ManageEngine

EventLog Analyzer

# Distributed Edition Guide

https://www.manageengine.com/products/eventlog/

# Table of contents

**Overview**

**1.** Introduction to EventLog Analyzer Distributed edition

**2.** Prerequisites for EventLog Analyzer distributed edition
- 2.1 Prerequisites for converting to distributed edition
- 2.2 Best practices to deploy the admin and managed server
- 2.3 Licensing details of distributed edition

**3.** Standalone installation to Distribution Conversion
- 3.1 Pre Conversion (Common Steps)
- 3.2 Admin Server
- 3.3 managed server

**4.** Manage Server Settings
- 4.1 Introduction to Manage Server Settings
- 4.2 Edit user login details
- 4.3 Delete managed server
- 4.4 Sync now
- 4.5 Auto upgrade
- 4.6 Upgrade now

**5.** Centralized Log Archival

**6.** Upgrading EventLog Analyzer distributed edition
- 6.1 Steps to upgrade the EventLog Analyzer Distributed edition
- 6.2 Types of Upgrading Managed Server

**7.** Integration with Log360
- 7.1 Integration
- 7.2 Device Allocation Management

**8.** Frequently Asked Questions

8.1 General

8.2 Secure Communication Mode (HTTPS)

8.3 Licensing

**9.** Troubleshooting

9.1 Sync

9.2 Connection /Registration

9.3 Centralized Archiving

9.4 Grey out tab

9.5 Migration Managed Server to another machine

9.6 Migration Admin Server to another machine

9.7 Integration with Log360

**10.** Download link

# Overview

In the globalized world, the landscape of the Enterprises with global presence is changing. The offices, branches, factories, and workshops are spread in different countries. It is becoming increasingly difficult for Enterprises to manage the IT resource. More so with security monitoring and management of IT infrastructure.

The Enterprises seek a scalable solution to manage the increasing IT resources. In most of the cases, solutions are poorly scalable or they themselves consume a lot of resources. Next to scalability, enterprises look for distributed security monitoring of IT resources because their branches/offices are present worldwide in different geographical locations. The enterprises are in need of a truly scalable and distributed monitoring security solution. With all these, they want to view all the monitoring in a single place to facilitate centralized management.

EventLog Analyzer appreciates the IT security needs of large enterprises with global presence and MSSPs. It has come up with a distributed solution, which will scale up to monitor thousands of hosts/applications and be deployed at locations around the globe. To cater for the MSSPs, it offers customizable dashboards and user specific views. EventLog Analyzer Distributed Edition is scalable and deployable in distributed model. It offers centralized monitoring of all distributed locations in a single console. It provides exclusive segmented, secured view for different users.

## 1. Introduction to EventLog Analyzer Distributed edition

EventLog Analyzer's distributed edition (Refer to Figure 1) is useful when your network consists of over a thousand log sources, or if it's spread across multiple geographic regions. This edition encompasses one admin server and one or more managed servers. It's also the perfect model for Managed Security Service Providers (MSSPs) to deploy. It follows a distributed architecture with multiple managed servers centrally aggregating and viewing the log data in a single, central admin server.

Here are a few highlights of the EventLog Analyzer distributed edition:

- Centralizes log management
- Auto upgrade all the managed servers once the admin server updated.
- Supports multiple devices across different geographical locations
- Ensures secured communication between the components.
- Exclusive segmented and secured view for various customers of the MSSP.

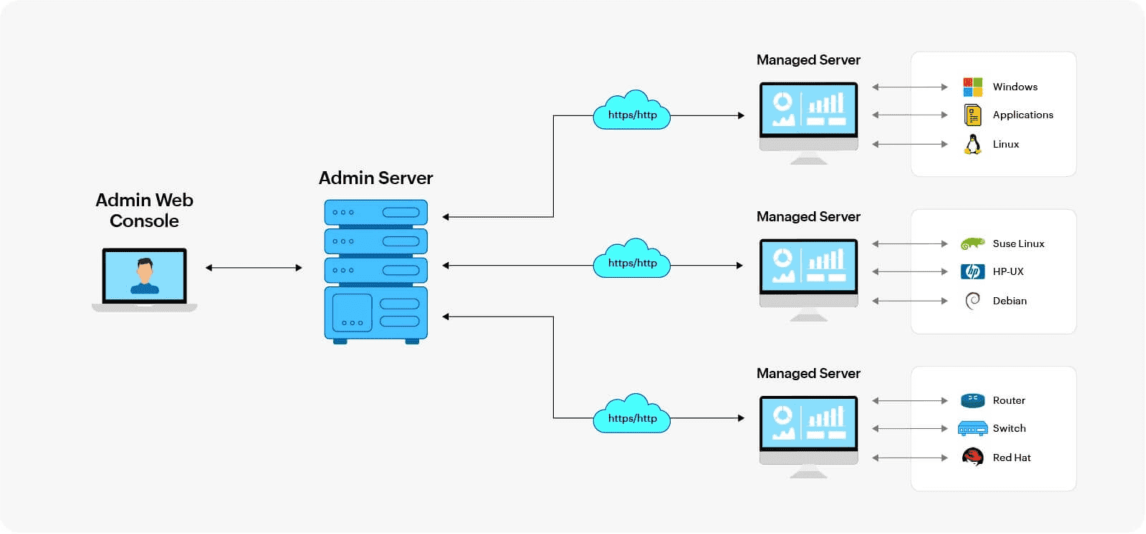


**Figure 1 EventLog Analyzer's Distributed Edition**

# 2. Prerequisites for EventLog Analyzer distributed edition

## 2.1 Prerequisites for converting to distributed edition

Here are a few of the prerequisites which needs to be taken care of before converting a standalone setup to the distributed edition:

1. With the Prerequisites of a standalone Event log Analyzer.
2. Distributed editions system requirements
3. We need to open the webserver port bidirectionally both in admin and managed server or via VPN and optimal functionality by opening the port in the firewall.
4. Using a Fully Qualified Domain Name (FQDN) as the hostname for the multiple server communication is not recommended; it is recommended to use either the IP address or the host name.
5. EventLog Analyzer requires the following ports to be free for web server and PostgreSQL communication:

- **33335 (TCP)** - This is the port used for connecting to the bundled PostgreSQL database in EventLog Analyzer.

- **8400 (Web server port)**- This is the default web server port used by EventLog Analyzer. This port is used for connecting to EventLog Analyzer using a web browser. You can change this port during installation.

By default, the admin and managed servers communicate using HTTP (port number 8400). There is also an option to convert the mode of communication to HTTPS. Verify port availability to ensure it is unoccupied by concurrent local applications.

## 2.2 Best practices to deploy the admin and managed servers

1. It is always recommended to convert the new EventLog Analyzer server as admin server to prevent data loss. You can follow the steps given here to convert the standard edition of EventLog Analyzer into an admin server.
2. For managed server, in case, you already have an existing EventLog Analyzer server, you can convert it into a managed server by following the steps here. The data in this case will remain on the same server and will not get lost/formatted unlike in the admin server.
3. Both the admin server and the managed servers should be in the same build. If they are not in the same build, follow the steps mentioned here to download and apply the latest service packs.

**Note :**
**a)** If both the admin and managed servers are not in the same build, it can lead to sync issues.

**b)** One admin server is designed to manage up to 100 managed servers.

## 2.3 Licensing details of distributed edition

EventLog Analyzer's Distributed Edition license will be applied to the admin server. From the admin server, it automatically propagates to all the managed servers, which happens at an interval of 5 minutes. The number of devices and applications for which the license has been purchased can be utilized among the registered managed servers. You can keep adding devices and applications to various managed servers until the purchased device licenses are exhausted. You can view the number of devices and applications managed by each managed server in the **Manage Server Settings** page of the admin server.

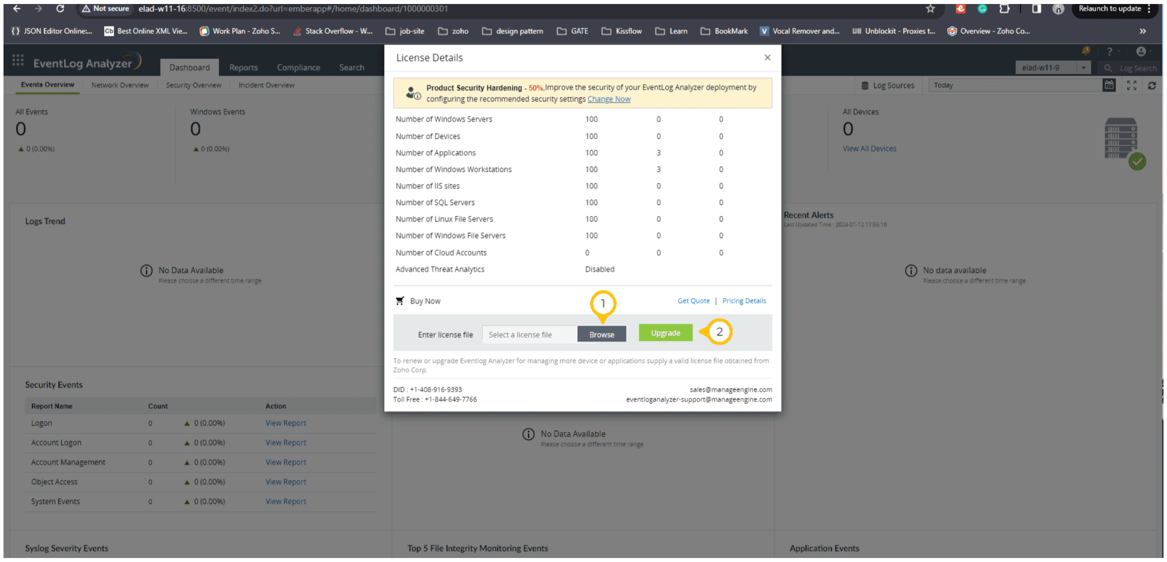
When the number of devices and applications managed by all the managed servers exceeds the number of licenses purchased, a warning message appears in the admin server. To resolve this warning, you can:

- Purchase the license to manage the additional devices and applications.
- Check the number of devices and applications managed by each managed server in the Managed Server Settings page of the admin server.
- Go to the individual managed server and manually manage the devices. Ensure that the number of devices and applications are within the license limit.

**Note:** Distributed License can apply only on the Admin Server.

## Steps to Apply License in the Admin server:

1. Open the License Details tab located on the **? icon → License** and Browse the license file from your local machine. (Refer to Figure2)
2. Click the **Upgrade** button.



License Details

**Product Security Hardening** - 50%,Improve the security of your EventLog Analyzer deployment by configuring the recommended security settings Change Now

| | | | |
|---|---|---|---|
| Number of Windows Servers | 100 | 0 | 0 |
| Number of Devices | 100 | 0 | 0 |
| Number of Applications | 100 | 3 | 0 |
| Number of Windows Workstations | 100 | 3 | 0 |
| Number of IIS sites | 100 | 0 | 0 |
| Number of SQL Servers | 100 | 0 | 0 |
| Number of Linux File Servers | 100 | 0 | 0 |
| Number of Windows File Servers | 100 | 0 | 0 |
| Number of Cloud Accounts | 0 | 0 | 0 |
| Advanced Threat Analytics | Disabled | | |

Buy Now Get Quote | Pricing Details

Enter license file Select a license file Browse Upgrade

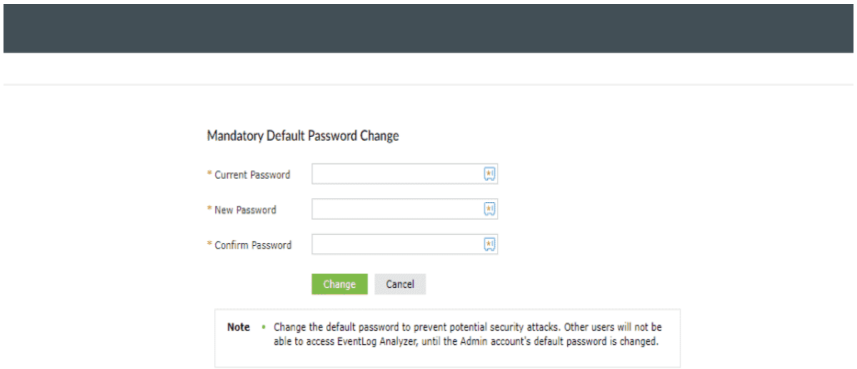
To renew or upgrade Eventlog Analyzer for managing more device or applications supply a valid license file obtained from Zoho Corp.

DID : +1-408-916-9393
Toll Free : +1-844-649-7766

sales@manageengine.com
eventloganalyzer-support@manageengine.com

**Figure 2 Applying License in the Admin server**

3. If it was a first time, to prevent potential security attacks and enhance security, perform **Mandatory Default Password Change** from default once after applying License. (Refer to Figure3)



Mandatory Default Password Change

* Current Password
* New Password
* Confirm Password

Change Cancel

**Note** • Change the default password to prevent potential security attacks. Other users will not be able to access EventLog Analyzer, until the Admin account's default password is changed.

**Fig 3 Mandatory Default Password Change**

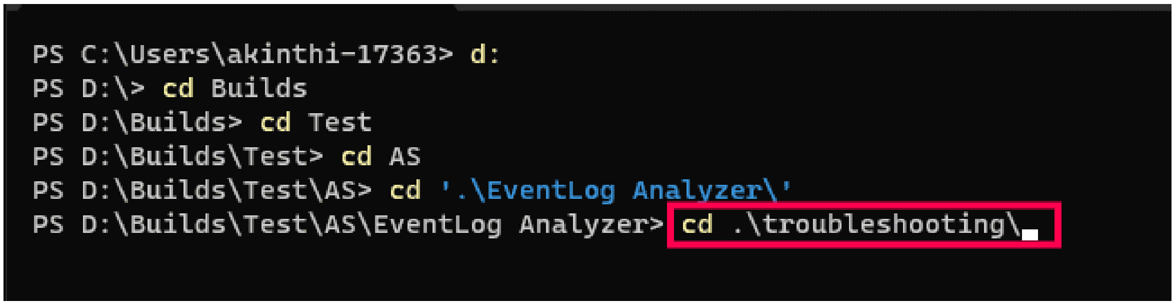
## 3. Standalone installation to Distribution Conversion

When it comes to distributed edition, conversion is the most basic part. It is what converts an EventLog Analyzer instance to a distributed instance. Let's assume you want a simple distributed setup with a single admin server and a single managed server to be set-up. Let's see how to create such an environment with basic configurations.

### 3.1 Pre Conversion (Common Steps)

1. Select a machine/server of your preference to be set up as the admin server or the managed server.
2. Follow the installation steps as they are.

Once you are in the home folder, which is named **EventLog Analyzer** by default, type "***cd .\troubleshooting***". This will take you to the troubleshooting folder. (Refer to Figure4)



```
PS C:\Users\akinthi-17363> d:
PS D:\> cd Builds
PS D:\Builds> cd Test
PS D:\Builds\Test> cd AS
PS D:\Builds\Test\AS> cd '.\EventLog Analyzer\'
PS D:\Builds\Test\AS\EventLog Analyzer> cd .\troubleshooting\
```

**Figure 4 Troubleshooting**

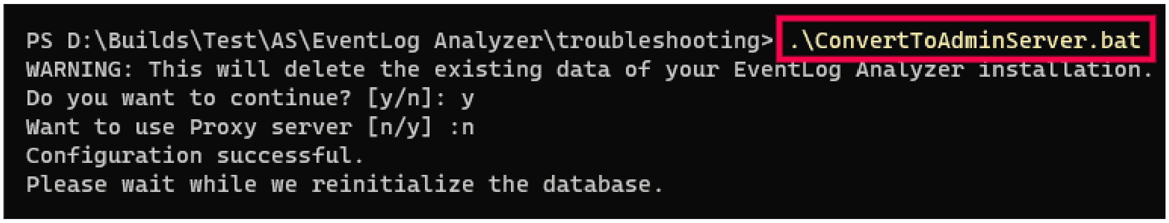
### 3.2 Admin Server

A central server that provides the administrator with viewing over the entire network.

**Convert EventLog Analyzer standard edition to an admin server:**

Converting the standard edition of EventLog Analyzer into an admin server will result in the deletion of data present in the standard edition. You can follow the steps given below to convert the standard edition of EventLog Analyzer into an admin server:

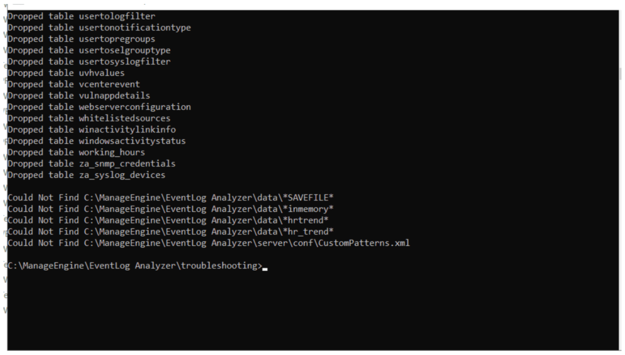
1. Shut down EventLog Analyzer (if exist).
2. Open the command prompt with administrative privilege and execute the **ConvertToAdminServer.bat/sh** file located in <EventLog Analyzer Home>/troubleshooting. (Refer to Figure5)



```
PS D:\Builds\Test\AS\EventLog Analyzer\troubleshooting> .\ConvertToAdminServer.bat
WARNING: This will delete the existing data of your EventLog Analyzer installation.
Do you want to continue? [y/n]: y
Want to use Proxy server [n/y] :n
Configuration successful.
Please wait while we reinitialize the database.
```

**Figure 5 ConvertToAdminServer.bat/sh**

3. A warning message about the deletion of data of your existing installation will be displayed.  (Refer to Figure 6)
    a. Type **"y"** for the first prompt ("Do you want to continue?")
    b. The next one ("Want to use a proxy server") is based on your preference; if chosen yes, the prompt will proceed to ask for proxy details.



```
Dropped table usertologfilter
Dropped table usertonotificationtype
Dropped table usertopregroups
Dropped table usertoselgrouptype
Dropped table usertosyslogfilter
Dropped table uvhvalues
Dropped table vcenterevent
Dropped table vulnappdetails
Dropped table webserverconfiguration
Dropped table whitelistedsources
Dropped table winactivitylinkinfo
Dropped table windowsactivitystatus
Dropped table working_hours
Dropped table za_snmp_credentials
Dropped table za_syslog_devices

Could Not Find C:\ManageEngine\EventLog Analyzer\data\*SAVEFILE*
Could Not Find C:\ManageEngine\EventLog Analyzer\data\*inmemory*
Could Not Find C:\ManageEngine\EventLog Analyzer\data\*hrtrend*
Could Not Find C:\ManageEngine\EventLog Analyzer\data\*hr_trend*
Could Not Find C:\ManageEngine\EventLog Analyzer\server\conf\CustomPatterns.xml

C:\ManageEngine\EventLog Analyzer\troubleshooting>
```

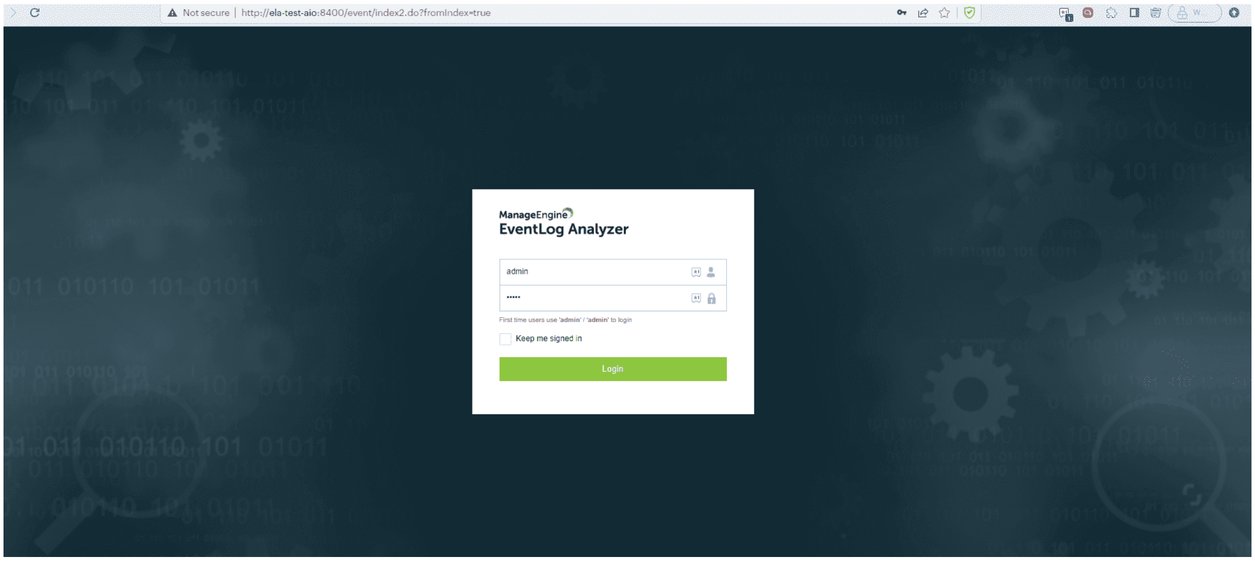
**Figure 6 Console output of converting to admin server**

4. Once you perform the previous step, you will see a bunch of verbose run on your screen, and once it stops, your server will be converted from the standalone edition into an admin server of the distributed edition.

**Verify you have converted to admin server in Userinterface(UI),**

1. Start the product EventLog Analyzer Admin Server.

2. Access EventLog Analyzer with port:  **http://localhost:8400**, **username: admin, password: admin** (Refer to Figure7)



Not secure | http://ela-test-aio:8400/event/index2.do?fromIndex=true

ManageEngine
EventLog Analyzer

admin

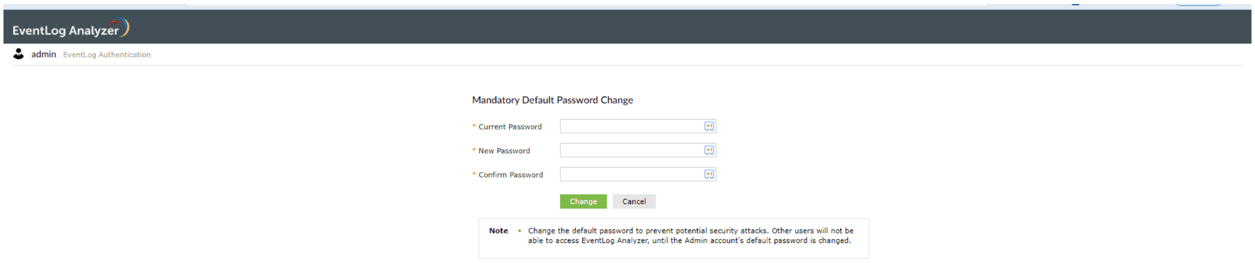
•••••

First time users use 'admin' / 'admin' to login

□ Keep me signed in

**Figure 7 Access EventLog Analyzer**

3. Change the default password. (Refer to Figure8)



EventLog Analyzer

admin EventLog Authentication

Mandatory Default Password Change

* Current Password

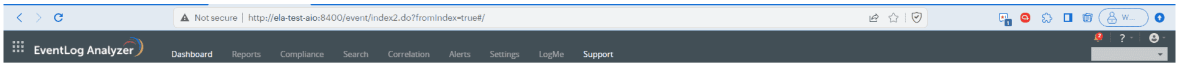
* New Password

* Confirm Password

**Note** • Change the default password to prevent potential security attacks. Other users will not be able to access EventLog Analyzer, until the Admin account's default password is changed.

**Figure 8 Changing the default password**

4. The console will look like the below image. (Refer to Figure 9)



Not secure | http://ela-test-aio:8400/event/index2.do?fromIndex=true#/

**Figure 9 EventLog Analyzer Console**

5. Click on the **?** at the top right corner and then on **About**. (Refer to Figure10)

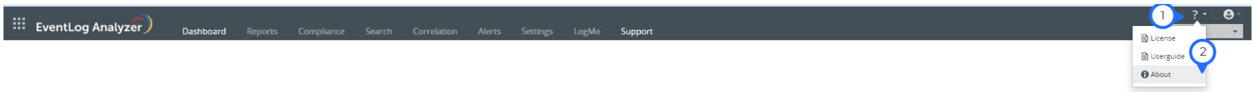
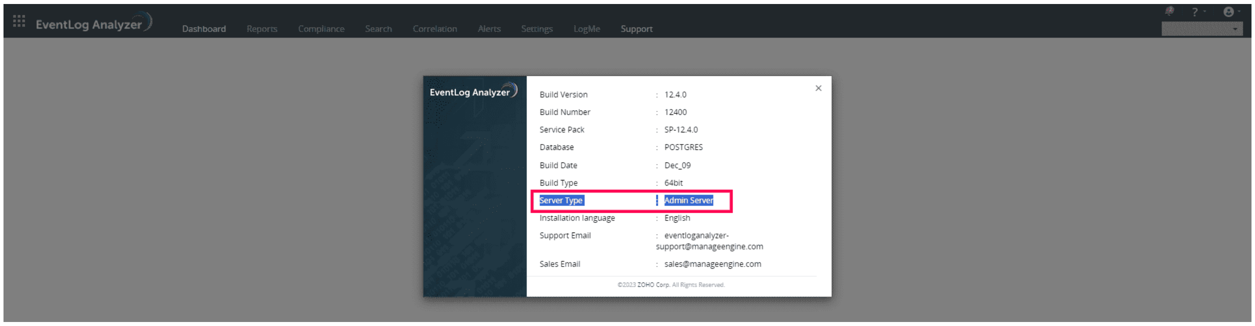


**Figure 10 About section**

6. The server type will change to **Admin Server**. (Refer to Figure11)



```
Build Version          :  12.4.0
Build Number           :  12400
Service Pack           :  SP-12.4.0
Database               :  POSTGRES
Build Date             :  Dec_09
Build Type             :  64bit
Server Type            :  Admin Server
Installation language  :  English
Support Email          :  eventloganalyzer-
                       support@manageengine.com
Sales Email            :  sales@manageengine.com

©2023 ZOHO Corp. All Rights Reserved.
```

**Figure 11 Server changed to Admin Server**

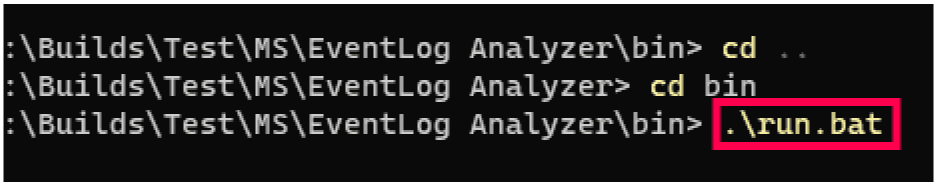
### 3.3 Managed Server - link

Each managed server oversees a smaller portion of the network, and it works exactly like the standalone edition described above.

**Convert EventLog Analyzer standalone edition to a managed server**

You can convert your standalone EventLog Analyzer installation (Standard Edition) into a managed server installation of distributed edition by following the below steps:

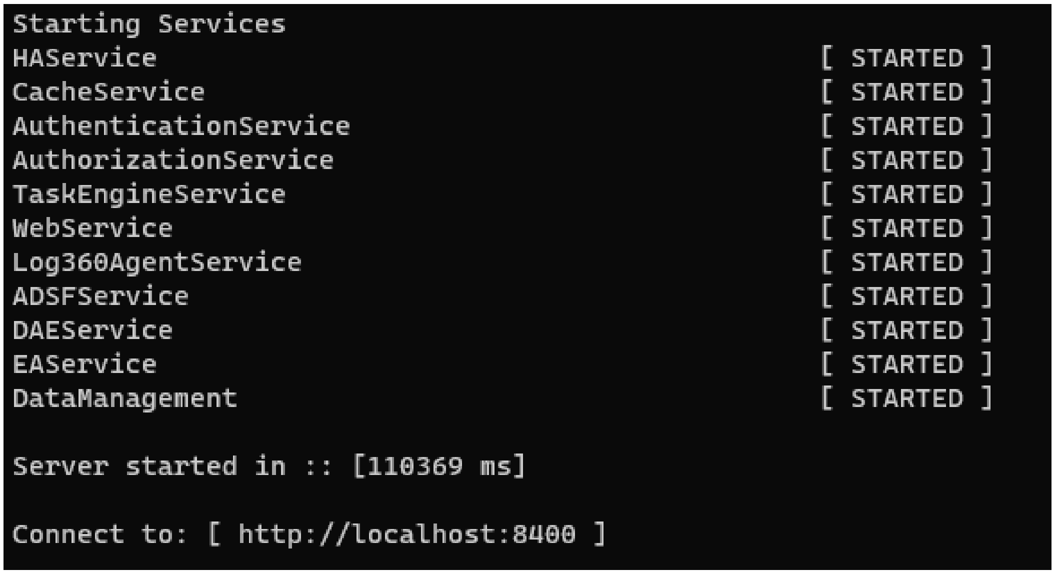
1. Now open the terminal/command line of your choice and use the **cd** command to route to the home location of your instance.
2. Now, on your machine preferred for the managed server, from inside the ***bin*** folder, run the bat file as shown in the image below by typing ".***run.bat***". This will start the standalone EventLog Analyzer instance. (Refer to Figure12)



```
:\Builds\Test\MS\EventLog Analyzer\bin> cd ..
:\Builds\Test\MS\EventLog Analyzer> cd bin
:\Builds\Test\MS\EventLog Analyzer\bin> .\run.bat
```

**Figure 12 Executing command .\*run.bat***

3. When you see a display similar to the image below, Shut down EventLog Analyzer by using the key binding "***Ctrl+C***". Type "***y***" to continue stopping the server. (Refer to Figure13)



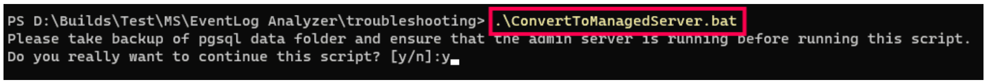
```
Starting Services
HAService                                            [ STARTED ]
CacheService                                         [ STARTED ]
AuthenticationService                                [ STARTED ]
AuthorizationService                                 [ STARTED ]
TaskEngineService                                    [ STARTED ]
WebService                                           [ STARTED ]
Log360AgentService                                   [ STARTED ]
ADSFService                                          [ STARTED ]
DAEService                                           [ STARTED ]
EAService                                            [ STARTED ]
DataManagement                                       [ STARTED ]

Server started in :: [110369 ms]

Connect to: [ http://localhost:8400 ]
```

**Figure 13 Stopping EventLog Analyzer**

4. Back up the database.

5. Now navigate to the "***troubleshooting***" folder by typing "***cd ..\troubleshooting***".

6. Now run the bat file as shown in the figure 14 by typing "***./ConvertTomanaged server.bat***". You will see a warning like in the below image based on your choice of database. Take necessary actions on preference and proceed to type "***y***" for further processing.

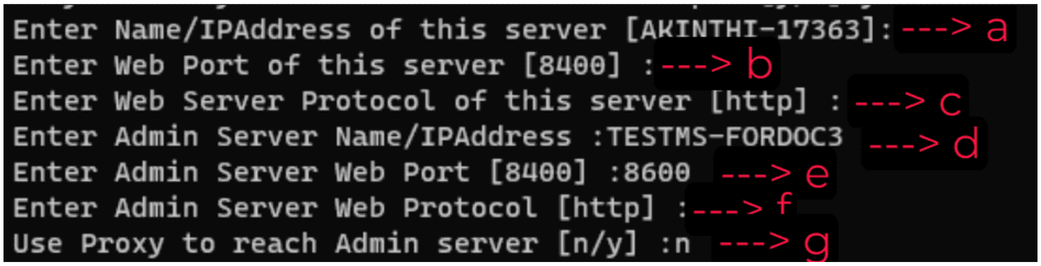


```
PS D:\Builds\Test\MS\EventLog Analyzer\troubleshooting> .\ConvertToManagedServer.bat
Please take backup of pgsql data folder and ensure that the admin server is running before running this script.
Do you really want to continue this script? [y/n]:y
```

**Figure 14 Executing *./ConvertTomanaged server.bat***

7. You will be asked for the configuration details. You will be asked for a total of seven prompts. They are as follows:

   a. Hostname/IP of the managed server
   b. Port of the managed server (EventLog Analyzer instance)
   c. Web Server Protocol of the managed server (http/https)
   d. Hostname/IP of the admin server
   e. Port of the Admin Server
   f. Web Server Protocol of the admin server (http/https)
   g. Proxy preference; if chosen yes, the prompt will proceed to ask for further proxy server details.   As shown in the image, type all the proper details. (Refer to Figure15)



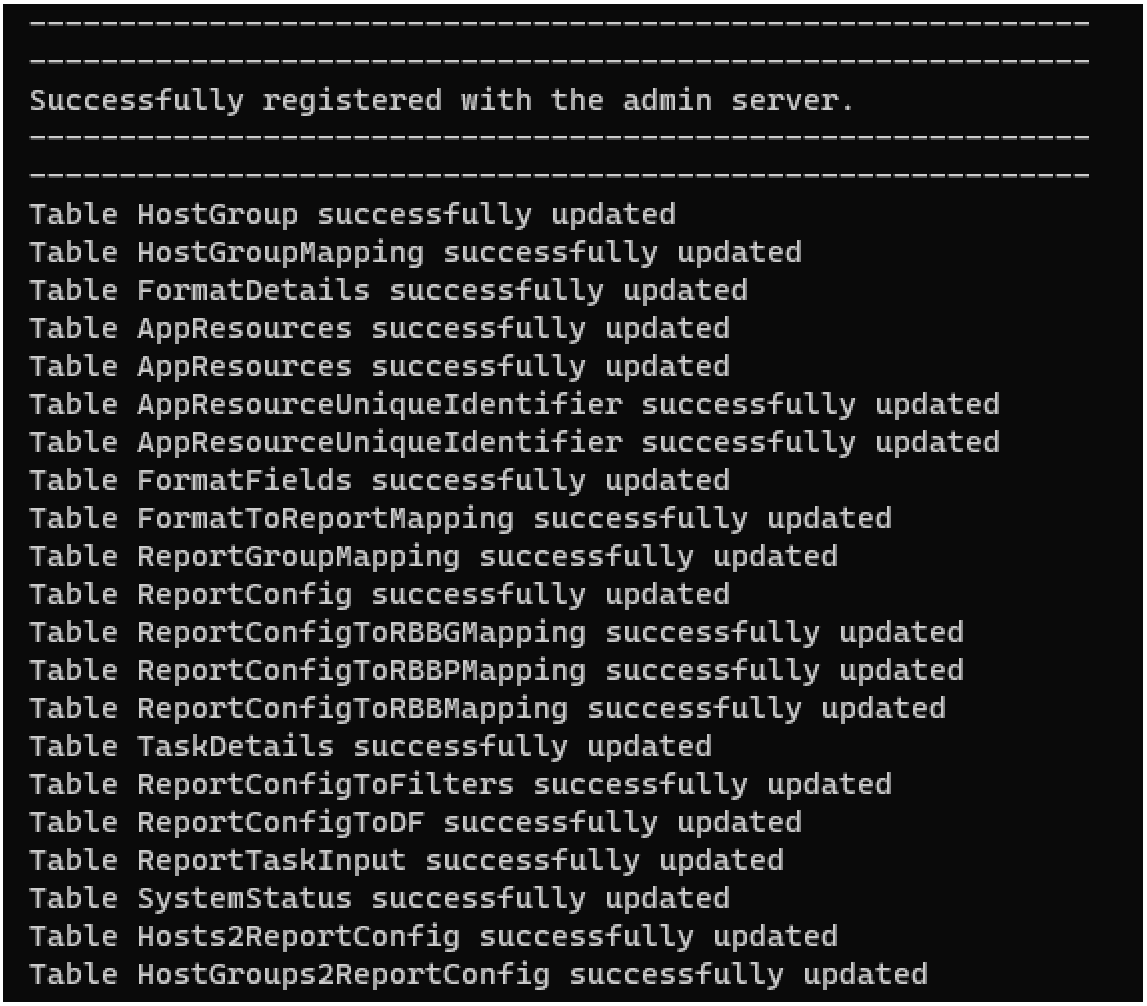
```
Enter Name/IPAddress of this server [AKINTHI-17363]:
Enter Web Port of this server [8400] :
Enter Web Server Protocol of this server [http] :
Enter Admin Server Name/IPAddress :TESTMS-FORDOC3
Enter Admin Server Web Port [8400] :8600
Enter Admin Server Web Protocol [http] :
Use Proxy to reach Admin server [n/y] :n
```

**Figure 15 Configuration Details**

**Note:**

1. For options a,b, and c, default options are provided in the prompt itself; if preferred, you can leave it empty so that the default values will be used.
2. Skip using Fully Qualified Domain Name (FQDN) as the hostname

8. If followed properly until this step, you will see a display similar to the below image. You can find this in the middle of the load of verbose presented to you when the process is running. (Refer to Figure16)



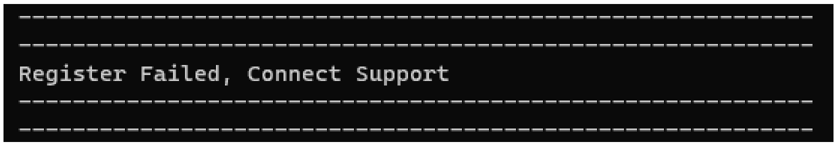
```
-----------------------------------------------------------
-----------------------------------------------------------
Successfully registered with the admin server.
-----------------------------------------------------------
-----------------------------------------------------------
Table HostGroup successfully updated
Table HostGroupMapping successfully updated
Table FormatDetails successfully updated
Table AppResources successfully updated
Table AppResources successfully updated
Table AppResourceUniqueIdentifier successfully updated
Table AppResourceUniqueIdentifier successfully updated
Table FormatFields successfully updated
Table FormatToReportMapping successfully updated
Table ReportGroupMapping successfully updated
Table ReportConfig successfully updated
Table ReportConfigToRBBGMapping successfully updated
Table ReportConfigToRBBPMapping successfully updated
Table ReportConfigToRBBMapping successfully updated
Table TaskDetails successfully updated
Table ReportConfigToFilters successfully updated
Table ReportConfigToDF successfully updated
Table ReportTaskInput successfully updated
Table SystemStatus successfully updated
Table Hosts2ReportConfig successfully updated
Table HostGroups2ReportConfig successfully updated
```

**Figure 16 Converting to managed server**

9. Also, there will be a line visible in the verbose before it stops saying "***Server noted as Converted Collector***" (Don't worry about finding it; this is just a FYI) This means the conversion and registration of the managed server have been carried out successfully.

10. If steps 7 and 8 doesn't look like what is on your screen, kindly check with the below exceptional cases.

    1. If you see a message like this during conversion, there could be several issues like, (Refer to Figure17)



```
----------------------------------------------------------
----------------------------------------------------------
Register Failed, Connect Support
----------------------------------------------------------
----------------------------------------------------------
```

**Fig 17 Conversion failed**

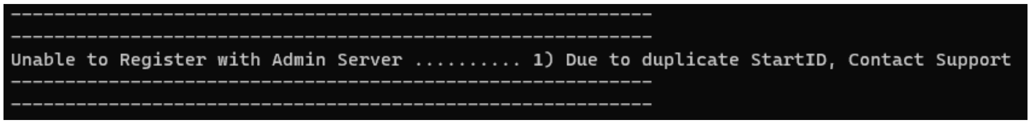
       a. Admin Server is turned off. Check if your Admin Server is up and running.

       b. Admin Server is not reachable from the managed server's network. At this point, check for firewalls (whitelisting), network scope. If everything is okay and if you still are getting this exception, kindly plan on contacting our support.

       c. The admin server to which you want to link the new managed server is accessible on the given port using the mentioned protocol.

       d. If the admin server is using a proxy server, check whether the provided proxy server details are correct.

    2. If you see this message (Refer to Figure 18), this could be because of multiple reasons. But make sure of the below things; they might help you solve the above issue.



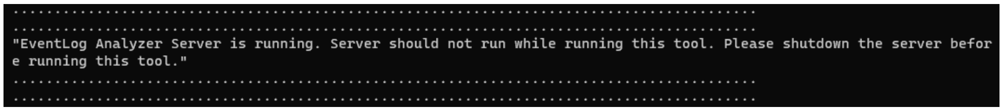
```
-----------------------------------------------------------
-----------------------------------------------------------
Unable to Register with Admin Server ......... 1) Due to duplicate StartID, Contact Support
-----------------------------------------------------------
-----------------------------------------------------------
```

**Figure 18 Error message: Registration failed**

       a. Make sure the IPs/hostnames and ports supplied are right.

       b. If you find any of the above issues, alter the "***enterprise.txt***" available under "***Eventlog_Analyzer***" home folder. But this is only when you are totally sure about the details; else, delete the file and try conversion again.

3. If you see this below message (Refer to Figure 19), then turn off your managed server and try again.



```
.....................................................................................
.....................................................................................
"EventLog Analyzer Server is running. Server should not run while running this tool. Please shutdown the server befor
e running this tool."
.....................................................................................
.....................................................................................
```

**Figure 19 Error message: Shut down server**

4. To add a managed server under the admin server again, follow the step given below

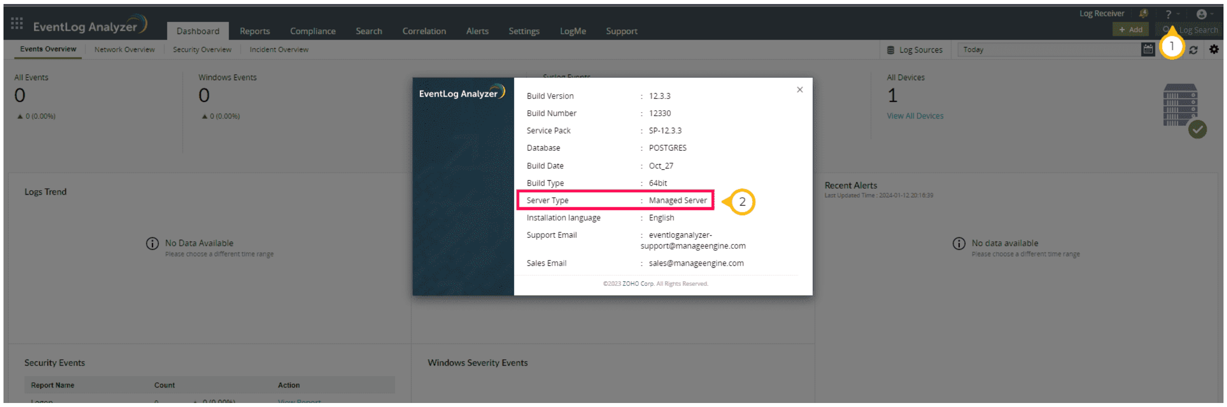
   Register the managed server with the admin server by executing the **registerWithAdminServer.bat/sh** file located in <EventLog Analyzer Home>/troubleshooting.

### Further Conversion (managed servers)

When setting up more managed servers, follow the same steps in their own environment without any change. For every conversion and registration, you can see the newly added managed server in the admin server's Managed Server Settings page.

### <u>Verify you have converted to managed server in User interface(UI).</u>

Open the managed server console and navigate to the **? icon → About** to ensure that the conversion. (Refer to Figure20)



EventLog Analyzer

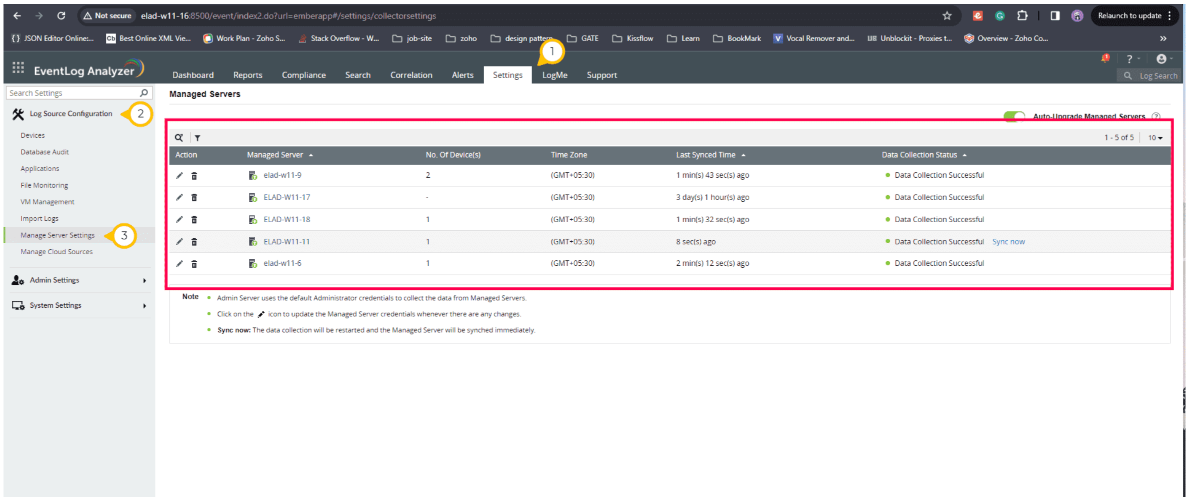
Build Version : 12.3.3
Build Number : 12330
Service Pack : SP-12.3.3
Database : POSTGRES
Build Date : Oct_27
Build Type : 64bit
Server Type : Managed Server
Installation language : English
Support Email : eventloganalyzer-support@manageengine.com
Sales Email : sales@manageengine.com

©2023 ZOHO Corp. All Rights Reserved.

**Figure 20 Verification of the conversion to Managed Server**

## Verify managed servers registered with Admin Server in User interface(UI).

Open the admin server console to which you've linked this managed server and navigate to **Settings → Log Configurations → Manage Server Settings** to ensure that the converted server is listed. (Refer to Figure21)



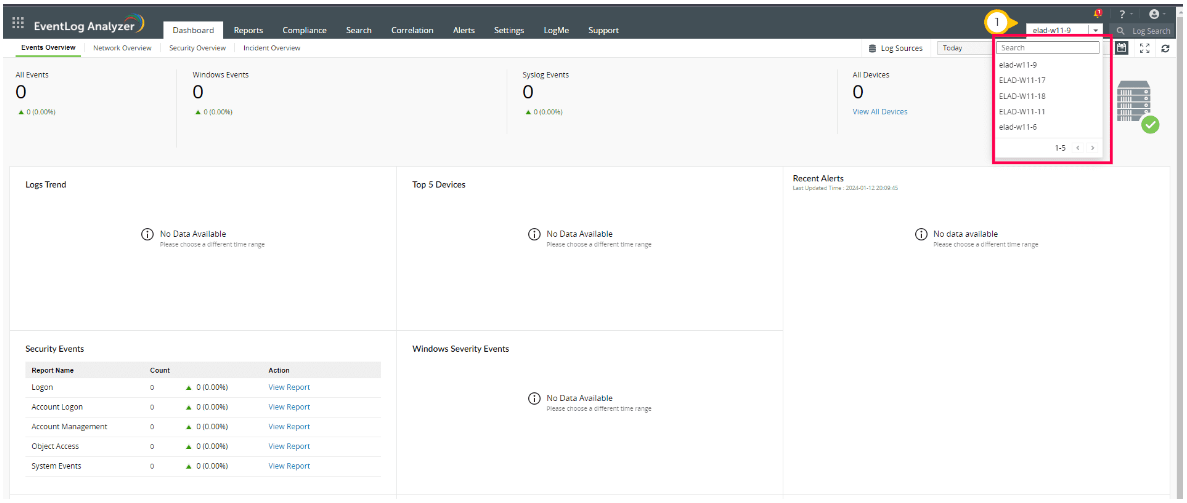
Managed Servers

| Action | Managed Server | No. Of Device(s) | Time Zone | Last Synced Time | Data Collection Status |
|---|---|---|---|---|---|
| | elad-w11-9 | 2 | (GMT+05:30) | 1 min(s) 43 sec(s) ago | ● Data Collection Successful |
| | ELAD-W11-17 | - | (GMT+05:30) | 3 day(s) 1 hour(s) ago | ● Data Collection Successful |
| | ELAD-W11-18 | 1 | (GMT+05:30) | 1 min(s) 32 sec(s) ago | ● Data Collection Successful |
| | ELAD-W11-11 | 1 | (GMT+05:30) | 8 sec(s) ago | ● Data Collection Successful Sync now |
| | elad-w11-6 | 1 | (GMT+05:30) | 2 min(s) 12 sec(s) ago | ● Data Collection Successful |

Note
- Admin Server uses the default Administrator credentials to collect the data from Managed Servers.
- Click on the icon to update the Managed Server credentials whenever there are any changes.
- **Sync now:** The data collection will be restarted and the Managed Server will be synched immediately.

**Figure 21 Confirmation of converted Managed Server**

You can switch between the managed servers in the drop-down box on top navigation bar. (Refer to Figure 22)



All Events
0
▲ 0 (0.00%)

Windows Events
0
▲ 0 (0.00%)

Syslog Events
0
▲ 0 (0.00%)

All Devices
0
View All Devices

Logs Trend

No Data Available
Please choose a different time range

Top 5 Devices

No Data Available
Please choose a different time range

Recent Alerts
Last Updated Time : 2024-01-12 20:09:45

No data available
Please choose a different time range

Security Events

| 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 |

Windows Severity Events

No Data Available
Please choose a different time range

**Figure 22 Managed Server dropdown**

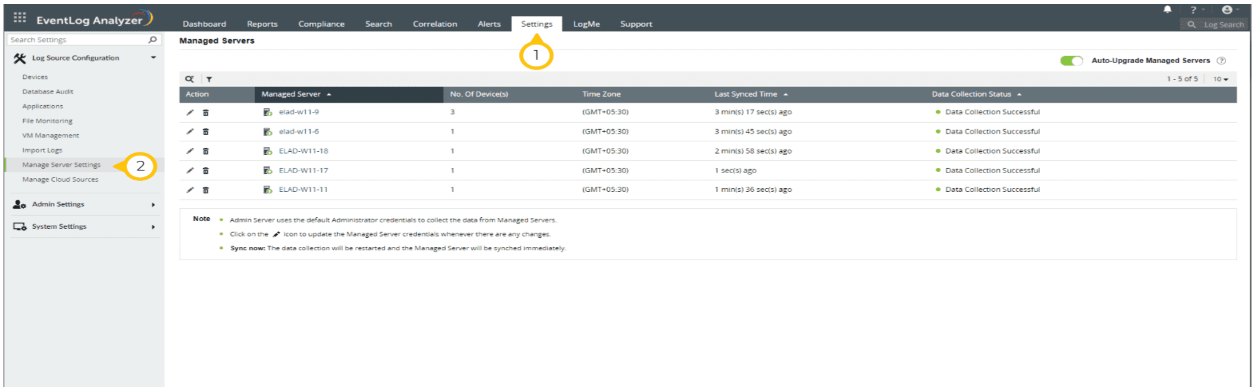
# 4. Manage Server Setting

## 4.1 Introduction to Manage Server Settings

In the Admin Server, the configuration for all Managed Servers is conducted on the "Manage Server Settings" page located on the **Settings** tab **> Log Source Configurations > Manage Server Settings** (Refer to Figure 23).  Default Admin credentials are used for data collection from Managed Servers, and in case there are any changes in login details, they can be managed through the "Edit User Login Details" option.

The Manage Server Settings offers the following information and options:

- The total number of devices associated with the Managed Server, including disabled ones.
- Last synced time, adjusted based on the specified time zone.
- Display name with a hyperlink reference to the Managed Server.
- Sync Now: Initiates a restart of data collection, syncing the managed server immediately.
- Auto-upgrade managed server: Enables automatic upgrades for the managed server.
- Upgrade now: When the Auto upgrade option is disabled, Individual upgrade for the managed server.



Managed Servers

Auto-Upgrade Managed Servers

1 - 5 of 5 | 10

| Action | Managed Server | No. Of Device(s) | Time Zone | Last Synced Time | Data Collection Status |
|---|---|---|---|---|---|
| | elad-w11-9 | 3 | (GMT+05:30) | 3 min(s) 17 sec(s) ago | ● Data Collection Successful |
| | elad-w11-6 | 1 | (GMT+05:30) | 3 min(s) 45 sec(s) ago | ● Data Collection Successful |
| | ELAD-W11-18 | 1 | (GMT+05:30) | 2 min(s) 58 sec(s) ago | ● Data Collection Successful |
| | ELAD-W11-17 | 1 | (GMT+05:30) | 1 sec(s) ago | ● Data Collection Successful |
| | ELAD-W11-11 | 1 | (GMT+05:30) | 1 min(s) 36 sec(s) ago | ● Data Collection Successful |

Note
- Admin Server uses the default Administrator credentials to collect the data from Managed Servers.
- Click on the icon to update the Managed Server credentials whenever there are any changes.
- **Sync now:** The data collection will be restarted and the Managed Server will be synched immediately.

**Figure 23 Manage Server Settings**

## 4.2 Edit user login details

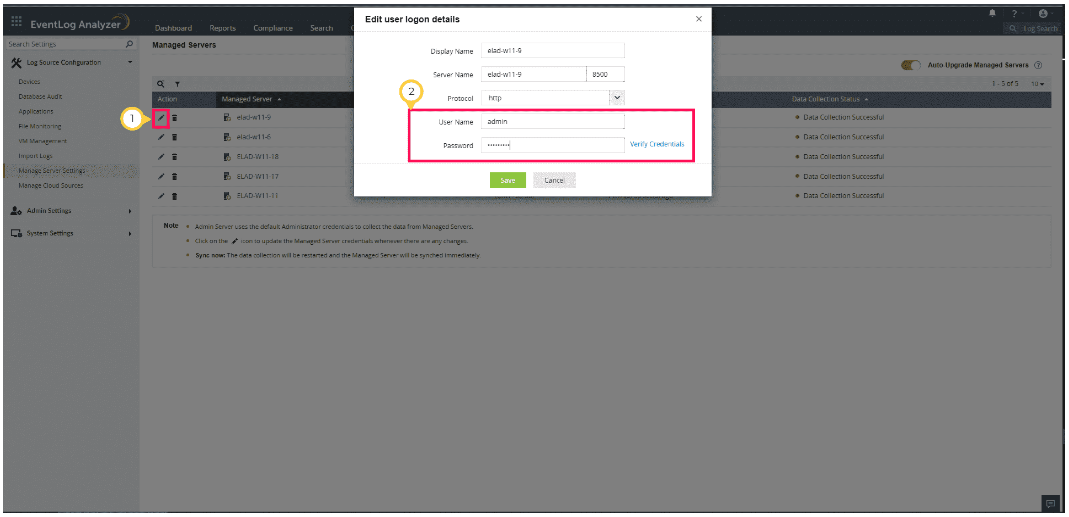
The scope of the Admin Server user interface i.e dashboard, reports, and other features, will be determined directly by the credentials of technician that associated with the specified Managed Server. To update the credentials for the managed server, click on the Edit icon. (Refer to Figure 24)

1. Display name: Enter the name for the Managed Server to be displayed on the UI.
2. Server name: Enter the Managed Server name with its port.
3. Protocols: The protocol to be used for communication (HTTP & HTTPs).
4. User Name and Password: Credentials used by the admin server for logging into the managed server.

**Note:**

1. When the Managed Server protocol is changed, ensure corresponding changes are made in the Manage Server Settings of the Admin Server.

2. You may use different Techincian credentials with admin privileges.



Edit user logon details

Display Name: elad-w11-9

Server Name: elad-w11-9 8500

Protocol: http

User Name: admin

Password: ••••••••••

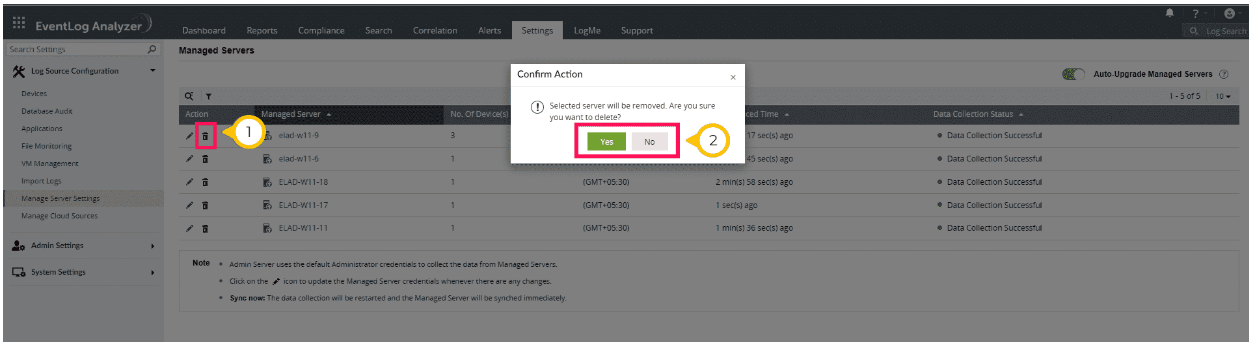
| Action | Managed Server | Data Collection Status |
|---|---|---|
| | elad-w11-9 | Data Collection Successful |
| | elad-w11-6 | Data Collection Successful |
| | ELAD-W11-18 | Data Collection Successful |
| | ELAD-W11-17 | Data Collection Successful |
| | ELAD-W11-11 | Data Collection Successful |

Note
- Admin Server uses the default Administrator credentials to collect the data from Managed Servers.
- Click on the icon to update the Managed Server credentials whenever there are any changes.
- **Sync now:** The data collection will be restarted and the Managed Server will be synched immediately.

**Figure 24 Edit user logon details**

## 4.3 Delete Managed Server

Deleting the managed server will result in the deletion of all its associated data from the Admin Server, leading to disruption in synchronization. This action should be carried out before deleting the managed server on the local machine. (Refer to Figure 25)



Managed Servers

Confirm Action

Selected server will be removed. Are you sure you want to delete?

| Action | Managed Server | No. Of Device(s) | | ced Time | Data Collection Status |
|---|---|---|---|---|---|
| | elad-w11-9 | 3 | | 17 sec(s) ago | Data Collection Successful |
| | elad-w11-6 | 1 | | 45 sec(s) ago | Data Collection Successful |
| | ELAD-W11-18 | 1 | (GMT+05:30) | 2 min(s) 58 sec(s) ago | Data Collection Successful |
| | ELAD-W11-17 | 1 | (GMT+05:30) | 1 sec(s) ago | Data Collection Successful |
| | ELAD-W11-11 | 1 | (GMT+05:30) | 1 min(s) 36 sec(s) ago | Data Collection Successful |

Note
- Admin Server uses the default Administrator credentials to collect the data from Managed Servers.
- Click on the icon to update the Managed Server credentials whenever there are any changes.
- **Sync now:** The data collection will be restarted and the Managed Server will be synched immediately.

**Figure 25 Delete Managed Server**

## 4.4 Sync now

The **Sync now** option initiates data collection, causing the data in the managed server to synchronize immediately with the admin server and update the status.

Following are the different data collection status types.

**Success Status:**

- Data Collection Successful - Sync succeeded.
- Scheduled for data collection - Sync scheduled when adding a new managed server.

**In-Process Status**

- Delete action is triggered. Please refresh after some time - Deleting request call sent to the managed server.
- Requested action triggered. Please refresh after some time - Data request sent to the managed server.
- Collector is down for patch process - Managed server down for a upgrade.

**Warning Status:**

- Build number mismatch between admin and this distributed server. managed server needs an upgrade - The Admin server is in higher version.
- Build number mismatch between Admin and this distributed server. managed server running a higher version - Managed server is at a higher version.
- Unable to upgrade managed server from Admin server. Please try to update manually - Auto Upgrade fails to upgrade the manager server with build less than 12216.
- Unable to contact remote machine - Managed server is not reachable.

**Failed Status:**

- Deletion failed - Managed server deletion failed.
- Error occurred during sync. Please contact support - Sync failed.
- Unable to upgrade managed server. Please contact support. - Auto upgrade failed.
- Exception during data collection - Failed to store/fetch data.
- Error during reset in collector server - Sync schedule was not restarted.

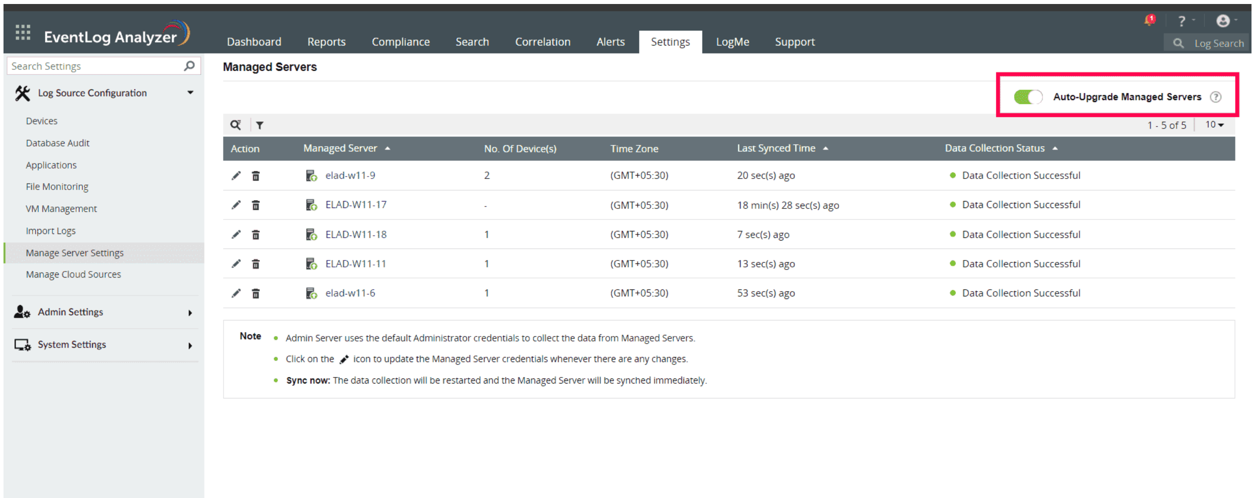
The service pack required to upgrade the managed server is unavailable. Please contact support - The latest patch does not exist in the Admin Server.

During the data collection cycle

- Licenses will sync to all managed servers.
- Auto-upgrade will be triggered in case of build mismatches between the servers if the "Auto Upgrade managed server" toggle is enabled.

## 4.5 Auto-Upgrade

When the "Auto-Upgrade Managed Servers" toggle is enabled, the admin server will automatically upgrade the managed servers once the PPM is applied to the admin server. (Refer to Figure 26)



Managed Servers

Auto-Upgrade Managed Servers

| Action | Managed Server | No. Of Device(s) | Time Zone | Last Synced Time | Data Collection Status |
|---|---|---|---|---|---|
| | elad-w11-9 | 2 | (GMT+05:30) | 20 sec(s) ago | ● Data Collection Successful |
| | ELAD-W11-17 | - | (GMT+05:30) | 18 min(s) 28 sec(s) ago | ● Data Collection Successful |
| | ELAD-W11-18 | 1 | (GMT+05:30) | 7 sec(s) ago | ● Data Collection Successful |
| | ELAD-W11-11 | 1 | (GMT+05:30) | 13 sec(s) ago | ● Data Collection Successful |
| | elad-w11-6 | 1 | (GMT+05:30) | 53 sec(s) ago | ● Data Collection Successful |

Note
- Admin Server uses the default Administrator credentials to collect the data from Managed Servers.
- Click on the icon to update the Managed Server credentials whenever there are any changes.
- **Sync now:** The data collection will be restarted and the Managed Server will be synched immediately.

**Figure 26 Auto-Upgrade Managed Servers**

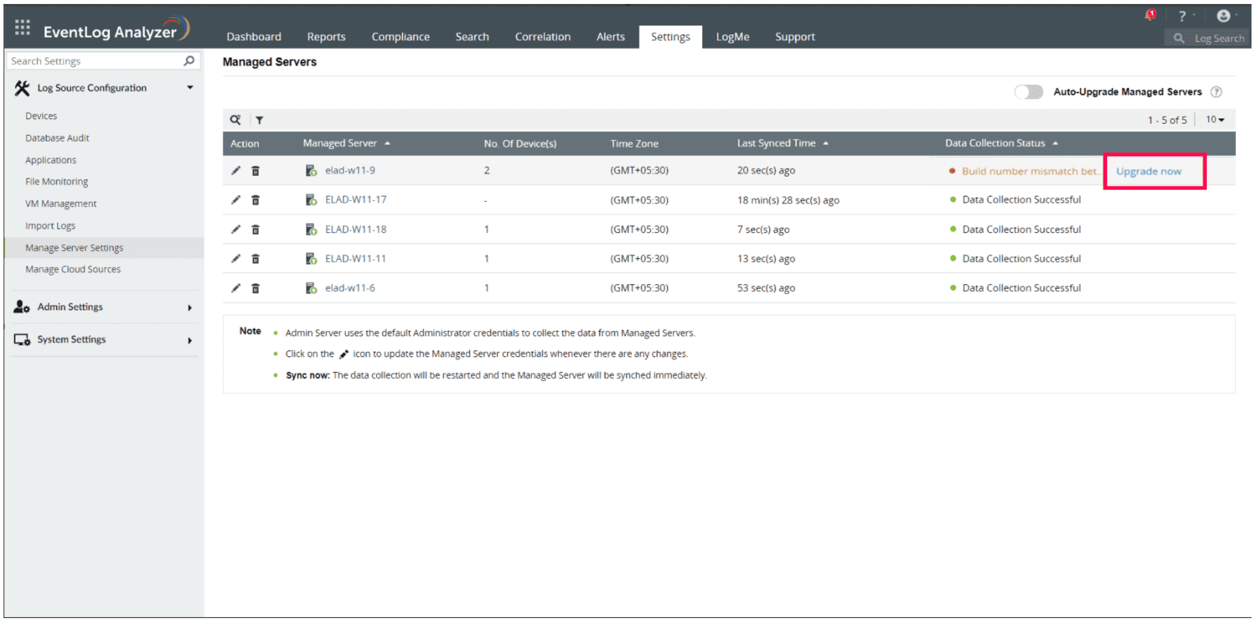
Enable Auto-Upgrade Managed Servers using these steps:

1. Setting up Auto upgrade
2. Go to **Settings → Manage Server Settings** page
3. If the **Auto-Upgrade Managed Servers** toggle is *enabled*, the admin server will automatically upgrade the managed servers once the PPM is applied to the admin server.
4. After configuring auto upgrade settings in the admin server, check all managed servers are in sync.<Syncing MS and AS link>
5. Backup (snapshot or folder backup) the admin server and all the managed servers.
6. Download the Service pack from the EventLog Analyzer site . Link
7. Apply it in the admin server and start the product.

**Note:** The auto-upgrade will attempt to upgrade each managed server only once.

### 4.6 Upgrade now

When the "Auto-Upgrade Managed Servers" toggle is disabled, the **Upgrade now** option will be shown across each managed server; if clicked, it will individually upgrade the selected managed server. (Refer to Figure 27)



Managed Servers

| Action | Managed Server | No. Of Device(s) | Time Zone | Last Synced Time | Data Collection Status | |
|---|---|---|---|---|---|---|
| | elad-w11-9 | 2 | (GMT+05:30) | 20 sec(s) ago | ● Build number mismatch bet... | Upgrade now |
| | ELAD-W11-17 | - | (GMT+05:30) | 18 min(s) 28 sec(s) ago | ● Data Collection Successful | |
| | ELAD-W11-18 | 1 | (GMT+05:30) | 7 sec(s) ago | ● Data Collection Successful | |
| | ELAD-W11-11 | 1 | (GMT+05:30) | 13 sec(s) ago | ● Data Collection Successful | |
| | elad-w11-6 | 1 | (GMT+05:30) | 53 sec(s) ago | ● Data Collection Successful | |

Note
- Admin Server uses the default Administrator credentials to collect the data from Managed Servers.
- Click on the icon to update the Managed Server credentials whenever there are any changes.
- **Sync now:** The data collection will be restarted and the Managed Server will be synched immediately.

**Fig 27 Upgrade now**

## 5. Centralized Log Archival

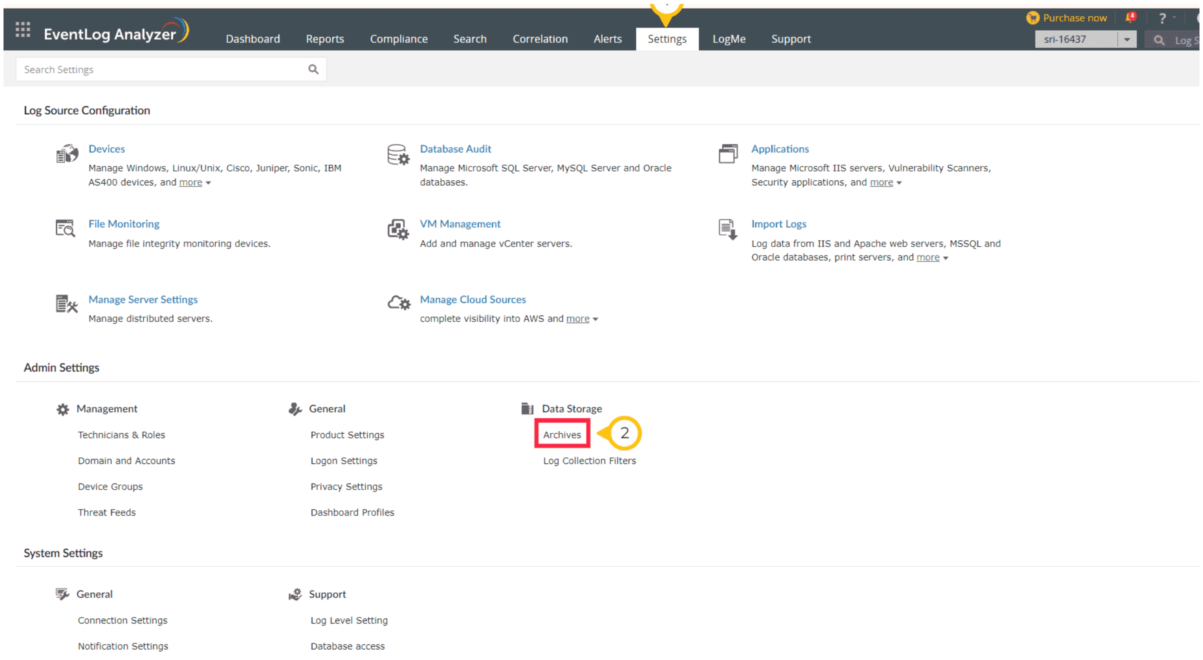
EventLog Analyzer's distributed edition supports centralized archival of event logs received from each host. During log archival configuration in managed servers, if the centralized archival option is enabled, the managed servers will send all their archived logs to the admin server. The admin server will act as a centralized repository for viewing all the logs in your network.

The steps followed by EventLog Analyzer for log archival in the distributed set up are given below:

- Logs are zipped at periodic intervals, and the file to be archived is transported to the admin server using Secured Shell (SSH).
- The file will be received by the admin server, and a confirmation message for the receipt of the file is sent by the admin server to the respective managed server.
- The managed server, upon receiving the confirmation message, deletes the archive file.

## Configuring centralized archival in the admin server:

1. Click the **Settings → Archive** Tab in the Homepage.(Refer to Figure 28)



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

File Monitoring
Manage file integrity monitoring devices.

VM Management
Add and manage vCenter servers.

Import Logs
Log data from IIS and Apache web servers, MSSQL and Oracle databases, print servers, and more

Manage Server Settings
Manage distributed servers.

Manage Cloud Sources
complete visibility into AWS and more

Admin Settings

Management
Technicians & Roles
Domain and Accounts
Device Groups
Threat Feeds

General
Product Settings
Logon Settings
Privacy Settings
Dashboard Profiles

Data Storage
Archives
Log Collection Filters

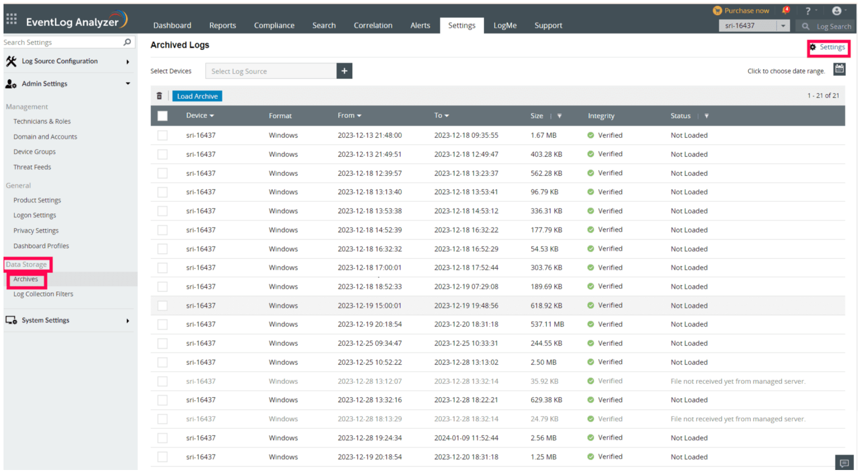
System Settings

General
Connection Settings
Notification Settings

Support
Log Level Setting
Database access

**Figure 28 Archive Tab**

2. Select the **Archive** option under Data Storage. (Refer to Figure 29)



Archived Logs

Select Devices

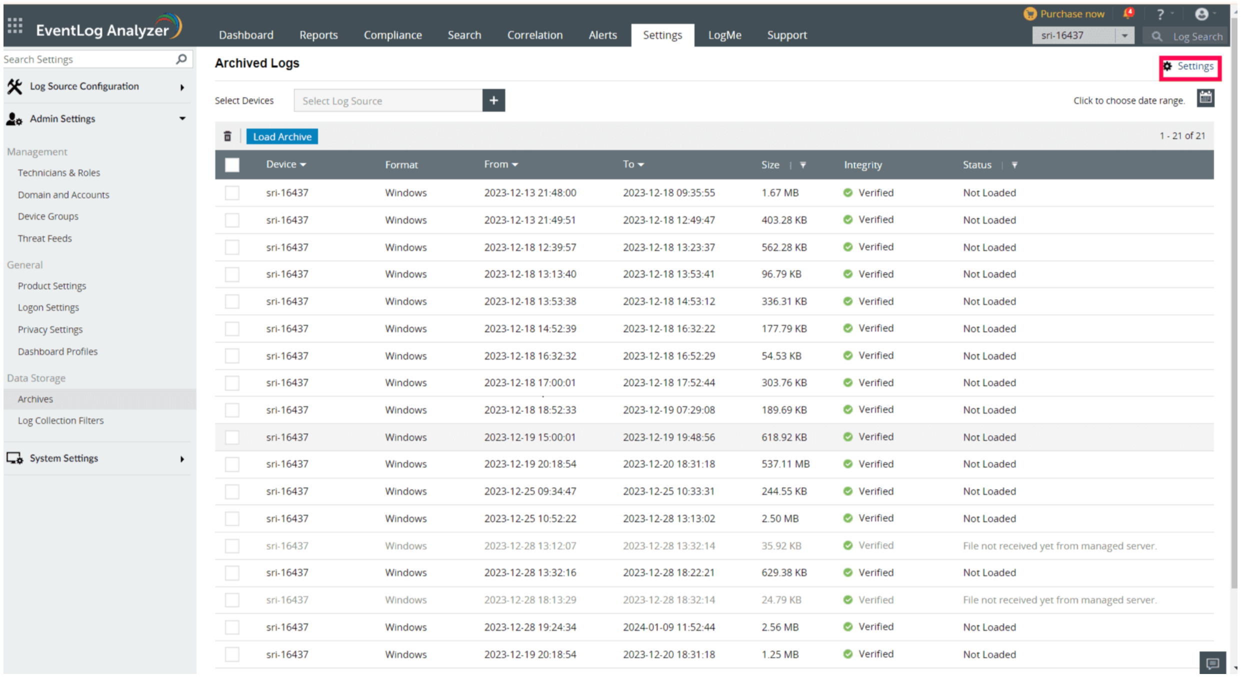
Click to choose date range.

1 - 21 of 21

| □ | Device | Format | From | To | Size | Integrity | Status |
|---|---|---|---|---|---|---|---|
| □ | sri-16437 | Windows | 2023-12-13 21:48:00 | 2023-12-18 09:35:55 | 1.67 MB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-13 21:49:51 | 2023-12-18 12:49:47 | 403.28 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-18 12:39:57 | 2023-12-18 13:23:37 | 562.28 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-18 13:13:40 | 2023-12-18 13:53:41 | 96.79 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-18 13:53:38 | 2023-12-18 14:53:12 | 336.31 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-18 14:52:39 | 2023-12-18 16:32:22 | 177.79 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-18 16:32:32 | 2023-12-18 16:52:29 | 54.53 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-18 17:00:01 | 2023-12-18 17:52:44 | 303.76 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-18 18:52:33 | 2023-12-19 07:29:08 | 189.69 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-19 15:00:01 | 2023-12-19 19:48:56 | 618.92 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-19 20:18:54 | 2023-12-20 18:31:18 | 537.11 MB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-25 09:34:47 | 2023-12-25 10:33:31 | 244.55 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-25 10:52:22 | 2023-12-28 13:13:02 | 2.50 MB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-28 13:12:07 | 2023-12-28 13:32:14 | 35.92 KB | ✓ Verified | File not received yet from managed server. |
| □ | sri-16437 | Windows | 2023-12-28 13:32:16 | 2023-12-28 18:22:21 | 629.38 KB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-28 18:13:29 | 2023-12-28 18:32:14 | 24.79 KB | ✓ Verified | File not received yet from managed server. |
| □ | sri-16437 | Windows | 2023-12-28 19:24:34 | 2024-01-09 11:52:44 | 2.56 MB | ✓ Verified | Not Loaded |
| □ | sri-16437 | Windows | 2023-12-19 20:18:54 | 2023-12-20 18:31:18 | 1.25 MB | ✓ Verified | Not Loaded |

**Figure 29 Archived Logs**

3. Click **Settings** Button (Refer to Figure 30)



**Archived Logs**

Settings

Select Devices: Select Log Source +

Click to choose date range.

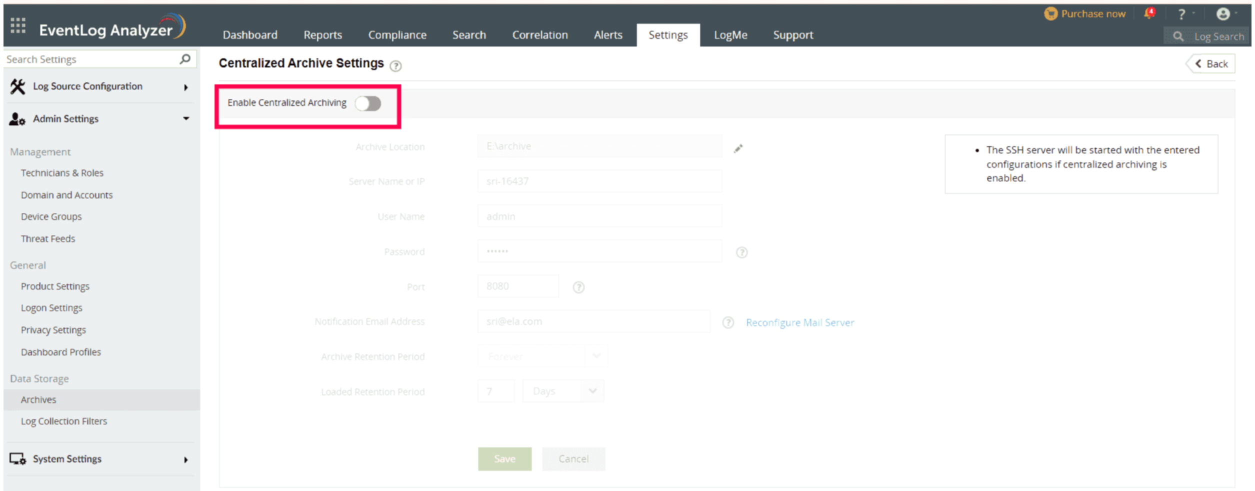
Load Archive

1 - 21 of 21

| Device | Format | From | To | Size | Integrity | Status |
|---|---|---|---|---|---|---|
| sri-16437 | Windows | 2023-12-13 21:48:00 | 2023-12-18 09:35:55 | 1.67 MB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-13 21:49:51 | 2023-12-18 12:49:47 | 403.28 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-18 12:39:57 | 2023-12-18 13:23:37 | 562.28 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-18 13:13:40 | 2023-12-18 13:53:41 | 96.79 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-18 13:53:38 | 2023-12-18 14:53:12 | 336.31 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-18 14:52:39 | 2023-12-18 16:32:22 | 177.79 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-18 16:32:32 | 2023-12-18 16:52:29 | 54.53 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-18 17:00:01 | 2023-12-18 17:52:44 | 303.76 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-18 18:52:33 | 2023-12-19 07:29:08 | 189.69 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-19 15:00:01 | 2023-12-19 19:48:56 | 618.92 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-19 20:18:54 | 2023-12-20 18:31:18 | 537.11 MB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-25 09:34:47 | 2023-12-25 10:33:31 | 244.55 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-25 10:52:22 | 2023-12-28 13:13:02 | 2.50 MB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-28 13:12:07 | 2023-12-28 13:32:14 | 35.92 KB | Verified | File not received yet from managed server. |
| sri-16437 | Windows | 2023-12-28 13:32:16 | 2023-12-28 18:22:21 | 629.38 KB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-28 18:13:29 | 2023-12-28 18:32:14 | 24.79 KB | Verified | File not received yet from managed server. |
| sri-16437 | Windows | 2023-12-28 19:24:34 | 2024-01-09 11:52:44 | 2.56 MB | Verified | Not Loaded |
| sri-16437 | Windows | 2023-12-19 20:18:54 | 2023-12-20 18:31:18 | 1.25 MB | Verified | Not Loaded |

**Figure 30 Settings**

4. Toggle **Enable Central Archiving** Button to enable this feature. (Refer to Figure 31)



**Centralized Archive Settings**

Enable Centralized Archiving

Archive Location: E:\archive

Server Name or IP: sri-16437

User Name: admin

Password: ••••••

Port: 8080

Notification Email Address: sri@ela.com Reconfigure Mail Server

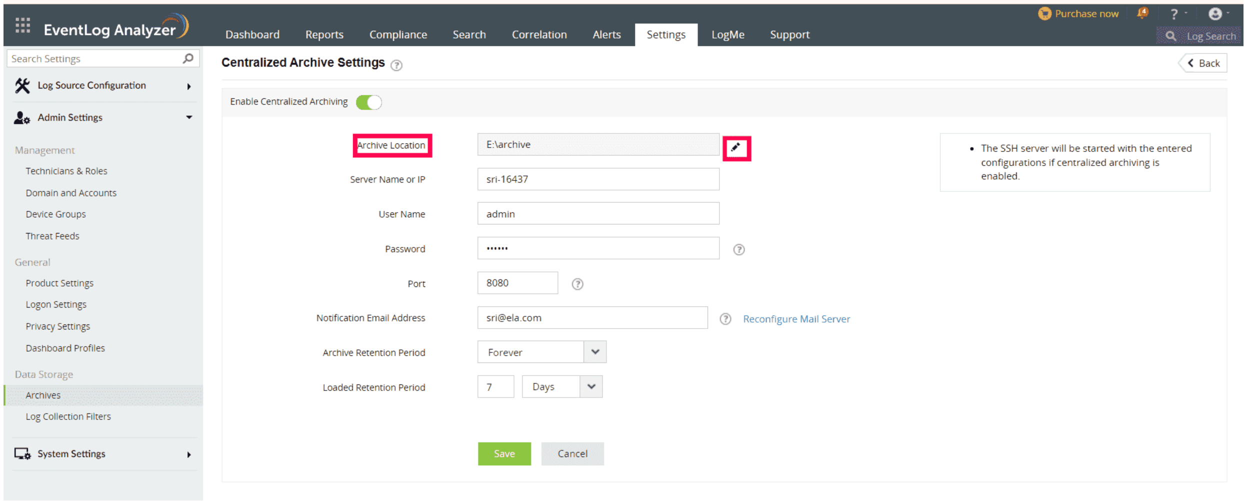
Archive Retention Period: Forever

Loaded Retention Period: 7 Days

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 31 Enable Central Archiving**

5(i). You can change the **Archive location** by clicking the edit icon. (Refer to Figure 32)



Centralized Archive Settings

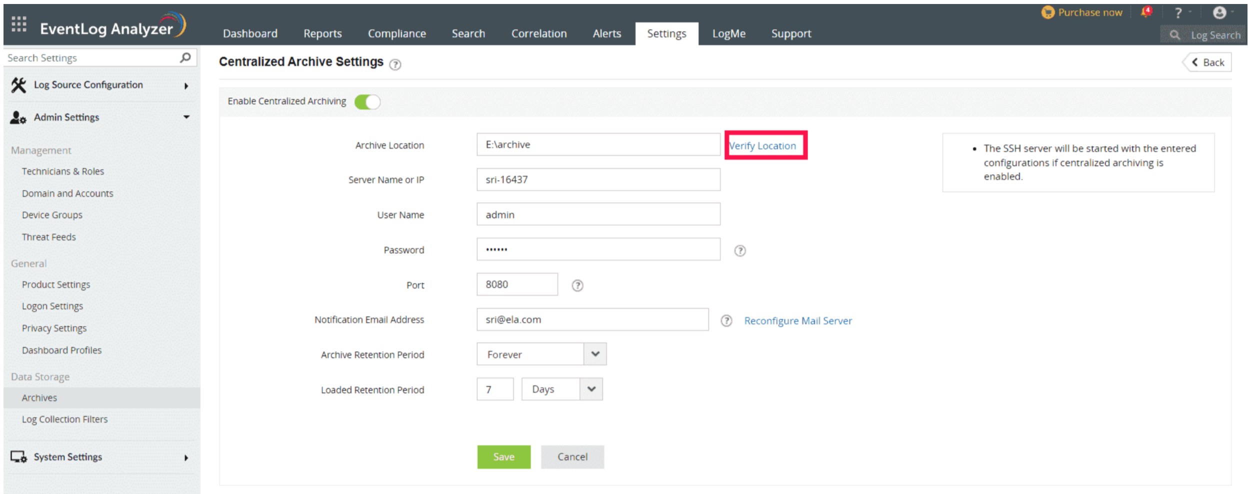
Enable Centralized Archiving

| | |
|---|---|
| Archive Location | E:\archive |
| Server Name or IP | sri-16437 |
| User Name | admin |
| Password | •••••• |
| Port | 8080 |
| Notification Email Address | sri@ela.com |
| Archive Retention Period | Forever |
| Loaded Retention Period | 7 Days |

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 32 Changing Archive location**

(ii). You check the entered location is accessible by clicking the **Verify Location** Button. (Refer to Figure 33)



Centralized Archive Settings

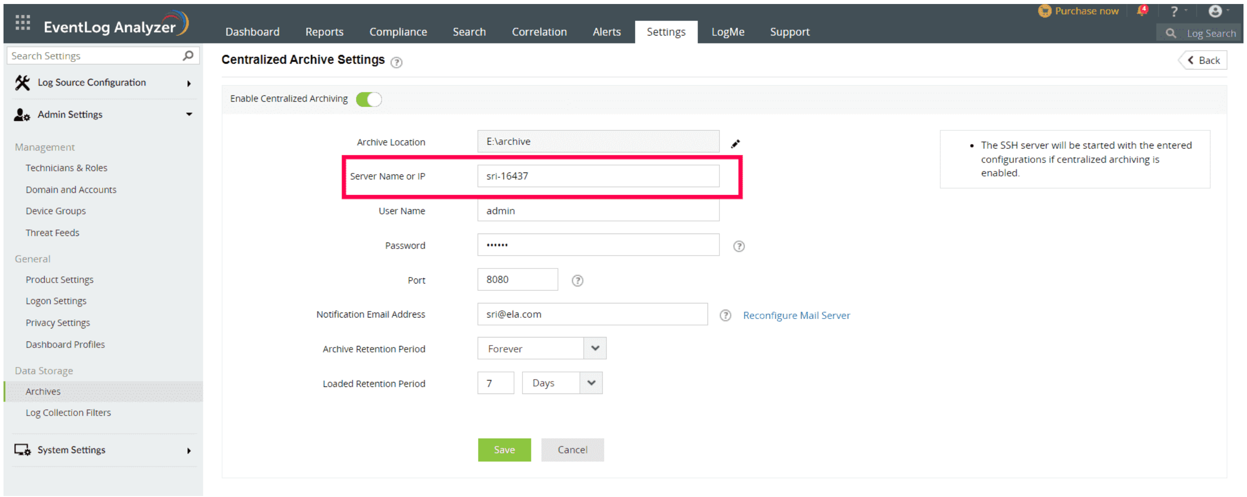
Enable Centralized Archiving

| | |
|---|---|
| Archive Location | E:\archive |
| Server Name or IP | sri-16437 |
| User Name | admin |
| Password | •••••• |
| Port | 8080 |
| Notification Email Address | sri@ela.com |
| Archive Retention Period | Forever |
| Loaded Retention Period | 7 Days |

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 33 Verify Location**

6. You can Edit the name of the **SSH Server**. (Refer to Figure 34)



**Centralized Archive Settings**

Enable Centralized Archiving

Archive Location: E:\archive

Server Name or IP: sri-16437

User Name: admin

Password: ••••••

Port: 8080

Notification Email Address: sri@ela.com

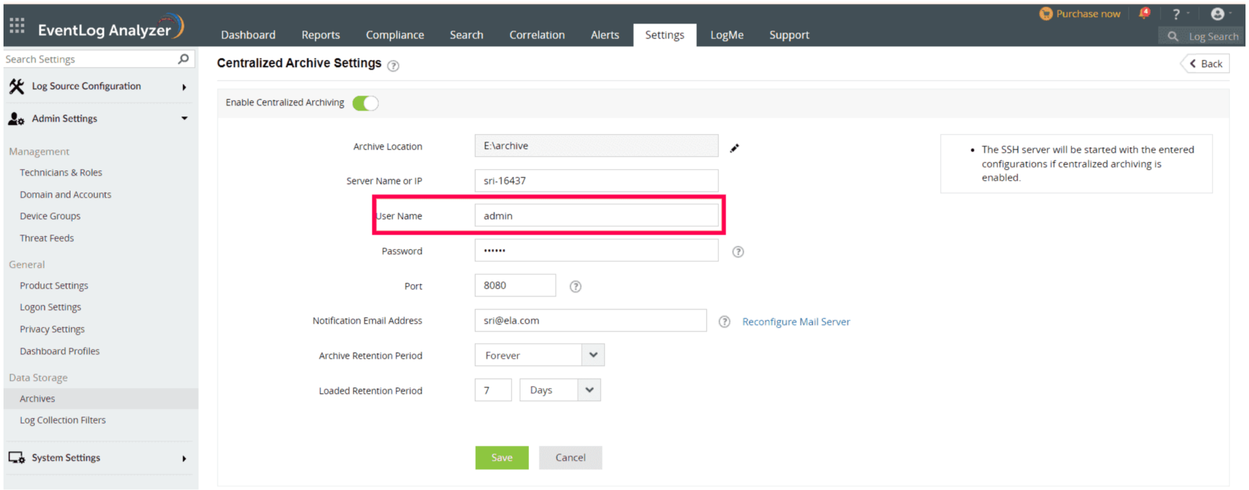
Archive Retention Period: Forever

Loaded Retention Period: 7 Days

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 34 SSH Server Field**

7. You can edit the **SSH Username,** but the default name will be admin. (Refer to Figure 35)



**Centralized Archive Settings**

Enable Centralized Archiving

Archive Location: E:\archive

Server Name or IP: sri-16437

User Name: admin

Password: ••••••

Port: 8080

Notification Email Address: sri@ela.com

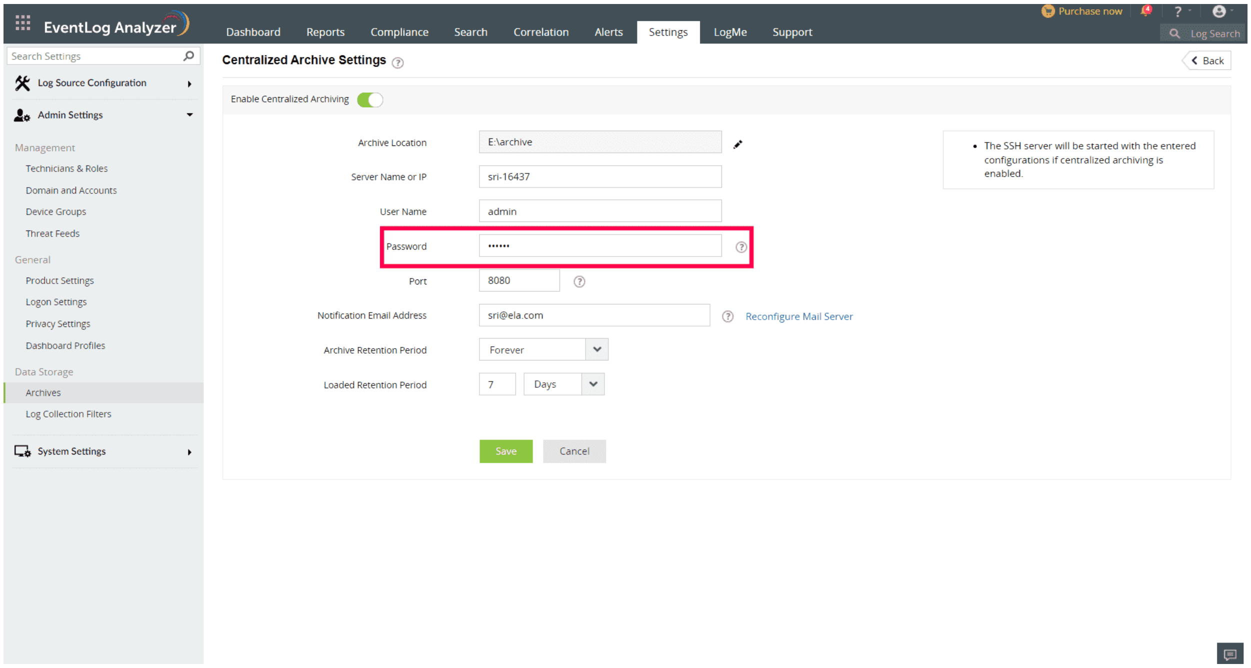
Archive Retention Period: Forever

Loaded Retention Period: 7 Days

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 35 SSH Username Field**

8. You can edit the **password** of the SSH Server. (Refer to Figure 36)



Centralized Archive Settings

Enable Centralized Archiving

Archive Location: E:\archive

Server Name or IP: sri-16437

User Name: admin

Password: ••••••

Port: 8080

Notification Email Address: sri@ela.com

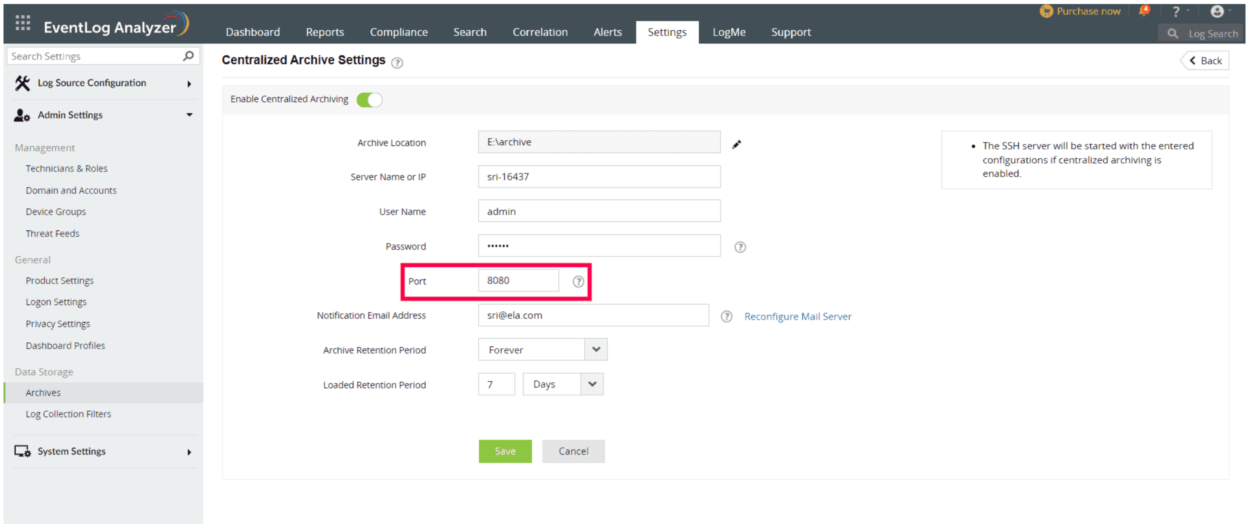
Archive Retention Period: Forever

Loaded Retention Period: 7 Days

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 36 Password Field**

9. You can change the **SSH port number**. It can be 22 or any value between 1024 and 65535. (Refer to Figure 37)



Centralized Archive Settings

Enable Centralized Archiving

Archive Location: E:\archive

Server Name or IP: sri-16437

User Name: admin

Password: ••••••

Port: 8080

Notification Email Address: sri@ela.com

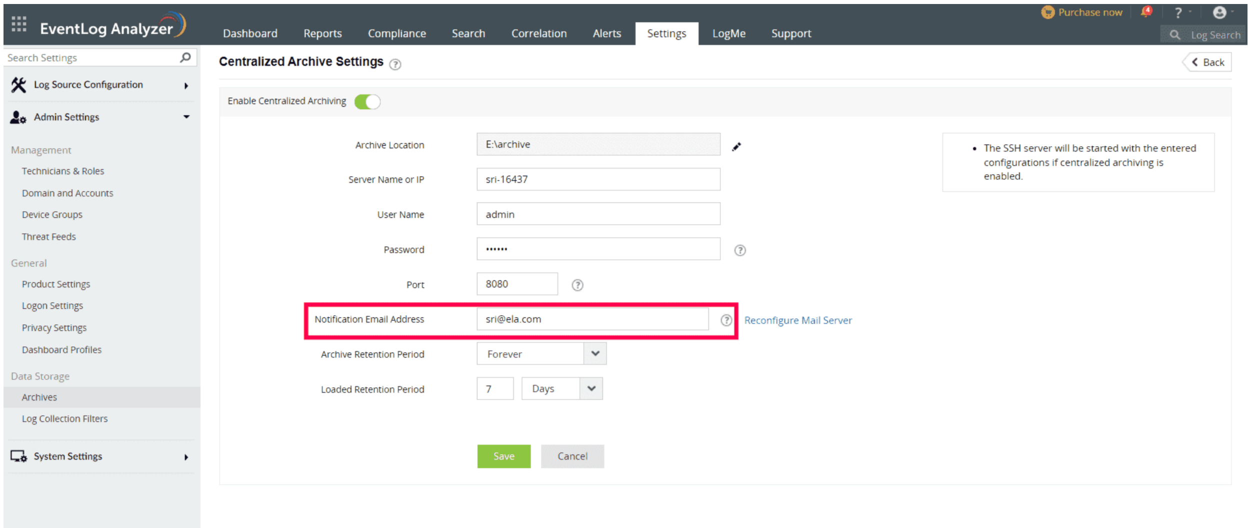
Archive Retention Period: Forever

Loaded Retention Period: 7 Days

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 37 SSH Port Number Field**

10. You can edit the **Notification Mail Address.** The e-mail IDs mentioned in the field will receive notification emails regarding log archival processes. (Refer to Figure 38)



Centralized Archive Settings

Enable Centralized Archiving

Archive Location: E:\archive

Server Name or IP: sri-16437

User Name: admin

Password: ••••••

Port: 8080

Notification Email Address: sri@ela.com

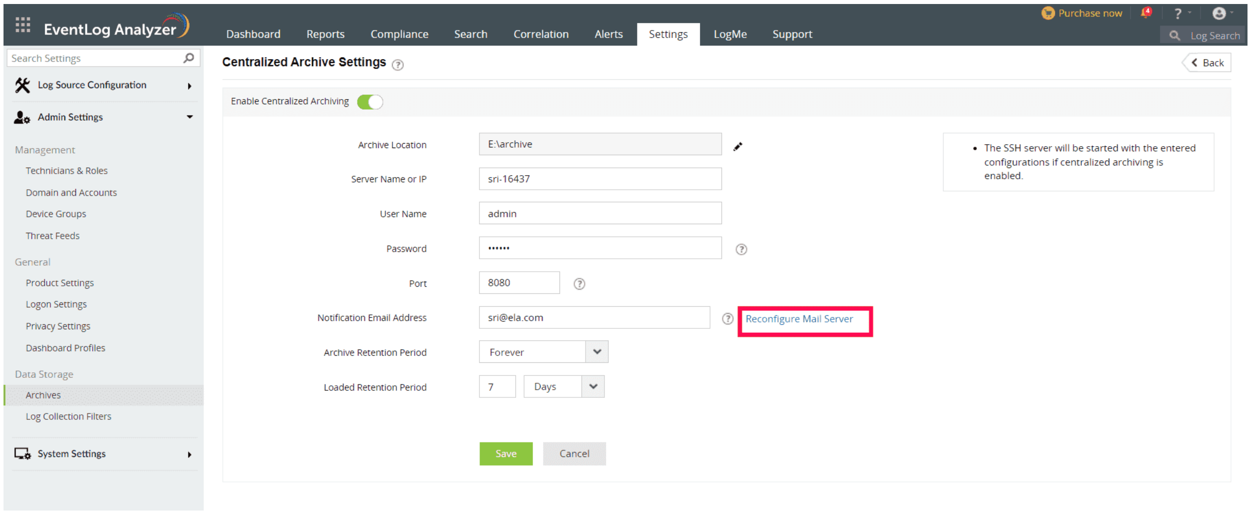
Archive Retention Period: Forever

Loaded Retention Period: 7 Days

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 38 Notification Mail Address Field**

11. You can Reconfigure Mail Server with the desired mail server by clicking the **Reconfigure Mail Server** Button. (Refer to Figure 39)



Centralized Archive Settings

Enable Centralized Archiving

Archive Location: E:\archive

Server Name or IP: sri-16437

User Name: admin

Password: ••••••

Port: 8080

Notification Email Address: sri@ela.com

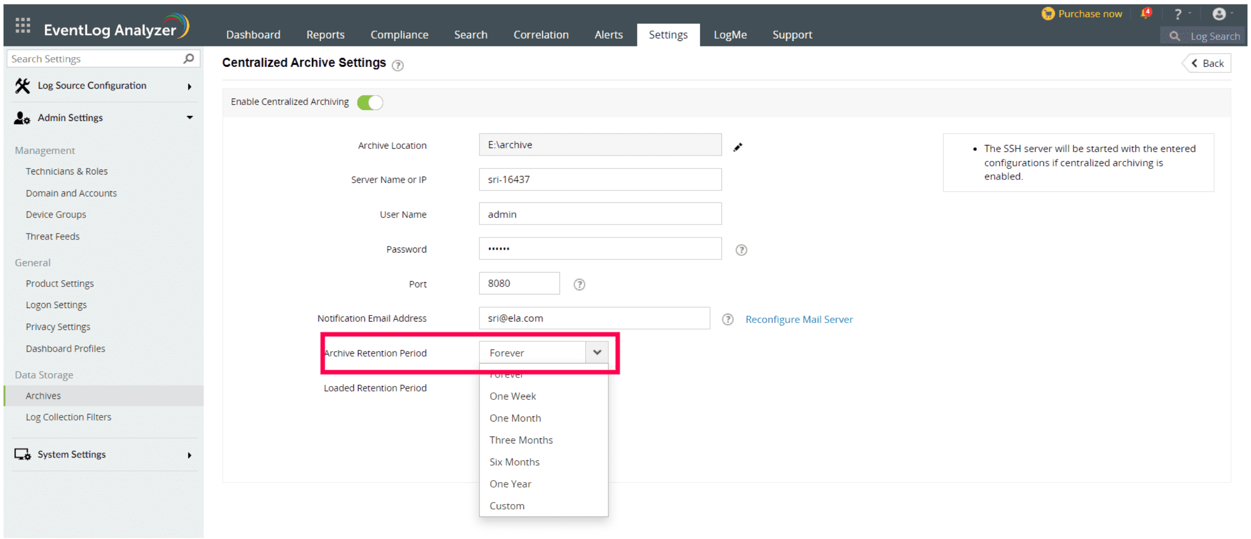
Archive Retention Period: Forever

Loaded Retention Period: 7 Days

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 39 Reconfigure Mail Server**

12. You can change the **Archive Retention Period** By Clicking the dropdown button and selecting the value of the dropdown value. Specify how long these archive files should be kept in the server. Once the period elapses, the files will be deleted from the EventLog Analyzer server. (Refer to Figure 40)



Centralized Archive Settings

Enable Centralized Archiving

Archive Location: E:\archive

Server Name or IP: sri-16437

User Name: admin

Password: ••••••

Port: 8080

Notification Email Address: sri@ela.com

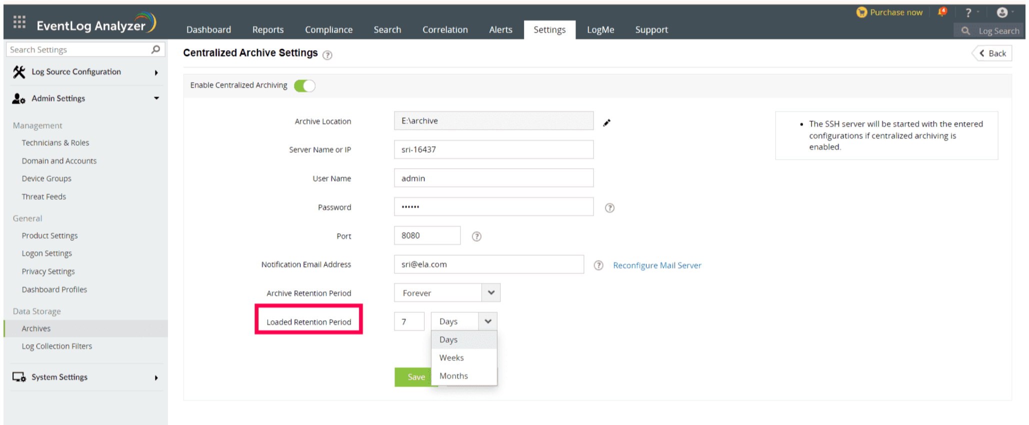
Archive Retention Period: Forever

Loaded Retention Period

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 40 Archive Retention Period**

13. You can change the **loaded retention period** by clicking the drop-down button and selecting the value of the drop-down, but the Minimum period is 1 Day. Specify the period for which the archive files should remain loaded. (Refer to Figure 41)



Centralized Archive Settings

Enable Centralized Archiving

Archive Location: E:\archive

Server Name or IP: sri-16437

User Name: admin

Password: ••••••

Port: 8080

Notification Email Address: sri@ela.com

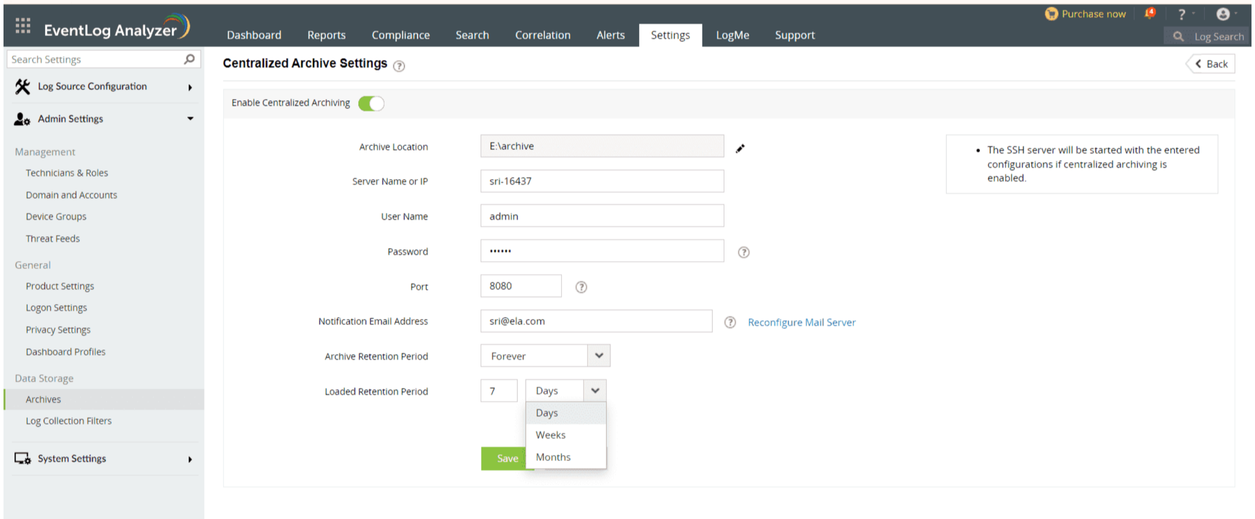
Archive Retention Period: Forever

Loaded Retention Period: 7 Days

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 41 Loaded Retention Period**

14. To save the changes, click the **Save** Button. (Refer to Figure 42)



Centralized Archive Settings

Enable Centralized Archiving

Archive Location: E:\archive

Server Name or IP: sri-16437

User Name: admin

Password: ••••••

Port: 8080

Notification Email Address: sri@ela.com

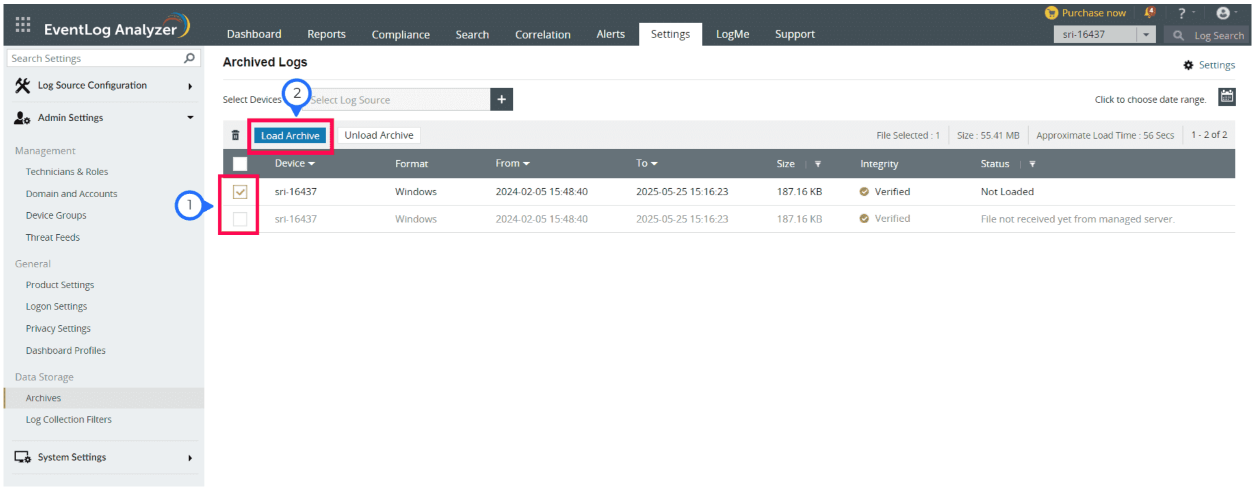
Archive Retention Period: Forever

Loaded Retention Period: 7 Days

- The SSH server will be started with the entered configurations if centralized archiving is enabled.

**Figure 42 Save**

15. Click the check box to select the Archive file you want to Load. After you select, click the **Load Archive** Button to load the Archive file. (Refer to Figure 43)



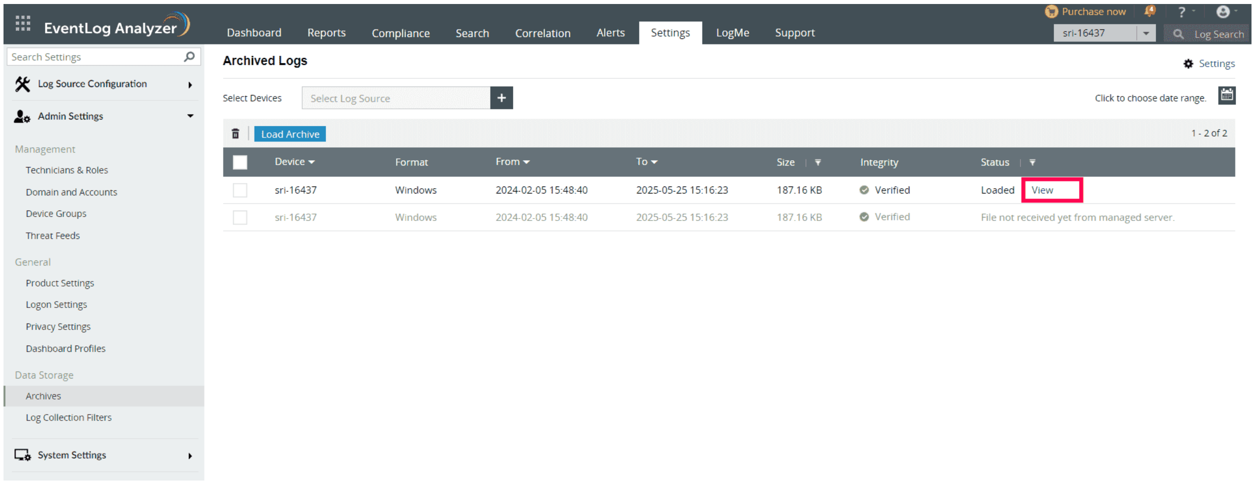
Archived Logs

File Selected : 1 | Size : 55.41 MB | Approximate Load Time : 56 Secs | 1 - 2 of 2

| | Device | Format | From | To | Size | Integrity | Status |
|---|---|---|---|---|---|---|---|
| ☑ | sri-16437 | Windows | 2024-02-05 15:48:40 | 2025-05-25 15:16:23 | 187.16 KB | Verified | Not Loaded |
| □ | sri-16437 | Windows | 2024-02-05 15:48:40 | 2025-05-25 15:16:23 | 187.16 KB | Verified | File not received yet from managed server. |

**Figure 43 Load Archive**

16. To view the loaded archive, click the **View** button. (Refer to Figure 44)

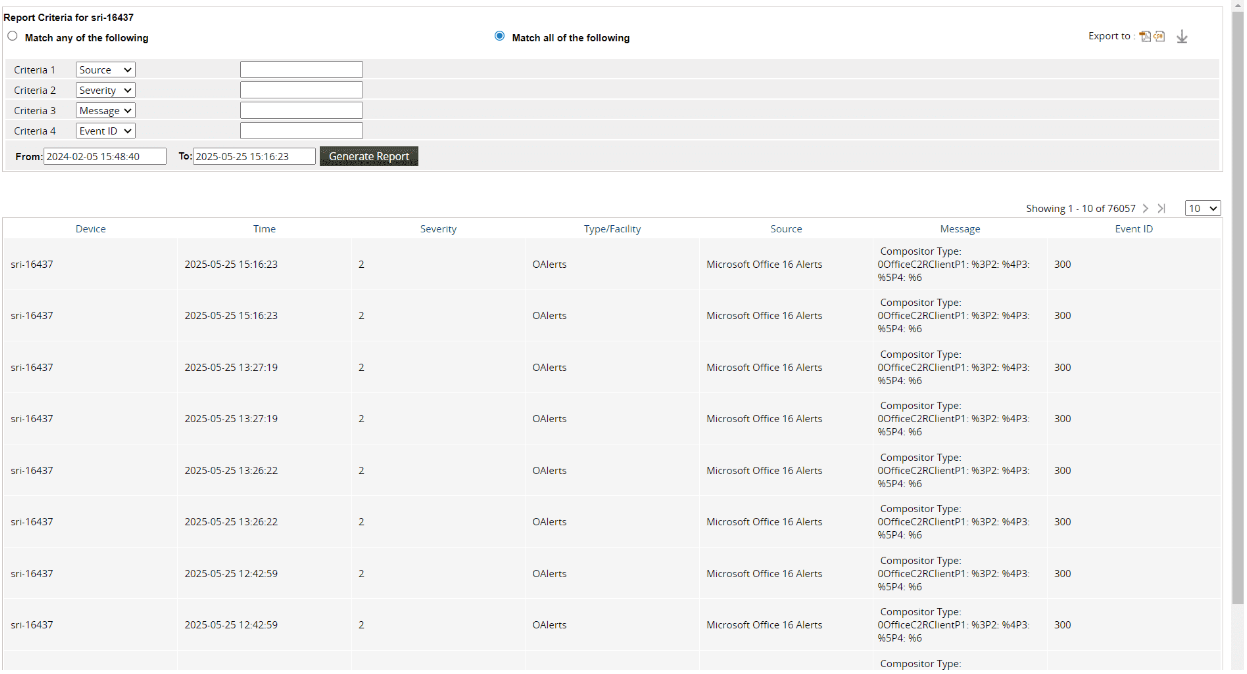


Archived Logs

| Device | Format | From | To | Size | Integrity | Status |
|---|---|---|---|---|---|---|
| sri-16437 | Windows | 2024-02-05 15:48:40 | 2025-05-25 15:16:23 | 187.16 KB | Verified | Loaded View |
| sri-16437 | Windows | 2024-02-05 15:48:40 | 2025-05-25 15:16:23 | 187.16 KB | Verified | File not received yet from managed server. |

**Figure 44 View Status**

17. The reports will be shown like the below image. (Refer to Figure 45)



Report Criteria for sri-16437

○ Match any of the following ● Match all of the following

| | | |
|---|---|---|
| Criteria 1 | Source | |
| Criteria 2 | Severity | |
| Criteria 3 | Message | |
| Criteria 4 | Event ID | |

From: 2024-02-05 15:48:40 To: 2025-05-25 15:16:23

| Device | Time | Severity | Type/Facility | Source | Message | Event ID |
|---|---|---|---|---|---|---|
| sri-16437 | 2025-05-25 15:16:23 | 2 | OAlerts | Microsoft Office 16 Alerts | Compositor Type: 0OfficeC2RClientP1: %3P2: %4P3: %5P4: %6 | 300 |
| sri-16437 | 2025-05-25 15:16:23 | 2 | OAlerts | Microsoft Office 16 Alerts | Compositor Type: 0OfficeC2RClientP1: %3P2: %4P3: %5P4: %6 | 300 |
| sri-16437 | 2025-05-25 13:27:19 | 2 | OAlerts | Microsoft Office 16 Alerts | Compositor Type: 0OfficeC2RClientP1: %3P2: %4P3: %5P4: %6 | 300 |
| sri-16437 | 2025-05-25 13:27:19 | 2 | OAlerts | Microsoft Office 16 Alerts | Compositor Type: 0OfficeC2RClientP1: %3P2: %4P3: %5P4: %6 | 300 |
| sri-16437 | 2025-05-25 13:26:22 | 2 | OAlerts | Microsoft Office 16 Alerts | Compositor Type: 0OfficeC2RClientP1: %3P2: %4P3: %5P4: %6 | 300 |
| sri-16437 | 2025-05-25 13:26:22 | 2 | OAlerts | Microsoft Office 16 Alerts | Compositor Type: 0OfficeC2RClientP1: %3P2: %4P3: %5P4: %6 | 300 |
| sri-16437 | 2025-05-25 12:42:59 | 2 | OAlerts | Microsoft Office 16 Alerts | Compositor Type: 0OfficeC2RClientP1: %3P2: %4P3: %5P4: %6 | 300 |
| sri-16437 | 2025-05-25 12:42:59 | 2 | OAlerts | Microsoft Office 16 Alerts | Compositor Type: 0OfficeC2RClientP1: %3P2: %4P3: %5P4: %6 | 300 |
| | | | | | Compositor Type: | |

**Figure 45 Reports**

# 6. Upgrading EventLog Analyzer distributed edition

This section explains how users can upgrade the EventLog Analyzer Distributed Edition. In order to access the latest features and enhancements, users are required to upgrade to the latest version.

## 6.1 Steps to upgrade the EventLog Analyzer Distributed edition

The managed servers should be synchronized and registered with the admin server, facilitating proper connectivity between them. This ensures a seamless auto upgrade without any issues. Before upgrading, you need to back up both the managed and admin servers. This is essential in the event of an upgrade failure, ensuring a swift recovery.

Here are the steps for upgrading:

### A) Taking a manual backup of Admin Server

1. Shutdown the EventLog Analyzer Admin server.
2. Copy the following folders/files as backup
   - <Home>/Conf
   - <Home>/adsdata
   - <Home>/lib/AdventNetLicense.xml
3. Database backup

Please follow the same steps as for the Standalone server.

### B) Taking a manual backup of managed server

1. Shutdown the EventLog Analyzer managed server(s).
2. Copy the following folders/files as backup
   - <Home>/Conf
   - <Home>/adsdata
   - <Home>/lib/AdventNetLicense.xml
3. Database backup

Please follow the same steps as for the Standalone server.

### C) Prerequisites before performing the upgrade:

1. Ensure all the managed servers are in sync and registered with the admin server. This is required in order to achieve a smooth auto upgrade without encountering any issues.
2. During the upgrade within the same storage drive of EventLog Analyzer, a backup is executed. Hence, it is important to ensure that there is sufficient space available for backup.(more than twice the space occupied by conf folder and Database)
3. Please stop the EventLog Analyzer service and take a copy of the entire EventLog Analyzer folder or a server snapshot. Please note that backing up EventLog Analyzer is mandatory so that you can restore the installation to this version in case of upgrade failures. For Distributed Edition of EventLog Analyzer, back up the admin server and all managed servers.
4. If you use a MS SQL database, we strongly recommend you take a snapshot of your database as well.
5. In case you apply more than one service pack at a time, please start the EventLog Analyzer application after each service pack upgrade.

### D) Performing the upgrade on the Admin Server:

Apply the latest service pack in the PPM(Portable Pixmap Format) on the Admin Server. Please check the instructions to apply the service pack.

## 6.2 Types of Upgrading managed server

Upon completion of the Admin Server upgrade, the subsequent step involves upgrading the managed servers.

There are two ways to achieve this:

1. Auto upgrading all managed servers through the Admin Server
2. Manually upgrading managed servers.

### Case - I: Auto upgrading all managed servers through the Admin Server

When the admin server is upgraded through a service pack, all its managed servers will be automatically upgraded by default.

Here are the steps for auto upgrading the managed servers:

- Shutdown the admin server and all the managed servers.
- Take snapshots or folder backup of all the servers.(Either folder backup or snapshot)
- Apply PPM in the admin server.
- Start the admin server.
- After ensuring that the admin server is up and running, start all the managed servers one by one.
- Wait for the admin server to upgrade all the managed servers before applying the next PPM on the admin server.

note: Stopping all managed servers is not mandatory.

### Case - II: Manually upgrading managed servers

In this case, the managed servers will be upgraded individually. During this process, a space check is conducted on the managed servers before applying the service pack. This is to ensure that there is enough storage space to accommodate the backup files of the existing system.

In the event of a backup failure, due to insufficient storage or other reasons, users can choose to skip the backup provided they have manually taken the backup of the managed servers as mentioned in **Step B**.

Here are the steps to upgrade each managed server manually:

- Shutdown the admin server and all the managed servers.
- Take snapshots or folder backup of all the servers.
- Add **DisablePPMCheck=true** in enterprise.txt of all the managed servers.
- Upgrade the managed server one by one using updatemanager.bat
- After upgrading all the managed servers, apply PPM on the admin server.
- Start the admin server.

After ensuring that the admin server is up and running, start all the managed servers one by one.

Steps to Upgrade Distribution Edition - Link

## 7. Integration with Log360 - Link

Integrating Distributed EventLog Analyzer with Log360 gives users the functionality to directly view Dashboard, Reports, Compliance and Configuration tabs for each managed server individually.

**Note:**

1. Kindly ensure that you integrate EventLog Analyzer version 12150 or above and upcoming builds of Log360 (Build 5214 and above).
2. The integration of Distributed EventLog Analyzer will not support the UEBA and SIEM features.

### 7.1 Integration:

To integrate distributed EventLog Analyzer with Log360 on the Log360 integration page, it is necessary to provide the EventLog Analyzer Admin Server details.

**From the Log360 console, navigate to Admin → Administration → Log360 Integration → EventLog Analyzer**

**Note:**

- Ensure that the admin server is running before proceeding with the steps given below. Also, check whether you have the appropriate versions of the components with respect to the Log360 version you are currently running.

- To convert the integrated standalone edition of EventLog Analyzer to an admin server, you need to remove its integration from Log360 by navigating to **Admin ->Administration → Log360 Integration → EventLog Analyzer** and clicking **Remove**. You can then convert the Standalone EventLog Analyzer to admin server and then integrate the distributed edition of EventLog Analyzer component with Log360 .

The steps to be followed are given below:

1. Go to **Admin → Log360 integration.** You will be presented with two tabs, each representing a component of Log360. (Refer to Figure 46)

2. Click on any one of the tabs (say EventLog Analyzer).

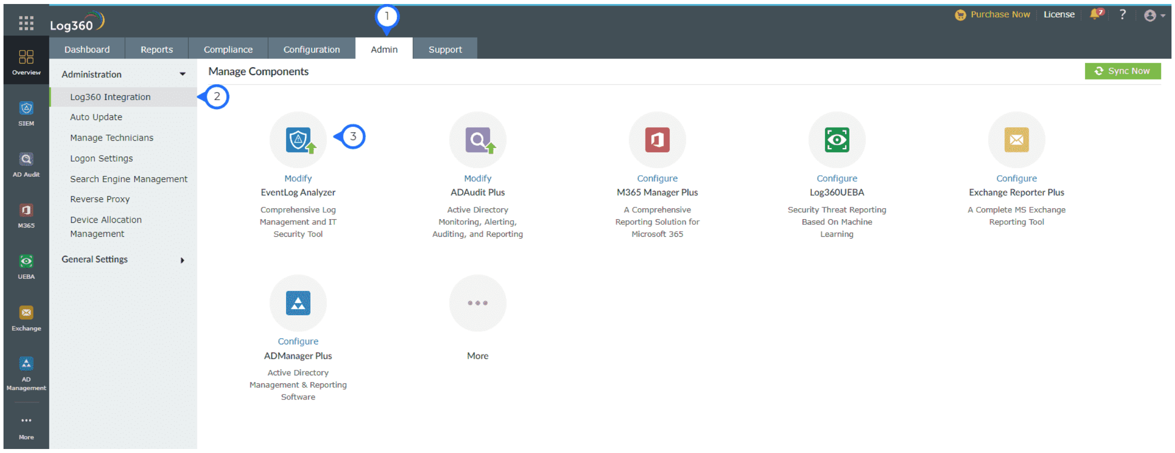
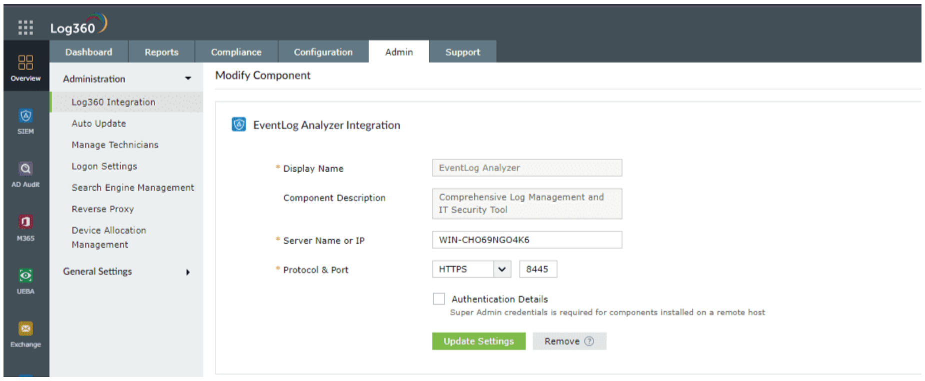


**Figure 46 Log360 Integration**

3. Enter the name or IP address and port number of the server on which that particular component is running.

4. Select the connection **Protocol** from the drop down menu.

5. Click **Integrate Now.** (Refer to Figure 47)



Modify Component

EventLog Analyzer Integration

* Display Name: EventLog Analyzer

Component Description: Comprehensive Log Management and IT Security Tool

* Server Name or IP: WIN-CHO69NGO4K6

* Protocol & Port: HTTPS 8445

□ Authentication Details
Super Admin credentials is required for components installed on a remote host

Update Settings   Remove

**Figure 47 EventLog Analyzer Integration page**

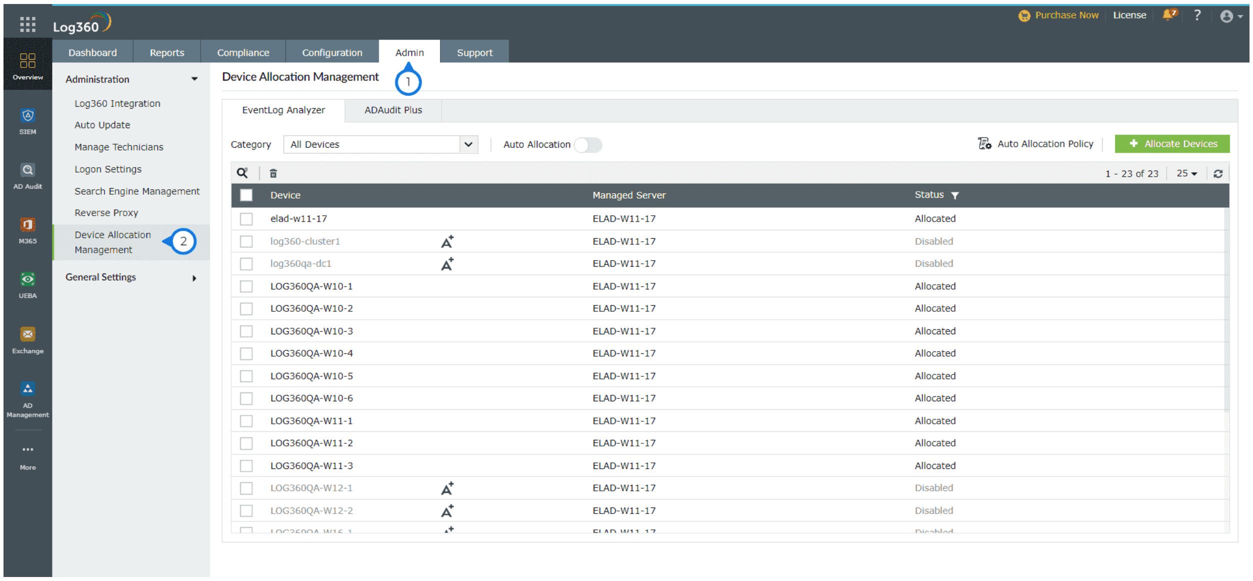
## 7.2 Device Allocation Management

EventLog Analyzer Admin Server and ADAudit Plus are two of the components of Log360 that predominantly work based on the number of devices they monitor. To avoid duplication of devices, Log360 device allocation module synchronize all the devices in the network between EventLog Analyzer with the ADAudit Plus and allows you to control the Windows devices added to them from a single console. You can enable auto allocation to avoid adding devices manually.

**Note:** The Device Allocation Management feature can be accessed by the default admin only.

You can check out the device allocation feature by following the steps below

1. Navigate to **Admin → Administration → Device Allocation Management**. You can view the existing devices here. (Refer to Figure 48)

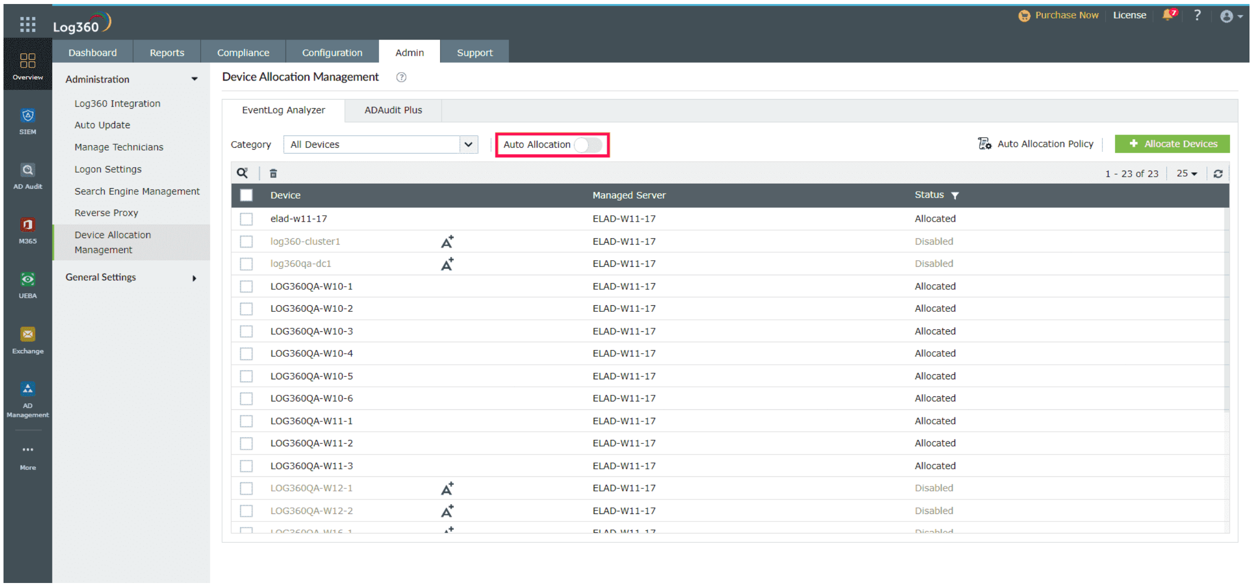


| Device | Managed Server | Status |
|---|---|---|
| elad-w11-17 | ELAD-W11-17 | Allocated |
| log360-cluster1 | ELAD-W11-17 | Disabled |
| log360qa-dc1 | ELAD-W11-17 | Disabled |
| LOG360QA-W10-1 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-2 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-3 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-4 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-5 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-6 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-1 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-2 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-3 | ELAD-W11-17 | Allocated |
| LOG360QA-W12-1 | ELAD-W11-17 | Disabled |
| LOG360QA-W12-2 | ELAD-W11-17 | Disabled |

**Figure 48: Device Allocation Management**

Users can view all allocated devices along with their status, inheritance status, and the managed server to which they are allocated.

2. To activate or deactivate the auto-allocation feature, toggle the **"Auto Allocation"** switch. (Refer to Figure 49)

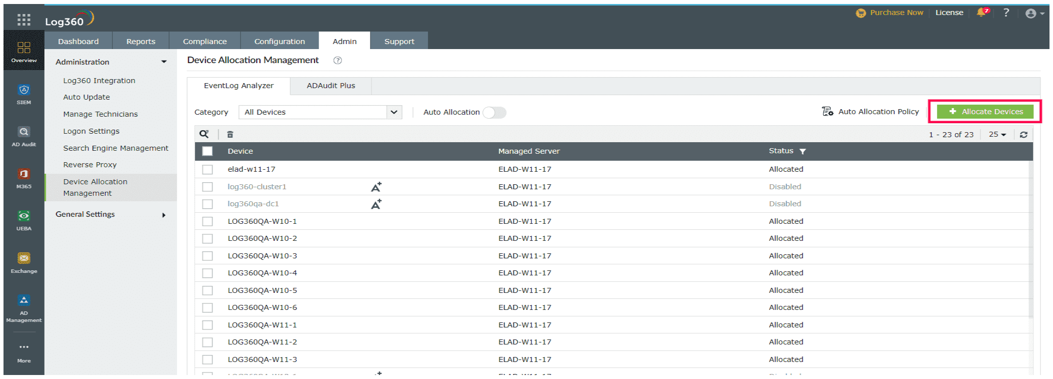


| Device | Managed Server | Status |
|---|---|---|
| elad-w11-17 | ELAD-W11-17 | Allocated |
| log360-cluster1 | ELAD-W11-17 | Disabled |
| log360qa-dc1 | ELAD-W11-17 | Disabled |
| LOG360QA-W10-1 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-2 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-3 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-4 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-5 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-6 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-1 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-2 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-3 | ELAD-W11-17 | Allocated |
| LOG360QA-W12-1 | ELAD-W11-17 | Disabled |
| LOG360QA-W12-2 | ELAD-W11-17 | Disabled |

**Figure 49 Auto Allocation**

## To configure devices manually, follow the steps outlined below

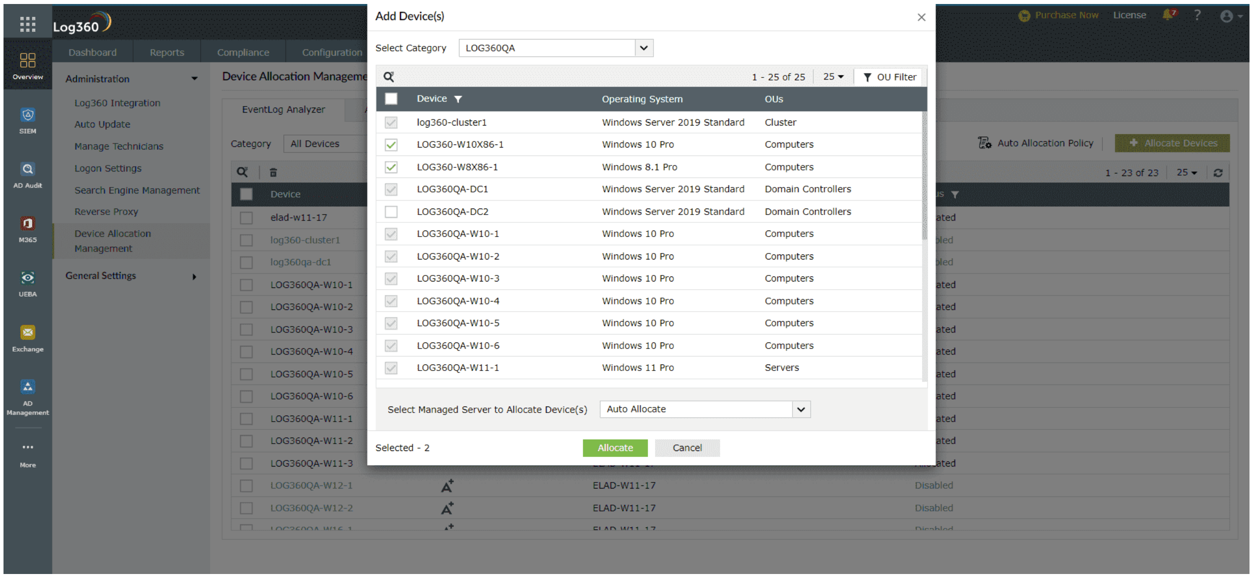
1) Click on the **Allocate Devices** option, to allocate devices to EventLog Analyzer. (Refer to Figure 50)



| Device | Managed Server | Status |
|---|---|---|
| elad-w11-17 | ELAD-W11-17 | Allocated |
| log360-cluster1 | ELAD-W11-17 | Disabled |
| log360qa-dc1 | ELAD-W11-17 | Disabled |
| LOG360QA-W10-1 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-2 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-3 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-4 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-5 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-6 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-1 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-2 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-3 | ELAD-W11-17 | Allocated |

**Figure 50 Allocate Devices**

2) Select category from the drop-down and select the devices from the **Add Devices** window. (Refer to Figure 51)



Add Device(s)

Select Category: LOG360QA

1 - 25 of 25 | 25 | OU Filter

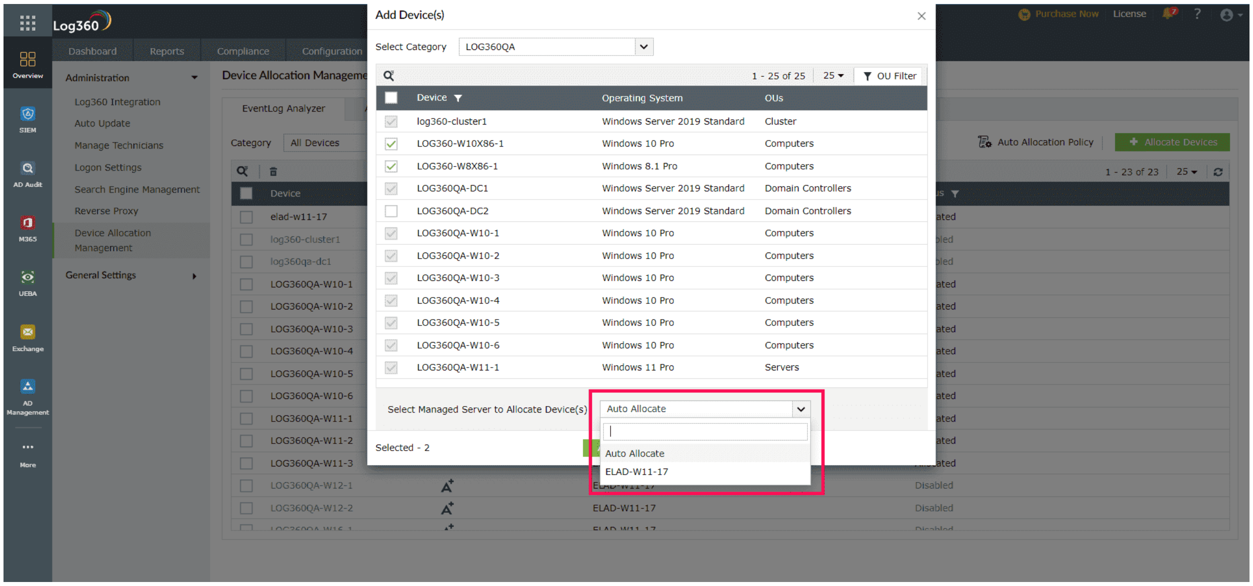
| | Device | Operating System | OUs |
|---|---|---|---|
| ☑ | log360-cluster1 | Windows Server 2019 Standard | Cluster |
| ☑ | LOG360-W10X86-1 | Windows 10 Pro | Computers |
| ☑ | LOG360-W8X86-1 | Windows 8.1 Pro | Computers |
| ☑ | LOG360QA-DC1 | Windows Server 2019 Standard | Domain Controllers |
| ☐ | LOG360QA-DC2 | Windows Server 2019 Standard | Domain Controllers |
| ☑ | LOG360QA-W10-1 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W10-2 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W10-3 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W10-4 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W10-5 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W10-6 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W11-1 | Windows 11 Pro | Servers |

Select Managed Server to Allocate Device(s): Auto Allocate

Selected - 2

**Figure 51 Add Device(s)**

3) Select the allocation type, either manually to any managed server or automatically allocate to available managed servers. (Refer to Figure 52)



Add Device(s)

Select Category: LOG360QA

1 - 25 of 25 | 25 | OU Filter

| | Device | Operating System | OUs |
|---|---|---|---|
| ☑ | log360-cluster1 | Windows Server 2019 Standard | Cluster |
| ☑ | LOG360-W10X86-1 | Windows 10 Pro | Computers |
| ☑ | LOG360-W8X86-1 | Windows 8.1 Pro | Computers |
| ☑ | LOG360QA-DC1 | Windows Server 2019 Standard | Domain Controllers |
| ☐ | LOG360QA-DC2 | Windows Server 2019 Standard | Domain Controllers |
| ☑ | LOG360QA-W10-1 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W10-2 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W10-3 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W10-4 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W10-5 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W10-6 | Windows 10 Pro | Computers |
| ☑ | LOG360QA-W11-1 | Windows 11 Pro | Servers |

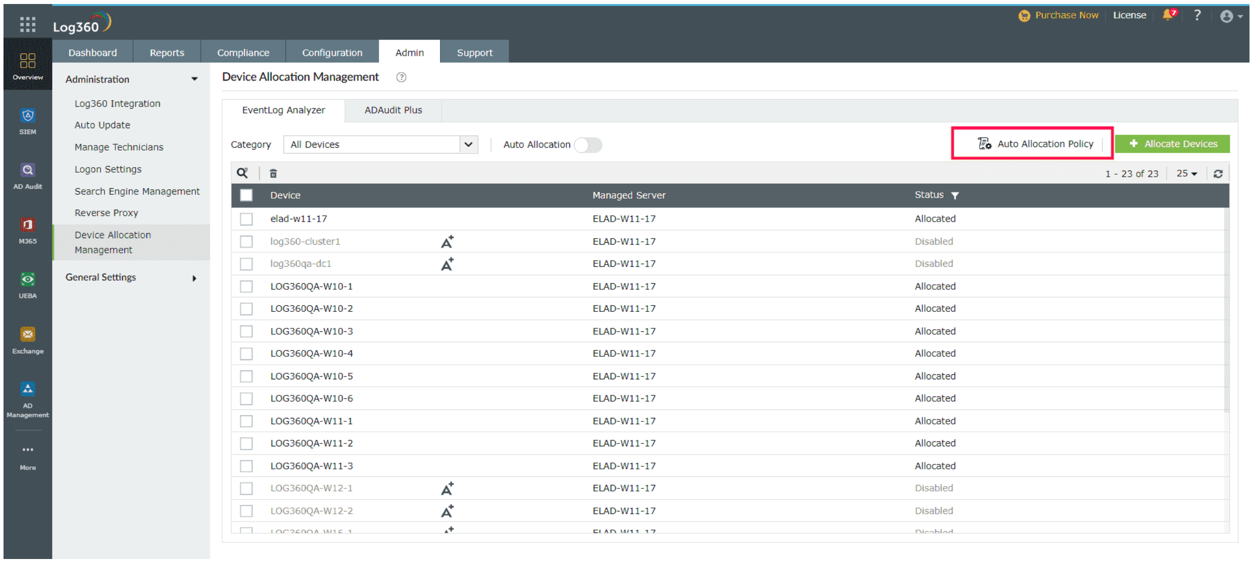
Select Managed Server to Allocate Device(s): Auto Allocate

Selected - 2

**Figure 52 Select managed Server to allocate device(s)**

4) After choosing the allocation type, click on the "Allocate" button.

5) For configuring auto-allocation policies, Click **Auto Allocation Policy** to view the device allocation. (Refer to Figure 53 & 54)

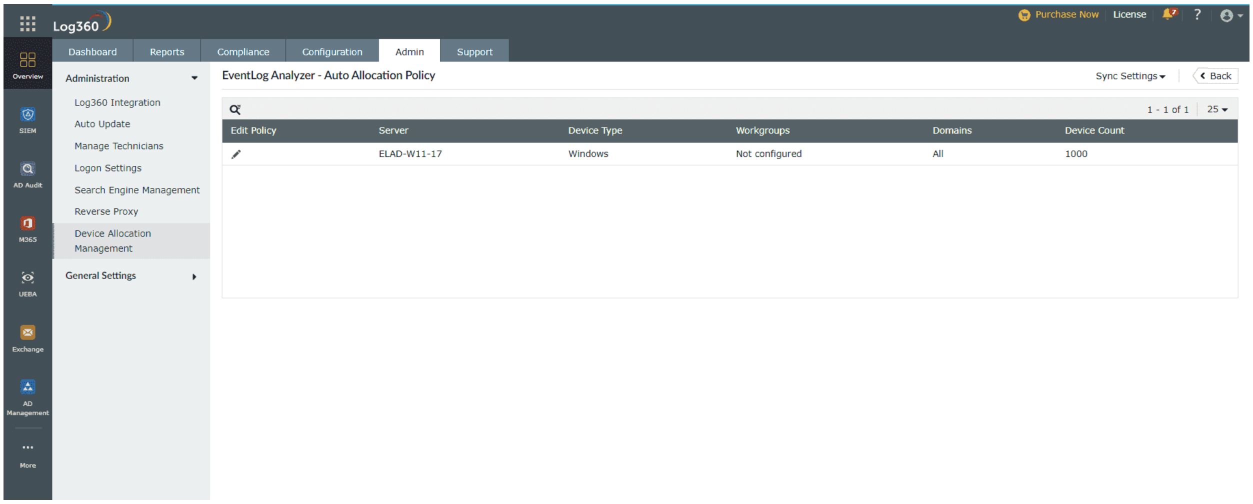


Category: All Devices

Auto Allocation

| Device | Managed Server | Status |
|---|---|---|
| elad-w11-17 | ELAD-W11-17 | Allocated |
| log360-cluster1 | ELAD-W11-17 | Disabled |
| log360qa-dc1 | ELAD-W11-17 | Disabled |
| LOG360QA-W10-1 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-2 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-3 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-4 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-5 | ELAD-W11-17 | Allocated |
| LOG360QA-W10-6 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-1 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-2 | ELAD-W11-17 | Allocated |
| LOG360QA-W11-3 | ELAD-W11-17 | Allocated |
| LOG360QA-W12-1 | ELAD-W11-17 | Disabled |
| LOG360QA-W12-2 | ELAD-W11-17 | Disabled |
| LOG360QA-W16-1 | ELAD-W11-17 | Disabled |

**Figure 53 Auto Allocation Policy**

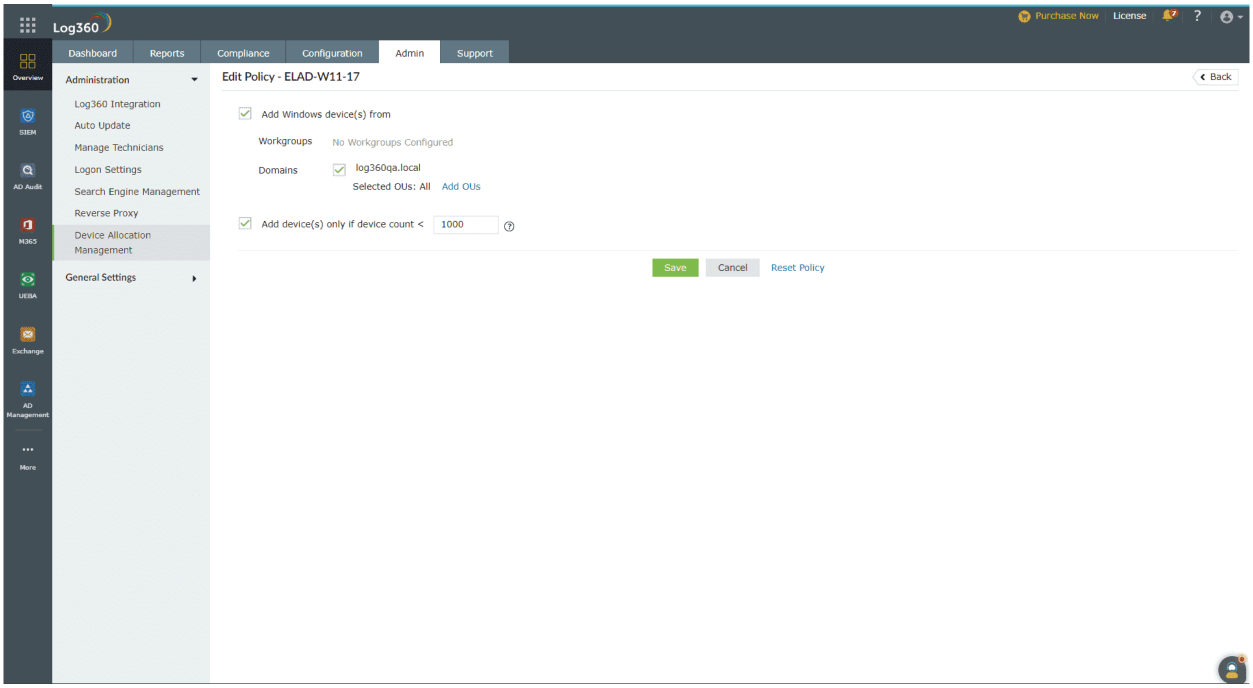


EventLog Analyzer - Auto Allocation Policy

| Edit Policy | Server | Device Type | Workgroups | Domains | Device Count |
|---|---|---|---|---|---|
| ✎ | ELAD-W11-17 | Windows | Not configured | All | 1000 |

**Figure 54 Auto Allocation Policy view**

6) You can customize the policy according to your requirements. (Refer to Figure 55)



Edit Policy - ELAD-W11-17

☑ Add Windows device(s) from

Workgroups No Workgroups Configured

Domains ☑ log360qa.local

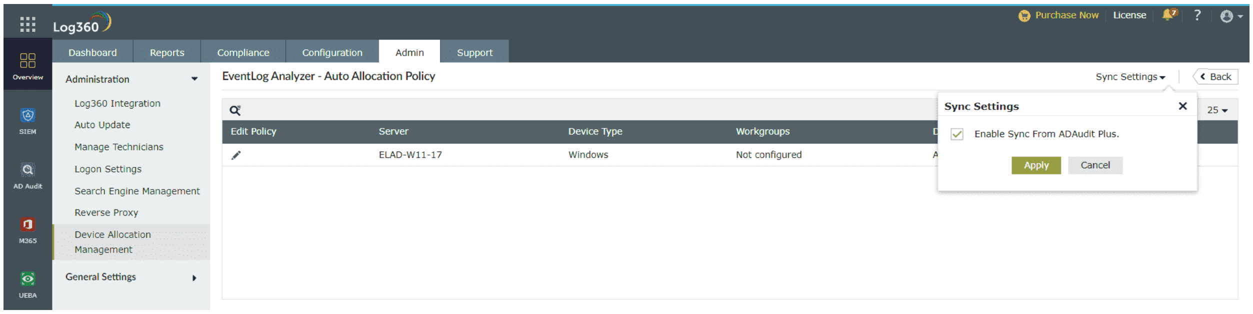
Selected OUs: All Add OUs

☑ Add device(s) only if device count < 1000

**Figure 55 Edit Policy**

7) In the **Edit Policy** window, you can select the Workgroup and the Domain from which the devices must be added.

8) To activate or deactivate inheritance from ADAP. (Refer to Figure 56)



EventLog Analyzer - Auto Allocation Policy

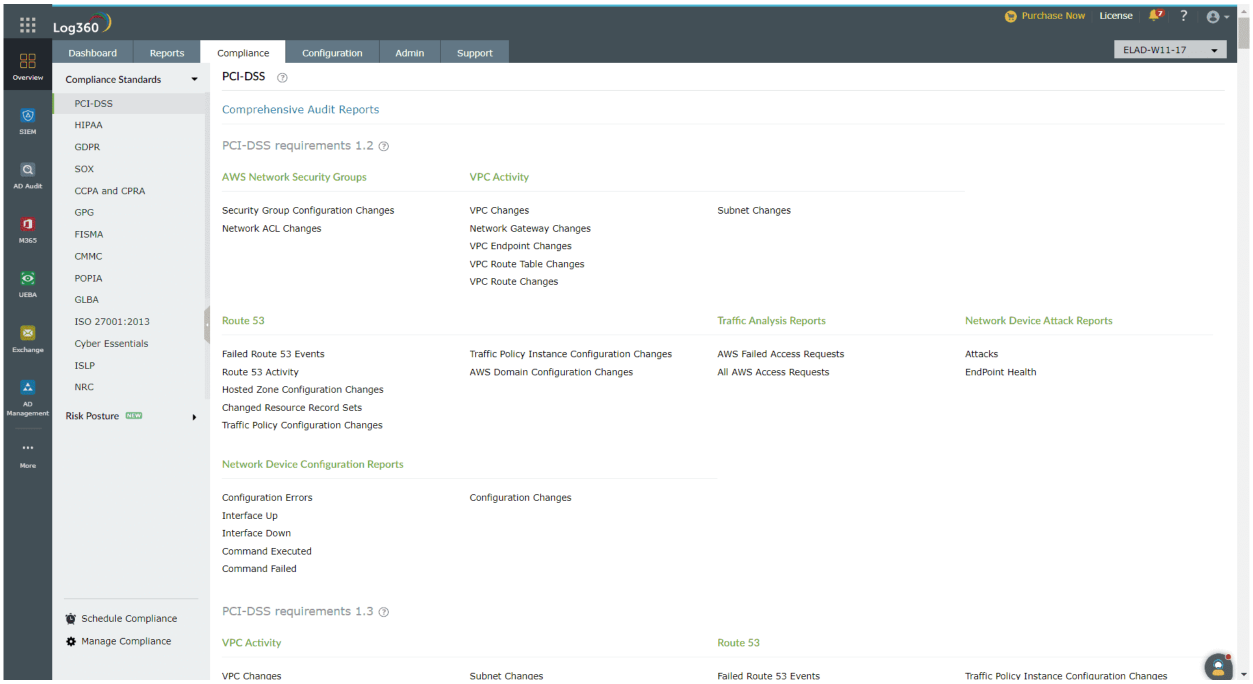
| Edit Policy | Server | Device Type | Workgroups | D |
|---|---|---|---|---|
| ✎ | ELAD-W11-17 | Windows | Not configured | A |

Sync Settings

☑ Enable Sync From ADAudit Plus.

**Figure 56 Sync settings**

9) In the Dashboard, Reports, Compliance, and Configuration tabs, users can choose and view data from the respective managed servers by selecting the managed server at the top right corner. (Refer to Figure 57)



PCI-DSS

Comprehensive Audit Reports

PCI-DSS requirements 1.2

AWS Network Security Groups

Security Group Configuration Changes
Network ACL Changes

VPC Activity

VPC Changes
Network Gateway Changes
VPC Endpoint Changes
VPC Route Table Changes
VPC Route Changes
Subnet Changes

Route 53

Failed Route 53 Events
Route 53 Activity
Hosted Zone Configuration Changes
Changed Resource Record Sets
Traffic Policy Configuration Changes
Traffic Policy Instance Configuration Changes
AWS Domain Configuration Changes

Traffic Analysis Reports

AWS Failed Access Requests
All AWS Access Requests

Network Device Attack Reports

Attacks
EndPoint Health

Network Device Configuration Reports

Configuration Errors
Interface Up
Interface Down
Command Executed
Command Failed
Configuration Changes

PCI-DSS requirements 1.3

VPC Activity

VPC Changes
Subnet Changes

Route 53

Failed Route 53 Events
Traffic Policy Instance Configuration Changes

**Figure 57 Compliance Standards**

# 8. Frequently Asked Questions - EventLog Analyzer Distributed Edition

## 8.1 General

- **Why should you go for the distributed edition of EventLog Analyzer?**
  If your organization has multiple network devices, servers, applications, and databases spread across geographical locations, using the distributed edition of EventLog Analyzer will help you unify all your logs and gain actionable insights from a single console. The distributed edition is also useful for manageSecurity Service Providers (MSSPs).

- **Who should go for EventLog Analyzer - distributed setup (Distributed Edition)?**
  We recommend the distributed setup (Distributed Edition) if

  1. You are a large enterprise across different geographical locations with hundreds of log sources like Windows devices, Linux/Unix servers, network devices including routers, switches, firewalls, IDS/IPS, or applications such as IIS and Apache web servers, Oracle and Microsoft SQL Server databases, and print servers.

  2. You are a manageSecurity Service Provider (MSSP) with a large customer base spread across geographical locations.

- **What are managed and admin servers?**
  The distributed setup of EventLog Analyzer consists of one admin server and one or more managed servers. The managed servers can be installed at different geographical locations and must be connected to the admin server. The admin server centralizes log management across all the managed servers. You can view and manage all the managed servers from the admin server console.

- **How many managed servers can a single admin server manage?**
  One admin server is designed to manage up to 100 managed servers.

- **Can I convert the existing standalone edition of EventLog Analyzer to the distributed edition?**
  Yes, you can. You need to install a new admin server and convert the existing installation to a managed server. Please refer to the steps given here. Ensure that the build number of your existing EventLog Analyzer installation is 6000 or above.

- **While converting the standard edition to an admin server, I'm prompted to specify the proxy server details. Why should I configure it?**
  Configuring the proxy server is optional. You need to configure the proxy server details during admin server conversion, for the admin server needs to pass through a proxy server to contact the managed servers.

- **I have deleted a managed server from the admin server. How do I add it again?**

  To add a managed server under the admin server again, follow the steps given below-

  1. Register the managed server with the admin server by executing the registerWithAdminServer.bat/sh file located in <EventLog Analyzer Home>/troubleshooting.

  2. Restart the managed server.

- **Difference between Free Edition and (Premium and Distributed) Edition?**

  The Free Edition of EventLog Analyzer is limited to handling event logs from a maximum of five log sources, whereas the Paid Editions (Premium and Distributed) can handle event logs from an unlimited number of log sources. The features and functionality are the same for both free and paid editions.

  The logs collected by the managed server are stored only in the managed server database. You cannot store the logs in the admin server. However, you can forward the logs to the admin server by archiving them.

- **Does high availability support in EventLog Analyzer Distributed?**

  Yes, high availability support in EventLog Analyzer Distributed. you can refer details here

- **Can we alter the managed server data from admin server UI?**

No, it is not possible an admin server that provides the administrator with viewing /monitoring in a single place over the entire network.

- **How do I find out my current build number?**
  - Open the 'Eventlog Analyzer' web client.
  - Click on the question mark '?' on the right side of the top pane
  - Select the 'About' option.
  - A pop-up window appears containing details of your EventLog Analyzer version. You can find the build number from this window

- **As EventLog Analyzer can be accessed using a web-browser, does that mean I can access it from anywhere?**
  Yes, you can. Ensure that the existing EventLog Analyzer installation is Version 6.0 or later. Download the EXE/BIN of the latest EventLog Analyzer version on another server and convert it to the admin server. Then the existing server with the Premium Edition license of EventLog Analyzer can be converted to a managed server.

## 8.2 Secured Communication Mode (HTTPS)

- **Working of HTTPS?**

The HTTPS protocol provides several features that enable secure transmission of web traffic. These features include data encryption, server authentication, and message integrity. You can enable secure communication between the web clients and the EventLog Analyzer server using HTTPS. for more details given here.

- **What is the mode of communication between the admin server and the managed server?**
  By default, the managed and admin servers communicate using HTTP. There is also an option to convert the mode of communication to HTTPS. To modify the mode of communication, you can refer to the steps given here.

- **I have changed the managed server communication mode to HTTPS after installation. How to update this change in the admin server?**
  In the Admin Server, click on the Settings tab > Configurations > Managed Server Settings > Edit icon of specific managed server. Select the required protocol to configure the web server port details.

## 8.3 Licensing

- **What are the licensing terms for EventLog Analyzer's distributed edition?**
  EventLog Analyzer's Distributed Edition license will be applied to the admin server. The number of devices and applications for which the license has been purchased can be utilized among the registered managed servers. You can keep adding devices and applications to various managed servers till the total number of licenses purchased gets exhausted. You can view the number of devices and applications managed by each managed server in the Managed Server Settings page.

If the number of devices and applications managed by all the managed servers exceeds the number of licenses purchased, a warning message appears in the admin server. To resolve this warning, you can

1. Purchase the license to manage the additional devices and applications.
2. Check the number of devices and applications managed by each managed server in the Managed Server Settings page of the admin server.
3. Go to the individual managed server and manually manage the devices. Ensure that the number of devices and applications is equal to the number of licenses.

- **Is there an option to apply the license to the managed servers?**
  There is no option to apply the license to the managed servers. The license must be applied to the admin server, and it will be automatically propagated to all the managed servers.

- **Why do I encounter the "License Restricted" alert even after reconfiguring the managed servers?**
  The status of devices in the managed server synchronizes with the admin server during the data collection cycle, which happens at an interval of 5 minutes. Try to add other devices and applications to the managed server after a few minutes.

# 9. Troubleshooting

## 9.1 Sync

1. Check 9.2 Registration/Connection.
2. Update the credential in the Admin Server "Manages Server Settings" page.

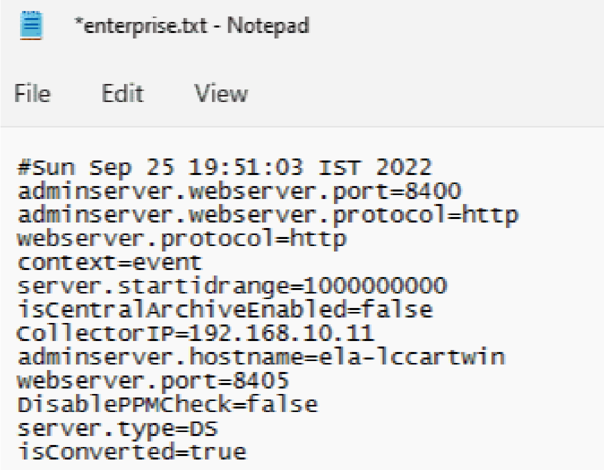
## 9.2 Registration/Connection

1) **Reachability**: Check whether both the admin server and managed server are up and open bidirectionally.

2) **Connectivity**: Check whether the admin server console can be accessed in the managed server machine and the managed server console in the admin server machine.

3) **Build** : Check whether the admin server build and all managed server build are the same.

4) **Enterprise.txt** : Check whether Enterprise.txt values are correctly present in managed server. (Refer to Figure 58)



```
#Sun Sep 25 19:51:03 IST 2022
adminserver.webserver.port=8400
adminserver.webserver.protocol=http
webserver.protocol=http
context=event
server.startidrange=1000000000
isCentralArchiveEnabled=false
CollectorIP=192.168.10.11
adminserver.hostname=ela-lccartwin
webserver.port=8405
DisablePPMCheck=false
server.type=DS
isConverted=true
```

**Figure 58 Enterprise.txt**

**adminserver.webserver.port** = admin server running port.

**adminserver.webserver.protocol** = admin server running protocol.

**webserver.protocol** = managed server running port.

**server.startidrange** = managed server using startid.

**isCentralArchiveEnabled** = set true if Customer using Centralized Archives.

**CollectorIP** = managed server IP address/ hostname

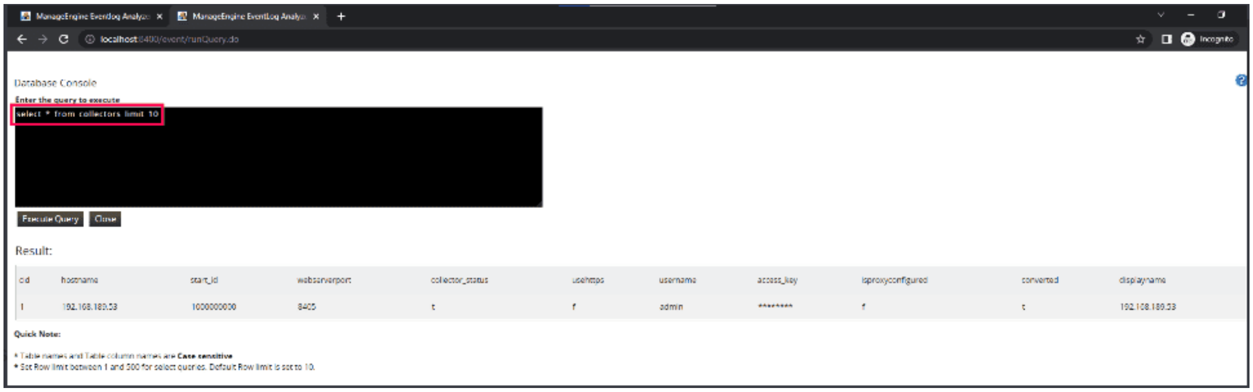
**adminserver**.**hostname** = admin server name.

**webserver.port** = managed server running port.

**DisablePPMCheck** = Set false to auto upgrade managed server when Admin Server is upgraded, else set true for Manual upgrade.

### i) Case 1

Query to find the managed server details - hostname, startid, port, protocol, SSL enabled status in Admin Server : Select * from Collectors (Refer to Figure 59)



ManageEngine EventLog Analyz
ManageEngine EventLog Analyz
localhost:8400/event/runQuery.do
Incognito

Database Console

Enter the query to execute

```
select * from collectors limit 10
```

Result:

| cid | hostname | start_id | webserverport | collector_status | usehttps | username | access_key | isproxyconfigured | converted | displayname |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 192.168.189.53 | 1000000000 | 8405 | t | f | admin | ******** | f | t | 192.168.189.53 |

Quick Note:

- Table names and Table column names are **Case sensitive**
- Set Row limit between 1 and 500 for select queries. Default Row limit is set to 10.

**Figure 59 DisablePPMCheck**

The **CollectorIP** value in the managed server enterprise file and the hostname column in the admin server collectors table need to be the same.

If not same, edit correct details in managed server enterprice.txt and restart the managed server or update in Admin Server **Manage Server Settings** page.

### ii) Case 2

**<u>Change in IP and hostname on managed server</u>**

If any changes in port and protocol alter that changes in Enterprise.txt file in EventLog Analyzer managed server and restart the EventLog Analyzer managed server and change managed server details in "Edit user logon details" in admin server.

**<u>Change in IP and hostname in admin server</u>**

If any changes in port and protocol alter that changes in Enterprise.txt file of all EventLog Analyzer managed server and restart the all EventLog Analyzer managed server.

## 9.3 Centralized Archiving

**Reachability**: Check whether both the Admin Server and managed server are Up and both SSH ports are open bidirectionally.

## 9.4 Grey out tab

**Admin Server grayed out due to the license count exceeded**

1. If the License count is exceeded, then the tabs will be grayed out in the admin server.

a. Disable some devices in the managed server and restart the admin server and managed server.

**Admin server grayed out due to build mismatch**

1. When the admin server and managed server build varies, then the tabs will be grayed out in the admin server.

a. Upgrade the admin server and managed server to the same build.

**Admin server grayed out due to HTTP 500 error code series.**

1. tomcat web Server Unavailable /Internal Server error 503.

Restart the machine or upgrade the product to the latest\

## 9.5 Migration Managed Server to another machine

1. Follow the standalone steps - link
2. When successfully copied, finalize the IP and port for this Managed Server
3. Open enterprise.txt in Managed Server and update/add the entry:
4. CollectorIP=<hostName/IP> and also update the webserver.port entry to match with the new one
5. Also open the Admin Server UI collector Settings page and edit the Managed Server that is being moved and update the IP, Port and all the other details that is changed now.
6. Restart the Admin Server.
7. Now, start the Managed Server.

## 9.6 Migration Admin Server to another machine

1. Follow the standalone steps - link
2. When successfully copied, finalize the IP and port for this Admin Server
3. Changes in Enterprise.txt file of all EventLog Analyzer managed server adminserver.hostname and adminserver.webserver.port entry to match with an new one
4. Restart all EventLog Analyzer managed server.
5. Run RegisterWithAdminServer.bat in managed server located on <ELA_HOME>/troubleshooting folder the commend prompt as administrator privilege it need to be success.

**If Centralized Archiving is enabled**

In Admin Server, change the Admin Server Hostname/IP in SSH Server Settings located on **Settings → Admin Settings → Archives → Settings**

## 9.7 Integration with log360

If you integrate the admin server with log360, change the IP or hast name and protocol & port in **Admin → Log360 Integration → EventLog Analyzer** Integration.

1. The server is down. Make sure the component's server is up and running.

This error occurs when the component you are trying to integrate is not running. Make sure that you have installed the component that you are trying to integrate with Log360 and that the component is running. If not go to **Start** → **All Programs** → **Click XYZ** → **Click Start XYZ**. Here XYZ is the component's name.

2. Incompatible component. Please check whether the component's version is compatible with Log360.

This error occurs when the version of a component that you are trying to integrate is lower/higher than the version supported by the version of your Log360. Update the component or Log360 to the latest version.

3. Super Admin credential is required for components installed on a remote host.

When you try to integrate a component that has been installed on a remote host, you will need the credentials of the super administrator of the installed component. Please enter the credentials of the super admin to proceed with the integration.

4. Incorrect Server Details

The server details that you have entered either belongs to a different component or are invalid. Ensure that the values you have entered belong to the selected component and try again.

5. Please try after updating the component settings in Log360.

To rectify this issue, follow the steps listed below:

- Navigate to **Admin -→ Administration -→ Log360 Integration** . You will be presented with two tabs, each representing a component of Log360.
- Click on the component that has to be fixed.
- Enter the server Name or IP address and port number of the server on which that particular component is running in their respective text boxes.

- Select the connection protocol from the drop down menu.
- Click **Update Settings**.

6. Communication Failure

Ensure that the product has a valid SSL certificate and that SSL 3.0 is disabled. If the problem persists, contact log360-support@manageengine.com

7. Communication failure. Please verify the port and protocol.

To rectify this issue:

- Make sure the component you are trying to integrate is up and running.
- Make sure the firewall is not blocking the port number.
- Make sure the protocol you've selected is correct for that particular component.

If the problem persists, contact log360-support@manageengine.com

8. Invalid Component Details

This error occurs when you have two or more instances of the same component installed in your environment, and you try to integrate the second component with Log360.

To integrate the second component, follow the steps listed below:

- Navigate to **Admin -→ Administration -→ Log360 Integration** .
- Select the component that you wish to integrate with Log360.
- To add the new component, remove the existing component from Log360 by clicking on **Remove** and then clicking **OK**.

- Now, enter the server Name and port number of the component to be added and click **Integrate Now**.

  The component will now be integrated with Log360.

9. Invalid Server URL

Check the server URL that you have entered.

- Enter the server Name or IP address and port number of the server from which that particular component is running in their respective text boxes.
- Select the connection protocol from the drop down menu.
- Click **Integrate Now**.

**EventLog Analyzer Distributed edition Download-** Here is the link to download the EventLog Analyzer Distributed edition.