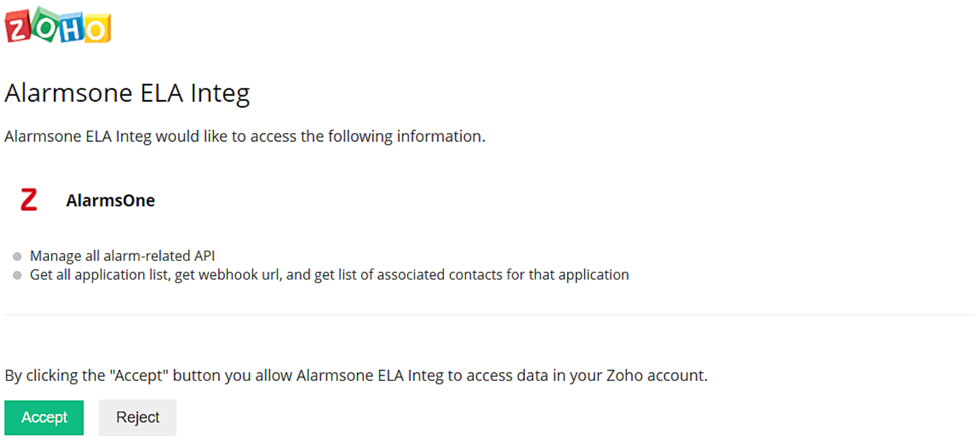
10. Enter the Subject and the Message for the alert. You can select them from the predefined list available under Macros or type your own. Click the Test and Save button. On clicking the Test and Save button, a verify popup will be displayed. Click the URL to approve the usage of the clients of ManageEngine AlarmsOne.



Verify

Kindly approve the usage of API clients of ManageEngine AlarmsOne for creating tickets in this URL

11. Click Accept for API approval.



Alarmsone ELA Integ

Alarmsone ELA Integ would like to access the following information.

AlarmsOne

- Manage all alarm-related API
- Get all application list, get webhook url, and get list of associated contacts for that application

By clicking the "Accept" button you allow Alarmsone ELA Integ to access data in your Zoho account.

Click Verify button in ELA. The ticketing tool will now be configured successfully.

Note

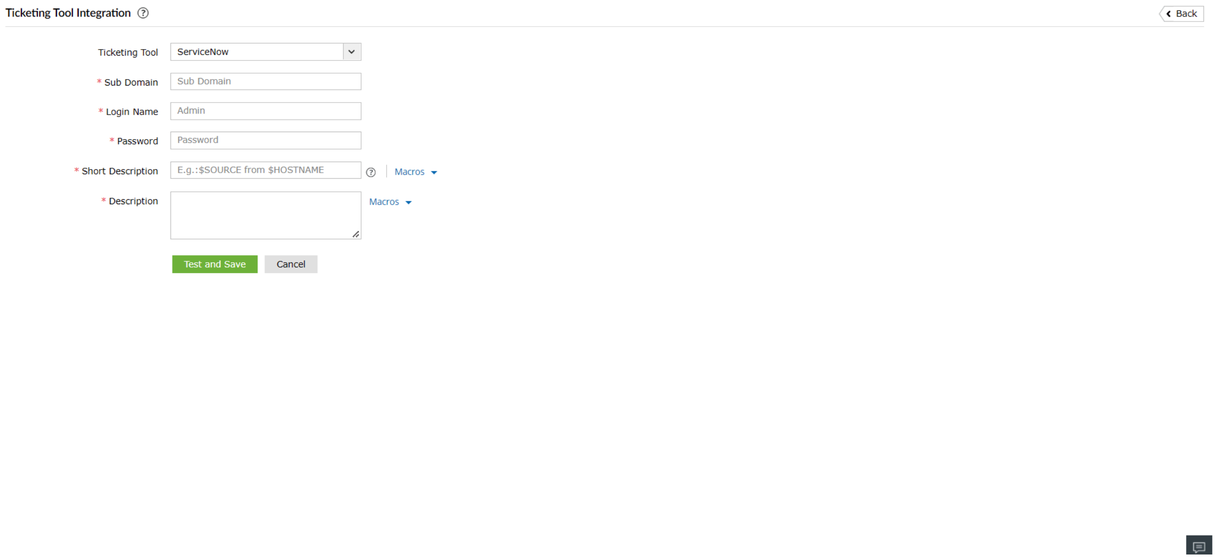
The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For ServiceNow

Note

Only users with permissions to view and edit requests can proceed with the configuration.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select ServiceNow.



Ticketing Tool Integration

Ticketing Tool: ServiceNow

* Sub Domain: Sub Domain

* Login Name: Admin

* Password: Password

* Short Description: E.g.:$SOURCE from $HOSTNAME

* Description:

1. Enter the ServiceNow subdomain name or IP address.
2. Enter the login name and password of a valid account in the ticketing tool.
3. Enter the Short Description and the Description for the alert. You can select them from the predefined list available under Macros or type your own.
4. Click the Test and Save button to establish communication and complete configuration.

> Note
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For JIRA Service Desk On-Demand

> Note
>
> Only users with permissions to view and edit requests can proceed with the configuration.

To configure EventLog Analyzer with Jira Service Desk On-Demand, you need to first get some details from your Jira ticketing tool. Go to the Official JIRA Cloud Doc to get the API Token.

1. After logging into your Jira Service Desk On-Demand account, click the settings icon on the top right corner

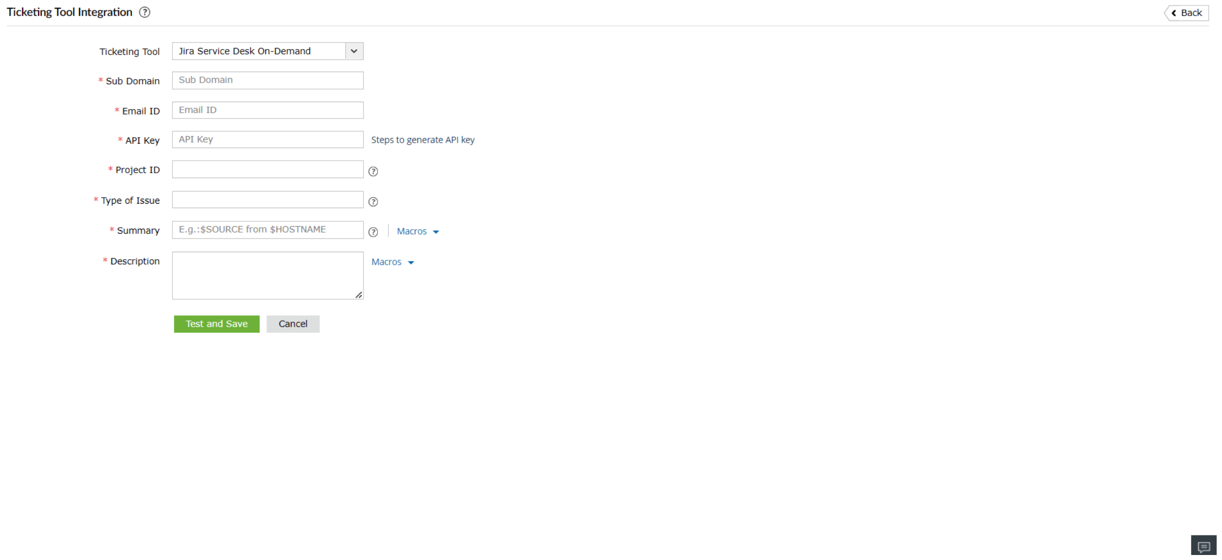
and select Projects.

2. In the project list, note down the Key corresponding to the project in which you want your tickets to be raised.

3. Click the settings icon on the top right corner and select Issues.

4. Note down the type of issues that the particular project can hold. The issues raised from EventLog Analyzer should have the same type for a ticket to be successfully raised in Jira Service Desk On-Demand.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select Jira Service Desk On-Demand.



Ticketing Tool Integration

Ticketing Tool: Jira Service Desk On-Demand

* Sub Domain: Sub Domain

* Email ID: Email ID

* API Key: API Key

* Project ID:

* Type of Issue:

* Summary: E.g.:$SOURCE from $HOSTNAME

* Description:

1. Enter the Jira Service Desk On-Demand Subdomain.

2. Enter your JIRA Account Email ID.

3. Enter the API key that we got in the previous step.

4. Enter the Project ID. This is the Key of the particular project noted from the ticketing tool.

5. Enter the type of issue. This has to be the same issue type that the project has been configured to hold.

6. Enter the Summary and the Description for the alert. You can select them from the predefined list available under Macros or type your own.

7. Click the Test and Save button to establish communication and complete configuration.

> ⓘ Note
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For Zendesk

> ⓘ Note

Only users with Admin/Agent privilege can proceed with the configuration.

Configuring Zendesk with OneAuth authentication:

> ⓘ Note
>
> If your EventLog Analyzer server is running on HTTP, you can configure Zendesk using OAuth only from the installed machine.

To configure EventLog Analyzer with Zendesk, you will need to retrieve some information from your Zendesk ticketing tool:

1. After logging into your Zendesk account, click the tray icon in the top bar and click Admin Center.
2. In Admin Center, click Apps and integrations in the sidebar > select APIs > Zendesk API > OAuth Clients.
3. Click the + icon to create a new OAuth Client
4. Enter the client name, description, and name of the company. Select a logo.
5. Select Confidential for Client Kind field.
6. Enter the redirect URL as given in the EventLog Analyzer console in Redirect URLs field.
7. Copy the value that appears corresponding to Unique Identifier and save it in a separate document.
8. Once you click Save, a secret code will appear above the Save button. Click Copy and save it in a separate document. This would also be needed while configuring Zendesk in EventLog Analyzer.
9. Click Close and open EventLog Analyzer to complete the configuration process.

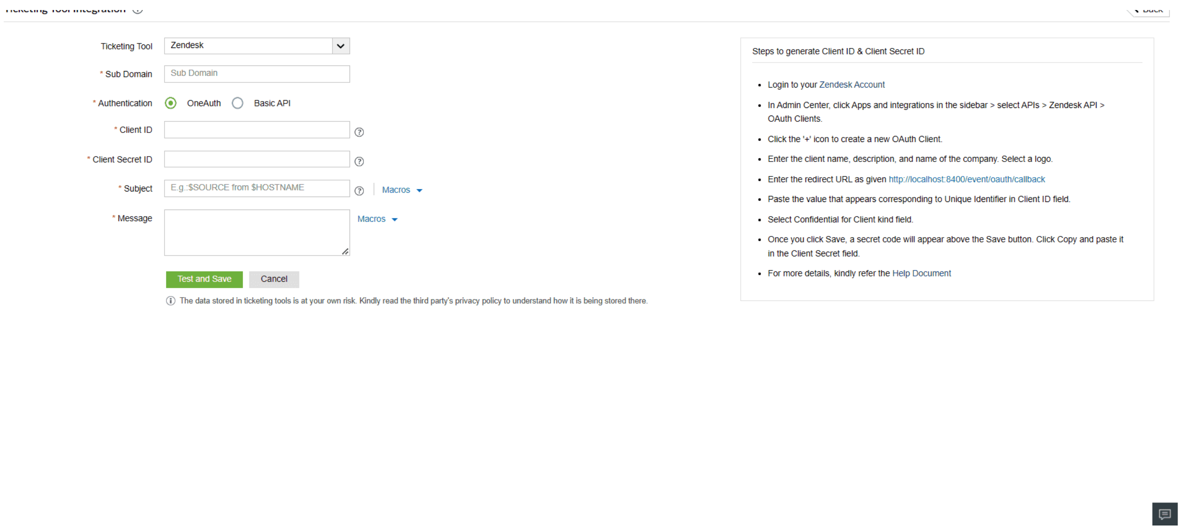
Configuring Zendesk with Basic API authentication:

1. Click the Admin icon in the sidebar, then select Channels → API.
2. Click the Settings tab, and make sure Token Access is enabled.
3. Click the + button to the right of Active API Tokens.
4. Optionally, enter a description under API Token Description. The token is generated, and displayed.
5. Copy the token, and paste it somewhere secure. Once you close this window, the full token will never be displayed again.
6. Click Save to return to the API page. A truncated version of the token is displayed.

Configuration in EventLog Analyzer for Zendesk integration:

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select Zendesk.

1. Enter the Zendesk subdomain name in the given field.
2. Under Authentication, you can choose either OneAuth or Basic API.
3. If you choose OneAuth under Authentication, follow the steps given below.



Ticketing Tool: Zendesk

* Sub Domain: Sub Domain

* Authentication: ● OneAuth ○ Basic API

* Client ID:

* Client Secret ID:

* Subject: E.g.:$SOURCE from $HOSTNAME

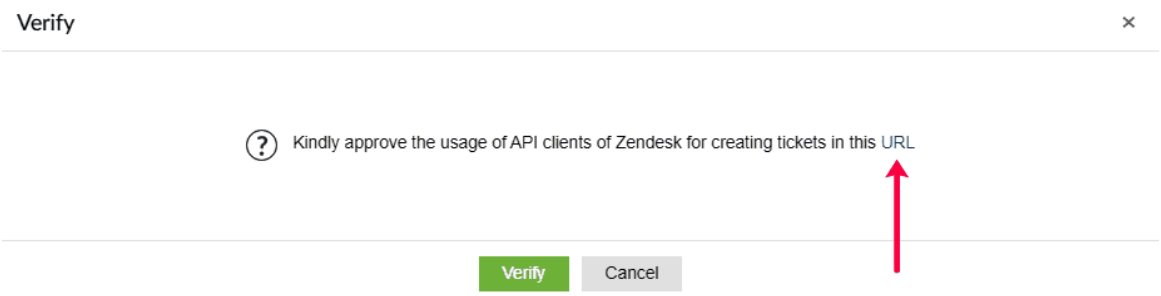
* Message:

The data stored in ticketing tools is at your own risk. Kindly read the third party's privacy policy to understand how it is being stored there.

Steps to generate Client ID & Client Secret ID

- Login to your Zendesk Account
- In Admin Center, click Apps and integrations in the sidebar > select APIs > Zendesk API > OAuth Clients.
- Click the '+' icon to create a new OAuth Client.
- Enter the client name, description, and name of the company. Select a logo.
- Enter the redirect URL as given http://localhost:8400/event/oauth/callback
- Paste the value that appears corresponding to Unique Identifier in Client ID field.
- Select Confidential for Client kind field.
- Once you click Save, a secret code will appear above the Save button. Click Copy and paste it in the Client Secret field.
- For more details, kindly refer the Help Document

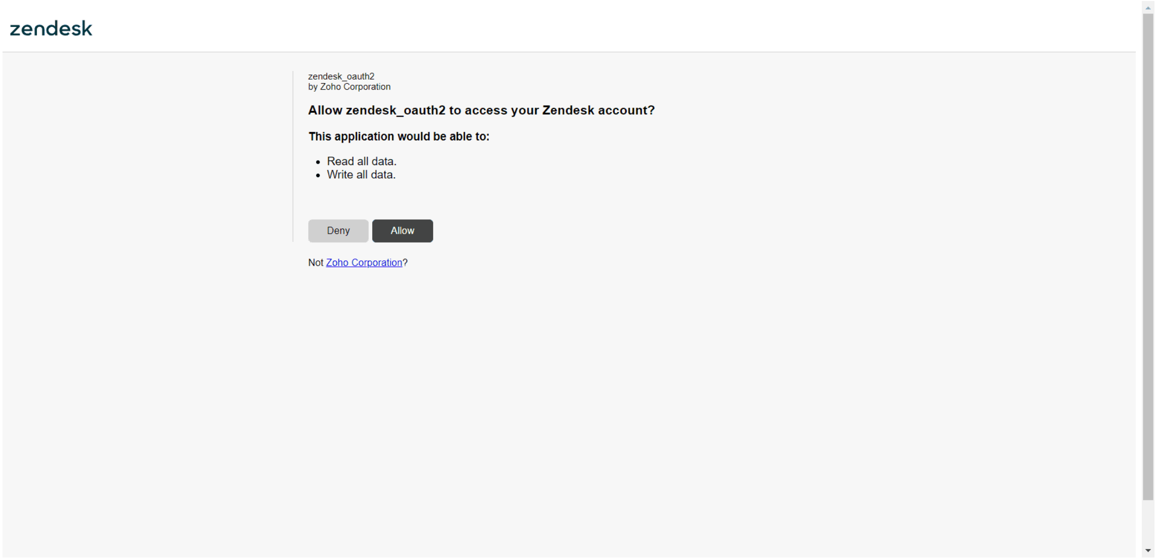
- Enter the Client ID in the corresponding field. This is value of the Unique Identifier noted from the ticketing tool.
- Enter the Client Secret ID in the corresponding field. This is the value of the secret code obtained from the ticketing tool.
- Enter the Subject and the Message for the alert. You can either select them from the predefined list available under Macros or enter your own. Click the Test and Save button. On clicking the Test and Save button, a verify popup will be displayed. Click the URL to approve the usage of the clients of Zendesk.



Verify

Kindly approve the usage of API clients of Zendesk for creating tickets in this URL

- Click Allow for API approval.



zendesk

zendesk_oauth2
by Zoho Corporation

Allow zendesk_oauth2 to access your Zendesk account?

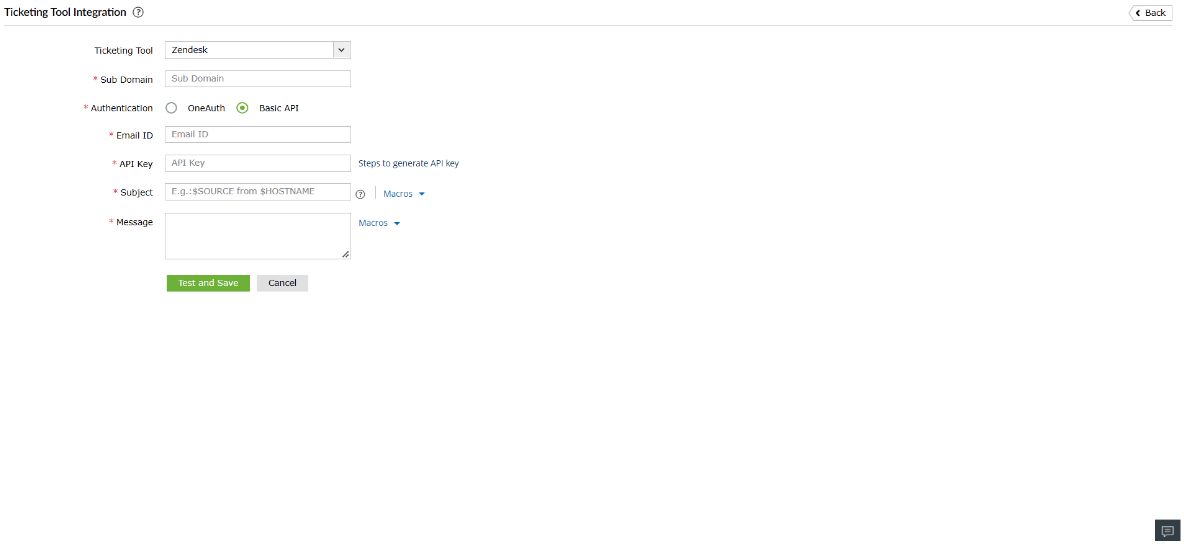
This application would be able to:

- Read all data.
- Write all data.

Not Zoho Corporation?

- Click the Verify button in EventLog Analyzer console. The ticketing tool will now be configured successfully.

4. If you choose Basic API under Authentication, follow the steps given below:



Ticketing Tool Integration

Ticketing Tool: Zendesk

* Sub Domain: Sub Domain

* Authentication: ○ OneAuth ● Basic API

* Email ID: Email ID

* API Key: API Key — Steps to generate API key

* Subject: E.g.:$SOURCE from $HOSTNAME — Macros

* Message — Macros

- Provide the Email Id in the given field.
- Click on Steps to Generate API Key for steps to generate an API key.
- Follow the given steps to generate the API key. After generation, provide the API key in the corresponding field.

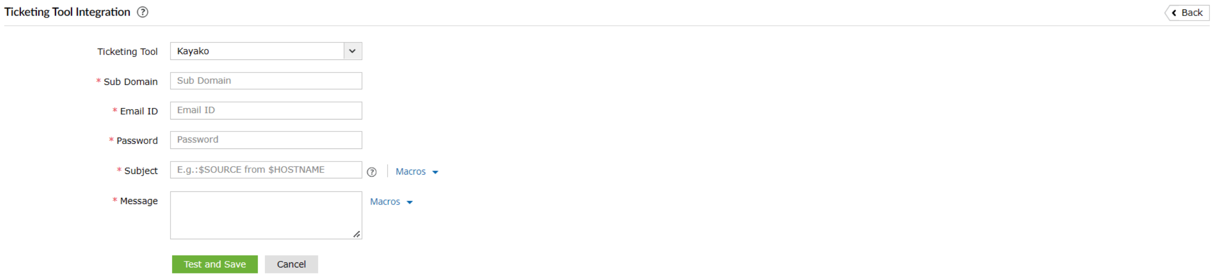
5. Enter the Subject and the Message for the alert. You can select them from the predefined list available under Macros or provide your own.
6. Click the Test and Save button to establish communication and complete configuration.

Note

The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For Kayako

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select Kayako.



Ticketing Tool Integration

Ticketing Tool: Kayako

* Sub Domain: Sub Domain

* Email ID: Email ID

* Password: Password

* Subject: E.g.:$SOURCE from $HOSTNAME — Macros

* Message — Macros

1. Enter the Kayako subdomain name.
2. Enter the emailId and password of a valid user in the ticketing tool.
3. Enter the Subject and the Message for the alert. You can select them from a predefined list available under Macros or type your own.
4. Click the Test and Save button to establish communication and complete configuration.

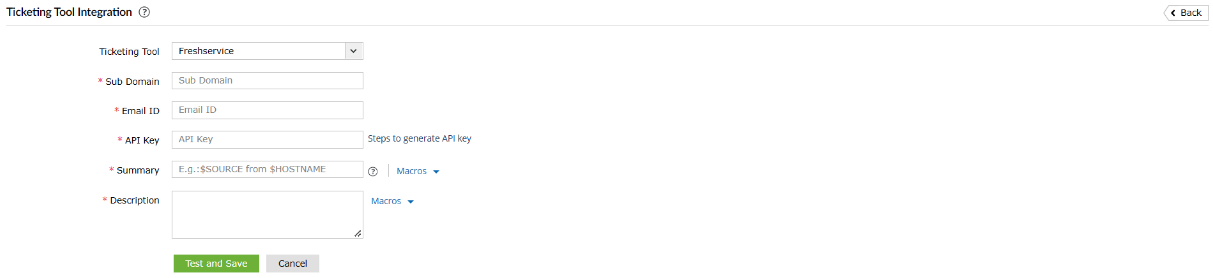
> ⓘ Note
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For FreshService

> ⓘ Note
>
> Only users with either of the following privileges can proceed with the configuration:
>
> - Permissions to create, reply, edit, and delete tickets.
>
>   Or
> - SD Agent, SD Supervisor, Admin, or Account admin role.

To configure EventLog Analyzer with FreshService, you need to first get some details from your FreshService ticketing tool. Go to the official Freshservice Doc to get the API Token.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select Freshservice.



Ticketing Tool Integration

Ticketing Tool: Freshservice

* Sub Domain: Sub Domain

* Email ID: Email ID

* API Key: API Key

* Summary: E.g.:$SOURCE from $HOSTNAME

* Description:

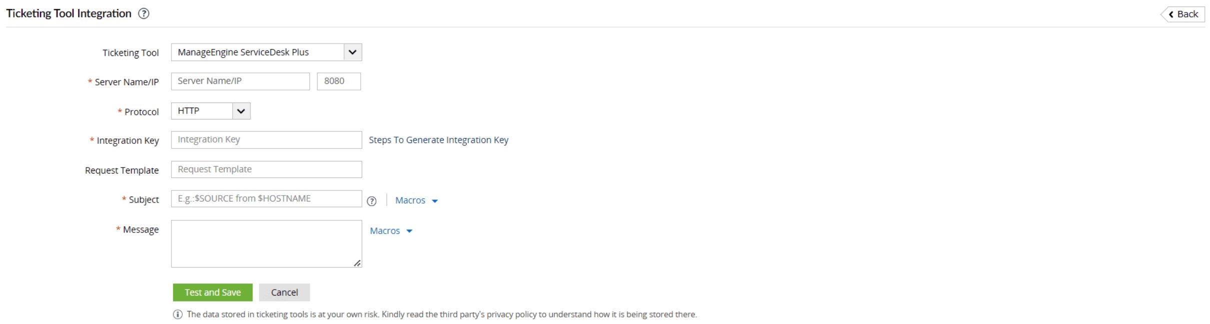
1. Enter the Freshservice Subdomain.
2. Enter Freshservice account Email ID.
3. Enter the API key that we got in the previous step.
4. Enter the Summary and the Description for the alert. You can select them from the predefined list available under Macros or type your own.
5. Click the Test and Save button to establish communication and complete configuration.

> Note
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For ManageEngine ServiceDesk Plus

> Note
>
> Only users with permissions to view and edit requests can proceed with the configuration.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select ManageEngine ServiceDesk Plus.



Ticketing Tool Integration ⓘ

‹ Back

Ticketing Tool: ManageEngine ServiceDesk Plus

* Server Name/IP: Server Name/IP 8080

* Protocol: HTTP

* Integration Key: Integration Key — Steps To Generate Integration Key

Request Template: Request Template

* Subject: E.g.:$SOURCE from $HOSTNAME ⓘ | Macros ▾

* Message: Macros ▾

Test and Save   Cancel

ⓘ The data stored in ticketing tools is at your own risk. Kindly read the third party's privacy policy to understand how it is being stored there.

1. Enter the ManageEngine ServiceDesk Plus server name or IP address.
2. Enter the port number.

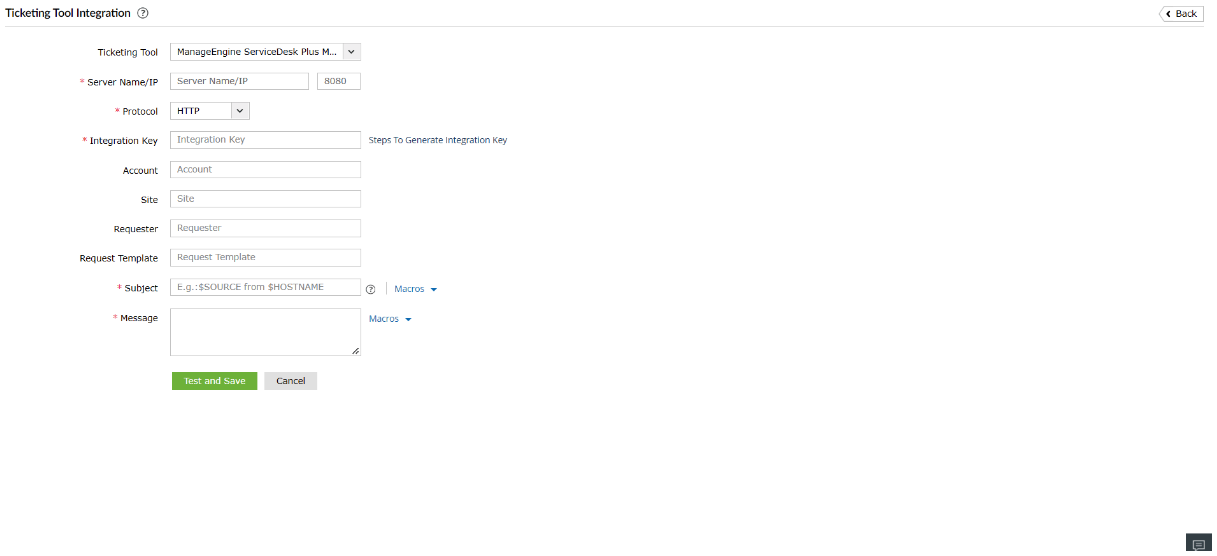
2. Enter the port number.
3. Choose the protocol for communication - HTTP/HTTPS.
4. Enter the Integration Key in the appropriate column. If you do not have an API key click on Steps to Generate API Key for instructions on generating an API key in ServiceDesk Plus.
5. Please specify the Request Template you want to use for creating tickets in ServiceDesk Plus. Leaving it empty would raise tickets using the Default Template.
6. Provide the Subject and Message for the alert—these can be selected from a predefined list under Macros or entered manually as per your requirements.
7. Click the Test and Save button.

> ⓘ Note
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For ManageEngine ServiceDesk Plus MSP

> ⓘ Note
>
> Only users with permissions to view and edit requests can proceed with the configuration.

In EventLog Analyzer, navigate to the Alerts tab and click Ticketing Tool Integration under Alert Configuration. From the Ticketing Tool drop-down list, select ManageEngine ServiceDesk Plus MSP.



Ticketing Tool Integration ⓘ

‹ Back

Ticketing Tool	ManageEngine ServiceDesk Plus M...
* Server Name/IP	Server Name/IP 8080
* Protocol	HTTP
* Integration Key	Integration Key — Steps To Generate Integration Key
Account	Account
Site	Site
Requester	Requester
Request Template	Request Template
* Subject	E.g.:$SOURCE from $HOSTNAME ⓘ Macros ▾
* Message	Macros ▾

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

3. Choose the protocol for communication - HTTP/HTTPS.

4. Enter the API key in the appropriate column. If you do not have an API key, click Steps to Generate API Key for instructions on generating an API key in ServiceDesk Plus MSP.

5. If applicable, you may provide the following optional details:

   - Account – Denotes the account to which this request belongs
   - Site – Denotes the site associated with this request
   - Requester – Indicates the requester of the request
   - Request Template – Indicates the template used to create the request

6. Enter the Subject and the Message for the alert. You can choose them from the predefined list available under Macros or type your own.

7. Click the Test and Save button.

> ⓘ Note
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For JIRA Service Desk

To configure EventLog Analyzer with Jira Service Desk, you would first need to get a few details from your Jira ticketing tool.

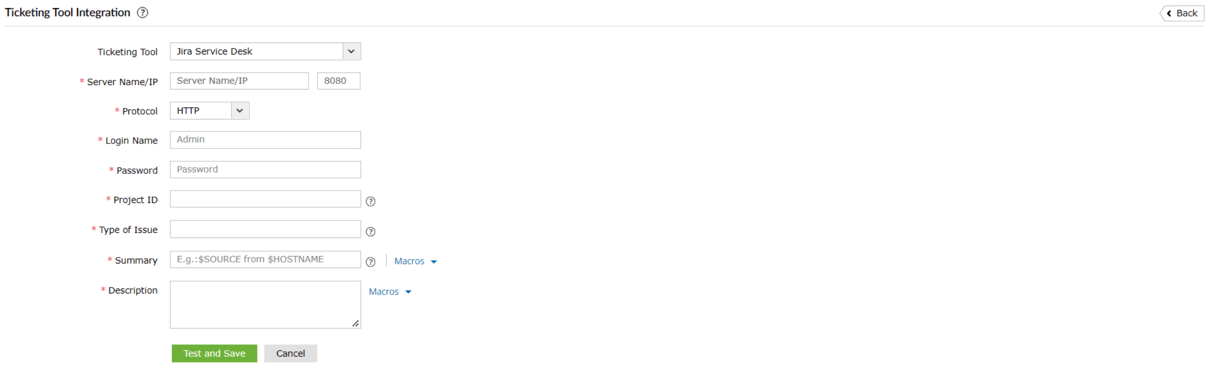
1. After logging into your Jira Service Desk account, click the settings icon on the top right corner and select Projects.

2. In the project list, note down the Key corresponding to the project in which you want your tickets to be raised.

3. Navigate to the Issues tab and reenter your username and password when prompted.

4. Note down the type of issues that the particular project can hold. The issues raised from EventLog Analyzer should have the same type for a ticket to be successfully raised in Jira Service Desk.

5. Close Jira Service Desk and open EventLog Analyzer to complete the configuration process.



Ticketing Tool Integration ⓘ

Ticketing Tool	Jira Service Desk
* Server Name/IP	Server Name/IP 8080
* Protocol	HTTP
* Login Name	Admin
* Password	Password
* Project ID	
* Type of Issue	
* Summary	E.g.:$SOURCE from $HOSTNAME
* Description	

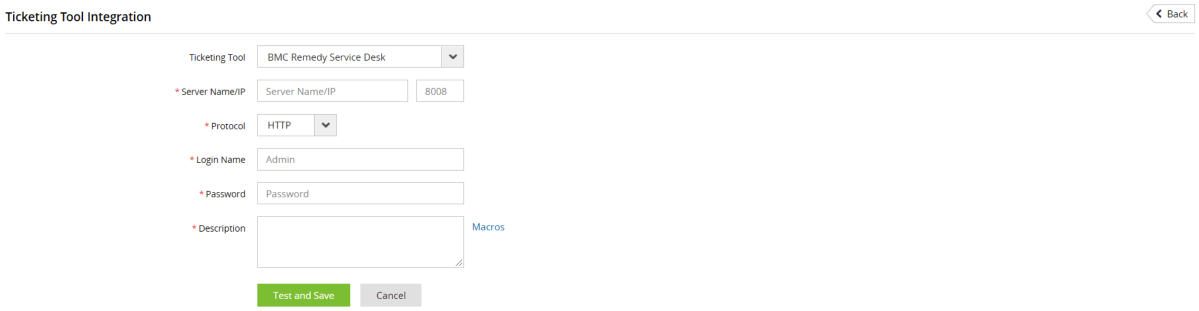
In EventLog Analyzer, navigate to the Alerts tab and click on ticketing tool integration under Alert Configuration. From the Ticketing Tool drop-down list, select Jira Service Desk.

1. Enter the Jira Service Desk server name or IP address.
2. Enter the port number.
3. Choose the protocol for communication - HTTP/HTTPS.
4. Enter the login name and password of the account having admin privileges.
5. Enter the project ID. This is the Key of the particular project noted from the ticketing tool.
6. Enter the type of issue. This needs to be same as the issue type that the project has been configured to hold.
7. Enter the Summary and the Description for the alert. You can select them from a predefined list available under Macros or type your own.
8. Click the Test and Save button to establish communication and complete configuration.

> Note
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

For BMC Remedy Service Desk

In EventLog Analyzer, navigate to the Alerts tab and click on ticketing tool integration under Alert Configuration. From the Ticketing Tool drop-down list, select BMC Remedy Service Desk.



Ticketing Tool Integration

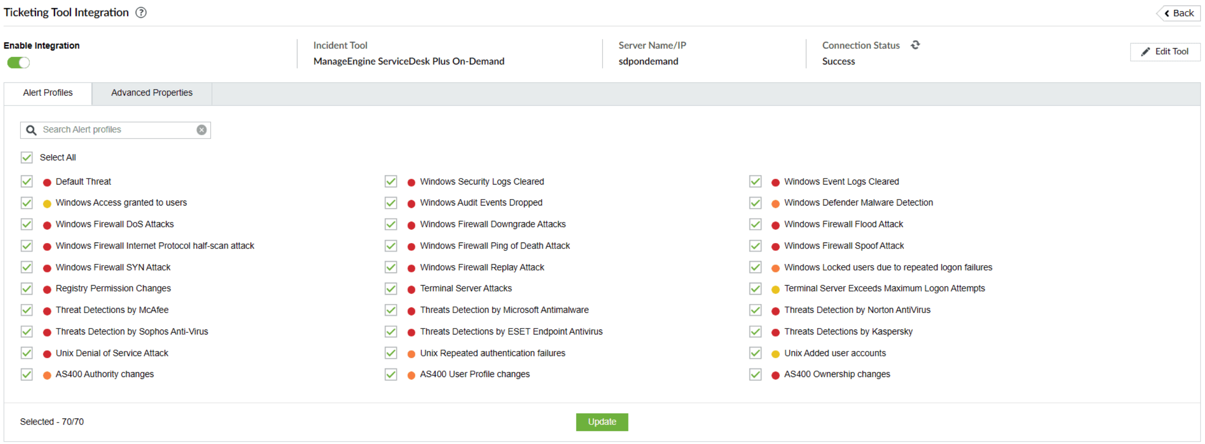
Ticketing Tool	BMC Remedy Service Desk
* Server Name/IP	Server Name/IP · 8008
* Protocol	HTTP
* Login Name	Admin
* Password	Password
* Description	

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.

3. Choose the protocol for communication - HTTP/HTTPS.
4. Enter the login name and password of the account having admin privileges.
5. Enter the Description for the alert. You can choose it from a predefined list available under Macros or type your own.
6. Click the Test and Save button to establish communication and complete the configuration.

> ⓘ Note
>
> The ticketing tool as a configuration will fail if you have an organization-wide proxy configured. Please follow these steps to include the organization-wide proxy certificate in EventLog Analyzer.

Mapping Alert Profiles with Configured Ticketing Tools



Ticketing Tool Integration ⓘ

Enable Integration

Incident Tool
ManageEngine ServiceDesk Plus On-Demand

Server Name/IP
sdpondemand

Connection Status
Success

☑ Select All

☑ ● Default Threat
☑ ● Windows Access granted to users
☑ ● Windows Firewall DoS Attacks
☑ ● Windows Firewall Internet Protocol half-scan attack
☑ ● Windows Firewall SYN Attack
☑ ● Registry Permission Changes
☑ ● Threat Detections by McAfee
☑ ● Threats Detection by Sophos Anti-Virus
☑ ● Unix Denial of Service Attack
☑ ● AS400 Authority changes
☑ ● Windows Security Logs Cleared
☑ ● Windows Audit Events Dropped
☑ ● Windows Firewall Downgrade Attacks
☑ ● Windows Firewall Ping of Death Attack
☑ ● Windows Firewall Replay Attack
☑ ● Terminal Server Attacks
☑ ● Threats Detection by Microsoft Antimalware
☑ ● Threats Detections by ESET Endpoint Antivirus
☑ ● Unix Repeated authentication failures
☑ ● AS400 User Profile changes
☑ ● Windows Event Logs Cleared
☑ ● Windows Defender Malware Detection
☑ ● Windows Firewall Flood Attack
☑ ● Windows Firewall Spoof Attack
☑ ● Windows Locked users due to repeated logon failures
☑ ● Terminal Server Exceeds Maximum Logon Attempts
☑ ● Threats Detection by Norton AntiVirus
☑ ● Threats Detections by Kaspersky
☑ ● Unix Added user accounts
☑ ● AS400 Ownership changes

Selected - 70/70

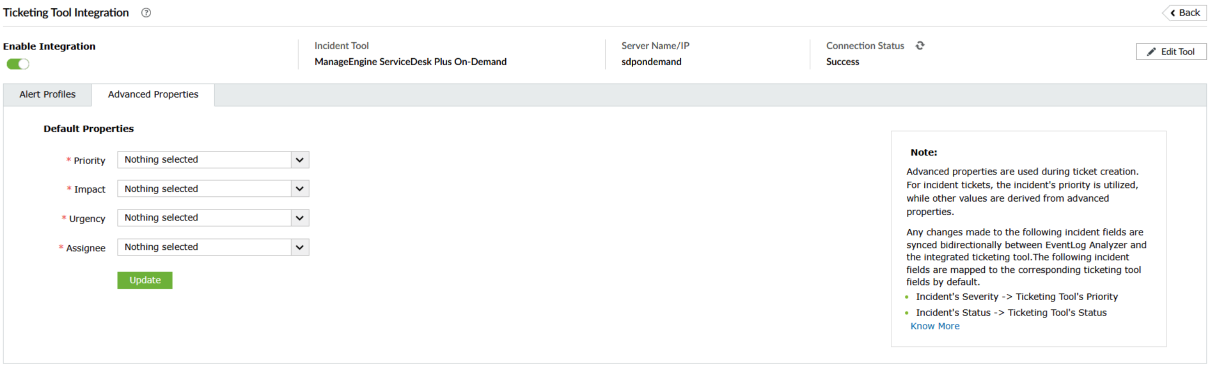
After configuring EventLog Analyzer with the ticketing tool, you can select specific alert profiles from where tickets should be created.

1. Access the Ticketing Tool Integration page - Here, you'll find a list of existing alert profiles.
2. Select Alert Profiles:
   - To select specific profiles for which tickets should be raised, use the search box to find them.
   - To select all alert profiles, check the Select All box. Any future profiles will also be automatically selected.
3. Update Settings: Once you've made your selections, click Update to apply the changes.
4. Manage Ticketing Tool Integration:
   - Enable/Disable Integration: Toggle the integration on or off as needed.
   - Check Connection Status: Click the Refresh icon next to the connection status to verify if Eventlog Analyzer is successfully connected to the ticketing tool.

Advanced Properties Configuration

1. Navigate to the Advanced Properties tab to begin customization.
2. Configure each property by entering the desired values. These settings will be applied to any new tickets in the ticketing tool.

> Note
>
> 1. The Priority selected under Advanced Properties will not be applicable for tickets created from Incidents.
> 2. For seamless functioning of Advanced Properties, users integrating with Freshservice must disable the Priority Matrix in their Freshservice account.



Enable Integration

Incident Tool: ManageEngine ServiceDesk Plus On-Demand

Server Name/IP: sdpondemand

Connection Status: Success

Default Properties

* Priority: Nothing selected
* Impact: Nothing selected
* Urgency: Nothing selected
* Assignee: Nothing selected

Note:

Advanced properties are used during ticket creation. For incident tickets, the incident's priority is utilized, while other values are derived from advanced properties.

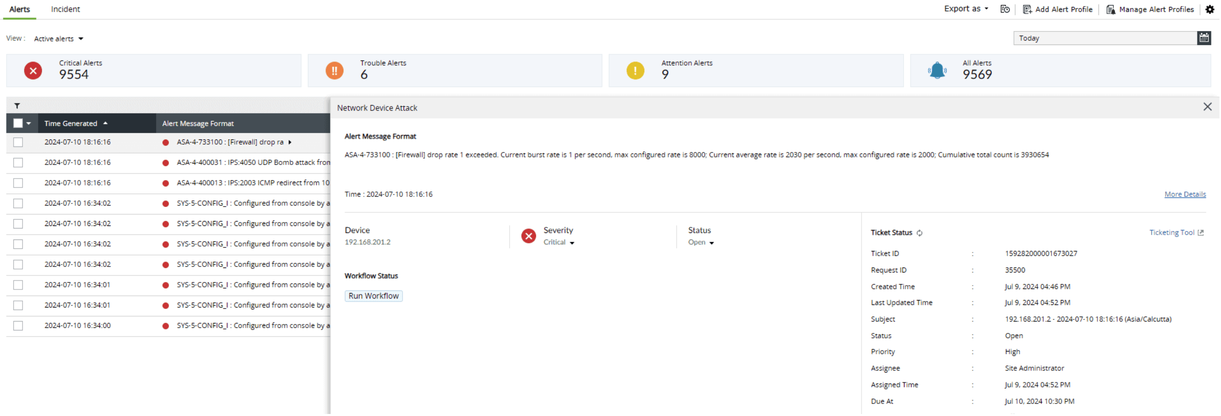
Any changes made to the following incident fields are synced bidirectionally between EventLog Analyzer and the integrated ticketing tool.The following incident fields are mapped to the corresponding ticketing tool fields by default.

- Incident's Severity -> Ticketing Tool's Priority
- Incident's Status -> Ticketing Tool's Status

Know More

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.



Critical Alerts 9554 | Trouble Alerts 6 | Attention Alerts 9 | All Alerts 9569

Time Generated	Alert Message Format
2024-07-10 18:16:16	ASA-4-733100 : [Firewall] drop ra
2024-07-10 18:16:16	ASA-4-400031 : IPS:4050 UDP Bomb attack fron
2024-07-10 18:16:16	ASA-4-400013 : IPS:2003 ICMP redirect from 10
2024-07-10 16:34:02	SYS-5-CONFIG_I : Configured from console by a
2024-07-10 16:34:02	SYS-5-CONFIG_I : Configured from console by a
2024-07-10 16:34:02	SYS-5-CONFIG_I : Configured from console by a
2024-07-10 16:34:02	SYS-5-CONFIG_I : Configured from console by a
2024-07-10 16:34:01	SYS-5-CONFIG_I : Configured from console by a
2024-07-10 16:34:01	SYS-5-CONFIG_I : Configured from console by a
2024-07-10 16:34:00	SYS-5-CONFIG_I : Configured from console by a

Network Device Attack

Alert Message Format

ASA-4-733100 : [Firewall] drop rate 1 exceeded. Current burst rate is 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max configured rate is 2000; Cumulative total count is 3930654

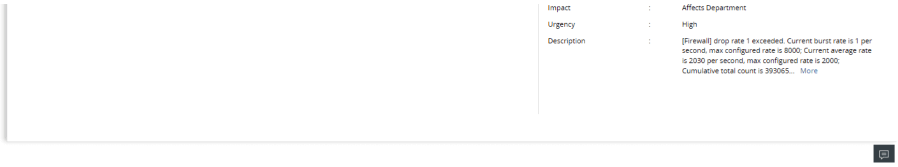
Time : 2024-07-10 18:16:16

Device: 192.168.201.2 | Severity: Critical | Status: Open

Workflow Status

Ticket Status

Ticket ID	:	159282000001673027
Request ID	:	35500
Created Time	:	Jul 9, 2024 04:46 PM
Last Updated Time	:	Jul 9, 2024 04:52 PM
Subject	:	192.168.201.2 - 2024-07-10 18:16:16 (Asia/Calcutta)
Status	:	Open
Priority	:	High
Assignee	:	Site Administrator
Assigned Time	:	Jul 9, 2024 04:52 PM
Due At	:	Jul 10, 2024 10:30 PM



Impact	:	Affects Department
Urgency	:	High
Description	:	[Firewall] drop rate 1 exceeded. Current burst rate is 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max configured rate is 2000; Cumulative total count is 393065... More

Database Settings

5.1.1. Automatic database backup

Last updated on: September 12, 2025

Log360 can automatically back up its database and the databases used in the integrated products at regular intervals, as scheduled by you. Using this option, you can back up the built-in PostgreSQL DB or external PostgreSQL and MS SQL databases configured in the product.

Supported DB versions for auto backup

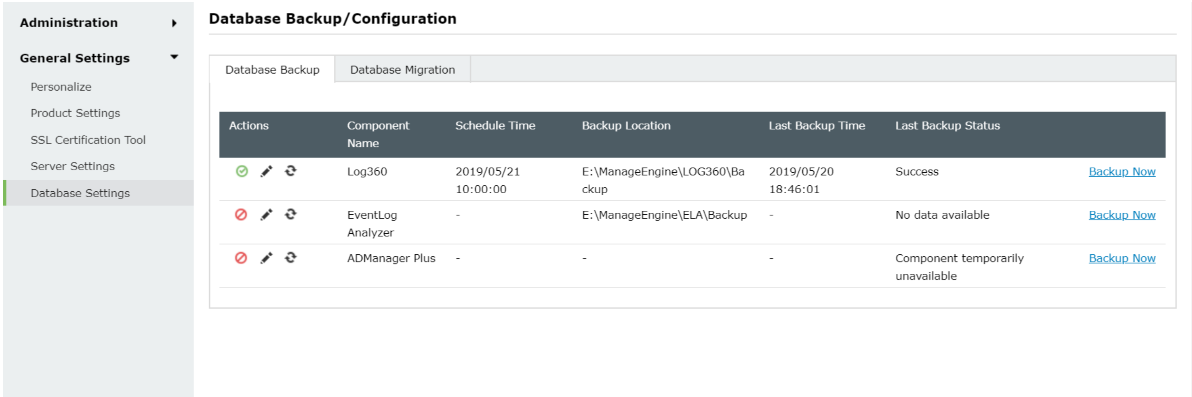
- PostgreSQL: Version 10 to 14
- MS SQL: Version 2008 and above

Prerequisite for backing up external PostgreSQL

1. In the machine where PostgreSQL is installed, go to <postgresql_installdir>/data and open the posgresql.conf file. Search for wal_level entry. Uncomment the entry and change its value to archive.
2. Copy all the files in <postgresql_installdir>/lib and <postgresql_installdir>/bin folders and paste them in <product_home>/pgsql/lib and <product_home>/pgsql/bin folders respectively. <product_home> refers to the home directory of Log360 or the integrated products for which you're configuring the auto backup scheduler.
3. Restart the external PostgreSQL server.
4. Repeat the steps 1 to 3 from above whenever you update the PostgreSQL server.

Steps to schedule database backup

1. Navigate to Admin → General Settings → Database Settings → Database Backup.
2. Choose Log360 or an integrated product for which you want to schedule auto backup, and click the edit ✎ icon.



Database Backup/Configuration

Actions	Component Name	Schedule Time	Backup Location	Last Backup Time	Last Backup Status	
✓ ✎ ⟳	Log360	2019/05/21 10:00:00	E:\ManageEngine\LOG360\Backup	2019/05/20 18:46:01	Success	Backup Now
⊘ ✎ ⟳	EventLog Analyzer	-	E:\ManageEngine\ELA\Backup	-	No data available	Backup Now
⊘ ✎ ⟳	ADManager Plus	-	-	-	Component temporarily unavailable	Backup Now

3. Select whether you want to schedule the backup daily, weekly, or monthly and at what time from the Backup Frequency drop-down.

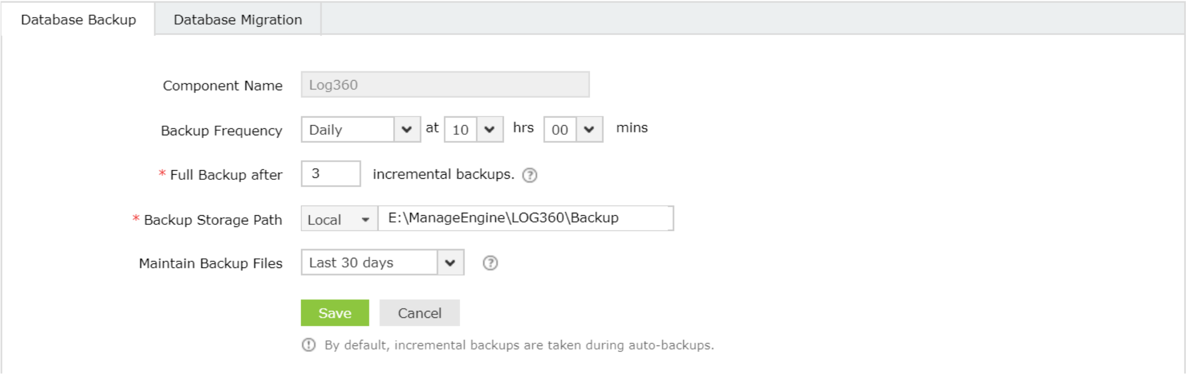
4. Enter the number of incremental backups to take for every full backup in the Full Backup after __ incremental backups box. Enter 0 if you want to take only full backups.

5. Enter the Backup Storage Path.
   - You can either choose a local folder or shared folder to store the backups.
   - If the shared folder you've chosen needs permission to store the backups, then put a check against the Authentication Required box, and enter the necessary credentials.

> ⓘ Note 1
>
> If the shared folder is located in a workgroup computer, then create a new domain account in AD. This new account should have the same username and password as that of a local account in the workgroup computer. Use the credentials of this new account for authentication.

> ⓘ Note 2
>
> If the specified path is wrong or unreachable, the backup will be stored in the default backup folder (<Installation_Folder\Backup>).

6. Set a retention period for the backup files from the Maintain Backup Files drop-down.



Component Name: Log360

Backup Frequency: Daily at 10 hrs 00 mins

* Full Backup after: 3 incremental backups.

* Backup Storage Path: Local E:\ManageEngine\LOG360\Backup

Maintain Backup Files: Last 30 days

ⓘ By default, incremental backups are taken during auto-backups.

7. Click Save.

Other settings

- To disable auto backup for Log360 or a particular integrated product, click the ✓ icon located in the Actions column of the auto backup configuration table.

- To get the status of the latest backup, click the ⟳ icon.
- To edit the backup schedule for a particular component, click on the ✎ icon located in the action column of the component.
- Use the Backup Now option to initiate a backup instantly.
- Use the Recent Backups icon in the status column to view all available backups.

Restoring backup from an old version of MS SQL server to new MS SQL server

If you've installed a new version of MS SQL server and want to configure it in Log360 or its integrated products in place of the old MS SQL server, you can do so by using the backup you've taken using Log360. Just note that, in addition to the backup you've taken using Log360, you need to copy the files in <MS_SQL_Old_Version>/Backup to <MS_SQL_New_Version>/backup.

Troubleshooting tips

If you get an error while backing up the database, please check whether:

- The database server is running.
- There is sufficient space in the backup storage location.

5.1.2. Database Migration

Last updated on: September 12, 2025

In this page

Using this option you can change the built-in database server (PostgreSQL) of Log360 to MS SQL Server or another instance of a PostgreSQL Server.

Important points to remember

- Supported database migrations:
  - PostgreSQL Server to MS SQL Server or another instance of PostgreSQL Server.
  - MS SQL Server to PostgreSQL Server or another instance of MS SQL Server.
- Supported database versions:
  - PostgreSQL: 10 to 14
  - MS SQL: 2008 and above
- Take a backup of the database before you proceed.
- We recommend applying the Windows service packs and cumulative updates suggested by Microsoft during your migration to MS SQL Server.

Prerequisites for MSSQL migration

1. Copy the bcp.exe and bcp.rll files from the installed SQL Server directory and paste them in the Log360 bin folder (<Log360_installed_directory/bin).
   - Location of the bcp.exe file: <MSSQL_installed_folder>\Client SDK\ODBC\...\Tools\Binn\bcp.exe. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\...\Tools\Binn\bcp.exe.
   - Location of the bcp.rll file: <MSSQL_installed_folder>\Client SDK\ODBC\...\Tools\Binn\Resources\1033\bcp.rll. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\...\Tools\Binn\Resources\1033\bcp.rll
2. For migration to MS SQL, please install the corresponding SQL Native Client in the Log360 machine as per the MS SQL Server version.

MS SQL Server Version	Native Client
2008	Download
2012	Download
2014	Download
2017	Download
2019	Download

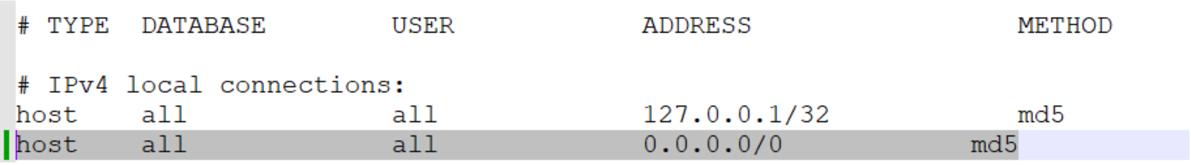
ⓘ Note

MS SQL server version 2022 is also supported by Log360.

3. If firewall is enabled in the MS SQL Server machine, the TCP and UDP ports must be opened.
4. If the MS SQL server you wish to migrate to has Force encryption enabled, follow the steps mentioned below.
   - Convert your certificate to .cer format.
     - Open IIS Manager.
     - In the middle pane, click Server Certificates.
     - Open the certificate you want to use, and click the Details tab.
     - Click Copy to file.
     - Click Next in the Certificate Export Wizard that appears.
     - On the Export Private Key screen, select No, do not export the private key, and click Next.
     - On the Export File Format screen, select either DER encoded binary X.509 (.CER) or Base-64 encoded X.509 (.CER), and click Next.
     - Enter a name for the file and click Next, and then Finish.
   - Open Command Prompt and navigate to <Installation directory>\jre\bin. Use the command below to associate the certificate with the Java KeyStore.
     keytool -import -v -trustcacerts -alias myserver -file pathofthecert\certname.cer -keystore "..\lib\security\cacerts" -keypass changeit -storepass changeit -noprompt
     where pathofthecert is the location where the certificate has been stored and certname is the certificate name.
     The certificate will be added to your Java KeyStore.

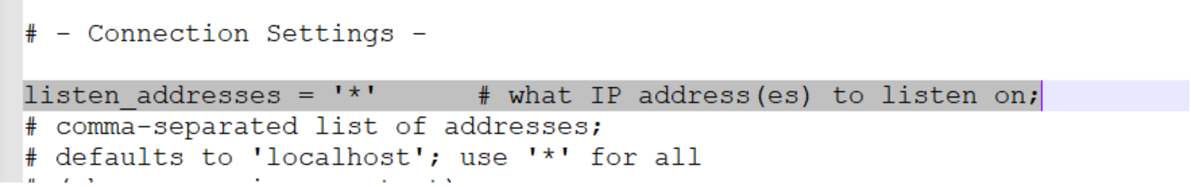
Prerequisites for PostgreSQL migration

1. Open the remote machine where the product is installed & navigate to Product Home\ pgsql\ data\ pg_hba.conf
2. Open pg_hba.conf file and add an entry of the host IP address and its subnet mask as 0.0.0.0/0 (Refer Pic).



```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
host    all             all             0.0.0.0/0            md5
```

3. Navigate to Product Home\ pgsql\ data \ postgresql.conf
4. Open postgresql.conf and change the Listen_addresses as '*' & remove the # in the start of the line. (Refer Pic)



```
# - Connection Settings -

listen_addresses = '*'        # what IP address(es) to listen on;
# comma-separated list of addresses;
# defaults to 'localhost'; use '*' for all
```

Database backup for External PostgreSQL

- In the machine where PostgreSQL is installed, go to <postgresql_installdir>/data and open the posgresql.conf file. Search for wal_level entry. Uncomment the entry and change its value to archive.
- Copy all the files in <postgresql_installdir>/lib and <postgresql_installdir>/bin folders and paste them in <product_home>/pgsql/lib and <product_home>/pgsql/bin folders respectively. Here, <product_home> refers to the home directory of Log360 or the integrated products for which you're configuring the auto backup scheduler.
- Restart the external PostgreSQL server.

Repeat the steps 1 to 3 from above whenever you update the PostgreSQL server.

Steps for Migration

> ⓘ Note
>
> Take a Backup/Snapshot of Log360 before proceeding with the steps (Important)

1. Open the Command Prompt and navigate to <Log360 home\bin> (Here, Log360 home is the location where Log360 is installed)

Log360 is installed).

2. Stop Log360 by running shutdown.bat.

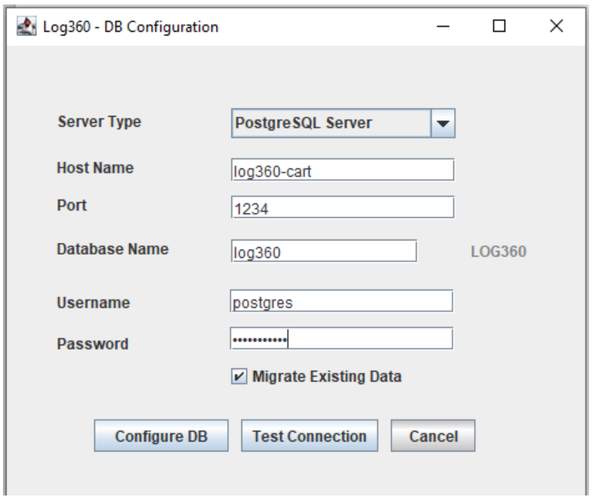
3. Run the ChangeDB.bat.

4. From the Server Type menu, select the database server you plan to switch to.

5. If you select PostgreSQL Server, then:

   - In the Host Name and Port field, enter the host name or IP address and the port number of the PostgreSQL database server.

   - Enter the username and password of a user with the necessary permissions to create a new database.



Log360 - DB Configuration

Server Type: PostgreSQL Server

Host Name: log360-cart

Port: 1234

Database Name: log360 LOG360

Username: postgres

Password: ••••••••••

☑ Migrate Existing Data

6. If you select MS SQL Server, then:

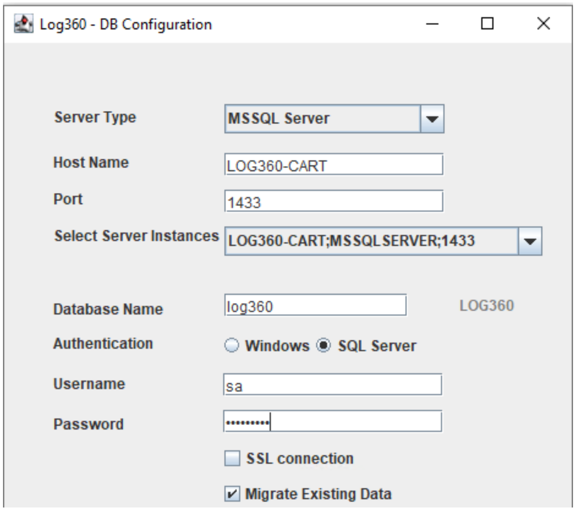
   - Move the bcp.exe and bcp.rll files into the bin folder manually.

   - 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.



Log360 - DB Configuration

Server Type: MSSQL Server

Host Name: LOG360-CART

Port: 1433

Select Server Instances: LOG360-CART;MSSQLSERVER;1433

Database Name: log360 LOG360

Authentication: ○ Windows ● SQL Server

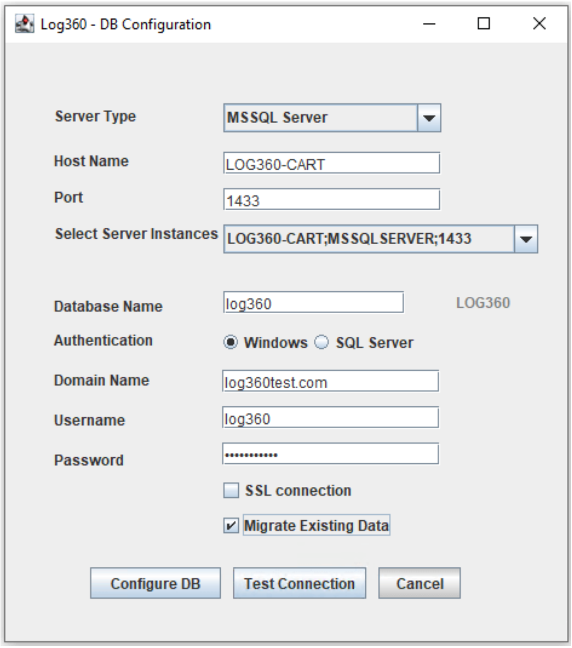
Username: sa

Password: •••••••••

☐ SSL connection

☑ Migrate Existing Data

- If you want to use Windows authentication, select Windows Authentication, and enter the username and password of a Windows domain user account.



Server Type: MSSQL Server
Host Name: LOG360-CART
Port: 1433
Select Server Instances: LOG360-CART;MSSQLSERVER;1433
Database Name: log360 LOG360
Authentication: ● Windows ○ SQL Server
Domain Name: log360test.com
Username: log360
Password: •••••••••••
□ SSL connection
☑ Migrate Existing Data

Note

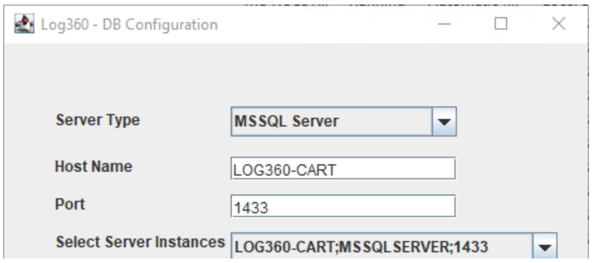
The user account used must have permission to create a database in the selected MS SQL Server.

7. Check the box next to Migrate Existing Data to copy the data from your old database to the new database.

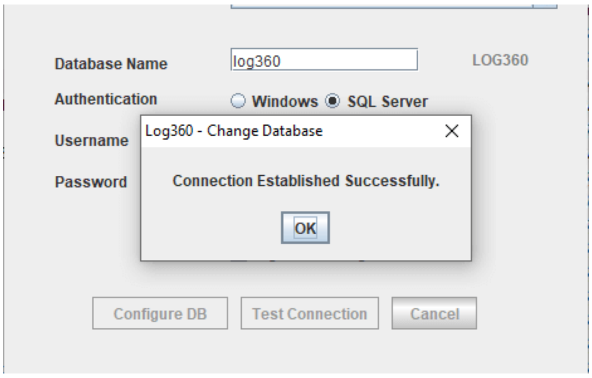
IMPORTANT

Leave this box unchecked only if you are changing the database of a fresh installation of Log360.

8. If the MS SQL server you wish to migrate to has Force encryption enabled, check the box next to SSL connection.
9. Click Test Connection and wait for the connection to be established.



Server Type: MSSQL Server
Host Name: LOG360-CART
Port: 1433
Select Server Instances: LOG360-CART;MSSQLSERVER;1433


Database Name: log360 LOG360

Authentication: ○ Windows ● SQL Server

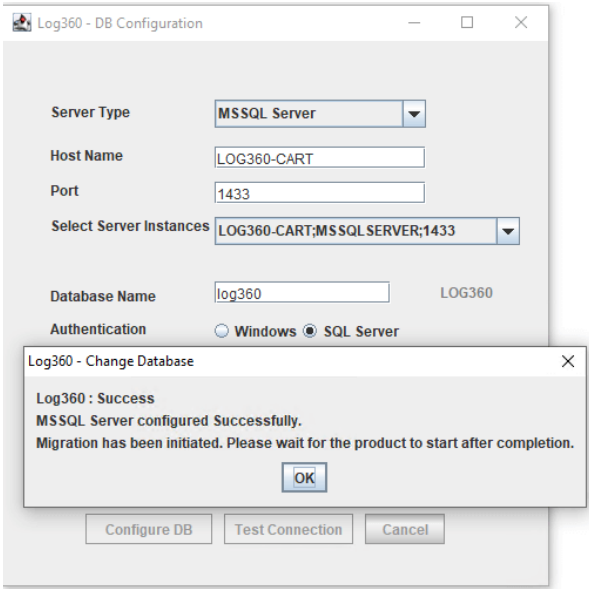
Username

Password

Log360 - Change Database

Connection Established Successfully.

10. Once Test Connection has been established successfully, click Configure DB to initiate migration.


Log360 - DB Configuration

Server Type: MSSQL Server

Host Name: LOG360-CART

Port: 1433

Select Server Instances: LOG360-CART;MSSQLSERVER;1433

Database Name: log360 LOG360

Authentication: ○ Windows ● SQL Server

Log360 - Change Database

Log360 : Success
MSSQL Server configured Successfully.
Migration has been initiated. Please wait for the product to start after completion.

5.1.3. Database Settings

Last updated on: September 12, 2025

Log360 allows you to configure periodic backup of the database that comes built-in with it and the integrated components. The product also allows you to migrate from the built-in database (PostgreSQL) to MS SQL.

- Database Auto Backup
- Database Migration

5.2. Product Settings

Last updated on: September 12, 2025

In this page

Overview

This document provides a comprehensive walkthrough of the Product Settings module in Log360, allowing administrators to tailor how the product behaves and responds to operational needs. From configuring product notifications to enforcing security measures, these settings offer granular control over performance and protection.

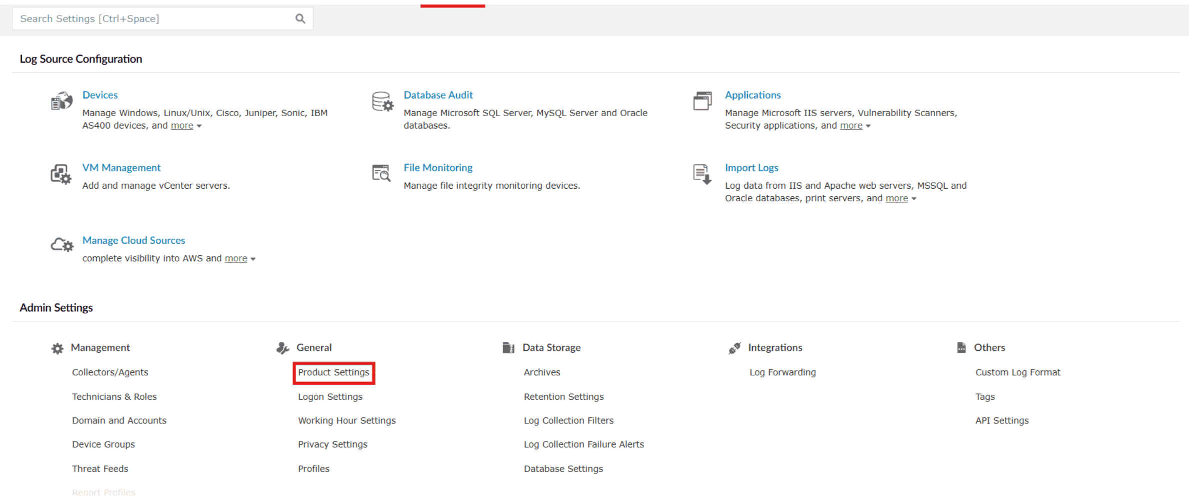
These configurations provide numerous customization capabilities, including limits for emails and SMSs, alert email formats, correlation permissions, and notification settings. The Product Settings tab has three sub-tabs, each having certain customization options:

- Product Configurations
- Product Notifications
- Security Hardening

Product Configurations

To configure settings such as views per page, number of rows displayed in reports, and so on in the product, follow the steps given below.

1. Navigate to the Settings tab and click on Product Settings listed under General in Admin Settings as highlighted below.



Search Settings [Ctrl+Space]

Log Source Configuration

Devices
Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more ▾

Database Audit
Manage Microsoft SQL Server, MySQL Server and Oracle databases.

Applications
Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more ▾

VM Management
Add and manage vCenter servers.

File Monitoring
Manage file integrity monitoring devices.

Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more ▾

Manage Cloud Sources
complete visibility into AWS and more ▾

Admin Settings

Management
Collectors/Agents
Technicians & Roles
Domain and Accounts
Device Groups
Threat Feeds
Report Profiles

General
Product Settings
Logon Settings
Working Hour Settings
Privacy Settings
Profiles

Data Storage
Archives
Retention Settings
Log Collection Filters
Log Collection Failure Alerts
Database Settings

Integrations
Log Forwarding

Others
Custom Log Format
Tags
API Settings

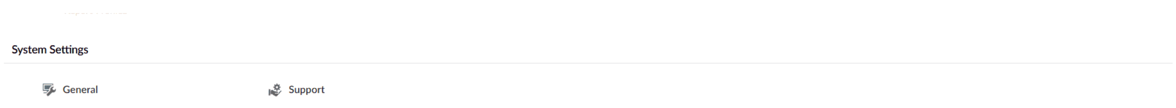
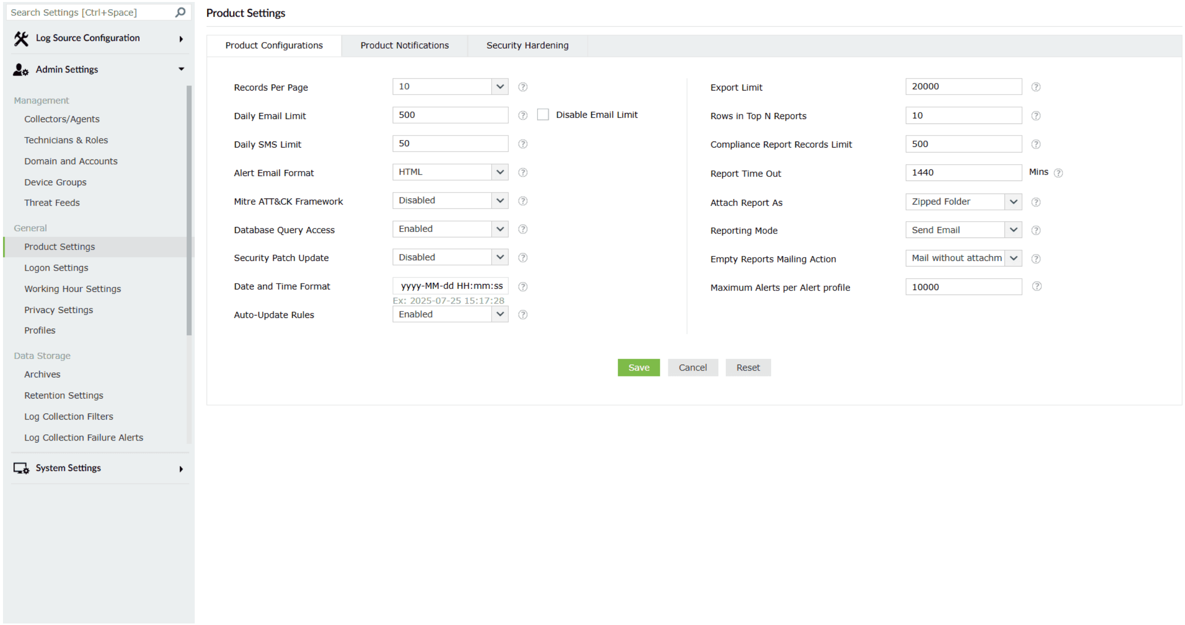


Image 1: Product settings via the Settings tab

2. You will be taken to the Product Settings module with the Product Configurations sub-tab displayed.



Records Per Page: 10
Daily Email Limit: 500 □ Disable Email Limit
Daily SMS Limit: 50
Alert Email Format: HTML
Mitre ATT&CK Framework: Disabled
Database Query Access: Enabled
Security Patch Update: Disabled
Date and Time Format: yyyy-MM-dd HH:mm:ss
Ex: 2025-07-25 15:17:28
Auto-Update Rules: Enabled

Export Limit: 20000
Rows in Top N Reports: 10
Compliance Report Records Limit: 500
Report Time Out: 1440 Mins
Attach Report As: Zipped Folder
Reporting Mode: Send Email
Empty Reports Mailing Action: Mail without attachm
Maximum Alerts per Alert profile: 10000

Image 2: Product Configurations sub-tab via the Product Settings tab

Below is the detailed list of all the fields present in these settings.

Configurations	Default Values	Description
Records Per Page	10	Select the number of records to be displayed in the pages of the user interface. The options available are: 10, 20, 50, and 100.
Daily Email Limit	500	Set the maximum permissible number of emails that can be sent per day. Enable or disable the mail limit alert by selecting the Enable/Disable Mail Limit Alert checkbox. There could be a mail server or client limitation for sending the emails.
Disable Email Limit (checkbox)	Empty checkbox	Ticking the checkbox will allow you to remove any limits for the maximum permissible number of emails that can be sent per day.
Daily SMS Limit	50	Set the maximum permissible number of SMS messages to be sent per day. The telecom service provider often sets a limit to the number of SMSs that can be sent per day.

Configurations	Default Values	Description
Alert Email Format	HTML	Select whether the alert emails are sent in HTML or plaintext format.
Mitre ATT&CK Framework	Disabled	Consolidated data from the Mitre reports will be displayed on the new dashboard tab Mitre Overview when this option has been enabled.Note: This feature will increase log processing and it might affect the performance.
Database Query Access	Enabled	Configure whether access to the product's database is allowed or denied. The product's database can be queried to access product data stored in it.
Security Patch Update	Disabled	Option to Automatically download Critical Security Patch to your Instance
Date and Time Format	yyyy-MM-dd HH:mm:ss	Set the format of date and time that needs to be displayed throughout the product. Other than the few predefined formats available, you can also create formats of your own. There are a few rules to be followed while creating your own date and time format: • The permitted separators are hyphen(-), slash (/), full stop(.), colon(:), comma(,), and space. • A space is the only separator that can be used between the date and the time. • There should not be any separators at the beginning or at the end. • Two continuous separators are not allowed. • Entering two digits for the month will display the month in numbers, whereas entering three digits will display it in words. Ex. 'MM' will display June as 06 and 'MMM' will display it as Jun.
Auto-Update Rules	Enabled	Option to Automatically download Critical Security Patch to your Instance
Export Limit	20000	Set the maximum number of records to be included in an exported report.
Rows in Top N	10	Set the number of rows to be displayed for reports under the Top

Reports N Reports section.

Configurations	Default Values	Description
Compliance Report Record Limit	500	Set the maximum number of records to be included in a Scheduled Compliance Report.
Report Time Out	1440 mins	Set the maximum time allowed to generate a report.
Attach Report As	Zipped Folder	Select the report format to be attached in email. The available options are: PDF/CSV Report and Zipped Folder.
Reporting Mode	Send Email	Configure whether you want to save the reports in a folder in the machine, send them as mail attachments, or both. For Save to Location and Send Email & Save to Location options, you have to enter the location to save the reports in the text box. The reporting mode options available are Send Email, Save to Location, and Send Email & Save to Location.
Empty Reports Mailing Action	Mail without attachment	Configure whether you want to receive a mail or not when the reports are empty. There are two types of mail that you can receive. By selecting Mail without attachment, you will receive a mail without the empty reports. Mail with attachment, will let you receive a mail with the empty reports attached. You can choose not to receive a mail by selecting Don't mail reports.
Maximum Alerts per Alert profile	10000	Maximum number of alerts that will be triggered for an alert profile in a day. The recommended value is a maximum of 10,000.

3. After making the necessary changes, click on Save.
4. Upon successful completion of action, the below pop-up appears.

Successfully updated

5. Click on the Reset button if you wish to reset all the configurations made in the fields and redo them.

Product Notifications

To configure the scenarios for which you want to receive notifications from the product, follow the steps given below.

1. Navigate to the Settings tab and click on Product Settings listed under General in Admin Settings as highlighted below.

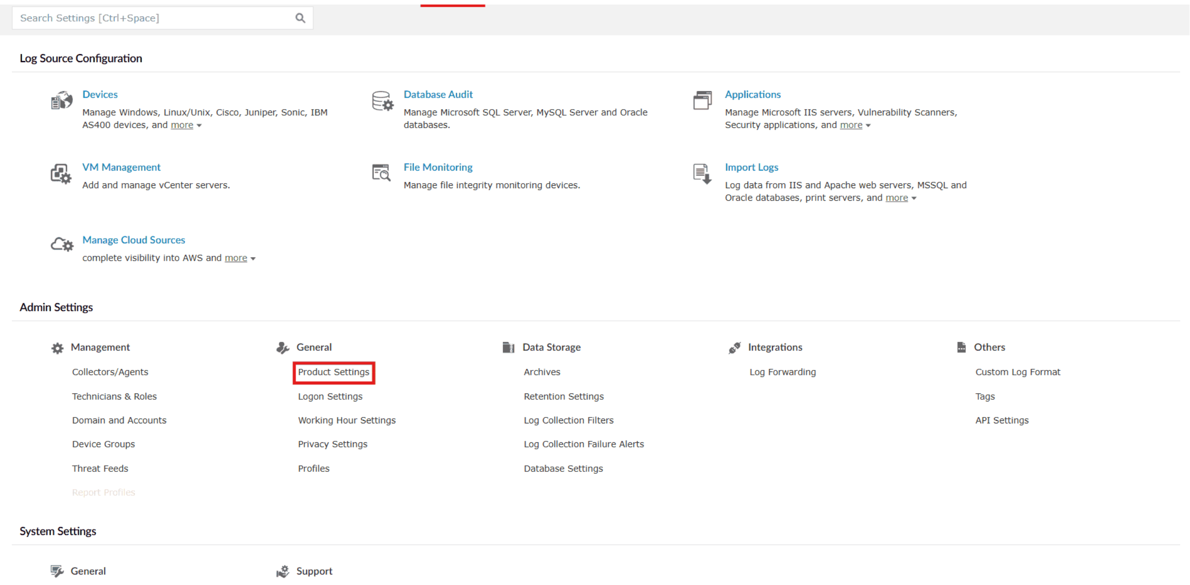
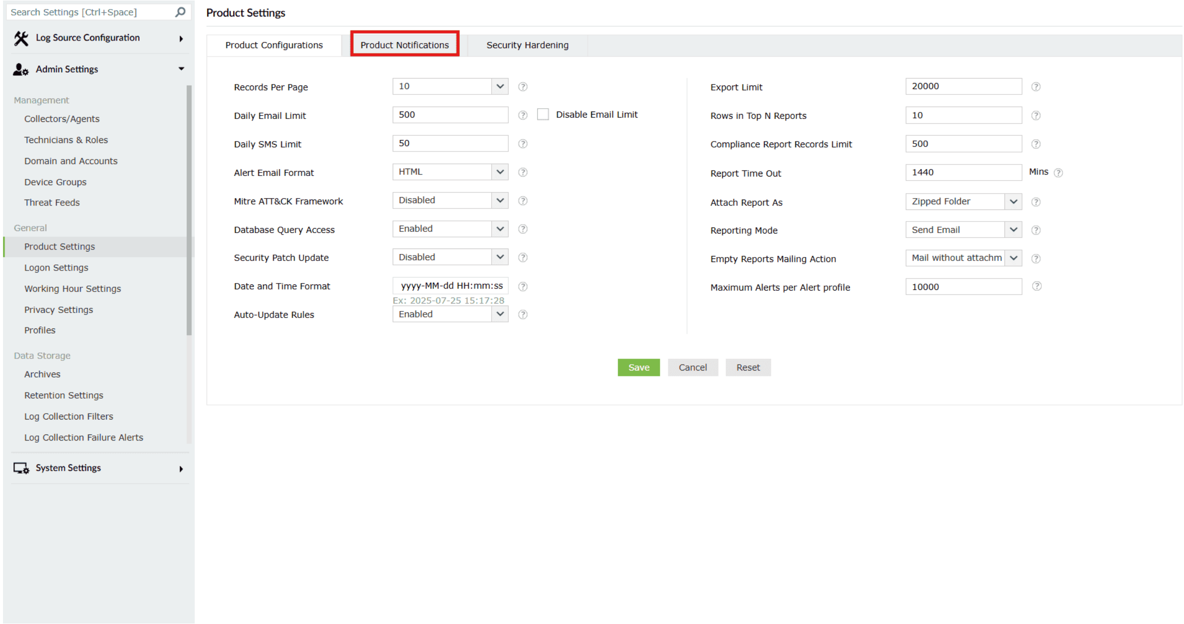


Image 3: Product settings via the Settings tab

2. You will be taken to the Product Settings module with the Product Configurations sub-tab displayed. Click on the Product Notifications sub-tab.



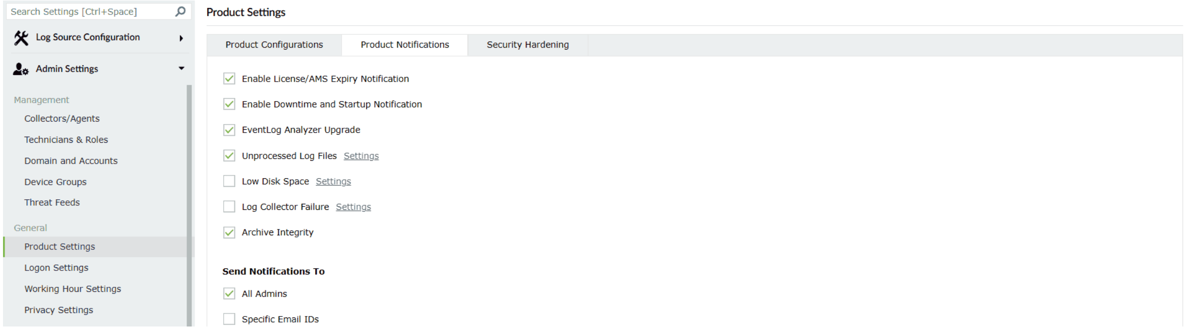
Product Settings

Records Per Page: 10
Daily Email Limit: 500 □ Disable Email Limit
Daily SMS Limit: 50
Alert Email Format: HTML
Mitre ATT&CK Framework: Disabled
Database Query Access: Enabled
Security Patch Update: Disabled
Date and Time Format: yyyy-MM-dd HH:mm:ss
Ex: 2025-07-25 15:17:28
Auto-Update Rules: Enabled

Export Limit: 20000
Rows in Top N Reports: 10
Compliance Report Records Limit: 500
Report Time Out: 1440 Mins
Attach Report As: Zipped Folder
Reporting Mode: Send Email
Empty Reports Mailing Action: Mail without attachm
Maximum Alerts per Alert profile: 10000

Image 4: Product Notifications sub-tab highlighted

3. The Product Notifications sub-tab opens as shown below.



Product Settings

☑ Enable License/AMS Expiry Notification
☑ Enable Downtime and Startup Notification
☑ EventLog Analyzer Upgrade
☑ Unprocessed Log Files Settings
□ Low Disk Space Settings
□ Log Collector Failure Settings
☑ Archive Integrity

Send Notifications To
☑ All Admins
□ Specific Email IDs

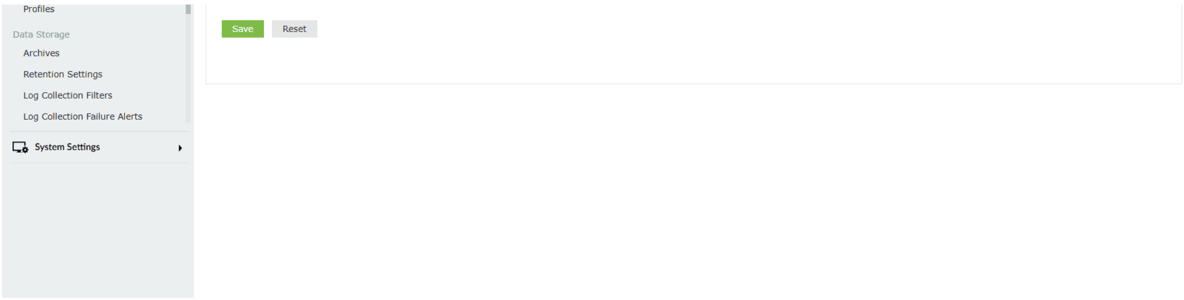


Image 5: Product Notifications sub-tab via the Product Settings tab

The different settings for enabling or disabling alerts have been listed below.

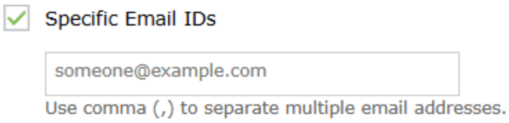
Configurations	Default configuration	Description
Enable License/AMS Expiry Notification	Enabled	You will be notified that your Log360 license is about to expire exactly 30 days, 7 days, and 1 day prior to the expiry date, as well as on the day of expiry.
Enable Downtime and StartUp Notification	Enabled	You will be notified when the Log360 service shuts down or is started.
Enable product Upgrade	Enabled	You will be notified when Log360 has been successfully upgraded.
Unprocessed Log Files	Enabled	When Log360 is unable to process the incoming logs fast enough, the unprocessed logs will be added to files. They will be processed one after the other once Log360 can process logs. You can set a limit on the number of files that get filled with unprocessed logs. You will be notified once the limit is exceeded.In a new installation of Log360, the default value for Unprocessed Log Files is 100.
Low Disk Space	Disabled	You will be notified when the free space available in the disk on which Log360 is installed goes below a certain value. You can set the limit in terms of GB of free disk space and give a suitable subject for the email that will get triggered.
Log Collector Failure	Disabled	You will be notified when Log360's log collector is unable to collect logs. You can configure the subject of the email that will get triggered.

Configurations	Default configuration	Description
Archive integrity	Enabled	You will be notified when the archive files are deleted or tampered via an email notification.

ⓘ NOTE

In a new installation of Log360, notifications will be turned on by default for Enable License/AMS Expiry Notification, Enable Downtime and StartUp Notification, Enable Product Upgrade, and Unprocessed Log Files.

4. Choose the mode for Send Notifications To:
   - After configuring the necessary notification settings, select if those notification emails need to be sent to all the product designated Admins. This option is enabled by default. You can click on the checkbox to disable this option.
   - Alternatively, you can choose to send the notification mails to specific email addresses. This option is disabled by default. Click on the checkbox to enable it.
     - Upon enabling, a box to enter the mail address(es) appears as the below.



☑ Specific Email IDs

someone@example.com

Use comma (,) to separate multiple email addresses.

   - You can opt for both modes at the same time.
5. After making the necessary configurations, click on the Save button.
6. Upon successful completion of action, the below pop-up appears.

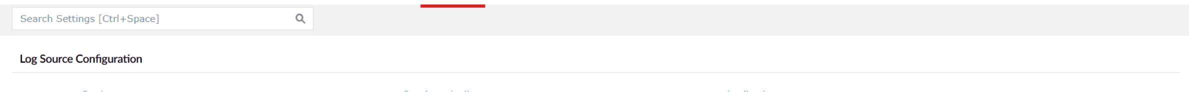
Successfully updated

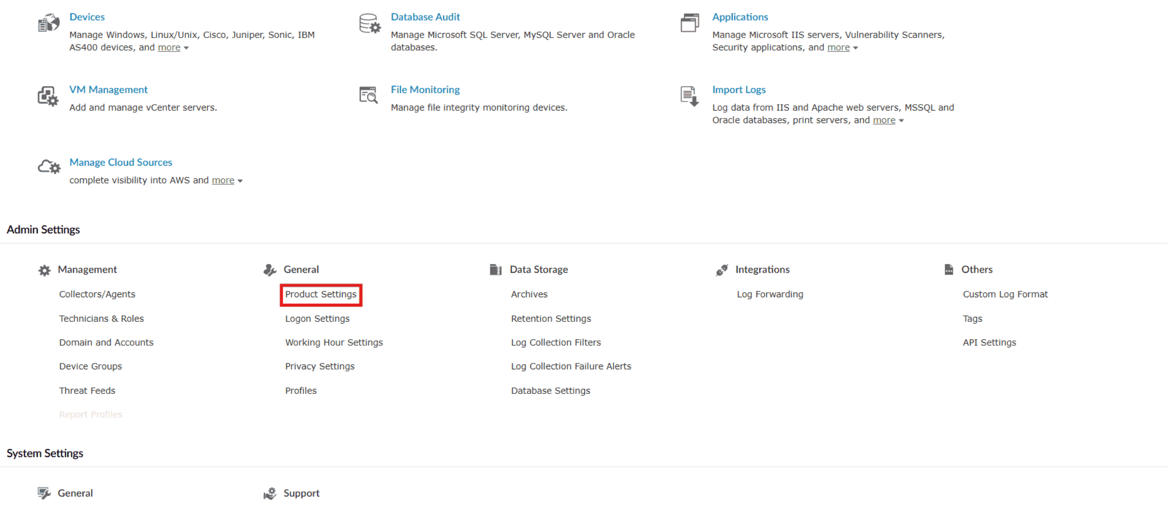
Security Hardening

Security hardening feature helps you manage and configure the security settings of the product console. This tab also displays a security score, which is calculated based upon the weightage given to each configuration.
To manage individual settings, click the Configure or Enable option corresponding to that security setting and make the required changes. Once configured, the setting will have a green ticked ✓ Configured/Enabled icon next to it.

Enabling Security Hardening:

1. Navigate to the Settings tab and click on Product Settings listed under General in Admin Settings as highlighted below.





Devices
Manage Windows, Linux/Unix, Cisco, Juniper, Sonic, IBM AS400 devices, and more

Database Audit
Manage Microsoft SQL Server, MySQL Server and Oracle databases.

Applications
Manage Microsoft IIS servers, Vulnerability Scanners, Security applications, and more

VM Management
Add and manage vCenter servers.

File Monitoring
Manage file integrity monitoring devices.

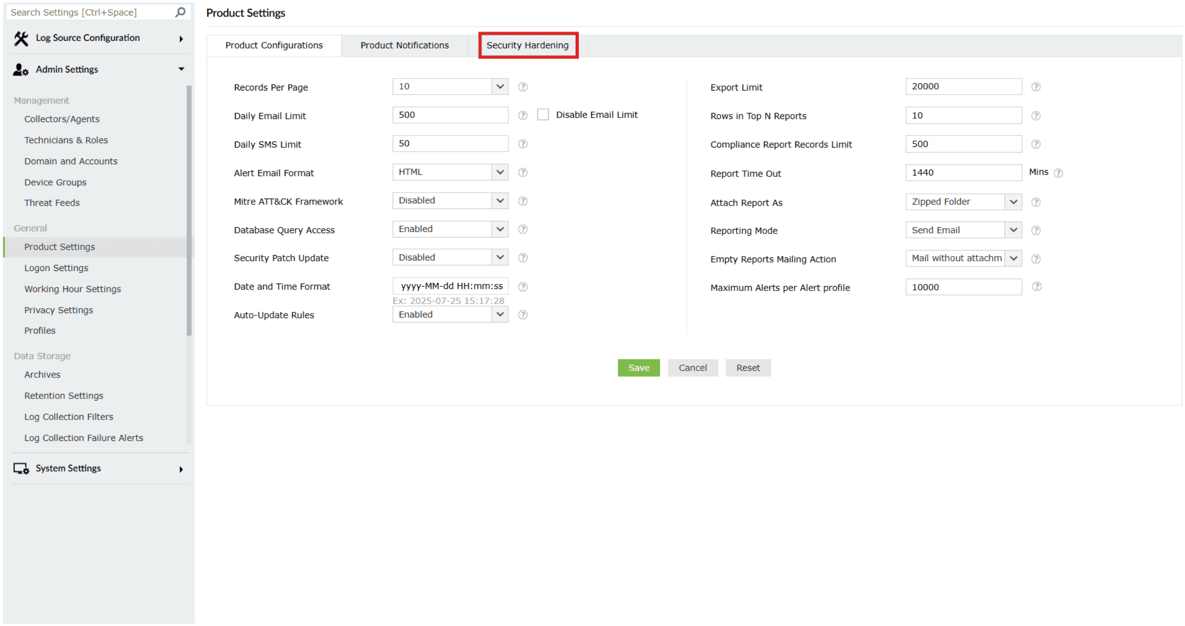
Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more

Manage Cloud Sources
complete visibility into AWS and more

Admin Settings

Image 6: Product settings via the Settings tab

2. You will be taken to the Product Settings module with the Product Configurations sub-tab displayed. Click on the Security Hardening sub-tab.

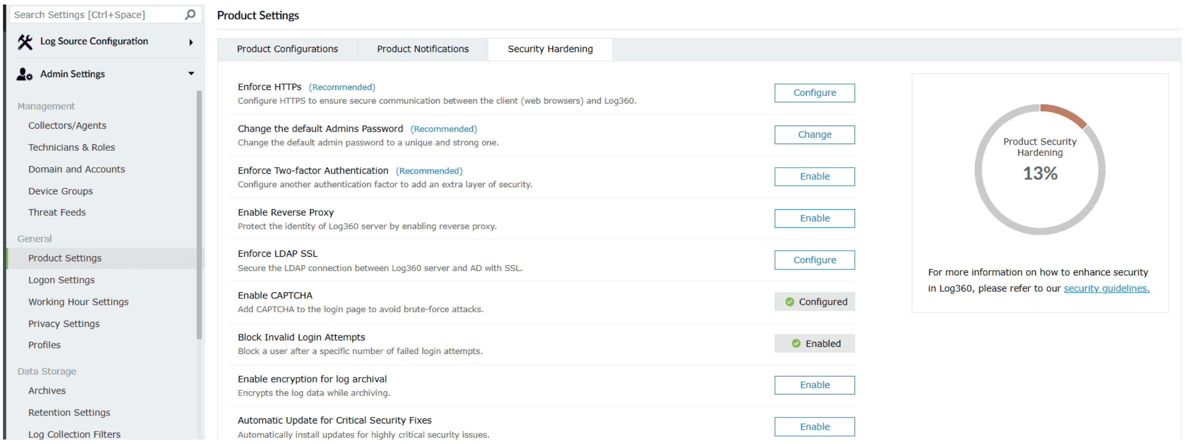


Records Per Page: 10
Daily Email Limit: 500 ☐ Disable Email Limit
Daily SMS Limit: 50
Alert Email Format: HTML
Mitre ATT&CK Framework: Disabled
Database Query Access: Enabled
Security Patch Update: Disabled
Date and Time Format: yyyy-MM-dd HH:mm:ss
Ex: 2025-07-25 15:17:28
Auto-Update Rules: Enabled

Export Limit: 20000
Rows in Top N Reports: 10
Compliance Report Records Limit: 500
Report Time Out: 1440 Mins
Attach Report As: Zipped Folder
Reporting Mode: Send Email
Empty Reports Mailing Action: Mail without attachm
Maximum Alerts per Alert profile: 10000

Image 7: Security Hardening sub-tab highlighted

3. The Security Hardening sub-tab opens as shown below.



Enforce HTTPS (Recommended)
Configure HTTPS to ensure secure communication between the client (web browsers) and Log360. — Configure

Change the default Admins Password (Recommended)
Change the default admin password to a unique and strong one. — Change

Enforce Two-factor Authentication (Recommended)
Configure another authentication factor to add an extra layer of security. — Enable

Enable Reverse Proxy
Protect the identity of Log360 server by enabling reverse proxy. — Enable

Enforce LDAP SSL
Secure the LDAP connection between Log360 server and AD with SSL. — Configure

Enable CAPTCHA
Add CAPTCHA to the login page to avoid brute-force attacks. — ✓ Configured

Block Invalid Login Attempts
Block a user after a specific number of failed login attempts. — ✓ Enabled

Enable encryption for log archival
Encrypts the log data while archiving. — Enable

Automatic Update for Critical Security Fixes
Automatically install updates for highly critical security issues. — Enable

Product Security Hardening
13%

For more information on how to enhance security in Log360, please refer to our security guidelines.

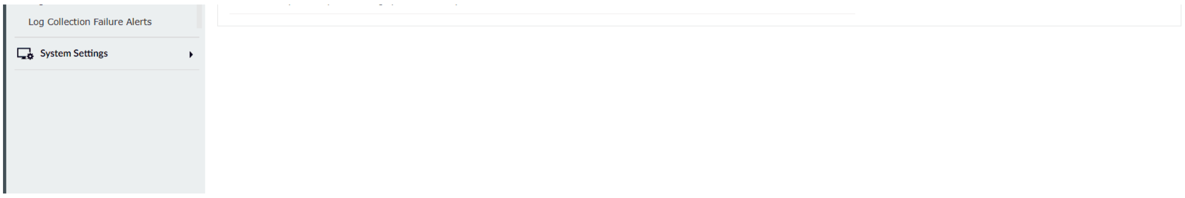


Image 8: Security Hardening sub-tab via the Product Settings tab

We recommend you configure all the settings and ensure your product security score is 100%. The security settings alert will be displayed in the notification center (□ icon on the top-right corner) until a security score of 100% is reached.

> NOTE
>
> For licensed customers, the alert will also be displayed after every successful login until all the mandatory security configurations (marked with * under List of security settings) are done.

List of available settings

- Enforce HTTPS: Configuring HTTPS helps you secure a connection between the web browser and the product's server. See how to enable HTTPS.
- Change the default Admins Password : It is recommended to use a strong password to access the product's dashboard. Use this setting to change both the admin and operator passwords.
- Enforce Two-factor Authentication: Two-factor authentication adds an additional layer of security. See how to configure two-factor authentication.
- Enable Reverse Proxy: Enabling reverse proxy helps protect the identity of the product's server. Click on Configure to navigate to the reverse proxy settings tab. See how to enable reverse proxy settings.
- Enforce LDAP SSL: This setting lets you secure the LDAP (Lightweight Directory Access Protocol) connection between the product server and Active Directory with SSL (Secure Sockets Layer). See how to enable LDAP SSL.
- Enable CAPTCHA: This setting adds a captcha to the login page to avoid brute-force attacks. See how to add captcha.
- Block Invalid Login Attempts: This setting allows you to block a specific user who fails to login after a specific number of attempts. See how to block invalid login attempts.
- Enable encryption for log archival: Enable this setting to encrypt the log data every time while archiving.
- Automatic Update for Critical Security Fixes: Enable this setting to automatically update your product to the latest build. See how to enable auto-update.

> NOTE
>
> The first three settings given in the above list are mandatory for Log360.

To ensure that you don't miss configuring any important security settings, Log360 sends the following alerts:

- Licensed users will receive a popup after every successful login to complete the mandatory security configurations.
- Admin accounts will be prompted to change the default admin password.
- A security alert will be displayed in the notification center until the security score reaches 100%.

Why we recommended Security Hardening?

To understand this, below is the breakdown of all the settings that the security hardening feature recommends:

1. Enforce HTTPS:

- This helps in preventing MITM attacks by encrypting the session between the browser and the Log360 server.
- Compliances like GDPR mandate organizations to use SSL encryption for secure data transmission.

2. Change the default Admins Password:

- Default passwords are publicly known and thus, can be easily exploited by attackers.
- Regular changes into strong passwords not only enhance security but also reduces the risk of privilege escalation.

3. Enforce two-factor authentication:

- In case the password does get compromised, attackers can still not login without the second factor.
- Also prevents unauthorized remote access.
- Some compliances make it mandatory to enable two-factor authentication.

4. Enable Reverse Proxy:

This conceals the actual IP addresses of the integrated components, making it hard for attackers to target them directly.

5. Enforce LDAP SSL:

Makes the connection secure by encrypting the traffic between Log360 and Active Directory.

6. Enable CAPTCHA:

Prevents automated brute force attacks by making manual human interaction necessary.

7. Block Invalid Login Attempts:

- Protects you against password guessing attacks and brute force attacks.
- Disables accounts temporarily after multiple repeated failed attempts.
- Flags suspicious login attempts for investigation and improves overall security monitoring.

8. Enable encryption for log archival:

Enable flat file encryption to encrypt the log data while archiving.

9. Automatic Update for Critical Security Fixes:

- Ensures that Log360 stays up to date with the latest builds and fixes for any vulnerabilities without needing any administrative burden.
- Ensures delivery of the latest security protocols of the comprehensive SIEM tool.
- Prevents exploitation of known vulnerabilities.

Security patch updates

Whenever critical vulnerabilities are discovered in the product, a security patch update is pushed to help mitigate any security threats. This option has to be enabled for automatic download of security patches whenever available.

Prerequisites for the security patch updates:

- Internet connection should be available
- Zoho creator website should be whitelisted as the patches will download from here.

Read also

This document detailed the configuration of product settings, including customization, notification preferences, and security hardening best practices. For additional features that help enhance security, administration, and automation, refer to:

- Administration settings
- Agent administration and settings

6.1.1. Extensions

Last updated on: September 12, 2025

In this page

Extensions are pre-built software components that can either add a set of custom features into EventLog Analyzer or integrate other third-party applications into EventLog Analyzer. EventLog Analyzer's flexible platform enables it to address a wide-range of industry specific use cases.

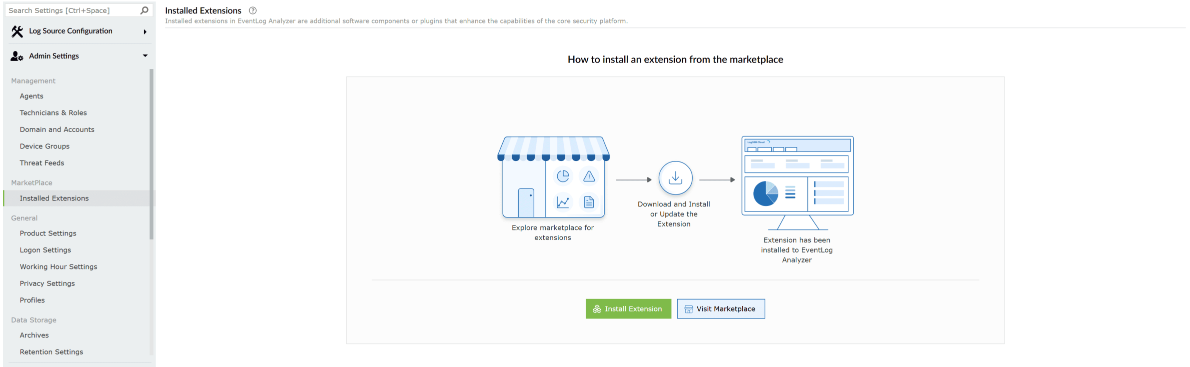
Third-party Application Extensions

Third-party application extensions enable users to integrate data from external security or business applications into EventLog Analyzer. Customers can download the extension for the application they use in their organization from the Marketplace, install it, and utilize it seamlessly.

How to download and install extensions

To install an extension for EventLog Analyzer, you need to first download the extension from the Marketplace and must be uploaded to EventLog Analyzer. Here's how you can achieve this.

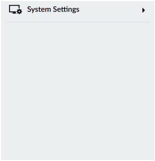
1. Download the required EventLog Analyzer extension from the Marketplace.
2. Once the download is completed, open EventLog Analyzer and navigate to Settings > Admin Settings > Marketplace > Installed Extensions.



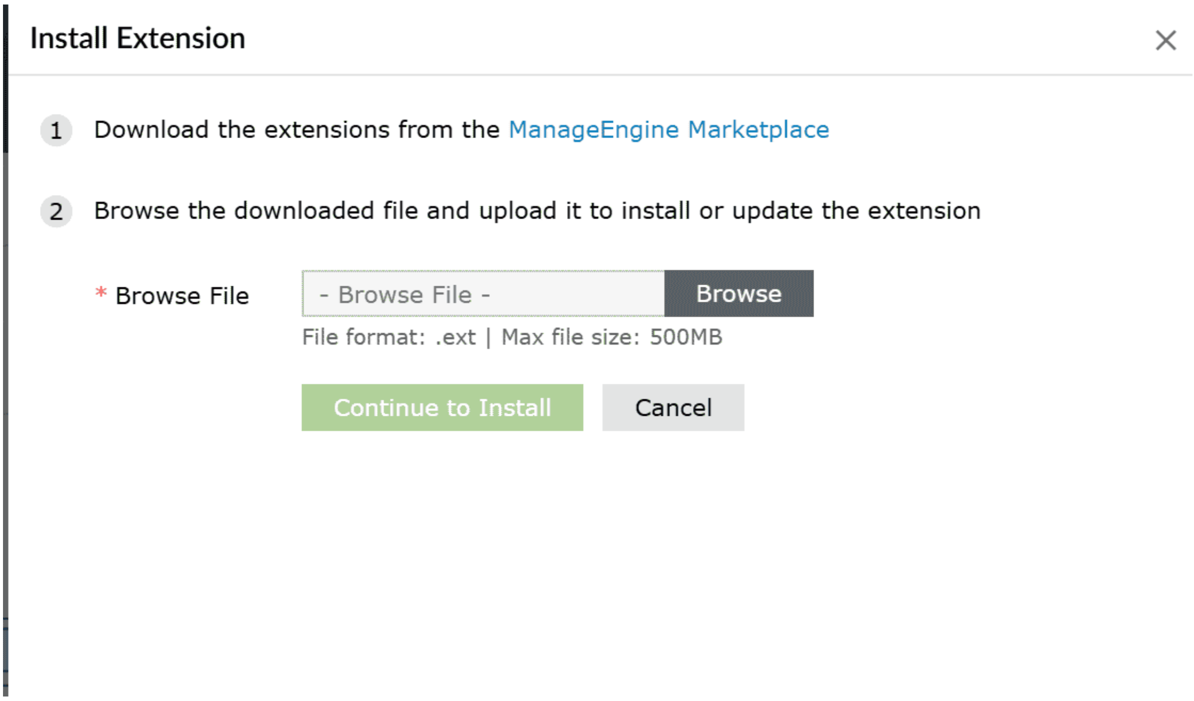
Installed Extensions

Installed extensions in EventLog Analyzer are additional software components or plugins that enhance the capabilities of the core security platform.

How to install an extension from the marketplace



3. Click Install Extension and upload the extension.



Install Extension

1 Download the extensions from the ManageEngine Marketplace

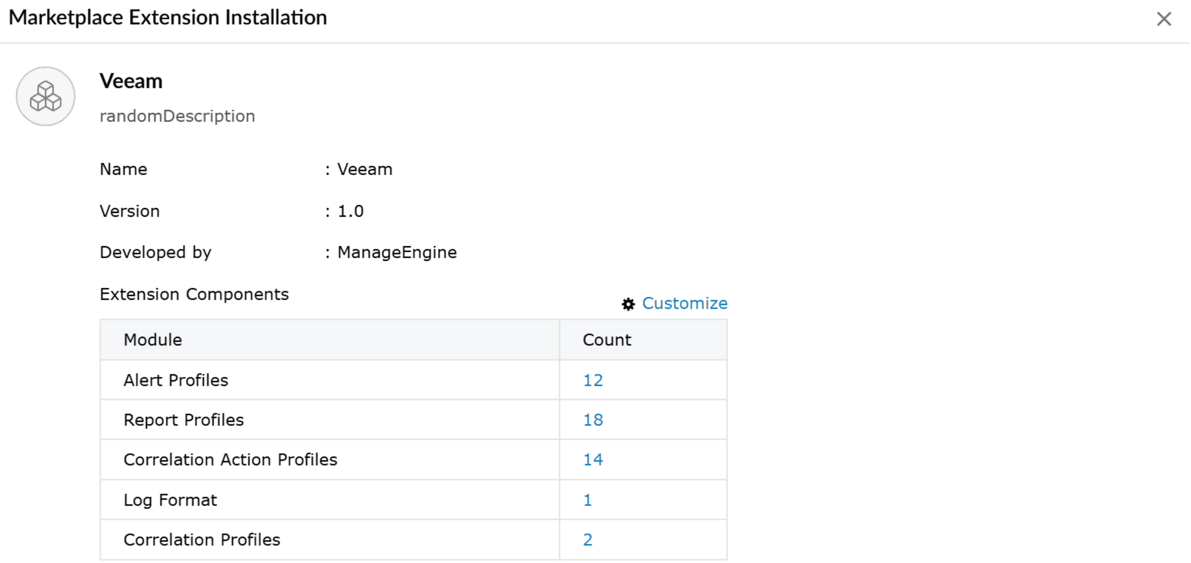
2 Browse the downloaded file and upload it to install or update the extension

* Browse File - Browse File - Browse

File format: .ext | Max file size: 500MB

4. Click Continue to Install to finalise the installation.

5. Before installing, you can customize extension components such as reports, log formats, and other configurations using the Customize feature.



Marketplace Extension Installation

Veeam

randomDescription

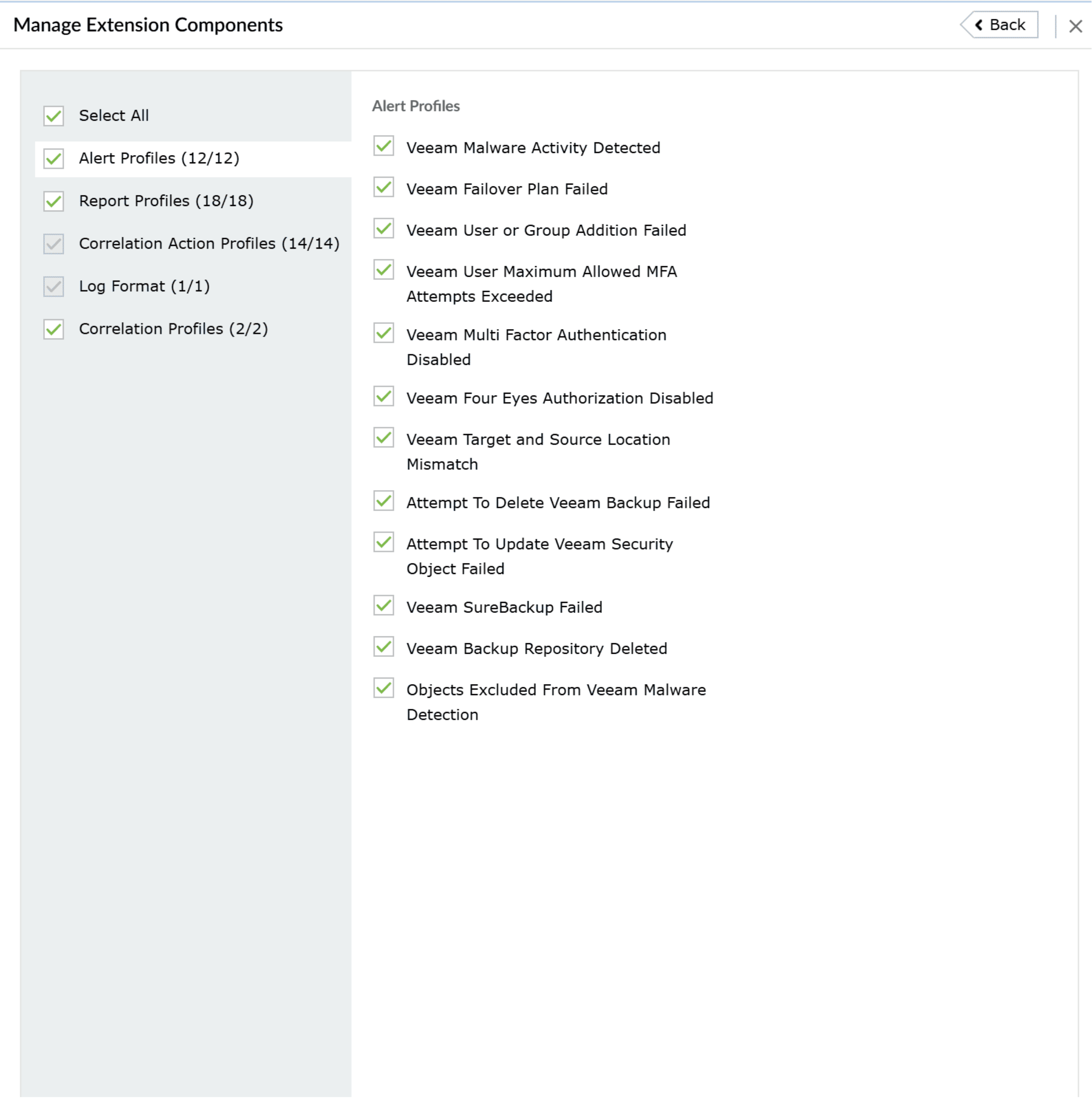
Name : Veeam

Version : 1.0

Developed by : ManageEngine

Extension Components

Module	Count
Alert Profiles	12
Report Profiles	18
Correlation Action Profiles	14
Log Format	1
Correlation Profiles	2



☑ Select All

☑ Alert Profiles (12/12)

☑ Report Profiles (18/18)

☑ Correlation Action Profiles (14/14)

☑ Log Format (1/1)

☑ Correlation Profiles (2/2)

Alert Profiles

☑ Veeam Malware Activity Detected

☑ Veeam Failover Plan Failed

☑ Veeam User or Group Addition Failed

☑ Veeam User Maximum Allowed MFA Attempts Exceeded

☑ Veeam Multi Factor Authentication Disabled

☑ Veeam Four Eyes Authorization Disabled

☑ Veeam Target and Source Location Mismatch

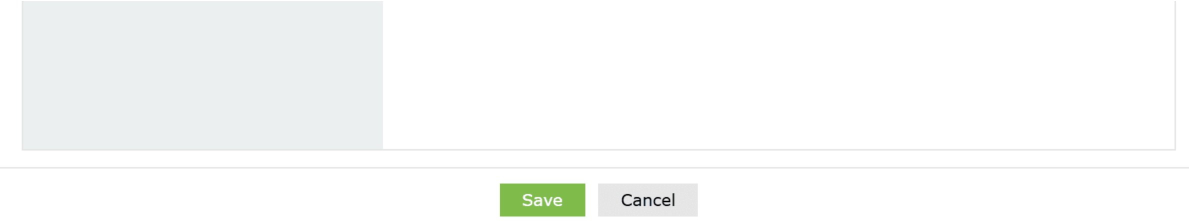
☑ Attempt To Delete Veeam Backup Failed

☑ Attempt To Update Veeam Security Object Failed

☑ Veeam SureBackup Failed

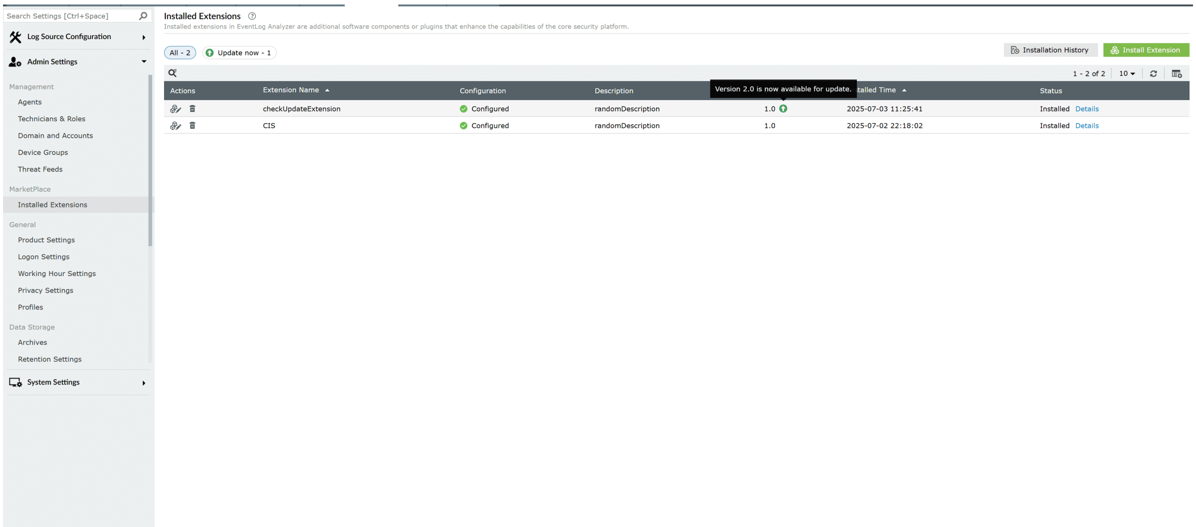
☑ Veeam Backup Repository Deleted

☑ Objects Excluded From Veeam Malware Detection



Updating an Extension

1. If an update is available for an installed extension, an Update icon will appear in the Installed Extensions table.

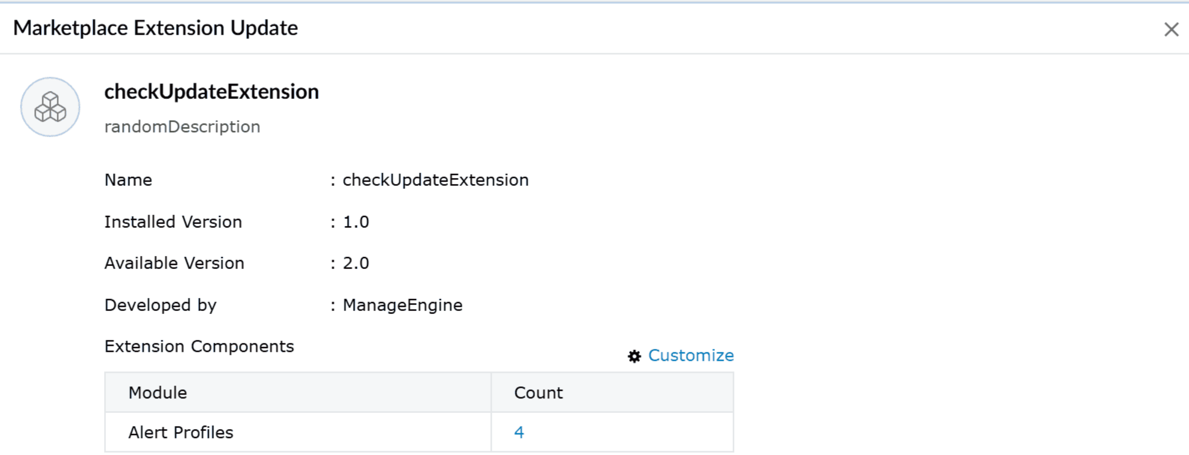


Installed Extensions

Installed extensions in EventLog Analyzer are additional software components or plugins that enhance the capabilities of the core security platform.

Version 2.0 is now available for update.

Actions	Extension Name	Configuration	Description		talled Time	Status
	checkUpdateExtension	Configured	randomDescription	1.0	2025-07-03 11:25:41	Installed Details
	CIS	Configured	randomDescription	1.0	2025-07-02 22:18:02	Installed Details



Marketplace Extension Update

checkUpdateExtension

randomDescription

Name	: checkUpdateExtension
Installed Version	: 1.0
Available Version	: 2.0
Developed by	: ManageEngine

Extension Components

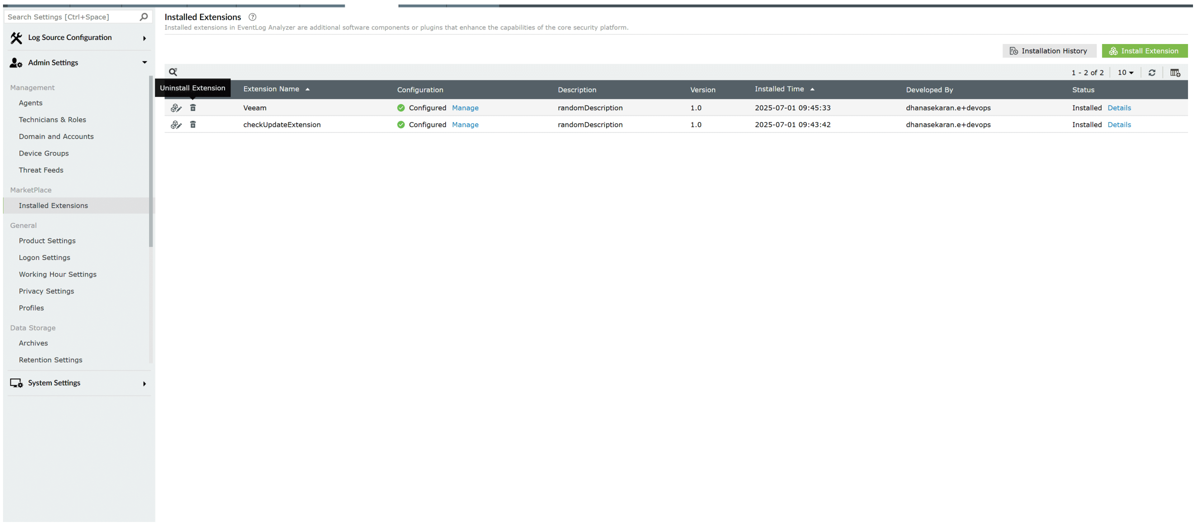
Module	Count
Alert Profiles	4

2. Click the Update icon to update the extension. You can customize the components that need to be updated.
3. The user can also manually update the extension by uploading the updated version, following the same steps used during extension installation.

Uninstalling an Extension

To uninstall an extension:

1. Click the Delete icon in the Manage Extensions table.
2. When an extension is deleted, all configurations associated with it will also be removed.



Installed Extensions

Installed extensions in EventLog Analyzer are additional software components or plugins that enhance the capabilities of the core security platform.

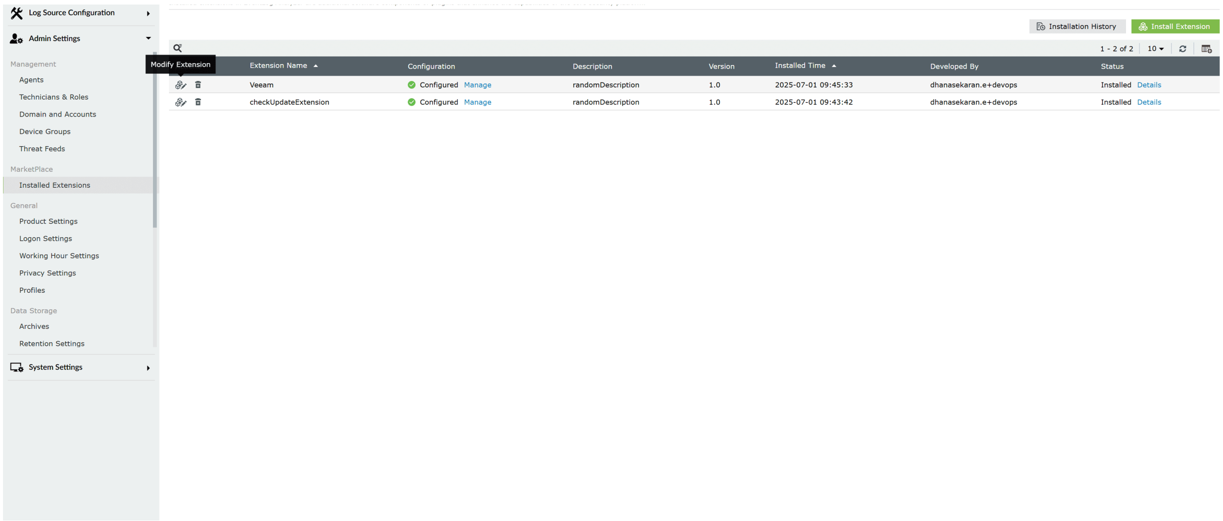
Extension Name	Configuration	Description	Version	Installed Time	Developed By	Status
Veeam	✓ Configured Manage	randomDescription	1.0	2025-07-01 09:45:33	dhanasekaran.e+devops	Installed Details
checkUpdateExtension	✓ Configured Manage	randomDescription	1.0	2025-07-01 09:43:42	dhanasekaran.e+devops	Installed Details

Modifying an Extension

After an extension has been customized and installed, users can reinstall components that were not initially installed by clicking the Modify icon in the Manage Extensions table.

Installed Extensions

Installed extensions in EventLog Analyzer are additional software components or plugins that enhance the capabilities of the core security platform.



	Extension Name	Configuration	Description	Version	Installed Time	Developed By	Status
	Veeam	✓ Configured Manage	randomDescription	1.0	2025-07-01 09:45:33	dhanasekaran.e+devops	Installed Details
	checkUpdateExtension	✓ Configured Manage	randomDescription	1.0	2025-07-01 09:43:42	dhanasekaran.e+devops	Installed Details

Extension Details

To view an extension's summary, usage statistics, installation history, and contents, click Details in the Manage Extensions table.

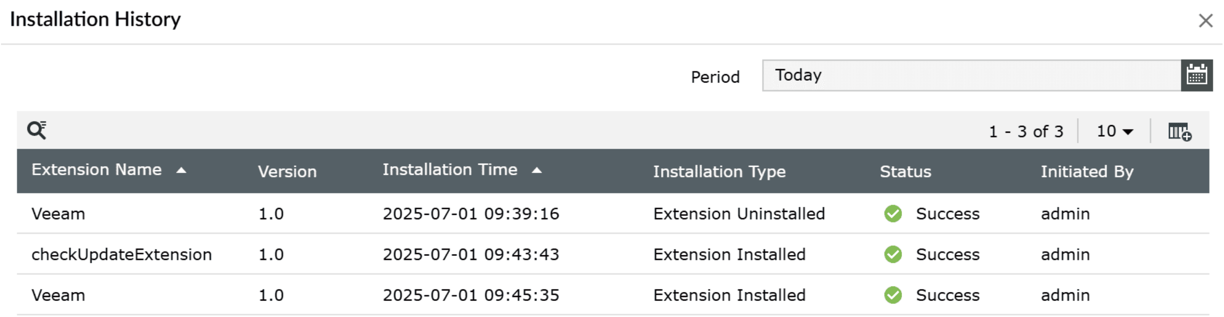
Extension Configurations

To configure applications or log sources for an extension:

1. Click Manage in the Manage Extensions table.
2. The configuration details window will open, allowing users to configure applications or log sources.

Installation History

To view the installation history of an extension, click the Installation History button.


Installation History

Period: Today

Extension Name	Version	Installation Time	Installation Type	Status	Initiated By
Veeam	1.0	2025-07-01 09:39:16	Extension Uninstalled	✓ Success	admin
checkUpdateExtension	1.0	2025-07-01 09:43:43	Extension Installed	✓ Success	admin
Veeam	1.0	2025-07-01 09:45:35	Extension Installed	✓ Success	admin

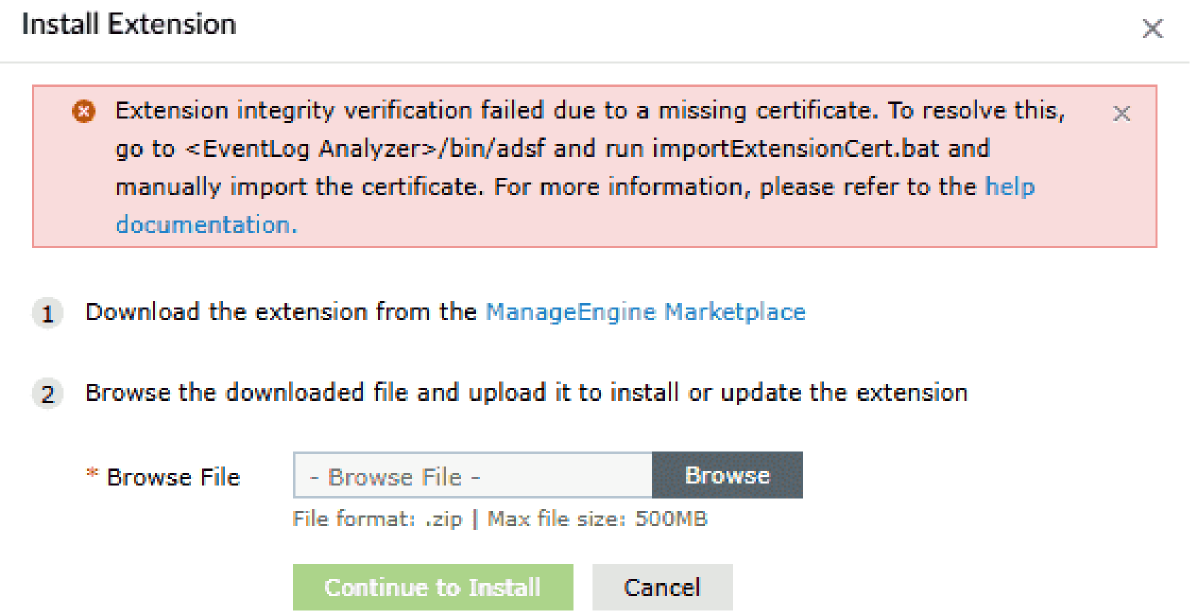
Troubleshooting Steps for Extension Installation Failure

Step 1: Verify that the extension is compatible with your application's version.
Step 2: Clear your browser cache and retry the installation.
Step 3: Check the failure status in the Installation History for more details.

Step 4: If the issue persists, contact our support team or the extension developer for further assistance.

Manual Certificate Sync if Automatic Certificate Download Fails:

- If automatic certificate synchronization fails due to network issues, extension integrity verification will not occur. In such cases, the following error will appear:



Install Extension

Extension integrity verification failed due to a missing certificate. To resolve this, go to <EventLog Analyzer>/bin/adsf and run importExtensionCert.bat and manually import the certificate. For more information, please refer to the help documentation.

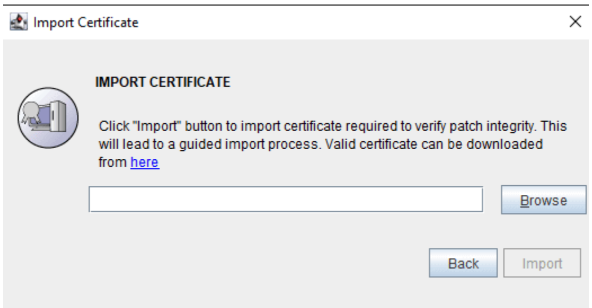
1 Download the extension from the ManageEngine Marketplace

2 Browse the downloaded file and upload it to install or update the extension

* Browse File - Browse File - Browse

File format: .zip | Max file size: 500MB

- To import the certificate manually, navigate to server_home/bin/adsf and execute importCertificate.bat (for Windows) or importCertificate.sh (for Linux/macOS).



Import Certificate

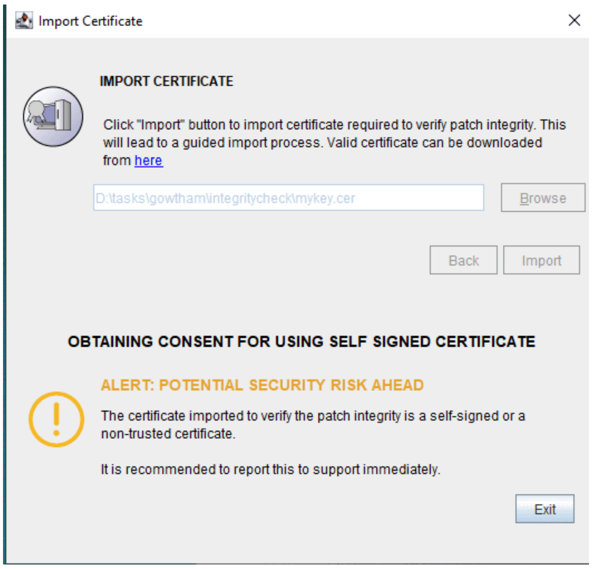
IMPORT CERTIFICATE

Click "Import" button to import certificate required to verify patch integrity. This will lead to a guided import process. Valid certificate can be downloaded from here

- The certificate download link will be available within the popup. Once downloaded, browse to the file and import the certificate.

ⓘ Note

Only the certificate downloaded from the provided link can be synced. Attempting to import any other certificate will result in an error.



Import Certificate

IMPORT CERTIFICATE

Click "Import" button to import certificate required to verify patch integrity. This will lead to a guided import process. Valid certificate can be downloaded from here

D:\tasks\gowtham\integritycheck\mykey.cer

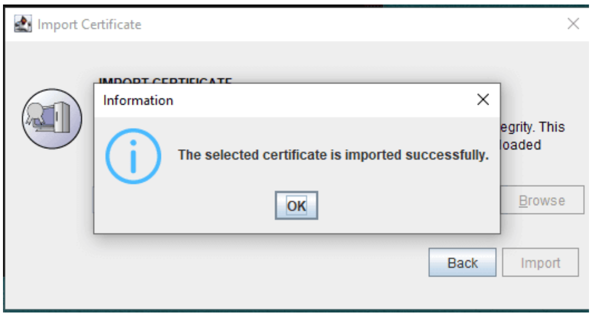
OBTAINING CONSENT FOR USING SELF SIGNED CERTIFICATE

ALERT: POTENTIAL SECURITY RISK AHEAD

The certificate imported to verify the patch integrity is a self-signed or a non-trusted certificate.

It is recommended to report this to support immediately.

- After importing the appropriate certificate, a success popup will appear.



Import Certificate

Information

The selected certificate is imported successfully.

- Once the certificate is successfully imported, you can retry installing the same extension.

6.1.2. Compliance Extensions

Last updated on: September 12, 2025

In this page

Overview

Compliance Extensions provide predefined support to help you adhere to industry standards and regulatory requirements. Below are the compliance extensions available for EventLog Analyzer.

Supported Compliance Extensions

- DORA (Digital Operational Resilience Act)
  - DORA is an EU regulation designed to enhance the financial sector’s ability to withstand cyber threats by establishing strict ICT risk management, incident reporting, and resilience testing requirements. To download the DORA extensions, visit marketplace.
- DPDP (Digital Personal Data Protection Act)
  - The DPDP Act is India’s comprehensive data protection law that governs the processing of personal data, ensuring user rights, lawful data handling, and corporate accountability. To download the DPDP extensions, visit marketplace.
- CJIS (Criminal Justice Information Services)
  - The CJIS Security Policy sets standards for protecting sensitive law enforcement data in the U.S., ensuring strict access control, encryption, and auditing requirements for agencies and service providers. To download the CJIS extensions, visit marketplace.
- CIS (Center for Internet Security Controls)
  - CIS Controls are a set of best practices and security guidelines designed to help organizations protect

    against cyber threats by implementing essential security measures and system hardening techniques. To download the CIS extensions, visit marketplace.

- Standard Framework for Education
    - The Standard Framework for Education provides guidelines and best practices for educational institutions to ensure compliance with relevant regulations and standards. To download the Standard Framework for Education extensions, visit marketplace.

Related resources

1. How to install an extension

6.1.3. Veeam

Last updated on: September 12, 2025

In this page

Overview

Veeam is a data protection and disaster recovery solution designed for modern IT environments. It provides backup, replication, and recovery capabilities for virtual, physical, cloud, and SaaS workloads.

Veeam extension scope

The Veeam extension for EventLog Analyzer is designed to enable seamless integration of log data from Veeam Backup & Replication or Veeam ONE into the EventLog Analyzer ecosystem. This extension provides features such as log collection, parsing, reporting, alerting, correlation, and advanced log search capabilities.

Audited Veeam events

Authentication and authorization

- MFA management
- Password and credential management
- Four-eyes authorization events

Identity management

- User and group management

Malware detection

- Malware detection configuration changes

- Malware detection configuration changes
- Malware detection session completion events
- Malware activity detection events
- Malware remediation actions

Configuration management

- Global network traffic rule changes
- Global VM exclusion changes
- General settings changes
- Host configurations

Jobs

- Job sessions history
- Job configurations
- Restore sessions history

Infrastructure management

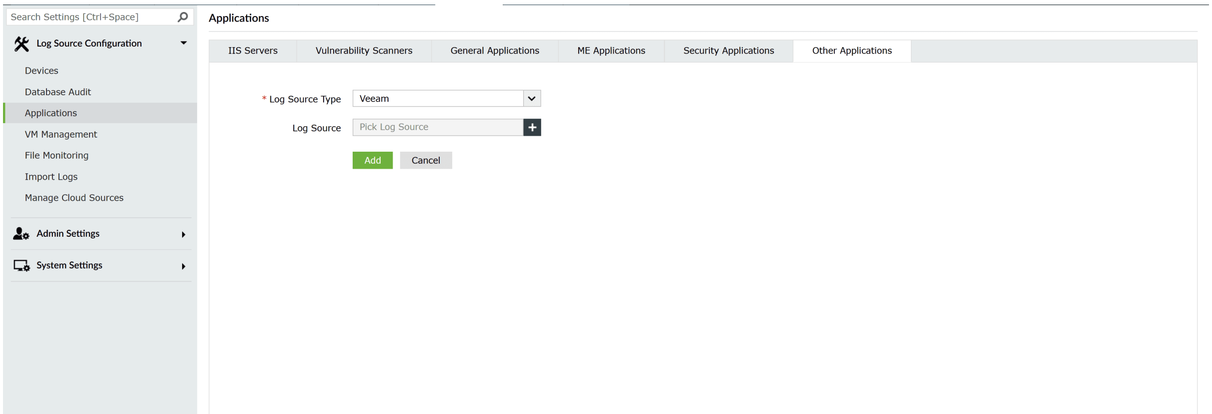
- Failover plan management
- Failover plan execution history
- Infrastructure location changes

Licensing

- License updates

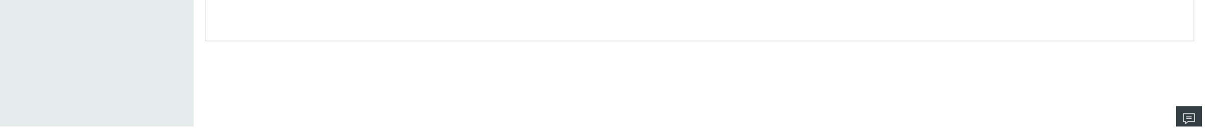
How to configure Veeam log source

1. After installing the Veeam extension, configure the log sources by navigating to Settings > Applications > Other Applications.
2. Select Veeam from the Log Source Type dropdown.
3. Click the + icon to add a new device.

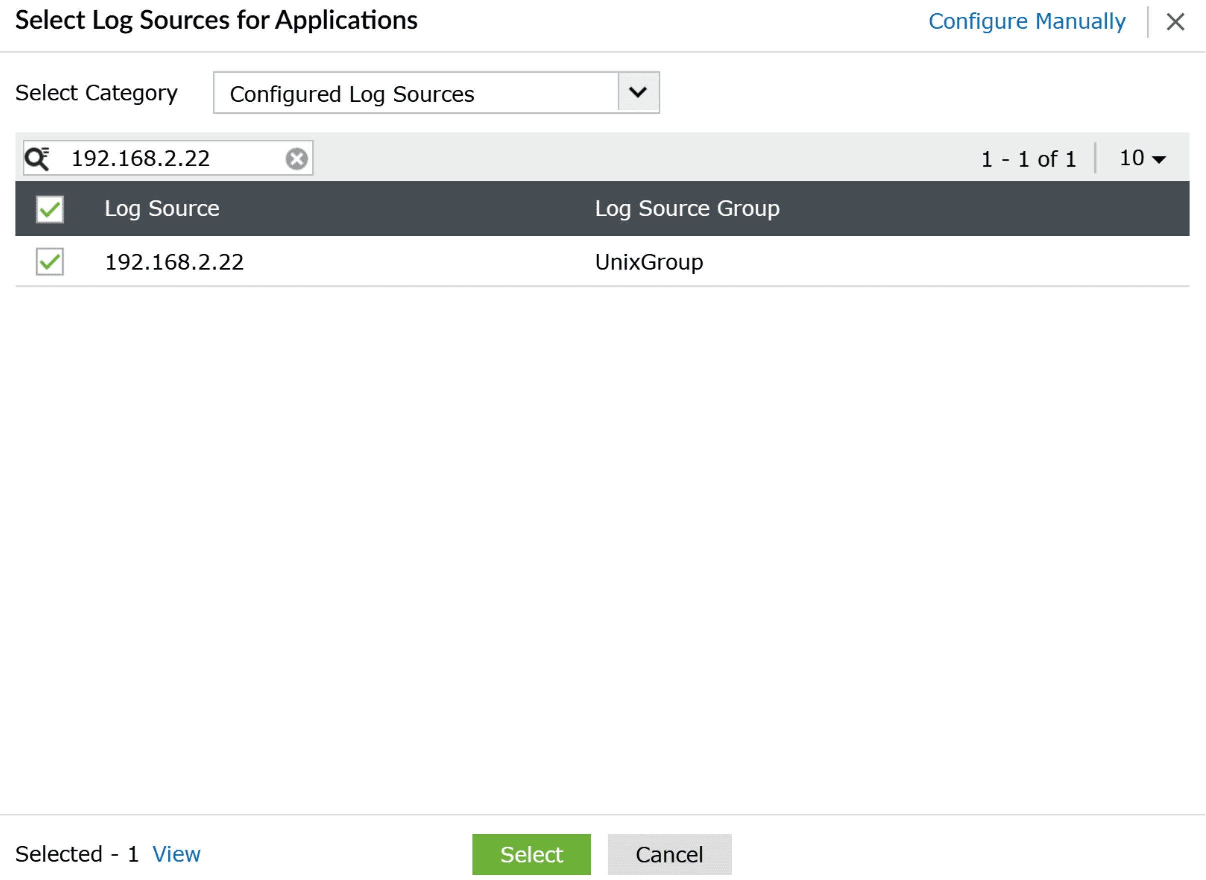


* Log Source Type: Veeam

Log Source: Pick Log Source +



4. Choose a pre-configured host where Veeam Backup & Replication Server or Veeam ONE Server is installed. If the host is not pre-configured, click Configure Manually and enter the hostname or IP.



Select Log Sources for Applications

Configure Manually

Select Category: Configured Log Sources

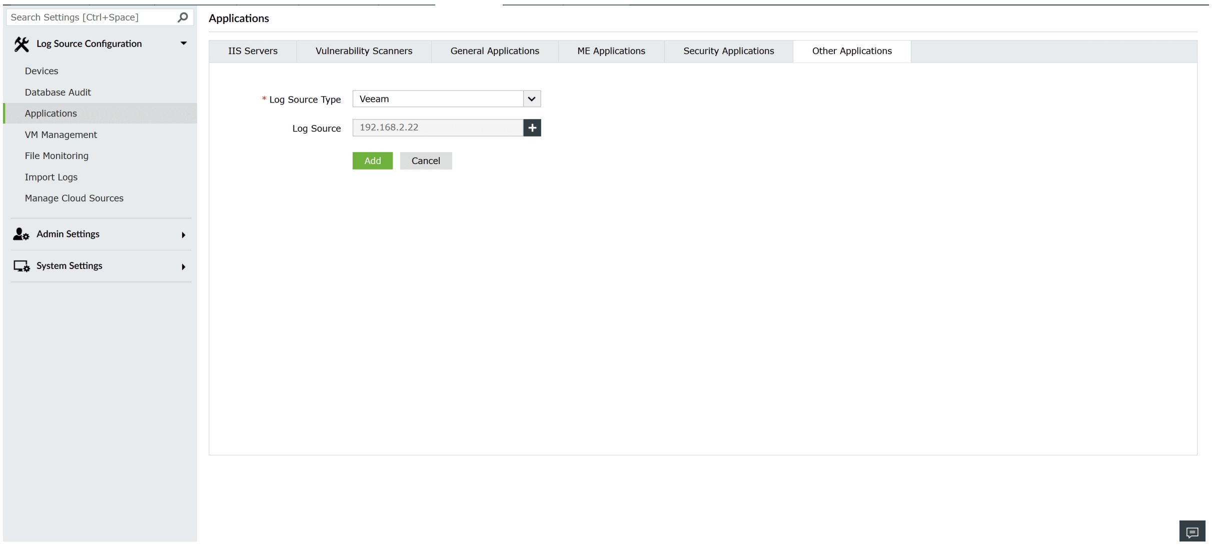
192.168.2.22

1 - 1 of 1 | 10

☑	Log Source	Log Source Group
☑	192.168.2.22	UnixGroup

Selected - 1 View

5. Click Add to save the configuration.



* Log Source Type: Veeam

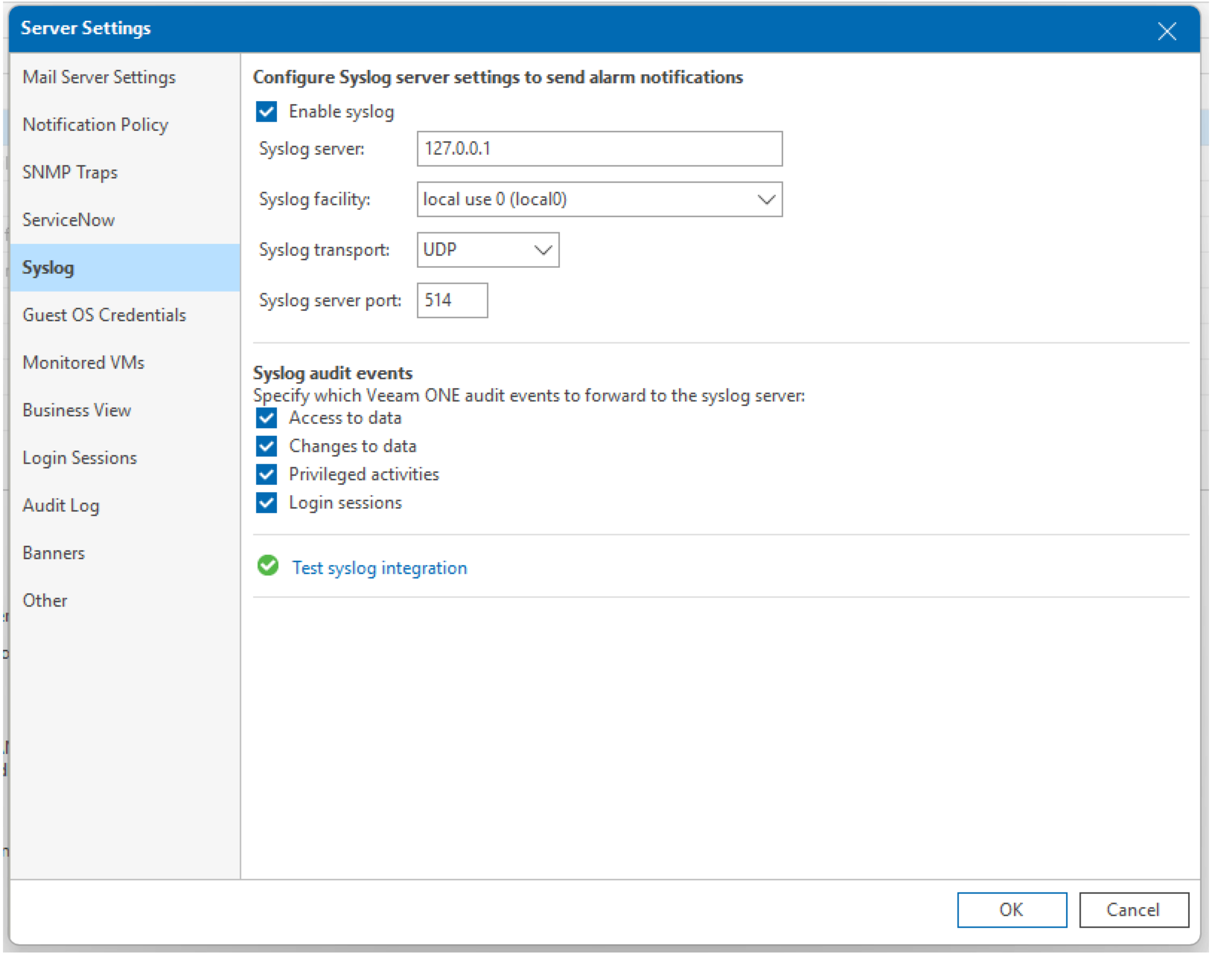
Log Source: 192.168.2.22

Enabling event forwarding

After configuring the log source, enable event forwarding in either Veeam ONE or Veeam Backup & Replication to send events to EventLog Analyzer. This requires a Veeam Data Platform Advanced or Premium license that supports syslog event forwarding.

Event forwarding in Veeam ONE

1. Open Veeam ONE Client and navigate to Server Settings > Syslog.
2. Check Enable Syslog.
3. In Syslog server, enter the Hostname or IP of the EventLog Analyzer server in the log source.
4. Select mail under the Syslog facility dropdown.
5. Choose UDP or TCP under the Syslog transport dropdown.
6. Enter a port in which the EventLog Analyzer server is listening for Syslogs.
7. Check all options under Syslog audit events to enable comprehensive search and reporting in EventLog Analyzer.
8. Click OK to save the configuration.



Configure Syslog server settings to send alarm notifications

☑ Enable syslog

Syslog server: 127.0.0.1

Syslog facility: local use 0 (local0)

Syslog transport: UDP

Syslog server port: 514

Syslog audit events

Specify which Veeam ONE audit events to forward to the syslog server:

☑ Access to data

☑ Changes to data

☑ Privileged activities

☑ Login sessions

✓ Test syslog integration

For detailed steps, refer to the official guide on Syslog integration in Veeam ONE.

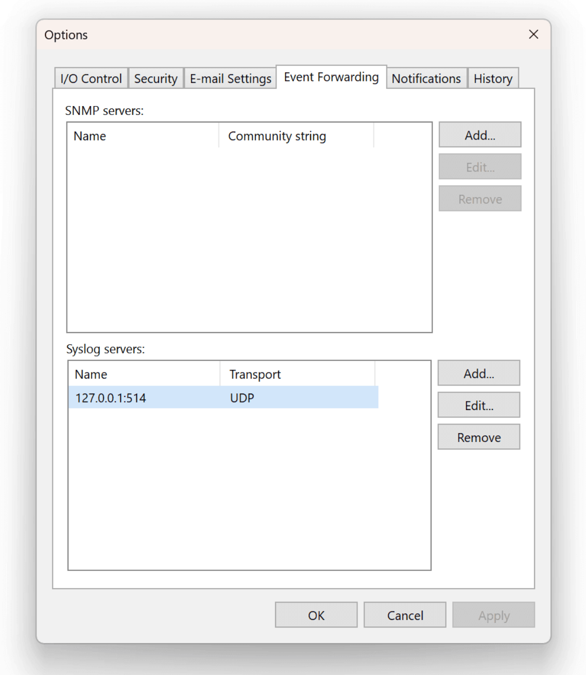
Event forwarding in Veeam Backup & Replication

1. Open Veeam Backup & Replication Console and go to Options > Event Forwarding.
2. Click Add under Syslog servers to configure a Syslog server.
3. In the Server field, provide the Hostname or IP of the EventLog Analyzer server.

4. Enter a port in which the EventLog Analyzer server is listening for Syslogs.

5. Select UDP or TCP under the Transport dropdown.

6. Click OK to add the syslog server, then click Apply to save changes.

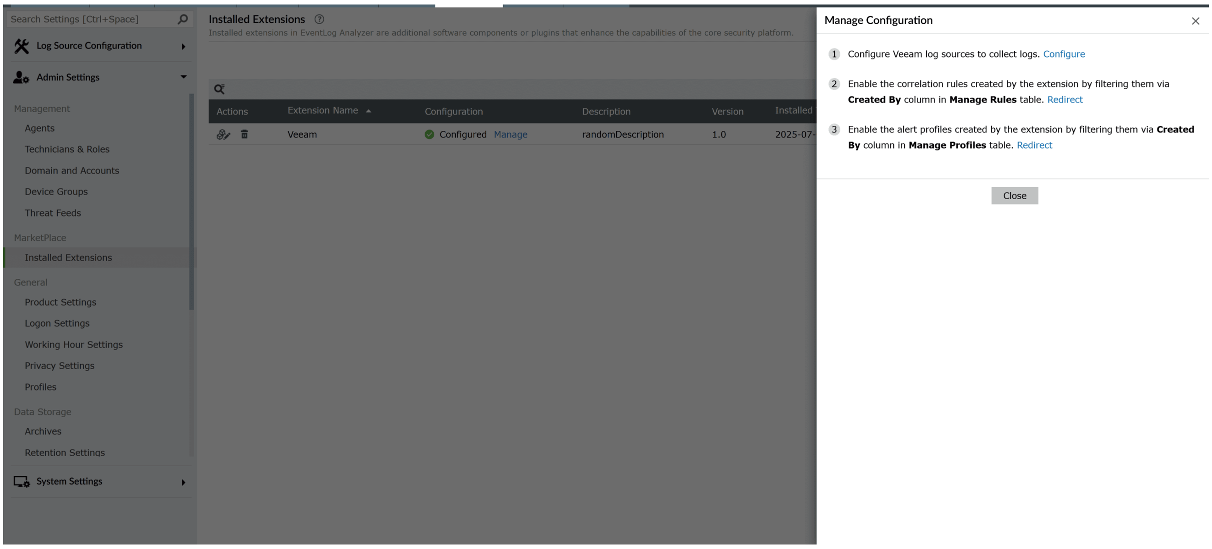


Name	Transport
127.0.0.1:514	UDP

For more details, refer to the official guide on Syslog integration in Veeam Backup & Replication.

Enabling correlation profiles

1. Go to Settings > Marketplace > Installed Extensions. Click Manage under Configuration to open the Manage Configuration page.



Installed extensions in EventLog Analyzer are additional software components or plugins that enhance the capabilities of the core security platform.

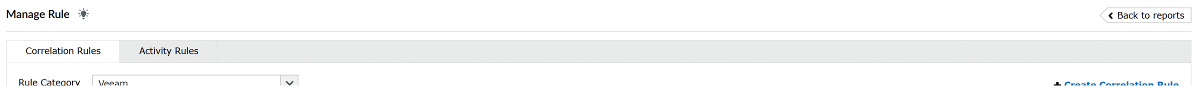
Actions	Extension Name	Configuration	Description	Version	Installed
	Veeam	Configured Manage	randomDescription	1.0	2025-07-

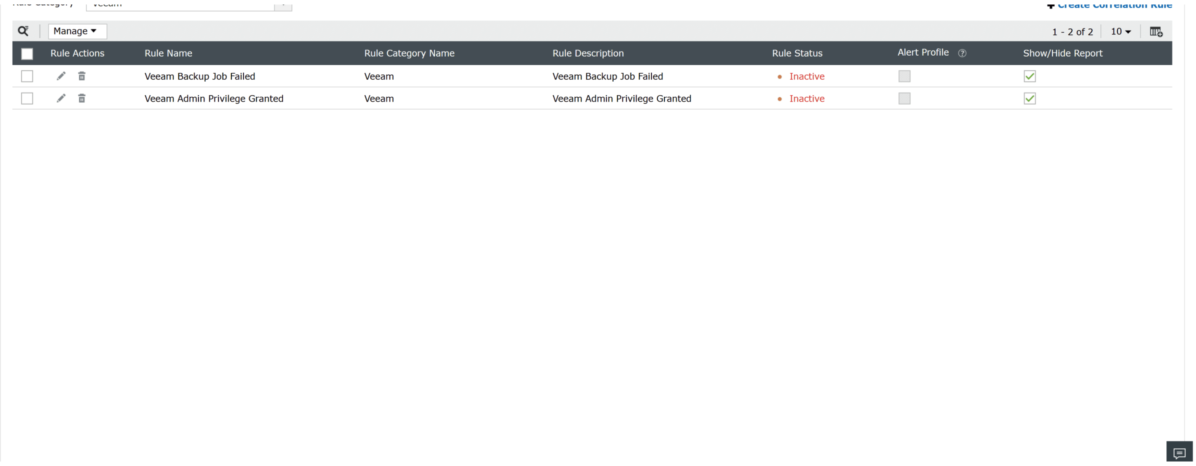
1 Configure Veeam log sources to collect logs. Configure

2 Enable the correlation rules created by the extension by filtering them via **Created By** column in **Manage Rules** table. Redirect

3 Enable the alert profiles created by the extension by filtering them via **Created By** column in **Manage Profiles** table. Redirect

2. Click Redirect next to Correlation Rules to open the Correlation tab. Select Veeam from the Rule Category selector to view the available correlation rules.



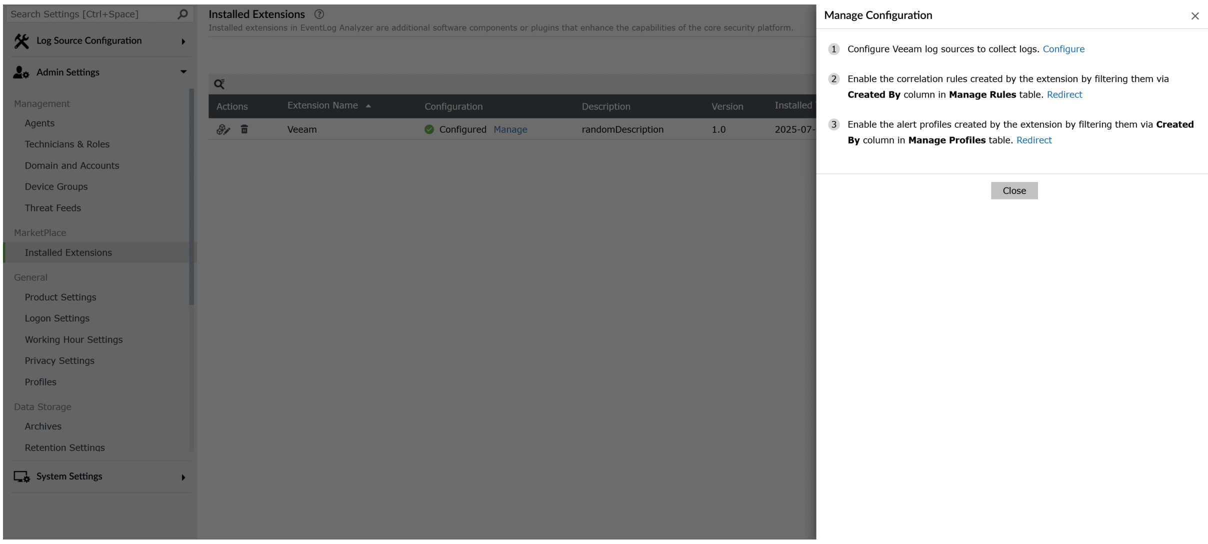


☐	Rule Actions	Rule Name	Rule Category Name	Rule Description	Rule Status	Alert Profile	Show/Hide Report
☐		Veeam Backup Job Failed	Veeam	Veeam Backup Job Failed	• Inactive	☐	☑
☐		Veeam Admin Privilege Granted	Veeam	Veeam Admin Privilege Granted	• Inactive	☐	☑

3. Review the available correlation rules and enable the required ones.

Enabling alert profiles

1. After configuring the log source, navigate to Settings > Marketplace > Installed Extensions. Click Manage under configuration to open the Manage Configuration page.



Installed Extensions

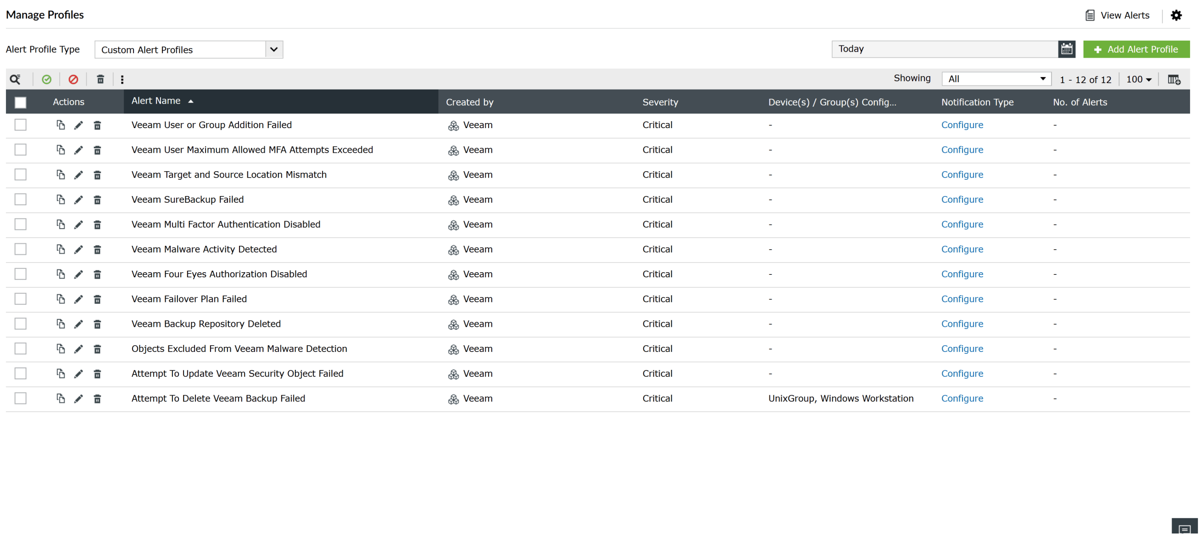
Installed extensions in EventLog Analyzer are additional software components or plugins that enhance the capabilities of the core security platform.

Actions	Extension Name	Configuration	Description	Version	Installed
	Veeam	Configured Manage	randomDescription	1.0	2025-07-

Manage Configuration

1. Configure Veeam log sources to collect logs. Configure
2. Enable the correlation rules created by the extension by filtering them via **Created By** column in **Manage Rules** table. Redirect
3. Enable the alert profiles created by the extension by filtering them via **Created By** column in **Manage Profiles** table. Redirect

2. Click Redirect next to Alert Profiles to navigate to the Alerts tab. Extension alert profiles appear under Custom Alert Profiles. Use the Created By column to identify Veeam alert profiles.


Manage Profiles

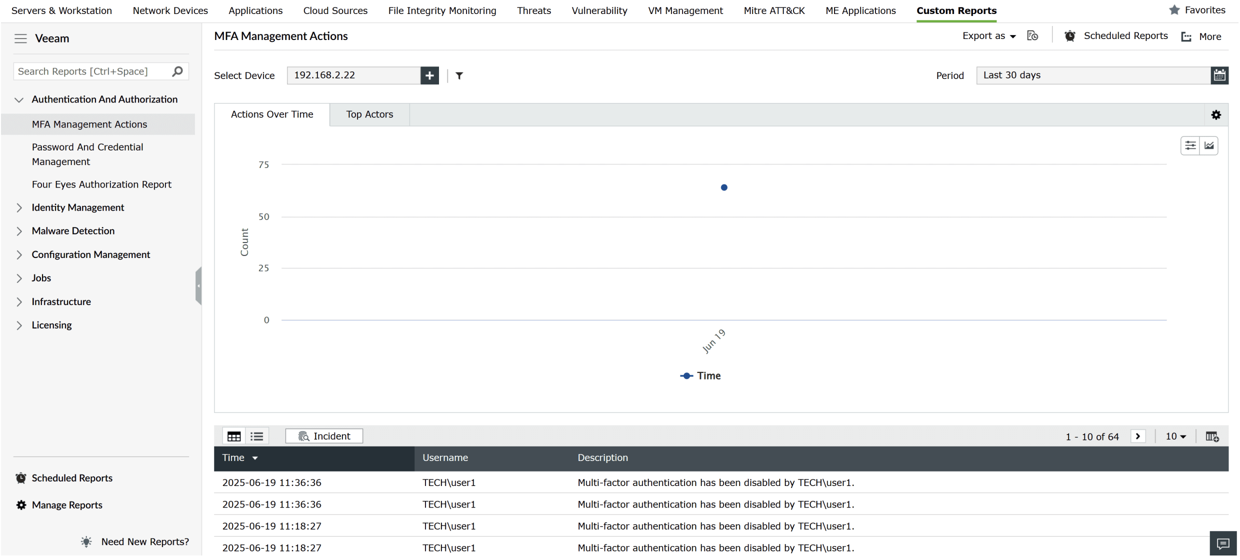
Alert Profile Type: Custom Alert Profiles

☐	Actions	Alert Name	Created by	Severity	Device(s) / Group(s) Config...	Notification Type	No. of Alerts
☐		Veeam User or Group Addition Failed	Veeam	Critical	-	Configure	-
☐		Veeam User Maximum Allowed MFA Attempts Exceeded	Veeam	Critical	-	Configure	-
☐		Veeam Target and Source Location Mismatch	Veeam	Critical	-	Configure	-
☐		Veeam SureBackup Failed	Veeam	Critical	-	Configure	-
☐		Veeam Multi Factor Authentication Disabled	Veeam	Critical	-	Configure	-
☐		Veeam Malware Activity Detected	Veeam	Critical	-	Configure	-
☐		Veeam Four Eyes Authorization Disabled	Veeam	Critical	-	Configure	-
☐		Veeam Failover Plan Failed	Veeam	Critical	-	Configure	-
☐		Veeam Backup Repository Deleted	Veeam	Critical	-	Configure	-
☐		Objects Excluded From Veeam Malware Detection	Veeam	Critical	-	Configure	-
☐		Attempt To Update Veeam Security Object Failed	Veeam	Critical	-	Configure	-
☐		Attempt To Delete Veeam Backup Failed	Veeam	Critical	UnixGroup, Windows Workstation	Configure	-

3. Browse the available alert profiles and enable the required ones.

Viewing Veeam reports

To view Veeam reports, navigate to the Reports tab and select Veeam under custom reports.



Select Device 192.168.2.22

Period Last 30 days

Time	Username	Description
2025-06-19 11:36:36	TECH\user1	Multi-factor authentication has been disabled by TECH\user1.
2025-06-19 11:36:36	TECH\user1	Multi-factor authentication has been disabled by TECH\user1.
2025-06-19 11:18:27	TECH\user1	Multi-factor authentication has been disabled by TECH\user1.
2025-06-19 11:18:27	TECH\user1	Multi-factor authentication has been disabled by TECH\user1.

Veeam events

Below is a list of Veeam events that EventLog Analyzer can track, helping you monitor backup and recovery activities effectively.

Instance ID	Event name
151	File Backup Job Finished
190	Backup Job Finished
194	File to Tape Job Finished
195	Tape Erase Job Finished
199	Tape Export Job Finished
200	Tape Copy Job Finished
203	Tape Eject Job Finished

205	Move To Media Pool Job Finished
206	Delete From Library Job Finished
208	Tape Import Job Finished
23010	Job Created
23050	Job Settings Updated
23090	Job Deleted
23110	Objects for Job Added
23130	Objects for Job Changed
23210	SureBackup Job Created
23220	SureBackup Job Settings Updated
23230	SureBackup Job Deleted
23310	Objects for SureBackup Job Added
23320	Objects for SureBackup Job Deleted
23410	Job Assigned as Secondary Destination
23420	Job No Longer Used as Secondary Destination
23440	Tape Job Created
23450	Tape Job Settings Updated
23490	Tape Job Deleted
23510	Objects for Tape Job Added

23520	Objects for Tape Job Deleted
23530	Objects for Tape Job Changed
24010	License Installed
24030	License Expired
24050	License Support Expired
24060	License Grace Period Started
24070	License Limit Exceeded
24080	License Removed
25300	Credential Record Added
25400	Credential Record Updated
25500	Credential Record Deleted
25900	Failover Plan Created
26000	Failover Plan Settings Updated
26010	Target Location Does Not Match Source Location
26100	Failover Plan Deleted
26110	Failover Plan Failed
26600	Failover Plan Started
26700	Failover Plan Stopped

28300	Host Added
28400	Host Settings Updated
28500	Host Deleted
31000	General Settings Updated
31100	Global Settings for Network Traffic Rules Updated
31200	User or Group Added
31210	Adding User or Group Failed
31400	User or Group Deleted
31600	Encryption Password Added
31700	Encryption Password Updated
31800	Encryption Password Deleted
31900	SSH Credentials Changed
32120	Objects for Job Deleted
32300	Global Network Traffic Rules Added
32400	Global Network Traffic Rules Deleted
32500	Global Network Traffic Rules Updated
32600	Preferred Networks Updated
32700	Preferred Networks Added

32800	Preferred Networks Deleted
36022	Backup Job for Application Backup Policy Finished
36026	Log Backup Job for Application Backup Policy Finished
390	SureBackup Job Finished
40200	Multi-Factor Authentication Enabled
40201	Multi-Factor Authentication Disabled
40202	Multi-Factor Authentication Token Revoked
40203	Multi-Factor Authentication for User Enabled
40204	Multi-Factor Authentication for User Disabled
40206	Allowed Attempts for Multi-Factor Authentication Exceeded
40290	Restore Session Finished
40400	Global VM Exclusions Added
40500	Global VM Exclusions Deleted
40600	Global VM Exclusions Changed
40700	Configuration Backup Job Finished
40900	Location Added
40901	Location Settings Updated
40902	Location Deleted

40903	Object Location Changed
41600	Malware Activity Detected
41710	Health Check Job Finished
41800	Attempt to Delete Backup Failed
41810	Attempt To Update Security Object Failed
42210	Malware Detection Session Finished
42260	Objects Added to Malware Detection Exclusions
42270	Objects Deleted from Malware Detection Exclusions
42280	Malware Detection Exclusions List Updated
42290	Malware Detection Settings Updated
42400	Four-Eyes Authorization Enabled
42401	Four-Eyes Authorization Disabled
42402	Four-Eyes Authorization Request Created
42403	Four-Eyes Authorization Request Approved
42404	Four-Eyes Authorization Request Rejected
42405	Four-Eyes Authorization Request Expired
451	File Backup Copy Job Finished
490	Backup Copy Job Finished
590	File Copy Job Finished

592	VM Copy Job Finished
610	Quick Migration Finished
28200	Backup Repository Deleted
42260	Objects Added to Malware Detection Exclusions
41610	Object Marked as Clean
42220	Restore Point Marked as Infected
42230	Restore Point Marked as Clean

Related resources

1. How to install an extension

6.1.4. Dropbox

Last updated on: September 12, 2025

Dropbox is a cloud-based file storage and collaboration platform that enables users to securely store, sync, and share files across multiple devices. It provides businesses and individuals with easy access to files from anywhere, ensuring seamless collaboration and data protection.

Dropbox extension scope

The Dropbox Audit Log Monitoring Extension empowers organizations to monitor continuously and analyze Dropbox audit logs, ensuring comprehensive visibility into critical activities. By capturing and evaluating events such as user actions, access patterns, and security changes, this extension helps mitigate risks, ensure compliance, and enhance operational efficiency. It enables organizations to detect unusual login attempts, identify potential insider threats, and stay ahead of evolving security challenges.

Audited Dropbox events

Security events

- Ransomware and admin alerts
- Authentications and sessions
- Passwords and TFA
- Encryption and key management

File and folder events

- File and folder operations
- File request and transfer events

Integrations and apps

- Integrations and apps events

Members and groups

- Invite link activity
- Member management activity
- Group management activity

Device management

- Device link and status Changes

Legal holds

- Legal hold events

Reports management

- Report management activity

Sharing

- Shared content
- Link actions

Team policies

- Web session policy
- Password and TFA policy
- Sharing and smart sync policy
- Signature policy
- Member and team policy
- Third party policy
- File and backup policy
- Governance policy

Team profile

- Data residency migration
- Team profile customization actions

Signatures

- Signature management Activity

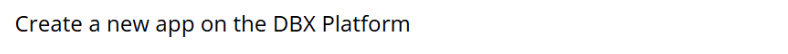
Trusted teams

- Enterprise management activity
- Team merge activity

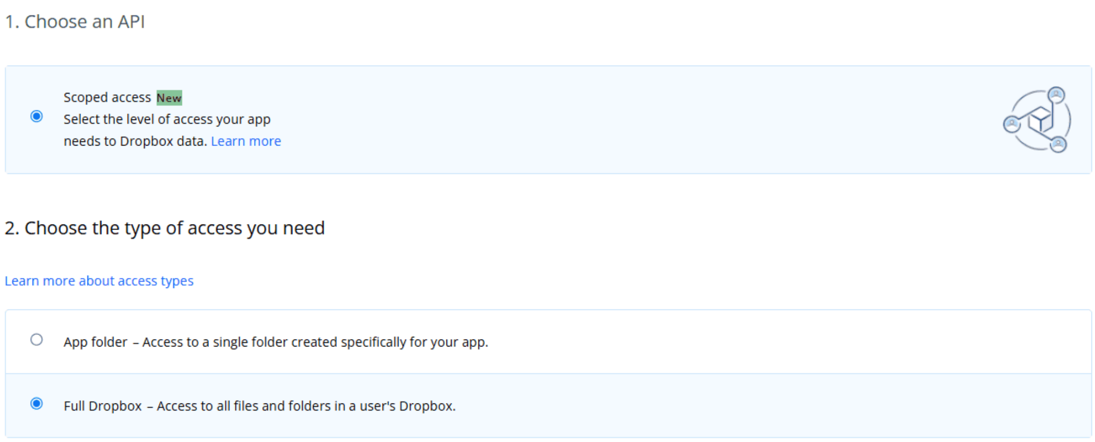
Configuring Dropbox integration

Setting up a Dropbox account and application

1. Sign in to your Dropbox account and navigate to the Dropbox Developers Console.
2. Click Create New App and select Scoped Access.
3. Choose Full Dropbox Access as the access type.



Create a new app on the DBX Platform



1. Choose an API

● Scoped access New
Select the level of access your app needs to Dropbox data. Learn more

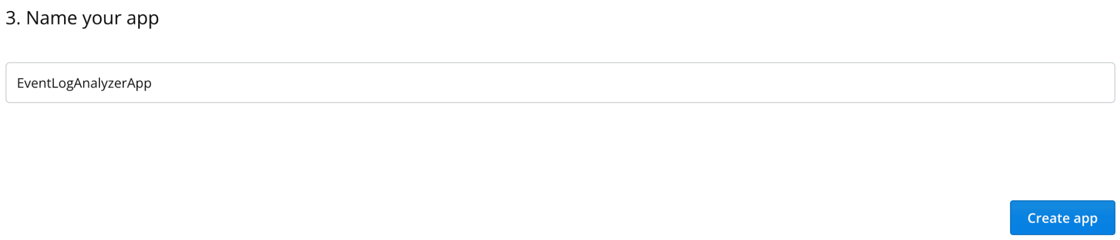
2. Choose the type of access you need

Learn more about access types

○ App folder – Access to a single folder created specifically for your app.

● Full Dropbox – Access to all files and folders in a user's Dropbox.

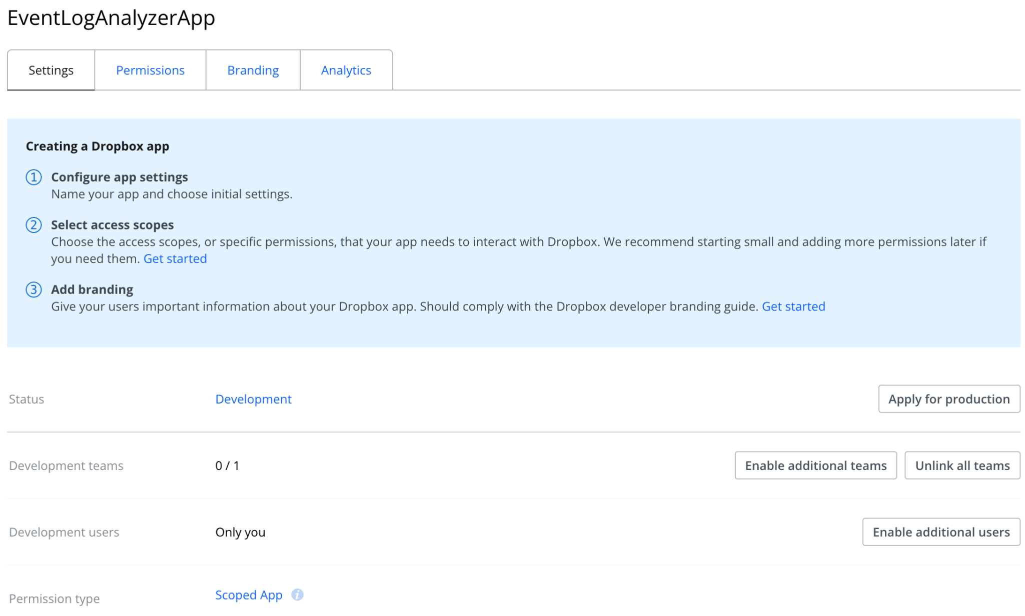
4. Provide a name for your app, agree to the Dropbox terms and conditions, and then click Create App.



3. Name your app

EventLogAnalyzerApp

5. Once the app is created, the App Settings page will be displayed.



EventLogAnalyzerApp

Creating a Dropbox app

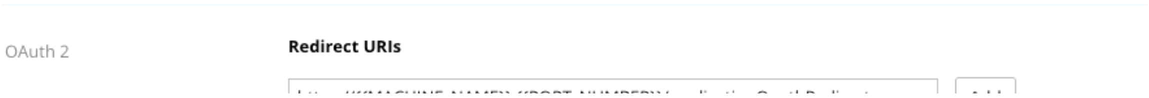
① **Configure app settings**
Name your app and choose initial settings.

② **Select access scopes**
Choose the access scopes, or specific permissions, that your app needs to interact with Dropbox. We recommend starting small and adding more permissions later if you need them. Get started

③ **Add branding**
Give your users important information about your Dropbox app. Should comply with the Dropbox developer branding guide. Get started

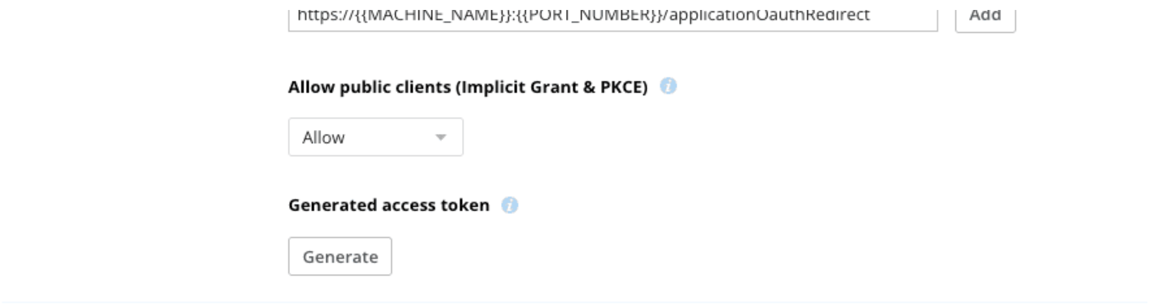
Status	Development	Apply for production
Development teams	0 / 1	Enable additional teams Unlink all teams
Development users	Only you	Enable additional users
Permission type	Scoped App	

6. In the App Settings tab, enter the specified Redirect URL in the Redirect URLs textbox. Replace {{MACHINE_NAME}} and {{PORT_NUMBER}} with the actual machine name and the port number where the EventLog Analyzer instance is running.



OAuth 2

Redirect URIs



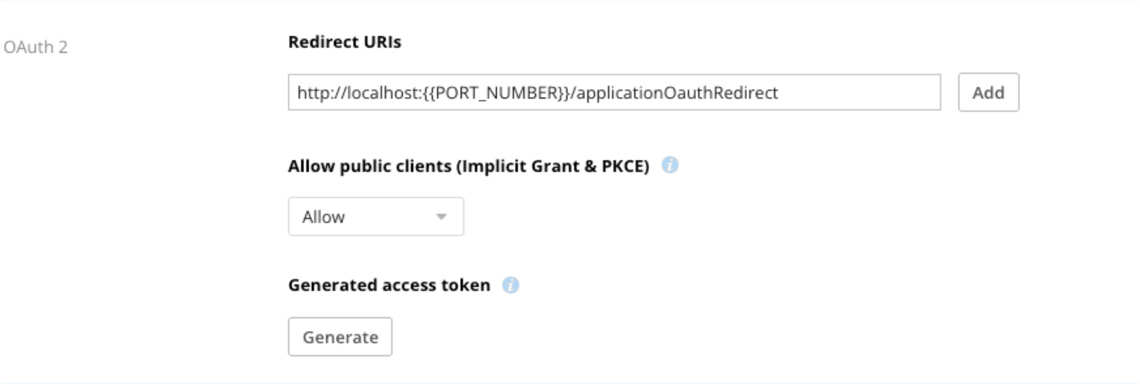
https://{{MACHINE_NAME}}:{{PORT_NUMBER}}/applicationOauthRedirect

Allow public clients (Implicit Grant & PKCE)

Allow

Generated access token

- If EventLog Analyzer is running in HTTP mode, use localhost as the machine name along with the appropriate {{PORT_NUMBER}}.



OAuth 2

Redirect URIs

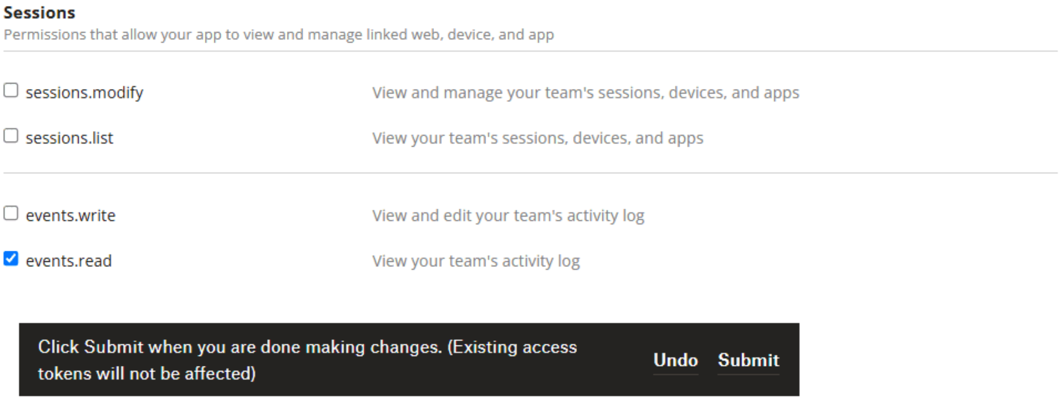
http://localhost:{{PORT_NUMBER}}/applicationOauthRedirect

Allow public clients (Implicit Grant & PKCE)

Allow

Generated access token

7. Navigate to the Permissions tab, scroll down, and enable team_data.member, events.read, members.read, files.metadata.read, sharing.read and sessions.list permissions.



Sessions

Permissions that allow your app to view and manage linked web, device, and app

□ sessions.modify	View and manage your team's sessions, devices, and apps
□ sessions.list	View your team's sessions, devices, and apps
□ events.write	View and edit your team's activity log
☑ events.read	View your team's activity log

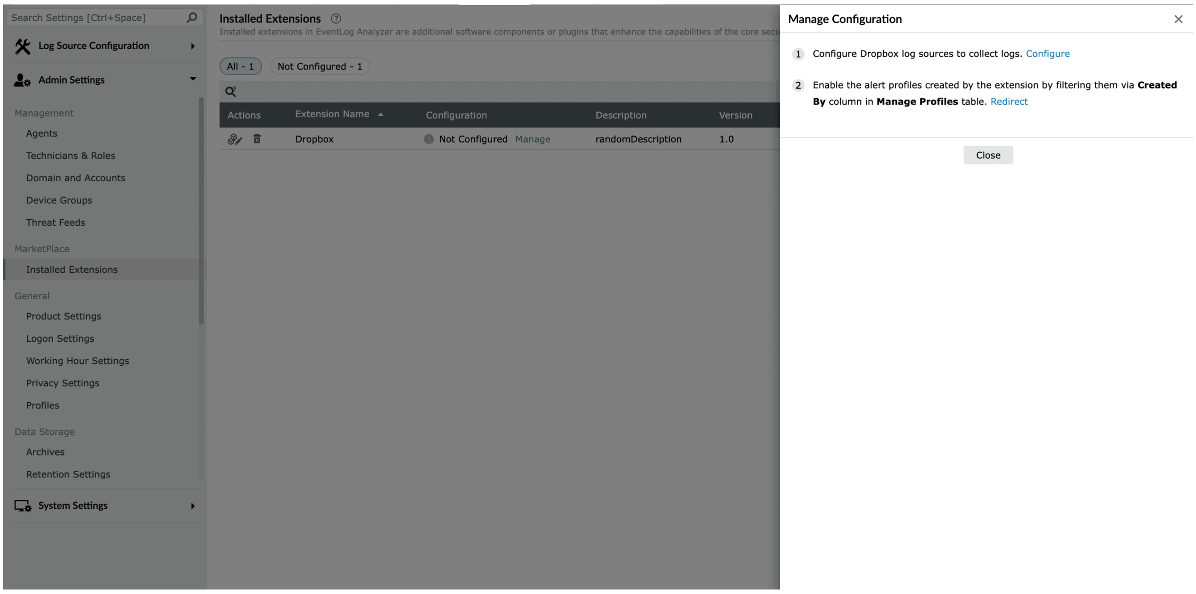
Click Submit when you are done making changes. (Existing access tokens will not be affected)

8. Click Submit to complete the Dropbox app configuration.
9. From the Settings tab, copy the Client ID and Client Secret values from the App ID and App Secret fields. These will be needed later while configuring Dropbox in EventLog Analyzer.

Configuring Dropbox in EventLog Analyzer

- In EventLog Analyzer, navigate to Settings → Marketplace.
- Locate and install the Dropbox Extension from the Marketplace.
- To verify installation, go to Settings → Marketplace → Installed Extensions and ensure Dropbox is listed.

- Click Manage under the Dropbox extension to open the Manage Configuration page.



Installed Extensions

Installed extensions in EventLog Analyzer are additional software components or plugins that enhance the capabilities of the core secu

All - 1 | Not Configured - 1

Actions	Extension Name	Configuration	Description	Version
	Dropbox	Not Configured Manage	randomDescription	1.0

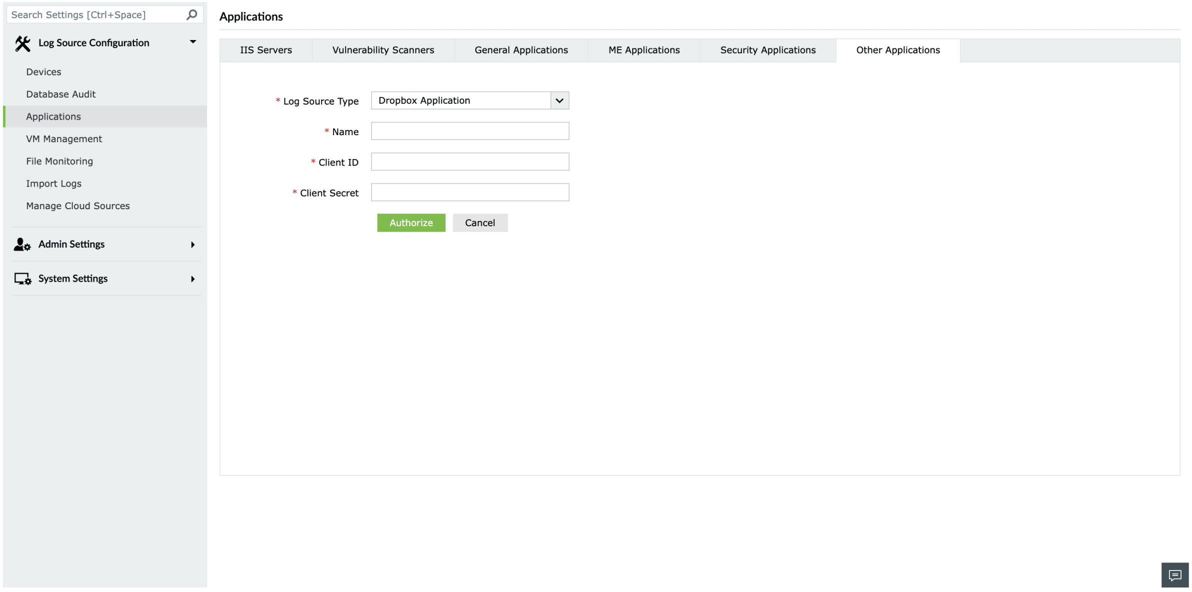
Manage Configuration

1 Configure Dropbox log sources to collect logs. Configure

2 Enable the alert profiles created by the extension by filtering them via **Created By** column in **Manage Profiles** table. Redirect

Close

- Click Configure to open the configuration page or navigate to Settings → Applications → Other Applications .



Applications

* Log Source Type: Dropbox Application

* Name

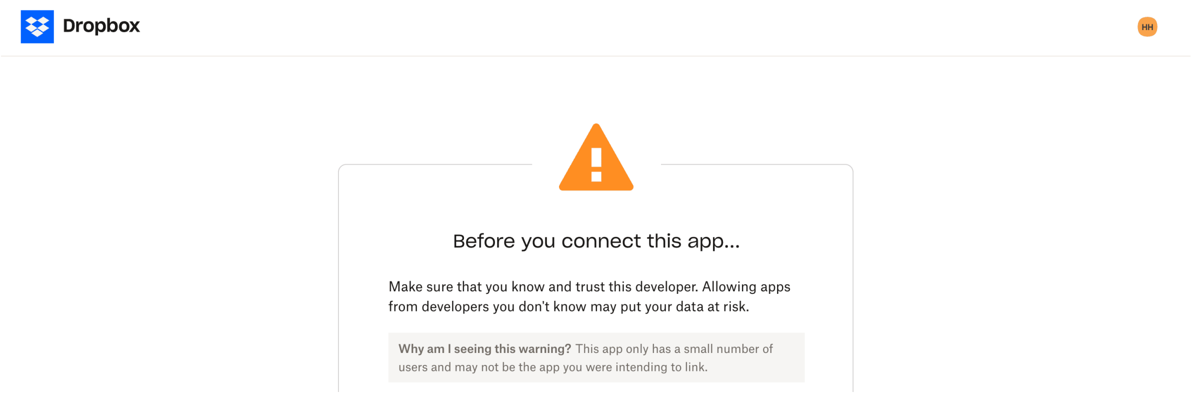
* Client ID

* Client Secret

Authorize | Cancel

- Enter the Client ID and Client Secret obtained from the Dropbox Developer Console.

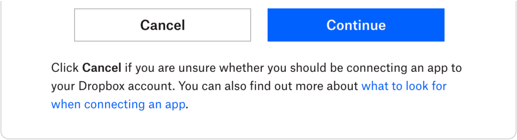
- Click Authorize. A pop-up will appear requesting consent.



Before you connect this app...

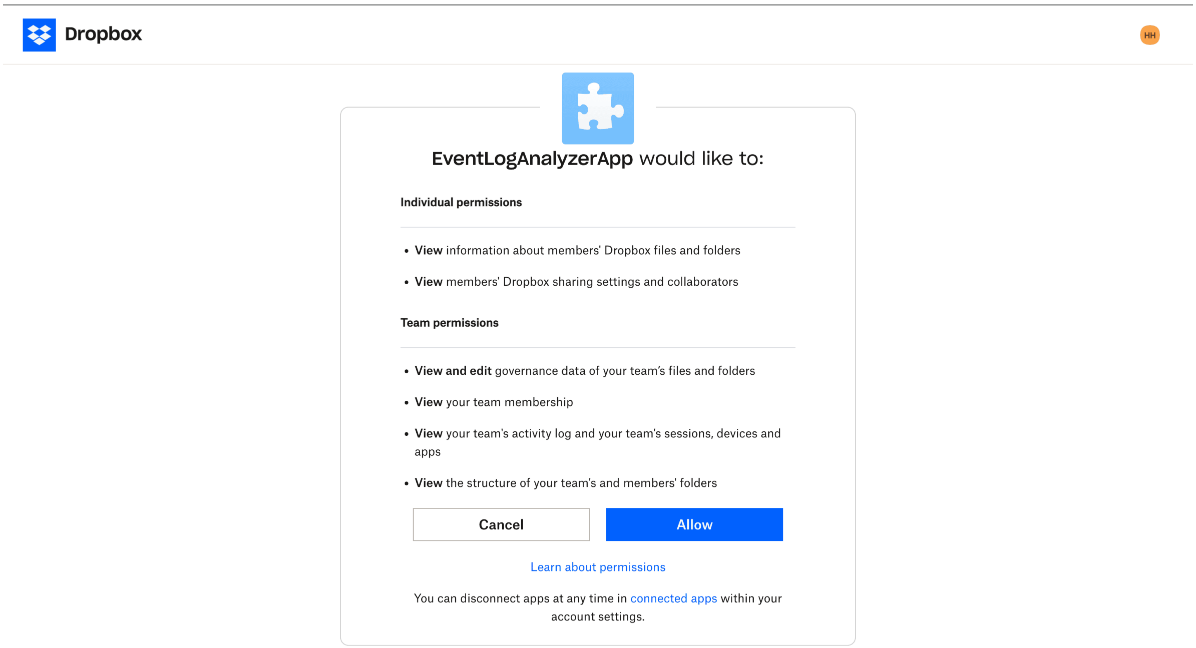
Make sure that you know and trust this developer. Allowing apps from developers you don't know may put your data at risk.

Why am I seeing this warning? This app only has a small number of users and may not be the app you were intending to link.



Click **Cancel** if you are unsure whether you should be connecting an app to your Dropbox account. You can also find out more about what to look for when connecting an app.

- Accept the consent request to complete the configuration.



EventLogAnalyzerApp would like to:

Individual permissions

- **View** information about members' Dropbox files and folders
- **View** members' Dropbox sharing settings and collaborators

Team permissions

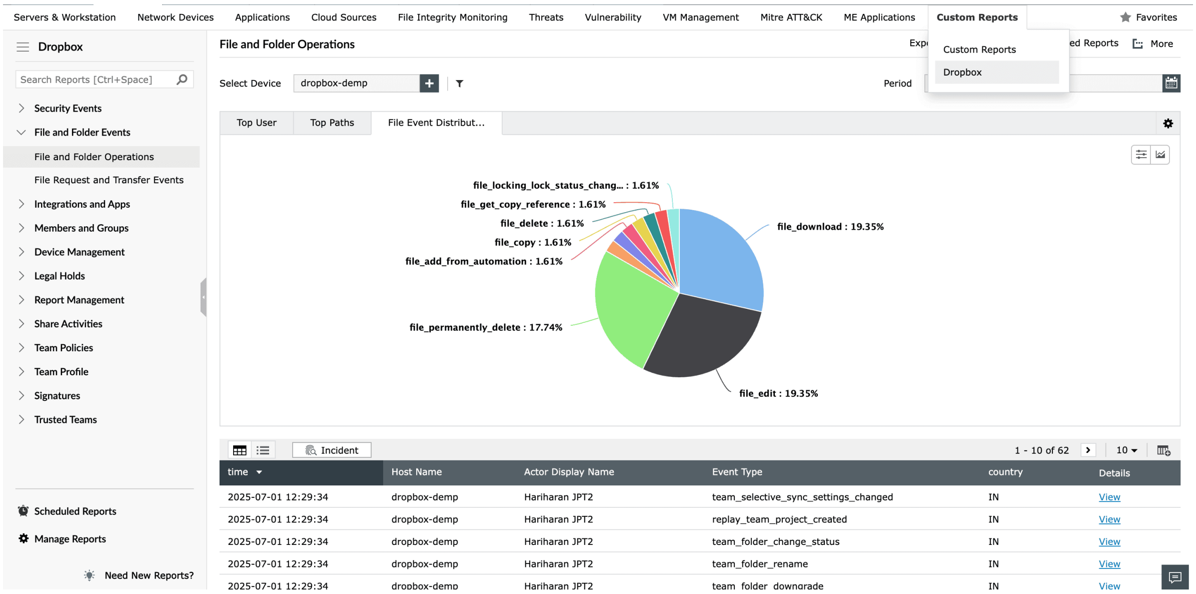
- **View and edit** governance data of your team's files and folders
- **View** your team membership
- **View** your team's activity log and your team's sessions, devices and apps
- **View** the structure of your team's and members' folders

Learn about permissions

You can disconnect apps at any time in connected apps within your account settings.

Accessing Dropbox reports

- Navigate to Reports → Custom Reports → Dropbox to view Dropbox-related reports.

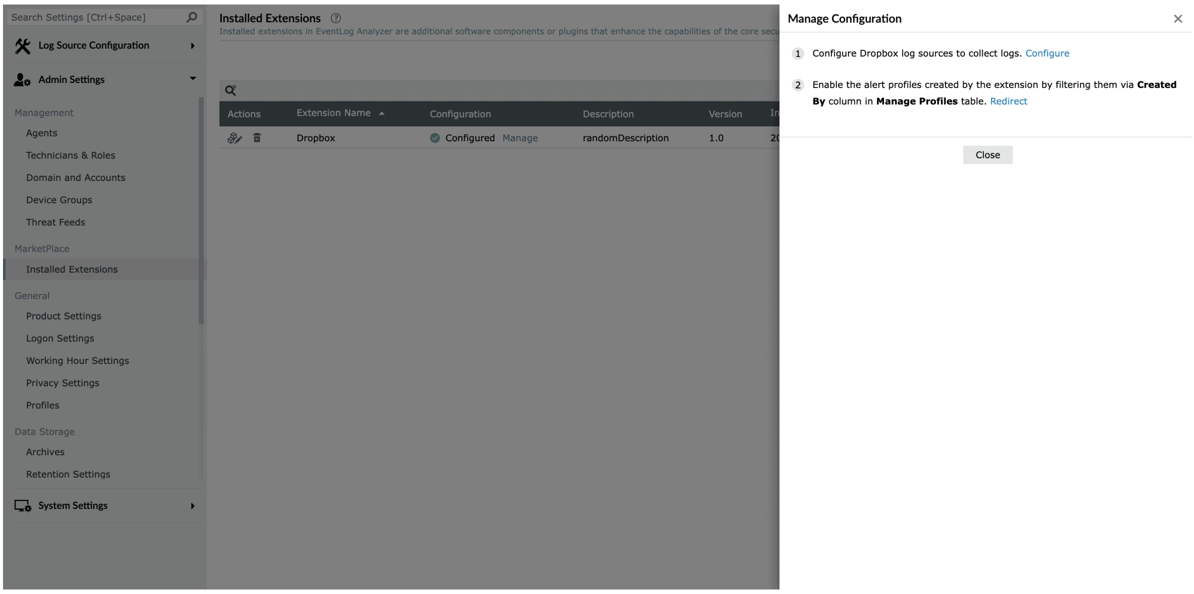


Select Device: dropbox-demp

time	Host Name	Actor Display Name	Event Type	country	Details
2025-07-01 12:29:34	dropbox-demp	Hariharan JPT2	team_selective_sync_settings_changed	IN	View
2025-07-01 12:29:34	dropbox-demp	Hariharan JPT2	replay_team_project_created	IN	View
2025-07-01 12:29:34	dropbox-demp	Hariharan JPT2	team_folder_change_status	IN	View
2025-07-01 12:29:34	dropbox-demp	Hariharan JPT2	team_folder_rename	IN	View
2025-07-01 12:29:34	dropbox-demp	Hariharan JPT2	team_folder_downgrade	IN	View

Configuring Dropbox alerts

- After configuring the log source, go to Settings → Marketplace → Installed Extensions.
- Click Manage under the Dropbox extension to open the Manage Configuration page.



Installed Extensions

Installed extensions in EventLog Analyzer are additional software components or plugins that enhance the capabilities of the core secu

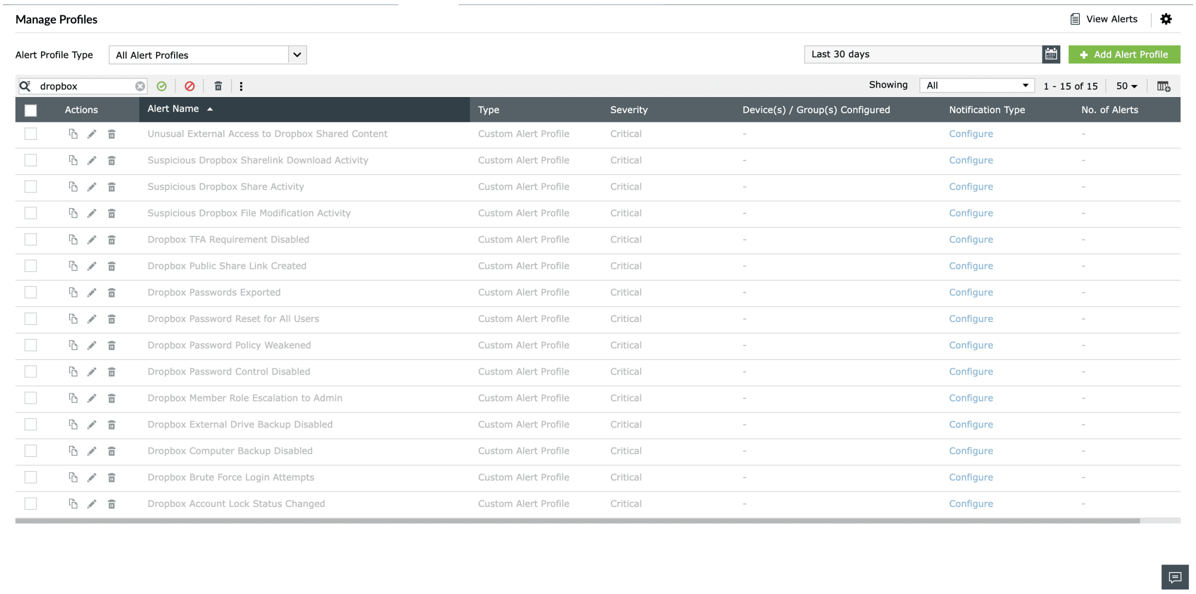
Actions	Extension Name	Configuration	Description	Version	In
	Dropbox	Configured Manage	randomDescription	1.0	20

Manage Configuration

1 Configure Dropbox log sources to collect logs. Configure

2 Enable the alert profiles created by the extension by filtering them via **Created By** column in **Manage Profiles** table. Redirect

- Click Redirect next to Alert Profiles to open the Alerts tab. Browse the available Dropbox alert profiles and enable the required ones.

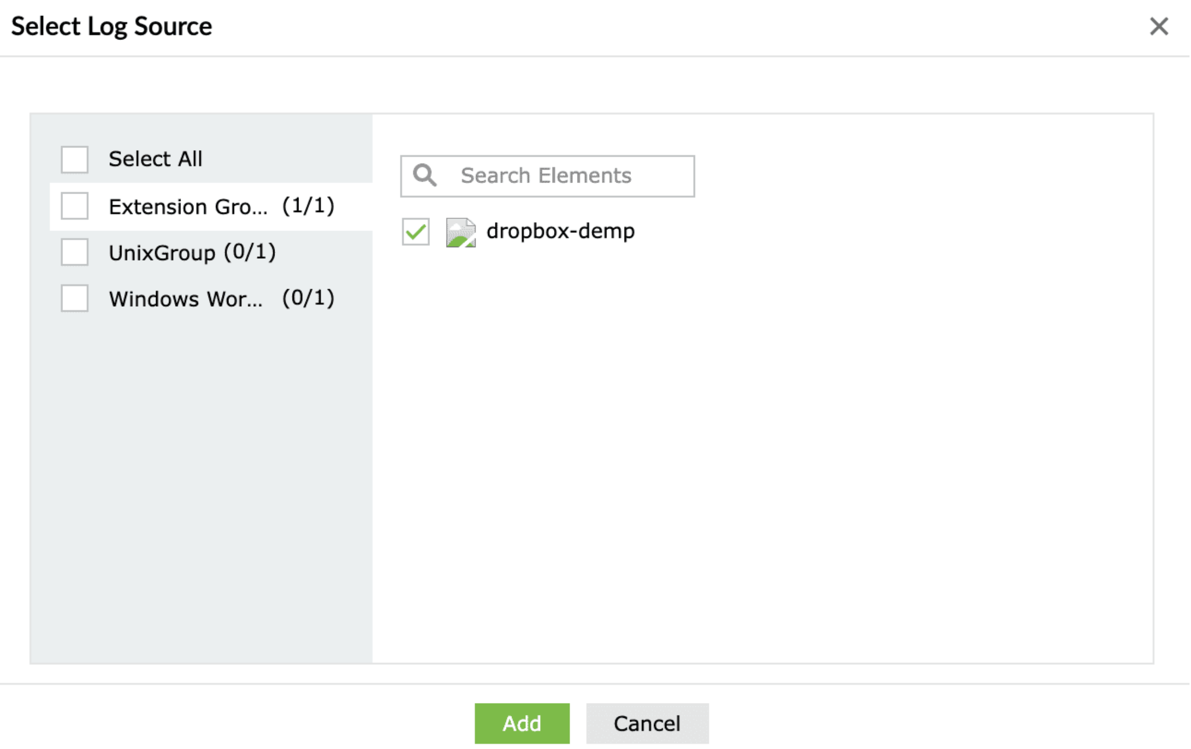


Actions	Alert Name	Type	Severity	Device(s) / Group(s) Configured	Notification Type	No. of Alerts
	Unusual External Access to Dropbox Shared Content	Custom Alert Profile	Critical	-	Configure	-
	Suspicious Dropbox Sharelink Download Activity	Custom Alert Profile	Critical	-	Configure	-
	Suspicious Dropbox Share Activity	Custom Alert Profile	Critical	-	Configure	-
	Suspicious Dropbox File Modification Activity	Custom Alert Profile	Critical	-	Configure	-
	Dropbox TFA Requirement Disabled	Custom Alert Profile	Critical	-	Configure	-
	Dropbox Public Share Link Created	Custom Alert Profile	Critical	-	Configure	-
	Dropbox Passwords Exported	Custom Alert Profile	Critical	-	Configure	-
	Dropbox Password Reset for All Users	Custom Alert Profile	Critical	-	Configure	-
	Dropbox Password Policy Weakened	Custom Alert Profile	Critical	-	Configure	-
	Dropbox Password Control Disabled	Custom Alert Profile	Critical	-	Configure	-
	Dropbox Member Role Escalation to Admin	Custom Alert Profile	Critical	-	Configure	-
	Dropbox External Drive Backup Disabled	Custom Alert Profile	Critical	-	Configure	-
	Dropbox Computer Backup Disabled	Custom Alert Profile	Critical	-	Configure	-
	Dropbox Brute Force Login Attempts	Custom Alert Profile	Critical	-	Configure	-
	Dropbox Account Lock Status Changed	Custom Alert Profile	Critical	-	Configure	-

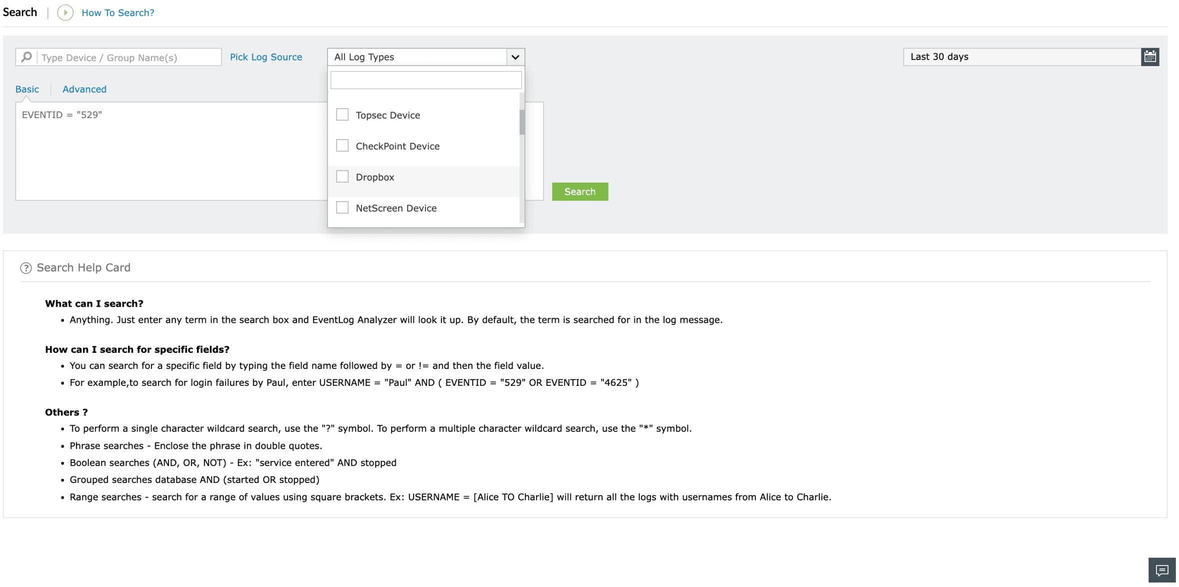
- Alternatively, go to the Alerts → Manage Profiles and choose Custom Alert Profiles under Alert Profile Type.
- Enable the required alert profiles.

Searching Dropbox Logs

- To search for Dropbox logs, select Dropbox Application under Extensions Group as the log source.



- Alternatively, filter logs by selecting Dropbox as the log type.



EVENTID = "529"

Search Help Card

What can I search?

- Anything. Just enter any term in the search box and EventLog Analyzer will look it up. By default, the term is searched for in the log message.

How can I search for specific fields?

- You can search for a specific field by typing the field name followed by = or != and then the field value.
- For example,to search for login failures by Paul, enter USERNAME = "Paul" AND (EVENTID = "529" OR EVENTID = "4625")

Others ?

- To perform a single character wildcard search, use the "?" symbol. To perform a multiple character wildcard search, use the "*" symbol.
- Phrase searches - Enclose the phrase in double quotes.
- Boolean searches (AND, OR, NOT) - Ex: "service entered" AND stopped
- Grouped searches database AND (started OR stopped)
- Range searches - search for a range of values using square brackets. Ex: USERNAME = [Alice TO Charlie] will return all the logs with usernames from Alice to Charlie.

Chapter 7 **Developer Space**

7.1. Custom Widgets

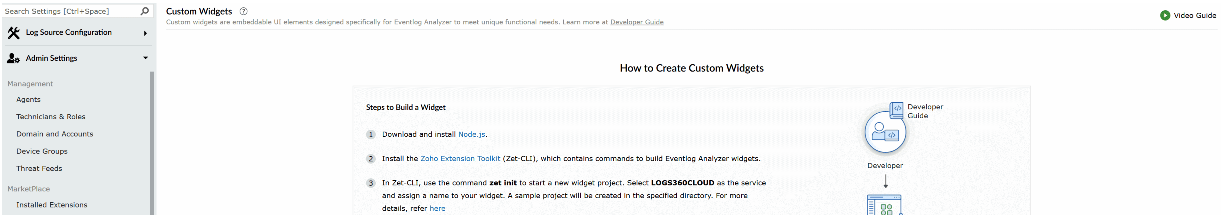
Last updated on: September 12, 2025

In this page

Widgets in ManageEngine EventLog Analyzer are embeddable UI components that you can create on your own, using our JS Software Development Kit. These widgets can be used to perform certain functions that utilize data from third-party applications seamlessly.
For example, with a custom widget in EventLog Analyzer, you can seamlessly integrate data from your EDR or email security solution into EventLog Analyzer, enabling you to monitor, analyze, and take necessary actions—all from a single platform.

Note

- Custom widgets can be created in all editions of EventLog Analyzer.
- You can create up to a maximum of 200 widgets in EventLog Analyzer.



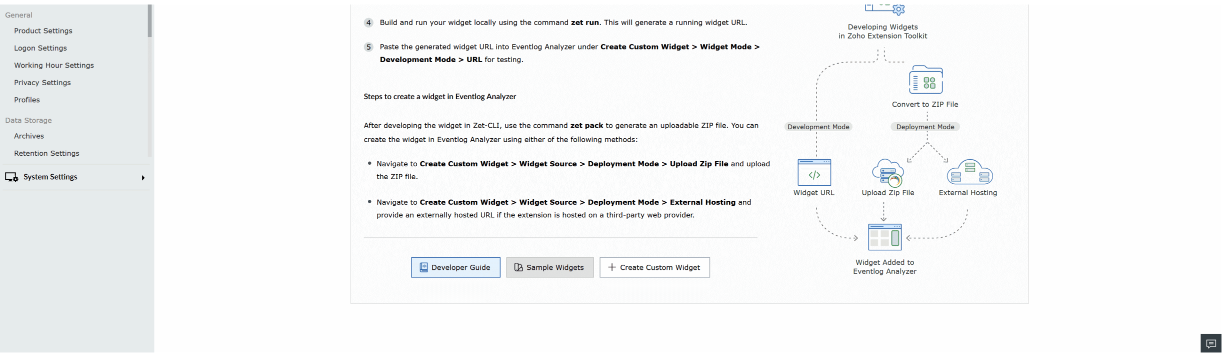
Custom Widgets

Custom widgets are embeddable UI elements designed specifically for Eventlog Analyzer to meet unique functional needs. Learn more at Developer Guide

How to Create Custom Widgets

Steps to Build a Widget

1. Download and install Node.js.
2. Install the Zoho Extension Toolkit (Zet-CLI), which contains commands to build Eventlog Analyzer widgets.
3. In Zet-CLI, use the command **zet init** to start a new widget project. Select **LOGS360CLOUD** as the service and assign a name to your widget. A sample project will be created in the specified directory. For more details, refer here



4. Build and run your widget locally using the command **zet run**. This will generate a running widget URL.
5. Paste the generated widget URL into Eventlog Analyzer under **Create Custom Widget > Widget Mode > Development Mode > URL** for testing.

Steps to create a widget in Eventlog Analyzer

After developing the widget in Zet-CLI, use the command **zet pack** to generate an uploadable ZIP file. You can create the widget in Eventlog Analyzer using either of the following methods:

- Navigate to **Create Custom Widget > Widget Source > Deployment Mode > Upload Zip File** and upload the ZIP file.
- Navigate to **Create Custom Widget > Widget Source > Deployment Mode > External Hosting** and provide an externally hosted URL if the extension is hosted on a third-party web provider.

ⓘ Note

These steps will be replaced by the widget list after you create your first widget. Refer to this image to follow the setup steps easily.

Reference URLs:

1. Node.js
2. Zoho Extension Toolkit

Types of Widgets in EventLog Analyzer

- Dashboard Widget
- Custom Report Widget
- Incident Workbench Widget

Dashboard Widget

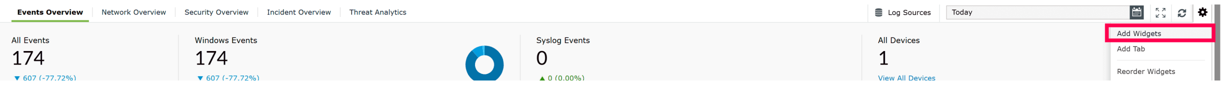
You can build a custom widget for your dashboard in EventLog Analyzer. After creating the custom widget under Settings → Admin Settings → Developer Space → Custom Widgets, you can add it to your dashboard by using the Add Tab menu, where it will be listed in the dashboard settings.

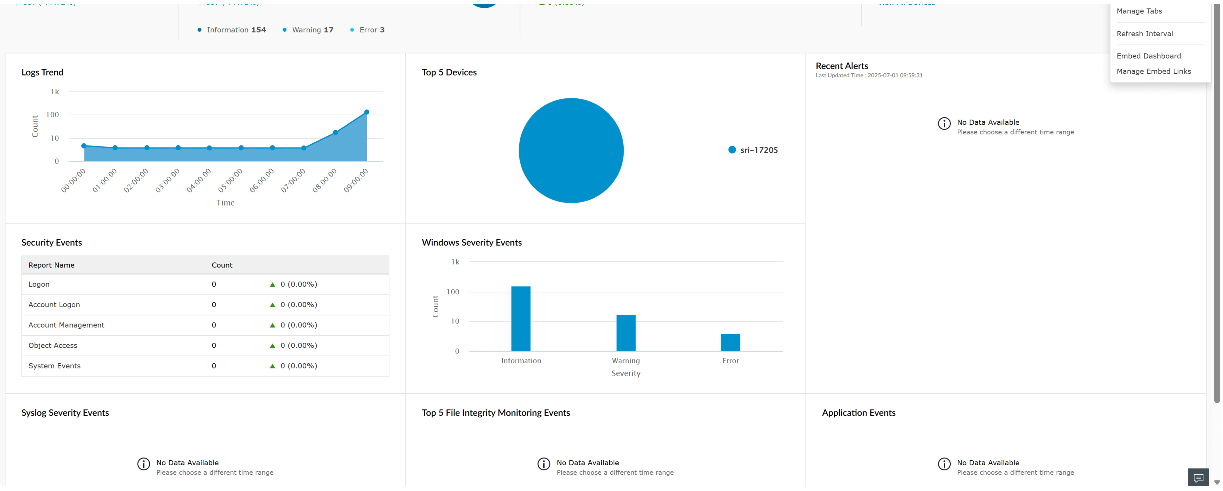
ⓘ Note

Only users with access to view or create widgets in a dashboard can view custom widgets.

The user who have access to view or create widgets in dashboard can view the custom widgets.

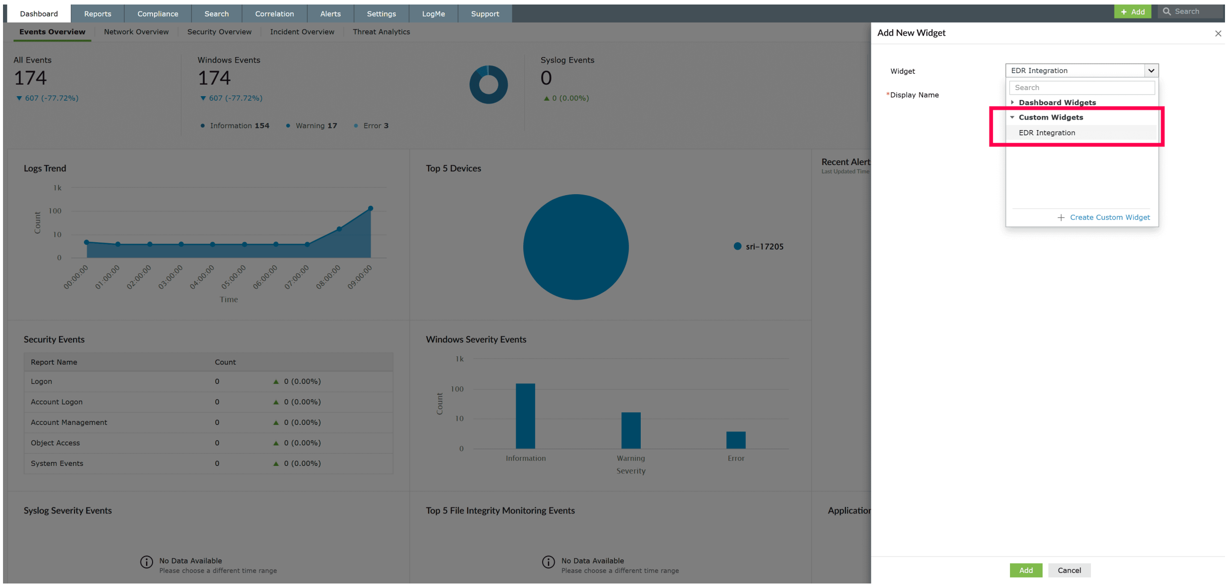
How to create a custom widget in Dashboard





Report Name	Count	
Logon	0	▲ 0 (0.00%)
Account Logon	0	▲ 0 (0.00%)
Account Management	0	▲ 0 (0.00%)
Object Access	0	▲ 0 (0.00%)
System Events	0	▲ 0 (0.00%)

From the dropdown menu in the top right corner, choose Add widgets.



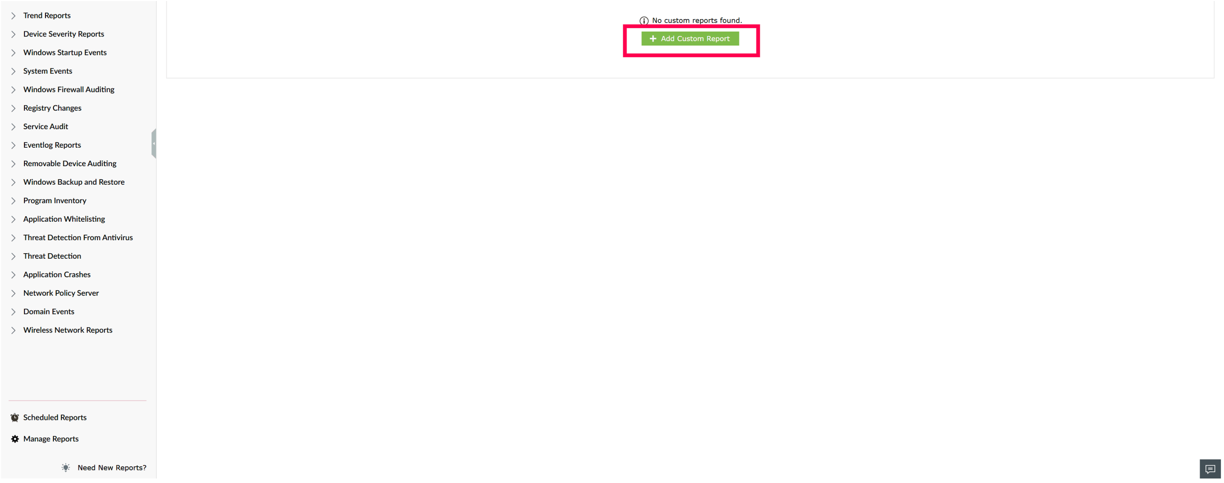
Select the custom widget that you want to add to the dashboard, and then click Add.

Custom Report Widget

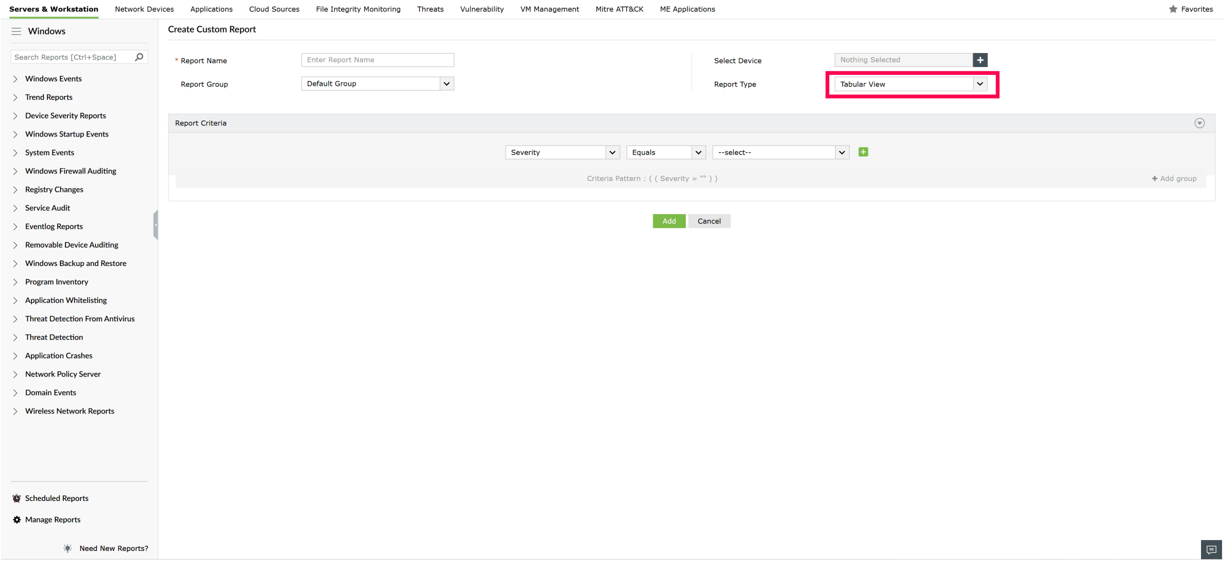
A widget can be added as a custom report in EventLog Analyzer. After creating the custom widget under Settings → Admin → Developer Space → Custom Widgets, you can add it as a custom report by navigating to Reports → Manage Custom Reports → Add Report, and then selecting the Report Type as Custom Widget.

> Note: Only users with access to view or create reports in custom reports can view custom widgets.

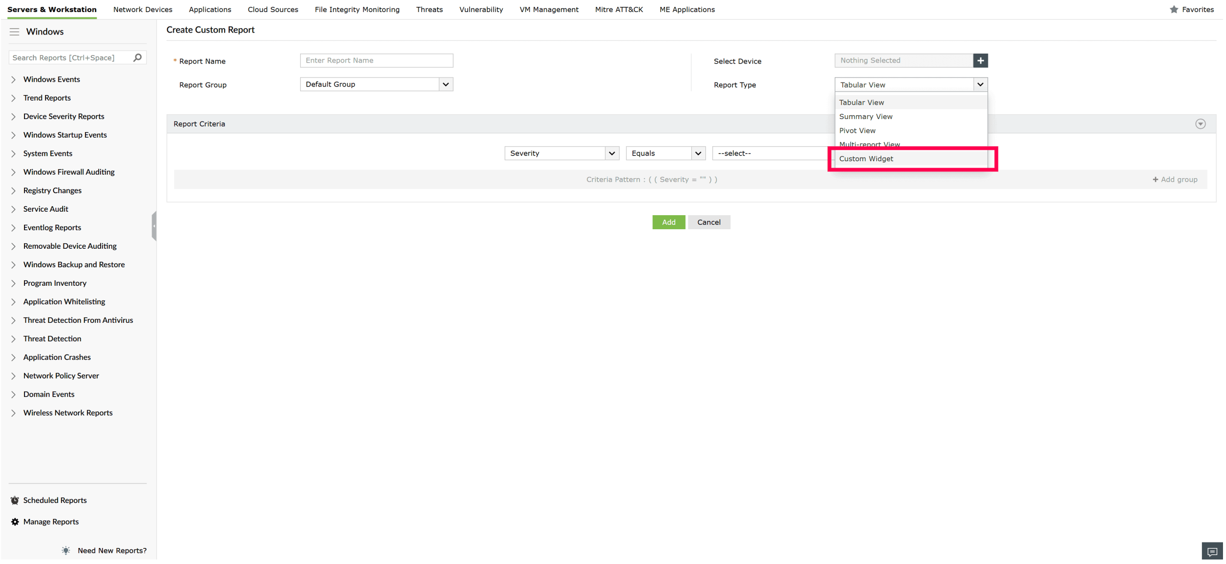
How to create a custom widget in Custom Reports



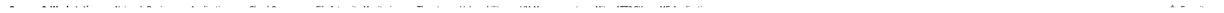
Click the Add Custom Report button.

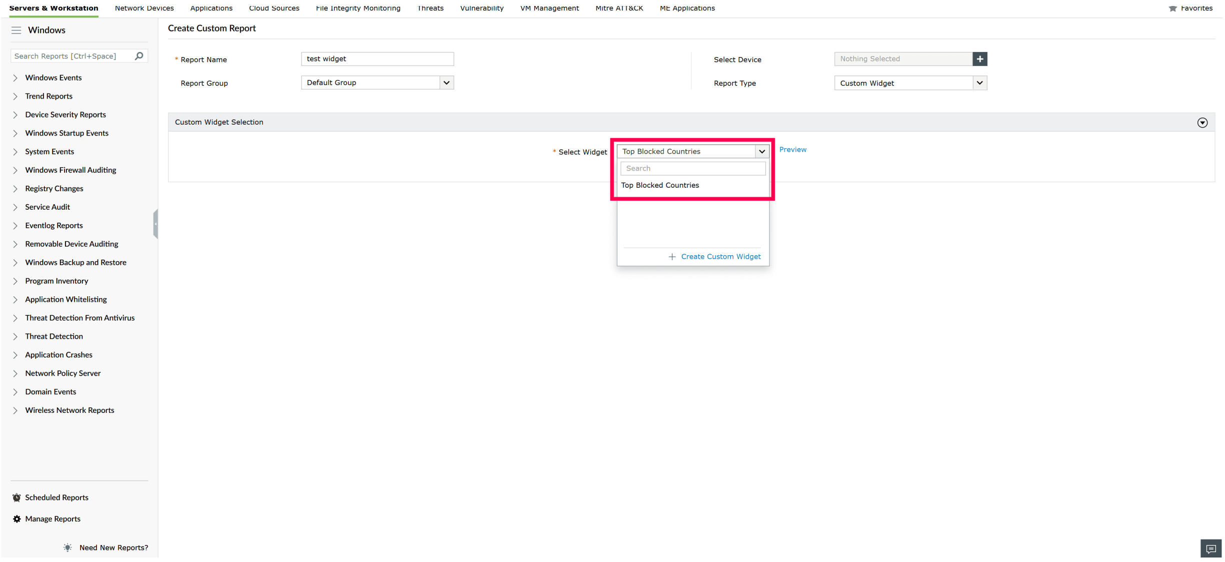


Click the Report type dropdown.



In the Report Type dropdown, select Custom Widget.





Create Custom Report

* Report Name: test widget

Report Group: Default Group

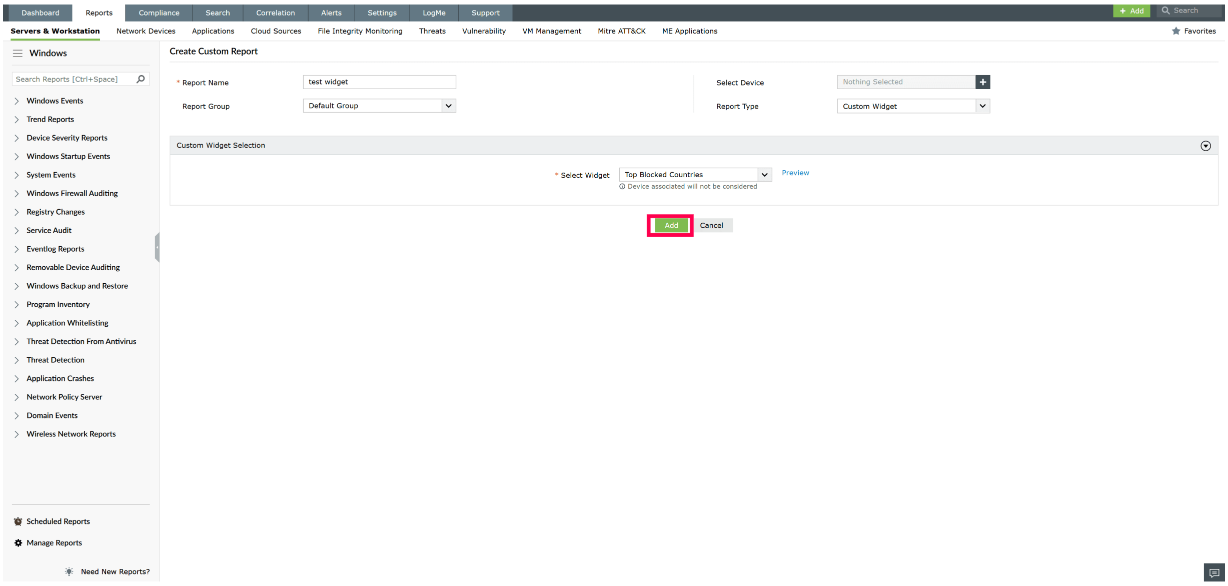
Select Device: Nothing Selected

Report Type: Custom Widget

Custom Widget Selection

* Select Widget: Top Blocked Countries

Under Custom Widgets, select the desired custom widget.



Create Custom Report

* Report Name: test widget

Report Group: Default Group

Select Device: Nothing Selected

Report Type: Custom Widget

Custom Widget Selection

* Select Widget: Top Blocked Countries

Device associated will not be considered

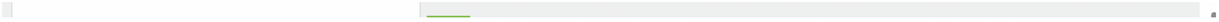
Then, click Add to create the custom report with the custom widget.

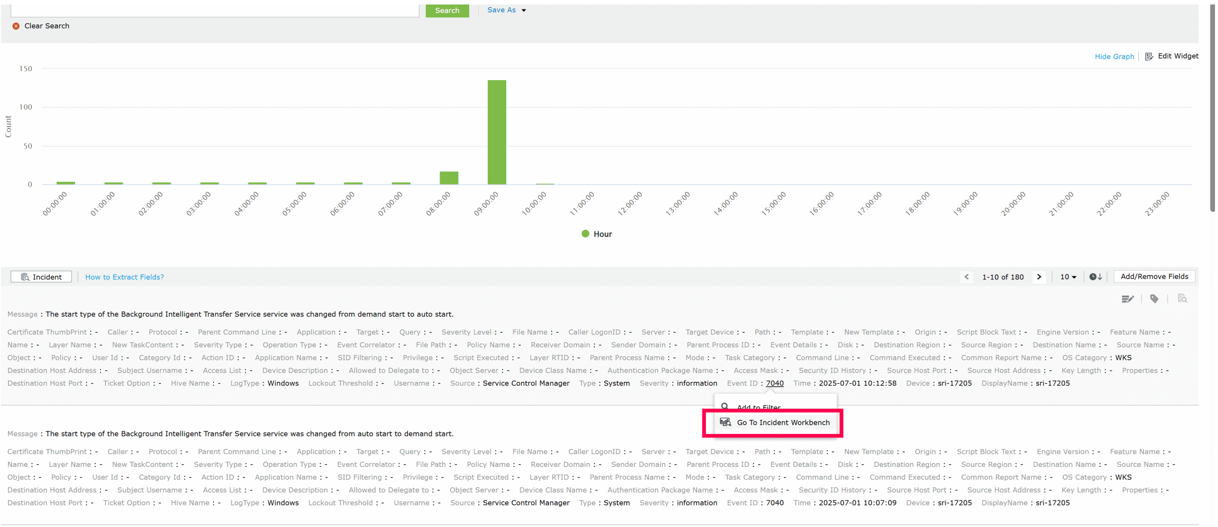
Incident Workbench Widget

A widget can be added to the Incident Workbench in EventLog Analyzer. This can be done directly from the Custom Widgets tab in the Settings, allowing you to integrate the custom widget seamlessly into the Incident Workbench.

> Note: Only users with access to view incident workbench can view custom widgets.

How to view a custom widget in Incident Workbench





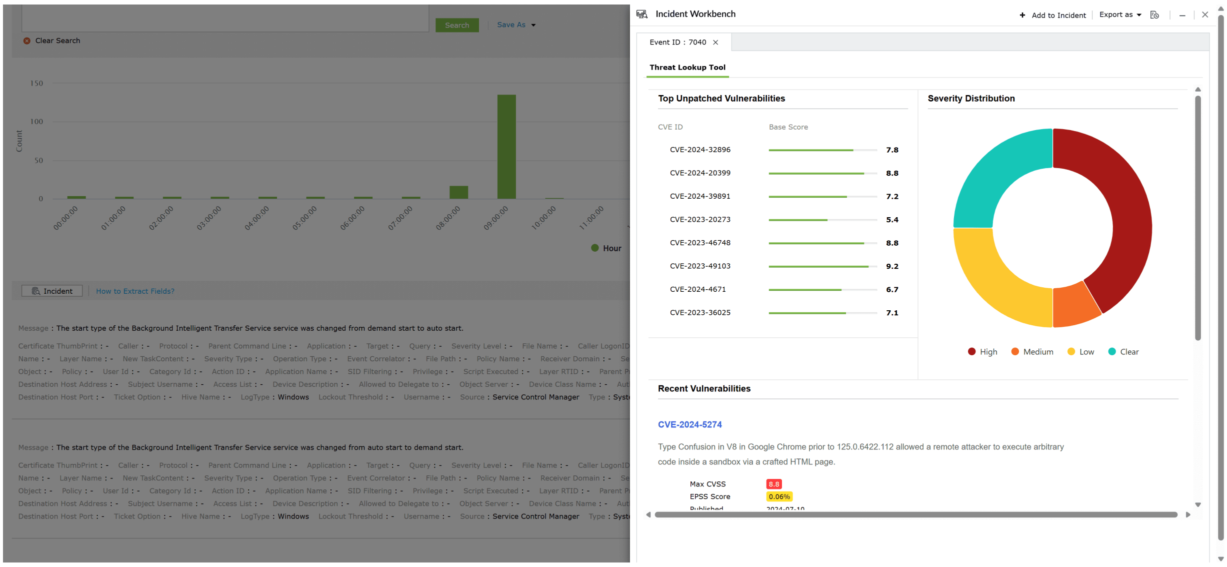
Message : The start type of the Background Intelligent Transfer Service service was changed from demand start to auto start.

Certificate ThumbPrint : - Caller : - Protocol : - Parent Command Line : - Application : - Target : - Query : - Severity Level : - File Name : - Caller LogonID : - Server : - Target Device : - Path : - Template : - New Template : - Origin : - Script Block Text : - Engine Version : - Feature Name : -
Name : - Layer Name : - New TaskContent : - Severity Type : - Operation Type : - Event Correlator : - File Path : - Policy Name : - Receiver Domain : - Sender Domain : - Parent Process ID : - Event Details : - Disk : - Destination Region : - Source Region : - Destination Name : - Source Name : -
Object : - Policy : - User Id : - Category Id : - Action ID : - Application Name : - SID Filtering : - Privilege : - Script Executed : - Layer RTID : - Parent Process Name : - Mode : - Task Category : - Command Line : - Command Executed : - Common Report Name : - OS Category : WKS
Destination Host Address : - Subject Username : - Access List : - Device Description : - Allowed to Delegate to : - Object Server : - Device Class Name : - Authentication Package Name : - Access Mask : - Security ID History : - Source Host Port : - Source Host Address : - Key Length : - Properties : -
Destination Host Port : - Ticket Option : - Hive Name : - LogType : Windows Lockout Threshold : - Username : - Source : Service Control Manager Type : System Severity : information Event ID : 7040 Time : 2025-07-01 10:12:58 Device : sri-17205 DisplayName : sri-17205

Message : The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start.

Certificate ThumbPrint : - Caller : - Protocol : - Parent Command Line : - Application : - Target : - Query : - Severity Level : - File Name : - Caller LogonID : - Server : - Target Device : - Path : - Template : - New Template : - Origin : - Script Block Text : - Engine Version : - Feature Name : -
Name : - Layer Name : - New TaskContent : - Severity Type : - Operation Type : - Event Correlator : - File Path : - Policy Name : - Receiver Domain : - Sender Domain : - Parent Process ID : - Event Details : - Disk : - Destination Region : - Source Region : - Destination Name : - Source Name : -
Object : - Policy : - User Id : - Category Id : - Action ID : - Application Name : - SID Filtering : - Privilege : - Script Executed : - Layer RTID : - Parent Process Name : - Mode : - Task Category : - Command Line : - Command Executed : - Common Report Name : - OS Category : WKS
Destination Host Address : - Subject Username : - Access List : - Device Description : - Allowed to Delegate to : - Object Server : - Device Class Name : - Authentication Package Name : - Access Mask : - Security ID History : - Source Host Port : - Source Host Address : - Key Length : - Properties : -
Destination Host Port : - Ticket Option : - Hive Name : - LogType : Windows Lockout Threshold : - Username : - Source : Service Control Manager Type : System Severity : information Event ID : 7040 Time : 2025-07-01 10:07:09 Device : sri-17205 DisplayName : sri-17205

Select the field you need to analyze, then click Go to Incident Workbench.



Top Unpatched Vulnerabilities

CVE ID	Base Score
CVE-2024-32896	7.8
CVE-2024-20399	8.8
CVE-2024-39891	7.2
CVE-2023-20273	5.4
CVE-2023-46748	8.8
CVE-2023-49103	9.2
CVE-2024-4671	6.7
CVE-2023-36025	7.1

Recent Vulnerabilities

CVE-2024-5274

Type Confusion in V8 in Google Chrome prior to 125.0.6422.112 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.

Max CVSS 8.8
EPSS Score 0.06%
Published 2024-07-10

The available widgets for the selected fields, including any custom widgets, are displayed in tabs.

Adding a custom widget in EventLog Analyzer

A custom widget can be added to EventLog Analyzer using the Zoho Extension Toolkit (ZET).

Create a custom widget using ZET

ZET, or the Zoho Extension Toolkit, is a command-line interface (CLI) designed to help developers build and package custom widgets for ManageEngine EventLog Analyzer.

A CLI is a text-based interface that allows users to interact with software by typing specific commands, receiving responses, and executing actions directly from the terminal or command prompt. While graphical user interfaces (GUIs) offer visual interaction, CLIs provide a simpler and more efficient way for developers to work, particularly when it comes to creating applications, managing software, or even building operating systems.

Here's how you can build custom widgets using ZET and package and integrate these widgets with ManageEngine EventLog Analyzer for enhanced functionality.

Install the necessary components

Prerequisites

- Visit the official Node.js website: https://nodejs.org/en/download/
- Choose the appropriate version for your operating system (Windows, macOS, or Linux) and download the installer.
- Once the installation is complete, verify that Node.js and npm are correctly installed by running the following commands in your terminal:

Check Node.js version
This will return the installed version of Node.js, e.g., v14.18.1.
Check npm version
This will return the installed version of npm, e.g., 6.14.12.
If both commands return a version number, it means Node.js and npm have been successfully installed.

Installing the CLI for Zoho Extension Toolkit (ZET)

To install the Zoho Extension Toolkit (ZET) CLI, follow these steps:

Install the ZET CLI package

Run the following command to install the zapps CLI node package:

Verify the installation

Once installed, run the following command to ensure that the installation was successful:
If the installation is successful, help information related to the zet command will be displayed.
Creating a New Project Using ZET
Follow these steps to create a new project using the Zoho Extension Toolkit (ZET):
Initialize a New Project
Run the following command to create a new project:
This command will display a list of available Zoho and ManageEngine services. Select the Log360 Cloud service for which you want to create a project template.

Verify the Server Startup

Once the project is created and the local development server starts running, verify its status by opening one of the following URLs in your browser:

- Manifest File: https://localhost:5000/plugin-manifest.json
- Widget Preview: https://localhost:5000/app/widget.html

If these URLs load correctly, your project has been successfully created and the local server is running.

Including Resources in Your Widget Project

All necessary files required for rendering your custom widget are stored inside the "app" folder of your project.

Starting the Server

To run your app locally and test it in your sandbox instance, start a local HTTPS server using the following command:

This will start the HTTPS server on your local machine at port 5000. Ensure that this port is not occupied by any other process before running the command.

Verify the Server

Once the server starts, open the following URL in your web browser to check if it is running successfully:
https://127.0.0.1:5000/app/widget.html
If the page loads correctly, your widget is now running in a local environment and is ready for testing.

Validating and Packaging the Application

Before uploading your application, it is essential to validate and package it correctly. Follow these steps:

Validate the Application

Run the following command to check for any issues in your app package:
This will scan your application for any violations. If issues are detected, they must be resolved before proceeding with the upload.

Package the Application

Once validation is successful, generate an uploadable ZIP file by running:
This will create a ZIP file inside the "dist" folder of your project directory. The packaged file can then be uploaded to EventLog Analyzer for deployment.

Adding the Created Widget to EventLog Analyzer

Follow these steps to add the custom widget to EventLog Analyzer:

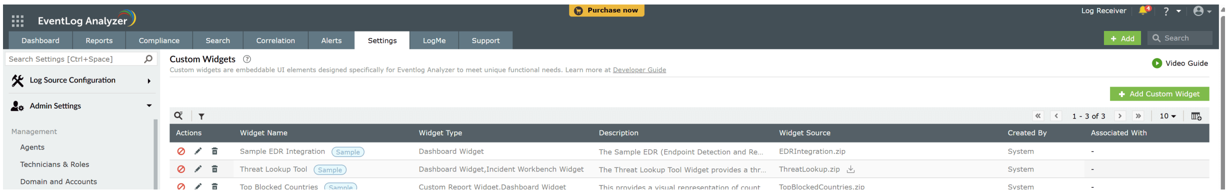
a) Navigate to Developer Space

Go to Settings → Developer Space → Custom Widgets in EventLog Analyzer.

b) Check Sample Widgets

The Sample Widgets section takes you to pre-created widgets within EventLog Analyzer.

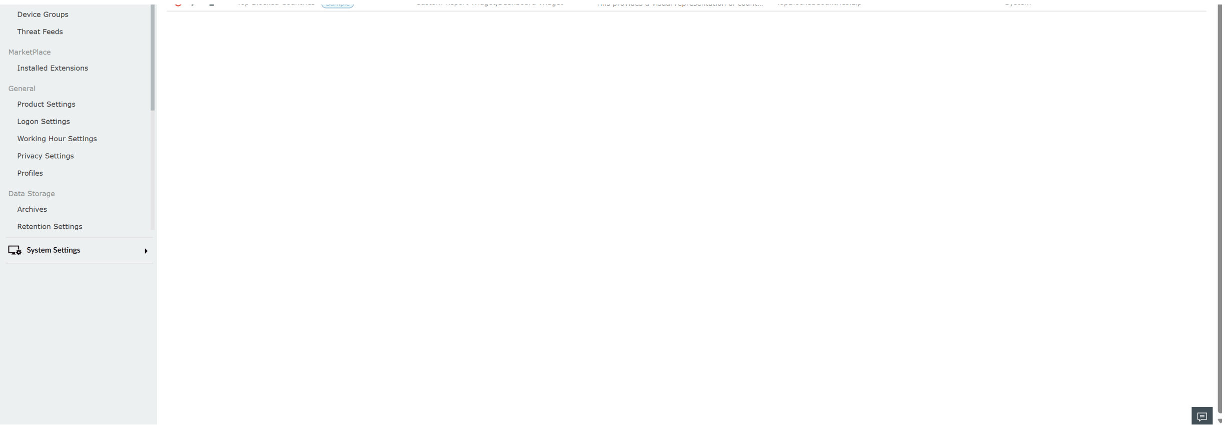
- These default widgets serve as examples, helping you understand how custom widgets can be designed and used.
- You can download and unzip the sample widgets, then open them in a code editor to see how they work.



Custom Widgets

Custom widgets are embeddable UI elements designed specifically for Eventlog Analyzer to meet unique functional needs. Learn more at Developer Guide

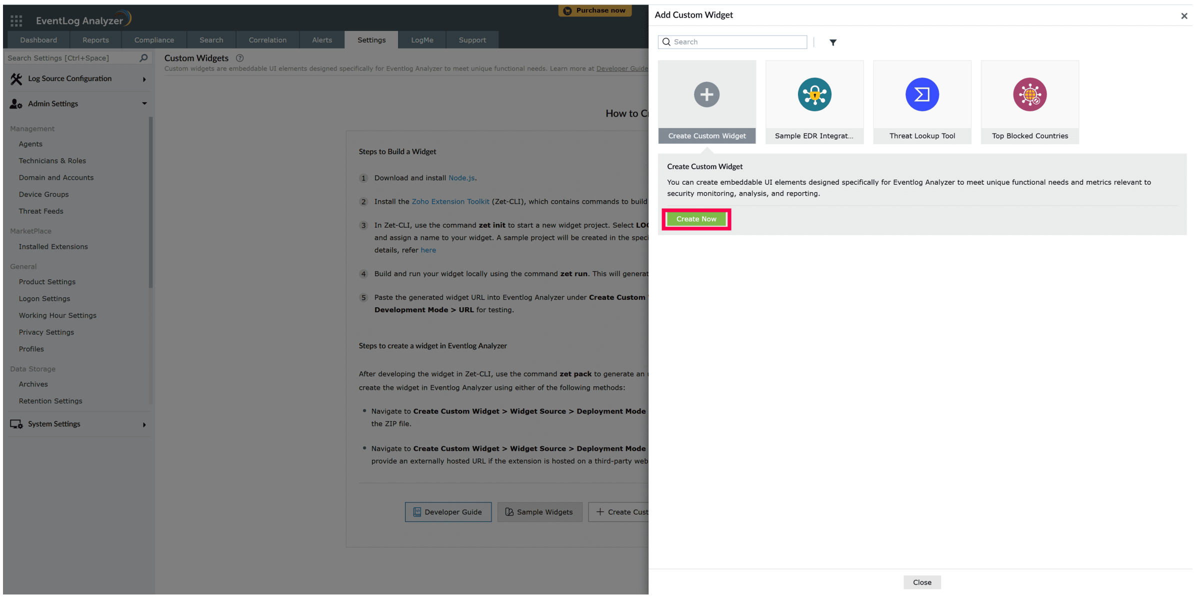
Actions	Widget Name	Widget Type	Description	Widget Source	Created By	Associated With
	Sample EDR Integration Sample	Dashboard Widget	The Sample EDR (Endpoint Detection and Re...	EDRIntegration.zip	System	-
	Threat Lookup Tool Sample	Dashboard Widget,Incident Workbench Widget	The Threat Lookup Tool Widget provides a thr...	ThreatLookup.zip	System	-
	Top Blocked Countries Sample	Custom Report Widget,Dashboard Widget	This provides a visual representation of count	TopBlockedCountries.zip	System	-



c) Create a New Widget

To create a new widget, click on Create Custom Widget → Create Now.

- EventLog Analyzer also offers a list of available widgets that you can add by selecting the custom widget.



Custom widgets are embeddable UI elements designed specifically for Eventlog Analyzer to meet unique functional needs. Learn more at Developer Guide

Steps to Build a Widget

1. Download and install Node.js.
2. Install the Zoho Extension Toolkit (Zet-CLI), which contains commands to build
3. In Zet-CLI, use the command **zet init** to start a new widget project. Select **LO** and assign a name to your widget. A sample project will be created in the speci details, refer here
4. Build and run your widget locally using the command **zet run**. This will generat
5. Paste the generated widget URL into Eventlog Analyzer under **Create Custom** **Development Mode > URL** for testing.

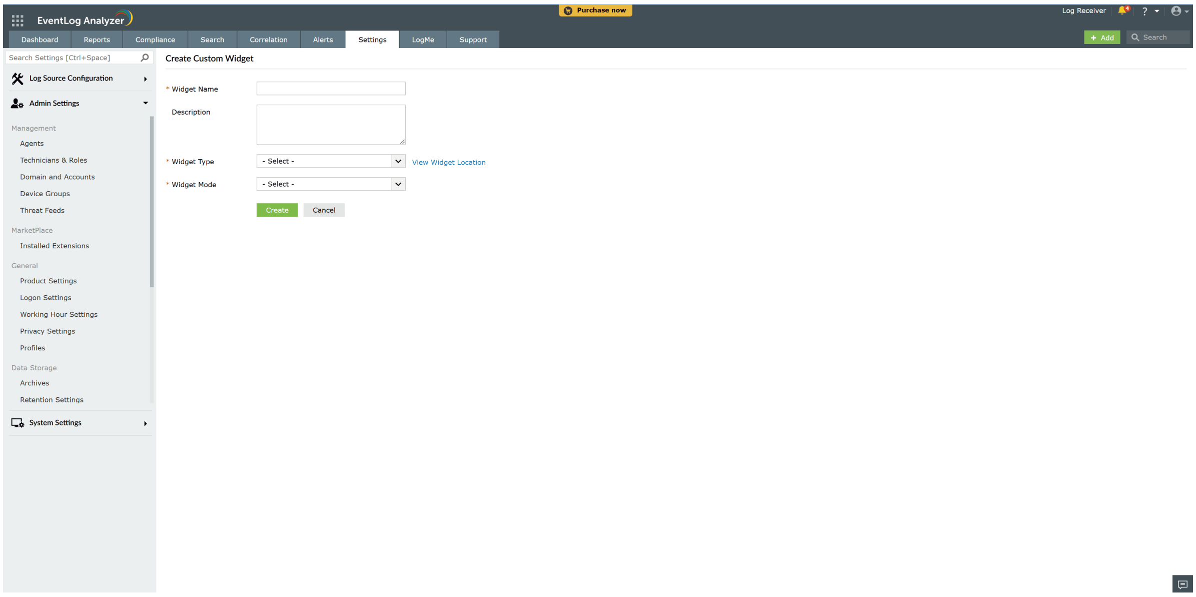
Steps to create a widget in Eventlog Analyzer

After developing the widget in Zet-CLI, use the command **zet pack** to generate an create the widget in Eventlog Analyzer using either of the following methods:

- Navigate to **Create Custom Widget > Widget Source > Deployment Mode** the ZIP file.
- Navigate to **Create Custom Widget > Widget Source > Deployment Mode** provide an externally hosted URL if the extension is hosted on a third-party web

Create Custom Widget

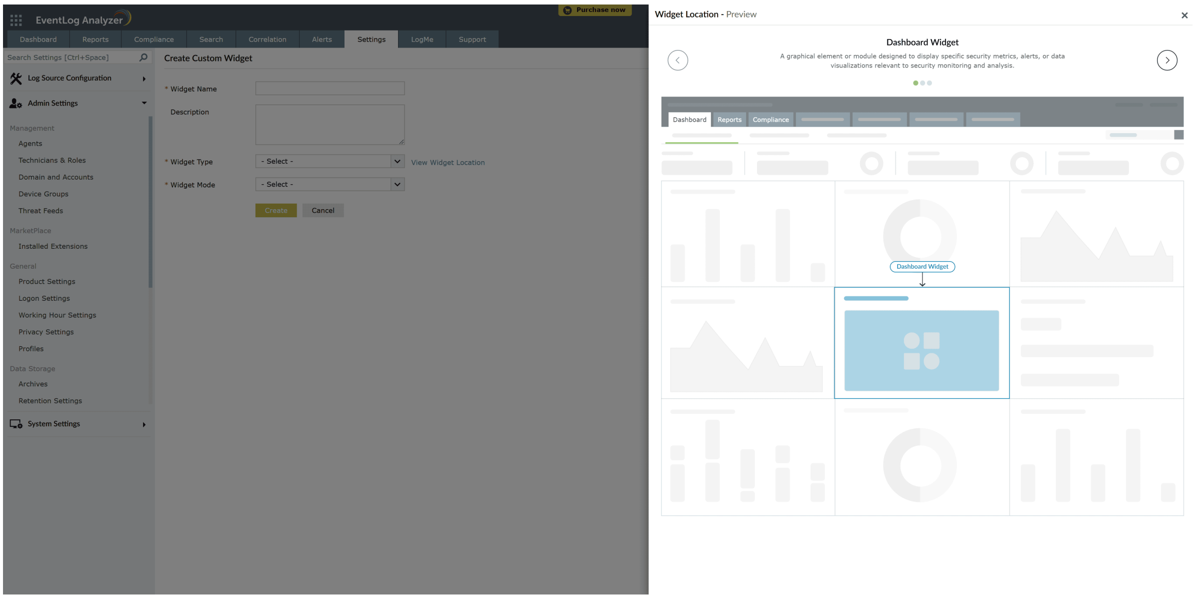
You can create embeddable UI elements designed specifically for Eventlog Analyzer to meet unique functional needs and metrics relevant to security monitoring, analysis, and reporting.



d) Fill Out the Widget Creation Form

In the Create Custom Widget Form:

- Provide the Widget Name and Description.
- Select the Widget Type from the following options:
  - Dashboard Widget
  - Custom Report Widget
  - Incident Workbench Widget
- Choose the View Widget Location to determine where your custom widget will be placed within EventLog Analyzer.



Create Custom Widget

* Widget Name

Description

* Widget Type - Select - View Widget Location

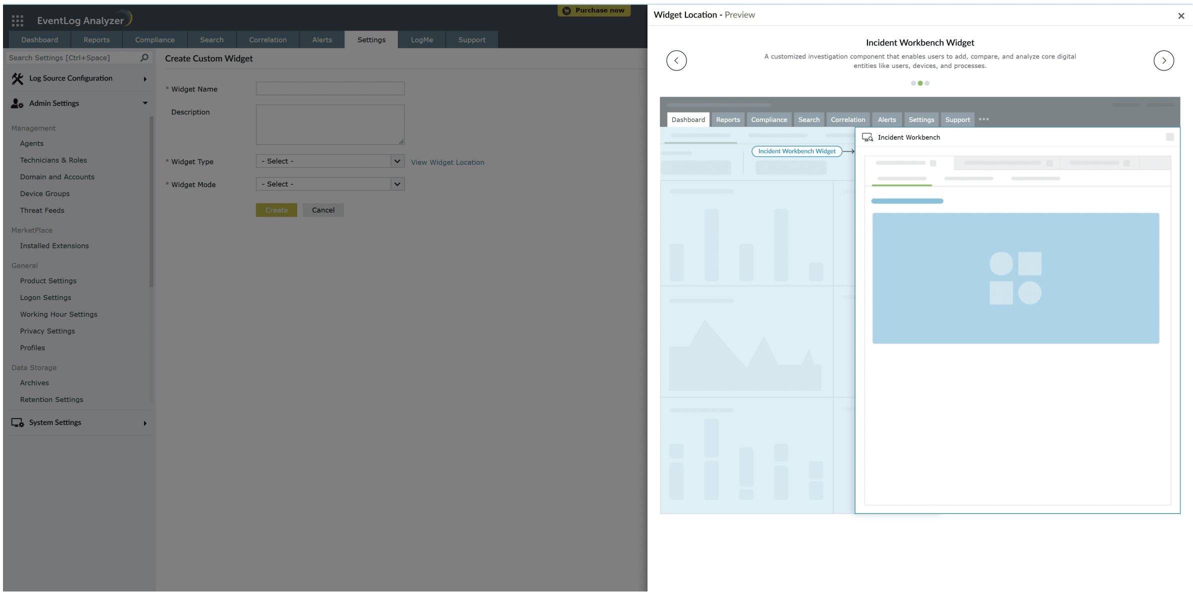
* Widget Mode - Select -

Create Cancel

Widget Location - Preview

Dashboard Widget

A graphical element or module designed to display specific security metrics, alerts, or data visualizations relevant to security monitoring and analysis.



Create Custom Widget

* Widget Name

Description

* Widget Type - Select - View Widget Location

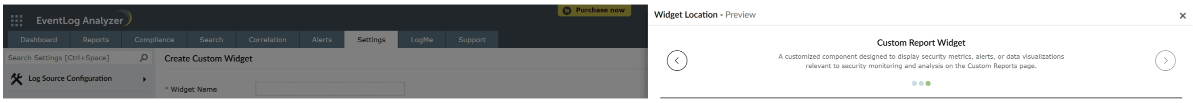
* Widget Mode - Select -

Create Cancel

Widget Location - Preview

Incident Workbench Widget

A customized investigation component that enables users to add, compare, and analyze core digital entities like users, devices, and processes.



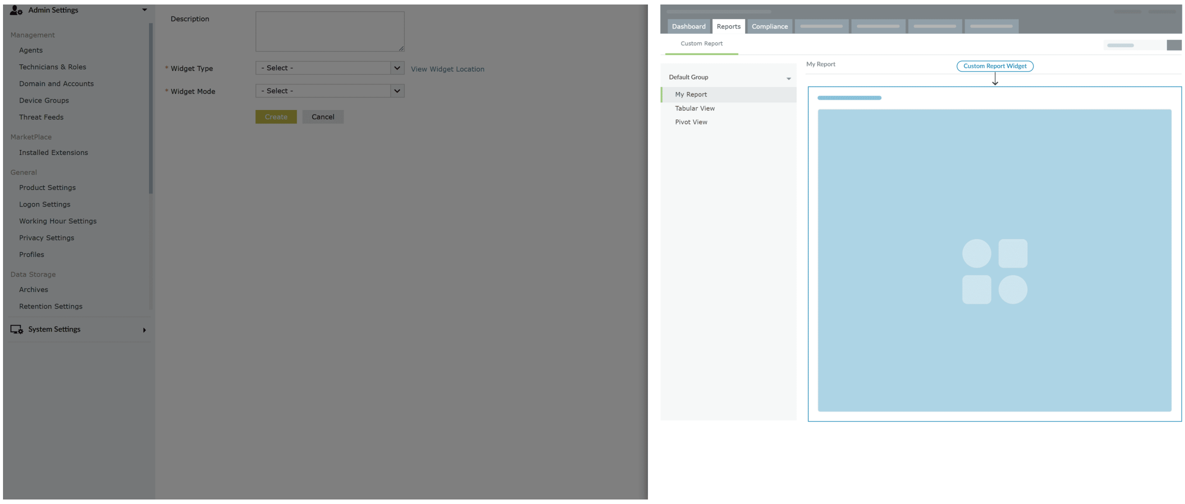
Create Custom Widget

* Widget Name

Widget Location - Preview

Custom Report Widget

A customized component designed to display security metrics, alerts, or data visualizations relevant to security monitoring and analysis on the Custom Reports page.



e) Custom Widget Creation Modes in EventLog Analyzer

EventLog Analyzer supports two modes for custom widget creation:

1. Development Mode

- In this mode, you can run and test your custom widget locally before deploying it.
- Start the widget by running:
- Add the URL (ex: https://localhost:5000/app/widget.html) of your widget to the Widget URL input field in EventLog Analyzer.

Note

- Any changes made to the widget code automatically reflect in EventLog Analyzer (whether in the dashboard or custom report).
- Development Mode is not available for Incident Workbench Widgets, as field mapping is required in plugin-manifest.json.
- The custom widget in development mode is visible only to the developer and not to other users.

2. Deployment Mode

In deployment mode, you have two options to add the widget to EventLog Analyzer:

a) Upload ZIP File (ZET Package)

- After developing the custom widget, package it using:
- This creates a ZIP file inside the dist folder of your project.
- Upload this ZIP file to EventLog Analyzer to deploy the widget.

b) External URL Embedding

- Instead of using ZET, you can embed any external URL as a widget inside EventLog Analyzer.
- This option allows seamless integration of third-party dashboards or web apps.

How to Include a Custom Widget in EventLog Analyzer

Custom widgets can be added to the following sections of EventLog Analyzer:

- Dashboard
- Custom Reports
- Incident Workbench

Adding a Custom Widget to the Dashboard

After creating an HTML page for the custom widget, add the following configuration to the plugin-manifest.json file inside the widgets list:
This will ensure that the widget appears on the EventLog Analyzer dashboard.

Adding a Custom Widget to Custom Reports

For adding a custom widget to Custom Reports, add the following configuration to the plugin-manifest.json file inside the widgets list:
This allows the widget to be used as a custom report widget.

Adding a Custom Widget to the Incident Workbench

For including a custom widget in Incident Workbench, use the configuration below:
This ensures the widget is integrated with the Incident Workbench for real-time incident analysis.
Important
Modifying and uploading the name attribute for a custom widget after it has been added will result in the removal of the widget from its mapped module (Dashboard, Reports or Incident Workbench).
Following are the locations allowed in EventLog Analyzer:

- "dashboard"
- "reports"
- "incident-workbench"

Adding a custom widget in Incident Workbench differs from other modules as it requires mapping specific fields to the widget. When adding a widget to the Incident Workbench, you must specify options where the fieldName will be mapped with the custom widget.
Here are some of the important fields.

- HOSTNAME → Device name (source of data/log collection)
- USERNAME → User associated with the data/log
- IPADDRESS → Captured IP in the data/log
- FILENAME → Name of the file in the data/log
- PROCESSNAME → Name of the process in the data/log
- FILEHASH → Hash of the file in the data/log
- EMAIL → User email captured in the data/log
- DOMAINNAME → AD domain name captured in the data/log

- PORT → Port associated with the entity in the data/log
- PROTOCOL → Protocol associated with the entity in the data/log

Passing Log Data to Custom Widgets in Incident Workbench

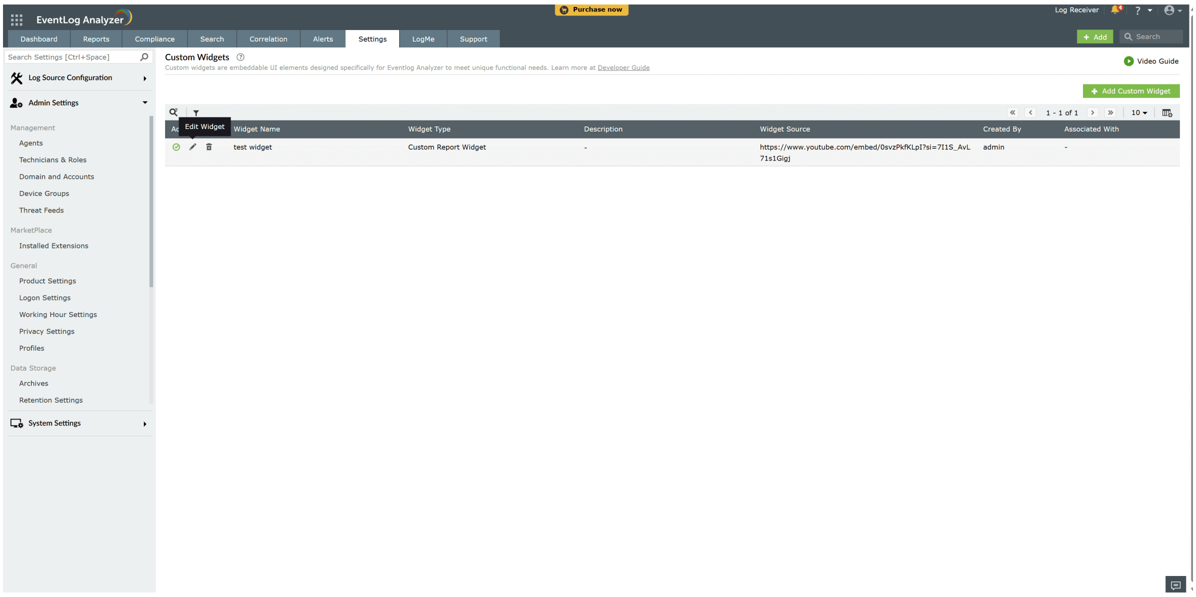
When a field associated with Incident Workbench is clicked, the log data corresponding to that row will be passed from the table data to the Custom Widget.

Example Log Data Structure:

```
{
  "logUUID": 430453503444,
  "HOSTNAME": "EVENT-TEST",
  "USERNAME": "admin",
  ...
}
```

How to edit Custom Widgets

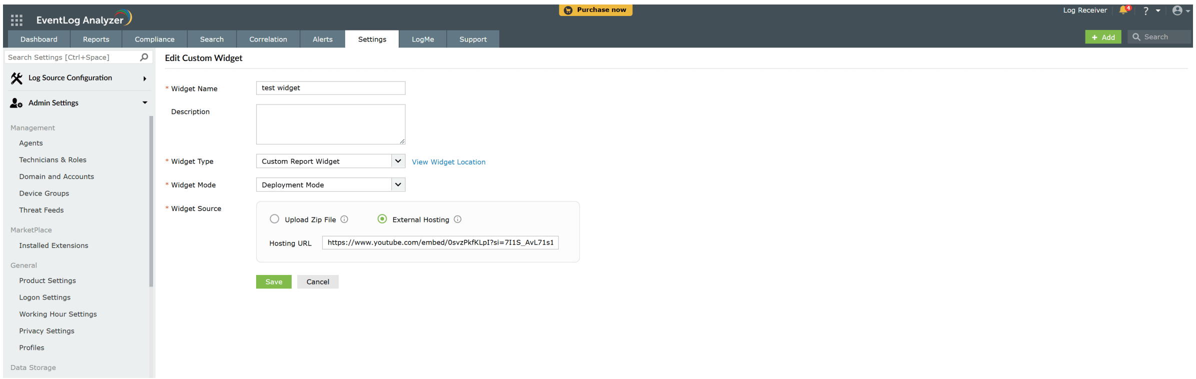
1. Go to Settings -> Admin -> Developer Space -> Custom Widgets
2. In the Manage Custom Widgets table, click on edit icon to edit the Custom Widget



Custom Widgets

Custom widgets are embeddable UI elements designed specifically for Eventlog Analyzer to meet unique functional needs. Learn more at Developer Guide

Ac	Widget Name	Widget Type	Description	Widget Source	Created By	Associated With
	test widget	Custom Report Widget	-	https://www.youtube.com/embed/0svzPkfKLpI?si=7I1S_AvL71s1Gigj	admin	-



Edit Custom Widget

* Widget Name: test widget

Description:

* Widget Type: Custom Report Widget

* Widget Mode: Deployment Mode

* Widget Source: ○ Upload Zip File ● External Hosting

Hosting URL: https://www.youtube.com/embed/0svzPkfKLpI?si=7I1S_AvL71s1

When editing a custom widget, certain changes can affect its associations with other modules.

To Retain Associations:

1. The Widget Name must remain the same.
   - For ZIP uploads, the name inside plugin-manifest.json is used.
   - For Development Mode or External Hosting, the Widget Name entered in the form is used.
2. You can safely update the widget URL or ZIP contents as long as the widget name remains unchanged.

> **Note**
>
> The widget name serves as the primary key for maintaining associations.

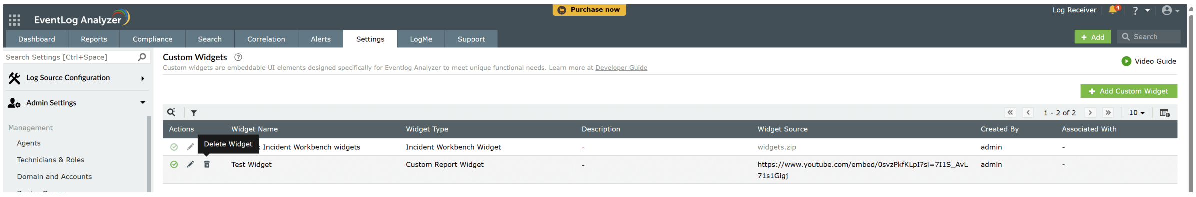
Associations Will Be Removed If:

1. The Widget Type is changed or removed.
2. A new ZIP is uploaded with a different widget name in plugin-manifest.json.
3. The widget source is changed between:
   - ZIP ↔ Development Mode / External Hosting
   - Development Mode / External Hosting ↔ ZIP
     → Only if the widget name (in the form or ZIP) is also changed.

> **Note**
>
> To avoid breaking associations, keep both the Widget Source and Widget Name unchanged when making edits.

How to delete Custom Widgets

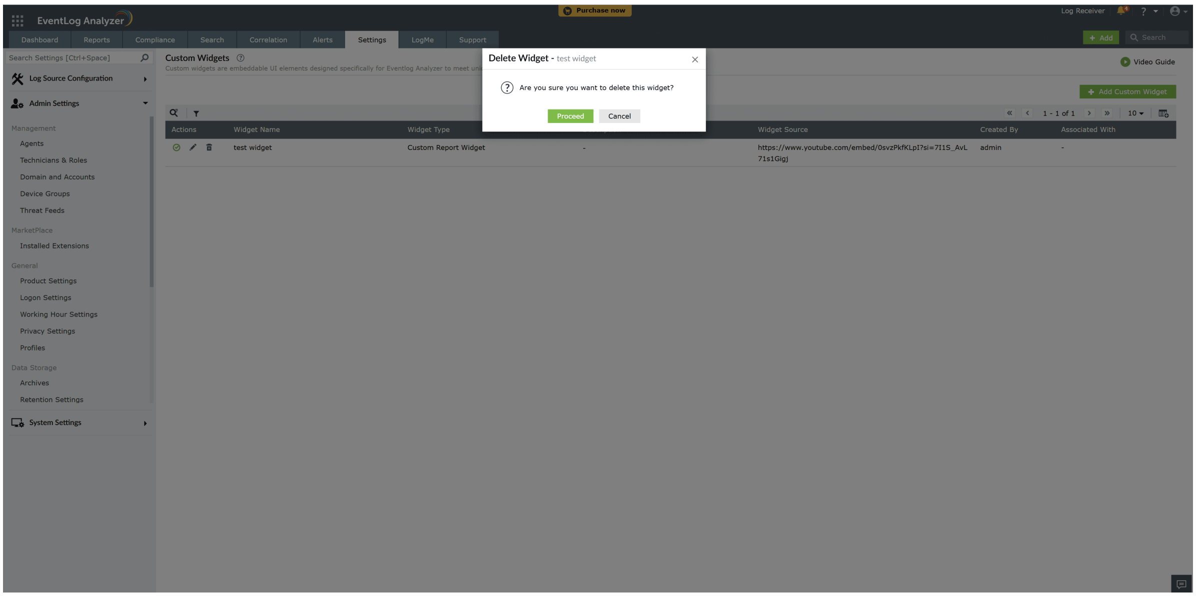
1. Navigate to Settings → Admin → Developer Space → Custom Widgets.
2. In the Manage Custom Widgets table, click the delete icon to remove the custom widget.



Custom Widgets

Custom widgets are embeddable UI elements designed specifically for Eventlog Analyzer to meet unique functional needs. Learn more at Developer Guide

Actions	Widget Name	Widget Type	Description	Widget Source	Created By	Associated With
	Incident Workbench widgets	Incident Workbench Widget	-	widgets.zip	admin	-
	Test Widget	Custom Report Widget	-	https://www.youtube.com/embed/0svzPkfKLpI?si=7I1S_AvL71s1Gigj	admin	-



Custom Widgets

Custom widgets are embeddable UI elements designed specifically for Eventlog Analyzer to meet uni

Delete Widget - test widget

Are you sure you want to delete this widget?

Proceed Cancel

Actions	Widget Name	Widget Type		Widget Source	Created By	Associated With
	test widget	Custom Report Widget	-	https://www.youtube.com/embed/0svzPkfKLpI?si=7I1S_AvL71s1Gigj	admin	-

JS SDK:

JS SDK provides a set of JavaScript functions to integrate EventLog Analyzer functionalities into your custom widget. These APIs enable seamless interaction between your widget and the platform.

Widget usage:

Note

The service name LOGS360CLOUD is used for both EventLog Analyzer and Log360 Cloud.

LOGS360CLOUD.init()

This function acts as a foundational call to establish a connection between the custom widget and the product. Other JS APIs will be defined only when the initialization is completed.
Returns promise

LOGS360CLOUD.get(options)

Fetch the product data, such as meta data, or any input data in the custom widget, from the product server. Note that only Logs360 APIs can be invoked using this function.

LOGS360CLOUD.add(options)

> ⓘ Note
>
> Please ensure that only api/v2 APIs are used.

Add data to the server from the custom widget.Note that only Logs360 APIs can be invoked using this function.

LOGS360CLOUD.showLoader(opts)

The function is used to display a loading indicator on the widget window. This helps improve user experience by visually indicating that a process is in progress, such as data fetching, API calls, or background computations.

LOGS360CLOUD.hideLoder(opts)

The function is used to remove or hide the loading indicator from the widget window. It is typically called after a process, such as data retrieval or API execution, has been completed.

LOGS360CLOUD.showNotification(opts)

The function is used to display a top notification in the widget. This notification can be utilised to inform users about important updates, alerts, or process statuses.

LOGS360CLOUD.HideNotification(opts)

The function is used to hide or remove the top notification from the widget window. This can be useful when you need to manually dismiss a notification before its auto-dismissal time or when clearing notifications based on user interactions.

LOGS360CLOUD.getConnections()

Fetches the details of all successfully installed API applications.

LOGS360CLOUD.invokeUrl()

The function is used to fetch data from integrated third-party applications by making API calls. This function supports multiple configuration options, such as URL, HTTP method, headers, parameters, and payload, allowing seamless interaction with external services.

Chapter 8 **FAQ and troubleshooting**

8.1. EventLog Analyzer - Troubleshooting Tips

Last updated on: September 12, 2025

General

Where do I find the log files to send to EventLog Analyzer Support?

For Build 8010 onwards

The log files are located in the <EventLogAnalyzer_Home>logs directory. Typically when you run into a problem, you will be asked to send the serverout.txt file from this directory to EventLog Analyzer Support.

For Build 8000 or earlier

The log files are located in the <EventLogAnalyzer_Home>server/default/log directory. Typically when you run into a problem, you will be asked to send the serverout.txt file from this directory to EventLog Analyzer Support.

I find that EventLog Analyzer keeps crashing or all of a sudden stops collecting logs. What could be the reason?

The inbuilt PostgreSQL/MySQL database of EventLog Analyzer could get corrupted if other processes are accessing these directories at the same time. So exclude ManageEngine installation folder from

- Anti-virus scans
- Automatic backup softwares
- Snapshots in case of VMware installation

Ensure that no snap shots are taken if the product is running on a VM.

How to create SIF (Support Information File) and send it to ManageEngine when you are not able to perform the same from the Web client?

The SIF will help us to analyze the issue you have come across and propose a solution for the same.

If you are unable to create a SIF from the Web client UI,

For Build 8010 onwards

You can zip the files under 'logs' folder, located in C:/ManageEngine/Eventlog/logs (default path) and upload the zip file to the following ftp link: http://bonitas.zohocorp.com/upload/index.jsp?to=eventloganalyzer-support@manageengine.com

For Build 8000 or earlier

You can zip the files under 'log' folder, located in C:/ManageEngineEventlog/server/default/log (default path) and upload the zip file to the following ftp link: http://bonitas.zohocorp.com/upload/index.jsp?

path) and upload the zip file to the following ftp link: http://bonitas.zohocorp.com/upload/index.jsp?to=eventloganalyzer-support@manageengine.com

How to register dll when message files for event sources are unavailable?

To register dll, follow the procedure given in the link below: http://ss64.com/nt/regsvr32.html

How to register/unregister bundled postgres as a service?

Why register/unregister bundled postgres as a service?

Depending on your environment, you may occasionally experience challenges with starting EventLog Analyzer due to a Postgres database startup failure. To avoid this, it is advisable that you register the database first, making it run in the background irrespective of the product's start up or shutdown.

How to register/unregister bundled postgres as a service?

To register bundled postgres as a service:

For Build 12440 onwards

- Execute the following command in the Elevated Command Prompt Window within "<EventLog Analyzer Home>bin" directory.
  register_pgdbservice.bat "<Specify the name of the DB Service to be registered>"
- Stop the EventLog Analyzer service/server and start it after the registered DB service is started.

For Build 12440 or earlier

- Copy register_pgdbservice.bat from "<EventLog Analyzer Home\tools\postgres\bin" and paste it in "<EventLog Analyzer Home\bin" directory
- Execute the following command in the Elevated Command Prompt Window within <EventLog Analyzer Home>bin directory.
  register_pgdbservice.bat "<Specify the name of the DB Service to be registered>"
- Stop the EventLog Analyzer service/server and start it after the registered DB service is started.

Should you no longer wish to be in charge of the database, you may opt to unregister, which will cause the product to start and stop the database, along with its own start and stop.

To unregister the bundled postgres service:

For Build 12440 onwards

- Execute the following command in the Elevated Command Prompt Window within the <EventLog Analyzer Home>bin directory.
  unregister_pgdbservice.bat "<Specify the name of the DB Service to be unregistered>"

For Build 12440 or earlier

- Copy unregister_pgdbservice.bat from "<EventLog Analyzer Home\tools\postgres\bin" and paste it in "<EventLog Analyzer Home\bin"
- Execute the following command in the Elevated Command Prompt Window within the <EventLog Analyzer Home>bin directory.

unregister_pgdbservice.bat "<Specify the name of the DB Service to be unregistered>"

Installation

EventLog Analyzer displays "Enter a proper ManageEngine license file" during installation

This can happen under two instances:

- Case 1: Your system date is set to a future or past date. In this case, uninstall EventLog Analyzer, reset the system date to the current date and time, and re-install EventLog Analyzer.
- Case 2: You may have provided an incorrect or corrupted license file. Verify that you have applied the license file obtained from ZOHO Corp. If neither is the reason, or you are still getting this error, contact licensing@manageengine.com

Binding EventLog Analyzer server (IP binding) to a specific interface.

For Build 8010 onwards

To bind EventLog Analyzer server to a specific interface, follow the procedure given below:

For Eventlog Analyzer running as application:

- Shutdown EventLog Analyzer
- Open the run.bat file which is under <EventLog Analyzer Home>bin directory and go to "RESTART Command block", uncomment the below RESTART command line and replace <ip-address> with the IP address to which you want to bind the application, comment the existing RESTART command line and save the file.

  to

  to

- Open setcommonenv.bat file which is under <EventLog Analyzer Home>bin directory and go to "JAVA_OPTS Setting command Block", uncomment the below JAVA_OPTS setting command line and replace <ip-address> with the IP address to which you want to bind the application and comment the existing JAVA_OPTS setting command.

  to

  to

- Save the file
- Open the database_param.conf file which is under <EventLog Analyzer Home>conf directory and replace localdevice in url tag with the <binding IP address> to which you want to bind the application and save the file.

- Open the postgresql.conf file which is under <EventLog Analyzer Home>pgsqldata directory and uncomment the line '#listen_addresses = 'localdevice'' in the CONNECTIONS AND AUTHENTICATION section and replace the 'localdevice' with the '<binding IP address>' to which you want to bind the application and save the file.
- Open the pg_hba.conf file which is under <EventLog Analyzer Home>pgsqldata directory and add the line

  device all all <binding IP address in IPv4 format>/32 trust

  after the line

  device all all 127.0.0.1/32 trust

  and save the file.

  # TYPE DATABASE USER ADDRESS METHOD

  # IPv4 local connections:

  device all all 127.0.0.1/32 trust

  # IPv6 local connections:

  device all all ::1/128 trust

  to

  # TYPE DATABASE USER ADDRESS METHOD

  # IPv4 local connections:

  device all all 127.0.0.1/32 trust

  device all all <binding IP address in IPv4 format>/32 trust

  # IPv6 local connections:

  device all all ::1/128 trust

- Restart EventLog Analyzer

  For Eventlog Analyzer running as service:

  Before proceeding further, stop the EventLog Analyzer service and make sure that 'SysEvtCol.exe','Postgres.exe' and 'java.exe' are not running.

  There are 7 files that must be modified for IP binding.

  Note: data-doc-rid="255l9469213c93f3f4d8cb899c7bf8471fb58">Before editing the files ensure that you have a backup copy of the files.

  Assume xxx.xxx.xxx.xxx is the IP address you wish to bind with EventLog Analyzer.

  File 1)

  <ELA home>\bin\setCommonEnv.bat

- Search for line set JAVA_OPTS=-Djava.library.path=..\lib;..\lib\native -Duser.country=US -Duser.language=en -Xms256m -Xmx1024m
- Append -Dspecific.bind.address= xxx.xxx.xxx.xxxto the line. It will now look as: set JAVA_OPTS=-Djava.library.path=..\lib;..\lib\native -Duser.country=US -Duser.language=en -Xms256m -Xmx1024m -Dspecific.bind.address= xxx.xxx.xxx.xxx

  File 2)

File 2)

<ELA home>\bin\runSEC.bat

- Search for line "%SERVER_HOME%\bin\SysEvtCol.exe" -port 513 %syslogPort% -dbhome "%dbhome%" -ELAhome "%serverHome%" -loglevel 2 %RelayIP% %IPadd% %IgnoreHost% %IPadd% %*
- Add -bindip xxx.xxx.xxx.xxx to the line, so that it looks like "%SERVER_HOME%\bin\SysEvtCol.exe" -bindip xxx.xxx.xxx.xxx -port 513 %syslogPort% -dbhome "%dbhome%" -ELAhome "%serverHome%" -loglevel 2 %RelayIP% %IPadd% %IgnoreHost% %IPadd% %*

File 3)

<ELA home>\server\conf\wrapper.conf

- Search for line #wrapper.app.parameter.1=com.adventnet.mfw.Starter
- Remove the # from the line, it should now look like wrapper.app.parameter.1=com.adventnet.mfw.Starter
- The next line from current position should be #wrapper.app.parameter.2=-L../lib/AdventNetDeploymentSystem.jar . Add the following two lines after this line, one after the other.
- wrapper.app.parameter.2=-b xxx.xxx.xxx.xxx
- wrapper.app.parameter.3=-Dspecific.bind.address= xxx.xxx.xxx.xxx
- The block should now look like this :-

wrapper.app.parameter.1=com.adventnet.mfw.Starter

#wrapper.app.parameter.2=-L../lib/AdventNetDeploymentSystem.jar

wrapper.app.parameter.2=-b xxx.xxx.xxx.xxx

wrapper.app.parameter.3=-Dspecific.bind.address= xxx.xxx.xxx.xxx

File 4)

<ELA home>\conf\server.xml

Search for the following block:

<Connector SSLEnabled="false" URIEncoding="UTF-8" acceptCount="100" address="0.0.0.0" clientAuth="false" compressableMimeType="text/html,text/xml" compression="force" compressionMinSize="1024" connectionTimeout="20000" disableUploadTimeout="true" enableLookups="false" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" name="WebServer" noCompressionUserAgents="gozilla, traviata" port="8095" protocol="HTTP/1.1" scheme="http" secure="false"/>

- Replace address="0.0.0.0" with address="xxx.xxx.xxx.xxx"
- It should now look like the following

<Connector SSLEnabled="false" URIEncoding="UTF-8" acceptCount="100" address="xxx.xxx.xxx.xxx" clientAuth="false" compressableMimeType="text/html,text/xml" compression="force" compressionMinSize="1024" connectionTimeout="20000" disableUploadTimeout="true" enableLookups="false" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" name="WebServer" noCompressionUserAgents="gozilla, traviata" port="8095" protocol="HTTP/1.1" scheme="http" secure="false"/>

File 5)

<ELA home>\conf\database_params.conf

- Search for the line url=jdbc:postgresql://127.0.0.1:33335/eventlog?stringtype=unspecified
- Replace the 127.0.0.1 with your xxx.xxx.xxx.xxx, the line should now look like url=jdbc:postgresql://xxx.xxx.xxx.xxx:33335/eventlog?stringtype=unspecified

File 6)

<ELA home>\pgsql\data\postgresql.conf

- Search for the line #listen_addresses = 'localhost'
- Remove the # from the line.
- Replace the 'localhost' with 'xxx.xxx.xxx.xxx', the line should now look like listen_addresses = 'xxx.xxx.xxx.xxx'

File 7)

<ELA home>\pgsql\data\pg_hba.conf

Search for the following block

IPv4 local connections:

    host all all 127.0.0.1/32 trust

We need to replicate the host all all 127.0.0.1/32 trust line with the new IP address in place of 127.0.0.1 and add it after that line. For replication, please copy this line itself and paste it in next line and then edit out the IP address.

It should look like this

IPv4 local connections:

host all all 127.0.0.1/32 trust

host all all xxx.xxx.xxx.xxx/32 trust

Start EventLog Analyzer and check <ELA home>\logs\wrapper.log for the current status.

EventLog Analyzer displays "java.lang.Error: Probable fatal error: No fonts found"

ELA employs the Dejavu-seriff font, which is preinstalled on Windows OS, when exporting reports. However, this font is not preinstalled for some Linux distributions. An error occurs in these cases.

In such cases, install the font manually based on the distribution. The command required is listed below:

- Case 1 : RHEL/CentOS
- Case 2 : Ubuntu/Debian
- Case 3 : SLES

Startup and Shut Down

MySQL-related errors on Windows machines

Probable cause: An instance of MySQL is already running on this machine.

Solution: Shut down all instances of MySQL and then start the EventLog Analyzer server.

Probable cause: Port 33335 is not free

Solution: Kill the other application running on port 33335. If you cannot free this port, then change the MySQL port used in EventLog Analyzer.

EventLog Analyzer displays "Port 8095 needed by EventLog Analyzer is being used by another application. Please free the port and restart EventLog Analyzer" when trying to start the server

Probable cause: The default web server port used by EventLog Analyzer is not free.

Solution: Kill the other application running on port 8095. Carry out the following steps.

- Stop the EventLog Analyzer service
- Open wrapper.conf which is available under <EventLog Analyzer Home>server/conf folder.
- Append the below line under # Java Additional Parameters section,

wrapper.java.additional.21=-Djava.net.preferIPv4Stack=true

Before adding:

wrapper.java.additional.20=-Dorg.tanukisoftware.wrapper.WrapperManager.mbean=false

After adding:

wrapper.java.additional.20=-Dorg.tanukisoftware.wrapper.WrapperManager.mbean=false
wrapper.java.additional.21=-Djava.net.preferIPv4Stack=true

- Start EventLog Analyzer service

If you cannot free this port, then change the web server port used in EventLog Analyzer.

EventLog Analyzer displays "Can't Bind to Port <Port Number>" when logging into the UI.

Probable cause:The syslog listener port of EventLog Analyzer is not free. Solution:

- Check for the process that is occupying the syslog listener port, using netstat -anp -pudp . And if possible, try to free up this port.
- If you have started the server in UNIX machines, please ensure that you start the server as a root user.
- or, configure EventLog Analyzer to listen to a different syslog listener port and ensure that all your configured devices send their syslog to the newly configured syslog listener port of EventLog Analyzer

Start up and shut down batch files not working on Distributed Edition when taking backup.

Probable cause: Path names given incorrectly.

Solution:

- Download the "Automated.zip" and extract the files "startELAservice.bat"and "stopELAservice.bat" to

<ELA home>//bin/ folder.

- Create a Windows schedule as per your requirement and ensure that the path should be <ELA Home>//bin folder.
- If you would like to have the files to a different folder, you need to edit the downloaded files and give the absolute path as below: < eg. is the application is installed on e:\ >

- e:\ManageEngine\EventLog\bin\wrapper.exe -p ..\server\conf\wrapper.conf ---> to stop the EventLog Analyzer service.
- e:\ManageEngine\EventLog\bin\wrapper.exe -t ..\server\conf\wrapper.conf ---> to start the EventLog Analyzer service.

Note:The script will work only if the application is started as a service.

EventLog Analyzer displays "Couldn't start elasticsearch at port 9300".

Probable cause: requiretty is not disabled

Solution: To disable requiretty, please replace requiretty with !requiretty in the etc/sudoers file.

Note:Elasticsearch uses multiple thread pools for different types of operations. It is important for new threads to be created whenever necessary. Please make sure that the number of threads that an elasticsearch user can create is at least 4096 by setting ulimit -u 4096 as root before starting Elasticsearch or by adding elasticsearch - nproc 4096 in /etc/security/limits.conf.

Service pack

How to upgrade your service pack if failure is due to lack of permission?

Navigate to <PRODUCT_HOME>\bin and invoke StartDB.bat as administrator. If you see access denied error, Execute setAppPermission.bat and wait for its completion.

Note: EventLog Analyzer directory permissions will be modified on executing the setAppPermission.bat as mentioned in this document here.

Troubleshooting PPM backup and failure cases

Note: Backup will be done only for the instances with PGSQL or MSSQL database. PPM backup feature is not available for MySQL database.

- If the database size exceeds 10GB, the auto-backup won't work and the user will be notified to backup manually before proceeding with the upgrade.
- For PGSQL database, backup will be done only if there is enough free space available in the EventLog Analyzer installed drive. Incase of MSSQL database, the backed up data will be stored in the default backup folder configured for MSSQL. The availability of free space will be checked before backup operation and if enough space is not available, the user will be notified. Users can either clear-up enough space for auto-backup or they can proceed to back up manually.
- For PGSQL database, only two PPM backups will be maintained and older backups will be deleted upon

rotation.

- For MSSQL database, backups won't be deleted automatically. Users will have to manually clear them.
- Incase of upgrade failure, the backups can be used to restore the last known working state of the instance. Please contact support for the restoration process.

Configuration

While adding device for monitoring, the 'Verify Login' action throws RPC server unavailable error

The probable reason and the remedial action is: Probable cause: The device machine RPC (Remote Procedure Call) port is blocked by any other Firewall. Solution: Unblock the RPC ports in the Firewall.

While adding device for monitoring, the 'Verify Login' action throws 'Access Denied' error.

The probable reasons and the remedial actions are:

Probable cause: The device machine is not reachable from EventLog Analyzer machine.

Solution: Check the network connectivity between device machine and EventLog Analyzer machine, by using PING command.

Probable cause: The device machine running a System Firewall and REMOTEADMIN service is disabled.

Solution: Check whether System Firewall is running in the device. If System Firewall is running, execute the following command in the command prompt window of the device machine:
netsh firewall set service type=REMOTEADMIN mode=ENABLE profile=all

When WBEM test is carried out. it fails and shows error message with code 80041010 in Windows Server 2003.

The probable reasons and the remedial actions are:

Probable cause: By default, WMI component is not installed in Windows 2003 Server

Solution: Win32_Product class is not installed by default on Windows Server 2003. To add the class, follow the procedure given below:

- In Add or Remove Programs, click Add/Remove Windows Components.
- In the Windows Components Wizard, select Management and Monitoring Tools, then click Details.
- In the Management and Monitoring Tools dialog box, select WMI Windows Installer Provider and then click OK.
- Click Next.

How to enable Object Access logging in Linux OS?

The probable reasons and the remedial actions are:

Probable cause: The object access log is not enabled in Linux OS.

Solution: Steps to enable object access in Linux OS, is given below:

In the file /etc/xinted.d/wu-ftpd, edit the server arguments as mentioned below:

server_args = -i -o -L

What are commands to start and stop Syslog Deamon in Solaris 10?

The probable reasons and the remedial actions are:

Probable cause: Unable to start or stop Syslog Daemon in Solaris 10

Solution: In Solaris 10, the commands to stop and start the syslogd daemon are:

# svcadm disable svc:/system/system-log:default

# svcadm enable svc:/system/system-log:default

In Solaris 10, to restart the syslogd daemon and force it to reread /etc/syslog.conf:

# svcadm refresh svc:/system/system-log:default

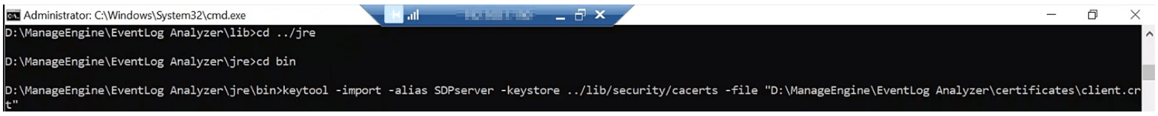
(or)
# svcadm -v restart svc:/system/system-log:default

While configuring incident management, I am facing SSL Connection error.

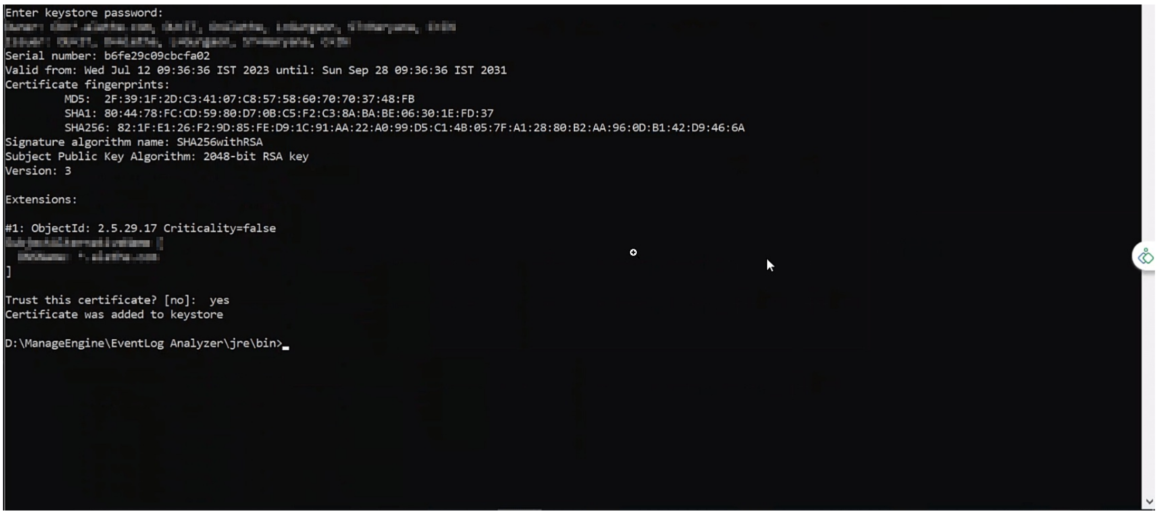
This error can occur if the ticketing tool server's HTTPS certificate is not included in EventLog Analyzer's JRE certificate store. To import the certificate to EventLog Analyzer's JRE certificate store, follow the steps below:

- Place the server's certificate in your browser's certificate store by allowing trust when your browser throws up the error saying that the certificate is not trusted.
- Export the certificate as a binary DER file from your browser.
- For Firefox, you can do this by following the steps below:

- Click the lock symbol next to the URL and click More Information.
- Select the Security tab, click View certificate, and click the Details tab.
- Select the certificate and click Export. Select a location in your local machine and save the certificate.
- For IE, Internet Options > Content > Certificates > Personal > Export
- For Chrome, Settings > Show Advanced Settings > Manage Certificates
- Use the keytool utility to import the certificate into EventLog Analyzer's JRE certificate store. The command should be executed from <Eventlog Analyzer Home>/jre/bin.



```
D:\ManageEngine\EventLog Analyzer\lib>cd ../jre

D:\ManageEngine\EventLog Analyzer\jre>cd bin

D:\ManageEngine\EventLog Analyzer\jre\bin>keytool -import -alias SDPserver -keystore ../lib/security/cacerts -file "D:\ManageEngine\EventLog Analyzer\certificates\client.cr
t"
```



```
Enter keystore password:
[redacted]
Serial number: b6fe29c09cbcfa02
Valid from: Wed Jul 12 09:36:36 IST 2023 until: Sun Sep 28 09:36:36 IST 2031
Certificate fingerprints:
         MD5:  2F:39:1F:2D:C3:41:07:C8:57:58:60:70:70:37:48:FB
         SHA1: 80:44:78:FC:CD:59:80:D7:0B:C5:F2:C3:8A:BA:BE:06:30:1E:FD:37
         SHA256: 82:1F:E1:26:F2:9D:85:FE:D9:1C:91:AA:22:A0:99:D5:C1:4B:05:7F:A1:28:80:B2:AA:96:0D:B1:42:D9:46:6A
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.17 Criticality=false
[redacted]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore

D:\ManageEngine\EventLog Analyzer\jre\bin>_
```

- Enter the keystore password. Note that the default password is changeit.

While configuring EventLog Analyzer with JIRA On-Premise, the 'Test and Save' action throws Captcha Verification failed error.

If you are facing problems while configuring EventLog Analyzer with JIRA On-Premise even after entering the valid credentials, please follow the steps below:

- Go to the ticketing tool instance and try logging in to your account.
- Enter the valid credentials and complete the captcha verification.
- You can now try configuring EventLog Analyzer with JIRA On-Premise again. The Test and Save action will complete successfully without any errors.

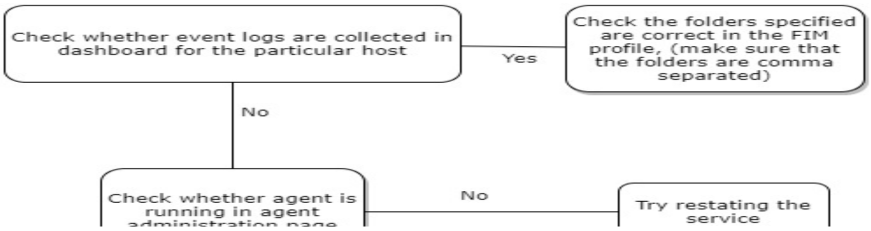
Help link: https://developer.atlassian.com/cloud/jira/software/basic-auth-for-rest-apis/#captcha

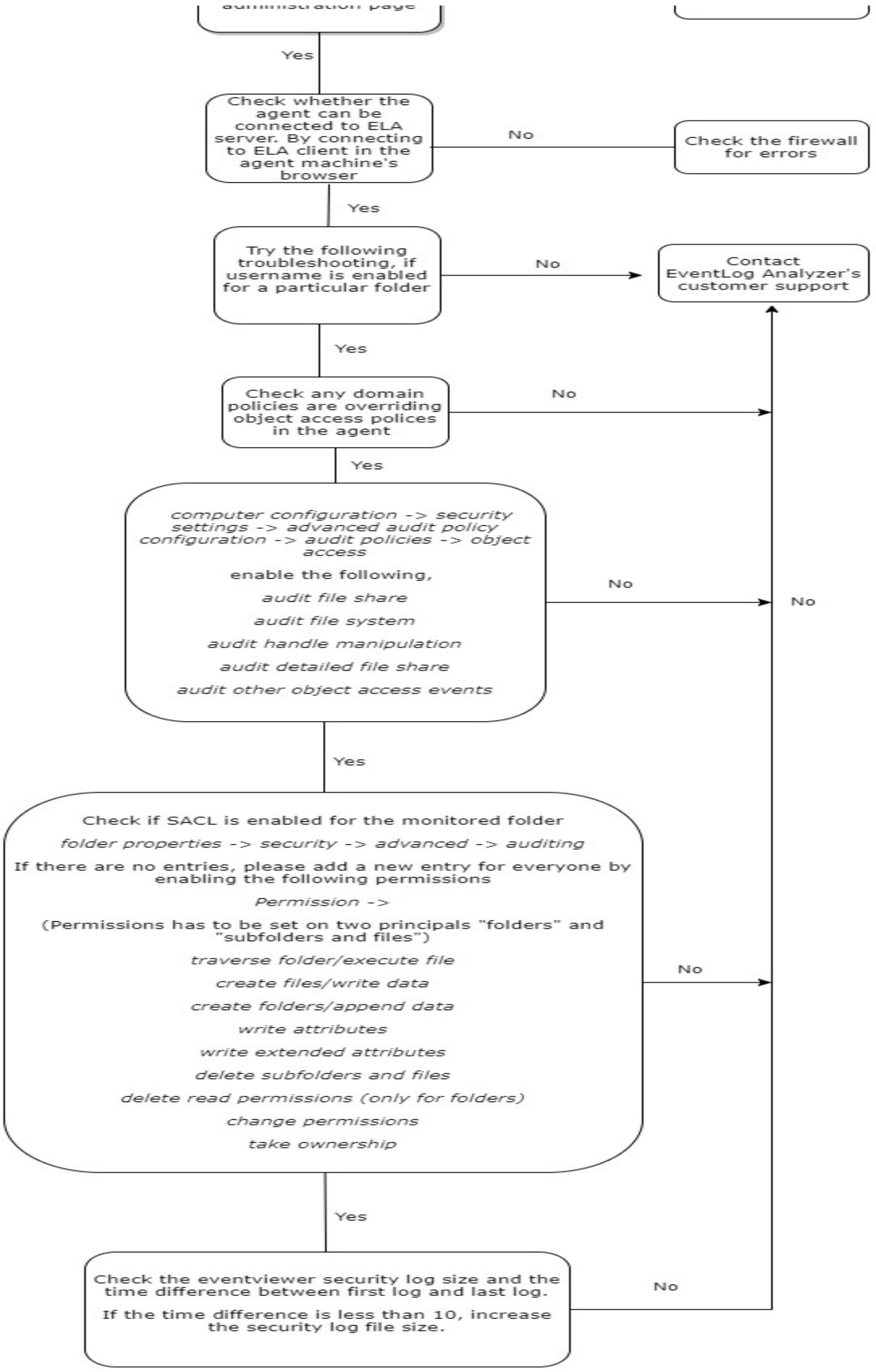
Steps to edit maximum attempts or disable captcha:

- Login to your JIRA On-Premise account.
- In the top right corner, select Administration and go to System > General Configuration > Edit Settings.
- Go to the Maximum Authentication Attempts Allowed field and enter the desired value. When you exceed this limit, you have to login to your JIRA On-Premise account with captcha verification again. Otherwise, you won't be able to configure EventLog Analyzer with JIRA On-Premise even with valid credentials.
- If you leave this field blank, captcha will be disabled. You can attempt to integrate EventLog Analyzer with JIRA On-Premise even after multiple authentication failures.

File Integrity Monitoring (FIM) troubleshooting

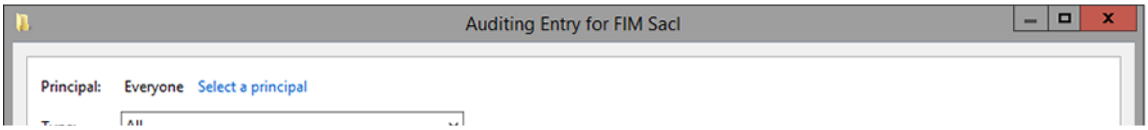
Try the following troubleshooting, if username is enabled for a particular folder.


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


administration page
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 polices 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 by 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

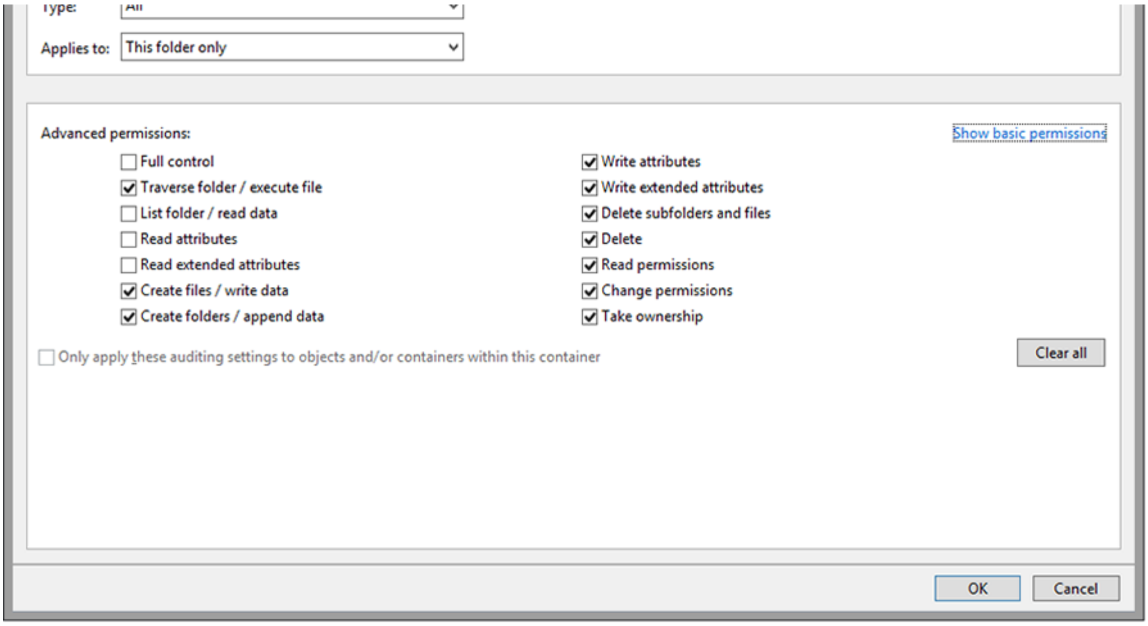
The following GUI is for the SACL entry in folder properties.



Auditing Entry for FIM Sacl

Principal: Everyone Select a principal

Type: All



Type: All

Applies to: This folder only

Advanced permissions:

☐ Full control
☑ Traverse folder / execute file
☐ List folder / read data
☐ Read attributes
☐ Read extended attributes
☑ Create files / write data
☑ Create folders / append data
☑ Write attributes
☑ Write extended attributes
☑ Delete subfolders and files
☑ Delete
☑ Read permissions
☑ Change permissions
☑ Take ownership

☐ Only apply these auditing settings to objects and/or containers within this container

Port management error codes

The following are some of the common errors, its causes and the possible solution to resolve the condition. Feel free to contact our support team for any information.

Port already used by some other application

Cause: Cannot use the specified port because it is already used by some other application.

Solution: This can be solved either by changing the port in the specified application or by using a new port.

If you use a new port, make sure to change the ports in the forwarding device either manually or using auto log forwarding configuration.

TLS not configured

Cause: HTTPS not configured to support TLS encrypted logs.

Solution: Configure the server to use either a self-signed certificate or a valid PFX certificate.

For more details visit Connection settings.

PFX not configured

Cause: HTTPS is configured, but the type of certificate is not supported.

Solution 1: If no valid certificate is used, it's recommended to use SelfSignedCertificate.

To find the type of certificate used,

- Open Conf/Server.xml file check for connector tag.
- Check the extention for the attribute keystoreFile.

Solution 2: If valid KeyStore certificate is used, execute the following command in the <EventLog Analyzer home>/jre/bin terminal.

keytool -importkeystore -srckeystore <certificate path> -destkeystore server.pfx -deststoretype PKCS12 -deststorepass <password> -srcalias tomcat -destalias tomcat

For more details visit Connection settings.

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>

Handling duplicated Windows devices

Problem statement:

Some Windows devices appear duplicated due to a user interface issue identified as ELA 12260.

Action taken:

Local collector association:

Duplicated devices with the oldest log collection timestamps will be deleted if they are linked to a local collector.

Remote collector association with shorter last message time:

Duplicated devices with the oldest log collection timestamps will be disabled if:

They are linked to a remote collector.

The difference between the current date and the last message time is less than the retention period.

Remote collector association with longer last message time:

Duplicated devices with the oldest log collection timestamps will be deleted if:

They are associated with a remote collector.

The difference between the current date and the last message time exceeds the retention period.

Profile remapping:

If any of the deleted or disabled devices were previously configured under the following profiles: Application, Import, Alert, Report, Log Collection Filter, Syslog Forwarder, Agent, they will be remapped to ensure continued functionality.

Action required by the customer:

Device reconfiguration:

For configurations pertaining to device groups, log collection failure alerts, compliance and custom log parser, please reconfigure the respective device. The erroneous device may have been mistakenly configured due to the UI issue mentioned above.

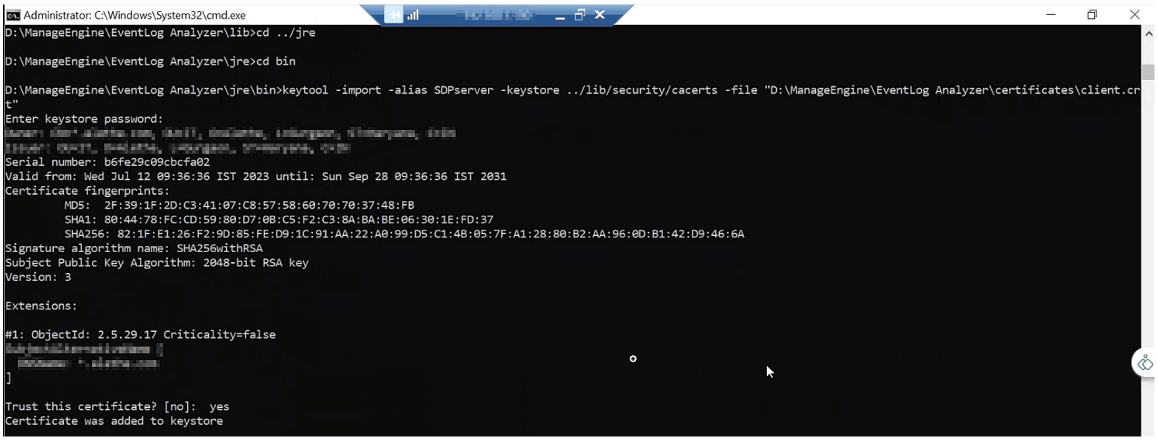
When forwarding audit logs, sometimes default policies in Red Hat systems with Security enhancement (SElinux) won't allow the audit logs to be read.

- Issue: When SELinux (Security Enhancement) is enabled, some default policies prevent audit logs from Red Hat Linux systems from being read during the forwarding process.
- Solution: The audit logs can be forwarded by adding "active=yes" in etc/audisp/plugins.d/syslog.conf or create the file in etc/audit/plugins.d/syslog.conf for CentOS/RHEL v8 and later with the below entries:

Note: This will forward the audit logs to the syslog service. Log Forwarding via Syslog Service should be enabled to receive the logs in EventLog Analyzer server.

How to add an organization-wide proxy certificate in EventLog Analyzer?

- Ensure that you have the proxy certificate file available before running the command.
- Use the keytool utility to import the proxy certificate into EventLog Analyzer's JRE certificate store. The command should be executed from <EventLog Analyzer Home>/jre/bin.



```
D:\ManageEngine\EventLog Analyzer\lib>cd ../jre

D:\ManageEngine\EventLog Analyzer\jre>cd bin

D:\ManageEngine\EventLog Analyzer\jre\bin>keytool -import -alias SDPserver -keystore ../lib/security/cacerts -file "D:\ManageEngine\EventLog Analyzer\certificates\client.cr
t"
Enter keystore password:
[redacted]
Serial number: b6fe29c09cbcfa02
Valid from: Wed Jul 12 09:36:36 IST 2023 until: Sun Sep 28 09:36:36 IST 2031
Certificate fingerprints:
         MD5:  2F:39:1F:2D:C3:41:07:C8:57:58:60:70:70:37:48:FB
         SHA1: 80:44:78:FC:CD:59:80:D7:0B:C5:F2:C3:8A:BA:BE:06:30:1E:FD:37
         SHA256: 82:1F:E1:26:F2:9D:85:FE:D9:1C:91:AA:22:A0:99:D5:C1:4B:05:7F:A1:28:80:B2:AA:96:0D:B1:42:D9:46:6A
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.17 Criticality=false
[redacted]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

```
D:\ManageEngine\EventLog Analyzer\jre\bin>_
```

- Enter the keystore password. Note that the default password is changeit.

Error statuses in File Integrity Monitoring (FIM).

Permission denied

Causes

- Credentials may be incorrect.
- Credentials with insufficient privileges.
- There might be a temp folder available with insufficient privileges for the user.
- The user does not have privileges for agent folder.

Solutions

- Credentials can be checked by accessing the SSH terminal.
- Credentials with the privilege to start, stop, and restart the audit daemon, and also transfer files to the Linux device are necessary.
- Setting Privilege for temp if available.
- Setting Privileges for the agent folder. For CentOS/RHEL v8 and later/Ubuntu/openSUSE/Debian/Fedora: For CentOS/RHEL v6 to v7.9:

Audit service unavailable

Cause

- The audit daemon service is not present in the selected Linux device.

Solution

- The audit daemon package must be installed along with Audisp.

Access restriction from SELinux

Cause

- SELinux hinders the running of the audit process.

Solutions

- SELinux's presence could be checked using getenforce command.
- Configure SELinux in permissive mode. After changing it to the permissive mode, navigate to Manage Agent page and click on Reinstall to reinstall the agent.

Agent upgrade failure

Causes

- No connectivity with the agent during product upgrade.
- Incorrect credentials.

Solutions

- Manually install the agent by navigating to the Manage Agent page.
- To install agent:

  Windows device: Run the EventLogAgent.msi.

  Linux device: Execute chmod +x EventLogAgent.bin, then run EventLogAgent.bin.

Agent Installation Failed

Causes

- Machine may be in the offline mode.
- Machine may not exist.
- Network path may not be reachable.

Solutions

- To confirm if the device exists, it could be pinged.
- Manually install the agent by navigating to the Manage Agent page.

Agent Installation on Incompatible Platform

Causes

- The agent is installed on a host which has neither a Linux nor a Windows OS.

Solutions

- Supported Linux distributions are CentOS, Debian, Fedora, openSUSE, Red Hat, and Ubuntu.
- Windows versions greater than 5.2 (Windows Server 2003) are supported.

ACL Package is not installed

Cause:

The acl package is not present in the selected Linux device.

Solution:

The acl package must be installed.

Agent could not be connected using SSH

Causes:

- Due to the missing SSH Algorithm.
- Insufficient privileges for the "/opt/ManageEngine"

Solutions:

- Ensure that any of the SSH Algorithms are present in the "/etc/ssh/sshd_config" file.
- Setting privilege for the " /opt/ManageEngine "

How to check if Immutable Rule is enabled in auditd?

Execute the following command to verify that the immutable rule is enabled:

If "enabled 2" is present in the configuration, it indicates that the immutable rule is active. This setting will prevent the Linux agent from applying any newly configured audit rules to monitor the locations specified in EventLog Analyzer.

Solution:

- Run the below command to locate the immutable rule (-e 2) and comment out or remove the configuration from the relevant file.
- Reboot the machine to apply the updated configuration.
- To confirm that the immutable rule is no longer active, run the below command and check that "enabled 1" is present in the configuration.

Log Receiver

What should I do if the network capture driver is not available?

Network capture drivers are files that allow EventLog Analyzer to capture and process incoming network logs from various sources. These include files such as npf.sys, Packet.dll, and wpcap.dll. These files must be stored in the Windows System Directories to ensure they are accessible to any application that requires them.

If the network capture driver is unavailable, you should move the files from the EventLog Analyzer installation directory to the Windows System Directories. To do so, follow the steps below.

Steps to move network capture driver files to Windows system directories

- Navigate to <EventLogAnalyzer_Installation_Directory>\bin directory.
- Open command prompt with admin privileges and execute register-driver.exe.
- Check the output in the console to ensure that the files are copied successfully.

In case of failure, proceed with the manual procedure, given below.

Steps to copy network capture driver files manually

- Copy the npf.sys, wpcap.dll and Packet.dll files from <EventLogAnalyzer_Installation_Directory>\lib\native folder.
- Paste the files in the following folders:

- npf.sys to C:\Windows\system32\drivers\
- wpcap.dll, Packet.dll to C:\Windows\system32\

Finally, open and refresh the Log Receiver window in EventLog Analyzer.

Note: These steps are applicable only if EventLog Analyzer is installed on Windows.

Auto Log Forwarding

Permission Denied

Causes:
Insufficient privileges for the rsyslog.conf or syslog.conf file.

Solutions:
Setting privilege for rsyslog.conf or syslog.conf file.

Log Collection and Reporting

I've added a device, but EventLog Analyzer is not collecting event logs from it

Probable cause: The device machine is not reachable from the EventLog Analyzer server machine
Solution: Check if the device machine responds to a ping command. If it does not, then the machine is not reachable. The device machine has to be reachable from the EventLog Analyzer server in order to collect event logs.
Probable cause: You do not have administrative rights on the device machine
Solution: Edit the device's details, and enter the Administrator login credentials of the device machine. Click Verify Login to see if the login was successful.

Error Code 0x251C

Probable cause: The device was added when importing application logs associated with it. In this case, only the specified application logs are collected from the device, and the device type is listed as unknown.

Solution:

- Click on the update icon next to the device name.
- Select the appropriate device type.
- Provide any other required information for the selected device type.
- Click on update.

I get an Access Denied error for a device when I click on "Verify Login" but I have given the correct login credentials

Probable cause: There may be other reasons for the Access Denied error.

Probable cause: There may be other reasons for the Access Denied error.

Solution: Refer the Cause and Solution for the Error Code you got during Verify login.

Error Code 00x80070005, 5

Scanning of the Windows workstation failed due to one of the following reasons:

- The login name and password provided for scanning is invalid in the workstation. Solution: Check if the login name and password are entered correctly.
- Remote DCOM option is disabled in the remote workstation Solution:
  Check if Remote DCOM is enabled in the remote workstation. If not enabled, then enable the same in the following way:

- Select Start > Run.
- Type dcomcnfg in the text box and click OK.
- Select theDefault Propertiestab.
- Select theEnable Distributed COMin this machine checkbox.
- Click OK.
  To enable DCOM on Windows XP devices:

  Select Start > Run

- Type dcomcnfg in the text box and clickOK
- Click on Component Services > Computers > My Computer
- Right-click and selectProperties
- Select the Default Propertiestab
- Select theEnable Distributed COM in this machine checkbox
- ClickOK
- User account is invalid in the target machine.

Check if the user account is valid in the target machine by opening a command prompt and executing the following commands:

If these commands show any errors, the provided user account is not valid on the target machine.

Error Code 0x80041003

The user name provided for scanning does not have sufficient access privileges to perform the scanning operation. This user may not belong to the Administrator group for this device machine.

Solution: Move the user to the Administrator Group of the workstation or scan the machine using an administrator (preferably a Domain Administrator) account.

Error Code 0x800706ba

A firewall is configured on the remote computer. Such exceptions mostly occur in Windows XP (SP 2), when the default Windows firewall is enabled.

Solution:

- Disable the default Firewall in the Windows XP machine:
  SelectStart > Run

  Type Firewall.cpl and click OK

In the General tab, click Off

Click OK

- If the firewall cannot be disabled, launch Remote Administration for administrators on the remote machine by executing the following command:
  After scanning, you can disable Remote Administration using the following command:

Error Code 0x80040154

- WMI is not available in the remote windows workstation. This happens in Windows NT. Such error codes might also occur in higher versions of Windows if the WMI Components are not registered properly.
  Solution: Install WMI core in the remote workstation.
- WMI Components are not registered.
  Solution: Register the WMI DLL files by executing the following command in the command prompt:
  winmgmt /RegServer

Error Code 0x80080005
There is some internal execution failure in the WMI service (winmgmt.exe) running in the device machine. The last update of the WMI Repository in that workstation could have failed.

Solution:
Restart the WMI Service in the remote workstation:

- Select Start > Run
- Type Services.msc and click OK
- In the Services window that opens, select Windows Management Instrumentation service.
- Right-click and select Restart

Error Code 1722, 1726, 1753, 1825

Probable cause: The device machine RPC (Remote Procedure Call) port is blocked by another firewall.
Solution: Unblock the RPC ports in the firewall.

For any other error codes, refer the MSDN knowledge base.

I have added an Custom alert profile and enabled it. But the alert is not generated in EventLog Analyzer even though the event has occurred in the device machine

Probable cause: The alert criteria have not been defined properly

Solution: Please ensure that the required fields in the Add Alert Profile screen have been given properly.Check if the e-mail address provided is correct. Ensure that the Mail server has been configured correctly.

When I create a Custom Report, I am not getting the report with the configured message in the Message Filter

Probable cause: The message filters have not been defined properly
Solution:When you are entering the string in the Message Filters for matching with the log message, ensure you copy/enter the exact string as shown in the Windows Event Viewer.
e.g., Logon Name:John

MS SQL server for EventLog Analyzer stopped

Probable cause: The transaction logs of MS SQL could be full
Solution: If the EventLog Analyzer MS SQL database transaction logs are full, shrink the same with the procedure given below:

- Stop the Eventlog Analyzer Server/Service (Check the Eventlog Analyzer server machine's Task Manager to ensure that the processes 'SysEvtCol.exe', 'Java.exe' are not running).
- Connect MS SQL client (using Microsoft SQL Server Management Studio) and execute the below query:
  sp_dboption 'eventlog', 'trunc. log on chkpt.', 'true'
  To execute the query, select and highlight the above command and press F5 key.
- After executing the above command, select and highlight the below command and press F5 key to execute it.
  DBCC SHRINKDATABASE (eventlog)
- Note: This process will take some time, based on the EventLog Analyzer database size.
- Start the Eventlog Analyzer.

I successfully configured Oracle device(s), still cannot view the data

If Oracle device is Windows, open Event viewer in that machine and check for Oracle source logs under Application type. If Linux, check the appropriate log file to which you are writing Oracle logs. If the Oracle logs are available in the specified file, still EventLog Analyzer is not collecting the logs, contact EventLog Analyzer Support.

The user name provided for scanning does not have sufficient access privileges to perform the scanning operation. Probably, this user does not belong to the Administrator group for this device machine

The Syslog host is not added automatically to EventLog Analyzer/the Syslog reception has suddenly stopped

Check EventLog Analyzer's live Syslog Viewer for incoming Syslog packets.

If you are able to view the logs, it means that the packets are reaching the machine, but not to EventLog Analyzer. You need to check your Windows firewall or Linux IP tables.

If you are not able to view the logs in the Syslog viewer, then check if the EventLog Analyzer server is reachable. This can be done in the following ways:

- Ping the server.
- For TCP, you can try the command telnet <ela_server_name> <port_no> where 514 is the default TCP port.
- tcpdump

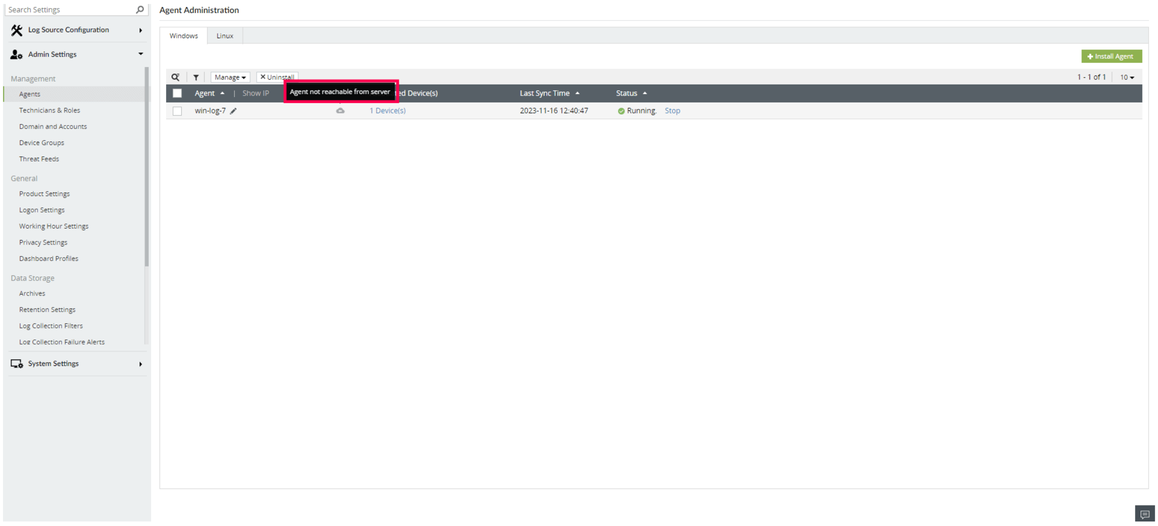
If reachable, it means there was some issue with the configuration. If not reachable, then you are facing a network issue.

EventLog Analyzer agent management

If you have trouble installing the agent using the EventLog Analyzer console, GPOs or software installation tools, you can try to install the agent manually. Here the the steps for manual agent installation.

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).



Agent	Show IP		ed Device(s)	Last Sync Time	Status
win-log-7		☁	1 Device(s)	2023-11-16 12:40:47	✓ Running. Stop

In such a state, the following actions performed on the agent will not reflect immediately.

- Force restart agent
- Stopping agent
- Updating device IP and credentials
- Adding, deleting, enabling or disabling Device/LogCollection Filter/FIM
- Updating FIM template
- Updating monitoring interval

ⓘ Note

This icon does not hinder the log collection process, logs will be collected regardless of the presence of this icon.

Furthermore, actions such as starting and uninstalling the agent must be manually executed, as they cannot be performed through the UI due to invalid credentials.

If the cloud icon, indicating that the agent is unreachable from the server, is to be hidden or if real-time actions are required, please make sure to update the credentials accurately.

Agent not communicating is displayed as the agent status

"Agent not communicating" is the agent status that appears if there has been a prolonged time of no communication between the agent and the server.

In such a state, the following actions should be performed:

- Ensure the EventLog Analyzer server is accessible from the agent device.
- Verify if the latest server details are updated in the registry [Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ZOHO Corp\EventLogAnalyzer\ServerInfo]
- Check if any antivirus or firewall is blocking the communication between the server and agent. If so, provide an exclusion for EventLog Analyzer agent from AntiVirus.
- Ensure the EventLog Analyzer Agent service is running, and start it if necessary.

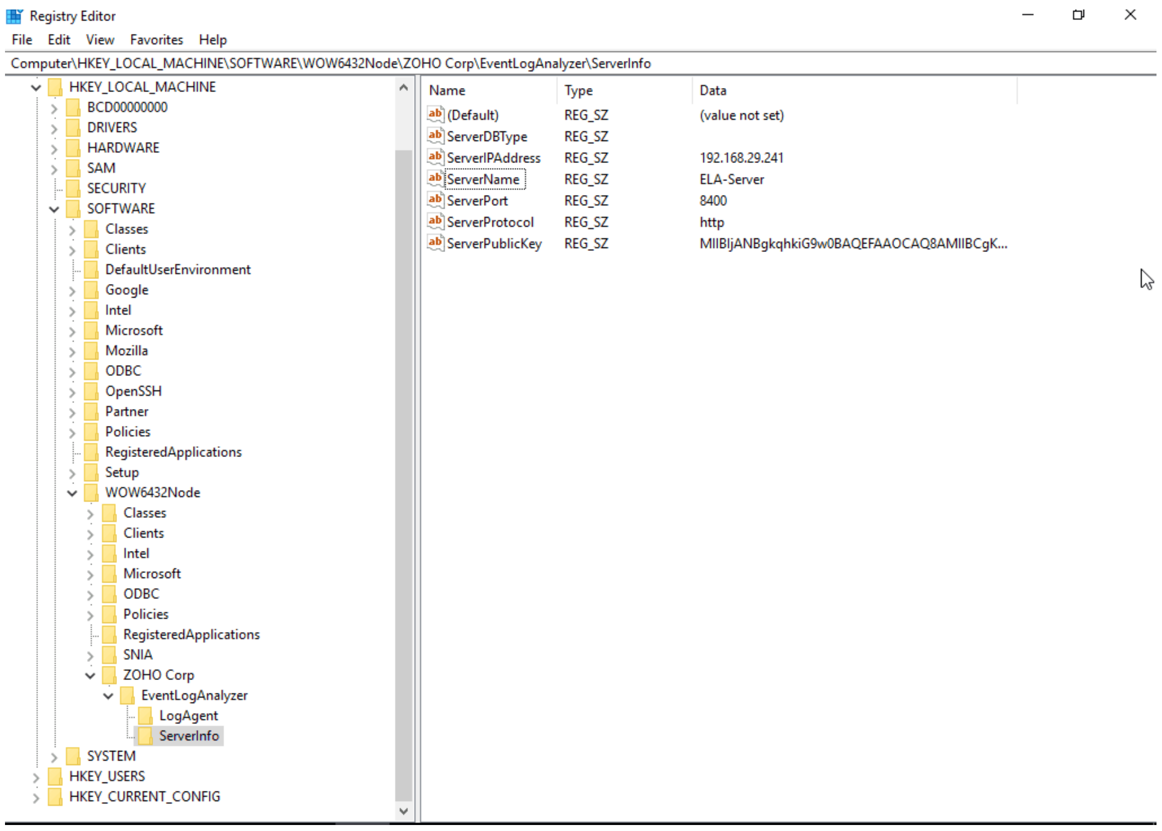
> ⓘ Note
>
> Contact support if the issue persists even after following the above steps.

How to update ServerInfo in an EventLog Analyzer agent after server migration?

Steps to update ServerInfo in an EventLog Analyzer agent after server migration

Windows Agent

- Open Registry Editor and navigate to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ZOHO Corp\EventLogAnalyzer\



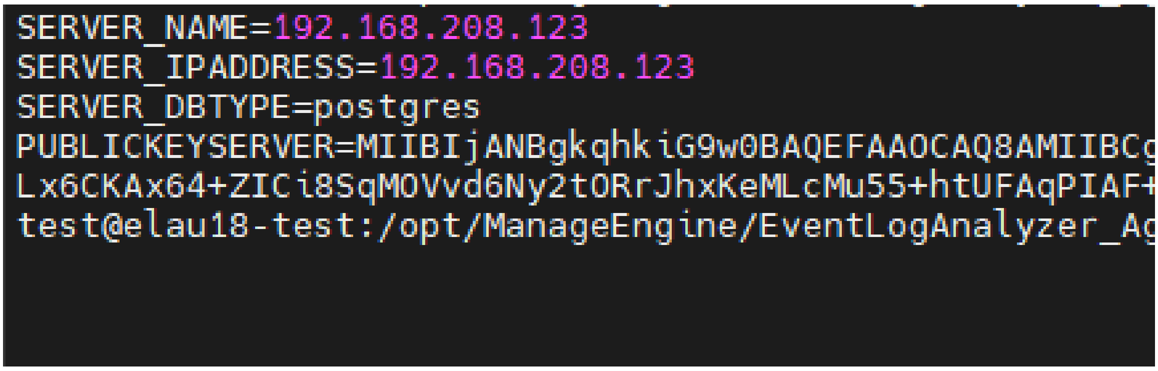
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ZOHO Corp\EventLogAnalyzer\ServerInfo

Name	Type	Data
(Default)	REG_SZ	(value not set)
ServerDBType	REG_SZ	
ServerIPAddress	REG_SZ	192.168.29.241
ServerName	REG_SZ	ELA-Server
ServerPort	REG_SZ	8400
ServerProtocol	REG_SZ	http
ServerPublicKey	REG_SZ	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgK...

- 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:

- Check if other applications are blocking the CPU cycle for EventLog Analyzer.
- If a virtual machine is used, check for over provisioning or if snapshots are affecting the performance.
- If the log flow rate is high, please check our tuning guide.

Error messages while adding STIX/TAXII servers to EventLog Analyzer

While I was trying to add a STIX/TAXII server to EventLog Analyzer, I got the following error messages. What do they mean?

This feature has been disabled for Online Demo!

This error message pops up when the feature you tried to use is not available in the online demo version of EventLog Analyzer. To try out that feature, download the free version of EventLog Analyzer.

Connection failed. Please try configuring proxy server.

This error message can be caused because of different reasons. It might be due to network issues, proxy related issues, bad requests in the network, or if the URL is unable to locate a STIX/TAXII server.

Failed to connect to the URL.

This error message denotes that the URL entered is malformed.

Authorization failed.

This error message signifies that the credentials entered are wrong.

SSL Troubleshooting steps

Certificate name mismatch

Description:

This error occurs when the common name of the SSL Certificate doesn't exactly match the hostname of the server in which the EventLog Analyzer is installed.

Solution:

Please get a new SSL certificate for the current hostname of the server in which EventLog Analyzer is installed.

Invalid Certificate

Description:

This error occurs when the SSL certificate you have configured with EventLog Analyzer is invalid. A certificate can become invalid if it has expired or other reasons.

Solution:

Please configure EvnetLog analyzer to use a valid SSL certificate.

Certificate is not trusted by JVM

Description:

This exception occurs when you configure a SMTP mail server or a web server with SSL in EventLog Analyzer, and the server uses a self-signed certificate. The Java Runtime Environment used in EventLog Analyzer will not trust self-signed certificates unless it is explicitly imported.

Solution:

You need to import the self-signed certificates used by the server in the JRE package used by EventLog Analyzer. Follow the steps given below:

Step 1: Download the certificate

For SMTP servers:

Note:

- To download the certificate used by SMTP server, you must have OpenSSL installed. You can download it from here.
- Open the command prompt and change to the bin folder in the OpenSSL installed location.
- Now run the following command,

- For example, openssl.exe s_client -connect smtp.gmail.com:587 -starttls smtp > gmailcert.cer

For Web Servers:

- Open the web URL in a browser.
- Click the padlock icon on the address bar.
- Click More Information. This opens the Certificate Viewer window showing the certificate used by that web server.
- Click View Certificate.
- When the Certificate window showing Certificate Information Authority opens, click the Details tab.
- Click Copy to File.
- In the Certificate Export Wizard that opens, click Next.
- Select the format as DRE encoded binary X.509 (.CER) and click Next.
- Enter the path where you wish to save the file and click Finish.

Step 2: Import the certificates in JRE package of EventLog Analyzer.

- Open a command prompt and change to the \jre\bin folder. For example: C:\ManageEngine\EventLogAnalyzer\jre\bin.
- Run the following command,
- For example: Keytool -importcert -alias myprivateroot -keystore ..\lib\security\cacerts -file C:\smtpcert.cer
- Enter changeit when prompted for a password.
- Enter y when prompted Yes or No.
- Close the command prompt and restart EventLog Analyzer.

Threat Intelligence Troubleshooting Tips

IP Geolocation data store corruption

This may happen when the product is shutdowns while the data store is updating and there is no backup available.

Troubleshooting steps:

- This is a rare scenario and it happens only when the product shuts down abruptly during the first ever download of IP geolocation data.
- There is no need for a troubleshoot as EventLog Analyzer will automatically download the data in the next schedule. Please note that the IP geolocation data gets automatically updated daily at 21:00 hours.

IP Geolocation data update failure

This occurs when there is no internet connection on EventLog Analyzer server or if the server is

This occurs when there is no internet connection on EventLog Analyzer server or if the server is unreachable.

Troubleshooting steps:

- Make sure you have a working internet connection.
- Whitelist the following in your firewall:

- https://creator.zoho.com/
- https://creatorapp.zohopublic.com/

Log360 Cloud threat feed server is unavailable

This may happen when the product is unable to connect to the Log360 Cloud feeds server.

Case 1: Access is Blocked under firewall

Probable cause: The access to Log360 Cloud feeds server may be blocked under the firewall.

Solution:

- Review the firewall settings and look for any rules that might block the access.
- If you find any blocking rules, create a new rule that allows the traffic to the Log360Cloud feeds server.
- Save the new rule and update the firewall with the new settings.

Case 2: Unable to resolve DNS

Probable cause: The machine could not resolve the domain using its DNS resolver.

Solution:

- Check the DNS settings on the machine on which the product is running. Ensure that the DNS server settings are correct and that the machine is able to communicate with the DNS server.
- Try to resolve the domain name using a command line tool such as nslookup or dig to confirm that the DNS resolution is failing.
- Check if there are any firewalls or security settings that may be blocking DNS traffic.
- If using a proxy server resolves the DNS of the host involved, configure the proxy server in the product connection settings.

If none of the above works and the issue persists, contact our Technical Support team.

License file not found

If the license file cannot be accessed in the following page https://licensing.manageengine.com , kindly contact eventlog-support@manageengine.com

Update Access Key(Log360 Cloud Threat Analytics)

This can happen if the access key gets invalidated.

To regenerate the access key, please follow the below steps:

- Login to https://log360feeds.manageengine.com/
- Click on Regenerate Key.
- In the product, go to Settings > Admin Settings > Threat Feeds > Advanced Threat Analytics > Log360 Cloud Threat Analytics and add the new key.

VirusTotal API Quota Limit Exceeded

This happens when you exceed one of your quotas (per minute, per day or per month). Daily quotas are reset every day at 00:00 UTC.

Troubleshooting steps:

- Sign in into VirusTotal Account.
- Find your API quota under Profile → API Key → API Consumption for last 30 days (Check API limit for the day)

Internal Server Error

There may be various reasons for receiving this error.

- The request has been submitted to VirusTotal and there are server-side internal issues.
- The request has been submitted to Log360 Cloud Threat Analytics, and there are server-side internal issues.

Customers are advised to retry in a while, and if the same error is encountered, kindly contact " eventlog-support@manageengine.com "

Default Threat Sync Failure

This occurs when EventLog Analyzer server faces network connectivity issues.

Troubleshooting steps:

Make sure you have a working internet connection.

Whitelist the following in your firewall:

- https://creator.zoho.com/
- https://creatorapp.zohopublic.com/

Time zone

What to do if Daylight Savings Time(DST) is practiced in your region, but the product is not DST updated?

This occurs, when the JRE present in the product is not updated of the changes.

- Download Java SE TZUpdater from the official Oracle site. link "https://www.oracle.com/java/technologies/javase-tzupdater-downloads.html"

- Take back up of <Eventlog Analyzer_HOME>\jre
- After downloading, extract and copy the file tzupdater.jar to <EventLog Analyzer HOME>\jre\bin
- Stop EventLog Analyzer Service.
- Open Command Prompt as Administrator, navigate to <EventLog Analyzer HOME>\jre\bin.
- Execute the following command
  "java -jar tzupdater.jar -l <please select the latest time zone updater link from https://data.iana.org/time-zones/releases/>"
  For example
  Note:
  Incase customer environment is restricted from Online access follow 6.1 and 6.2.

  6.1: please select the latest time zone updater link from https://data.iana.org/time-zones/releases/ and download the latest timezone zip in tar.gz format.

  6.2 Execute the following command "java -jar tzupdater.jar -l file:downloaded_timezone_data_zip.tar.gz"

  For example
- Start EventLog Analyzer Service

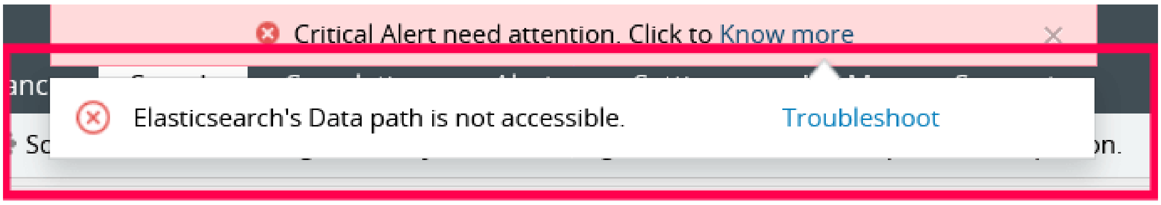
Search Engine - Elasticsearch

Data path not accessible

What is Elasticsearch data path?

Elasticsearch writes the data you index to indices, and data streams to a data directory which is available in elasticsearch.yml. Search and indexing will not work if the data path is not accessible.

If the data path is not accessible to write, the following notification will be shown.


Critical Alert need attention. Click to Know more

Elasticsearch's Data path is not accessible.

Troubleshooting steps

- Open elasticsearch.yml file,search for path.data and find its value. elasticsearch.yml file can be found in <Installation Dir>/EventLog Analyzer/ES/config/elasticsearch.yml
- Make sure that both read and write permissions are enabled for the service account running EventLog Analyzer.
- If the path is a network location, then ensure connectivity and that the network path is accessible from the machine running EventLog Analyzer. Verify that there are no latency issues between the server and remote data path.

If there is a need to change the data path of Elasticsearch, kindly follow this guide.

Device Auto Allocation

Failed to disable Auto Allocation.

Issue Description: Failed to disable Auto Allocation.

Possible Causes: Unable to update the database values due to environment issues.

Resolution: Try again after sometime.

Failed to enable Auto Allocation.

Issue Description: Failed to enable Auto Allocation.

Possible Causes: Unable to update the database values due to environment issues.

Resolution: Try again after sometime.

Failed to enable Auto Allocation Policies.

Issue Description: Failed to enable Auto Allocation Policies.

Possible Causes: Unable to update the database values due to environment issues.

Resolution: Try again after sometime.

Failed to disable Auto Allocation Policies.

Issue Description: Failed to disable Auto Allocation Policies.

Possible Causes: Unable to update the database values due to environment issues.

Resolution: Try again after sometime.

Failed to update Auto Allocation Policy.

Issue Description: Failed to update Auto Allocation Policy.

Possible Causes: Unable to update the database values due to environment issues.

Resolution: Try again after sometime.

Failed to update sync settings.

Issue Description: Failed to update Auto Allocation Policy.

Possible Causes:

- Unable to update the database values due to environment issues.
- Unable to communicate with ADAudit Plus.
- ADAudit Plus server may down.

Resolution: Check ADAudit Plus Server status and Communication. If those are correct, Try again after sometime it may be an environment issue.

8.2. EventLog Analyzer - Frequently Asked Questions

Last updated on: September 12, 2025

What is the difference between the Free and Professional Editions?

The Free Edition of EventLog Analyzer is limited to handling event logs from a maximum of five devices, whereas the Professional Edition can handle event logs from an unlimited number of devices. There is no other difference between the two editions, with respect to features or functionality.

Is a trial version of EventLog Analyzer available for evaluation?

Yes, a 30-day free trial version can be downloaded here. At the end of 30 days it automatically becomes a Free Edition, unless a new license is applied.

Does the trial version have any restrictions?

The trial version is a fully functional version of EventLog Analyzer Premium Edition. When the trial period expires, EventLog Analyzer automatically reverts to the Free Edition.

Do I have to reinstall EventLog Analyzer when moving to the paid version?

No, you do not have to reinstall or shut down the server. You just need to enter the new license file in the Upgrade License box.

What devices can EventLog Analyzer collect event logs from?

ManageEngine EventLog Analyzer can collect and analyze logs from a wide range of sources, including Windows and Linux/Unix systems, network devices like Cisco switches and routers, and other syslog-supported devices.

However, the capability depends on the operating system where it is installed:

- On Windows, it can collect event logs from Windows devices and syslogs from Unix systems, network devices, and applications.
- On Linux/Unix, it primarily collects syslogs from Unix systems, network devices, and other syslog-supported sources, but can also collect event logs from Windows machines using agent-based or agentless methods.

How many users can access the application simultaneously?

This depends only on the capacity of the server on which EventLog Analyzer is installed. The EventLog Analyzer license does not limit the number of users accessing the application at any time.

EventLog Analyzer runs in a web browser. Does that mean I can access it from anywhere?

Yes. As long as the web browser can access the server on which EventLog Analyzer is running, you can work with EventLog Analyzer from any location.

How do I buy EventLog Analyzer?

You can buy EventLog Analyzer directly from the ManageEngine Online Store, or from a reseller near your location.

Can EventLog Analyzer work if DCOM is disabled on remote systems?

For EventLog Analyzer to collect logs from remote Windows systems, DCOM must be enabled if you're using agentless log collection. However, if you're using agent-based collection, DCOM is not required.

How to monitor Windows Events in EventLog Analyzer Linux Installation?

You can collect logs from Windows devices in two ways with EventLog Analyzer:

- Convert Windows event logs to syslogs and forward them to EventLog Analyzer.
- Install an agent on the Windows device to directly monitor and collect logs.

What are the differences between ELA installed in Windows and Linux machines?

Most features from windows and linux are identical. Tight integration for windows machines are not available in linux builds, Although there are manual steps available to achieve the missing windows functionality.

#	Feature	UI	Windows Instance	Linux Instance	How to achieve the missing functionality?
1	Domain and workgroup discovery	ELA UI → Settings → Domains and Workgroup	Available	N/A	N/A
2	Device discovery	ELA UI → Settings → Devices → Windows Devices →	Available	N/A	Manually enter device name and associate them with

#	Feature	Devices → Add Device(s) UI	Windows Instance	Linux Instance	them with Agents. How to achieve the missing functionality?
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	
		ELA UI →			We can collect logs from MSSQL in

#	Feature	UI	Windows Instance	Linux Instance	How to achieve the missing functionality?
7	MSSQL Discovery	Settings → Database Audit → Mssql Servers	Available	Not Available.	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:

- Processor - 6
- RAM - 16GB
- Disk Space - 1.2 TB
- Operating System - Windows 7, 2000, XP, 2003, Linux Ubuntu 8.0/9.0
- Web Browser - Microsoft Edge, or Mozilla Firefox 1.0

Look up System Requirements to see the minimum configuration required to install and run EventLog Analyzer.

Can I install EventLog Analyzer as a root user?

Yes, you can install EventLog Analyzer as the root user on Linux systems. However, it’s generally recommended to use a dedicated user account for better security. Installing as root modifies the installation directory’s permissions, which may cause issues if you attempt to start the server using a different user account later.

When I try to access the web client, another web server comes up. How is this possible?

The web server port you have selected during installation is possibly being used by another application. Configure that application to use another port, or change the EventLog Analyzer web server port.

Is a database backup necessary, or does EventLog Analyzer take care of this?

If you need to back up the database, you can do so via Settings > Data Storage > Database Settings. It's also recommended to regularly take snapshots or backups of the EventLog Analyzer installation directory for added data protection.

Please visit this page.

Configuration

How do I add devices to EventLog Analyzer so that it can start collecting event logs?

Please refer to the relevant pages below for detailed steps:

- Windows devices
- Syslog devices
- Application addition

How do I see session information of all users registered to log in to EventLog Analyzer?

The session information for each user can be accessed from the User Management link. Click the View link under Login Details against each user to view the active session information and session history for that user.

How to move EventLog Analyzer to a different machine/server?

Please follow these steps given here to migrate your existing EventLog Analyzer installation to a new machine/server.

How long can I store data in the EventLog Analyzer database?

EventLog Analyzer stores data in two formats: live logs in Elasticsearch and compressed logs in archives.

By default, live logs are retained for 32 days, but this duration can be customized based on your requirements.

For archived logs, retention can also be configured as per your needs; options include indefinite storage, 6 months, 3 months, and more.

How to change the log collection interval for Linux devices?

The log collection interval cannot be changed for Linux devices as EventLog Analyzer keeps listening for logs that come through open ports configured for syslog collection. Therefore, you will not be able to view the 'Change Monitor Interval' icon in the Device Management page for Syslog Devices.

Reporting

Why am I seeing empty graphs?

Graphs are empty if no data is available. If you have started the server for the first time, wait for at least one minute for graphs to be populated.

What are the types of report formats that I can generate?

Reports can be generated in HTML, CSV, and PDF formats. All reports are generally viewed as HTML in the web browser, and then exported to CSV or PDF format. However, reports that are scheduled to run automatically, or be emailed automatically, are generated only as PDF files.

Can't find an answer here? Check out the EventLog Analyzer user forum

Chapter 9 **Technical Support**

9.1. EventLog Analyzer Technical Support

Last updated on: September 12, 2025

EventLog Analyzer offers comprehensive, best-in-class technical assistance and documentation to support deployment and troubleshooting.

Take a look at our resources to find the answers:

- Go through the FAQ
- Look up the troubleshooting tips
- Browse through the EventLog Analyzer forum

Still finding trouble? Get in touch with our technical support team:

- Send an email to eventlog-support@manageengine.com
- Call toll free telephone number (+1 844 649 7766)
- Ask for a meeting (Zoho Meeting) – web conference

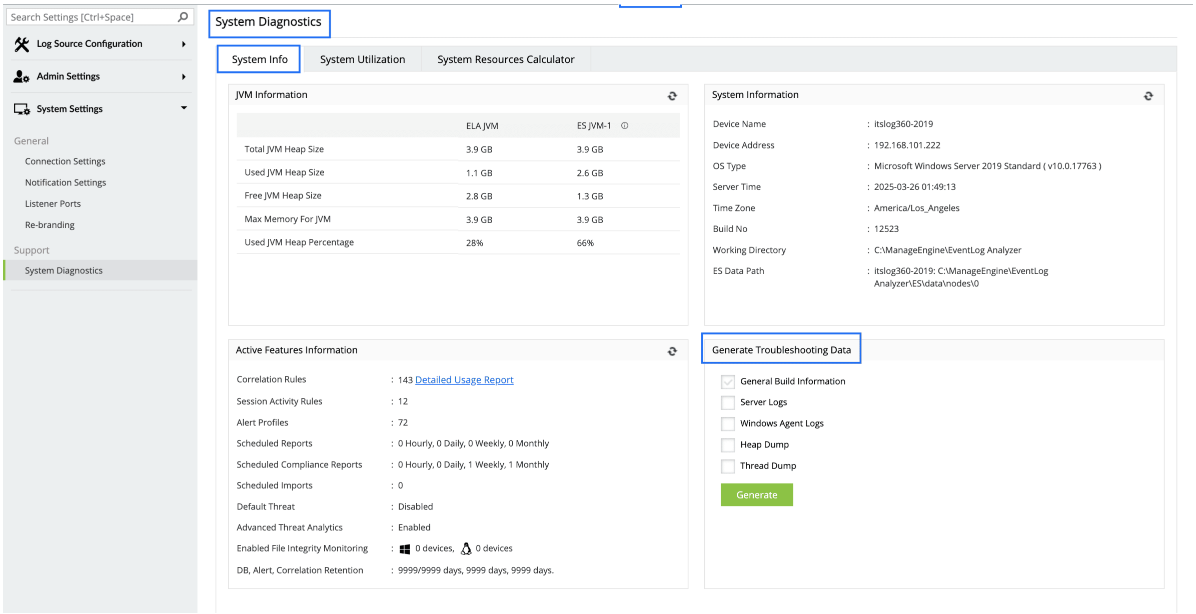
9.2. Create an EventLog Analyzer Support Information File (SIF)

Last updated on: September 12, 2025

In case you face an issue with log collection or any other aspect of EventLog Analyzer, please create a SIF and send it to support@eventloganalyzer.com. The SIF will help us analyze the issue and propose a solution. This article gives you the steps to generate SIF in different scenarios:

Creating SIF automatically

1. Login to the EventLog Analyzer web client and go to Settings -> System Diagnostics -> System Info tab.



JVM Information

	ELA JVM	ES JVM-1
Total JVM Heap Size	3.9 GB	3.9 GB
Used JVM Heap Size	1.1 GB	2.6 GB
Free JVM Heap Size	2.8 GB	1.3 GB
Max Memory For JVM	3.9 GB	3.9 GB
Used JVM Heap Percentage	28%	66%

System Information

Device Name	: itslog360-2019
Device Address	: 192.168.101.222
OS Type	: Microsoft Windows Server 2019 Standard (v10.0.17763)
Server Time	: 2025-03-26 01:49:13
Time Zone	: America/Los_Angeles
Build No	: 12523
Working Directory	: C:\ManageEngine\EventLog Analyzer
ES Data Path	: itslog360-2019: C:\ManageEngine\EventLog Analyzer\ES\data\nodes\0

Active Features Information

Correlation Rules	: 143 Detailed Usage Report
Session Activity Rules	: 12
Alert Profiles	: 72
Scheduled Reports	: 0 Hourly, 0 Daily, 0 Weekly, 0 Monthly
Scheduled Compliance Reports	: 0 Hourly, 0 Daily, 1 Weekly, 1 Monthly
Scheduled Imports	: 0
Default Threat	: Disabled
Advanced Threat Analytics	: Enabled
Enabled File Integrity Monitoring	: 0 devices, 0 devices
DB, Alert, Correlation Retention	: 9999/9999 days, 9999 days, 9999 days.

Generate Troubleshooting Data

☑ General Build Information
☐ Server Logs
☐ Windows Agent Logs
☐ Heap Dump
☐ Thread Dump

Generate

2. Under the Generate Troubleshooting Data window, you will see the following log upload options:

- General Build Information (Selected by default)- Provides general information about the server and product configuration.
- Server Logs- Compiles logs of the EventLog Analyzer instance, including Elasticsearch logs.
- Windows Agent Logs- Collects logs from Windows agents managed by this server. Requires access to the agent installed machine and credentials to collect the agent logs automatically.

  > Note: Logs from manually installed agents must be collected manually.

  How to collect agent logs manually?

  - Log in to the agent-installed machine.
  - Navigate to the installation folder of the agent (e.g., C:\Program Files (x86)\EventLogAnalyzer_Agent).
  - Locate the logs folder and compress it.

    - Upload the compressed logs to https://bonitas.zohocorp.com/.

- Heap Dump & Thread Dump- Logs are collected by the support team upon request when the server encounters performance issues.

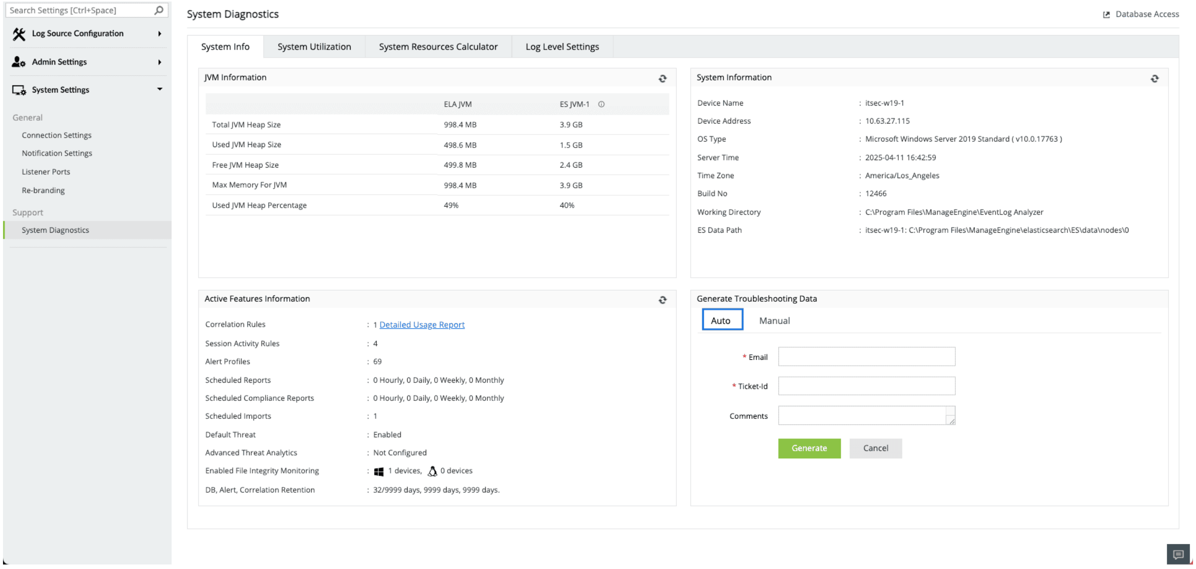
> ⓘ Note
>
> The generated logs will be present under: ManageEngine\EventLog Analyzer\server\support folder in ZIP format.

Steps to upload logs: Auto and Manual SIF creation

After selecting the required logs and clicking 'Generate', you can create a SIF file using either the Auto or Manual upload option.

Automated upload process:

1. Utilize the Auto option to compress and upload logs directly to the support team.
2. Provide the necessary details, such as your email ID and ticket ID (can be left blank if unavailable).
3. Upon uploading, an acknowledgment mail will be sent.



JVM Information

	ELA JVM	ES JVM-1 ⓘ
Total JVM Heap Size	998.4 MB	3.9 GB
Used JVM Heap Size	498.6 MB	1.5 GB
Free JVM Heap Size	499.8 MB	2.4 GB
Max Memory For JVM	998.4 MB	3.9 GB
Used JVM Heap Percentage	49%	40%

System Information

Device Name	: itsec-w19-1
Device Address	: 10.63.27.115
OS Type	: Microsoft Windows Server 2019 Standard (v10.0.17763)
Server Time	: 2025-04-11 16:42:59
Time Zone	: America/Los_Angeles
Build No	: 12466
Working Directory	: C:\Program Files\ManageEngine\EventLog Analyzer
ES Data Path	: itsec-w19-1: C:\Program Files\ManageEngine\elasticsearch\ES\data\nodes\0

Active Features Information

Correlation Rules	: 1 Detailed Usage Report
Session Activity Rules	: 4
Alert Profiles	: 69
Scheduled Reports	: 0 Hourly, 0 Daily, 0 Weekly, 0 Monthly
Scheduled Compliance Reports	: 0 Hourly, 0 Daily, 0 Weekly, 0 Monthly
Scheduled Imports	: 1
Default Threat	: Enabled
Advanced Threat Analytics	: Not Configured
Enabled File Integrity Monitoring	: 1 devices, 0 devices
DB, Alert, Correlation Retention	: 32/9999 days, 9999 days, 9999 days.

Generate Troubleshooting Data

Auto | Manual

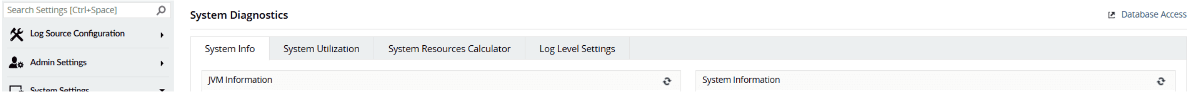
* Email

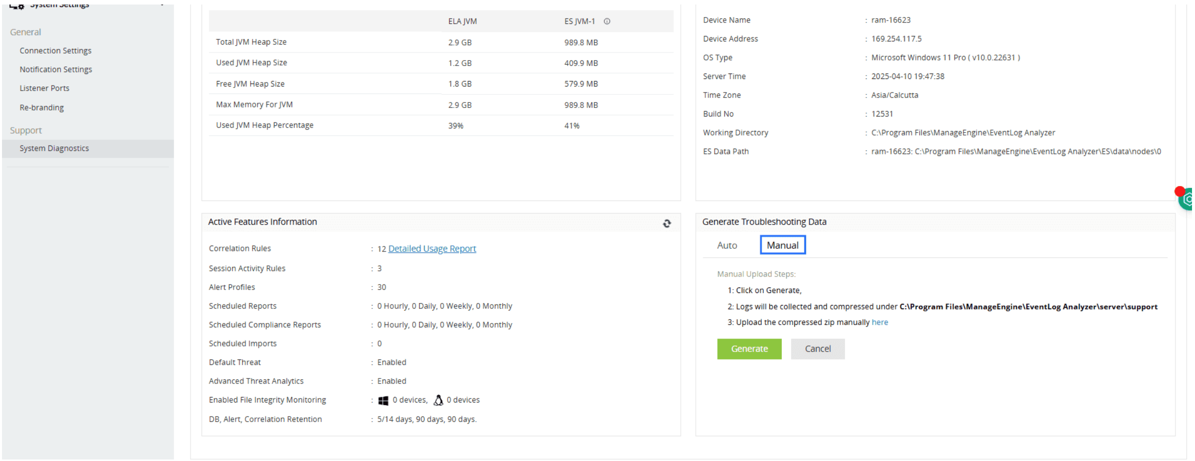
* Ticket-Id

Comments

Manual upload process:

1. Click on Generate.
2. Logs will be collected and compressed under C:\Program Files\ManageEngine\EventLog Analyzer\server\support.
3. Upload the compressed ZIP manually on the bonitas website.





	ELA JVM	ES JVM-1
Total JVM Heap Size	2.9 GB	989.8 MB
Used JVM Heap Size	1.2 GB	409.9 MB
Free JVM Heap Size	1.8 GB	579.9 MB
Max Memory For JVM	2.9 GB	989.8 MB
Used JVM Heap Percentage	39%	41%

Device Name : ram-16623
Device Address : 169.254.117.5
OS Type : Microsoft Windows 11 Pro (v10.0.22631)
Server Time : 2025-04-10 19:47:38
Time Zone : Asia/Calcutta
Build No : 12531
Working Directory : C:\Program Files\ManageEngine\EventLog Analyzer
ES Data Path : ram-16623: C:\Program Files\ManageEngine\EventLog Analyzer\ES\data\nodes\0

Active Features Information

Correlation Rules : 12 Detailed Usage Report
Session Activity Rules : 3
Alert Profiles : 30
Scheduled Reports : 0 Hourly, 0 Daily, 0 Weekly, 0 Monthly
Scheduled Compliance Reports : 0 Hourly, 0 Daily, 0 Weekly, 0 Monthly
Scheduled Imports : 0
Default Threat : Enabled
Advanced Threat Analytics : Enabled
Enabled File Integrity Monitoring : 0 devices, 0 devices
DB, Alert, Correlation Retention : 5/14 days, 90 days, 90 days.

Generate Troubleshooting Data

Manual Upload Steps:

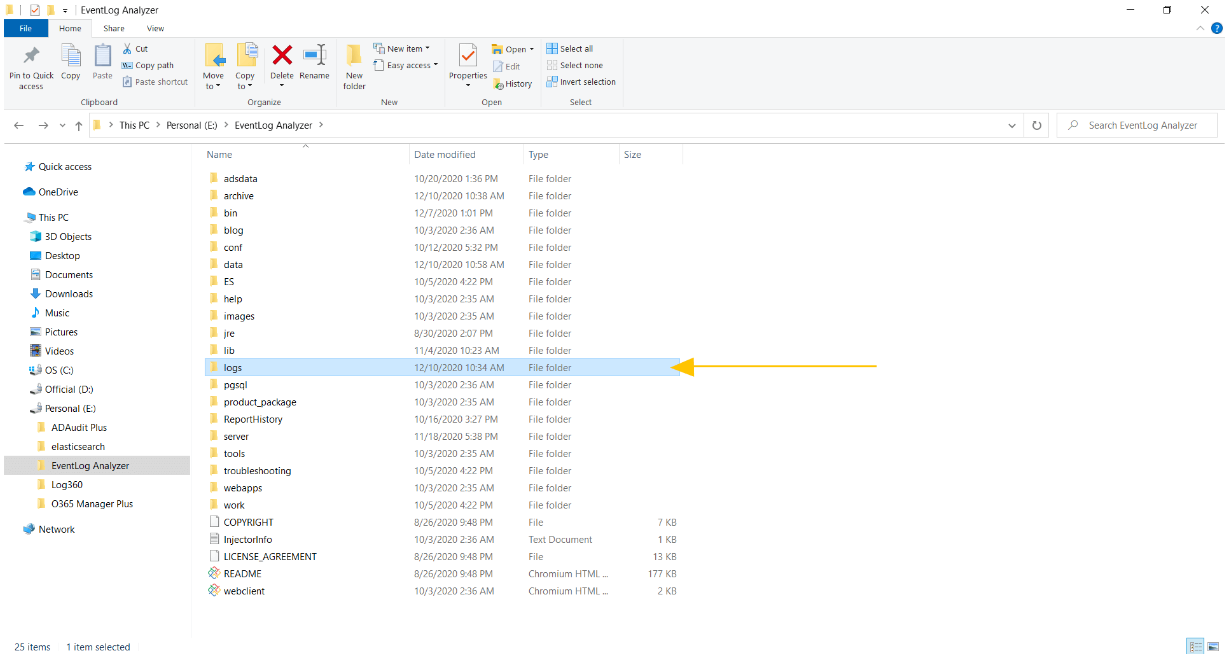
1: Click on Generate,

2: Logs will be collected and compressed under **C:\Program Files\ManageEngine\EventLog Analyzer\server\support**

3: Upload the compressed zip manually here

Procedure to create a SIF when the EventLog Analyzer server or web client is not working

If you are unable to create a SIF from the EventLog Analyzer GUI, you can zip the files under 'logs' folder, which is located in <EventLog Analyzer Home>/logs (default path) and upload the ZIP file using the following link: https://bonitas2.zohocorp.com/#to=eventlog-support@manageengine.com

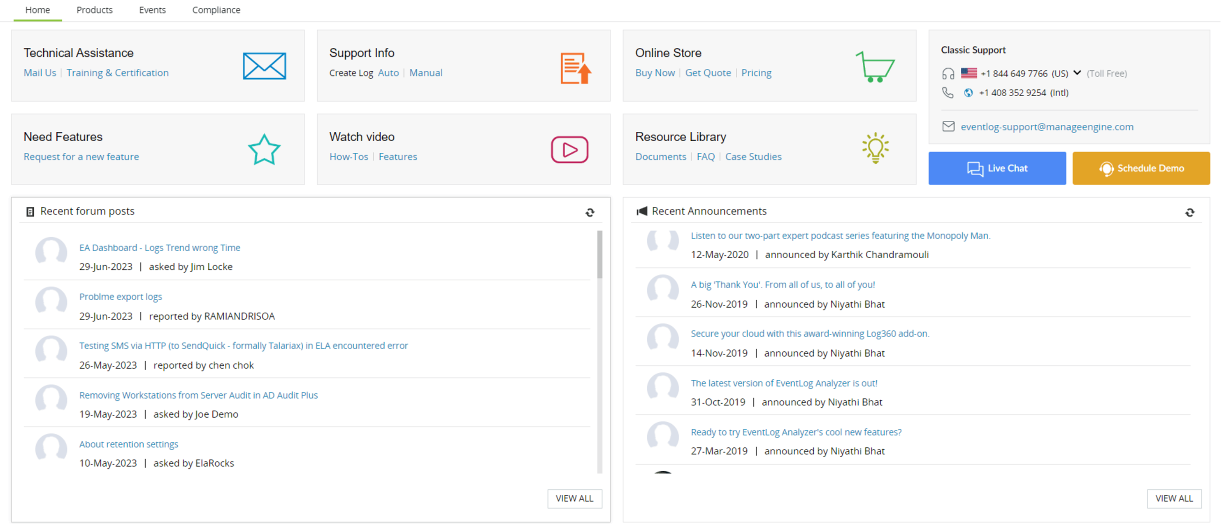


Name	Date modified	Type	Size
adsdata	10/20/2020 1:36 PM	File folder	
archive	12/10/2020 10:38 AM	File folder	
bin	12/7/2020 1:01 PM	File folder	
blog	10/3/2020 2:36 AM	File folder	
conf	10/12/2020 5:32 PM	File folder	
data	12/10/2020 10:58 AM	File folder	
ES	10/5/2020 4:22 PM	File folder	
help	10/3/2020 2:35 AM	File folder	
images	10/3/2020 2:35 AM	File folder	
jre	8/30/2020 2:07 PM	File folder	
lib	11/4/2020 10:23 AM	File folder	
logs	12/10/2020 10:34 AM	File folder	
pgsql	10/3/2020 2:36 AM	File folder	
product_package	10/3/2020 2:35 AM	File folder	
ReportHistory	10/16/2020 3:27 PM	File folder	
server	11/18/2020 5:38 PM	File folder	
tools	10/3/2020 2:35 AM	File folder	
troubleshooting	10/5/2020 4:22 PM	File folder	
webapps	10/3/2020 2:35 AM	File folder	
work	10/5/2020 4:22 PM	File folder	
COPYRIGHT	8/26/2020 9:48 PM	File	7 KB
InjectorInfo	10/3/2020 2:36 AM	Text Document	1 KB
LICENSE_AGREEMENT	8/26/2020 9:48 PM	File	13 KB
README	8/26/2020 9:48 PM	Chromium HTML ...	177 KB
webclient	10/3/2020 2:36 AM	Chromium HTML ...	2 KB

9.3. Contacting EventLog Analyzer Support

Last updated on: September 12, 2025

EventLog Analyzer provides a wide range of options to contact the support team, make feature requests, ask for a personalized demo, get online training, and more.
To go to the Support page, click the Support tab on the menu bar. The different channels through which you can reach out to us will be listed here. You can also click on the links below to reach our support team.



Home Products Events Compliance

Technical Assistance
Mail Us | Training & Certification

Support Info
Create Log Auto | Manual

Online Store
Buy Now | Get Quote | Pricing

Classic Support
+1 844 649 7766 (US) (Toll Free)
+1 408 352 9254 (Intl)
eventlog-support@manageengine.com

Need Features
Request for a new feature

Watch video
How-Tos | Features

Resource Library
Documents | FAQ | Case Studies

Live Chat
Schedule Demo

Recent forum posts

EA Dashboard - Logs Trend wrong Time
29-Jun-2023 | asked by Jim Locke

Problme export logs
29-Jun-2023 | reported by RAMIANDRISOA

Testing SMS via HTTP (to SendQuick - formally Talariax) in ELA encountered error
26-May-2023 | reported by chen chok

Removing Workstations from Server Audit in AD Audit Plus
19-May-2023 | asked by Joe Demo

About retention settings
10-May-2023 | asked by ElaRocks

VIEW ALL

Recent Announcements

Listen to our two-part expert podcast series featuring the Monopoly Man.
12-May-2020 | announced by Karthik Chandramouli

A big 'Thank You'. From all of us, to all of you!
26-Nov-2019 | announced by Niyathi Bhat

Secure your cloud with this award-winning Log360 add-on.
14-Nov-2019 | announced by Niyathi Bhat

The latest version of EventLog Analyzer is out!
31-Oct-2019 | announced by Niyathi Bhat

Ready to try EventLog Analyzer's cool new features?
27-Mar-2019 | announced by Niyathi Bhat

VIEW ALL

Request type	Link	Description
Technical Assistance	Mail Us	Click this link or click 'Mail Us' in the Support Page of EventLog Analyzer. Fill in the required fields with a detailed description of the problem that you encountered. Click on Submit.
Technical Assistance	EventLog Analyzer Training	Click this link or click 'Training & Certification' in the Support Page of EventLog Analyzer to take up a course and equip yourself with the knowledge required to work with EventLog Analyzer.
Create Log - Support Information Files		Go to 'Support Info' in the support page of EventLog Analyzer to create a support information file. It can be done automatically if you click the 'Auto' option. To do it manually, click the 'Manual' option. A set of instructions along with an upload link will be presented to you. Note: Click here to know more about Support Information Files.

Request type	Link	Description
Online Store - Get a Price Quote	Price Quote	Click this link or click 'Get Quote' under Online Store in the Support Page of EventLog Analyzer to get a personalized quote that best suits your requirements.
Online Store - Purchasing the product	Buy Now	Click this link or click 'Buy Now'/'Pricing' under Online Store in the Support Page of EventLog Analyzer.
New feature requests	Feature requests	If you'd like to see new features in the upcoming releases of EventLog Analyzer, click this link to give us your suggestions.
Configuration videos	How-To-Videos	Click this link or click 'How-Tos' under Watch Video in the support page of EventLog Analyzer. Under the 'How to' section, there are videos on configuring EventLog Analyzer for different use cases.
Feature videos	Feature-Videos	Click this link or click 'How-Tos' under Watch Video in the support page of EventLog Analyzer. Under the 'Features' section, there are videos on different features of EventLog Analyzer.
Knowledge Base	Documents	Click this link or click 'Documents' under Knowledge Base in the Support Page of the EventLog Analyzer solution to understand how to deploy, configure, and generate reports using EventLog Analyzer.
Knowledge Base FAQ	FAQ	Click this link or click 'FAQ' under Knowledge Base in the support page of EventLog Analyzer to view answers to frequently asked questions.
Knowledge Base Case Studies	Case Studies	Click this link or click 'Case Studies' under Knowledge Base in the support page of EventLog Analyzer. This page has case studies on how EventLog Analyzer has helped customers fulfill their requirements under different circumstances.
Contact our support team		Contact Us: Toll Free Number: US +1 844 649 7766 UK +44 800 028 6590 Australia +1 800 631 268

Request type	Link	Description
team		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.