ManageEngine
Log360

User Guide

CONTENTS

1. Welcome to Log360

Log360, a comprehensive SIEM tool, helps you resolve numerous IT security challenges including log management, Active Directory auditing, public cloud log management, meeting compliance requirements, protecting confidential data from security breaches, and much more through a simple and easy-to-use interface.

This integrated solution has the following components:

- ADAudit Plus for Active Directory auditing
- EventLog Analyzer for log management
- M365 Manager Plus for Microsoft 365 management
- Exchange Reporter Plus for Exchange environment reporting
- Log360 UEBA for User Entity and Behavior Analytics
- DataSecurity Plus for Data discovery and File storage analysis
- ADManager Plus for Active Directory management
- Cloud Security Plus for public cloud log management
- PAM360 for privilege access management

ADAudit Plus

ADAudit Plus, the Active Directory auditing component of Log360, helps you to monitor changes in the Active Directory environment. This component collects logs of all the changes happening in the AD infrastructure and processes them to generate reports and trigger alerts.

ADAudit Plus comes with prepackaged reports that help you to track user logon actions, changes to GPOs, OUs, groups, computers, and domain policies. It also provides real-time email or SMS notifications upon the occurrence of any anomalous change activities in your AD environment.

With this component,

- Generate reports based on your own rules - build reports that meet your specific internal requirements.
- Archive audit log data - automatically archive all collected audit log data thus making forensic analysis easier than ever before.
- Real-time alerts and email notifications - get instant alerts on audit events based on configured alert profiles.

And that's not all. Learn more about this component right here.

EventLog Analyzer

EventLog Analyzer centrally collects, normalizes, analyzes, correlates and archives log data from sources across the network. This component can process log data from 700+ sources including applications such as IIS web servers, Apache web servers, Oracle, MS SQL, vulnerability scanners, and more. In fact, this component can process your in-house or custom application logs with its Universal Log Parsing and Indexing (ULPI) technology.

This component provides,

- Both **agent based and agent-less log collection** mechanism.
- **Out-of-the-box reports** that help to gain complete visibility into your security framework.
- **Real-time email or SMS notification feature** that helps to mitigate security attack attempts instantly.
- **Powerful yet easy to use search engine** that helps you to conduct root cause analysis or forensic investigations.

And, this is a non-exhaustive list. Learn more about EventLog Analyzer.

M365 Manager Plus

M365 Manager Plus is a comprehensive Microsoft 365 tool to manage Exchange Online and Azure Active Directory from one place. It provides an exhaustive list of preconfigured reports, audits all user and admin activities, and lets you create custom alerts for critical events in your Microsoft 365 setup to get real-time email alerts.

With this component,

- Know about inactive, locked-out, and never-logged on users to take necessary action quickly.
- Audit non-owner mailbox accesses, admin activities, and mailbox delegations to check for malicious activities.
- Track owner, non-owner, and admin activities on Exchange Online groups, group delegations, emails sent as groups, and more.
- Check for failed logon attempts due to an invalid username or password, which are indicators of brute force attacks.
- Keep track of password, license, and group membership changes made.
- Ensure compliance with industrial mandates like SOX, PCI-DSS. FISMA, HIPAA, and GLBA.

Exchange Reporter Plus

Exchange Reporter Plus is a change auditing solution that allows you to monitor email traffic, audit your Exchange event logs, and receive real-time alerts about critical changes that require your attention.

This Log360 module allows you to:

- Audit non-owner mailbox logons.
- Track mailbox permission changes.
- Monitor Exchange databases that have been mounted or dismounted.
- View admins', owners', and delegates' mailbox activities.
- Get real-time alerts about Exchange Server changes.
- ...and do so much more.

Click here to know more about Exchange Reporter Plus.

User and Entity Behavior Analytics (UEBA)

Log360 UEBA, powered by Machine Learning (ML), detects anomalies by recognizing subtle shifts in user activity. It helps you identify, qualify, and investigate threats that might otherwise go unnoticed, by extracting more information from your logs to give better context.

The capabilities of Log360 UEBA include,

- **Anomalous User and Entity Behavior Analytics:** Spot deviant user and entity behavior such as logons at an unusual hour, excessive logon failures, and file deletions from a host that is not generally used by a particular user.
- **Score-based Risk assessment:** The Log360 UEBA dashboard gives you greater visibility into threats with its score-based risk assessment for users and entities. This approach helps you determine which threats actually merit investigation.
- **Threat Corroboration:** Log360 UEBA identifies indicators of compromise (IoC) and attack (IoA), exposing major threats including insider threats, account compromise, and data exfiltration.

DataSecurity Plus

DataSecurity Plus, is a data visibility and security solution, capable of data discovery, file storage analysis, and Windows file server auditing.

The capabilities of Data Security Plus include,

- **Data discovery:** Find, analyze, and track sensitive personal data also known as personally identifiable information (PII) stored in files, folders, or shares.
- **File server auditing:** Audit and monitor, report and alert on all file accesses and modifications made in your file server environment in real time.
- **Storage analysis:** Analyze and identify redundant, outdated, and trivial data to declutter your file servers and cut storage costs.

ADManager Plus

The ADManager Plus component of Log360 provides over 200 out-of-the-box reports on Active Directory users,computers, groups, OUs, Group Policy Objects, file server permissions, and more to help you visualize key security configurations in Active Directory.

Below are the salient capabilities of the ADManager Plus component:

- Generates critical reports such as recently created, deleted, and modified Active Directory objects.
- Helps you spot security loopholes such as groups without members.
- Provides crucial security details during a security investigation such as unused user accounts, NTFS permissions, and more in just a few clicks.
- Generates audit reports to help you meet regulatory mandates.

Cloud Security Plus

Cloud Security Plus is a public cloud log management tool for Amazon Web Services and Microsoft Azure. With comprehensive reports, easy search mechanism, and customizable alert profiles, it enables you to track, analyze, and react to events happening in your cloud infrastructure. Thus facilitating the smooth functioning of your business in a secure and protected cloud.

This Log360 component offers:

- **Detailed reports for the AWS cloud environment.**

  A number of predefined reports on events that occur in Amazon EC2, WAF, RDS, STS, EBS, VPC, ELB, and S3.
- **Activity tracker for the Microsoft Azure cloud.**

  Reports provide insights on user activity and any changes made to network security groups, virtual networks, DNS zones, virtual machines, databases, and storage accounts.
- **An easy search through log data.**

  Find what you're looking for with the smart log search engine and the advanced search options provided.
- **Alerts that keep you in loop.**

  Get notifications via email when unusual activities and other security threats occur.

Click here to know more about Cloud Security Plus.

PAM360

PAM360 is an enterprise-grade, unified privileged access management solution that enables organizations to manage, monitor, and secure privileged access to critical enterprise systems, applications, and assets. It offers granular access controls, AI and ML-based analytics, extensive auditing, and smart automation workflows.

Key capabilities of PAM360:

- Enterprise credential vault
- Just-in-time privilege elevation
- Secure remote access and session recording
- Privileged user behavior analytics
- SSH key management and SSL certificate management
- Application credential security
- Comprehensive reporting, auditing, and compliance reports

2.1. Getting Started

The following topics describe how to get started with Log360:

- System Requirements
- Prerequisites
- Installation
- Deployment Scenarios
- Working with Log360
- Licensing
- Migrating PGSQL to MSSQL

2.2. System Requirements

Product Requirements

Minimum

Product	CPU	RAM	Disk
Log360	2 Core	4 GB	50 GB
EventLog Analyzer	8 Core	12 GB *	400 GB **
ADAudit Plus	4 Core	8 GB	50 GB
M365 Manager Plus	4 Core	8 GB	200 GB
UEBA	2 Core	4 GB	40 GB

Additional Information on Eventlog Analyzer Requirements:

* The RAM requirement varies depending on the log flow rate and the retention settings configured for Elasticsearch (ES).

** The disk space requirement varies based on the log flow rate and the retention settings configured for Elasticsearch (ES) and Archives.

Recommended

Product	CPU	RAM	Disk
Log360	2 Core	4 GB	50 GB
EventLog Analyzer	20 Core	48 GB *	4 TB **
ADAudit Plus	8 Core	16 GB	100 GB
M365 Manager Plus	6 Core	16 GB	500 GB
UEBA	8 Core	8 GB	100 GB

Additional Information on Eventlog Analyzer Recommendation:

* The RAM requirement varies based on the log flow rate and the retention settings configured for Elasticsearch (ES). The specified RAM is designed to handle real-time log processing and search operations for up to 2TB of data. For searches spanning multiple days (>2TB of data), the required RAM can be calculated as: (Index Data Size in GB / 60) + 16 GB.

** The disk space requirement depends on the log flow rate and the retention settings configured for Elasticsearch (ES) and Archives. Disk space is calculated based on a high log flow with a retention period of 1 year for Archives and 32 days for ES.

EventLog Analyzer: https://www.manageengine.com/products/eventlog/system_requirement.html

M365 Manager Plus: https://www.manageengine.com/microsoft-365-management-reporting/system-requirements.html

Active Directory AuditPlus: https://www.manageengine.com/products/active-directory-audit/system-requirements.html

Log360 UEBA: https://www.manageengine.com/log-management/ueba/help/system-requirements.html

General Recommendations

VM infrastructure

- Allocate 100 percent RAM/CPU to the virtual machine running EventLog Analyzer. Sharing memory/CPU with other virtual machines on the same host may result in RAM/CPU starvation and may negatively impact EventLog Analyzer's performance.
- Enabling VM snapshots is not recommended as the host duplicates data in multiple blocks by increasing reads and writes, resulting in increased IO latency and degraded performance.

CPU & RAM

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

DISK

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

Log360

- Log360 components are resource intensive processes. It is recommended to provide each component with a dedicated server for better performance.
- It is recommended to split the load with **Multiple ES Nodes**, with Each node handling 800GB - 1.2 TB of Data.
- Log360 uses Elasticsearch, which is expected to utilize off-heap usage for better performance. Off-heap usage is maintained by OS and will free up when necessary.

Additional ES Node Recommendations:

Hardware	Minimum	Recommended
Base Speed	2.4 Ghz	3 Ghz
Core	12	16
RAM	64	64
Disk Space	1.2 TB	1.5 TB
Disk Type	SSD	SSD

Software Requirements

ManageEngine Log360 supports the following Microsoft Windows operating system versions:

- **Versions requirements for Evaluation**

  Windows 8 & above (or) Windows Server 2012

- **Version requirements for Production**

  Windows Server 2025/ 2022/ 2019/ 2016/ 2012 R2/ 2012

> **Note:** ManageEngine M365 Manager Plus does not support Windows OS versions 2003,2008, XP, and Vista. And it supports Windows OS versions 7 and 2008 R2 only when Service Pack 1 (SP1) is installed.

Supported Browsers

ManageEngine Log360 requires one of the following browsers to be installed on the system to access the Log360 web client.

- Microsoft Edge
- Firefox 4 and above
- Chrome 10 and above
- Safari 5 and above

2.3. Prerequisites applicable for Log360

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

Ports required for Log360

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

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

Ports required for ADAudit Plus

The following ports need to be opened for event collection:

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

The following ports are needed to access ADAudit Plus:

Port Number	Port Usage
8081	HTTP
8444	HTTPS

Ports required for EventLog Analyzer

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

Port Number(s)	Port Usage
8400 (TCP)	Web server port
513, 514 (UDP)	Syslog listener port
514 (TCP)	Syslog listener port
33335 (TCP)	PostgreSQL/MS SQL database port

Agentless log collection:

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

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

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

Agent-based Log collection:

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

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

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

Port Number	Port Usage
8400 (TCP)	TCP port for EventLog Analyzer remote agent-server communication

For IBM AS/400

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

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

Ports required for M365 Manager Plus

The following ports need to be opened for event collection:

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

The following ports are needed to access M365 Manager Plus:

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

Ports required for Exchange Reporter Plus

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

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

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

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

The following ports are needed for Exchange Reporter Plus:

Port Number	Port Usage
8181	HTTPS
3309	ERP product database

Ports required for ADManager Plus

The following ports are required for ADManager Plus:

Port Number	Port Usage
33306	Communication with database
31000	Java wrapper service
22	Secure Shell (SSH)
8080/8443	Web server
2000	Email
389/639	LDAP/LDAPS
80	Exchange server
80,443	G Suite, Microsoft365
3268	LDAP search for Global Catalog (GC)

Ports required for Cloud Security Plus

The following ports are needed to access Cloud Security Plus:

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

Using Log360 with Antivirus Applications

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

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

Ports required for Log360 UEBA

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

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

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

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

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

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

Ports used by PAM360

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

Port Name	Port Number	Direction
PostgreSQL port	3456	Outbound
Web client port	8282	Inbound
SSH port	22	Outbound
Telnet port	23	Outbound
LDAP without SSL port	389	Outbound
LDAP with SSL port	636	Outbound
SMTP port	25	Outbound
MS SQL port	1433	Outbound
Oracle port	1521	Outbound
Sybase ASE port	5000	Outbound
Password Verification port	135, 139, 445	Outbound
Auto Logon Spark View Gateway port	8283	Inbound
RDP	3389	Outbound
SSH API	6622	Inbound
REST API	8282	Inbound
Private CA-OCSP Respoder Server port	8080	Inbound

2.4. Installing Log360

ManageEngine Log360 can be installed on any machine in the domain provided that they meet the recommended system requirements.

You can install Log360 as:

- An Application
- A Windows Service

> **Note:** Ensure that you have necessary privileges and rights to install and run the product.

Install Log360 as an application

By Default Log360 will be installed as an application

1. Click here to download the executable from the website.

2. Double-click on the downloaded file **ManageEngine_LOG360.exe** to start the installation.

3. Follow the install shield wizard to complete the installation of Log360.

You can choose from three install types: Standard, Minimal and Custom.

- **Standard Installation:** Downloads and installs all the components along with Log360. This installation type is highly recommended as it installs Log360 along with all the components necessary for a comprehensive Active Directory and Exchange management.

- **Minimal Installation:** Installs Log360 alone. You can use this installation type if you are already running the components you need.

- **Custom Installation:** Allows you to pick and choose the components to install. You can use this installation type to install only the components you want along with Log360.

The application can be launched on a web browser by double-clicking the Log360 shortcut icon present on the desktop. When opened as an application, Log360 runs with the privileges of the user who has logged on to the computer**.**

Install Log360 as a Windows Service

To run Log360 as a service, you have to install Log360 as a Service. Follow the steps given below:

1. Install Log360 as an application.

2. Go to **Start Menu → All Programs**.

3. Select **Log360** and click on **Install Log360 as Service**.

Once the Log360 Service is installed, you can start the product as a Windows service. When started as a service, Log360 runs with the privileges of the system account. click here.

To Uninstall Log360

To uninstall Log360, select **Start Menu → All Programs → Log360 → Uninstall Log360**.

2.5. Deployment Scenarios

Enable SSL for secure communication over the internet:

You will need to enable SSL for enhanced security and secure communication by Log360 over the internet. To enable SSL on Log360 kindly follow the steps given below:

1. Logon to the Log360 by providing proper admin credentials.

2. Go to **Admin → General Settings → Product Settings**.

3. In the **Connection Type** section, choose the radio button corresponding to **HTTPS** and enter the port number you want to use.

4. Click **Save** to save the changes and restart Log360.

This will enable SSL and a secure communication by Log360 Plus over the internet is possible.

2.6. Working with Log360

This section discusses the following topics:

Starting Log360

To start Log360, double-click the Log360 shortcut icon placed in the desktop. It can also be started from the Start Menu as shown below:

- Go to **Start → All Programs → Log360 → Start Log360**.

This will open Log360 client in your default web browser.

Running Log360 as a service:

If you have installed Log360 as a service, you can start Log360 as a service as shown below:

- Go to **Start → Control Panel → Services → Start ManageEgnine Log360 service.**

Click here to learn how to install Log360 as a service.

Starting the Components

If all the components are installed on the same machine as Log360, then starting Log360 will automatically start the components as well. But if the components are installed on different machines, then you have to manually start the components before starting Log360.

To manually start the components, just double-click the components' shortcut icons placed on the desktop or click **Start → All Programs → <Component> → Start <component>.**

When you enter the user credentials an log in to any one of the component, you will be automatically logged in to the other components as well. There is no need for you to enter the log in details in each and every component.

Accessing Log360 Client

To launch the Log360 client, open a Web browser and type **http://<hostname>:8095** in the address bar. Here the <hostname> refers to the DNS name of the machine where Log360 is running and 8095 is the default port number of Log360. Specify the username and password as admin (for first time login) in the respective fields and click **Login**.

If you have changed the password, you should use the new password to login.

Stopping Log360

- To stop Log360, select **Start Menu → All Programs → Log360 → Stop Log360**.

2.7. Licensing

Log360 can be dowloaded and used for a 30-day trial period, with full access to all the components along with technical support . Once the 30-day trial ends, you have to purchase and apply the license to continue enjoying the full benefits of the product.

The product comes in a single edition viz., **Standard Edition**

After the purchase, you can apply the license file to the product using the **License link** available in the top right corner of the Log360 Web portal.

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

If you buy the auditing component license, you'll have only the ADAudit Plus in the Log360 product. On the other hand, if you purchase the log management component license alone, EventLog Analyzer alone will be available with Log360. If you purchase the license of both the components, you will be able to carry out both auditing and log management functionalities of Log360.

To get a customized price quote for Log360, Click here.

Contact our support team log360-support@manageengine.com for any further queries.

Applying License:

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

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

3. Click on the **Apply** button to apply the license.

2.8. Migrating the built-in database server (PostgreSQL) to Microsoft SQL Server or another instance of a PostgreSQL Server.

Supported database migrations

- PostgreSQL Server to Microsoft SQL Server or another instance of PostgreSQL Server.
- Microsoft SQL Server to PostgreSQL Server or another instance of Microsoft SQL Server.

Supported database versions

- PostgreSQL: 10 to 14
- MS SQL: 2008 and above

To migrate the built-in PostgreSQL to a different database, follow the steps listed below.

- Backup PostgreSQL Data
- Configure MS SQL Server
- Migrate database

Backup PostgreSQL Data

- Stop the Log360 Server/Service.
- Invoke the **<Log360 Home>\bin\app_ctl.bat backupDB** in command prompt to backup the data available in PostgreSQL database. By default, the backup file will be stored under <Log360 Home>\Backup\Log360_Backup<Backup_time> directory.

Configure Microsoft SQL Server

Common Settings to be performed in Microsoft SQL Server

- Open **SQL Server Configuration Manager.**
- Goto **SQL Server Services** and ensure the service **SQL Server Browse** is running.
- Goto SQL Server Network Configuration → Protocols for SQLEXPRESS (the given instance while configuring the MS SQL) → Enable TCP/IP. Then restart the SQL Server (SQLEXPRESS - the given instance) Service.
- Set the following configuration for the SQL Server Configuration Manager:
    - SQL Server Network Configuration → Protocols for <instances> → Enable everything.
    - SQL Native Client Configuration → Client Protocols → Enable all.

Providing credentials to other users in the domain

- Go to **SQL Server Management Studio**.
- Expand the following <MACHINE_NAME>\SQLEXPRESS → Security → Logins.
- Check whether the user provided in the Log360 Service is already in the list.

If not, right click the Logins, New Login and provide a corresponding user name. The New user must have the sysadmin server level role and database level role of db_owner.

Follow the steps to provide the sysadmin role permission: Right click the user, click 'Properties'

Go to 'Server Roles' → Check sysadmin and click 'OK'

> **Note**: Details about user roles: Refer the documents in the following links: For Server Level Roles: http://msdn.microsoft.com/en-us/library/ms188659.aspx For Database Level Roles: http://msdn.microsoft.com/en-us/library/ms189121.aspx

Server Role of the user should be 'sysadmin' and Database Role of the user should be 'db_owner'. The members of sysadmin server role can perform any activity in SQL Server and have completes control over all database functions. The members of db_owner database role can perform any activity in the database.

MS SQL Server in local computer

Copy the following files to <Log360 Home>\bin folder.

- Location of the bcp.exe file: <MSSQL_installed_folder>\Client SDK\ODBC\...\Tools\Binn\bcp.exe. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\...\Tools\Binn\bcp.exe.
- Location of the bcp.rll file: <MSSQL_installed_folder>\Client SDK\ODBC\...\Tools\Binn\Resources\1033\bcp.rll. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\...\Tools\Binn\Resources\1033\bcp.rll

MS SQL Server in remote computer

> **Note**: Please install the corresponding SQL Native Client / Command line Utilities in the Log360 machine as per the MS SQL Server version and CPU type of Log360 machine.

MS SQL Server Version	Native Client
2008	Download
2012	Download
2014	Download
2017	Download
2019	Download

> **Note**: MS SQL server version 2022 is also supported by Log360.

After installing the Command Line utilities, please copy the following files:

Copy the files to <Log360 Home>\bin folder.

- bcp.exe- <MSSQL_installed_folder>\Client SDK\ODBC\130\Tools\Binn\bcp.exe
- bcp.rll- <MSSQL_installed_folder>\Client SDK\ODBC\130\Tools\Binn\Resources\1033\bcp.rll

Windows Firewall Settings

If the Firewall is enabled in MS SQL Server machine, the TCP and UDP Ports need to be opened.
UDP Port is normally **1434**.
To check **TCP Port** settings, open **SQL Configuration Manager**:

- SQL Server Network Configuration → Protocols for <instances>
- Right click TCP/IP → Properties → Goto IP Addresses Tab and scroll until TCP Dynamic Ports and enter the current value in your Firewall.

Steps for Migration

Note: Take a Backup/Snapshot of Log360 before proceeding with the steps (**Important**)

1. Open the Command Prompt and navigate to <Log360 home\bin> (Here, Log360 home is the location where Log360 is installed).

2. Stop Log360 by running **shutdown.bat**.

3. Run the **ChangeDB.bat**.

4. From the **Server Type** menu, select the database server you plan to switch to.

5. If you select **PostgreSQL Server**, then:

   - In the **Host Name** and **Port** field, enter the host name or IP address and the port number of the PostgreSQL database server.

   - Enter the username and password of a user with the necessary permissions to create a new database.

6. If you select **MS SQL Server**, then:

- Move the **bcp.exe** and **bcp.rll files** into the bin folder manually.

- In the **Host Name and Port** field, enter the host name or IP address and the port number of the MS SQL database server.

- In the **Select Server Instance** field, select the SQL Server instance you want to use.

- For Authentication, you can use either Windows credentials or a SQL Server user account.

- If you want to use a SQL Server user account, then select **SQL Authentication** and enter the Username and Password.

- If you want to use Windows authentication, select **Windows Authentication**, and enter the username and password of a Windows domain user account.

- **Note**: The user account used must have permission to create a database in the selected MS SQL Server.

7. Check the box next to **Migrate Existing Data** to copy the data from your old database to the new database.

   IMPORTANT: Leave this box unchecked only if you are changing the database of a fresh installation of Log360.

8. If the MS SQL server you wish to migrate to has **Force encryption** enabled, check the box next to **SSL connection**.

9. Click **Test Connection** and wait for the connection to be established.

10. Once Test Connection has been established successfully, click **Configure DB** to initiate migration.

3. Dashboard View

Important: To view the dashboard of Log360, you have to ensure that the different components of Log360 are setup and that the domain network settings, and cloud accounts of each component are configured appropriately. Here's a checklist of settings to look over to get an unbridled view of the dashboard.

The Log360 dashboard provides a quick snapshot of all the important security events happening in your network, Active Directory infrastructure ,and public cloud accounts.

With the new features offered in the Log360 Dashboard, you can customize the widgets of all the components integrated in Log360.

Customizing Dashboard Views

The dashboard is populated using the data collected from various components.

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

Adding a new tab to the dashboard

To add a new tab in the dashboard:

- In Log360's dashboard, click the ⚙ icon on the top-right corner and select **Add Tab**.
- In the pop-up box that appears, click **Add Custom Tab**. Enter a name for the tab in the given field and click **Add**.
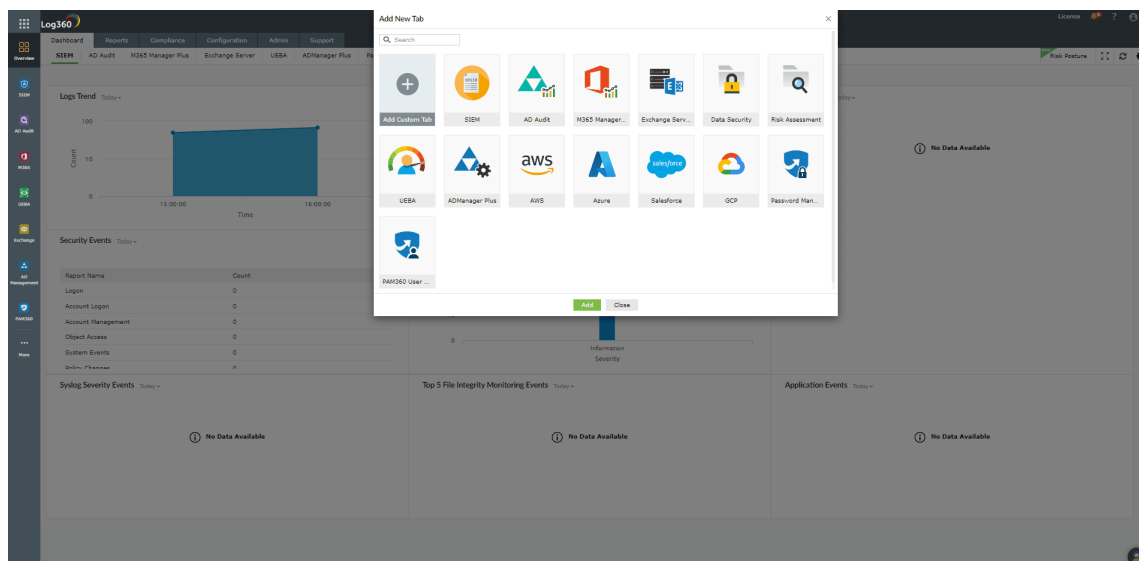
- Navigate to the new tab in your dashboard and click **Add Widget** to start adding widgets of your choice.

Adding a new widget to a tab

To add a new widget,

- In Log360's dashboard, click the ⚙ icon at the top-right corner and click **Add Widget**.
- In the pop-up box that appears, select the component, widget, widget type, chart type, chart color, and enter a display name for the widget. (Please note that widget type, chart type, and chart color options are only applicable for certain widgets.)
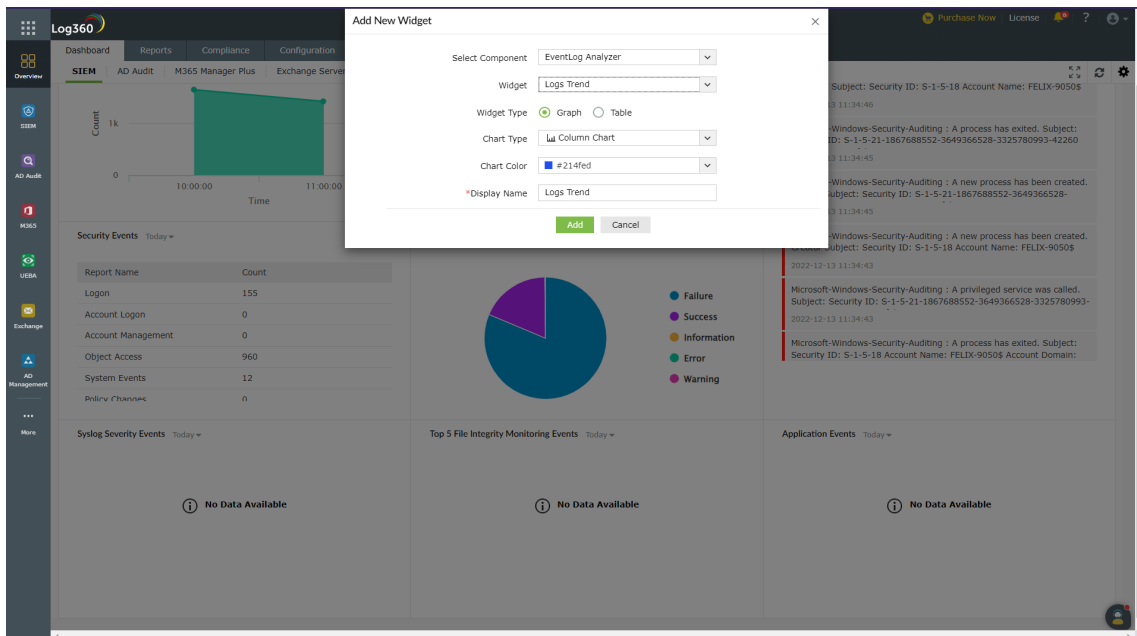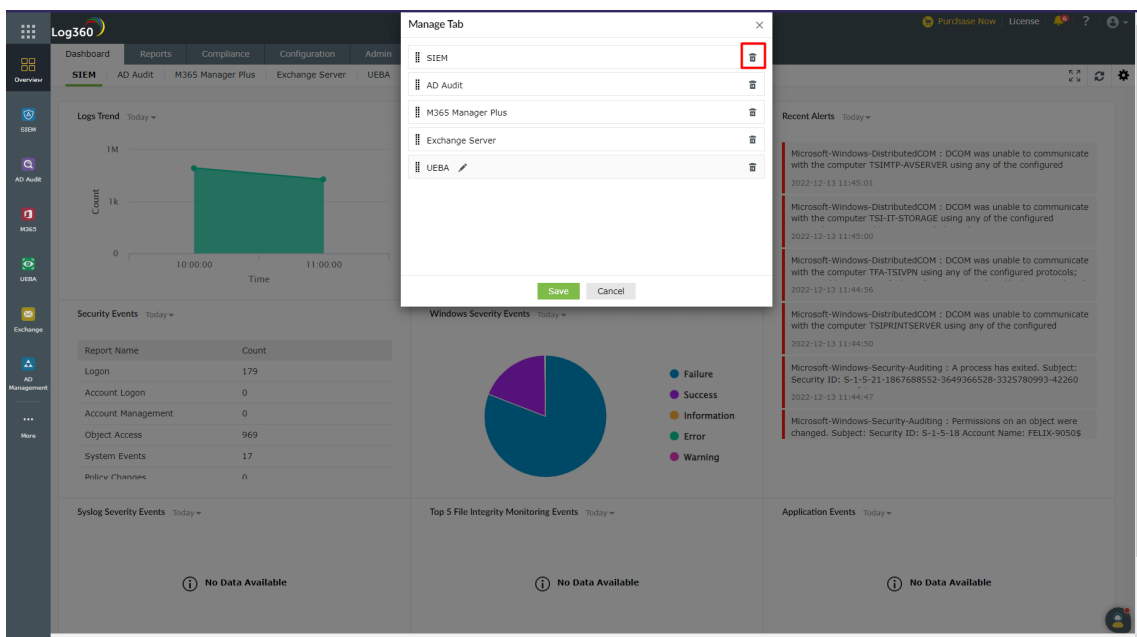
- Once you've entered all the details, click **Add**.

Deleting and reordering tabs in the dashboard

To delete tabs from the dashboard:

- In Log360's dashboard, click the ⚙ icon on the top-right corner and click **Manage Tabs**.
- In the **Manage Tab** dialog box that appears, click the 🗑 icon corresponding to the tab that you want to delete.

- In the pop-up confirmation box, click **Yes** to complete the deletion of the tab.

To edit the order of tabs in the dashboard:

- In Log360's dashboard, click the ⚙ icon on the top-right corner and click **Manage Tabs**.
- In the **Manage Tabs** dialog box that appears, hold the ⣿ icon, and drag and drop the tabs in the order of your choice.

Reordering and resizing widgets

To reorder the widgets in a tab,

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

Editing and deleting widgets

To edit a widget in a tab:

- In Log360's dashboard, click the ⋮ icon corresponding to the widget that you want to edit.
- Select **Edit Widget**. Update the necessary information and click **Update**.
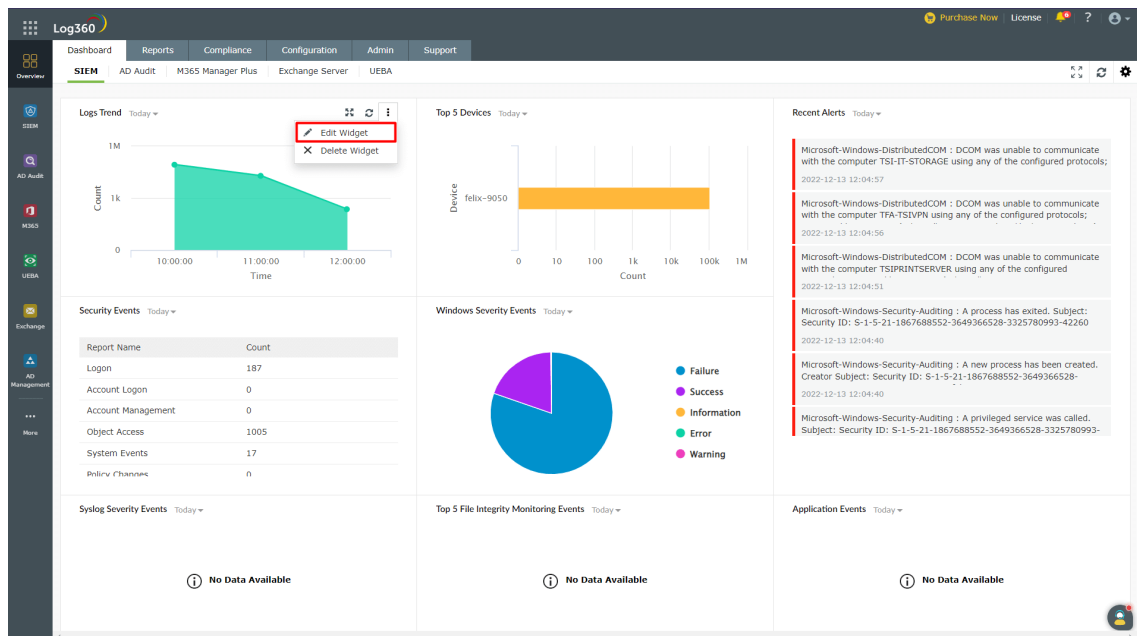
To delete a widget from a tab:

- In Log360's dashboard, click the ⋮ icon corresponding to the widget that you want to delete.

- Select **Delete Widget** and click **Yes** in the pop-up box that appears.
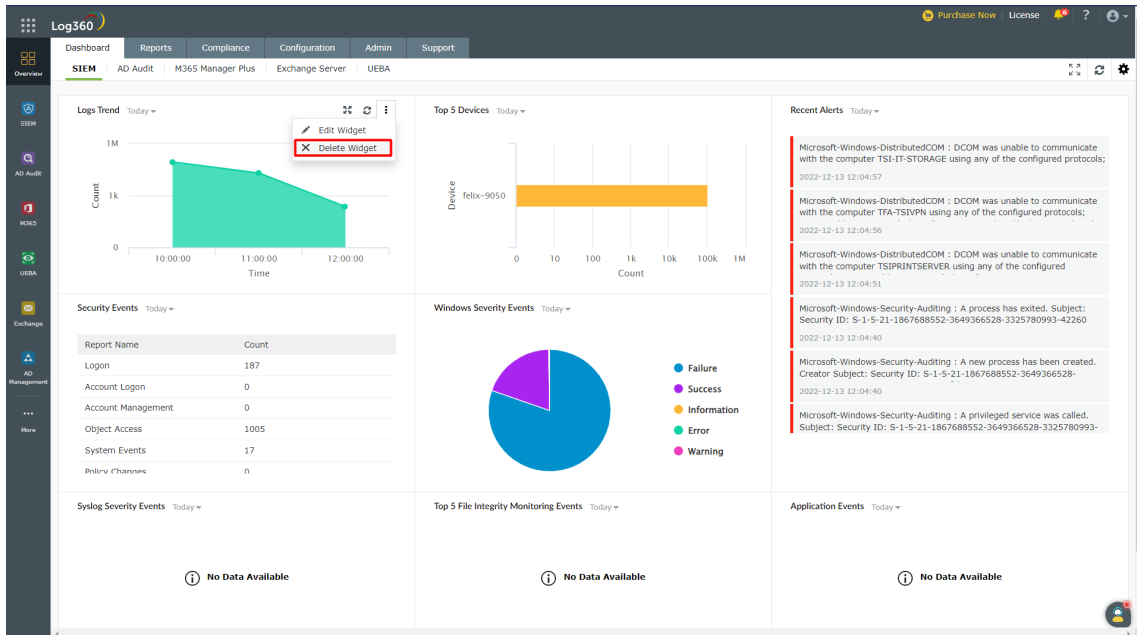
Date selection for widgets

You can select the time period for the data shown in the widgets.

- In the Log360 dashboard screen, click the date dropdown shown at the top-left corner of the screen
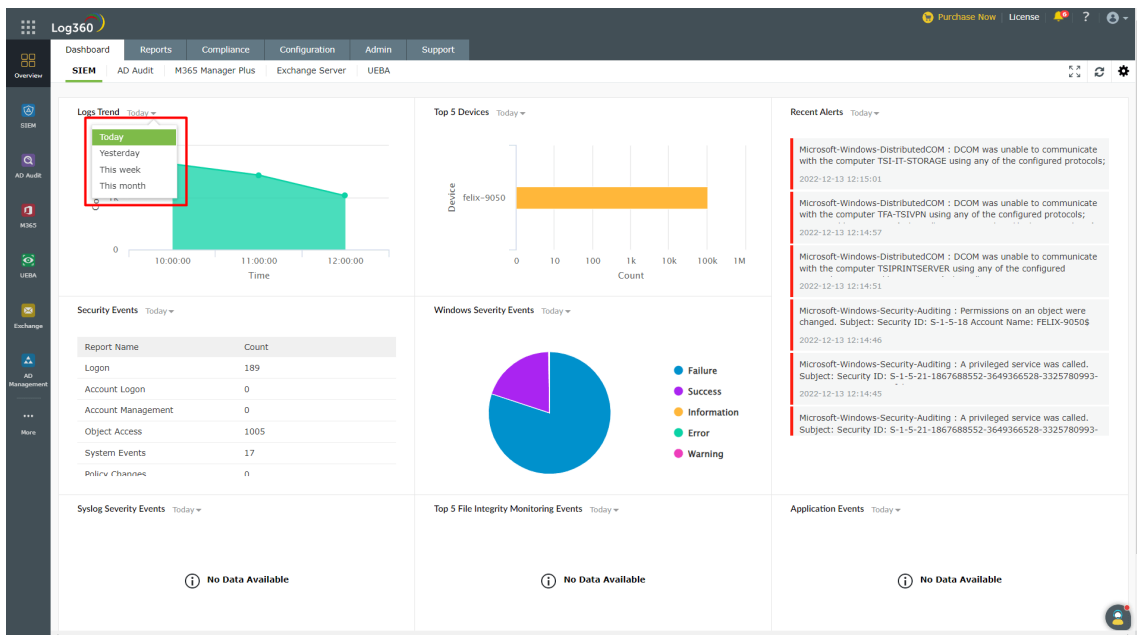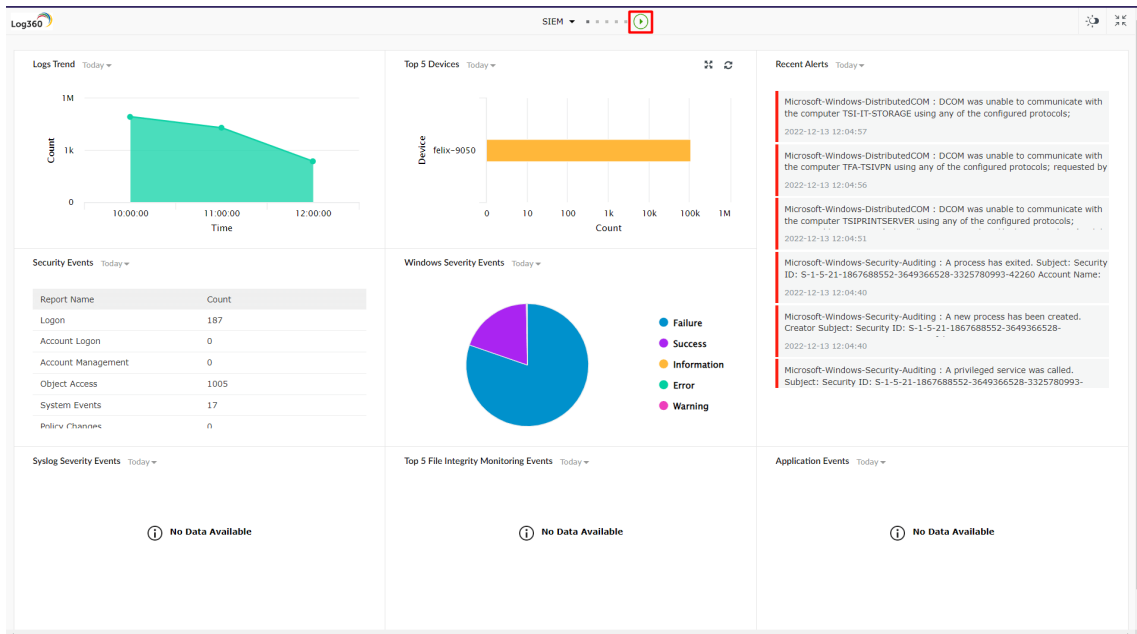

- Select the time period for which you want the data to be displayed.

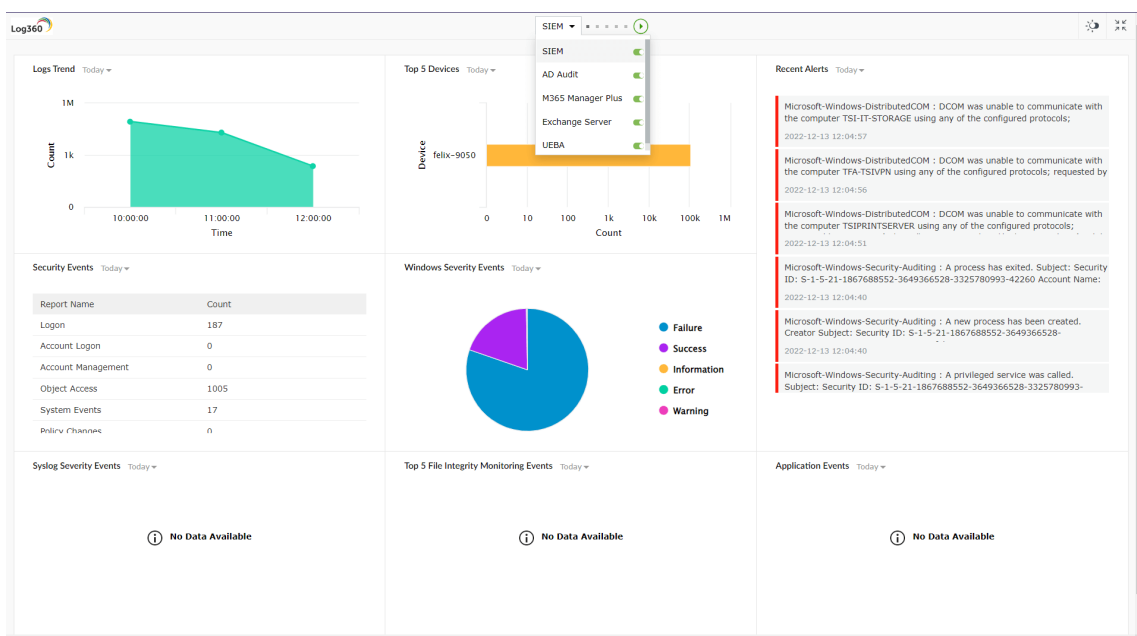## Viewing the dashboard in full screen mode

To view the dashboard in full screen,

- In Log360's dashboard, click the ⛶ icon at the top-right corner.
- In the full screen view, you can view a slideshow of the tabs by clicking the **play** icon located at the top of the screen.
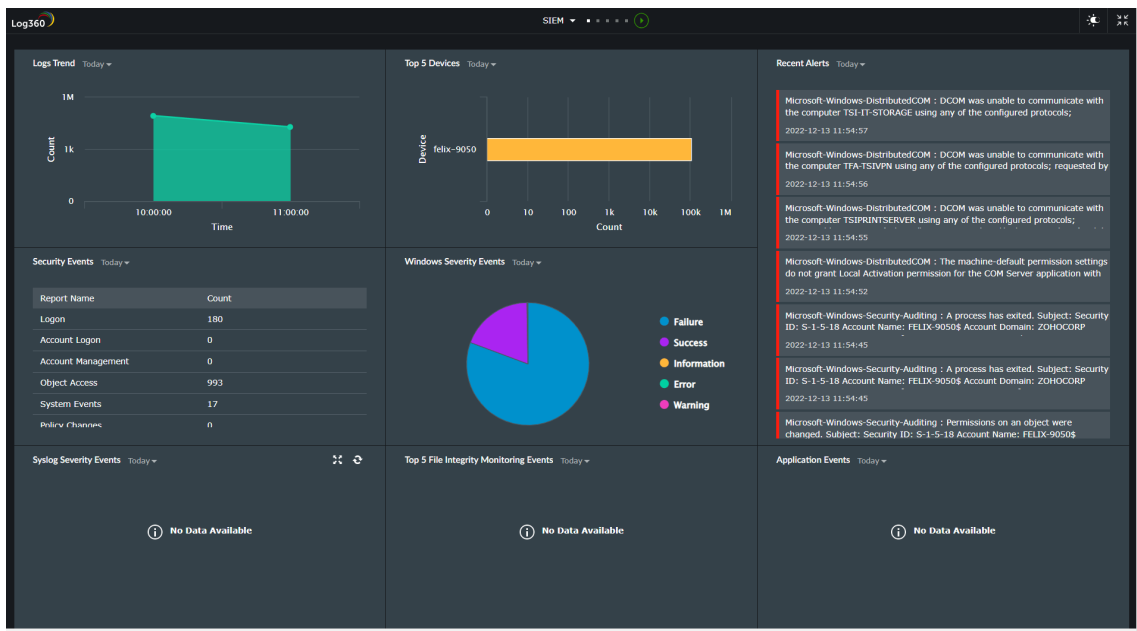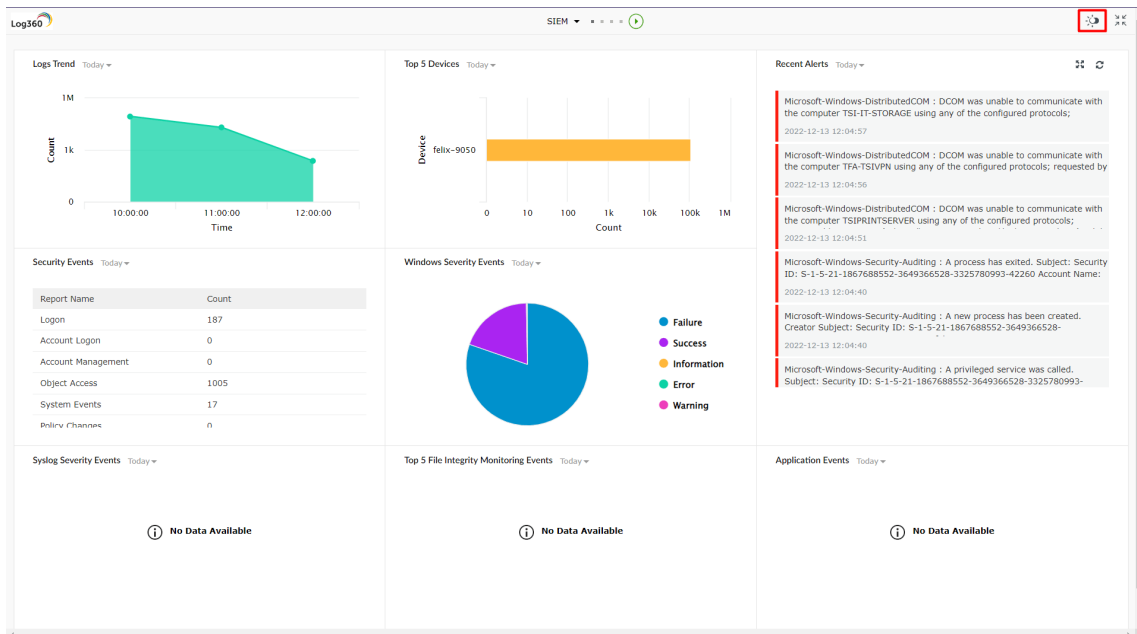
- You can switch to different tabs by clicking on the drop-down button located at the top of the screen.

- You can also remove a particular tab from the slideshow by clicking the toggle button next to the name of the tab in the drop-down list.
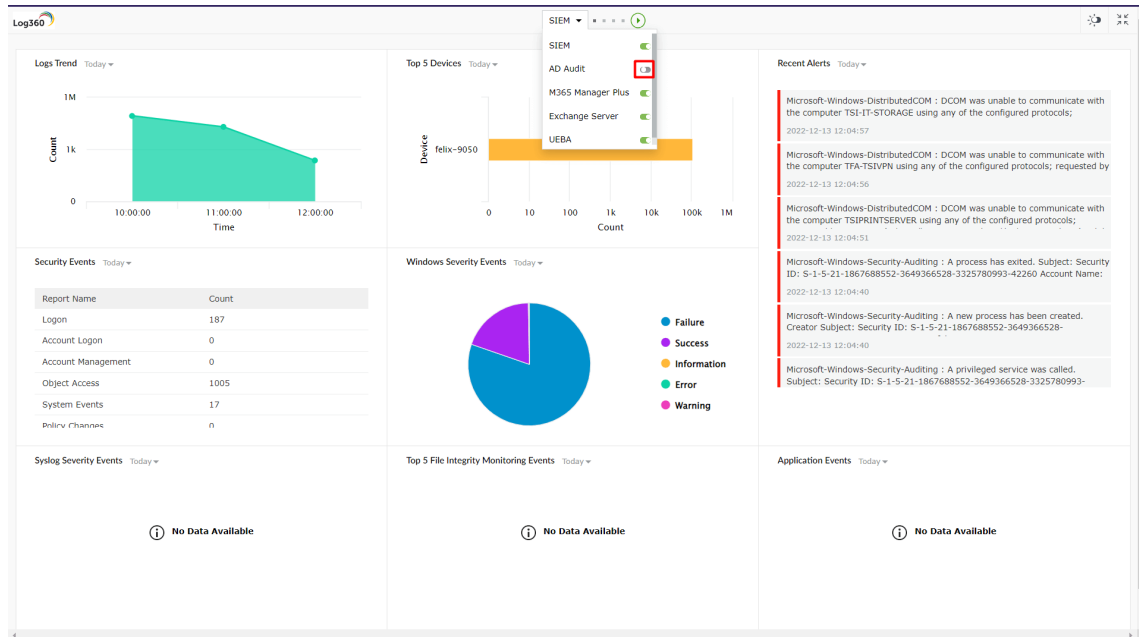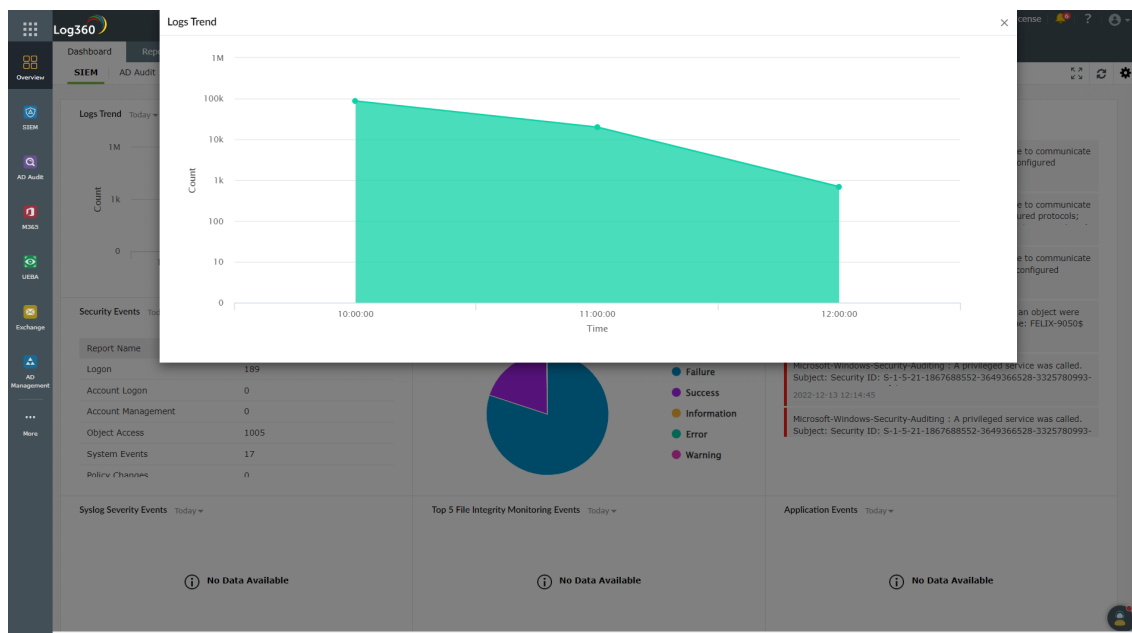
- You can also switch to dark mode by clicking the toggle button at the top-right corner of the screen.

- To go back to the normal viewing mode, click the ⊠ icon.

Viewing a widget in full screen mode

- To view a widget in full screen mode on Log360's dashboard, click the icon at the top-right corner of the widget you want to view.

Refreshing the dashboard and widgets

- To refresh the Log360 dashboard, click the ⟳ icon at the top-right corner of the screen.

- To refresh a particular widget, click the ⟳ icon on the top-right corner of the widget.
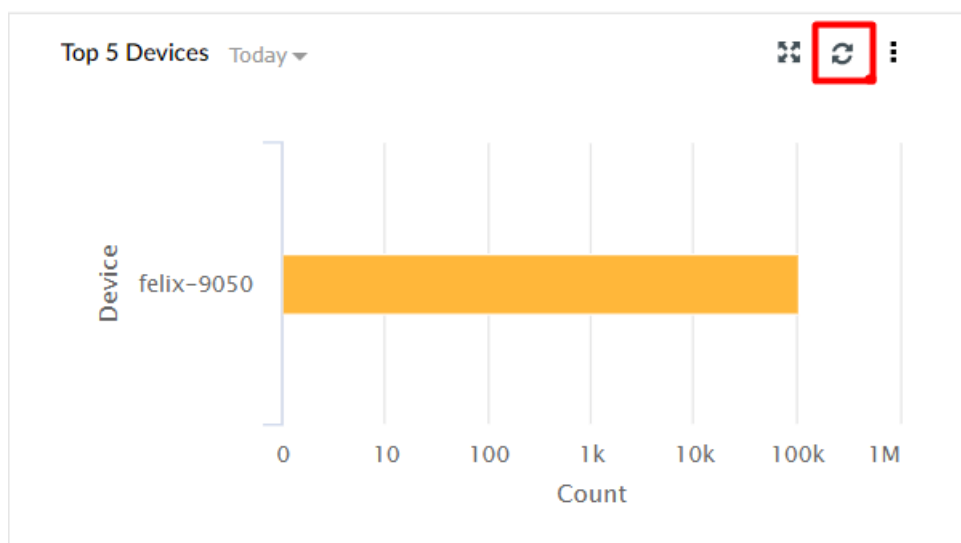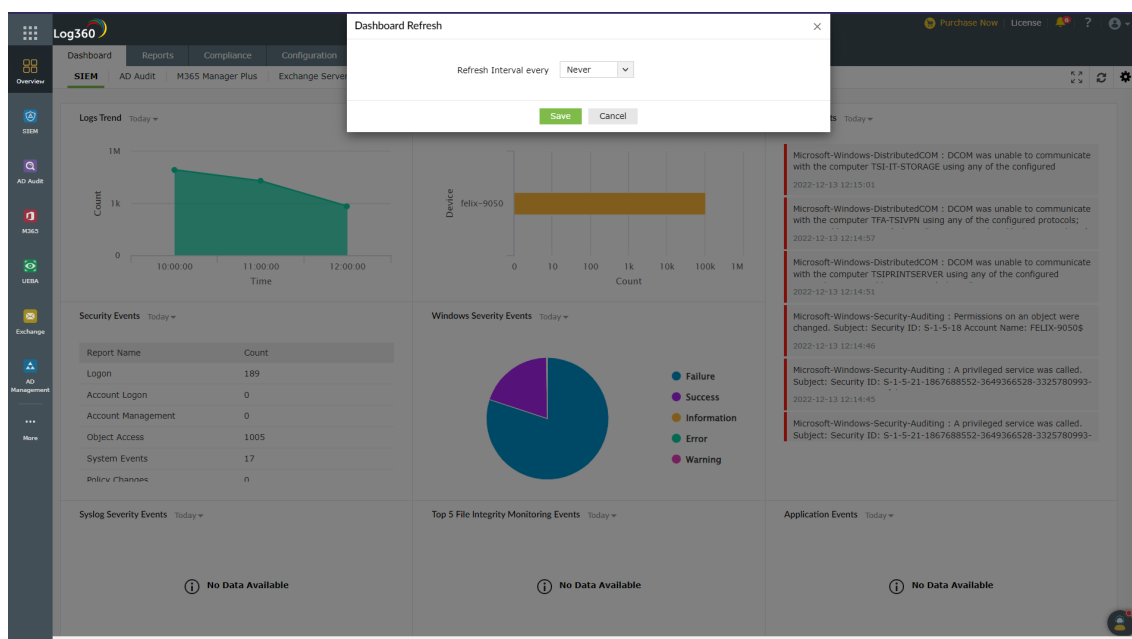

Changing refresh interval

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

- In Log360's dashboard, click the ✿ icon at the top-right corner and click **Refresh Interval**.

- In the pop-up box that appears, select the refresh interval—Never, 30 Secs, 1 Min, 5 Mins, 10 Mins, and 1 Hr.

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

Components that support the latest Log360 Dashboard v2 Feature

Product	Supported Version
AD Audit Plus	7061
Eventlog Analyzer	12231
M365 Manager Plus	4510
Cloud Security Plus	4141
Data Security Plus	6070
AD Manager Plus	7150
UEBA	4037
Exchange Reporter Plus	5703
PAM360	7000

Other Compatibility Issues and Fixes

1. For PPM Users, ADAP Widgets can be added again in the new Log360 Dashboard through **Add Widget** option, but they are not added immediately when the user upgrades through PPM.

2. Due to a breakage in 12250 EventlogAnalyzer, the widget doesn't load properly in EventlogAnalyzer. Kindly

upgrade to the latest version.

3. Due to security enhancements in UEBA, there is a widget loading breakage in 4039 and 4040. Kindly upgrade to the latest version

4. Due to security enhancements in M365, there is a widget customization breakage in 4510. Kindly upgrade to the latest version.

5. Cloud security plus tab in the existing Log360 has been modified and the user should be able to add it from Add tab option.

4. Reports

The **Reports** tab contains all the reports of ADAudit Plus and EventLog Analyzer. This will help you easily view all the AD and network auditing reports without navigating to the individual components.

> **Note:** Make sure you have integrated and enabled both ADAudit Plus and EventLog Analyzer or at least one of them with Log360. Click here to learn how to integrate products with Log360.

Viewing the reports

1. Log in to Log360 as an admin or a technician.

> **Note**: Only users who log in as admins through Log360 authentication can view reports from both the products.

   Only domain users who are assigned with technician roles in ADAudit Plus and EventLog Analyzer can view reports of their respective products.

2. Navigate to the **Reports** tab to view the reports.

Configuring the reports

You can enable or disable certain reports from being displayed under the **Reports** tab. To choose the reports to be displayed, follow the steps below:

1. Navigate to the **Reports** tab.

2. Click on **Configure Reports**.

3. First select the reports to be displayed. You can choose to view reports from either ADAudit Plus or EventLog Analyzer or also both.

4. Now select the categories of reports that you want and the individual reports under each category.

5. Click **Save**.

5.1. Compliance standards and risk posture

The compliance tab in Log360 contains:

- Compliance Reporting
- Risk Posture

5.2. Compliance standards

Regulatory compliance refers to the process of ensuring that an organization follows and adheres to the laws, regulations, guidelines, and industry standards that are relevant to its operations and industry. This includes laws and regulations related to areas such as data privacy, security, financial reporting, environmental practices, occupational health and safety, and many others.

Reports on compliance to regulatory policies are mandated by industry bodies and government authorities to assure minimum security to IT users in various industries. Non-compliance can result in penal action. Compliance reports are thus required to ensure credible security and address mandatory requirements. Log360 generates major compliance reports required for the IT department in various industries, such as healthcare, finance, etc.

- PCI-DSS 4.0
- HIPAA
- GDPR
- SOX
- CCPA and CPRA
- GPG
- FISMA
- CMMC
- POPIA
- GLBA
- ISO 27001:2013
- ISO 27001:2022
- Cyber Essentials
- ISLP
- NRC
- COCO
- NERC
- FERPA
- PDPA
- SAMA
- CJDN
- SOC 2
- QCF
- TISAX
- ECC
- PDPL
- UAE-NESA
- LGPD
- NIST
- NIS 2
- FADP

5.3.1. Risk Posture

A company's overall capacity to identify and respond to risks is referred to as its risk posture. It entails inspecting every aspect of a company's network and identifying potential vulnerabilities. All users, network elements, and any information that may be stored but is at risk of being hacked are included. It also involves examining current security practices and software to assess how well they can fend off attacks.

Log360 supports the below risk posture

- Active Directory
- SQL Server

5.3.2. Active Directory

The main factor that makes Active Directory security, or AD security, uniquely important in a business's overall security posture is that the organization's Active Directory controls all system access. Effective Active Directory management helps protect your business's credentials, applications and confidential data from unauthorized access. It's important to have a strong security system to prevent malicious users from breaching your network and causing damage.

The major predefined rules in risk posture are

Minimum Password Length

Description:

This security rule determines the least number of characters that a password for a user account may contain. You can set a value between 1 to 14 characters, or you can establish that no password is required by setting the number of characters to 0.

Default:

- 7 on domain controllers.
- 0 on stand-alone servers.

Vulnerability:

Minimum password length policy setting determines the least number of characters that can make up a password for a user account. Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Possible Values:

- User-specified number of characters between 0 and 14 (If the number of characters is set to 0, no password is required)
- Not defined

Best Practice:

Set minimum password length to at least a value of 8. In most environments, an eight-character password is recommended because it's long enough to provide adequate security and still short enough for users to remember easily. A minimum password length greater than 14 isn't supported at the moment. This value will help provide adequate defense against a brute force attack. Adding complexity requirements will help reduce the possibility of a dictionary attack. For more info, see Password must meet complexity requirements.

Recommendation:

Using GUI,

- On your Domain Controller Windows homepage, go to Start Menu → Administrative Tools → Group Policy Management.
- In the console tree, expand the Forest and then Domains. Select the domain for which the Account policies have to be set.
- Double-click the domain to reveal the GPOs linked to the domain.
- Right-click Default Domain Policy and select Edit. A Group Policy Editor console will open.

- Now, navigate to Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy.
- Double-click Password Policy. Right-click Minimum password length Policy settings and select Properties to define the policy setting.

Password Complexity

Description:

This security rule determines if passwords meet the complexity requirements. If this policy is enabled, passwords meet the following requirements: Not contain the user's account name or a part of the user's full name that exceeds two consecutive characters.

- Be at least six characters in length
- Contain characters from three of the following categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)

Complexity requirements are enforced when passwords are changed or created.

Default:

Enabled on domain controllers. Disabled on stand-alone servers.

Vulnerability:

Passwords that contain only alphanumeric characters are easy to discover with several publicly available tools.

Possible Values:

- Enabled
- Disabled
- Not defined

Best Practice:

Set "Passwords must meet complexity requirements" to Enabled. This policy setting, combined with a minimum password length of 8, ensures that there are at least 159,238,157,238,528 different possibilities for a single password. This setting makes a brute force attack difficult, but still not impossible.

- Passwords may not contain the user's samAccountName (Account Name) value or entire displayName (Full Name value). Neither of these checks is case-sensitive.
- The password contains characters from three of the following categories:
  - Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
  - Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
  - Base 10 digits (0 through 9)

- Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) Currency symbols such as the Euro or British Pound aren't counted as special characters for this policy setting.
- Any Unicode character that's categorized as an alphabetic character but isn't uppercase or lowercase. This group includes Unicode characters from Asian languages.
- Short passwords that contain only alphanumeric characters are easy to compromise by using publicly available tools. To prevent this vulnerability, passwords should contain other characters and/or meet complexity requirements.

Recommendation:

- **Using GUI,**
    - Go to Start Menu → Administrative Tools → Group Policy Management.
    - In the console tree, expand the Forest and then Domains. Select the domain for which the Account policies have to be set.
    - Double-click the domain to reveal the GPOs linked to the domain.
    - Right-click Default Domain Policy and select Edit. A Group Policy Editor console will open.
    - Now, navigate to Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy.
    - Double-click Password Policy. Right-click password must meet complexity requirements Policy settings and select Properties to define the policy setting and enable the policy setting.

Users with old password

Description:

This security rule checks if all the users have changed their password over the past 90 days.

Default:

Enabled on domain controllers. Disabled on stand-alone servers.

Vulnerability:

The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password.

Best Practice:

Set maximum password age to a value between 30 and 90 days, depending on your environment. This way, an attacker has a limited amount of time to compromise a user's password and have access to your network resources.

Recommendation:

- **Using GUI,**
    - Open the Active Directory Users and Computers tool
    - In the directory tree, select the OU containing the account that you want to reset password.
    - Choose Accounts. Then, select the account you want to reset password. Right-click Name and choose reset password from the context menu.
    - Enter the new password and click ok.
- **Using Power Shell,**
    - Change a specified account password

> Set-ADAccountPassword -Identity <account name> -Reset -NewPassword
> (ConvertTo-SecureString -AsPlainText "<new password>" -Force)

- Set a password for an account using a distinguished name

> Set-ADAccountPassword -Identity 'CN=<Common Name>,OU=<Organizational
> Unit>,DC=<Domain Component>,DC=<Domain Component>' -Reset -NewPassword
> (ConvertTo-SecureString -AsPlainText "<new password>" -Force)

Disable Guest Account

Description:

This security setting determines whether the Guest account is enabled or disabled. This account allows unauthenticated network users to gain access to the system by signing in as a Guest with no password. Unauthorized users can access any resources that are accessible to the Guest account over the network. This privilege means that any network shared folders with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network. This accessibility can lead to the exposure or corruption of data.

Default:

Enabled on domain controllers. Disabled on stand-alone servers.

Vulnerability:

The default Guest account allows unauthenticated network users to sign in as a Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any shared folders with permissions that allow access to the Guest account, the Guests group, or the Everyone group are accessible over the network, which could lead to the exposure or corruption of data.

Possible Values:

- Enabled
- Disabled
- Not defined

Best Practice:

Set Guest account status to Disabled so that the built-in Guest account is no longer usable. All network users will have to authenticate before they can access shared resources on the system. If the Guest account is disabled and Network access: Sharing and security model for local accounts is set to Guest only, network logons—such as those logons performed by the SMB Service—will fail.

Recommendation:

- **Using GUI,**
    - Follow the below steps in GPO.
        - Configure the policy value for Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → "Accounts: Guest account status" to "Disabled"

Disable Inactive Users

Description:

This security rule determines if all the inactive Active Directory users were disabled.

Vulnerability:

Active Directory has an account for every user. Over time, users leave the organization and those user accounts may not get removed from Active Directory. Stale user accounts are a significant security issue, as former employees and external attackers could use those accounts to attack the organization. Stale accounts also use up space in the directory database that could be reclaimed.

Best Practice:

You should carry out regular checks to look for any user accounts that have not changed their passwords the last three months, and then disable and remove those accounts from Active Directory. Users who are inactive for a period of 90 days need to be removed from the organization.

Recommendation:

- **Using GUI,**
    - Open the Active Directory Users and Computers tool.
    - In the directory tree, select the OU containing the account that you want to delete.
    - Choose Accounts. Then, select the account you want to delete. Right-click Name and choose Delete from the context menu.
    - Choose "Yes" in the dialog box, "Are you sure you want to delete this object?". This permanently deletes the selected account.

- **Using Power Shell,**
    - Remove a specified account

    ```
    > Remove-ADUser -Identity <account name>
    ```

    - Remove an account by distinguished name

    ```
    > Remove-ADUser -Identity "CN=<Common Name>,OU=<Organizational Unit>,DC=
        <Domain Component>,DC=<Domain Component>"
    ```

Disable Local Administrative Account

Description:

This security rule determines whether the local administrator account is enabled or disabled.

Default:

Disabled.

Vulnerability:

The built-in administrator account cannot be locked out no matter how many failed logons it accrues, making it a prime target for brute-force attacks that attempt to guess passwords.The account has a well-known Security Identifier (SID), and many non-Microsoft tools allow authentication by using only the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute-force attack by using the SID to log on.

Possible Values:

- Enabled
- Disabled

Best Practice:

It is best practice that the local administrator account is disabled.

Recommendation:

- **Using GUI,**
  - Follow the below steps in GPO.
    - Configure the policy value for Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → "Accounts: Administrator account status" to "Disabled".

Kerberos User Logon Restriction

Description:

This security rule determines if the Kerberos V5 Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the user account. Validation of each request for a session ticket is optional, because the extra step takes time and it may slow network access to services.

Default:

Enabled.

Vulnerability:

If you disable this policy setting, users could receive session tickets for services that they no longer have the right to use because the right was removed after they logged on.

Possible Values:

- Enabled
- Disabled
- Not defined

Best Practice:

If this policy setting is disabled, users might be granted session tickets for services that they do not have the right to use. It is advisable to set Enforce user logon restrictions to Enabled.

Recommendation:

- Follow the below steps in GPO.
  - Configure the policy value for Computer Configuration → Windows Settings → Security Settings → Account Policies → Kerberos Policy → "Enforce user logon restrictions" to "Enabled".

Maximum Lifetime for Kerberos Service Ticket

Description:

This security rule determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service. The setting must be greater than 10 minutes and less than or equal to the setting for maximum lifetime for user ticket.

Default:

600 minutes (10 hours).

Vulnerability:

If you configure the value for the Maximum lifetime for service ticket setting too high, users might be able to access network resources outside their logon hours. In addition, users whose accounts have been disabled might be able to continue accessing network services by using valid service tickets that were issued before their account was disabled.

Possible Values:

- A user-defined number of minutes from 10 through 99,999, or 0 (in which case service tickets don't expire).
- Not defined

Best Practice:

It's advisable to set "Maximum lifetime for service ticket" to 600 minutes.

Recommendation:

- Follow the below steps in GPO.
    - Configure the policy value for Computer Configuration → Windows Settings → Security Settings → Account Policies → Kerberos Policy → "Maximum lifetime for service ticket " to 600 minutes.

Account Lockout Threshold

Description:

This security rule determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

Default: 0.

Vulnerability:

Brute force password attacks can be automated to try thousands or even millions of password combinations for any or all user accounts. Limiting the number of failed sign-ins that can be performed nearly eliminates the effectiveness of such attacks.

Possible Values:

- A user-defined number from 0 through 999
- Not defined

Best Practice:

The threshold that you select is a balance between operational efficiency and security, and it depends on your organization's risk level. To allow for user error and to thwart brute force attacks, Windows security baselines recommend a value of 5 could be an acceptable starting point for your organization.

Recommendation:

- **From GUI**
    - Follow the below steps in GPO.
- Configure the policy value for Computer Configuration → Windows Settings → Security Settings → Account Policies → Account Lockout Policy → "Account lockout threshold" to "5".

Account Lockout Duration

Description:

This security rule checks the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it.

Default:

None, because this policy setting only has meaning when an account lockout threshold is specified.

Vulnerability:

A Denial-of-Service (DoS) condition can be created if an attacker abuses the account lockout threshold policy setting and repeatedly attempts to sign in with a specific account. After you configure the account lockout threshold policy setting, the account will be locked out after the specified number of failed attempts.

Possible Values:

- A user-defined number of minutes from 0 through 99,999 (the Account lockout duration is set to 0, the account will remain locked until an administrator unlocks it manually.)
- Not defined

Best Practice:

It's advisable to set Account lockout duration to approximately 30 minutes.

Recommendation:

- **Using GUI,**
    - Follow the below steps in GPO.
        - Configure the policy value for Computer Configuration → Windows Settings → Security Settings → Account Policies → Account Lockout Policy → "Account lockout duration" to "30" minutes.

Session Timeout Duration

Description:

Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session.

Default:

Not enforced.

Vulnerability:

Long session time out makes un-attended systems a potential end point for attackers. This policy setting helps you

prevent unauthorized access to devices under your control when the currently signed-in user leaves without deliberately locking the desktop.

Possible Values:

- The automatic lock of the device is set in elapsed seconds of inactivity, which can range from zero (0) to 599,940 seconds (166.65 hours).
- If the machine is locked after being set to zero (0) or has no value (blank), the policy setting is disabled and a user sign-in session is never locked after any inactivity.

Best Practice:

Set the time for elapsed user-input inactivity based on the device's usage and location requirements. For example, if the device or device is in a public area, you might want to have the device automatically lock after a short period of inactivity to prevent unauthorized access. However, if the device is used by an individual or group of trusted individuals, such as in a restricted manufacturing area, automatically locking the device might hinder productivity. Setting the machine inactivity timeout seconds to 1000 is recommended.

Recommendation:

- Follow the below steps in GPO.
    - Configure the policy value for Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → "Interactive logon: Machine inactivity limit" to "1000" seconds

User Password Expiry

Description:

This security rule determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the minimum password age must be less than the maximum password age. If the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days.

Default: 42.

Vulnerability:

The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password. Configuring the maximum password age policy setting to 0 so that users are never required to change their passwords allows a compromised password to be used by the malicious user for as long as the valid user is authorized access.

Possible Values:

- User-specified number of days between 0 and 999 (Set 0, so that users are never required to change their passwords)
- Not defined

Best Practice:

Set maximum password age to 90 days, depending on your environment. This way, an attacker has a limited amount of time in which to compromise a user's password and have access to your network resources.

Recommendation:

- **Using GUI,**
  - Follow the below steps in GPO.
    - Configure the policy value for Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy → "Maximum password age" to "90" days.

Admin Accounts with old password

Description:

This security rule checks if any admin accounts are with passwords that were last set more than 90 days.

Vulnerability:

The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the Admin, or by the Admin sharing the password.

Best Practice:

Reset the password once every 90 days. Use the below steps to reset the password.

Recommendation:

- **Using GUI,**
  - Open the Active Directory Users and Computers tool.
  - In the directory tree, select the OU containing the account that you want to reset password for.
  - Choose Accounts. Then, select the account you want to reset password. Right-click Name and choose reset password from the context menu.
  - Enter the new password and click ok.
- **Using Power Shell,**
  - Change a specified account password

    ```
    > Set-ADAccountPassword -Identity <account name> -Reset -NewPassword
      (ConvertTo-SecureString -AsPlainText "<new password>" -Force)
    ```

  - Set a password for an account using a distinguished name

    ```
    > Set-ADAccountPassword -Identity 'CN=<Common Name>,OU=<Organizational
      Unit>,DC=<Domain Component>,DC=<Domain Component>' -Reset -NewPassword
      (ConvertTo-SecureString -AsPlainText "<new password>" -Force)
    ```

Built-in Domain Administrator Account Usage

Description:

This security rule determines if any built-in administrator accounts have been active over the last 14 days.

Vulnerability:

Active Directory has an Administrator account for several needs but it should not be used regularly. If the administrator account is used regularly, it must be monitored. If any malicious activity is found, immediate action must be taken to

prevent attackers from attacking the organization.

Best Practice:

You should carry out regular checks to look for any Administrator accounts that have been active within the last 2 weeks and ensure that the built-in Domain Administrator account is legitimate and accounted for. If not accounted for, a breach is likely to occur and should be investigated. Take action for those administrator accounts, if any malicious activity is found.

Built-in Domain Administrator Account with Old Password

Description:

This security rule determines the period of time (in days) that a password can be used before the system requires the built in administrator user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the minimum password age must be less than the maximum password age. If the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days.

Vulnerability:

The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the Administrator, or by the Administrator sharing the password.

Best Practice:

Reset the password once every 90 days.

Recommendation:

- **Using GUI,**
  - Open the Active Directory Users and Computers tool
  - In the directory tree, select the OU containing the account that you want to reset the password for.
  - Choose Accounts. Then, select the account you want to reset the password for. Right-click Name and choose reset password from the context menu.
  - Enter the new password and click ok.
- **Using Power Shell,**
  - Change a specified account password

    ```
    > Set-ADAccountPassword -Identity <account name> -Reset -NewPassword
      (ConvertTo-SecureString -AsPlainText "<new password>" -Force)
    ```

  - Set a password for an account using a distinguished name

    ```
    > Set-ADAccountPassword -Identity 'CN=<Common Name>,OU=<Organizational
      Unit>,DC=<Domain Component>,DC=<Domain Component>' -Reset -NewPassword
      (ConvertTo-SecureString -AsPlainText "<new password>" -Force)
    ```

Disabled Admin Accounts

Description:

This security setting displays all the admin accounts that are disabled.

Vulnerability:

Admin user accounts which are disabled use up unwanted space in the directory database that could be removed from the database.

Best Practice:

You should carry out regular checks to look for privileged users which are all disabled and remove the disabled privilege users from Active Directory.

Recommendation:

- **Using GUI,**
    - Open the Active Directory Users and Computers tool
    - In the directory tree, select the OU containing the account that you want to delete.
    - Choose Accounts. Then, select the account you want to delete. Right-click Name and choose Delete from the context menu.
    - Choose "Yes" in the dialog box "Are you sure you want to delete this object?". This permanently deletes the selected account.
- **Using Power Shell,**
    - Remove a specified account

        ```
        > Remove-ADUser -Identity <account name>
        ```

    - Remove an account by distinguished name

        ```
        > Remove-ADUser -Identity "CN=<Common Name>,OU=<Organizational Unit>,DC=<Domain Component>,DC=<Domain Component>"
        ```

Inactive Enabled Admin Account

Description:

This security rule checks if all the enabled admin accounts are active over a specified time period.

Vulnerability:

Inactive admin accounts are a significant security issue, as former employees and external attackers could use those accounts to attack the organization. Inactive admin accounts also use up space in the directory database that could be reclaimed.

Best Practice:

You should carry out regular checks to look for any admin accounts that have not active for 90 days and remove those Admin accounts from Active Directory.

Recommendation:

- **Using GUI,**
    - Open the Active Directory Users and Computers tool

- In the directory tree, select the OU containing the account that you want to delete.
- Choose Accounts. Then, select the account you want to delete. Right-click Name and choose Delete from the context menu.
- Choose "Yes" in the dialog box "Are you sure you want to delete this object?" This permanently deletes the selected account.
- **Using Power Shell,**
    - Remove a specified account

    ```
    > Remove-ADUser -Identity <account name>
    ```

    - Remove an account by distinguished name

    ```
    > Remove-ADUser -Identity "CN=<Common Name>,OU=<Organizational Unit>,DC=
        <Domain Component>,DC=<Domain Component>"
    ```

Password Never Expired Users

Description:

This security rule checks if any users are configured with **Password Never Expires** Option.

Vulnerability:

Enabling the "Password Never Expires" option could lead to being compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password.

Possible Values:

- Enabled
- Disabled

Best Practice:

Disable the Password never expires option. It is best practice to uncheck the "Password never expires" check box while creating the user account.

Recommendation:

- **Using GUI,**
    - Open the Active Directory Users and Computers tool
    - In the directory tree, select the OU containing the account that you want to modify.
    - Choose Accounts. Then, select the account you want to modify. Right-click Name and choose properties from the context menu.
    - Open the account tab and under account option uncheck the Password never expires check box
- **Using Power Shell,**

    ```
    > set-aduser <account name> -PasswordNeverExpires $false
    ```

Enforce Password History

Description

This security rule checks if the active directory was configured to prevent password reuse.

Vulnerability:

If password changes are required but password reuse isn't prevented, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users can use the same small number of passwords repeatedly.

Possible Values:

You can specify a number from 0 to 24

Best Practice:

Set Enforce password history to 24. This setting will help mitigate vulnerabilities that are caused by password reuse.

Recommendation:

- Go to Start Menu → Administrative Tools → Group Policy Management.
- In the console tree, expand the Forest and then Domains. Select the domain for which the Account policies have to be set.
- Double-click the domain to reveal the GPOs linked to the domain.
- Right-click Default Domain Policy and select Edit. A Group Policy Editor console will open.
- Now, navigate to Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy.
- Double-click Password Policy. Right-click Enforce Password History Policy settings and select Properties to define the policy setting.

5.3.3. SQL Server

SQL Server is designed to be a secure database platform, however, using the default settings leaves security gaps in the system. SQL Server has many security features you should configure individually to improve security. Data is a critical asset of every organization, and poorly-secured databases are often the reason for security breaches. This article details SQL server security best practices and essential security considerations for protecting your databases from malicious attacks.

> **Note:** EventLog Analyzer needs to be upgraded to build 12323 for this feature to be available.

The major predefined rules in risk posture are

1. Ad Hoc Distributed Queries

Description:

Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0'

Vulnerability:

Enabling Ad Hoc Distributed Queries allows users to query data and execute statements on external data sources. This feature can be used to access remotely and exploit vulnerabilities on remote SQL Server instances and to run unsafe visual basic for application functions.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
> EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'Ad
  Hoc Distributed Queries', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options',
  0; RECONFIGURE;
```

2. CLR Assembly Functions

Description:

Ensure 'CLR Enabled' Server Configuration Option is set to '0'

Vulnerability:

The clr enabled option specifies whether user assemblies can be run by SQL Server. Enabling use of CLR assemblies widens the attack surface of SQL Server and puts it at risk from both inadvertent and malicious assemblies.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This functionality should be disabled if 'clr strict security' option is set to 0. Note that this option is only available since SQL Server 2017. If clr strict security is set to 1 this recommendation is not applicable. By default, clr strict security is enabled and treats SAFE and EXTERNAL_ACCESS assemblies as if they were marked UNSAFE. Though not recommended, the clr strict security option can be disabled for backward compatibility. To check the status of 'clr strict security' option, run the following T-SQL command:

```
> SELECT name, CAST(value as int) as value_configured, CAST(value_in_use as int) as value_in_use
    FROM sys.configurations WHERE name = 'clr strict security';
```

Recommendation:

Run the following T-SQL command:

```
> EXECUTE sp_configure 'clr enabled', 0; RECONFIGURE;
```

3. Cross DB Ownership Chaining

Description:

Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0'

Vulnerability:

This option allows a member of the db_owner role in a database to gain access to objects owned by a login in any other database, causing an unnecessary information disclosure. Cross-database ownership chaining should only be enabled for the specific databases requiring it, instead of enabling it at the instance level for all databases by using the ALTER DATABASESET DB_CHAINING ON command. This database option may not be changed on the master, model, or tempdb system databases.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
> EXECUTE sp_configure 'cross db ownership chaining', 0; RECONFIGURE; GO
```

4.Database Mail XPs

Description:

Ensure 'Database Mail XPs' Server Configuration Option is set to '0'

Vulnerability:

The Database Mail XPs option controls the ability to generate and transmit email messages from SQL Server.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'. Disabling the Database Mail XPs option reduces the SQL Server surface, eliminates a DOS attack vector and channel to exfiltrate data from the database server to a remote host.

Recommendation:

Run the following T-SQL command:

```
> EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure
  'Database Mail XPs', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0;
  RECONFIGURE;
```

5. OLE Automation Procedures

Description:

Ensure 'Ole Automation Procedures' Server Configuration Option is set to '0'

Vulnerability:

The OLE Automation Procedures option controls whether OLE Automation objects can be instantiated within Transact-SQL batches. These are extended stored procedures that allow SQL Server users to execute functions external to SQL Server. Enabling this option will increase the attack surface of SQL Server and allow users to execute functions in the security context of SQL Server.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
> EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'Ole
  Automation Procedures', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options',
  0; RECONFIGURE;
```

6. Remote Access

Description:

Ensure 'Remote Access' Server Configuration Option is set to '0'

Vulnerability:

The 'Remote Access' option controls the execution of local stored procedures on remote servers or remote stored procedures on local server. This functionality can be abused to launch a Denial-of-Service (DoS) attack on remote servers by off-loading query processing to a target.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
> EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure
  'remote access', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0;
  RECONFIGURE;
```

> **Note:** Restart the SQL Server service.

7. Remote Admin Connections

Description:

Ensure 'Remote Admin Connections' Server Configuration Option is set to '0'

Vulnerability:

The remote admin connections option controls whether a client application on a remote computer can use the Dedicated Administrator Connection (DAC).The DAC lets an administrator access a running server to execute diagnostic functions or Transact-SQL statements, or to troubleshoot problems on the server, even when the server is locked or running in an abnormal state and not responding to a SQL Server Database Engine connection.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

In a cluster scenario, the administrator may not actually be logged on to the same node that is currently hosting the SQL Server instance and thus is considered "remote". Therefore, this setting should usually be enabled (1) for SQL Server failover clusters; otherwise, it should be disabled (0).

Recommendation:

Run the following T-SQL command:

```
>   EXECUTE sp_configure 'remote admin connections', 0; RECONFIGURE; GO
```

8. Scan For Startup Procedures

Description:

Ensure 'Scan For Startup Procs' Server Configuration Option is set to '0'

Vulnerability:

The scan for startup procedures option, if enabled, causes SQL Server to scan for and automatically run all stored procedures that are set to execute upon service startup. Setting Scan for Startup Procedures to 0 will prevent certain audit traces and other commonly used monitoring stored procedures from re-starting on start up. Additionally, replication requires this setting to be enabled (1) and will automatically change this setting if needed.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

```
>   EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'scan
    for startup procs', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0;
    RECONFIGURE;
```

> **Note:** Restart the SQL Server service.

9. Trustworthy Database Property

Description:

Ensure 'Trustworthy' Database Property is set to 'Off'

Vulnerability:

The TRUSTWORTHY database option allows database objects to access objects in other databases under certain circumstances. Provides protection from malicious CLR assemblies or extended procedures.

Possible Values:

- Enabled or 'ON'
- Disabled or 'OFF'

Best Practice:

This configuration should be set to '0' except for msdb database which requires this to be 'ON'.

Recommendation:

Run the following T-SQL command for the databases where this property is turned on:

> EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'scan for startup procs', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;

> ALTER DATABASE [<database_name>] SET TRUSTWORTHY OFF;

10. SQL Mail XPs

Description:

Ensure 'SQL Mail XPs' Server Configuration Option is set to '0'

Vulnerability:

SQL Mail provides a mechanism to send, receive, delete, and process e-mail messages using SQL Server in 2008 R2 or Before.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

> EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'SQL Mail XPs', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;

11. Standard Port

Description:

Using default port(1433) makes the server vulnerable to the attacks directed to the default port.

Vulnerability:

Enabling Ad Hoc Distributed Queries allows users to query data and execute statements on external data sources. This feature can be used to access remotely and exploit vulnerabilities on remote SQL Server instances and to run unsafe Visual Basic for Application functions.

Possible Values:

Any port available in the server.

Best Practice:

The port can be anything but the default 1433.

Recommendation:

Using GUI,

- Open SQL Server Configuration Manager
- In the console pane, expand SQL Server Network Configuration, expand Protocols for <InstanceName>, and then double click the TCP/IP protocol.
- In the TCP/IP Properties dialog box, on the IP Addresses tab, several IP addresses appear in the format IP1, IP2, up to IPAll. One of these is for the IP address of the loopback adapter, 127.0.0.1. Additional IP addresses appear for each IP Address on the computer.
- Under IPAll, change the TCP Port field from 1433 to a non-standard port or leave the TCP Port field empty and set the TCP Dynamic Ports value to 0 to enable dynamic port assignment and then click OK.
- In the console pane, click SQL Server Services.
- In the details pane, right-click SQL Server (<InstanceName>) and then click Restart, to stop and restart SQL Server.

> **Note:** The connection settings of any application that uses port number to communicate with SQL server needs to be reconfigured while changing the port of SQL server.

Steps to reconfigure the port number of SQL server in Log360:

- Shutdown the product.
- Open <Log360 Home>\conf\database_params.conf
- Change existing port number to the required port number.
- Restart Log360 for the changes to take effect.

12. Hide Instance

Description:

Ensure 'Hide Instance' option is set to 'Yes' for Production SQL Server instances

Vulnerability:

Non-clustered SQL Server instances within production environments should be designated as hidden to prevent advertisements by the SQL Server Browser service. However, clustered instances may break if this option is selected. If you hide a clustered named instance, the cluster service may not be able to connect to the SQL Server.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '1'.

Recommendation:

Using GUI,

- Open SQL Server Configuration Manager
- Expand SQL Server Network Configuration, right-click Protocols for <InstanceName>, and then select Properties
- On the Flags tab, in the Hide Instance box, if Yes is selected, it is compliant.

Alternatively run the following T-SQL command:

```
> EXEC master.sys.xp_instance_regwrite @rootkey = N'HKEY_LOCAL_MACHINE', @key =
  N'SOFTWARE\Microsoft\Microsoft SQL Server\MSSQLServer\SuperSocketNetLib', @value_name
  = N'HideInstance', @type = N'REG_DWORD', @value = 1;
```

> **Note:**
> - Restart the SQL Server service.
> - Applications that use SQL Browser service to discover SQL Server instance will not be able to discover the instance automatically if 'Hide Instance' is enabled. Either the 'Hide Instance' should be temporarily disabled or port number should be used to connect to SQL Server instance.

13. Disable sa Login

Description:

Ensure the 'sa' Login Account is set to 'Disabled'

Vulnerability:

The sa account is a widely known and often widely used SQL Server account with sysadmin privileges. This is the original login created during installation and always has the principal_id=1 and sid=0x01. Enforcing this control reduces the probability of an attacker executing brute force attacks against a well-known principal.

Possible Values:

- Enabled
- Disabled

Best Practice:

It is not a good security practice to code applications or scripts to use the sa account. However, if this has been done, disabling the sa account will prevent scripts and applications from authenticating to the database server and executing required tasks or functions.

Recommendation:

Run the following T-SQL command:

```
> USE [master] GO DECLARE @tsql nvarchar(max) SET @tsql = 'ALTER LOGIN ' +
  SUSER_NAME(0x01) + ' DISABLE' EXEC (@tsql) GO
```

14. Rename sa Login

Description:

Ensure the 'sa' Login Account has been renamed

Vulnerability:

It is easier to launch password-guessing and brute-force attacks against the sa login if the name is known.

Possible Values:

Any set of characters that are allowed by Microsoft SQL login name restrictions

Best Practice:

The sa Login should be renamed.

Recommendation:

Run the following T-SQL command:

```
> ALTER LOGIN sa WITH NAME = <different_user>;
```

Note: The applications which use sa login to authenticate SQL Server connection need to be reconfigured with different user while altering the sa login.

15. XP CMDSHELL

Description:

Ensure 'xp_cmdshell' Server Configuration Option is set to '0'

Vulnerability:

The xp_cmdshell option controls whether the xp_cmdshell extended stored procedure can be used by an authenticated SQL Server user to execute operating-system command shell commands and return results as rows within the SQL client.The xp_cmdshell procedure is commonly used by attackers to read or write data to/from the underlying Operating System of a database server.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '0'.

Recommendation:

Run the following T-SQL command:

> EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'xp_cmdshell', 0; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;

16. Auto Close

Description:

Ensure 'AUTO_CLOSE' is set to 'OFF' on contained databases

Vulnerability:

AUTO_CLOSE determines if a given database is closed or not after a connection terminates. If enabled, subsequent connections to the given database will require the database to be reopened and relevant procedure caches to be rebuilt.

Possible Values:

- Enabled or 'ON'
- Disabled or 'OFF'

Best Practice:

This configuration should be set to 'OFF'.

Recommendation:

Run the following T-SQL command for databases where this configuration is 'OFF':

> ALTER DATABASE <database_name> SET AUTO_CLOSE OFF;

17. Restrict sa Login

Description:

Ensure no login exists with the name 'sa

Vulnerability:

The sa login (e.g. principal) is a widely known and often widely used SQL Server account. Therefore, there should not be a login called sa even when the original sa login (principal_id = 1) has been renamed.

Possible Values:

Login names can be of any set of characters allowed by Microsoft SQL Login name guidelines.

Best Practice:

No Logins should be named as 'sa'.

Recommendation:

Run the following T-SQL command for logins where name is 'sa':

> USE [master] GO ALTER LOGIN [sa] WITH NAME = <different_name>; GO

> **Note:** The applications which use the altered logins to authenticate SQL Server connection need to be reconfigured another user with equivalent privileges.

18. CLR Strict Security

Description:

Ensure 'clr strict security' Server Configuration Option is set to '1'

Vulnerability:

The clr strict security option specifies whether the engine applies the PERMISSION_SET on the assemblies in SQL Server 2017 and 2019.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '1'.

Recommendation:

Run the following T-SQL command:

```
> EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'clr
  strict security', 1; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0;
  RECONFIGURE;
```

19. Authentication Mode

Description:

Ensure 'Server Authentication' Property is set to 'Windows Authentication Mode'

Vulnerability:

Windows provides a more robust authentication mechanism than SQL Server authentication.

Possible Values:

- SQL Server Authentication
- Windows Authentication
- Mixed Authentication

Best Practice:

This configuration should be set to 'Windows Authentication Mode'.

Recommendation:

Using GUI,

- Open SQL Server Management Studio.

- Open the Object Explorer tab and connect to the target SQL Server instance.

- Right click the instance name and select Properties.

- Select the Security page from the left menu.

- Set the Server authentication setting to Windows Authentication Mode.

Alternatively run the following T-SQL command:

```
> USE [master] GO EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
  N'Software\Microsoft\MSSQLServer\MSSQLServer', N'LoginMode', REG_DWORD, 1 GO
```

Note: Restart the SQL Server service.

20. Guest Connect Permissions

Description:

Ensure CONNECT permissions on the 'guest' user is Revoked within all SQL Server databases excluding the master, msdb and tempdb

Vulnerability:

A login assumes the identity of the guest user when a login has access to SQL Server but does not have access to a database through its own account and the database has a guest user account. Revoking the CONNECT permission for the guest user will ensure that a login is not able to access database information without explicit access to do so.

Possible Values:

The guest users might have or might not have CONNECT permissions.

Best Practice:

CONNECT permission for guest users must be revoked in all databases except for master, msdb and tempdb.

Recommendation:

Run the following T-SQL command for the databases with guest connect permission on:

```
> USE <database_name>; GO REVOKE CONNECT FROM guest CASCADE;
```

21. Orphaned Users

Description:

Ensure 'Orphaned Users' are Dropped From SQL Server Databases

Vulnerability:

A database user for which the corresponding SQL Server login is undefined or is incorrectly defined on a server instance cannot log in to the instance and is referred to as orphaned and should be removed. Orphan users should be removed to avoid potential misuse of those broken users in any way.

Possible Values:

A Database might have or might not have any orphaned users

Best Practice:

No orphaned users must be present in a database server.

Recommendation:

Run the following T-SQL command for all the orphaned users:

```
>  USE <database_name>; GO DROP USER <username>;
```

> **Note:** The orphaned users can be troubleshooted if possible. Refer Microsoft learn for further details.

22. Contained Database Authentication

Description:

Ensure SQL Authentication is not used in contained databases

Vulnerability:

Contained databases do not enforce password complexity rules for SQL Authenticated users. The absence of an enforced password policy may increase the likelihood of a weak credential being established in a contained database.

Possible Values:

- SQL Server Authentication
- Windows Authentication
- Mixed Authentication

Best Practice:

This configuration should be set to 'Windows Authentication Mode'.

Recommendation:

Leverage Windows Authenticated users in contained databases. Refer Microsoft learn for further details.

If required use the following T-SQL command to drop logins:

```
>  USE <db_name> GO DROP USER <user_name>;
```

> **Note:** Applications that use dropped logins to authenticate the SQL server need to be reconfigured with different logins.

23. Public Default Permissions

Description:

Ensure only the default permissions specified by Microsoft are granted to the public server role

Vulnerability:

The 'public' is a special fixed server role containing all logins. Unlike other fixed server roles, permissions can be

changed for the public role. In keeping with the principle of least privileges, the public server role should not be used to grant permissions at the server scope as these would be inherited by all users. Every SQL Server login belongs to the public role and cannot be removed from this role. Therefore, any permissions granted to this role will be available to all logins unless they have been explicitly denied to specific logins or user-defined server roles. When the extraneous permissions are revoked from the public server role, access may be lost unless the permissions are granted to the explicit logins or to user-defined server roles containing the logins which require the access.

Possible Values:

Any number of permissions might be given to public role.

Best Practice:

No extraneous permission must be given to public role and should be removed if given and delegated to user defined role if needed.

Recommendation:

Add the extraneous permissions found in the results to the specific logins to user-defined server roles which require the access.

Run the following T-SQL command for the permissions found:

```
>  USE [master] GO REVOKE <permission_name> FROM public; GO
```

Note: For public role, 'View any database' and 'Connect' are permissible.

24. Builtin Group as Login

Description:

Ensure Windows BUILTIN groups are not SQL Logins

Vulnerability:

The BUILTIN groups (Administrators, Everyone, Authenticated Users, Guests, etc.) generally contain very extensive memberships which would not meet the best practice of ensuring only the necessary users have been granted access to a SQL Server instance. These groups should not be used for any level of access into a SQL Server Database Engine instance.

Possible Values:

Any group may it be BUILTIN or user defined, they can be SQL Logins.

Best Practice:

The Windows BUILTIN groups must be removed from SQL Logins. Note that before dropping the BUILTIN group logins, ensure that alternative AD Groups or Windows logins have been added with equivalent permissions. Otherwise, the SQL Server instance may become totally inaccessible.

Recommendation:

Using GUI,

- Open Computer Management

- Click on Local Users and Groups. If needed, create restrictive AD group containing only the required user accounts.
- Open SQL Server Management Studio → Connect to the database → Select New Login in the Left pane → Add the AD group or individual Windows accounts as a SQL Server login and grant it the permissions required.
- Drop the BUILTIN login using the syntax below after replacing <name>.

> USE [master] GO DROP LOGIN [<name>] GO

25. Local Group as Login

Description:

Ensure Windows Local groups are not SQL Logins

Vulnerability:

Local Windows groups should not be used as logins for SQL Server instances. Allowing local Windows groups as SQL Logins provides a loophole whereby anyone with OS level administrator rights (and no SQL Server rights) could add users to the local Windows groups and give themselves or others access to the SQL Server instance.

Possible Values:

Any windows group can be SQL Login.

Best Practice:

The Windows Local groups must be removed from SQL Logins. Note that before dropping the Local group logins, ensure that alternative AD Groups or Windows logins have been added with equivalent permissions. Otherwise, the SQL Server instance may become totally inaccessible.

Recommendation:

Using GUI,

- Open Computer Management
- Click on Local Users and Groups. If needed, create restrictive AD group containing only the required user accounts.
- Open SQL Server Management Studio → Connect to the database → Select New Login in the Left pane → Add the AD group or individual Windows accounts as a SQL Server login and grant it the permissions required.
- Drop the Local group name logins using the syntax below after replacing <name>.

> USE [master] GO DROP LOGIN [<name>] GO

26. Agent Proxy Access for public role

Description:

Ensure the public role in the msdb database is not granted access to SQL Agent proxies

Vulnerability:

Granting access to SQL Agent proxies for the public role would allow all users to utilize the proxy which may have high privileges. This would likely break the principle of least privileges.

Possible Values:

The public role might have access to any number of proxies.

Best Practice:

Revoke any agent proxy access to public role. Before revoking the public role from the proxy, ensure that alternative logins or appropriate user-defined database roles have been added with equivalent permissions. Otherwise, SQL Agent job steps dependent upon this access will fail.

Recommendation:

Using GUI,

- Open SQL Server Management Studio → Connect to the database → Select Server SQL Agent → Select the proxy in interest → Right Click and select Properties → Add specific security principals which require access.
- Alternatively use sp_grant_login_to_proxy T-SQL. Refer Microsoft learn for further details.
- Revoke access to the <proxyname> from the public role using the following T-SQL command:

> USE [msdb] GO EXEC dbo.sp_revoke_login_from_proxy @name = N'public', @proxy_name = N'<proxyname>'; GO

27. Check Password Expiration

Description:

Ensure 'CHECK_EXPIRATION' option is set to 'ON' for all SQL Authenticated Logins Within the Sysadmin Role

Vulnerability:

Applies the same password expiration policy used in Windows to passwords used inside SQL Server if turned on. Else the passwords in use might be weak.

Possible Values:

- Enabled or 'ON'
- Disabled or 'OFF'

Best Practice:

This option should be set to 'ON'. This is a mitigating recommendation for systems which cannot follow the recommendation to use only Windows Authenticated logins.

Recommendation:

Run the following T-SQL command for the login names where check expiration is set to 'OFF':

> ALTER LOGIN [<login_name>] WITH CHECK_EXPIRATION = ON;

28. Check Password Policy

Description:

Ensure 'CHECK_POLICY' Option is set to 'ON' for All SQL Authenticated Logins

Vulnerability:

Applies the same password complexity policy used in Windows to passwords used inside SQL Server if turned on. Else the passwords in use might be weak.

Possible Values:

- Enabled or 'ON'
- Disabled or 'OFF'

Best Practice:

This option should be set to 'ON'. The setting is only enforced when the password is changed. This setting does not force existing weak passwords to be changed. Thus existing passwords need to be changed manually.

Recommendation:

Run the following T-SQL command for the login names where check policy is set to 'OFF':

```
> ALTER LOGIN [<login_name>] WITH CHECK_POLICY = ON;
```

29. Number of Error Log Files

Description:

Ensure 'Maximum number of error log files' is set to greater than or equal to '12'

Vulnerability:

SQL Server error log files must be protected from loss. The log files must be backed up before they are overwritten. Retaining more error logs helps prevent loss from frequent recycling before backups can occur.

Possible Values:

All positive numerical values

Best Practice:

This option should be set to greater than or equal to 12.

Recommendation:

Using GUI,

- Open SQL Server Management Studio.
- Open Object Explorer and connect to the target instance.
- Navigate to the Management tab in Object Explorer and expand. Right click on the SQL Server Logs file and select Configure
- Verify the Limit the number of error log files before they are recycled checkbox is checked.
- Verify the Maximum number of error log files is greater than or equal to 12.

Alternatively run the following T-SQL command replacing <NumberGreaterThanOrEqualTo12>:

```
> EXEC master.sys.xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
  N'Software\Microsoft\MSSQLServer\MSSQLServer', N'NumErrorLogs', REG_DWORD,
  <NumberGreaterThanOrEqualTo12>;
```

30. Default Trace

Description:

Ensure 'Default Trace Enabled' Server Configuration Option is set to '1'

Vulnerability:

The default trace provides audit logging of database activity including account creations, privilege elevation and execution of DBCC commands.

Possible Values:

- Enabled or '1'
- Disabled or '0'

Best Practice:

This configuration should be set to '1'.

Recommendation:

Run the following T-SQL command:

> EXECUTE sp_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp_configure 'default trace enabled', 1; RECONFIGURE; GO EXECUTE sp_configure 'show advanced options', 0; RECONFIGURE;

31. Login Audit

Description:

Ensure 'Login Auditing' is set to 'failed logins'

Vulnerability:

This setting will record failed authentication attempts for SQL Server logins to the SQL Server Errorlog. Capturing failed logins provides key information that can be used to detect or confirm password guessing attacks. Capturing successful login attempts can be used to confirm server access during forensic investigations, however, using this audit level setting to also capture successful logins creates excessive noise in the SQL Server Errorlog which can hamper a DBA trying to troubleshoot problems.

Possible Values:

- None
- Failed
- Successful
- Both Failed and Successful

Best Practice:

This configuration should be set to 'failure'.

Recommendation:

Using GUI,

- Open SQL Server Management Studio.
- Right click the target instance and select Properties and navigate to the Security tab.
- Select the option Failed logins only under the Login Auditing section and click OK.

Alternatively run the following T-SQL command:

```
> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
  N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 2
```

Note: Restart the SQL Server service.

32. SQL Server Audit

Description:

Ensure 'SQL Server Audit' is set to capture both 'failed' and 'successful logins'

Vulnerability:

SQL Server Audit is capable of capturing both failed and successful logins and writing them to one of three places: the application event log, the security event log, or the file system. By utilizing Audit instead of the traditional setting under the security tab to capture successful logins, we reduce the noise in the ERRORLOG.

Possible Values:

Any number of Server Audits might be present in a Server with Audit Action Type of AUDIT_CHANGE_GROUP, FAILED_LOGIN_GROUP and SUCCESSFUL_LOGIN_GROUP.

Best Practice:

There should be atleast one Server Audit specification must be created/present with following audit names:

- AUDIT_CHANGE_GROUP
- FAILED_LOGIN_GROUP
- SUCCESSFUL_LOGIN_GROUP

Recommendation:

Using GUI,

- Open SQL Server Management Studio.
- Expand the SQL Server in Object Explorer.
- Expand the Security Folder.
- Right-click on the Audits folder and choose New Audit...
- Specify a name for the Server Audit.
- Specify the audit destination details and then click OK to save the Server Audit.
- Right-click on Server Audit Specifications and choose New Server Audit Specification...
- Name the Server Audit Specification.
- Select the just created Server Audit in the Audit drop-down selection.

- Click the drop-down under Audit Action Type and select AUDIT_CHANGE_GROUP.

- Click the new drop-down Audit Action Type and select FAILED_LOGIN_GROUP.

- Click the new drop-down under Audit Action Type and select SUCCESSFUL_LOGIN_GROUP.

- Click OK to save the Server Audit Specification.

- Right-click on the new Server Audit Specification and select Enable Server Audit Specification.

- Right-click on the new Server Audit and select Enable Server Audit.

Alternatively run the following T-SQL command replacing <Enter audit name here> and <Enter audit spec name here>:

```
> USE master GO CREATE SERVER AUDIT <Enter audit name here> TO APPLICATION_LOG; GO
  CREATE SERVER AUDIT SPECIFICATION <Enter audit spec name here> FOR SERVER AUDIT <Enter
  audit name here> ADD (FAILED_LOGIN_GROUP), ADD (SUCCESSFUL_LOGIN_GROUP), ADD
  (AUDIT_CHANGE_GROUP), ADD (SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP), ADD
  (FAILED_DATABASE_AUTHENTICATION_GROUP) WITH (STATE = ON); GO ALTER SERVER AUDIT
  <Enter audit name here> WITH (STATE = ON); GO
```

33. CLR Assembly Permission

Description:

Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies

Vulnerability:

Setting CLR Assembly Permission Sets to SAFE_ACCESS will prevent assemblies from accessing external system resources such as files, the network, environment variables, or the registry. Assemblies with EXTERNAL_ACCESS or UNSAFE permission sets can be used to access sensitive areas of the operating system, steal and/or transmit data and alter the state and other protection measures of the underlying Windows Operating System.

Possible Values:

- SAFE_ACCESS

- EXTERNAL_ACCESS

- UNSAFE

Best Practice:

All CLR Assemblies should have the permission set to 'SAFE_ACCESS' except for those which are Microsoft-created (is_user_defined = 0) are excluded from this check as they are required for overall system functionality. The remediation measure should first be tested within a test environment prior to production to ensure the assembly still functions as designed with SAFE permission setting.

Recommendation:

Run the following T-SQL command:

```
> USE <database_name>; GO ALTER ASSEMBLY <assembly_name> WITH PERMISSION_SET = SAFE;
```

34. Symmetric Key Encryption Algorithm

Description:

Ensure 'Symmetric Key Encryption algorithm' is set to 'AES_128' or higher in non-system databases

Vulnerability:

As per the Microsoft Best Practices, only the SQL Server AES algorithm options, AES_128, AES_192, and AES_256, should be used for a symmetric key encryption algorithm. The following algorithms (as referred to by SQL Server) are considered weak or deprecated and should no longer be used in SQL Server: DES, DESX, RC2, RC4, RC4_128.

Possible Values:

- DES
- Triple DES
- TRIPLE_DES_3KEY
- RC2
- RC4
- 128-bit RC4
- DESX
- 128-bit AES
- 192-bit AES
- 256-bit AES

Best Practice:

All Symmetric keys in database must use 'AES_128' or higher as encryption algorithm.

Recommendation:

Refer Microsoft learn for learning about Altering symmetric key.

If required, use the following T-SQL command to drop symmetric keys:

```
>  USE <database_name> GO DROP SYMMETRIC KEY <key_name>;
```

35. Asymmetric Key Size

Description:

Ensure Asymmetric Key Size is set to 'greater than or equal to 2048' in non-system databases

Vulnerability:

Microsoft Best Practices recommend to use at least a 2048-bit encryption algorithm for asymmetric keys. The RSA_2048 encryption algorithm for asymmetric keys in SQL Server is the highest bitlevel provided and therefore the most secure available choice.

Possible Values:

- 512 bit
- 1024 bit
- 2048 bit

Best Practice:

Asymmetric key size should be set to greater than or equal to 2048 bits.

Recommendation:

Refer Microsoft learn for learning about Altering asymmetric key.

If required, use following T-SQL command to drop asymmetric keys:

```
>  USE <database_name> GO DROP ASYMMETRIC KEY <key_name>;
```

5.4. Configuring, Editing, Exporting, Running Analysis and Scheduling compliances.

Configure Source

To configure the source for the first time for compliance/risk posture, click **Configure Source** button in the respective box. It will open the **Edit Compliance** page where you can edit the required sources.
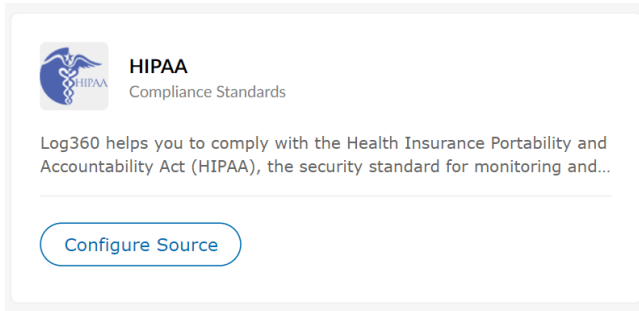
Edit Source

Go to edit compliance also by clicking the ✏ **Edit** button in the compliance/risk posture box. It will open the **Edit Compliance** page where you can edit the required sources for that compliance/risk posture.

Run Analysis

Start the analysis for the required Risk posture by clicking the ↻ **Run Analysis** button in the respective compliance widget.
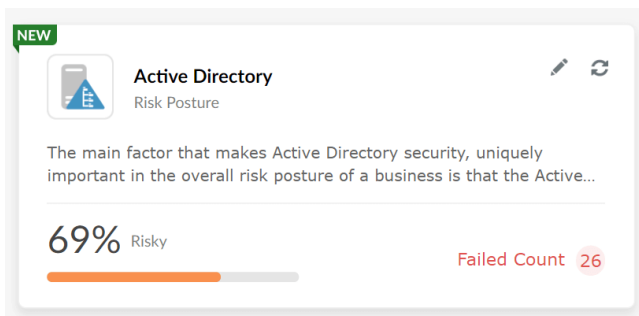
Enabling and disabling compliances

To enable/disable a particular compliance,

- In the **Compliance** Tab, Click **Manage Compliance** button at the top-right corner.
- You will see the list of enabled compliances in the Manage Compliance page. Enable/disable the required compliances by clicking the toggle.

Configure Analysis Schedules

- You can get the fresh analysis results by clicking the **Run Now** link at the top left corner of the Risk Posture

- The frequency can be set by clicking the ⟳ **Schedule** button next to the **Run Now** link. (By default, the schedule will run once per day. You can also change the frequency of the analysis.)
- Click the ⟳ **Schedule** button to see the time when the next analysis is scheduled to run.
- You can also see the time when the last analysis has been completed.

Exporting Compliance/Risk Posture

Log360 allows you to export compliance policy reports in either the PDF or CSV format. The exported data mirrors the information displayed in the user interface, ensuring accuracy and consistency. This PDF or CSV export can be valuable for audit purposes, providing a comprehensive and easily shareable record of your compliance policies.

To export the risk posture reports

1. Navigate to the risk posture you want to export.

2. Locate the **Export As** option in the top-right corner of the page.

3. Select export type:

   - In the **Export** menu, choose the type of export that suits your requirements. Options include:

     - Summary

     - Summary and Details

4. Run a fresh analysis (Optional):

   - If you require up-to-date data, check the **Run Analysis Before Export** checkbox to ensure a fresh analysis is performed.

5. Choose output format:

   - Under the **Export As** section, select the desired output file format. Options include:

     - PDF

     - CSV

6. Initiate the export:

   - To begin the export process, click the **Export** button.

7. Downloading the export:

   - Click on the 🗎 **Export History** icon, and click the download link.

To export the compliance reports

1. Navigate to the compliance you want to export.

2. Click on **Comprehensive Audit Reports**.

3. Select **Export Type**:

   - In the **Export** menu, choose the type of export that suits your requirements. Options include:

     - All reports

     - Currently viewed reports

     - Select reports

4. Choose output format:

   - Under the **Export As** section, select the desired output file format. Options include:

- PDF
- CSV

5. Initiate the export:
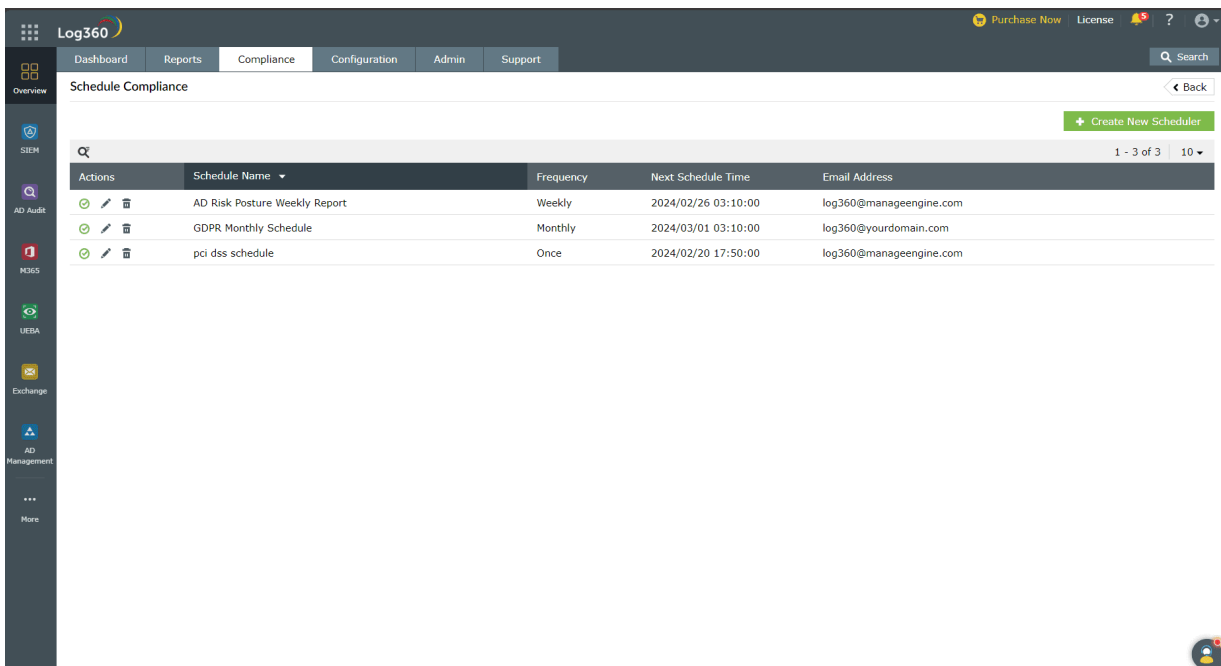
- To begin the export process, click the **Export** button.

6. Downloading the export:

- Click on the ▣ **Export History** Icon, and click the download link.

Scheduling compliance/risk posture:

You can create compliance report schedules in Log360 which will deliver the selected compliance reports for a specified duration directly to your email. This helps avoid repeated logging in to the product for report viewing.

Add compliance/risk posture schedule

To add a new compliance/risk posture schedule,

- In the **Compliance** tab, click **Schedule Compliance** at the top-right corner.
- Click **Create New Scheduler**.
- Enter a name for the scheduler and select the compliance/risk posture that you want to schedule.
- Select the frequency at which the reports need to be sent, the duration that should be covered in the reports, and the format of the reports.
- Enter the email IDs to which the reports need to be sent and the subject of the email.
- After entering all the information, click **Save**.

Edit compliance/risk posture schedule

To update an already created compliance/risk posture schedule

- In the **Compliance** tab, click **Schedule Compliance** at the top-right corner.
- Click the **Edit** icon corresponding to the schedule you want to edit.
- Make the necessary changes and click **Save**.

Delete compliance/risk posture schedule

To delete an already created compliance/risk posture schedule

- In the **Compliance** tab, click **Schedule Compliance** at the top-right corner.
- Click the **Delete** icon corresponding to the schedule you want to delete.
- In the pop-up box that appears, click **Yes**.

Disable compliance/risk posture schedule

You can also temporarily disable an Compliance/Risk posture schedule with the steps below.

- In the **Compliance** tab, click **Schedule Compliance** at the top-right corner.
- Click the **Disable** icon corresponding to the schedule you want to delete.

5.5. Creating custom compliances

Add, edit, or delete custom compliance sections:

Log360 enables you to create custom compliance sections for internal audits and other such requirements.
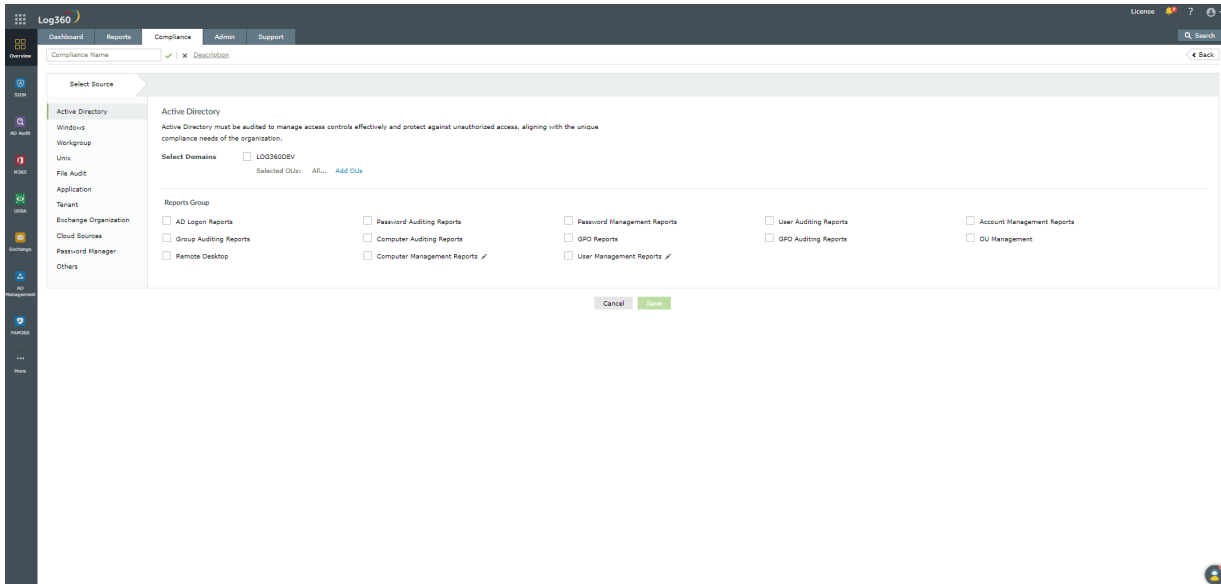
Adding custom compliance

To add a custom compliance,

- In the **Compliance** tab, click **Manage Compliance** at the top-right corner.
- Click **Create New Compliance**.
- Enter a name for the compliance and select the reports that you would like to add to it.
- To add the new compliance to Log360's list, click **Save**.

Editing custom compliance

To edit a custom compliance,

- In the **Compliance** tab, click **Manage Compliance** at the top-right corner.
- Click the **Edit** icon corresponding to the compliance section you want to edit.
- Make the necessary changes and click **Save**.

Deleting custom compliance

To delete a custom compliance,

- In the **Compliance** tab, click **Manage Compliance** at the top-right corner.
- Click the **Disable** icon corresponding to the schedule you want to delete.

5.6. Troubleshooting Tips

Rule Status and its definitions

Low/No Risk

✓ Low/No Risk

This status informs that the selected source's configurations have met the recommended/user set compliance value as per their norms.

High Risk

✗ High Risk

This status informs that the selected source's configurations have not met the recommended/user set compliance value as per their norms.

Unable to Verify

? Unable to Verify

This status informs that the Log360 server was unable to fetch the required data needed for analyzing the specific rule. It can be due to the following reasons.

Troubleshooting steps for 'Unable to Verify' status:

Active Directory

Possible reasons for the status "Unable to verify" are as follows:

1. Insufficient domain details
2. Access denied for SYSVOL folder.

1. Insufficient domain details:

This error occurs when the domain details or credentials haven't been synced properly while integrating with the child components.

Troubleshooting steps:

- Navigate to **Admin → Log360 integration**.
- Make sure any one of the child components has been integrated and at least one domain is configured.
- Click the **Sync Now** button.
- Make sure the credentials have been synced correctly by checking in **ADSCredentials table**. (To view the table data, you can go to **http(s)://<hostname>:<log360 port number>/runQuery.do** page and execute the below query.)

  select * from ADSCredentials;

- If there is no credentials data in the table, trigger **Sync Now** button once again.
- Now, go to the specified compliance/risk posture.
- Click the **Run Now** button.

2. Access denied for SYSVOL folder:

This error occurs when a Log360 installed machine was unable to access the **SYSVOL** folder of the domain controllers of the selected domain. This restriction was made by Microsoft after 2015.

- Make sure the **SYSVOL** folder (C:\Windows\SYSVOL\sysvol) of the domain controllers has been shared to the user with which the domain is configured.

Troubleshooting steps:

Using GPO of Log360 installed machine's domain:

- Go to **"Computer Configuration → Administrative Templates → Network → Network Provider "** in the Domain Controller.
- Enable the **Hardened UNC Paths**.
- In **Options**, click the **Show** button.
- Add **"*\SYSVOL"** value in **"Value Name"** Field.
- Add **"RequireMutualAuthentication=0,RequireIntegrity=0,RequirePrivacy=0"** value in the **"Value"** Field.
- For immediate results, open **Command** prompt as administrator and run **"gpupdate /force"** command in the Log360 installed Machine.
- Click **Ok**.

(or)

Using Local Security Policy Editor:

- Open Local Security Policy Editor with **"gpedit.msc"** in the Log360 installed Machine.
- Go to **Computer Configuration → Administrative Templates → Network → Network Provider**.
- Enable the **Hardened UNC Paths**. In **Options**, click the **show** button.
- Add **"*\SYSVOL"** value in **"Value Name"** Field.
- Add **"RequireMutualAuthentication=0,RequireIntegrity=0,RequirePrivacy=0"** value in **"Value"** Field.
- Click **Ok**.

(or)

Execute the below command in Command Prompt as Administrator in Log360 installed machine :

%COMSPEC% /C reg add
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths /v "*\SYSVOL" /d "RequireMutualAuthentication=0" /t REG_SZ

- After these troubleshooting steps, go to **Compliance → Risk Posture → Active Directory**, and click **Run Now** button.

SQL Server

Possible reasons for the status "Unable to verify" are as follows:

1. Dependent product down (EventLog Analyzer)

2. SQL Server down

3. Insufficient server details/user credentials

Dependent product down:

The analysis requires EventLog Analyzer to be up and running. If the product is down, the analysis cannot be completed. In case of distributed EventLog Analyzer setup, the respective managed server in which the concerned SQL server is configured should also be up and running.

Troubleshooting steps:

- Make sure EventLog Analyzer is integrated and running smoothly.

SQL server down

The analysis requires SQL Server to be up and running. If the SQL server is down, the analysis cannot be completed.

Troubleshooting steps:

- Make sure the selected SQL server(s) is up and running.

Insufficient server details/user credentials:

The selected SQL server(s) configuration details and credentials should be up-to-date and valid. Outdated or wrong details will cause analysis to fail. The configured user should have sysadmin role in the selected SQL server for all the rules to succeed.

Troubleshooting steps:

- Update credentials and server details in **EventLog Analyzer → Settings → Log Source Configuration → Database Audit**.
- Refer here for more details.

Possible Reasons for "No SQL Server(s) Configured" in 'Edit Compliance' are as follows:

1. No SQL server(s) is configured.

2. Advanced auditing is enabled for the SQL server.

1. No SQL server(s) is configured

To configure MS SQL DB, please refer here.

2. Advanced Auditing not enabled for the SQL server

To enable advanced auditing, please refer here.

6.1. Admin

The **Admin** tab in Log360 allows you to configure the below settings:

- Administration Settings
- General Settings

6.2.1. Administration Settings

These settings helps administrators to configure Log360 to suit the organization policies and convenience. The following settings can be configured under the **Admin Settings**:

- Log360 Integration
- Auto Update
- Manage Technicians
- Logon Settings
- Search Engine Management
- Reverse Proxy
- Device allocation management

6.2.2. Log360 Integration

Log360 contains nine components, with each of them providing a rich but unique set of features. These components are:

- ADAudit Plus
- ADManager Plus
- EventLog Analyzer
- User and Entity Behavior Analytics (UEBA)
- DataSecurity Plus
- M365 Manager Plus
- Exchange Reporter Plus
- Cloud Security Plus
- PAM360

To get a complete solution for all your security challenges and management problems, these components have to be integrated into Log360. Follow the steps shown below:

Step 1: Download and install the components

> **Note:** If you already have the components installed and running, you can skip this step and proceed with **Step 2 (Integrate the components)**

- Download the components either from the link available under the Dashboard of each component or from the Log360 Website.

  > **Note:** Kindly ensure that you integrate EventLog Analyzer version 12150 or above and ADAudit Plus version 6065 or above in the latest and upcoming builds of Log360 (Build 5214 and above).

- Install the components one-by-one by double-clicking the downloaded '.exe' files and following the install shield wizard.
- Once the installation is complete, start the different components by double-clicking on the desktop shortcut icons of the respective components.

Step 2: Integrate the components

> **Note:** Make sure that all the components are set up and running before proceeding with the steps given below. Also, check whether you have the appropriate versions of the components with respect to the Log360 version you are currently running.

- Go to **Admin → Log360 integration**. You will be presented with nine tabs, each representing a component of Log360.

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

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

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

- Provide the super administrator credentials of the component to be integrated.

- Click **Integrate Now**.

- Repeat the above 3 steps for other components as well under the respective tabs.

> **Note**:
> - To convert the integrated stand alone 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 convert EventLog Analyzer to admin server and then integrate the distributed edition of EventLog Analyzer component with Log360 .
>
> - When EventLog Analyzer is removed from Log360, the EventLog Analyzer service will be shut down. After removing EventLog Analyzer from Log360 successfully, please remember to restart the EventLog Analyzer service to ensure smooth functioning.
>
> - When PAM360 is integrated with Log360, Log360 UEBA and ADManager Plus won't integrate with PAM360 unless the respective product certificates are imported into PAM360.
>
> Click here to know how to integrate PAM360 with Log360 UEBA.
>
> Click here to know how to integrate PAM360 with ADManager Plus.

Switch between different components of Log360:

Once all the components have been integrated, you can switch between components to access the full feature set that each component offers.

- You can switch between different components by two methods.
  - By Clicking the **Jump to** Icon ⊞ on top left corner and selecting the component, or
  - By Clicking the **Component App** Icon in AppsPane.

> **Note**: If you are unable to see the Component app icon, click on **More** and select the component.

Data Synchronization Across Components

Once the different components of Log360 have been integrated, the data such as domain settings, component integration, and more will automatically be synchronized across each component. This saves a lot of time for the administrators, as they no longer have to configure the same settings across all the four components. Any changes made in any one of the components will automatically be reflected in the other components also. The data relating to the following configuration settings will be automatically synchronized across all the components of Log360:

Domain Settings:

If you want to add a domain to all the components in Log360, simply add the domain to any one of the components and it will be automatically added to all the other components. Also, if there is a change in the administrator credential used to configure a domain with a component, simply update the change in any one of the components and it will be synchronized across all the other components.

Integration Settings:

The different components of Log360 communicate with each other for various purposes like single sign-on, domain settings, and more. Any changes to the hostname and port number of a component must be reflected in the other components for smooth working of all the components. But with Log360, there is no need for you, the administrator, to manually make the changes in each of the components. Simply update these changes in the Log360 Integration settings page and the changes will be automatically synchronized across all the components.

6.2.3. Auto Update

- Navigate to **Admin → Administration → Auto Backup/Update → Auto Update.**

- To **enable** auto update for a particular component, click on the ⊘ icon located in the action column of the particular component.

- To **disable** auto update for a particular component, click on the ⊘ icon located in the action column of the particular component.

- To edit the update scheduler for a particular component, click on the ✏ icon located in the action column of the component.

- In **Check for Update** option, select whether you want to check for updates daily, weekly, or monthly.

- Selecting the option **Automatically Download and update Log360** will download and install any available updates automatically.

- You can also choose to receive notifications about available updates by selecting the options under **Notify me**.

  - **When updates are available:** Notifications will be sent when updates are available.

  - **After installing the update:** Notifications will be sent after the updates have been downloaded and installed.

- Click **Save**.

- Furthermore, you can use the **Update History** link to view all the installed updates.

Alternatively, you can also configure the auto update settings by following the steps listed below:

- Navigate to **Support** tab.

- Click on **Check for updates** box at the top right corner of the page.

- Click **Settings** link in the pop-up that appears, then click on **Auto Update** tab.

- Select the check box against **Enable Auto Update** to enable auto update.

- In **Check for Update** option, select whether you want to check for updates daily, weekly, or monthly.

- Selecting the option **Automatically Download and update Log360** will download and install any available updates automatically.

- You can also choose to receive notifications about available updates by selecting the options under **Notify me**.

  - **When updates are available:** Notifications will be sent when updates are available.

  - **After installing the update:** Notifications will be sent after the updates have been downloaded and installed.

- Click **Save**.

6.2.4. Centralized Technician Management

Log360 supports centralized management of user roles for all its components which include **ADAudit Plus, EventLog Analyzer, Cloud Security Plus, Exchange Reporter Plus, DataSecurity Plus, Log360 UEBA, ADManager Plus**, and **M365 Manager Plus**. When a user is declared as a technician, they are provided with the permissions to configure specific areas of Log360 and its various components. A user can be assigned as a technician of a single domain, or multiple domains.

Log360 allows adding users in two user groups, admin and operator.

Admin

An admin has full control over the entire application by default.

Operator
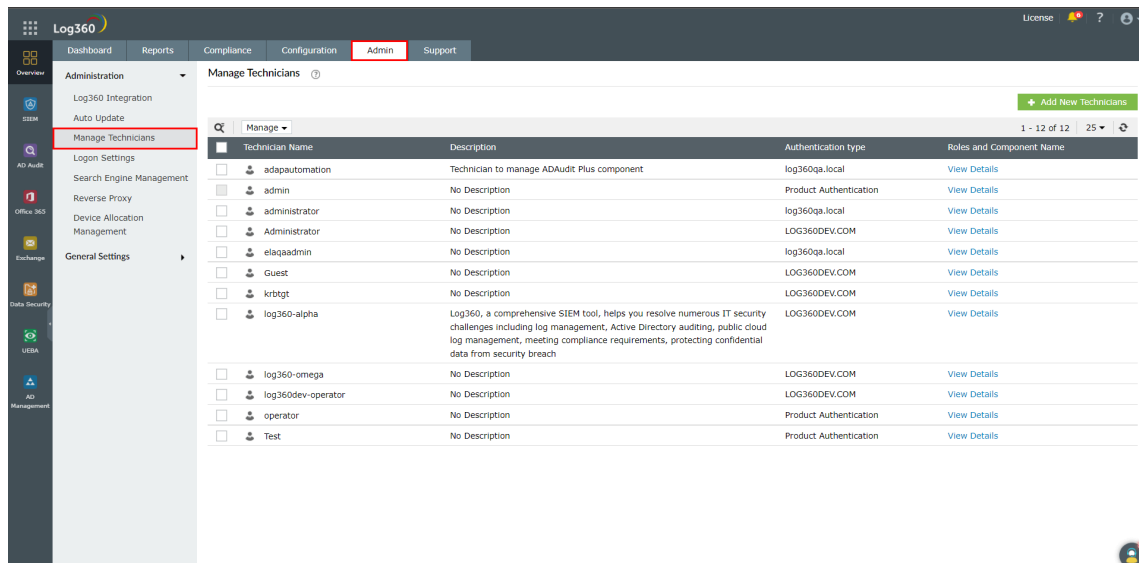
An operator can audit the operations taking place in the application.

How to add a new centralized technician?

A new centralized technician can be added with authentication by two methods - product authentication and Active Directory authentication.

To add new users with authentication by product, follow the steps given below:

- Under the **Admin** tab, navigate to **Administration → Manage Technicians**.

- Then click on the **+ Add New Technicians** button on the top-right corner.

- Enter a name for the technician in the **User Name** field. You can additionally add a description by clicking on the **Description** button.
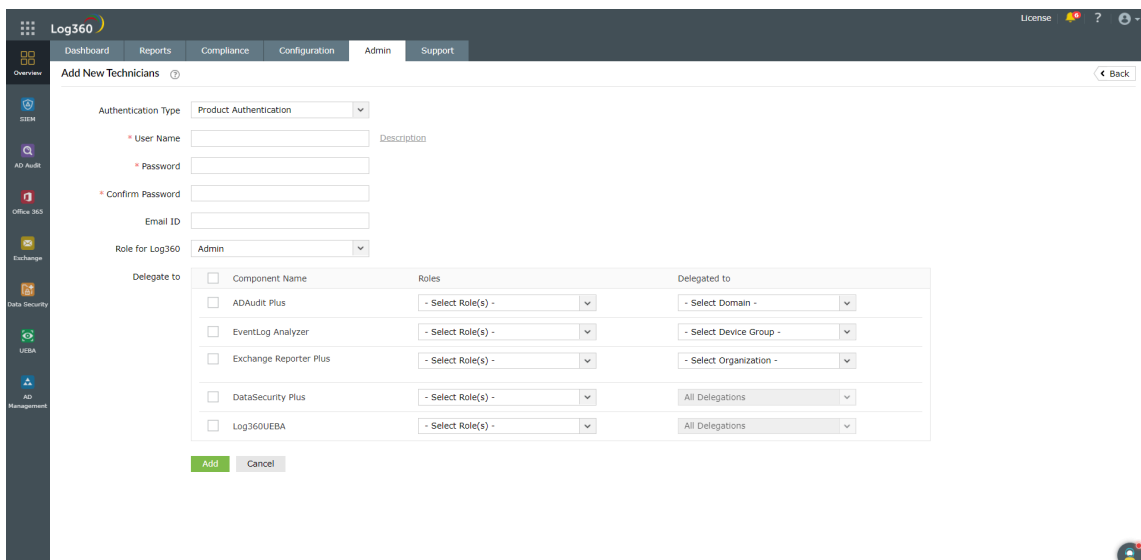
- Enter a new password and confirm it in the respective fields.

- Enter the email address of the technician in the **Email ID** field.

- In the **Roles** drop-down box, choose the role(s) you want to assign to the technician. The permissions applicable to the selected role will be assigned to the technician.

- In the **Delegate to** section, select the components to which you want to add the new technician, by ticking the respective checkboxes. For each component, select the roles and domains to be assigned in the appropriate fields.

- Complete the add user operation by clicking on the **Add** button.

To add new users with authentication by Active Directory, follow the steps given below:

- Under the **Admin** tab, navigate to **Administration → Manage Technicians**.

- Then click on the **+ Add New Technicians** button on the top-right corner.

- Under **Authentication Type**, select AD Authentication from the drop-down menu.
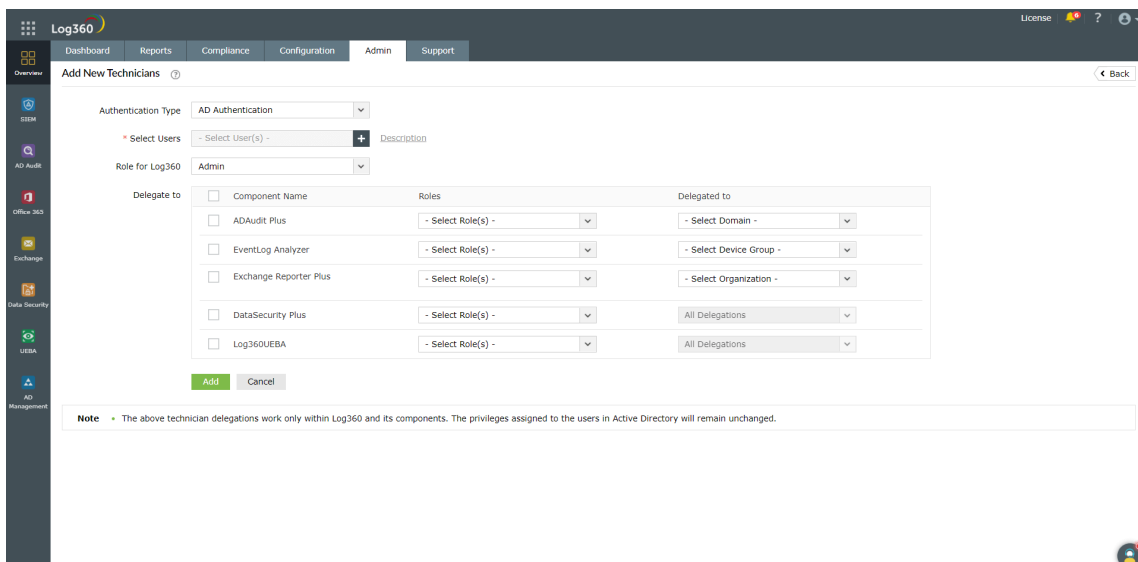
- In the **Select Users** field, select the required users in your AD by clicking on the **+** button.

- Select the **Role for Log360** from the drop-down menu.

- In the **Delegate to** section, select the components to which you want to add the new technician, by ticking the respective checkboxes. For each component, select the roles and domains to be assigned in the appropriate fields.

- Complete the add user operation by clicking on the **Add** button.

Note: Previously, auto addition of domain technicians in Exchange Reporter Plus and M365 Manager Plus was initiated when the user logs into Log360 using their AD credentials. Now, users are required to create domain technicians separately in each component, or from the centralized technician dashboard.

How to modify an existing technician from the centralized dashboard?

To edit the information of an existing technician, follow the steps given below.

- Under the **Admin** tab, navigate to **Administration → Manage Technicians**.

- Click the ✏ icon next to the name of the technician that you want to edit. The icon will appear when the cursor is hovered over the technician name.
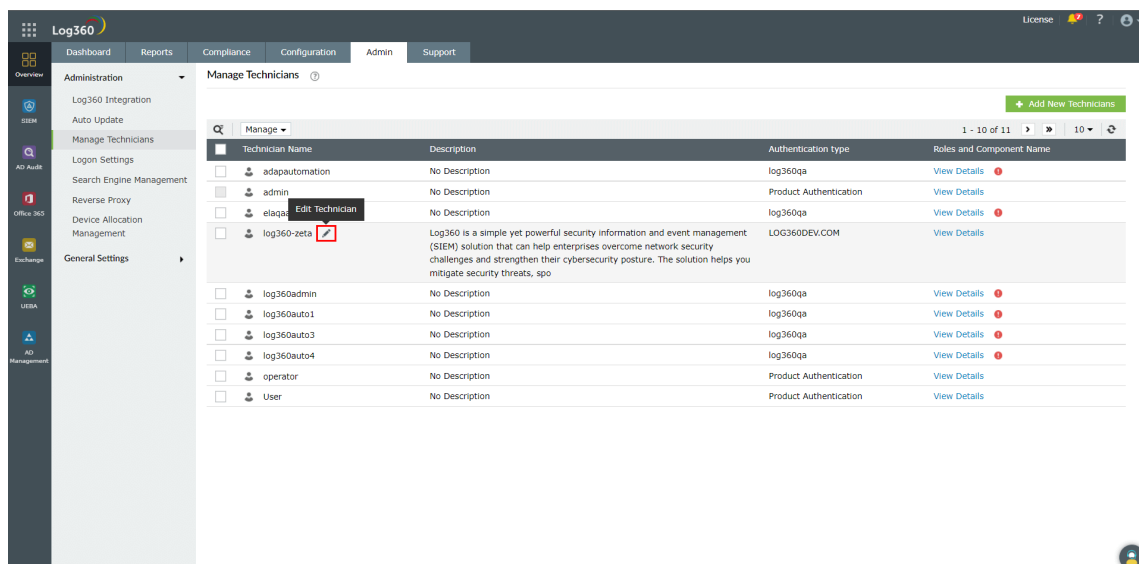
- Edit the information in the various fields as required.
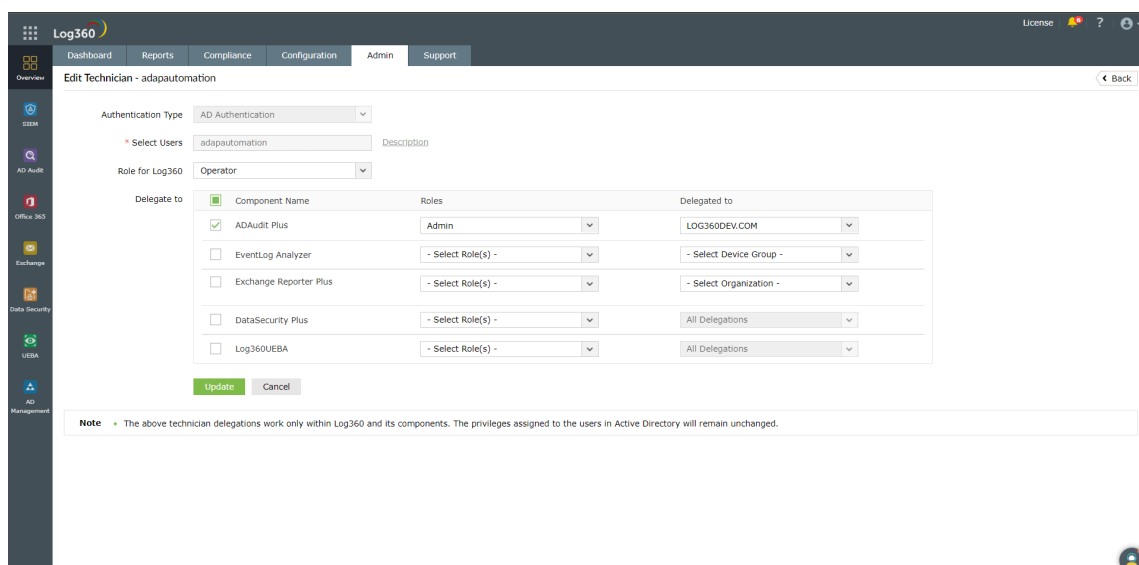
- To associate a new component for the technician, tick the check-box corresponding to the component in the **Delegate to** section. Similarly, to dissociate a component for the technician, untick the checkbox corresponding to the component.

> **Note**: A password reset is mandatory if a new component is added to an existing technician.

- To modify the roles and delegations associated with the technician, choose the required role and delegation from the drop-down for the respective component under the **Delegate to** section.
- Click on the **Update** button to save the changes.
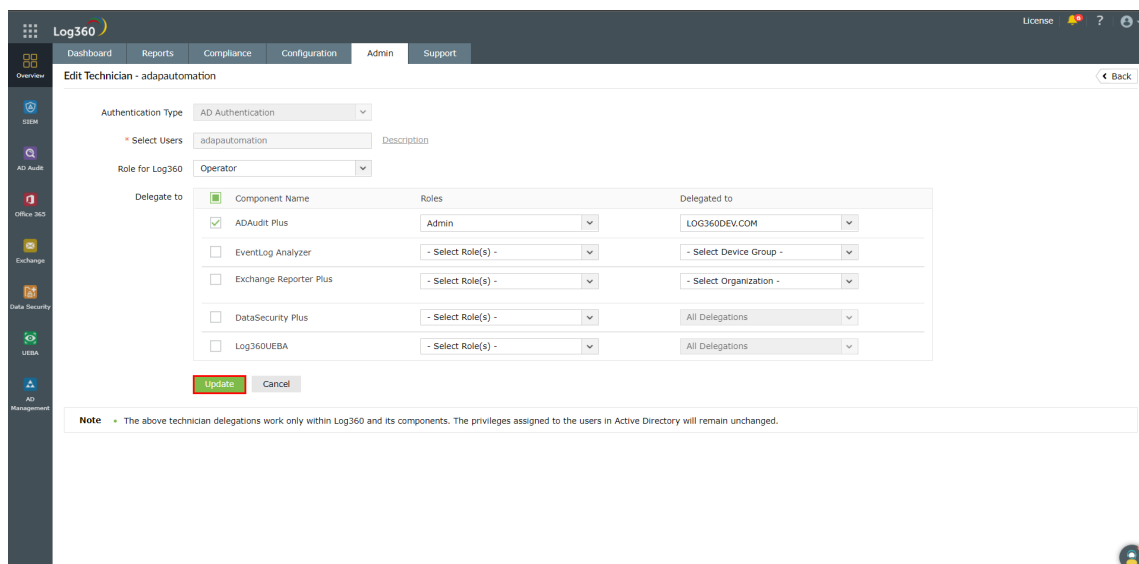
How to delete an existing technician from the centralized dashboard?

To delete an existing technician, follow the steps given below.

- Under the **Admin** tab, navigate to **Administration → Manage Technicians**.
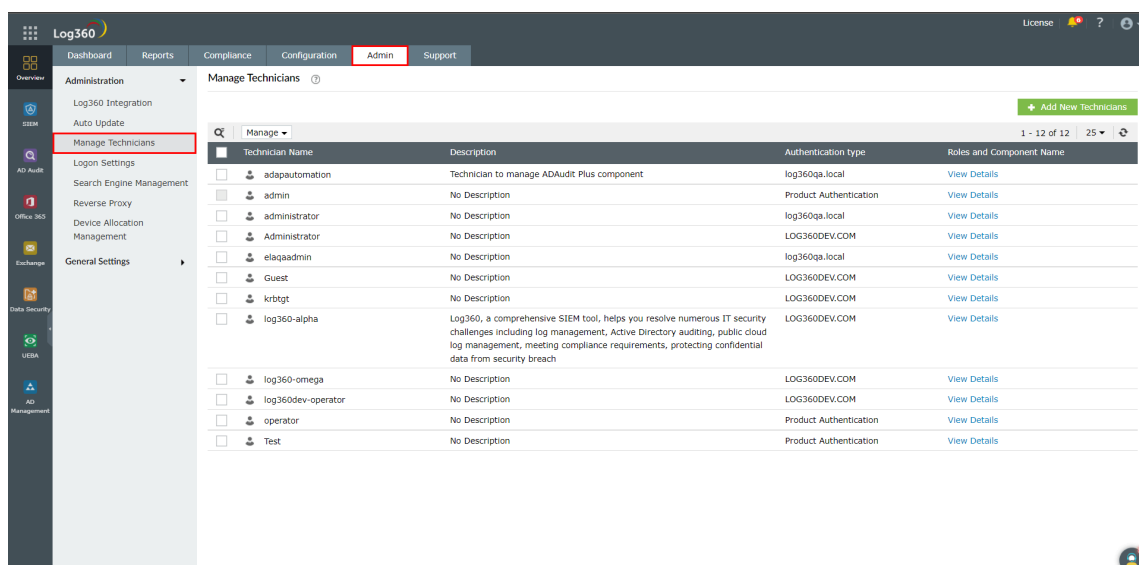
- Choose the technicians to be deleted by ticking the checkbox corresponding to the technician's name.
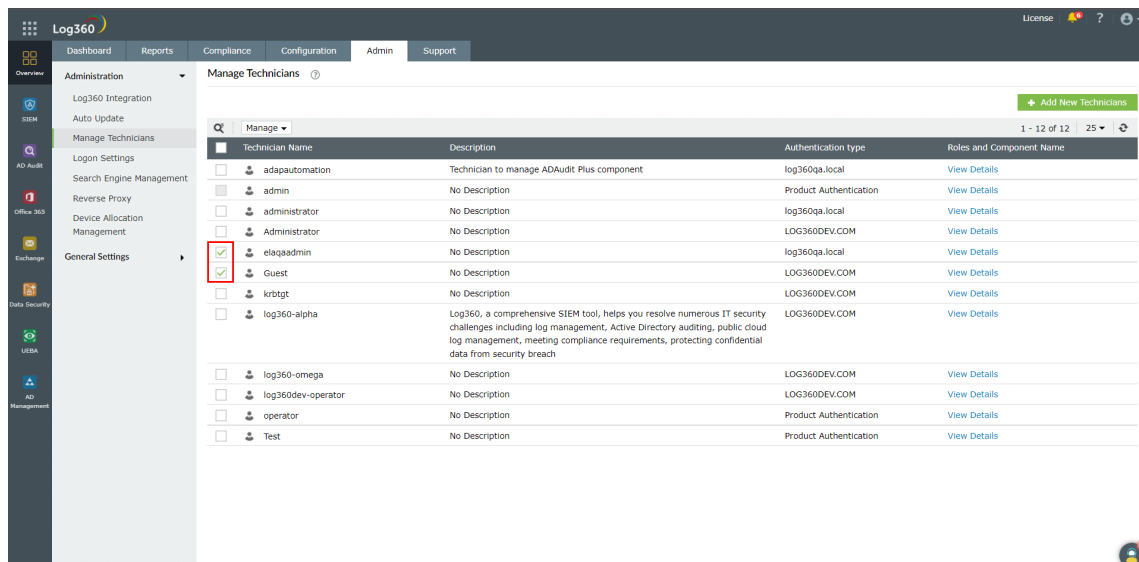
- Click on the **Manage** button above the table and select **Delete** from the drop-down menu.
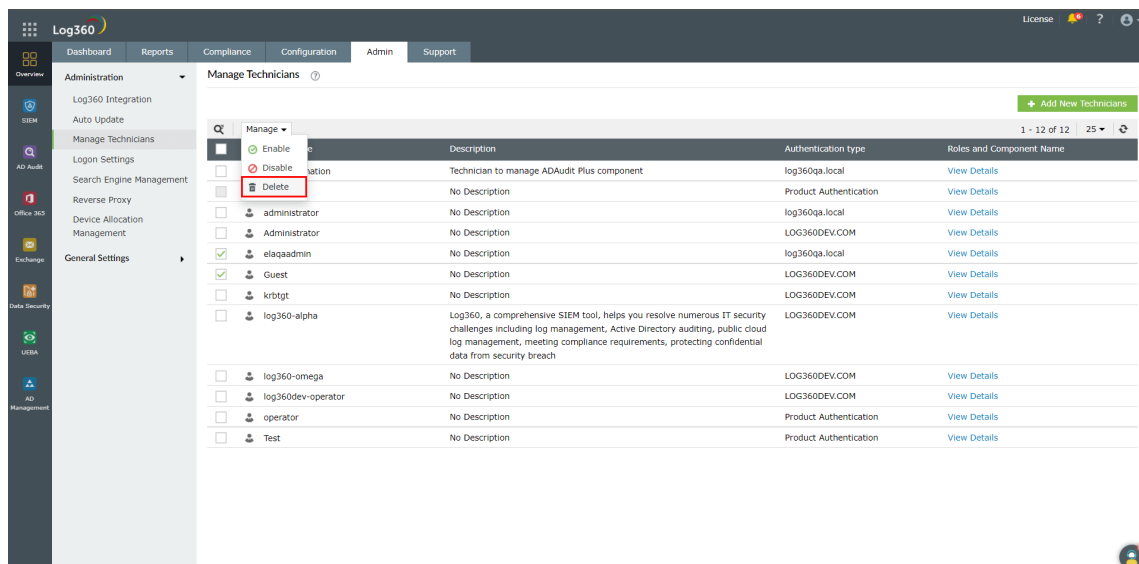
- Confirm the deletion by clicking **Yes** on the warning pop-up message.
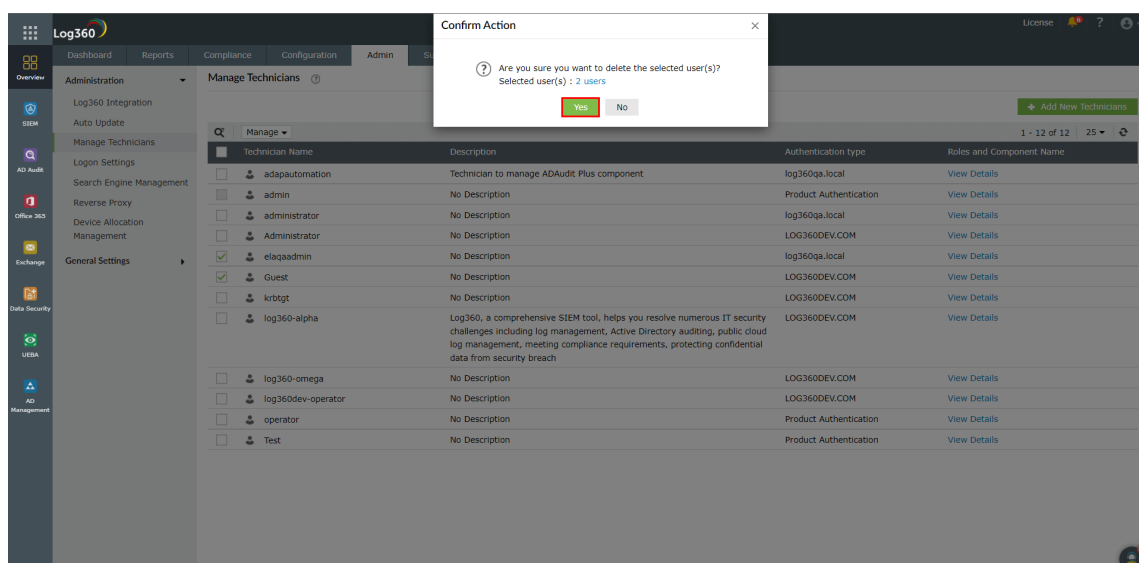
- The technician is now deleted.

How to enable or disable an existing technician?

To enable or disable an existing technician, follow the steps given below.

- Under the **Admin** tab, navigate to **Administration → Manage Technicians**.

- Choose the technicians to be enabled/disabled by ticking the checkbox corresponding to the technician's name.

- Click on the **Manage** button above the table and select **Enable** or **Disable** from the drop-down menu.
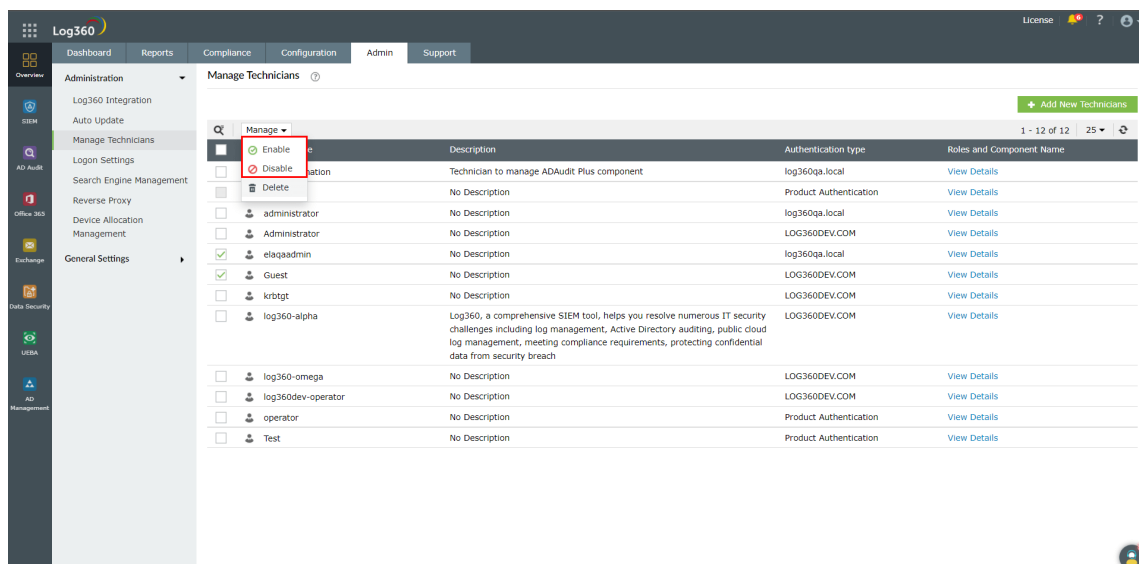
- The technician is now enabled/disabled.

To enable or disable an existing technician only for a specific component, follow the steps given below.

- Under the **Admin** tab, navigate to **Administration → Manage Technicians**.
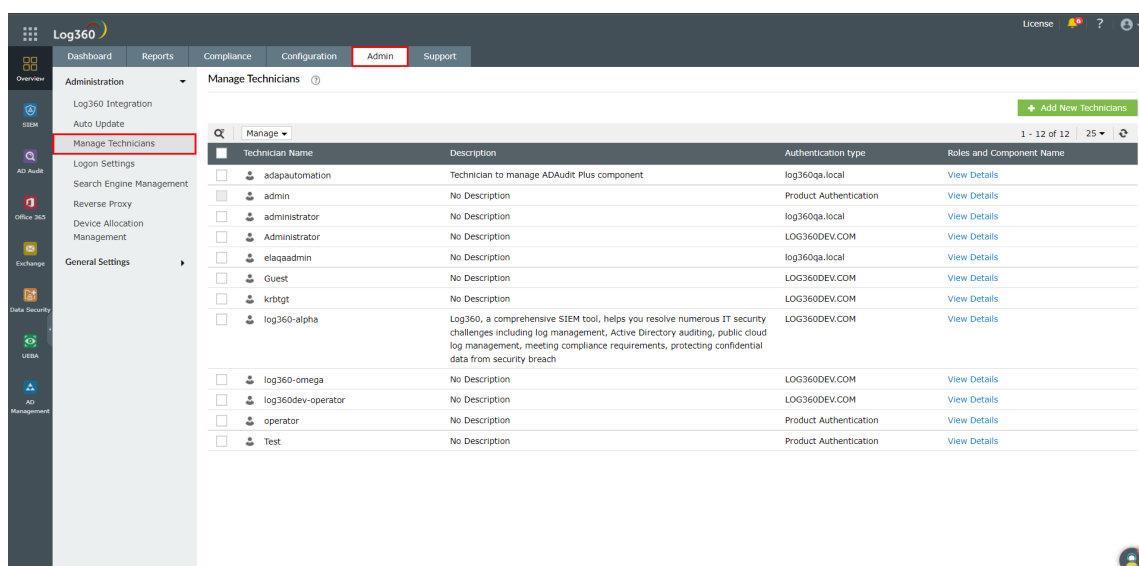
- Click on the **View Details** link under **Roles and Component Name** column corresponding to the required technician.
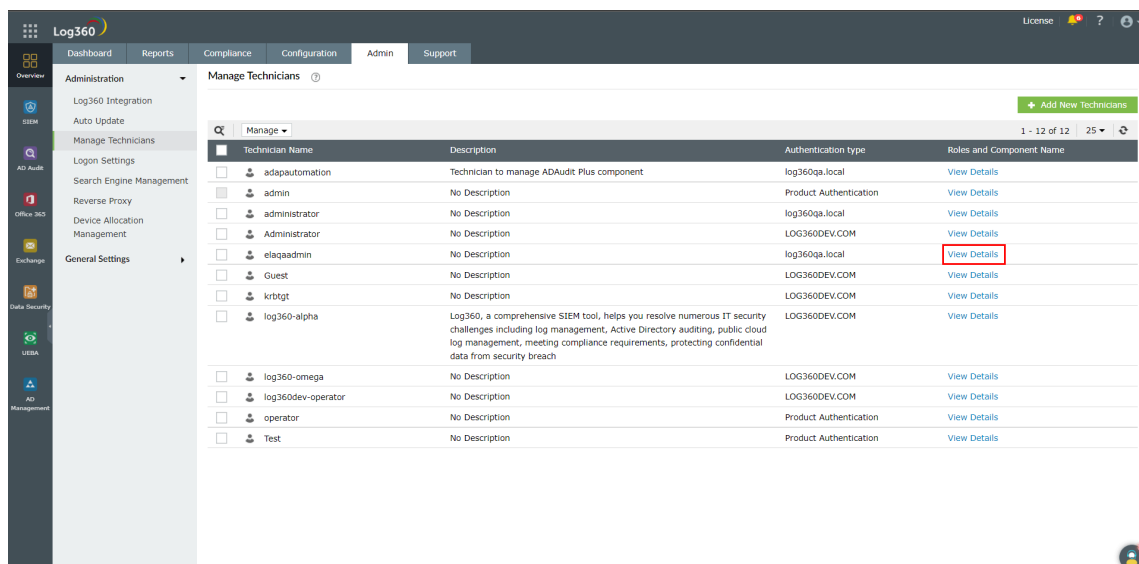
- In the pop-up box that appears, click on the ✅ or 🚫 icon under the **Action** column of the corresponding component to enable/disable it.
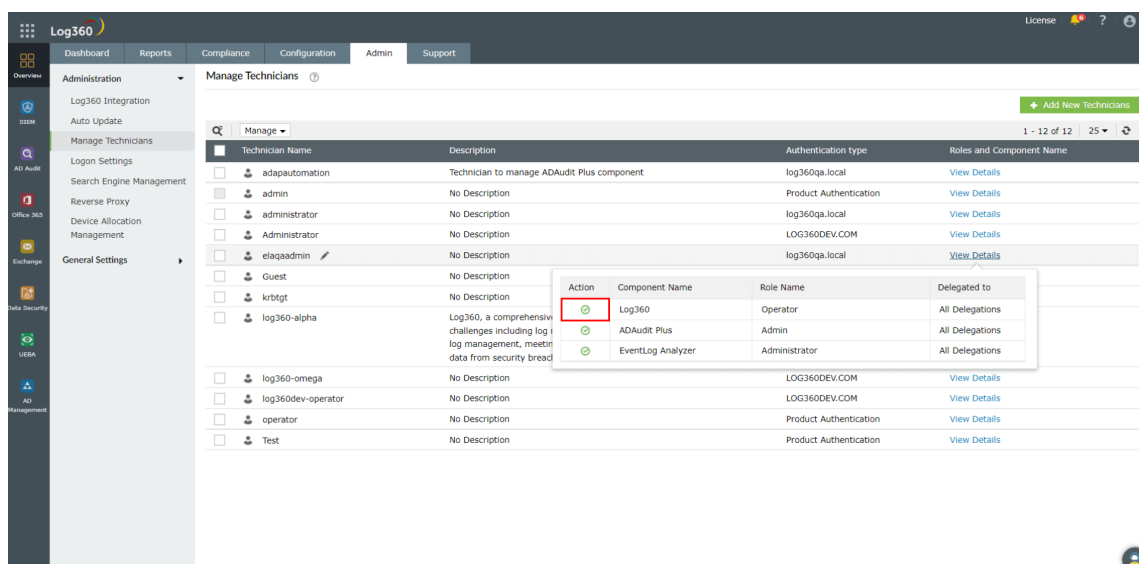
- The component is now enabled/disabled for the technician.

Log360 component versions that support centralized technician management

The following are the components that support the centralized technician management feature.

- ManageEngine ADAudit Plus (from build number 7009)
- ManageEngine EventLog Analyzer (from build number 12214)
- ManageEngine Cloud Security Plus (from build number 4130)
- ManageEngine Exchange Reporter Plus (from build number 5615)
- ManageEngine DataSecurity Plus (from build number 6061)
- ManageEngine Log360 UEBA (from build number 4033)
- ManageEngine M365 Manager Plus (from build number 4502)
- ManageEngine AD Manager Plus (from build number 7130)

> **Note**: Centralized Technician Management is not supported by PAM360

Management of technicians from the component

Though each component of Log360 has its own technician management settings, the technicians are advised to be managed from the centralized technician page. This is because you get a more comprehensible overview of the different technicians and their roles in different components when you look at them from the centralized dashboard.

> **Note**: Addition of non-domain technicians from a component product will not synchronize with Log360. Please add non-domain technicians from Log360's centralized technician management dashboard.

Frequently Asked Questions

1. What happens to the technicians which were existing/created in the components?

The domain technicians will be synced with Log360. The user will also have operator privilege in Log360.

For M365 Manager Plus, existing technicians available during bundled licensing will have operator extended role, which is also the bundled role. Upon purchasing a full license, you can change roles of existing users.

2. What will happen to the technicians that are modified directly in the component's console ?

The changes would be synced with Log360. This does not include changes made to passwords.

4. I have created a Product Technician in component products, but I am not able to view it in Log360 Technician page.

Product Authenticated technicians created in component will not be synced to Log360. Only AD Technicians created in component will be synced to Log360. You can create Product Technician from Log360 console.

4. Why are only a few roles shown in Add/Edit technician page for M365 Manager Plus, Exchange Reporter Plus and Active Directory Manager Plus?

When M365 Manager Plus, Exchange Reporter Plus and Active Directory Manager Plus are in the limited version, only Operator Extended, Log360User, and Super Admin Limited role can be managed respectively. Other roles can be managed only in the full version which you can upgrade to here:

- M365 Manager Plus
- Exchange Reporter Plus
- Active Directory Manager Plus

5. Why does ADManager Plus (ADMP) have only 25 technician limit in the limited edition?

In order to upgrade the technician limit in ADMP, you need to have the full version of the product. You can upgrade to the full version here: Active Directory Manager Plus

Troubleshooting

1. The component product has been updated to the required build version but an error message is shown.

- Under the **Admin** tab, navigate to **Administration → Log360 Integrations**.
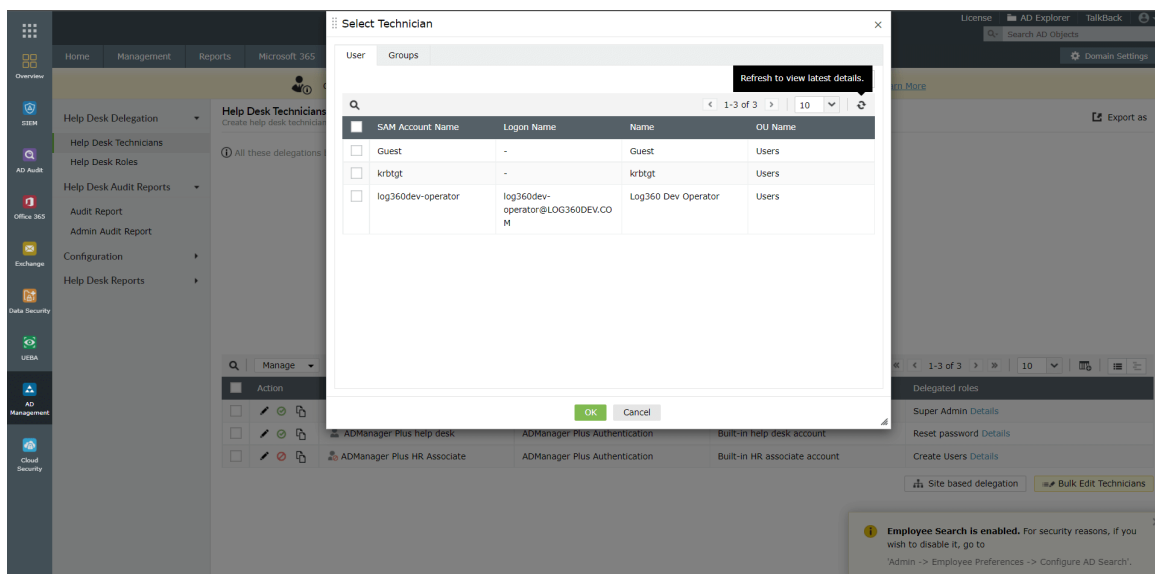- Update the integration settings for the required component.

2. The technicians, roles, and delegations are not in sync.

- Under the **Admin** tab, navigate to **Administration → Log360 Integrations**.
- Update the integration settings for the required component.

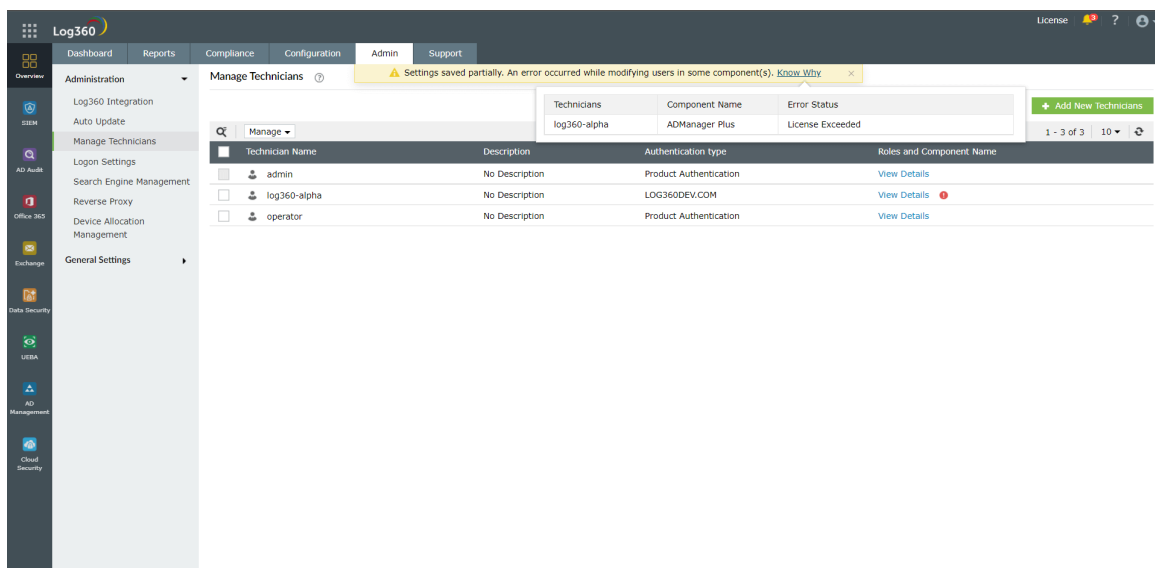## 3. Error status returns -'AD user not found' or 'User not discovered'
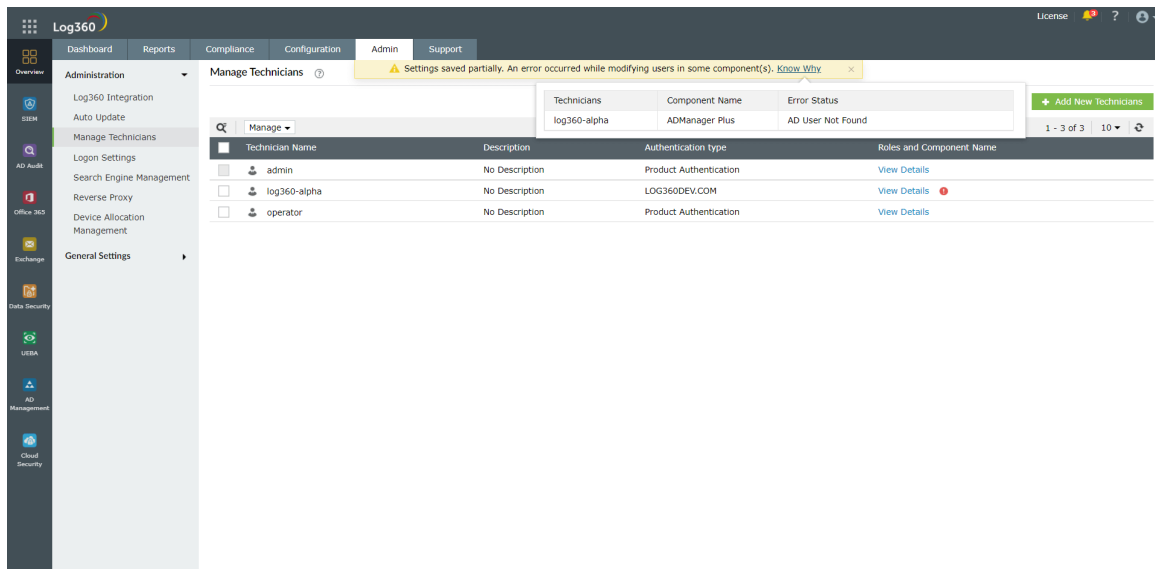
Solution:

- Go to the **delegation tab** inside the product.
- Refresh the AD user selection

4. Error status returns 'License Exceeded' when you add more technicians.

- Upgrade your license to add more technicians

  You can upgrade your license here:

  - [M365 Manager Plus](#)
  - [Active Directory Manager Plus](#)

5. Error returns 'unable to communicate with the component.

- Under the **Admin** tab, navigate to **Administration → Log360 Integrations**.
- Update the integration settings for the required component.

6. Error status returns 'Unknown Error Occurred'
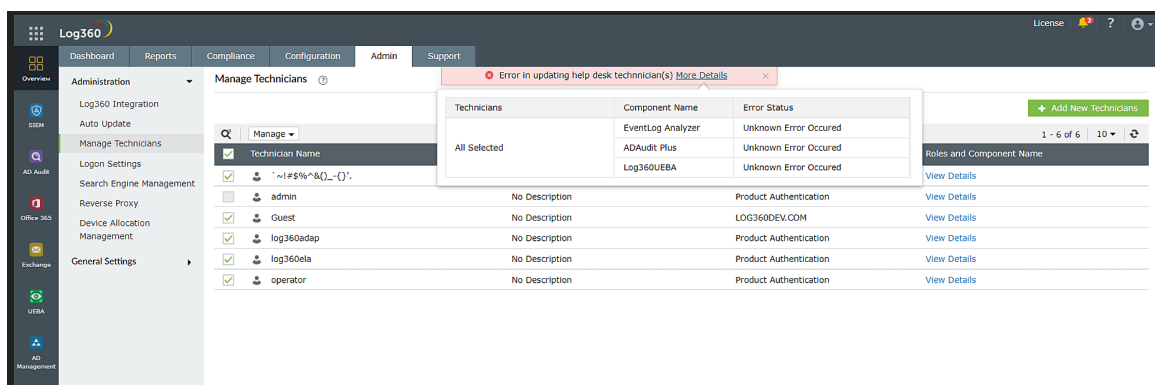
- Contact [Log360 support](#) in case this error occurs.

7. Error returns 'No products are integrated'.

- Under the **Admin** tab, navigate to **Administration → Log360 Integrations**.
- Next, integrate any supported product.

8. Error returns 'No products are supported'.

- Check if the integrated product is in its latest/supported version.
- Next, check if the integrated product belongs to the following build numbers.
  - ELA - 12214
  - UEBA - 4033
  - ADAP - 7009
  - M365 - 4502
  - DSP - 6061
  - ERP - 5615
  - CSP - 4130

- ADMP - 7130

6.2.5.1. Logon Settings

Learn how to configure the following logon settings.

- General: Learn how to enable CAPTCHA in the login page, block users after a certain number of invalid login attempts, and hide the **Forgot password?** link in the login page.
- Single Sign-On: Learn how to configure Single Sign-On to allow users who are already authenticated with their Windows domain to automatically log into Log360.
- Smartcard Authentication: Learn how to configure Log360 to authenticate users through smart cards, bypassing other first factor authentication methods.
- Two-factor Authentication: Learn how to enable two-factor authentication for users logging into Log360.
- Allow/restrict IPs: Learn how to allow or restrict access to Log360 and its integrated components based on the users' IP address.

6.2.5.2. General logon settings

Under the General tab of Logon Settings, you can configure the following settings.

- CAPTCHA Settings
- Block Users Settings
- Other Settings

CATPCHA Settings

Login CAPTCHA serves as a security measure against bot-based brute force attacks. Enabling this setting will display a CAPTCHA image on the login page. End-users must enter the characters shown in the CAPTCHA image to log into the Log360 web portal.

You can configure whether to always show CAPTCHA or only after a certain number of invalid login attempts. Apart from the CAPTCHA image, you can also enable Audio CAPTCHA to assist visually impaired users.

Steps to enable CAPTCHA

1. Log into Log360 as an administrator.

2. Navigate to **Admin → Administration → Logon Settings**, and click the **General** tab.

3. Select the option **Enable CAPTCHA on the login page.**

4. Select **Always show CAPTCHA** if you want users to go through CAPTCHA verification every time they login.

5. Select **Show CAPTCHA after invalid login attempts** if you want only those users who failed at login to go through the CATPCHA verification process.

   - Enter the number of invalid login attempts after which the CAPTCHA verification should appear.

   - Enter the threshold (in minutes) to reset the invalid login attempts. After the specified time period, the invalid login attempts will be reset.

   - **Illustration**: Consider the following limits:

     - Invalid login attempts limit **'3'**

     - Reset the invalid attempts limit after **'30'** minutes

   - In the above illustration, if a user fails to login 3 times consecutively in a 30-minute time interval, then a CATPCHA image will be displayed. The user now has to enter the correct credentials, plus the characters shown in the CAPTCHA image, to successfully log into Log360.

6. Select **Enable Audio CAPTCHA** to assist visually impaired users.

   Note: When audio CAPTCHA is enabled, only digits will be shown in the CAPTCHA image. If a browser doesn't support audio CAPTCHA, then the default CAPTCHA image (with letters and digits) will be shown.

7. Click **Save Settings.**

Block Users Settings

Using this option you can block users from accessing Log360 after a certain number of invalid login attempts for a defined time interval. A blocked user cannot log into Log360.

Steps to block users

1. Log into Log360 as an administrator.

2. Navigate to **Admin → Administration → Logon Settings**, and click the **General** tab.

3. Select the option **Block users after invalid login attempts.**

   - Enter the number of invalid login attempts after which users should be blocked.

   - Enter the threshold (in minutes) to reset the invalid login attempts. After the specified time period, the invalid login attempts will be reset.

   - Enter the number of minutes users should be blocked.

   - **Illustration**: Consider the following limits:

     - Invalid login attempts limit **'3'** within **'5'** minutes.

     - Reset the invalid attempts limit after **'30'** minutes

   - In the above illustration, if a user fails login 3 times in a 5-minute time interval, then the user will be blocked from logging into Log360 for 30 minutes.

4. Click **Save Settings.**

Other Settings

If you want to hide the 'Forgot Password?' link in the login page, then enable the **Hide 'Forgot Password?' link in login page** option.

6.2.5.3. Single Sign-On

This section allows to configure Single Sign-On, which will allow users who are already authenticated with their Windows domain to automatically log in to Log360.

To enable single sign-on for multiple components and domains, follow the steps listed below

- Navigate to **Admin → Administration → Logon Settings**.
- Mark the check-box **Enable Single-Sign On with Active Directory**.

> **Note**: To enable NTLMv2 SSO for ManageEngine Log360 and the integrated components in builds 5282 and above, you will have to download the Jespa JAR file and add it to the product's lib folder. For more information, click here. If you have already enabled NTLMv2 SSO, you can continue using the feature and no further actions are needed.

- Select the components that you wish to enable single sign-on from the **Select Components** drop-down box.

> **Note**: The component will only be displayed if the component supports single sign-on.

- Select the domains that you wish to enable single-sign on from the **Select Domains** drop-down box.
- Click **Save Settings**.

> **Note**:
> If Log360 is installed as a service, configure the service account with administrator privileges by following the steps listed below.
>
> - Click **Start → run → services.msc**.
> - Locate the service name **Manageengine Log360**.
> - Right click the service and select **Properties → Log On**.
> - Select **This account** and provide the credentials.

To modify existing single sign-on settings

- Navigate to **Admin → Administration → Logon Settings**.
- Click the ✐ icon in the status column against the domain that you wish to modify the settings.
- Enter the **Computer Name** and **Password** in the respective fields. Click on the **Create this computer account in the domain** check-box to create a computer with the entered credentials if it is already not present in the domain.

- Click **Advanced**. If the **DNS Servers** and **DNS Site** are not filled automatically after entering the computer name and password, enter them manually.
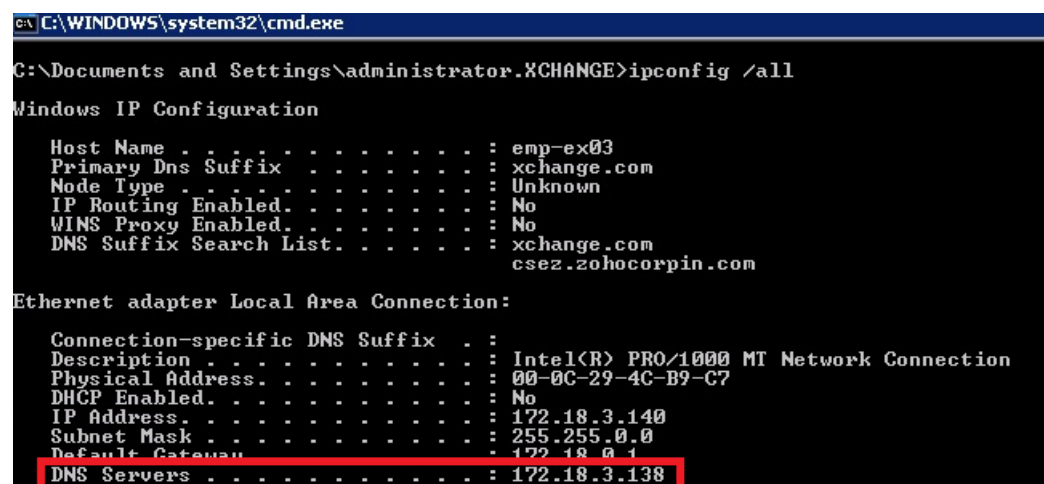- Click **Save**.

To identify the DNS Server IP address:

- Open Command Prompt from a machine belonging to the domain that you have selected
- Type ipconfig /all and press enter
- Use the first IP address displayed under DNS Server

To identify the DNS Site:

- Open Active Directory Sites and Services in Active Directory
- Expand the Sites and identify the Site in which the Domain Controller configured under the selected domain appear
- Use the Site name for DNS Site

See the images below for reference.

Troubleshooting steps for SSO

Please ensure that you have performed the following actions before troubleshooting.

- Ensure that you have added the site to trusted site.
- Ensure that you have added the technician in Log360 for the user which you have logged in your machine.
- Ensure that you were not accessing Log360 Web Client in Workgroup Machine.
- Ensure that you were accessing Log360 Web Client on the machine that belongs to the domain in which you configured SSO.
- Ensure that you were not accessing the Log360 Web Client in Private or Incognito Window.

I. Change browser settings to allow Single Sign-On

Trusted sites are the sites with which NTLM authentication can occur seamlessly. If SSO has failed, then the most probable cause is that the Log360 URL isn't a part of your browser's trusted sites. Kindly add the Log360 URL in the trusted sites list. Follow the steps given below:

1. Microsoft Edge
2. Chrome
3. Firefox

> **Note:**
> 1. It is recommended that you close all browser sessions after adding the URL to the trusted sites list for the changes to take effect.
> 2. Google Chrome and Microsoft Edge use the same internet settings. Changing the settings either in Microsoft Edge or in Chrome will enable NTLM SSO in both browsers. It is again recommended to close both the browser sessions for the changes to be enabled.

Microsoft Edge

1. Open Control Panel → click the **Internet Options** button.

2. In the Internet options dialog box that opens, click the Security tab, and then click a security zone (Local intranet, Trusted sites, or Restricted sites).

3. Click **Sites**.

4. click on the advanced button and add the Log360 site in the list of intranet site.

5. Click **Close**, and then click **OK.**

6. Close all browser sessions and reopen your browser.

Chrome

1. Open Chrome and click the **Customize and control Google Chrome** icon (3 horizontal lines icon on the far right of the Address bar).

2. Click **Settings**, scroll to the bottom and click the **Show advanced settings** link.

3. Under the **Network** section click **Change proxy settings**.

4. In the Internet Properties dialog box that opens, navigate to the **Security** tab → **Local Intranet**, and then click **Sites**.

5. Click **Advanced** and add the URL of Log360 in the list of intranet site.

6. Click **Close**, and then **OK.**

7. Close all browser sessions and reopen your browser.

Firefox

1. Open Firefox web browser and type **about:config** in the address bar.

2. Click **I'll be careful, I promise** in the warning window.

3. In the **Search** field, type: **network.automatic-ntlm-auth.trusted-uris**.

4. Double-click the "network.automatic-ntlm-auth.trusted-uris" preference and type the URL of Log360 in the prompt box. If there are sites already listed, type a comma and then the URL of Log360. Click **OK** to save the changes.

5. Close all browser sessions and reopen your browser.

II. Check the computer account configuration

Status: Error in Creating Computer Account
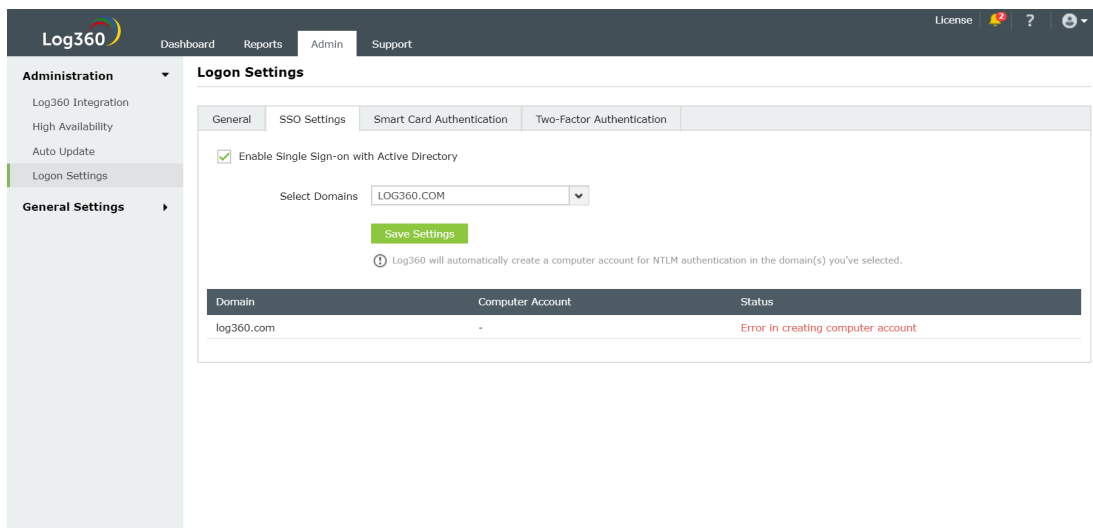
This error can be due to any of the reasons listed below:

1. **Invalid domain credentials in Log360**

   This could happen when the credentials of the user account specified in the domain settings section of Log360 are expired. To update the credentials and synchronize it with Log360, follow these steps:

   - Log into the Log360 web-console with admin credentials.

   - Navigate to the required component using the **Apps Pane** or the **Jump to** link.

   - Click on **domain settings** and update the domain credentials (i.e., username and password).

   - Synchronize the updated domain credentials with Log360 by navigating to **Log360 → Admin** tab and clicking on the **Sync now** button.

2. **Domain controllers are not accessible from Log360**

   When Log360 cannot reach the specified domain controllers (DCs), you must add another DC that it can access. the above error might occur. To do this:

   - Log into Log360 web-console with admin credentials.

   - Navigate to the required component through the **Apps Pane** or the **Jump to** link.

   - Click **domain settings** and specify the name of the relavent DC, and also the credentials of the account that the Log360 should use.

   - Synchronize the updated domain controller with Log360 by navigating to **Log360 → Admin** tab and clicking on the **Sync now** button.

3. **Non-conformance to password policy**

   When the password of the automatically created computer accounts for NTLM authentication does not meet the domain password policy settings, this error occurs. To resolve this issue, you need to create a computer account manually, with a password in accordance with the domain policy settings. To accomplish this, follow the steps given below:

   - Click the error message: 'Error in creating a new computer account', in the status column against the domain in which you wish to create a computer account.

- Create a computer account manually by entering **Computer Name** and **Password.**

6.2.5.4. Smart card Authentication

If you have a smart card authentication system enabled in your environment, you can configure Log360 to authenticate users through it, bypassing other first factor authentication methods.

This feature provides an additional authentication option for Log360 login by enabling the use of smart cards/ PKI/ certificates to grant access to the tool. Smart card authentication strengthens the security further because getting access to Log360 shall then require the user to possess the smart card and know the personal identification number (PIN) as well.

When a user attempts to access Log360's web-interface, they would be allowed to proceed further only after completing smart card authentication in the machine, i.e., by presenting the smart card and subsequently entering the PIN. Log360's web-interface supplements smart card technology with SSL communication. So, the user is prompted to specify the X.509 certificate for getting access.

Users can choose to provide the certificate from the smart card or the local certificate store, in which case Log360 performs the steps to authenticate the user with the certificate. The users can also choose to decline providing the certificate and the tool takes them to the usual login page for authentication.

Steps to configure smart card authentication settings:

- Click the **Admin** tab.
- SSL port must be enabled for configuring smart card authentication settings. To check your SSL port settings, click **Product Settings** provided under **General Settings**. If not enabled already, select the radio button against **HTTPS**, and specify the port number in the field. Click **Save**.
- Navigate to **Admin → Administration → Logon Settings → Smart Card Authentication**.
- In the **Import CA Root Certification** field, click **Browse** and import the required Certification Authority root certification file from your computer. Connect to **http://CertificateAuthorityServerName/certsrv/** to download CA root certification.
- In the **Mapping Attribute in Certificate** field, specify the certificate attribute for mapping. The user details need to be mapped between the smart card certificate and the Log360 database. This denotes that the attribute in the smart card certificate that uniquely identifies the user should match with the corresponding value in the Log360 user database. This mapping involves specifying which attribute in certificate should be taken up for comparison with which attribute in Log360 user store. Log360 provides the flexibility to specify any attribute of the smart card certificate that you feel uniquely identifies the user in your environment. You may choose any attribute among SAN.OtherName, SAN.RFC822Name, SAN.DirName, SAN.DNSName, SAN.URI, email, distinguishedName and CommonName. In case if any other attribute is used to uniquely identify the user in your environment, contact Log360 support to add that attribute.
- In the **Mapping Attribute in AD** field, specify the LDAP attribute that should be matched with the specified certificate attribute. Here you need to specify the particular LDAP attribute that uniquely identifies the user in Log360 user store, e.g., sAMAccountName. During authentication, Log360 reads the value corresponding to the certificate attribute that you specified in Mapping Attribute in Certificate and compares it with the specified LDAP attribute in Mapping Attribute in AD.
- In the **Linked Domains** field, select the appropriate domains from the drop down menu.
- Click the arrow sign next to the section OCSP Settings to expand the menu. During authentication, Log360 checks for certificate revocation status against an Online Certificate Status Protocol (OCSP) server, with details available in the certificate. If the certificate does not have the OCSP information, the information provided in the settings here will be used.
    - In the **OCSP Server Name** field, specify the name of the OCSP server.
    - In the **OCSP Server Port** filed, mention the OCSP server port number.
- Click **Save**.

After you have added a smartcard for authentication, you can perform any of the following functions:

- Add a new smartcard
- Edit a configured smartcard
- Enable/Disable a smartcard
- Delete a configured smartcard

Add a new smartcard

To add a new smartcard, follow the steps given below:

- Navigate to **Admin → Administration → Logon Settings → Smart Card Authentication**.
- Click the **Add a New Smartcard** button at the top-right corner of the screen.
- Enter all details required and click **Save**

Edit a configured smartcard

To edit a configured smartcard, follow the steps given below:

- Navigate to **Admin → Administration → Logon Settings → Smart Card Authentication**.
- Click the ✏ corresponding to the smartcard whose configuration you wish to edit.
- Modify the settings you wish to change.
- Click **Save**

Enable/Disable a smartcard

- Navigate to **Admin → Administration → Logon Settings → Smart Card Authentication**.
- To enable/disable a configured smartcard, click on the 🚫 / ✅ icon located in the action column of the particular smartcard.

Delete a configured smartcard

- Navigate to **Admin → Administration → Logon Settings → Smart Card Authentication**.
- Click the corresponding to the smartcard which you wish to delete.
- Click **Yes** to confirm the deletion.

6.2.5.5. Two-factor Authentication

To strengthen user logon security, Log360 supports two-factor authentication. Once enabled, Log360 will require users to authenticate using one of the authentication mechanisms below in addition to the Active Directory credentials whenever they log in.

- Email Verification
- SMS Verification
- Google Authenticator
- RSA SecurID
- Duo Security
- RADIUS Authentication
- Microsoft Authenticator
- Custom TOTP Authenticator
- Backup Verification Codes

Setting up 2-factor authentication

- Log in to Log360 as an administrator.
- Navigate to **Admin → Administration → Logon Settings**.
- Click the **Two-factor Authentication** tab.
- Toggle the Two-factor Authentication switch to the **ON** position.
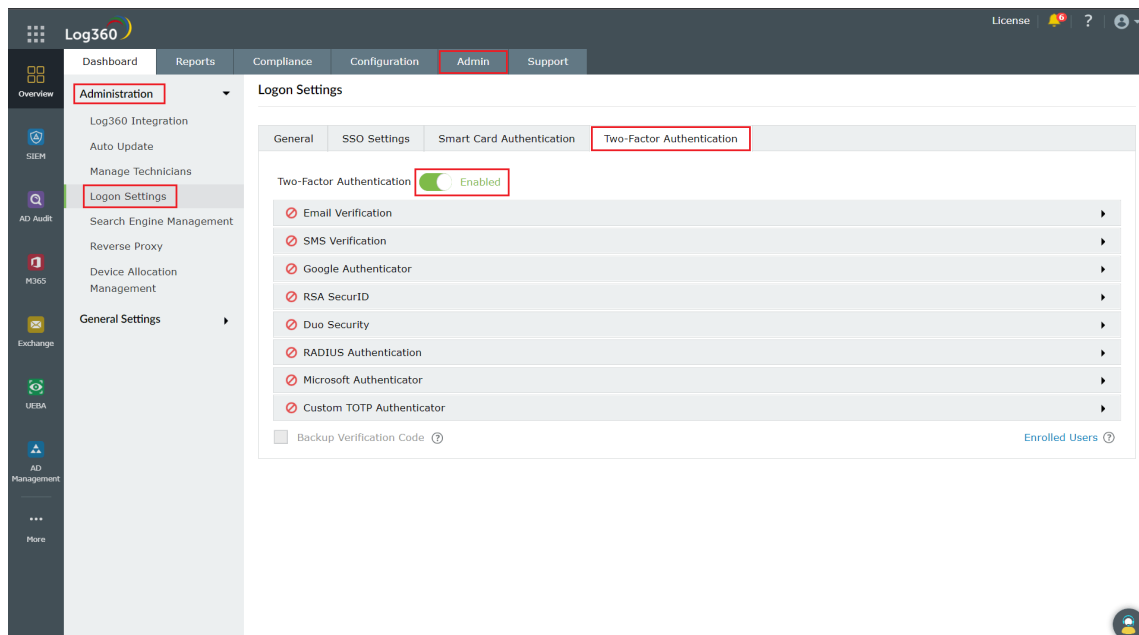
- Select the authentication methods of your choice from the list provided.
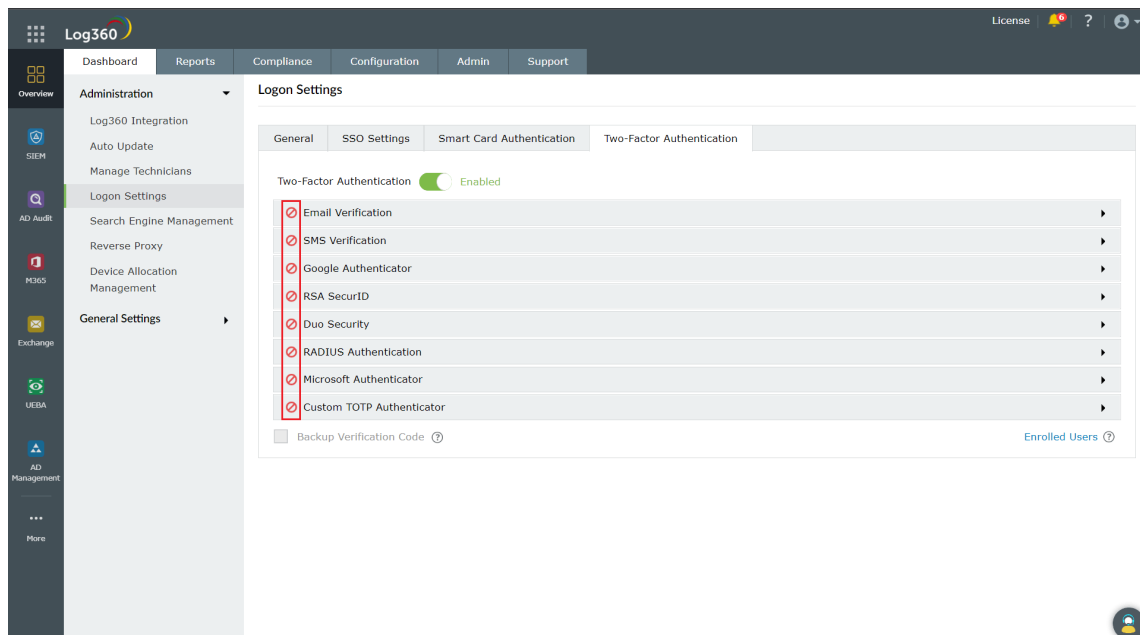
Note:

- If multiple authentication options are enabled, then the user will be asked to choose one at the time of logging in.

- Make sure you configure the authentication option you've chosen by entering all the required details. Click here for the steps.

- Click Save Settings.

Email Verification

When this option is selected, Log360 sends a verification code via email to the user's email address. The user has to enter the verification code to successfully login.

Configuration steps:

- Configure **mail server settings** if not done already.
- Enter a **Subject** for the email.
- Enter the **Message** in the box provided.
- Set the **priority** as per your requirement.
- Click **Macros** link at the bottom to insert them in the email message.
- Once you are done, click **Save Settings**.

Once enabled, users will be asked to enroll for two-factor authentication by entering their email address during login.

SMS Verification

When this option is selected, Log360 sends a verification code via SMS to the user's mobile number. The user has to enter the verification code to successfully login.

Configuration steps:

- Configure **SMS server settings** if not done already.
- Enter the **Message** in the box provided.
- Click **Macros** link at the bottom to insert them in the SMS.
- Once you are done, click **Save Settings**.

Once enabled, users will be asked to enroll for two-factor authentication by entering their mobile number during login.

Google Authenticator

Google Authenticator adds an extra layer of protection to the reset password/unlock account process. Once enabled, users will be required to enter a six-digit security code generated by the Google Authenticator app for identity verification.

Configuration Steps:

- Just click Enable Google Authenticator
- Click **Save Settings**.

Once enabled, users can enroll themselves for two-factor authentication using the Google Authenticator app.

RSA SecurID

RSA SecurID is a mechanism developed for performing two-factor authentication for a user to a network resource. Users can use the security codes generated by the RSA SecurID mobile app, hardware tokens, or tokens received via mail or SMS to log in to Log360.

Configuration steps:

- Log in to your RSA admin console (e.g., https://log360-rsa.testdomain.com/sc).
- Go to **Applications**. Under **Authentication Agents**, Click **Add New**.
- Add Log360 Server as an authentication agent and click **Save**.
- Go to **Access**. Under **Authentication Agents**, click **Generate Configuration File**.
- Download **AM_Config.zip** (Authentication Manager config).
- Extract sdconf.rec from the ZIP file.
- In Log360, under RSA SecurID configuration, click Browse and select the sdconf.rec file.
- Click **Save Settings**.

Once enabled, users will be asked to

Duo Security

If your organization uses Duo Security for two-factor authentication, it can be integrated with Log360 to secure logins. Users can approve or deny the Log360 login requests using a push notification or by entering the six-digit security code generated by the Duo mobile app. Authentication via Duo Security can be configured in two ways in Log360: Web v2 SDK and Web v4 SDK.

Web v2 SDK uses a traditional Duo prompt which will be displayed in an iframe in Log360, whereas Web v4 SDK uses Duo's OIDC-based universal prompt with a redesigned UI that redirects users to Duo for authentication.

> Duo Security has phased out Web v2 SDK, so it is recommended to switch to Web v4 SDK, which features the new Universal Prompt.

Prerequisites

- Add the API hostname and admin console (e.g., https://admin-325d33c0.duosecurity.com) as a trusted site or intranet site in the users' machine if they are using older versions of Internet Explorer.

- Please follow these steps in the Duo Admin Panel to migrate from Web v2 SDK, which uses the traditional prompt, to Web v4 SDK, which employs the new Universal Prompt.

Web v4 SDK configuration steps

> **Note**: It is required to have a secure connection to set up the Web v4 SDK authentication. Please make sure that you have enabled HTTPS connection.
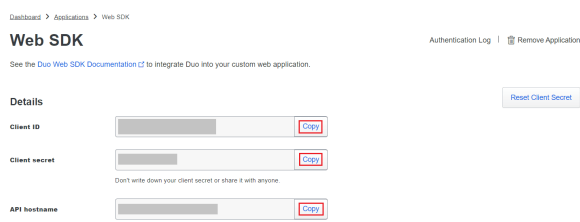
1. Log in to your Duo Security account (e.g., https://admin-325d33c0.duosecurity.com) or sign up for a new account and log in.

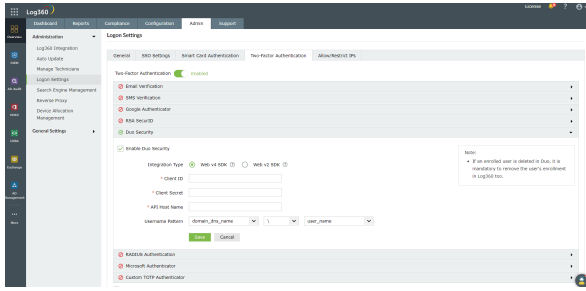2. Go to **Applications** and click **Protect an Application**.
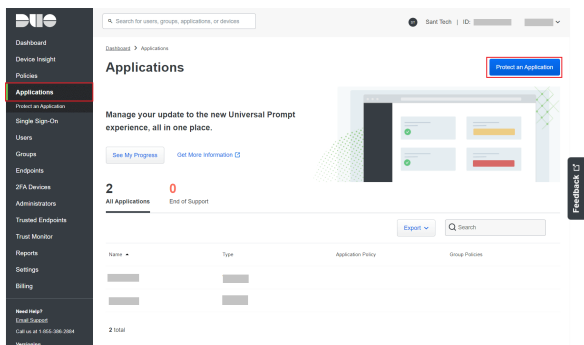
3. Search for Web SDK and click **Protect**.

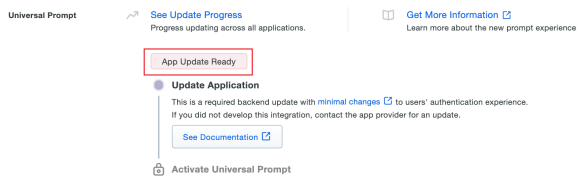4. Copy the **Client ID, Client secret**, and **API hostname** values.

5. In Log360, navigate to **Admin > Logon Settings > Two-Factor Authentication > Duo Security**.

6. Check the **Enable Duo Security** box and select **Web v4 SDK** for **Integration Type**.

7. Paste the Client ID, Client secret, and API hostname obtained from the Duo Admin Panel in the respective fields.

8. Enter the same username pattern used in Duo Security in the **Username Pattern** field.

9. Click **Save**.

Steps to migrate to the new Universal Prompt

1. In the Duo Admin Panel, select the **Web SDK** application, which was previously configured for Log360, and copy the **Integration key, Secret** key and **API hostname** values.

2. Scroll down to the Universal Prompt section. The **App Update Ready** message will be displayed, indicating that Universal Prompt can now be activated for Log360.

3. In Log360, navigate to **Admin > Logon Settings > Two-Factor Authentication > Duo Security**.

4. Click **Web v4 SDK** and paste the Integration key, Secret key, and API hostname values in the **Client ID, Client Secret**, and **API Host name** fields respectively.

5. Once the Web v4 SDK is configured in Log360 and a user authenticates through the frameless Duo v4 SDK, the App Update Ready message in Duo Admin Panel will be updated and the New Prompt Ready message will be displayed.
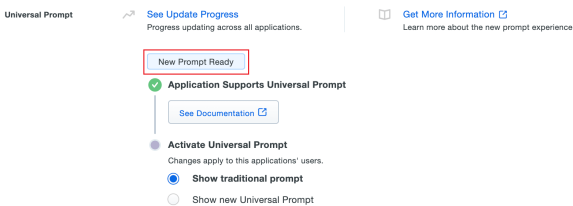
6. Select **Show new Universal Prompt** to activate the universal prompt for Log360.

RADIUS Authentication

Remote Authentication Dial-In User Service (RADIUS) is an industry standard client/server authentication protocol that enhances security by protecting networks from unauthorized access.

RADIUS based two-factor authentication for Log360 can be configured in just two simple steps.

Configuration Steps:

Step 1: Integrate RADIUS with Log360

- Log in to RADIUS server.
- Navigate to clients.conf file.(/etc/raddb/clients.conf).
- Add the following snippet in the clients.conf file.

```
> client Log360ServerName
  {
  ipaddr = xxx.xx.x.xxx
  secret = <secretCode>
  nastype = other
  }
```

- Restart RADIUS server.

Step 2: Configure Log360 for RADIUS

- Select **RADIUS Authentication** option.
- Enter the **IP address or the name of the RADIUS** server.
- Enter the **port number** for RADIUS authentication.
- Select the **protocol** used for RADIUS authentication from the drop-down list.
- Provide the **security key** that was added to the clients.conf file in RADIUS server.
- Set the **RADIUS user name pattern**.
- Set a duration for authentication request time-out duration.
- Click **Save Settings**.

Note: Username Pattern is case sensitive. Please make sure you select the exact pattern (uppercase or lowercase) you use in your RADIUS server.

Microsoft Authenticator

Administrators can add Microsoft authenticator as an additional factor for verifying identities during login.

Configuration Steps:

- Click **Enable Microsoft Authenticator**.
- Click **Save Settings**.

Once enabled, users can enroll themselves for two-factor authentication using the Microsoft Authenticator app when they log in to the application.
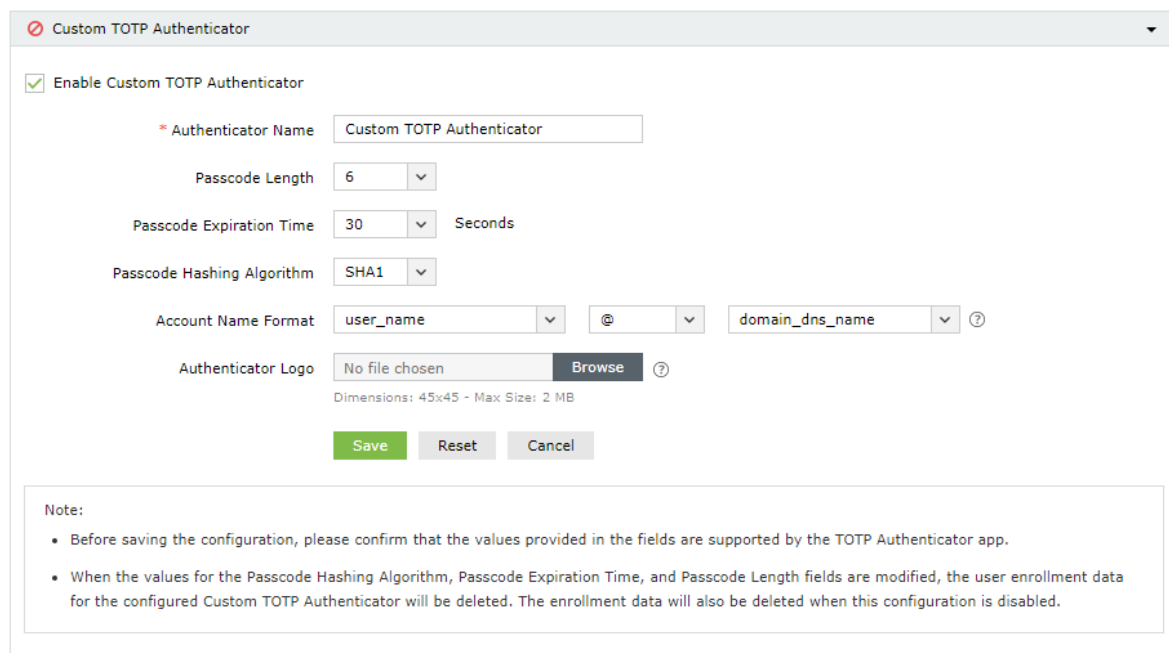
Custom TOTP Authenticator

In addition to the authenticators mentioned above, you can also add a custom TOTP authenticator as a means of verifying identities, provided the application satisfies the following criteria:

- The application can provide passcodes of varying lengths (6, 7, or 8 characters).
- The application supports any password hashing algorithm that Log360 utilizes (SHA1, SHA256, and SHA512).

Configuration steps:

1. Select **Enable Custom TOTP Authenticator**.
2. Enter the name of the authenticator application.
3. Select the **Passcode Length** and the **Passcode Expiration Time** from the available options.
4. Select the **Password Hashing Algorithm** of the TOTP authenticator.
5. Provide the format in which the username will be displayed in the authenticator.
6. Select the logo of the authenticator. The supported formats for the image are PNG, JPG, JPEG, BMP, and GIF. Please ensure the dimensions of the logo does not exceed 45x45 pixels and the size is less than 2MB.
7. Click **Save**.

Note: If the values for the passcode hashing algorithm, passcode expiration time, or the passcode length fields are modified, the user enrolment data for the configured custom TOTP authenticator will be deleted. The enrolment data will also be deleted when this configuration is disabled.

Once enabled, users can enrol themselves for two-factor authentication using the Custom TOTP Authenticator when they next log in to Log360.

Backup Verification Codes

Backup verification codes allow users to log in when they don't have access to their phone or face issues with one of the second-factor authentication method. When enabled, a total of five codes will be generated. A code once used will become obsolete and cannot be used again. Users also have the option to generate new codes.

Enabling backup verification code

- To enable backup verification code, put a check against the **Backup Verification Code** box.
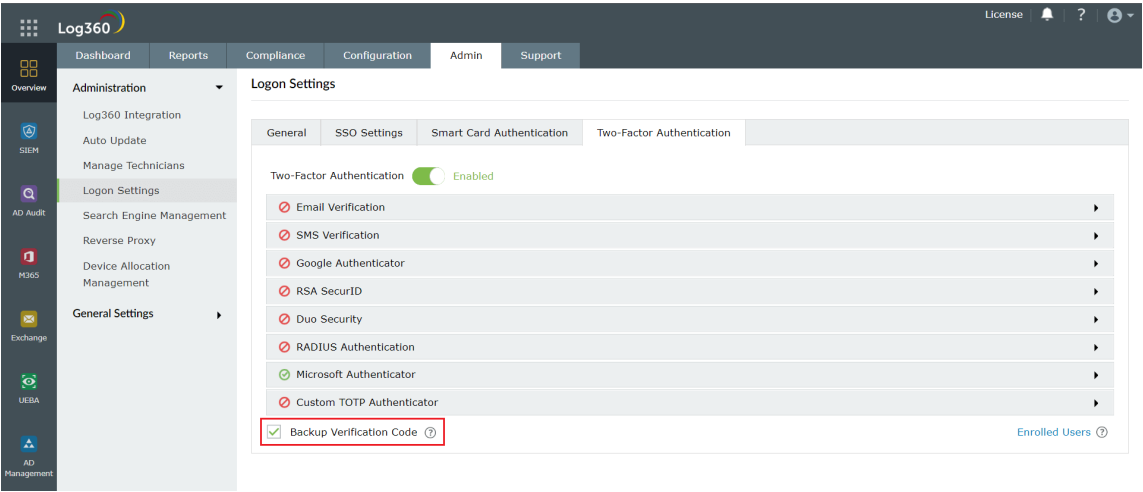
Registering for backup verification code

- Once enabled, users will be notified to configure their codes when they log in to Log360. On clicking **Configure Now**, they will be taken to the two-factor authentication settings page.
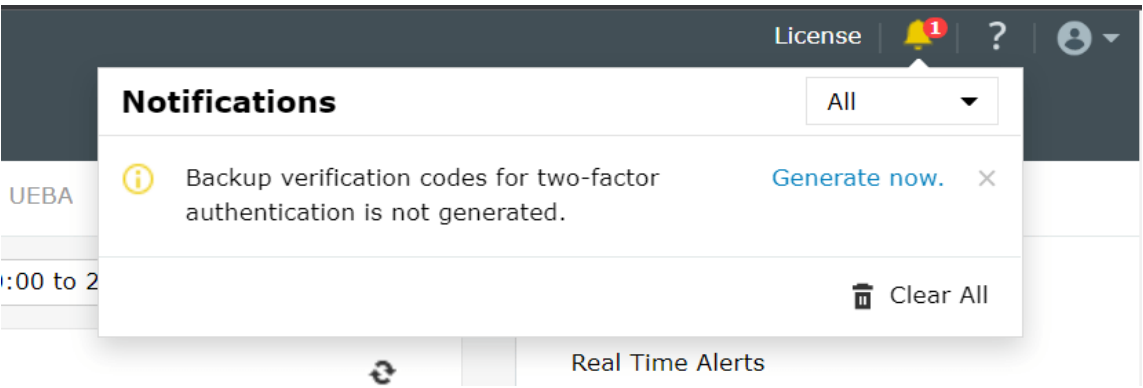
- Users need to click the **Manage Backup Verification Codes** link to view the codes.
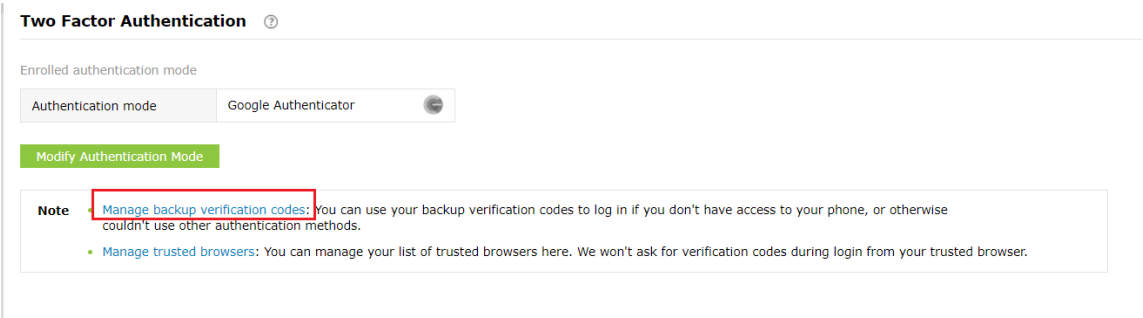
- Users can also download the codes as a text file, print them, get it delivered to their personal email address, or generate new codes.

Using the backup verification code to login

- To use backup verification codes during login, users need to click the **Use backup verification codes** link in the second-factor authentication page.

- In the backup verification code page, they need to enter one of their backup verification codes and click **Verify Code** to login.

Backup Verification Code

You can use your backup verification codes to log in, if you have don't have access to your phone, or otherwise couldn't use other authentication methods.

po9esdxgg9g7

☐ Trust this browser

We won't ask you to verify your account with codes for this browser on this computer for the next 180 days.

Verify Code   Back

Managing users for two-factor authentication

As an admin, you can view which authentication method users have enrolled for and remove users' enrollment for two-factor authentication using the Manage Users option.

To do so, follow the steps below:

- Under the **Two-factor Authentication** tab, click **Enrolled Users**.
- In the TFA Enrolled Users pop up, you can view the list of users enrolled for two-factor authentication and the authentication method they have chosen.
- To remove a user, select the user and click the Delete icon.

To personalize two-factor authentication method for domain users

Domain users enrolled for two-factor authentication can modify their preferred authentication method and manage trusted browsers by following the steps below:

- Go to the My Account profile icon at the top left corner.
- Select the Two Factor Authentication option.
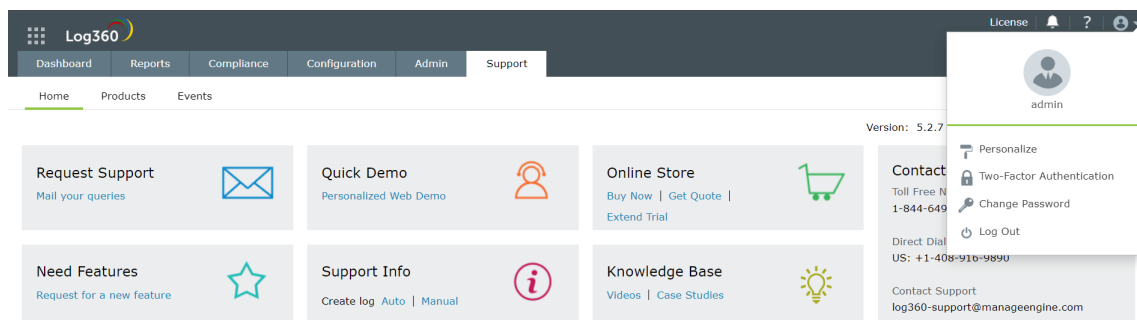
- To modify authentication mode, click **Modify Authentication mode**.
- To manage trusted browser, click **Manage Trusted Browsers**.

6.2.5.6. Allow/restrict IP addresses

One way to make Log360 and its integrated components more secure is by allowing or restricting inbound connections to specific IPs or IP ranges. This adds an additional layer of security by allowing connection from only trusted sources and blocking unwanted and malicious traffic.

The IP restriction can be applied for the entire product, specific URLs within the product, or APIs.

Controlling access to the product

1. Navigate to **Admin → Administration → Logon Settings**.

2. Click the **Allow/Restrict IPs** tab.

3. Under the **Actions** column, click the [🚫] icon to enable IP restriction.
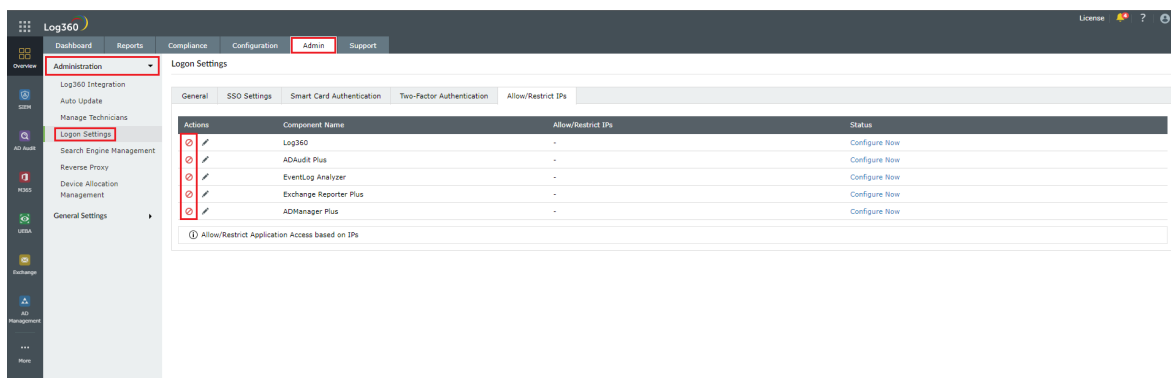
4. In the pop-up that appears, select the **Allowed IPs** or the **Restricted IPs** option.

5. Based on your requirements, **enter the desired IP addresses**.

   - **Adding multiple IP ranges**: Click [＋] icon if you want to allow or restrict access to multiple IP address ranges.

   - **Allow/restrict individual IPs**: Click **Add Individual IPs** if you want to allow or restrict access to individual IP addresses. You can add multiple individual IP addresses by separating the values using comma.

6. Refer to the Appendix for more information.

7. Finally, click **Save** to save the settings.

8. If you have changed the 3rd party reverse **proxy settings** of Log360 or any of its integrated components for which you are enabling IP-based restriction, then:

    - **Add the following line to the server.xml file** (default location: <InstallationDirectory>/conf/server.xml).

9. <Valve className="org.apache.catalina.valves.RemoteIpValve" internalProxies="192\.168\.0\.10|192\.168\.0\.11" trustedProxies="172\.168\.0\.10|176\.168\.0\.11" />

    - Edit the values of **internalProxies** and **trustedProxies** as per your environment.

    - Enter IP address while specifying the values for internalProxies and trustedProxies, and use the vertical bar (|) character to enter multiple values.

    - Restart for the changes to take effect.

    - Repeat these steps for the integrated components as well.

Controlling access to APIs and product URLs

1. Navigate to **Admin → Administration → Logon Settings**.

2. Click the **Allow/Restrict** IPs tab.

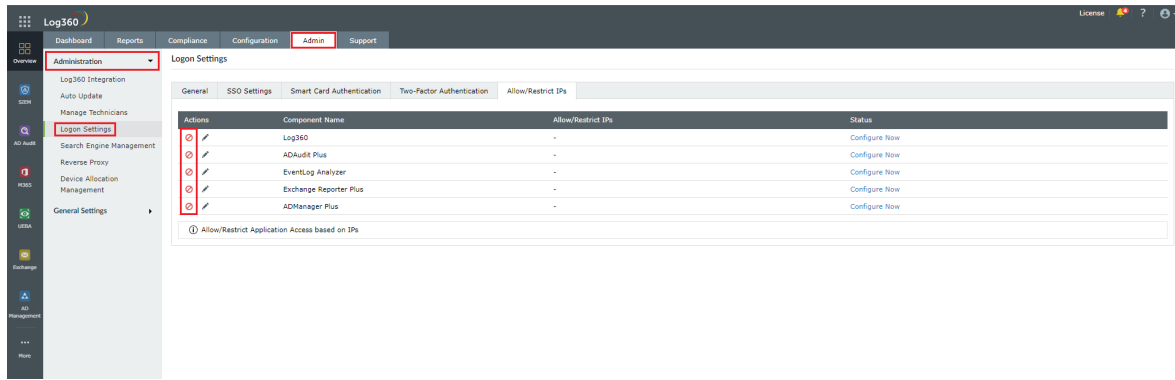3. Under the **Actions** column, click the [🚫] icon to enable IP restriction.

4. In the pop-up that appears, check the **Enable API/URL Access for Selected IPs** box.

5. Enter the **API/Product URLs** in the box provided.

6. Sample URL paths: /Admin.do, /Configuration.do, /Dashboard.do

   Sample API paths: /RestAPI/WC/Integration, /RestAPI/WC/LogonSettings

> **Note**:
> - Use * as a wildcard character to restrict access to a broader range of APIs or URLs. For example, use /RestAPI/WC/.* to restrict all API calls that start with /RestAPI/WC/.
> - The API/URL path should start with /. For example, /Admin.do and /RestAPI/WC/.
> - Enter only the path of the API or URL. For example, if the entire product URL is https:testserver:8095/Admin.do, then enter only /Admin.do.
> - Only alphanumeric characters (A-Z, a-z, 0-9) and the following special characters are allowed: period (.), forward slash (/), and asterisk (*).

7. **Enter the IP addresses** as per your requirement. Click [+] icon if you want to allow access to multiple IP address ranges.

8. Finally, click **Save** to save the settings.

9. If any changes are made to 3rd party reverse proxy for Log360, or any of its integrated components, then:

   - Add the following line to the **server.xml file** (default location: <InstallationDirectory>/conf/server.xml).

10. <Valve className="org.apache.catalina.valves.RemoteIpValve"

    internalProxies="192\.168\.0\.10|192\.168\.0\.11"

    trustedProxies="172\.168\.0\.10|176\.168\.0\.11" />

    - Edit the values of **internalProxies** and **trustedProxies** as per your environment.

    - Enter IP address while specifying the values for internalProxies and trustedProxies, and use the vertical bar (|) character to enter multiple values.

    - Restart Log360 for the changes to take effect.

    - Repeat these steps for the integrated components as well.

> **Note**:
>
> - The purpose of configuring InternalProxies and TrustedProxies is to determine which IP addresses are regarded as internal or trusted. By configuring these settings, organizations can improve their network security by controlling the access and use of IP addresses within their network.
>
> - InternalProxies are IP addresses that are trusted and from within the organization network. These IP addresses are typically used by internal services, such as printers and servers.
>
> - TrustedProxies are IP addresses that are external to the network but still maintain a high level of trust and reliability. These IP addresses are typically associated with external services like websites and databases.

Managing IP restriction

You can also make the following changes to this setting:

- **Disable/enable IP-based restriction**: Use the icon under the Actions column to enable or disable IP-based restriction. [⊘] icon means IP-based restriction is enabled for a component and [⊘] icon means IP-based restriction is disabled.

- **Edit IP-based restriction settings**: Click [✎] icon to add, delete, or edit the IP ranges and individual IP addresses.

- **Summary details**: Click the link under the Allow/Restrict IPs column to view the IPs that are allowed or restricted from accessing a component.

Appendix

- **Use * as wildcard character**: Individual IP addresses can include wildcard characters, so that all addresses within a certain class of address will be restricted. For example, denying access to address 192.168.2.* would restrict access to all addresses within that subnet.

- You can also enter **hostname** instead of IP addresses.

- You can allow or restrict only IPv4 addresses. **IPv6** is **not supported**.

- The Remote Integrated Child Components (RICC) server IP address cannot be restricted in Log360

- The implementation of IP restriction for forward proxy is not supported.

- After initially configuring IP Restriction or Reverse Proxy in Log360, manual restart of the child products is necessary.

- When the child products are installed remotely and the Reverse Proxy is set up in Log360, manually add the parent product server's IP as an internal proxy in the child product. Following this, manually restart the child products.

6.2.6. Search Engine Management

Elasticsearch is a distributed, RESTful search and analytics engine. When configured in Log360 it distributes data between the nodes that are added thereby optimizing disk space and also improving the performance of Log360.

> **Note**: Search Engine Management does not support EventLog Analyzer on Linux servers.
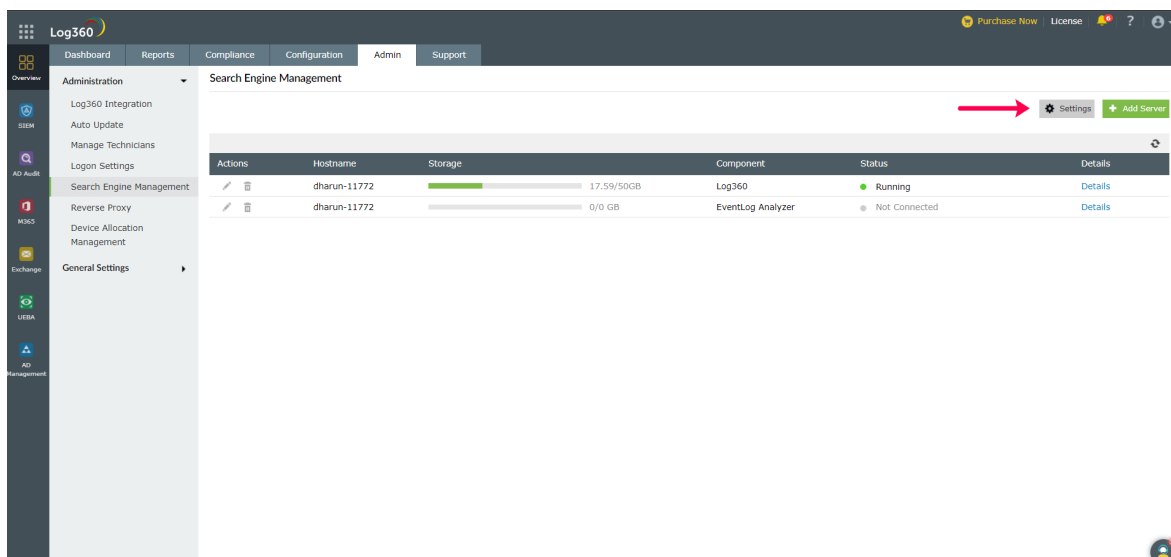
Search engine Settings

How to disable or enable ES auto restart

- If Auto Restart is enabled, starting Log360 will restart the child nodes and allow the child nodes to join Log360's cluster.
- Auto Restart can only be used when EventLog Analyzer is integrated with Log360. Also, the feature is enabled by default and it can be turned off if required.

Steps to disable/enable auto restart:

1. Open **Admin → Search Engine Management → Settings**

2. Disable Auto restart by disabling **Enable auto-restart for the configured product's node** option in **Settings** and click **Save**.
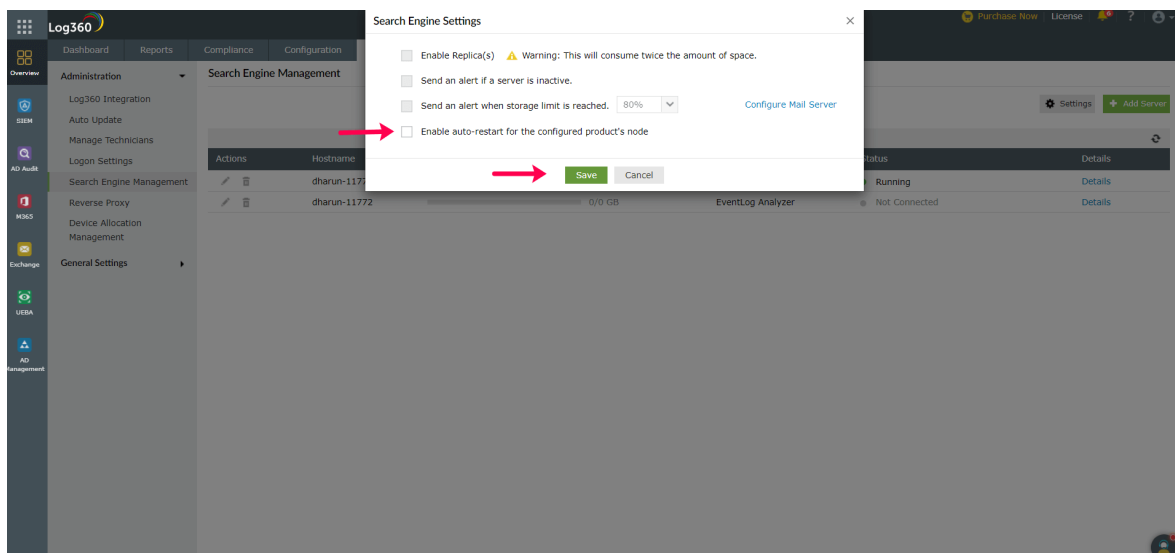
3. Once you click **Save**, auto restart is disabled. You can follow the same steps to enable auto restart.
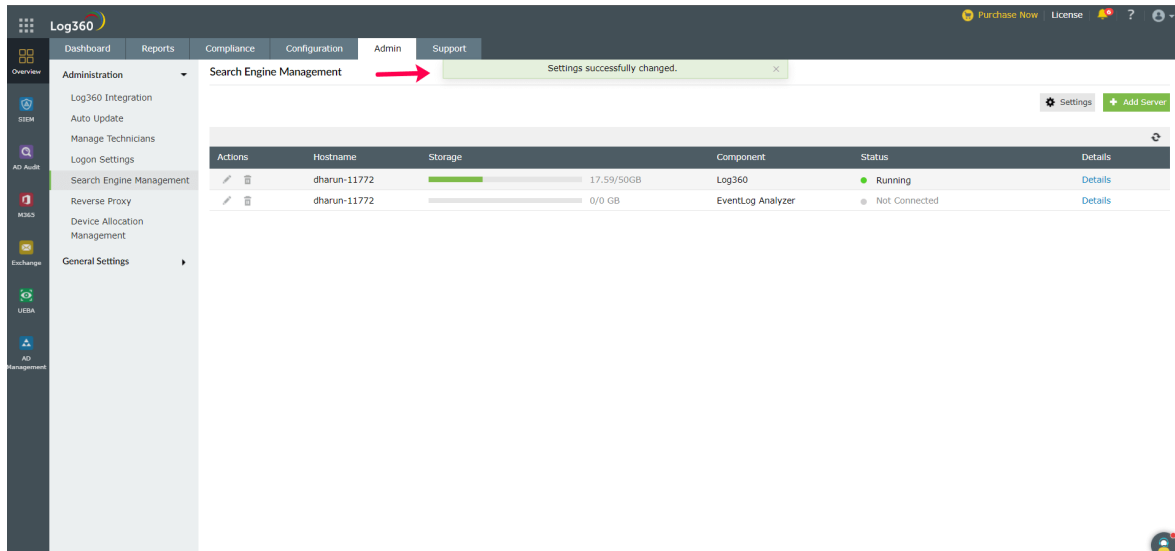
Actions on nodes

- **Adding a node**: Helps in the distibution of log storage as data will be split and stored between the nodes.
- **Starting a node**: The Elasticsearch service is started in the added node and the node then connects to the Log360 server.
- **Stopping a node**: The Elasticsearch service running in the machine is stopped and data present in the node will not be accessible when the node isn't connected.
- **Deleting a node**: Data is removed from the node and the node is deleted.

Prerequisites

1. Increase file descriptors

Make sure to increase the limit on the number of open files descriptors for the user running Elasticsearch to 65,536 or higher. For the .zip and .tar.gz packages, set **ulimit -n 65536** as root before starting Elasticsearch, or set **nofile** to **65536 in /etc/security/limits.conf**.

> **Note:** This is applicable only for Linux and macOS.

2. Ensure sufficient virtual memory

Elasticsearch uses a mmapfs directory by default to store its indices. The default operating system limits on mmap counts is likely to be too low, which may result in out of memory exceptions.

You can increase the limits by running the following command as root in Linux: **sysctl -w vm.max_map_count=262144**

3. Disable swapping

Usually Elasticsearch is the only service running on a box, and its memory usage is controlled by the JVM options. There should be no need to have swap enabled.

On Linux systems, you can disable swap temporarily by running: **sudo swapoff -a**

On Windows, the equivalent can be achieved by disabling the paging file entirely by going to **System Properties > Advanced > Performance > Advanced > Virtual memory**.

4. Ensure sufficient threads

Elasticsearch uses many thread pools for different types of operations. It is important that it can create new threads whenever needed. Make sure that the number of threads that the Elasticsearch user can create is at least 4096.

This can be done by setting **ulimit -u 4096** as root before starting Elasticsearch, or by setting **nprocto 4096 in /etc/security/limits.conf**.

5. JVM DNS cache settings

Elasticsearch runs with a security manager in place. With a security manager in place, the JVM defaults to caching positive host name resolutions indefinitely. If your Elasticsearch nodes rely on DNS in an environment where DNS resolutions vary with time, then you might want to modify the default JVM behavior. This can be modified by adding **networkaddress.cache.ttl=<timeout>** to your Java security policy.

6. Port availability

Ensure that **port 9322** is available on the machine that will run Elasticsearch.

7. Sharing of <Installation Dir>/EventLog Analyzer/ES/repo

Ensure that the folder **<Installation Dir>/EventLog Analyzer/ES/repo** is shared with the service account of the Log360 server. This folder will be used to create snapshot from Elasticserch to save archives. If the Log360 server is not in AD, it will be an open share or else make sure that the user has the permission to share the folder and follow the steps below.

1. Share the folder **<Installation Dir>/EventLog Analyzer/ES/repo** manually with the Log360 server.

2. Copy the shared path of **<Installation Dir>/EventLog Analyzer/ES/repo** directory.

3. Navigate to **<Installation Dir>/EventLog Analyzer/ES/config/dae.properties** file and specify the copied path as the value for **node.repo.sharedlocation**.

4. Restart the EventLog Analyzer server.

Setting up Elasticsearch

By default, uses self-signed certificates Elasticsearch security i.e authentication and encryption. If you want to use your own certificates for security, follow the steps below.

- First make sure you have a client, node, and root certificate in the PEM format.
- Rename the certificates and their corresponding keys as follows.
    - Client certificate to **client.pem** and its key to **client.key**
    - Node certificate to **localnode.pem** and its key to **localnode.key**
    - Root certificate to **root_ca.pem** and its key to **root_ca.key**
- Now, go to /ES/config and open the **dae.properties** file.
- Change the value of the parameter **use_custom_certificates** to true.
- In **/ES/config/certificates**, check if the following files exist. If they do exist, delete them.
    - client.key
    - client.pem
    - localnode.key
    - localnode.pem
    - root_ca.key
    - root_ca.pem
- Then, copy your certificates to **<Log360_Home>/ES/config/certificates**
- Now, go to **<Log360_Home>/ES/bin** and run the **verifyCertificates.bat** file.
- If you receive a message saying **Certificate Validation Done**, start the server. If you do not get the message, contact support at log360-support@manageengine.com

Setting up certificates for existing nodes

Follow the steps below to replace the certificates in the existing nodes:

- Go to the machine and then stop the elasticsearch service by opening the **taskmanager>services**.
- Move the certificates to **<INSTALLAITON DIR>\ES\config\certificates**
- Navigate to **<INSTALLAITON DIR>\ES\config**, open the **elasticsearch.yml** file and replace the following line with the respective details in both the **nodes.dn** and **admin_dn**

    CN=*.node,OU=none,O=none,L=none,ST=US,C=US
- Restart the service.

Configuring Elasticsearch in Log360

To configure Elasticsearch in Log360, follow the steps mentioned below.

1. Login to Log360.

2. Navigate to **Admin > Administration > Search Engine Management**.

3. Click on **Add Server**.

4. In the Add Server drop box, enter the server details and the path to installation directory along with TCP port (optional).

5. Click Save.

6.2.7. Securing your SEM nodes

A bug found in the Log4j library can allow an attacker to execute arbitrary code on your system. Therefore if the SEM nodes are added, please follow the steps given below to fix the log4j vulnerability:

1. Stop the Elasticsearch service (**elasticsearch-service-x64** or **elasticsearch-service-x86**) from services.msc.

2. Copy the following files from elasticsearch folder (**<Installation dir>/Log360/../elasticsearch/ES/lib**)

   - **log4j-1.2-api-2.15.0.jar**

   - **log4j-api-2.15.0.jar**

   - **log4j-core-2.15.0.jar**

3. Open the following ES node installation directory inside the installed SEM node

   - **<Installation folder>/ES/**

4. Paste the JAR files copied in Step 2 into the **<Installation folder>/ES/lib** folder.

5. Backup and delete the following jars from the **<Installation dir>/ES/lib folder**:

   - log4j-1.2-api-2.9.1.jar

   - log4j-api-2.9.1.jar

   - log4j-core-2.9.1.jar

6. Start the Elasticsearch service (**elasticsearch-service-x64** or **elasticsearch-service-x86**) from services.msc

6.2.8. Reverse Proxy

A reverse proxy is a proxy service that handles requests from clients, forwards them to the necessary servers, and subsequently delivers the servers' responses to the clients without revealing the identity of the servers. Log360 comes bundled with a reverse proxy server to prevent hackers from finding out, accessing, or exploiting the critical data that it holds.

Log360 lets you enable context-based reverse proxy, port-based reverse proxy, or both.

In context-based reverse proxy, the URL of Log360 server and the servers in which its components are installed should be given a unique context path. Whenever a user request access, it is forwarded to the respective servers based on the context path in the URL. The end user will not know the details of the servers from which they are accessing the resources.
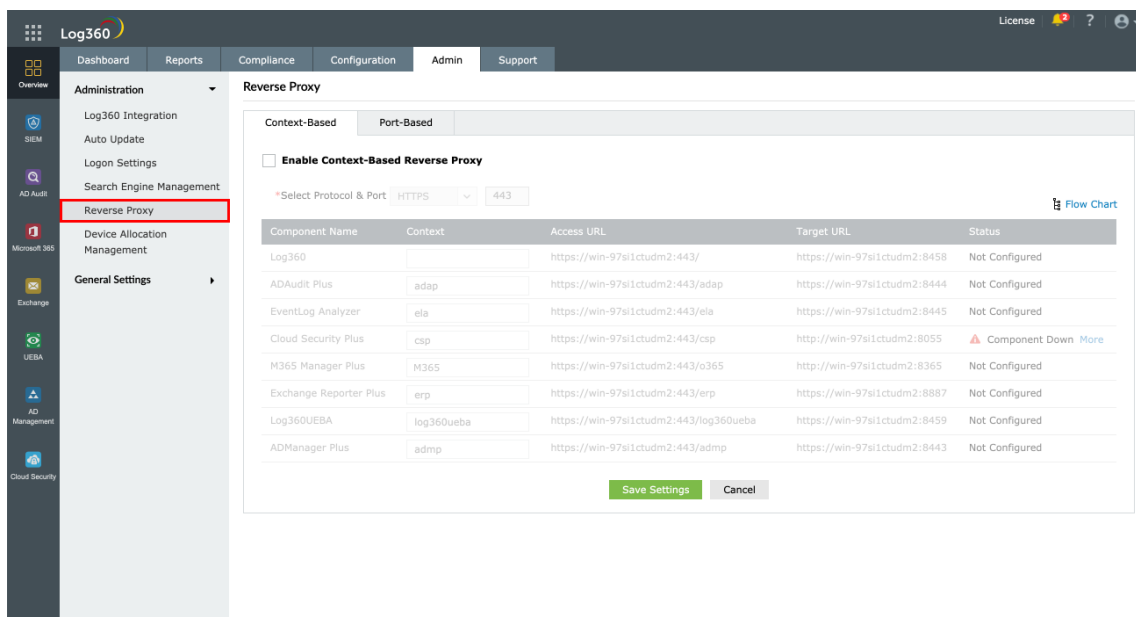
If you want to enable the port-based reverse proxy, you need to choose a unique port number and protocol, for Log360 and its components' servers. In this case, a unique port number for the servers is mandatory whereas specifying a unique protocol is optional. The hostname remains the same for all the servers. In such cases, the reverse proxy server will forward the user request to the appropriate server based on the port number in the URL and the protocol.

> **Note**: The hostname of the Log360 server will serve as the hostname for the components' servers when reverse proxy is enabled.

How to enable reverse proxy

To enable **context-based reverse proxy**, please follow the steps given below.

- Log into the Log360 console as an **administrator**.
- Select the **Admin** tab and navigate to **Administration → Reverse Proxy**.

- Under the **Context-Based** tab, **Enable Context-Based Reverse Proxy** by ticking the check box.
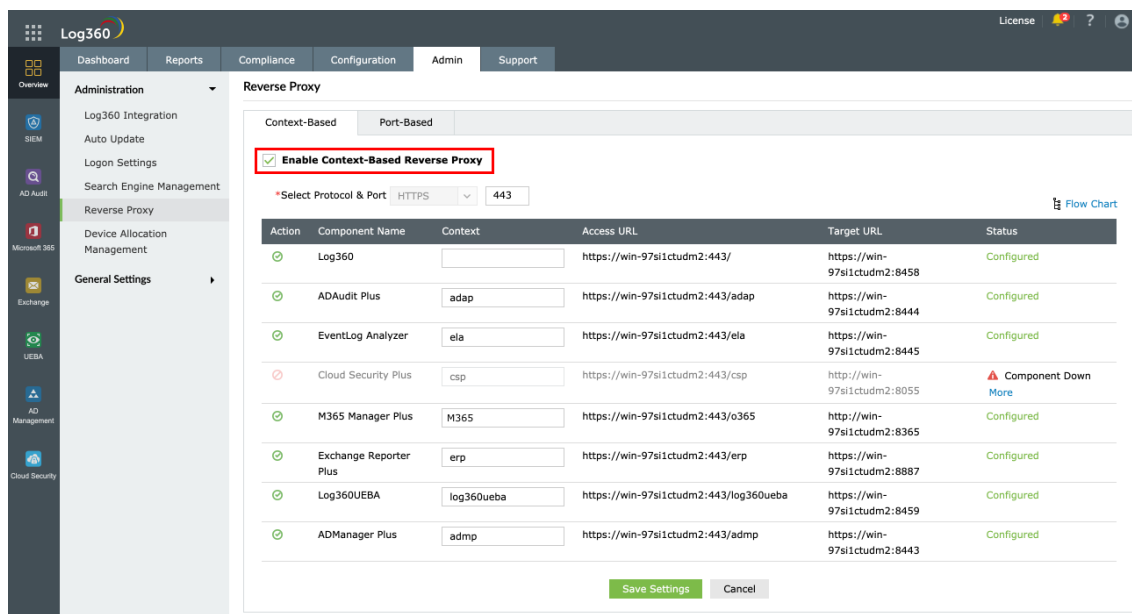
- In the **Protocol & Port** fields, select the required protocol and port number. Make sure the port number is not used by other applications.

- Now, for Log360 and each of the integrated components, enter a context path under the **Context** column. The context path must be unique to each component.

- Note down the **Access URLs** for Log360 and its components. External users can use these URLs to access the necessary products.

- Click **Save Settings**.

To enable **port-based reverse proxy**, please follow the steps given below.

- Log into the Log360 console as an **administrator**.

- Select the **Admin** tab and navigate to **Administration → Reverse Proxy**.
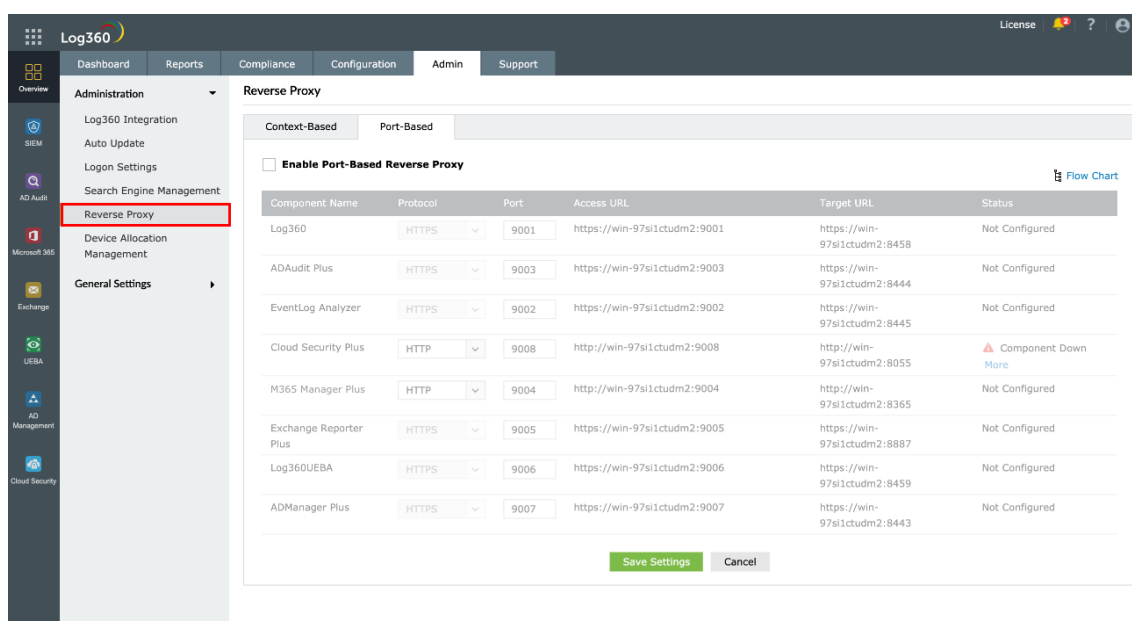
- Under the **Port-Based** tab, **Enable Port-Based Reverse Proxy** by ticking the check box.
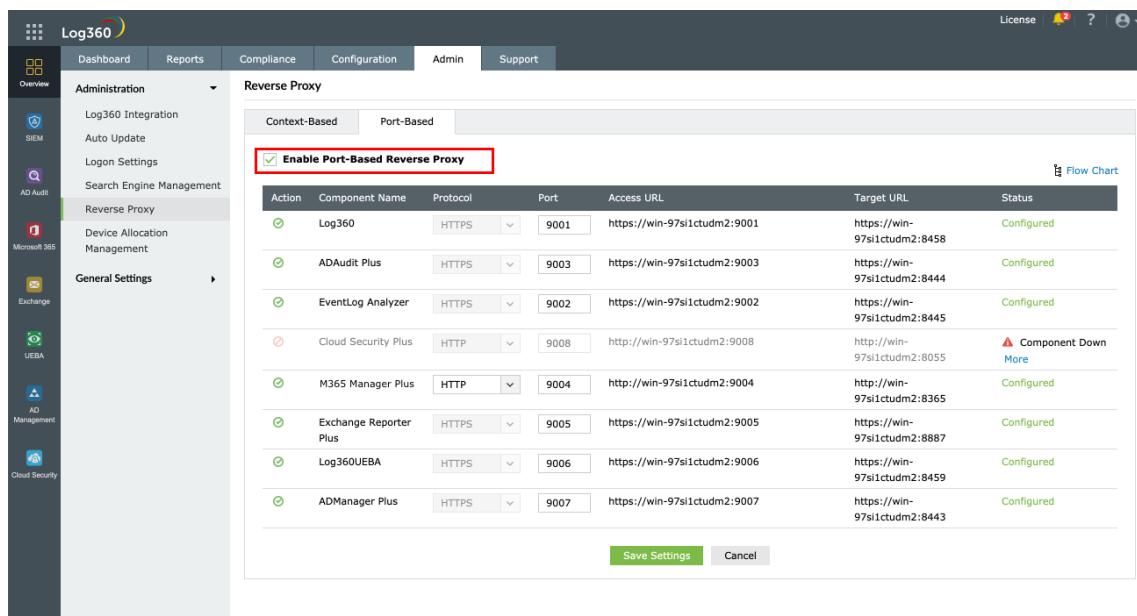
- In the **Protocol** column, select a protocol for Log360 and its components.
- In the **Port** column, enter a port number for Log360 and its components. The port number must be unique to each server.
- Note down the **Access URLs** for Log360 and its components. External users can use these URLs to access the necessary products.
- Click **Save Settings**.

Disabling reverse proxy

Log360 allows you to disable the configured reverse proxy for certain components, if required. You can disable a reverse proxy by clicking on the ⊘ icon, under the **Actions** column corresponding to the desired component.

6.2.9. Device allocation module

EventLog Analyzer and ADAudit Plus are two of the components of Log360 that predominantly works 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. You can check out the device allocation feature by following the steps below.

- Navigate to **Admin → Administration → Device Allocation Management**. You can view the existing devices here.
- To allocate devices to EventLog Analyzer and ADAudit Plus manually, click **Allocate Devices**.
- Select a category from the dropdown to filter devices.
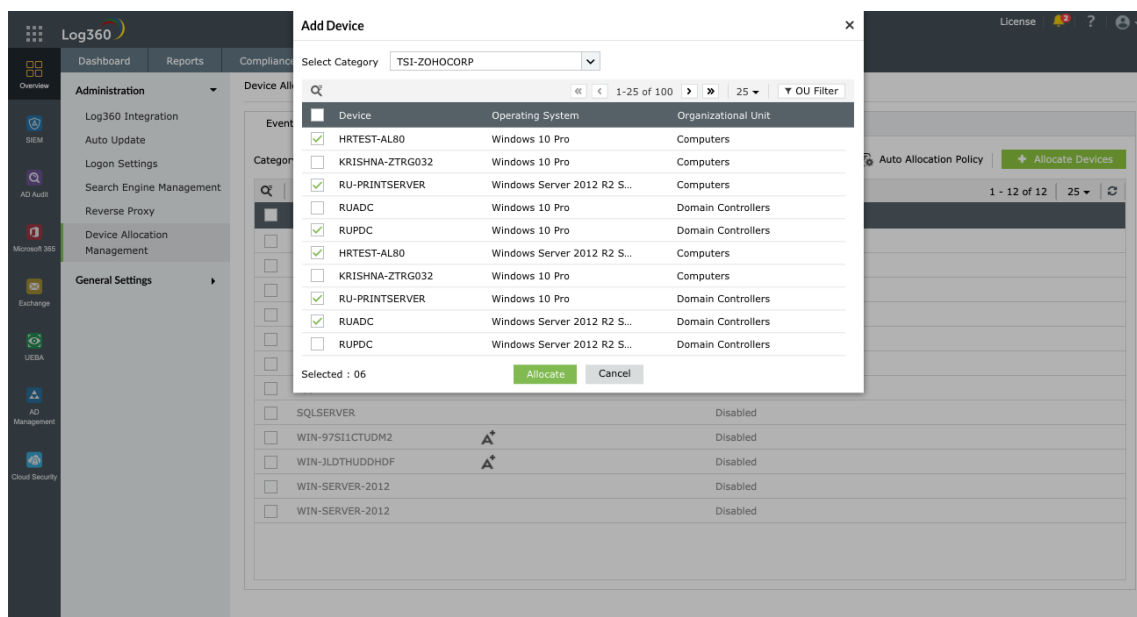
- Click **OU Filter** from the top-right corner to filter devices by Organizational Units (OUs).
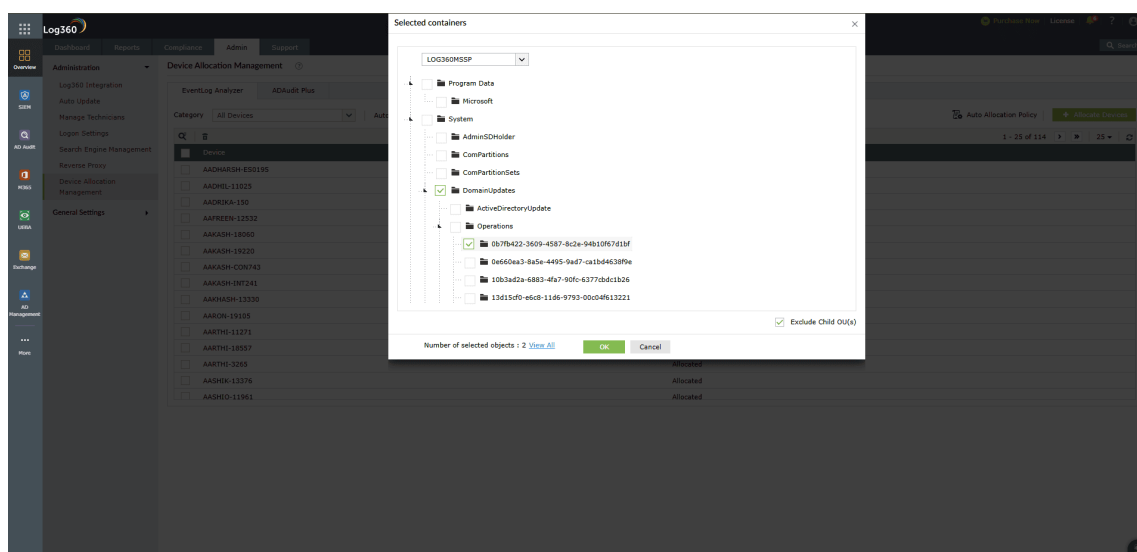
- In the OU tree view, select the desired OUs.

- Check **Exclude Child OU(s)** at the bottom-right corner to select a single parent OU without child OUs.

- Click **OK** to apply the filter.

- To enable **Auto Allocation**, click the slider.

- Click **Auto Allocation Policy** to view the device allocation by policy. You can customize the policy according to your requirements.

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

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

What is device inheritance?

Device inheritance in the Log360 license model involves the sharing of licenses between ADAudit Plus and EventLog Analyzer when they are integrated with Log360.

In the standard Log360 licensing configuration, workstation devices are granted licenses for both EventLog Analyzer and ADAudit Plus. This means that devices listed in the ADAudit Plus workstation with a workstation icon are also licensed for EventLog Analyzer, but they will not appear with the A+ icon in the EventLog Analyzer device list.

Similarly, server devices will be licensed to ADAudit Plus and will be shared with EventLog Analyzer, i.e., in EventLog Analyzer, there will be an A+ icon next to each server devices which share the license of ADAudit Plus, while the same device will not have any icon in the ADAudit Plus devices list.

There are other cases, where the user might use a seperate EventLog Analyzer license or an ADAudit Plus license which has both servers and workstation instead of using bundled Log360 license. In this instance, the other component will share the license and display the A+ icon in EventLog Analyzer or the workstation icon in ADAudit Plus, depending on the nativity of the license.

How to delete the devices?

- If the device to be deleted is a server, go to ADAudit Plus → Configuration → Member Servers and delete the device. (**Note**: The same device will be automatically deleted in EventLog Analyzer as well.)
- If the device to be deleted is a workstation, go to EventLog Analyzer → Settings → Devices and delete the devices. (**Note**: The same device will be automatically deleted in ADAudit Plus as well.)
- In case the deletion fails with the error "Unable to delete inherited devices", check the same device in the other component and delete it from there.

Troubleshooting

- Make sure the versions are up to date. It is recommended to have build numbers surpassing the current ones. The higher, the better.
  - **Log360** above **5267**
  - **EventLog Analyzer** above **12235**
  - **ADAudit Plus** above **7061**
- If the error "Unable to delete inherited devices" appears in both components for a specific device, the synchronization might not have been successfully completed. To address this issue, troubleshooting is necessary.
  - Go to Log360 → Admin - Administration → Integration Settings → EventLog Analyzer → Update Settings and wait for the synchronization to complete.
  - After this, hit back. Select ADAudit Plus → Update Settings and wait for the synchronization to complete.
  - Now check the above mentioned steps for deleting the devices again.
- If the device still could not be deleted, please use the below workaround as an immediate action and contact support if further assistance is required.
  - Remove ADAudit Plus from Log360 Integration (**DO NOT REMOVE** EventLog Analyzer from Log360 Integration).
  - After removing ADAudit plus, the inheritance will be reset in both EventLog Analyzer and ADAudit Plus. Now, the devices can be deleted manually on both EventLog Analyzer and ADAudit Plus.
  - Now, reintegrate ADAudit Plus with Log360.

6.3.1. General Settings

The general settings for Log360 include:

- Personalize

- Product Settings

- SSL Certification

- Server Settings

- Database Settings

- Notification Center

6.3.2. Personalize

Log360 provides administrators the ability to configure the product based on personal preferences and requirements.

Personalize

- Navigate to **Admin → General Settings → Personalize**.
- Under Personalize tab, there are two sections:
    - **Date & Time Settings**
    - **General Settings**
    - **Reordering components in apps pane**

Date & Time Settings

- Choose the language that you prefer from the drop-down menu of the **Language** field.
- Choose the time Zone and the formats of date and time from the drop-down menus of the respective fields.

General Settings

- To change the logo of the product, click on **Choose File** button adjacent to the **Change Logo** field.
- In the **Change Browser Title** field, you can edit the browser title of the product.
- Change the browser favicon by clicking on the **Choose File** button adjacent to the **Change Browser Favicon** field.
- You can also hide the **'Forgot Password?'** link in the login page by selecting the **Hide 'Forgot Password?' link in login page** check-box.
- Click **Save Settings**.

Reordering components in apps pane

- To reorder components click on **more → reorder components**.
- Next, click and drag the components to rearrange them, and click **save**.

6.3.3.1. Product Settings

You can change the following settings of Log360 from this tab.

- Connection Type
- Security Hardening
- General

Connection Type

1. Choose your connection type. You can choose to use either http or https.

2. Specify the port number of your choice after choosing they type of connection.

   - **Default ports** - HTTP : 8095, HTTPS : 8458.

3. To enable LDAP SSL, mark the check-box against the **Enable LDAP SSL** field.

4. Click **Save** to store the configured settings.

General

1. Be alerted when the available disk space falls below a pre-defined level (1 GB, 2 GB or 5 GB), by selecting the appropriate value from the drop-down box.

2. Select the **Session Expiry Time**, which is the time for which a user session would last, from the drop-down box.

3. Select the level of logs that is to be collected by the product. The default working mode for Log360 is **Normal** with minimal set of debugging information. Select **Debug** to collect detailed log reports.

4. Enable or disable collection of anonymous usage statistics gathering to be sent to us.

5. Click **Save** to store the configured settings.

6.3.3.2. Security Hardening

Security hardening feature helps you manage and configure the security settings of Log360. This tab also displays a security score which is calculated based upon the weightage given to each configuration.

To manage individual settings, click the Configure or Enable option corresponding to that security setting and make the required changes. Once configured, the setting will have a green ticked Configured/Enabled ✅ icon next to it, as shown in the image below.
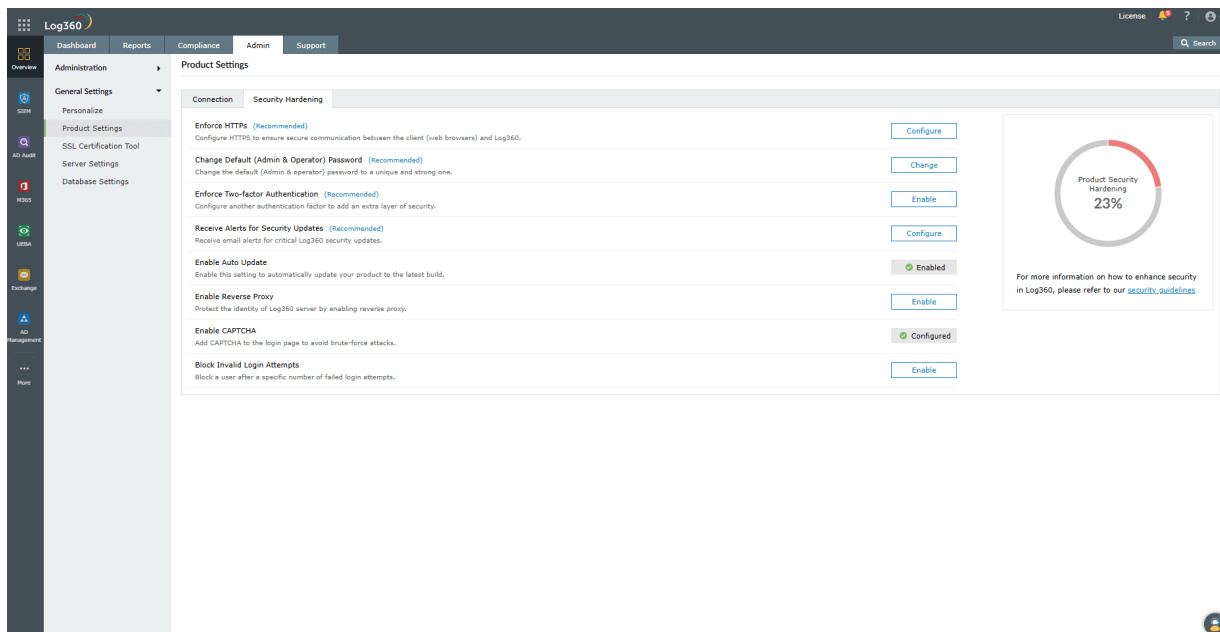
We recommend you to configure all the settings and ensure your product security score is 100%. The security settings alert will be displayed in the notification center (🔔 icon on the top-right corner) until a security score of 100% is reached.

> **Note**: For licensed customers, the alert will also be displayed after every successful login until all the mandatory security configurations (marked with * under **List of security settings**) are done.

List of security settings:

1. **Enforce HTTPS***

   Configuring HTTPS helps you secure connection between the web browser and the Log360 server. See how to enable HTTPS.

2. **Change Default (Admin & Operator) Password***

   It is recommended to use a strong password to access Log360 dashboard. Use this setting to change both the admin and operator password.

3. **Enforce Two-factor Authentication***

   Two-factor authentication adds an additional layer of security. See how to configure two-factor authentication.

4. **Receive Alerts for Security Updates***

Configuring this setting allows you to receive email notifications on the release of important security patches. This ensures that you are well-informed about important security updates for the product, enabling you to update it as soon as possible.

5. **Enable Auto Update**

   Enable this setting to automatically update your product to the latest build. Click on Configure to navigate to the auto-update settings tab. See how to enable auto-update.

6. **Enable Reverse Proxy**

   Enabling reverse proxy helps protect the identity of Log360 server. Click on Configure to navigate to the reverse proxy settings tab. See how to enable reverse proxy settings.

7. **Enable CAPTCHA**

   This setting adds captcha to the login page to avoid brute-force attacks. See how to add captcha.

8. **Block Invalid Login Attempts**

   This setting allows you to block a specific user who fails to login after a specific number of attempts. See how to block invalid login attempts.

> **Note**: The first three settings given in the above list are mandatory for Log360.

6.3.4.1. SSL configuration for Log360

Log360 supports SSL connection to ensure security of data transferred between the browser and the Log360 server.

Steps to apply SSL certificate and enable HTTPS

Let's see how to generate and apply a SSL certificate for LOg360 and its integrated components.

- Navigate to **Admin → General Settings → SSL Certification Tool**.
- If you don't have a SSL certificate, select the Generate Certificate option and follow the steps here.
- If you already have a SSL certificate, select the Apply Certificate option and follow the steps here.

> **Note**:SHA256 with RSA algorithm is currently supported for the SSL certificates.

Apply Certificate

If you already have a SSL certificate, follow the steps listed below to apply it.

- In the **Apply Certificate** to drop-down, select the component for which you want to apply the SSL certificate.
- Choose an **Upload Option** based on the certificate file type.
    - **ZIP upload:**
        1. If your CA has sent you a ZIP file, then select ZIP Upload, and upload the file.
        2. If your CA has sent you individual certificate files—user, intermediary, and root certificates, then you can put all these certificate files in a ZIP file and upload it.
    - **Individual Certificates:**
        1. If your CA has sent you just one certificate file (PFX or PEM format), then select Individual Certificates, and upload the file.
        2. If your CA has sent the certificate content, then paste the content in a text editor and save it as a CER, CRT, or PEM format, and upload the file.
    - **Certificate Content:**
        1. If your CA has sent just the certificate content, then choose Certificate Content option, and paste the entire content.
- If the certificate file requires a password, then enter it in the **Certificate Password** field. Or, if the certificate contains a password-protected private key, enter the password in the **Private Key Passphrase** field.

> **Note**: Only Triple DES encrypted private keys are currently supported.

- Click **Apply.**
- Finally, restart Log360.

Generate Certificate

- In the **Common Name field**, enter the name of the server.

  Example: For the URL **https://servername:9251**, the common name is **servername.**

- In the **SAN Names** field, specify the additional hostnames (e.g., sites, IP addresses, common names) that must be protected by the certificate.

- In the **Organizational Unit** field, enter the department's name which you want to be displayed in the certificate.

- In the **Organization** field, enter the legal name of your organization.

- In the **City** field, enter the name of the city as provided in your organization's registered address.

- In the **State/Province** field, enter the name of the state or province as provided in your organization's registered address.

- In the **Country Code** field, enter the two letter code of the country where your organization is located.

- In the **Password** field, enter a password that consists of at least 6 characters to secure the keystore.

- In the **Validity (In Days)** field, specify the number of days for which the SSL certificate will be considered valid.

> **Note**: When no value is entered, the certificate will be considered to be valid for 90 days.

- In the **Public Key Length (In Bits)** field, specify the size of the public key.

> **Note**: The default value is 2048 bits and its value can only be incremented in multiples of 64.

- After all values have been entered, you can select either of these two options:

  - **Generate CSR**

    This method allows you to generate the CSR file and submit it to your CA. Using this file, your CA will generate a custom certificate for your server.

    1. Click **Download CSR** or manually get it by going to the **<Install_dir>\Certificates** folder.

    2. Once you have received the certificate files from your CA, follow the steps listed under Apply Certificate to apply the SSL certificate.

  - **Apply Self-signed Certificate**

    This option allows you to create a self-signed certificate and apply it instantly in the product. However, self-signed SSL certificates come with a drawback. Anyone accessing the product secured with a self-signed SSL certificate will be shown a warning telling them that the website is not trusted, which may cause concern.

6.3.4.2. What is SSL?

Acronym for Secure Socket Layer, SSL is an encryption technology to secure the data exchange between a website and its visitor's web browser. Normally, when a user communicates with a website, say submits his credit card information, the data travels to the server as plain text, which is susceptible to data theft!

On the other hand if this data is encrypted, then no eavesdropper can read it! Thus, it's really very important to secure a website with SSL!

Certificates and Certifying Authority (CA)

SSL Certificate:

This is a digital identity of a company, which ensures that a visitor is talking only to its intended website and whatever data he submitted to the site is encoded and reach only the intended site. This system is analogous to banks recognizing their customers by their signatures. In this case, the browsers (thereby the end-users) are programmed to trust these CA presented certificates.

Certifying Authority:

Regulatory organizations, who, with the help of standard policies, issue certificates to a domain, declaring them trustworthy. Every certificate they generate is unique to the company they are certifying, which makes identification easy.

CAs secure all necessary information about a company before issuing a certificate for it and also keep updating it in their records, which adds to the trustworthiness.

Some of the popular CAs are Verisign, Comodo & GoDaddy etc.

Keystore

Keystore is specifically designed to store various kinds of encryption information.

CSR

In order for a CA to generate an SSL certificate for a company, it first collects the information about the company and other identifiers such as public key (digital signature), and then binds them all with its certificate (which could be a piece of encrypted token or something similar). In doing so, it generates a unique identifier for the company.

Thus every certificate issuance process begins with a "certificate request" from the company. CAs refer to this process as "Certificate Signing Request". The CAs accept the company information and digital signatures in a special form of file - the ".csr" file.

The Usual SSL Issuance Process

It involves 3 steps:

- First you generate a CSR and submit it to CA.
- CA binds this CSR with its digital signatures and returns it.
- Now, you bind all this with your company domain.

To enable SSL for Log360

For detailed instructions on how to enable SSL for Log360, click here.

6.3.5. Server Settings

Under server settings, you can configure the mail server for sending notifications, alerts, etc., from the product and proxy settings in case you are using a proxy server. The following settings can be found here:

Mail Settings

Log360 provides two modes of mail server configuration:

1. SMTP
2. API

SMTP

This method allows you to create and authenticate a mail server via Basic or OAuth authentication.

To configure an SMTP mail server,

1. In the **field**, select **SMTP**.

2. Enter your mail server's **Server Name or IP**, and **Port Number** in the respective fields.

3. In the **From Address** field, enter the email address that will be used to send out notifications, alerts, etc., from Log360.

4. In the **Admin Mail Address** field, enter your email address if you wish to receive notifications for the emails sent from Log360.

5. Select the connection security type from the available options: SSL, TLS, or None.

6. Select the authentication type from the options provided:

   - Basic authentication

   - OAuth authentication

7. **Basic authentication**

   - Enter the **Username** and **Password** to access the mail server.

   - If your mail server does not require authentication, leave the fields empty.

8. **OAuth authentication**

   - Select your mail provider from the available options: **Microsoft** or **Google**.

   - If your mail provider is Microsoft, provide the **Username, Tenant ID, Client ID**, and Client Secret in the respective fields. In Log360, the Azure Cloud is considered the default Azure environment. You can modify the Azure environment setting by clicking the **Choose the appropriate Azure environment** link.

   > **Note:** To learn how to find your Azure Tenant ID, Client ID, and Client Secret, click here.

9. If you have selected **Basic Authentication** in step 6, you can have Log360 send a test email by clicking the **Test Mail** button.

10. Click **Save Settings** to save your mail server configuration.

API

This method allows you to create and authenticate a mail server via your mail provider's API.

- In the **Mode** field, select **API**.
- Select your mail provider from the available options: **Microsoft** or **Google**.
- In the **From Address** field, enter the email address that will be used to send out notifications, alerts, etc., from Log360.
- In the **Admin Mail Address** field, enter your email address if you wish to receive notifications for the emails sent from Log360.
- If your mail provider is Microsoft, provide the **Tenant ID, Client ID**, and **Client Secret** in the respective fields. In Log360, the Azure Cloud is considered the default Azure environment. You can modify the Azure environment setting by clicking the **Choose the appropriate Azure environment** link.

> **Note:** To learn how to find your Google **Tenant ID, Client ID**, and **Client Secret**, click here.

- If your mail provider is Google, upload the **JSON private key** file.

> **Note:** To learn how to get your JSON private key file, click here.

- Click **Save settings**.

Steps to find your Azure Tenant ID, Client ID, and Client Secret for SMTP mail server configurtion

- Log in to portal.azure.com.
- Under **Azure services**, click **App registrations → New registration**.
- Provide a **Name** of your choice and select the **Supported account types**. (Leave it as default).
- In the **Redirect URI** field, select **web** & paste the following OAuth link:
  https://identitymanager.manageengine.com/api/public/v1/oauth/redirect (or) You can also add the localhost redirect API in the following syntax.
  protocol://localhost:port_number/context_if_any/RestAPI/WC/OAuthSetting
  For example, http://localhost:8095/RestAPI/WC/OAuthSetting. If you have only added localhost as the redirect URI, you must access the product using localhost to configure mail server.
- In the next page, you will find the application details. Copy the **Client ID & Tenant ID**.
- From the left pane, click **Certificates & secrets → New client secret**.
- Provide a **Description** for the client secret, and in the **Expires** field, choose the validity of the client secret and click **Add**.
- The client secret will be generated. Copy the string displayed under **Value**.
- Click **Save setting** and complete the authorization prompt.

Steps to find your Google Workspace Client ID, and Client Secret for SMTP mail server configurtion

- Log in to console.developers.google.com.
- In the dashboard, click **Create** to create a new project if there is no existing project or select any existing project and click **New Project**

- Enter the **Project Name**. In the **Location** field, click **Browse** and select the parent organization. Click **Create**.

- In the left pane of the displayed project details page, click **APIs & Services → Library**.

- From the available list of APIs, select **Gmail API** and click **Enable**. You can make use of the search option to find the API quickly.

- In the left pane, click **OAuth consent screen** and choose the **User Type**. If you don't have a Google workspace account, choose **External User**.

- Provide the **Application Name, Application Logo**, and the **support email** of your help desk, developer information, and click **Save & continue**.

- Click **Add or Remove Scopes**, choose **Gmail API (https://mail.google.com/)**, and click **Update**. Then, click **Save & Continue**.

- Add a test user and click **Save & continue**.

- In the left pane, click **Credentials → Create Credentials → OAuth Client ID**.

- Select the application type as **Web Application**. Provide a name of your choice.

- In the **Authorized Redirect URIs**, paste the following OAuth link:
  https://identitymanager.manageengine.com/api/public/v1/oauth/redirect (or) You can also add localhost redirect API in the following pattern.
  protocol://localhost:port_number/context_if_any/RestAPI/WC/OAuthSetting
  For example, http://localhost:8095/RestAPI/WC/OAuthSetting. If you have only added localhost as the redirect URI, you must access the product using localhost to configure the mail server.

- Click **Save**.

- Click **DOWNLOAD JSON** to download the file containing the authorization server details. Copy the Client ID and Client Secret displayed on the screen.

Steps to find your Azure Tenant ID, Client ID, and Client Secret for API mail server configurtion

- Log in to portal.azure.com.

- Under Azure services, click **App registrations → New registration**.

- Enter a **Name** of your choice and choose the **Supported account types**. (If you're unsure about the supported account types, select **Accounts in the organizational directory only**).

- In the left pane, click **API Permission → Add a permission**.

- Click **Microsoft Graph → Application permission**.

- Search Mail and select the permission **Mail.Send**. Click **Add Permission**.

- Click **Grant admin consent**.

- Copy the **Client ID & Tenant ID** displayed.

- In the left pane, click **Certificates & secrets → New client secret**.

- Provide a **Description** for the client secret. In the **Expires** field, choose the validity of the client secret and click **Add**.

- The client secret will be generated. Copy the string displayed under **Value**.

Steps to download JSON private key for API mail server configurtion

- Log in to console.developers.google.com.

- Open the **Service accounts** page.

- Click **Create Project**. Enter the project name, organization and location. Click **Create**.

- Click **+ Create service account** button from the top row.
- Under **Service account details**, type a name, ID, and description for the service account, then click **Create and continue**.
- If required, you can also select the IAM roles to be granted to the service account using the **Grant this service account access to project** option.
- Click **Continue**
- If required, you can add the users or groups that are allowed to use and manage the service account.
- Click **Done**.
- Click the email address for the service account you created.
- Click the **Keys** tab.
- In the **Add key** dropdown list, select **Create new key**.
- Select key type as **JSON**.
- Click **Create**.

Your new public/private key pair will be generated and downloaded to your machine. Please keep the private key safe as this will be the only copy, and you cannot generate the same private key again.

Once you have downloaded the JSON private key, you'll have to enable Gmail API service and provide domain-wide authority to the service account.

Enable Gmail API service

- Login to console.developers.google.com.
- Select the project from the dropdown menu.
- Click **+ Enable APIS and Services**.
- Select **Gmail API** and click **Enable**.

Delegating domain-wide authority to the service account

- Log in to the Google Workspace domain's Admin console as a super administrator.
- Navigate to **Main menu → Security → Access and data control → API Controls**.
- In the **Domain wide delegation** pane, select **Manage Domain Wide Delegation**.
- Click **Add new**.
- In the **Client ID** field, enter the service account's Client ID. You can find your service account's client ID on the Service accounts page.
- In the **OAuth scopes (comma-delimited)** field, enter the list of scopes that your application should be granted access to. For example, if your application needs domain-wide full access to the Google Mail API, enter: https://mail.google.com.
- Click **Authorize**.

Your application now has the authority to make API calls as users in your domain (to "impersonate" users). When you prepare to make authorized API calls, specify the user to impersonate as.

SMS Settings

You can configure Log360 to use your own GSM modem or your custom SMS gateway.

- GSM modem configuration
- Custom SMS Provider configuration

1. Configuring GSM Modem

- Navigate to **Admin → General Settings → Server Settings**.
- Click **SMS Settings** tab.
- Select **GSMModem** from the SMS Provider drop down box.
- Specify the **Modem Port Number**.
- Click **Save Settings**.

Steps involved in configuring the modem port & modem speed:

- Connect your GSM Modem to the Serial Communication Port.
- Only a serial cable must be used for connectivity.
- The port number for Window Devices will be comX. Eg. com7 or com8.
- Enter the Port Number to which the modem is connected :eg.(COM 1).

Requirements for Establishing SMS Server Connection:

- Modem/mobile must have GSM functionality with a provision to insert the SIM card.
- Should support 7-bit (GSM default alphabet), 8-bit and Unicode (UCS2) encoding.
- Make sure the GSM modem configured with Log360 is not used by any other application.
- If you experience any issue in sending SMS notifications through GSM modem, please restart Log360 and try again.
- Matching these criteria allows Log360 to support your modem/ mobile phone.

2. Configuring Custom SMS Provider

You can configure you own custom SMS gateway provided that the gateway is HTTP or SMTP based. Please follow the steps given below:

- HTTP-based SMS Provider
- SMTP-based SMS Provider
- SMPP-based SMS Provider

HTTP-based SMS provider:

- Navigate to **Admin → General Settings → Server Settings**.
- Click **SMS Settings** tab.
- Select **Custom** from the **SMS Provider** drop down box.
- Select **HTTP** from the **Send SMS via** drop down box.
- Select whether you want to use **Post** or **Get HTTP method** for sending SMS.
- Enter the **HTTTP URL** of your SMS gateway provider.
- Enter the **HTTP Parameters** specific to your SMS provider.

> **Note**:
> - Separate the HTTP parameters by an ampersand (&) sign.
> - Example format: **userName=xxx&password=yyy&mobileNumber=%mobNo&message=%message%**.
> - You can use the following parameters:
>   - **userName** = the parameter which is used to denote the API authentication username.
>   - **xxx** = API authentication username.
>   - **password** = the parameter which is used to denote the API authentication password.
>   - **yyy** = API authentication password.
>   - **mobileNumber** = recipient parameter.
>   - **%mobNo%** = this macro denotes the user's mobile number.
>   - **message** = message parameter.
>   - **%message%** = this macro denotes the SMS message content.
>   - **More HTTP Parameters** - If you SMS provider requires more parameters like unicode and apiID, include them as well using the '&' sign.
> - Specify the **response** you get from your provider to determine whether the SMS has been sent successfully.
> - Click **Advanced Settings**. Enter the **HTTP Request Headers** specific to your SMS provider.
> - Select the option **Convert Message into Unicode** to send SMS in Unicode format.
> - Click **Save**.

SMTP-based SMS provider:

- Navigate to **Admin → General Settings → Server Settings**.
- Click **SMS Settings** tab.
- Select **Custom** from the **SMS Provider** drop down box.
- Select **SMTP** from the **Send SMS via** drop down box.
- In the **From Address** field enter an email address from which you want to send the SMS. Eg: noreply@adselfserviceplus.com
- In the **To Address** field enter the %mobNo% macro followed by the email of your provider. For example: %mobNo%@clickatell.com. Refer your SMS provider to know the exact values.
- Enter the details required in the **Subject** field. Generally, it would be either mobile number or message depending upon your SMS provider.
- Enter the details required in the Content field. This also depends on your SMS provider. Please refer them to know the exact values.
- Click **SMTP Server Settings**.
- Enter the **name or IP address** of the "SMTP Server" and its **Port number**.
- Enter the **username** and **password** of the SMTP server.
- Click **Save**.

> **Note**: If you don't configure the SMTP server settings, then the mail server configured under the Mail Settings tab will be used.

SMPP-based SMS provider:

- Navigate to **Admin → General Settings → Server Settings**.
- Click **SMS Settings** tab.
- Select **Custom** from the **SMS Provider** drop down box.
- Select **SMPP** from the **Send SMS via** drop down box.
- Enter the **SMPP Server Name** and its **SMPP Server Port**.
- Enter the **Username** and **Password** of the SMPP server.
- Click **Advanced** Settings.
- Enter the **SMPP Source Address**.
- Select the **Source Address's TON** (type of number).
- Select the **Source Address's NPI** (Numeric Plan Indicator).
- Select the **Destination Address's TON**.
- Select the **Destination Address's NPI**.
- Click **Save Settings**.

Proxy Settings

- Navigate to **Admin → General Settings → Server Settings.**
- Click on the **Proxy Settings** tab.
- Select the **Enable Proxy Server** option.
- Enter the proxy server's name or IP address and the port number in their respective fields.
- Enter the **username** and **password** credentials for accessing the proxy server.
- Click **Save Settings**.

Alternatively, you can also change the Proxy settings by following the steps listed below:

- Navigate to **Support** tab.
- Click on **Check for updates** box at the top right corner of the page.
- Click **Settings** link in the pop-up that appears, then click on **Proxy Settings** tab.
- Select Enable **Proxy Server** option.
- Enter the proxy server's name or IP address and the port number in their respective fields.
- Enter the **username** and **password** credentials for accessing the proxy server.
- Click **Save Settings**.

Notification Settings

These settings help you select the notifications you receive from Log360.
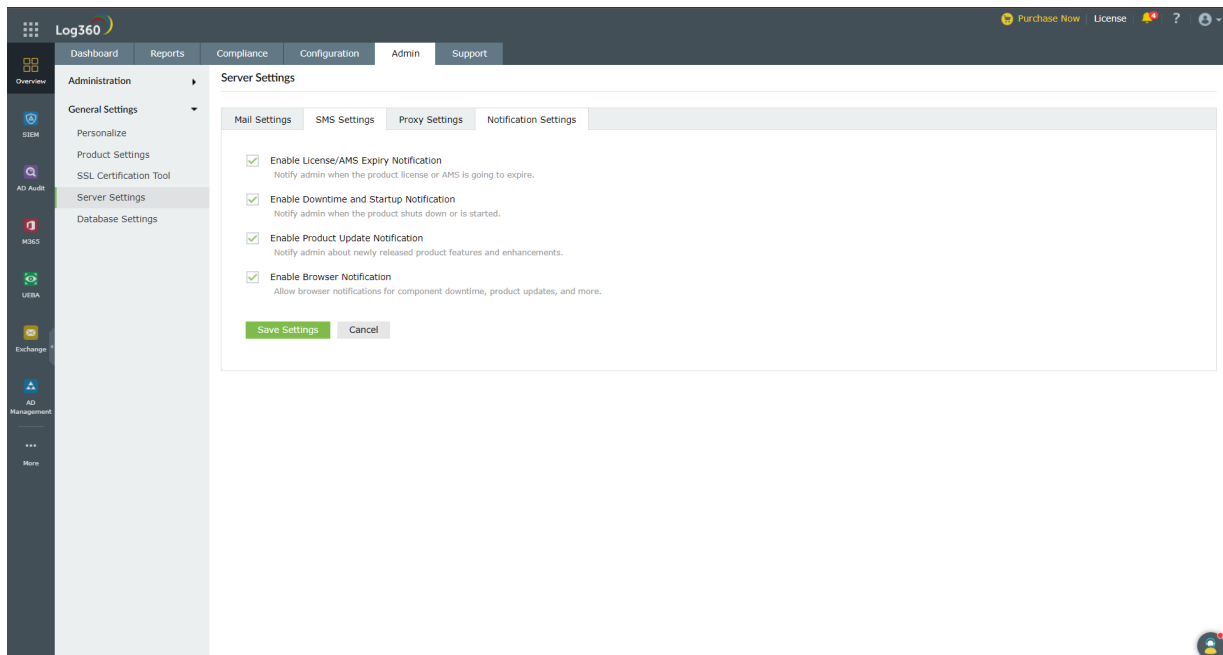
- Navigate to **Admin → General Settings → Server Settings → Notification settings**.
- To notify the admin when the license is about to expire, check the box next to **Enable License/AMS Expiry Notification**.
- To notify the admin when the application shuts down unexpectedly, check the box next to **Enable Downtime Notification**.
- To notify the admin about newly released product features and enhancements, check the box next to **Enable Product Update Notification**.
- To receive notifications from Log360 as push notifications straight to your web browser, check the box next to **Enable Browser Notification**.
- Click **Save Settings**.

6.3.6.1. Database Settings

Log360 allows you to configure periodic backup of the database that comes built-in with it and the integrated components. The product also allows you to migrate from the built-in database (PostgreSQL) to MS SQL.

- Database Auto Backup
- Database Migration

6.3.6.2. Automatic database backup

Log360 can automatically back up its database and the databases used in the integrated products at regular intervals, as scheduled by you. Using this option, you can back up the built-in PostgreSQL DB or external PostgreSQL and MS SQL databases configured in the product.
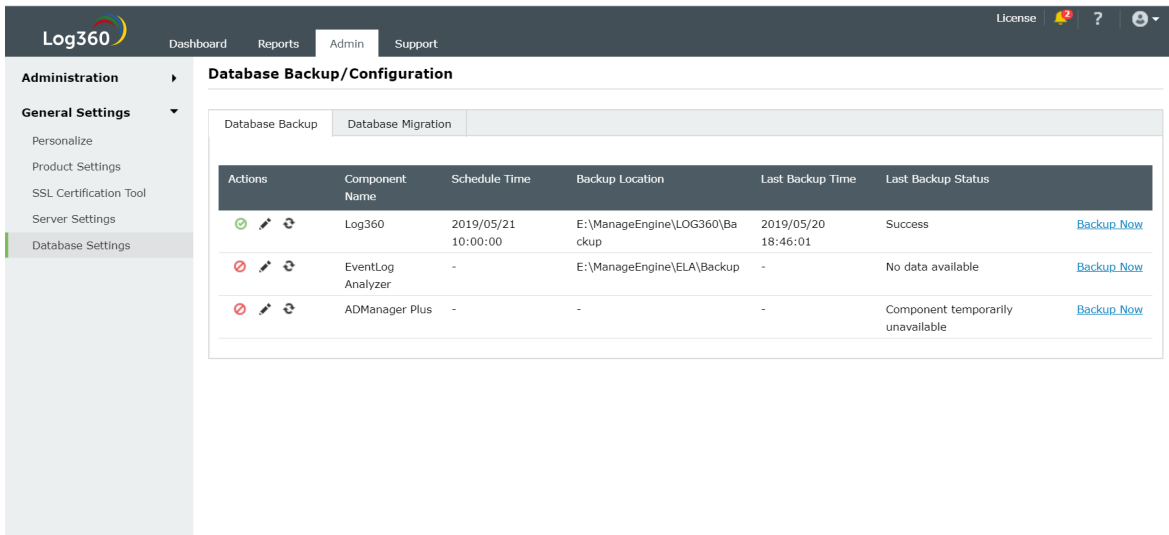
Supported DB versions for auto backup

- PostgreSQL: Version 10 to 14
- MS SQL: Version 2008 and above

Prerequisite for backing up external PostgreSQL

1. In the machine where PostgreSQL is installed, go to **<postgresql_installdir>/data** and open the **posgresql.conf** file. Search for **wal_level** entry. Uncomment the entry and change its value to **archive.**

2. Copy all the files in **<postgresql_installdir>/lib** and **<postgresql_installdir>/bin** folders and paste them in <product_home>/pgsql/lib and <product_home>/pgsql/bin folders respectively. <product_home> refers to the home directory of Log360 or the integrated products for which you're configuring the auto backup scheduler.

3. **Restart** the external PostgreSQL server.

4. Repeat the steps 1 to 3 from above whenever you update the PostgreSQL server.

Steps to schedule database backup

1. Navigate to **Admin → General Settings → Database Settings → Database Backup.**

2. Choose Log360 or an integrated product for which you want to schedule auto backup, and click the edit ✎ icon.

3. Select whether you want to schedule the backup daily, weekly, or monthly and at what time from the **Backup Frequency** drop-down.

4. Enter the number of incremental backups to take for every full backup in the **Full Backup after __ incremental backups** box. Enter 0 if you want to take only full backups.

5. Enter the **Backup Storage Path.**

- You can either choose a local folder or shared folder to store the backups.
- If the shared folder you've chosen needs permission to store the backups, then put a check against the **Authentication Required** box, and enter the necessary credentials.

> **Note 1**: If the shared folder is located in a workgroup computer, then create a new domain account in AD. This new account should have the same username and password as that of a local account in the workgroup computer. Use the credentials of this new account for authentication.

> **Note 2**: If the specified path is wrong or unreachable, the backup will be stored in the default backup folder (<Installation_Folder\Backup>).

6. Set a retention period for the backup files from the **Maintain Backup Files** drop-down.

7. Click **Save.**

Other settings

- To **disable** auto backup for Log360 or a particular integrated product, click the ⊘ icon located in the **Actions** column of the auto backup configuration table.
- To get the status of the latest backup, click the ⟳ icon.
- To edit the backup schedule for a particular component, click on the ✎ icon located in the action column of the component.
- Use the **Backup Now** option to initiate a backup instantly.
- Use the **Recent Backups** icon in the status column to view all available backups.

Restoring backup from an old version of MS SQL server to new MS SQL server

If you've installed a new version of MS SQL server and want to configure it in Log360 or its integrated products in place of the old MS SQL server, you can do so by using the backup you've taken using Log360. Just note that, in addition to the backup you've taken using Log360, you need to copy the files in <MS_SQL_Old_Version>/Backup to <MS_SQL_New_Version>/backup.

Troubleshooting tips

If you get an error while backing up the database, please check whether:

- The database server is running.
- There is sufficient space in the backup storage location.

6.3.6.3. Database Migration

Using this option you can change the built-in database server (PostgreSQL) of Log360 to MS SQL Server or another instance of a PostgreSQL Server.

Important points to remember

- Supported database migrations:
    - PostgreSQL Server to MS SQL Server or another instance of PostgreSQL Server.
    - MS SQL Server to PostgreSQL Server or another instance of MS SQL Server.
- Supported database versions:
    - PostgreSQL: 10 to 14
    - MS SQL: 2008 and above
- Take a backup of the database before you proceed.
- We recommend applying the Windows service packs and cumulative updates suggested by Microsoft during your migration to MS SQL Server.

Prerequisites for MSSQL migration

- Copy the **bcp.exe** and **bcp.rll** files from the installed SQL Server directory and paste them in the Log360 bin folder (<Log360_installed_directory/bin).
    - Location of the bcp.exe file: <MSSQL_installed_folder>\Client SDK\ODBC\...\Tools\Binn\bcp.exe. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\...\Tools\Binn\bcp.exe.
    - Location of the bcp.rll file: <MSSQL_installed_folder>\Client SDK\ODBC\...\Tools\Binn\Resources\1033\bcp.rll. For example, C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\...\Tools\Binn\Resources\1033\bcp.rll
- For migration to MS SQL, please install the corresponding SQL Native Client in the Log360 machine as per the MS SQL Server version.

MS SQL Server Version	Native Client
2008	Download
2012	Download
2014	Download
2017	Download
2019	Download

> **Note**: MS SQL server version 2022 is also supported by Log360.

- If firewall is enabled in the MS SQL Server machine, the TCP and UDP ports must be opened.
- If the MS SQL server you wish to migrate to has **Force encryption** enabled, follow the steps mentioned below.

    1. Convert your certificate to .cer format.

        1. Open **IIS Manager**.

        2. In the middle pane, click **Server Certificates**.

        3. Open the certificate you want to use, and click the **Details** tab.

        4. Click **Copy to file**.

        5. Click **Next** in the Certificate Export Wizard that appears.

        6. On the Export Private Key screen, select **No, do not export the private key**, and click **Next**.

        7. On the Export File Format screen, select either **DER encoded binary X.509 (.CER)** or **Base-64 encoded X.509 (.CER)**, and click **Next**.

        8. Enter a name for the file and click **Next**, and then **Finish**.

    2. Open Command Prompt and navigate to <Installation directory>\jre\bin. Use the command below to associate the certificate with the Java KeyStore.

        keytool -import -v -trustcacerts -alias myserver -file pathofthecert\certname.cer -keystore "..\lib\security\cacerts" -keypass changeit -storepass changeit -noprompt

        where pathofthecert is the location where the certificate has been stored and certname is the certificate name.

        The certificate will be added to your Java KeyStore.

Prerequisites for PostgreSQL migration

1. Open the remote machine where the product is installed & navigate to **Product Home\ pgsql\ data\ pg_hba.conf**

2. Open pg_hba.conf file and add an entry of the host IP address and its subnet mask as 0.0.0.0/0 (Refer Pic).

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
host    all             all             0.0.0.0/0            md5
```

3. Navigate to **Product Home\ pgsql\ data \ postgresql.conf**

4. Open postgresql.conf and change the Listen_addresses as '*****' & remove the **#** in the start of the line. (Refer Pic)

```
# - Connection Settings -

listen_addresses = '*'          # what IP address(es) to listen on;
# comma-separated list of addresses;
# defaults to 'localhost'; use '*' for all
```
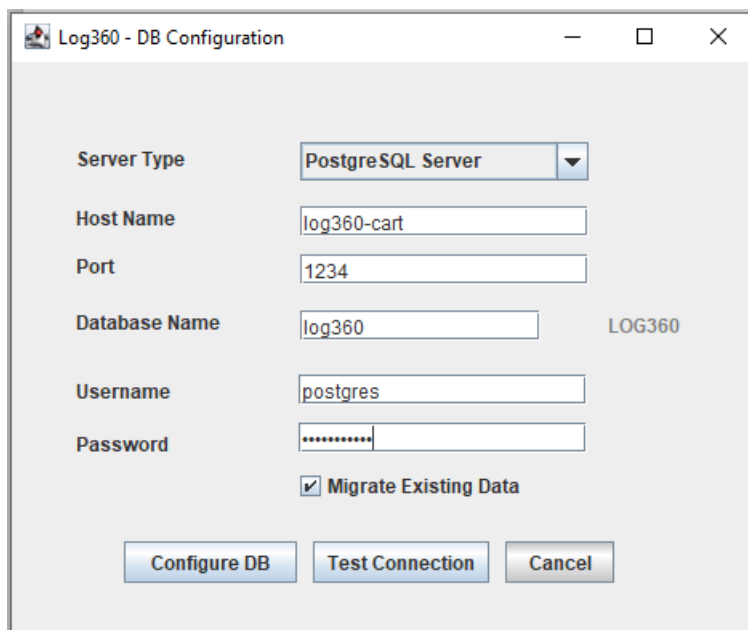
Database backup for External PostgreSQL

- In the machine where PostgreSQL is installed, go to <postgresql_installdir>/data and open the posgresql.conf file. Search for wal_level entry. Uncomment the entry and change its value to archive.
- Copy all the files in <postgresql_installdir>/lib and <postgresql_installdir>/bin folders and paste them in <product_home>/pgsql/lib and <product_home>/pgsql/bin folders respectively. Here, <product_home> refers to the home directory of Log360 or the integrated products for which you're configuring the auto backup scheduler.
- Restart the external PostgreSQL server.

Repeat the steps 1 to 3 from above whenever you update the PostgreSQL server.

Steps for Migration

> **Note**: Take a Backup/Snapshot of Log360 before proceeding with the steps (**Important**)

1. Open the Command Prompt and navigate to <Log360 home\bin> (Here, Log360 home is the location where Log360 is installed).
2. Stop Log360 by running **shutdown.bat**.
3. Run the **ChangeDB.bat**.
4. From the **Server Type** menu, select the database server you plan to switch to.
5. If you select **PostgreSQL Server**, then:
   - In the **Host Name** and **Port** field, enter the host name or IP address and the port number of the PostgreSQL database server.
   - Enter the username and password of a user with the necessary permissions to create a new database.

6. If you select **MS SQL Server**, then:

- Move the **bcp.exe** and **bcp.rll files** into the bin folder manually.

- In the **Host Name and Port** field, enter the host name or IP address and the port number of the MS SQL database server.

- In the **Select Server Instance** field, select the SQL Server instance you want to use.

- For Authentication, you can use either Windows credentials or a SQL Server user account.

- If you want to use a SQL Server user account, then select **SQL Authentication** and enter the Username and Password.

- If you want to use Windows authentication, select **Windows Authentication**, and enter the username and password of a Windows domain user account.

> **Note**: The user account used must have permission to create a database in the selected MS SQL
> Server.

7. Check the box next to **Migrate Existing Data** to copy the data from your old database to the new database.

   IMPORTANT: Leave this box unchecked only if you are changing the database of a fresh installation of Log360.

8. If the MS SQL server you wish to migrate to has **Force encryption** enabled, check the box next to **SSL connection**.

9. Click **Test Connection** and wait for the connection to be established.

10. Once Test Connection has been established successfully, click **Configure DB** to initiate migration.

6.3.7. Notification Center

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

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

Alert generating events in Log360

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

Manage Alerts

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

- To resolve, click on the action link corresponding to the alert. You will be directed to the screen where changes have to be made.

- To delete, click the ✖ icon to hide the alert from your notification tray.

7. Global Search

The global search capability can be used to search across all sections of Log360 including Reports, Compliances, Administrative settings, and Help documentation. This helps in finding particular sections of the product faster and improves productivity of the SOC team.

- Open global search by clicking on the search bar in the top right corner of the screen.

> **Note:** To open Global Search, you can also use the keyboard shortcut **Ctrl+Space**.
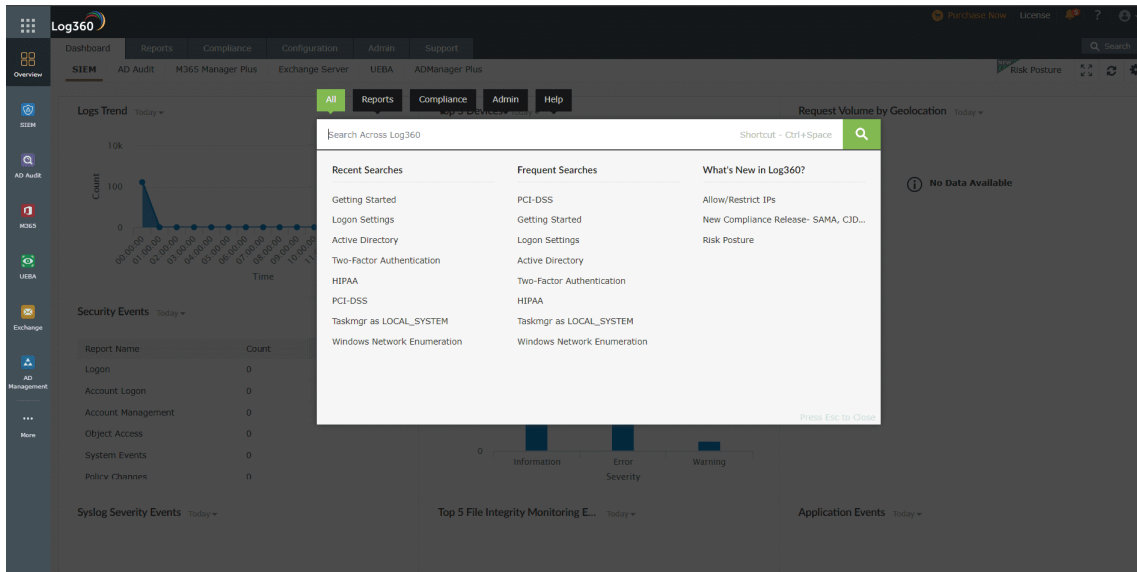
- Type the setting/report/compliance/help document that you're searching for and click on the desired result.

  (For instance, to search for reports related to file modifications, type "file modifications" in the search bar. All relevant reports, help documents, and settings will be displayed. You can directly navigate to the required page by clicking on the search results.)

  Note: If you click **Enter**, Global Search will open the page of the first result that is displayed.
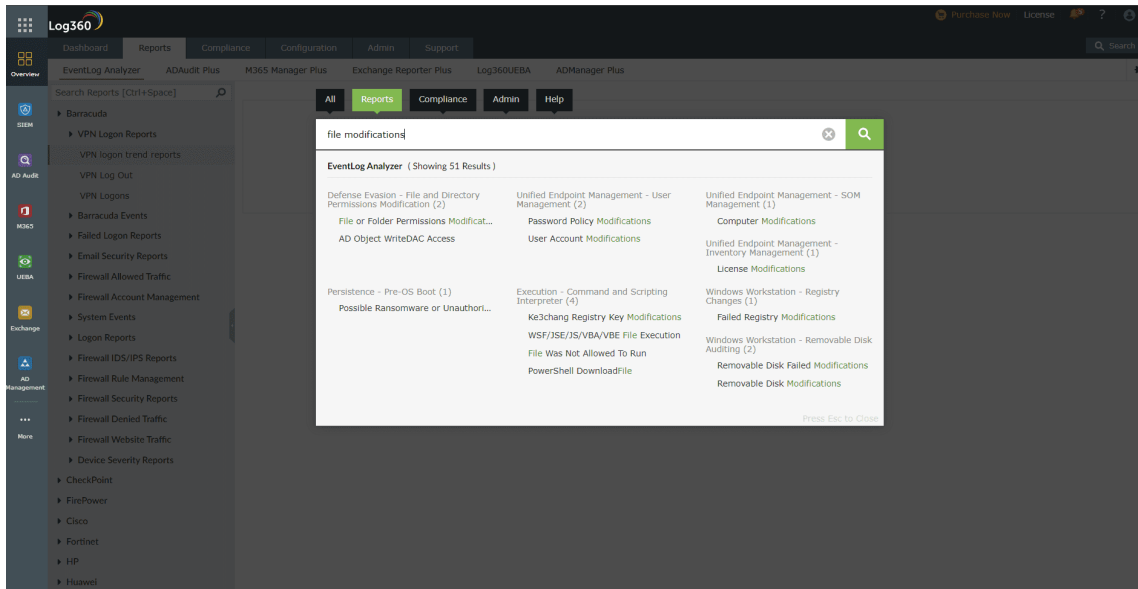
- Similarly, if you wish to search for a particular compliance mandate, you can type the name in the **Search** field, then click on the result to navigate to the required regulation.

Recent Searches:

The Recent Searches section displays recent searches for each tab in the Global Search feature.

Frequent Searches:

The Frequent Searches section displays the most searched queries in Log360.

What's New in Log360:

This section shows the most recently added features in Log360. Clicking on the features will redirect you to the particular feature section.
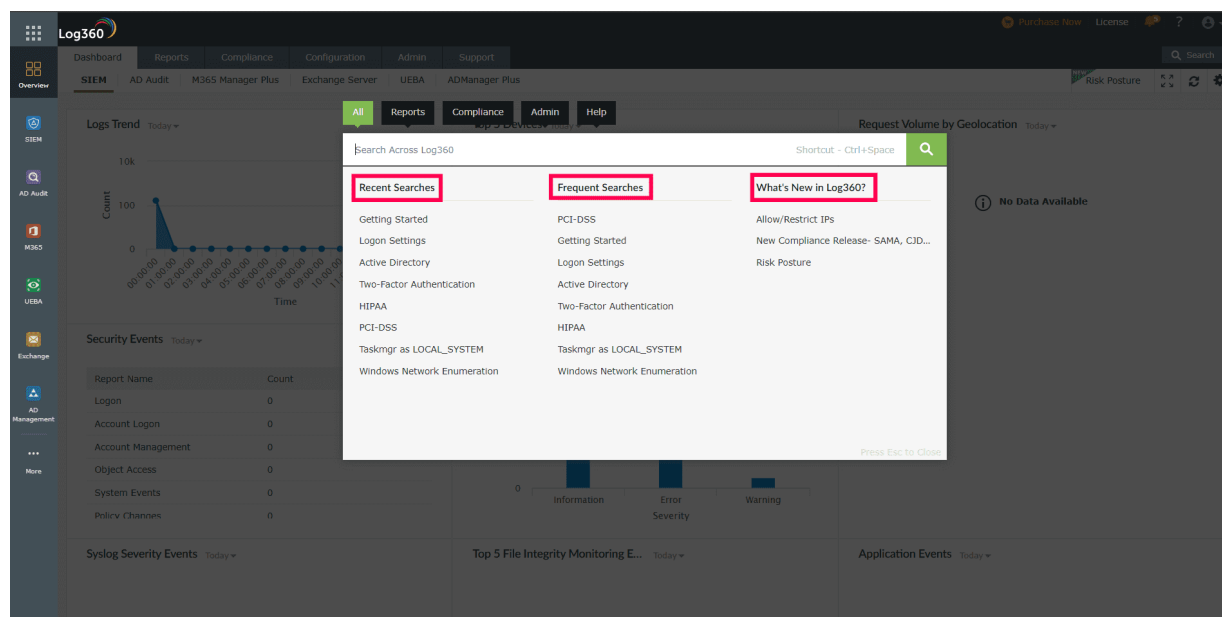
Note: The Reports tab will only appear in Global Search if Log360's Reports page has been accessed before.

8. Log360 Support

In order to analyze issues or other challenges faced by evaluators / customers, Log360 product team might request for product logs (Support Information). This will provide the team a clear understanding of the issue reported.

The creation of the support information can be done either automatically or manually.

How to automatically create and send information:

1. Click on **Support Tab → Support Info → Create System logs: Auto**.

2. This will automatically create a support info file.

> **Note**: The time taken for creating the support info file can vary from a few seconds to minutes depending on the quantity of logs that have been created by the product over time.

3. Once the support info files are ready, save the file locally by clicking on the link provided.

4. Attach the saved zip file and mail it to Log360-support@manageengine.com.

5. Alternatively if the file size is large you can upload the saved file to our server by following the below steps:

   - Type : https://bonitas.zohocorp.com/ on a web browser

   - Select "Log360" from the Product drop down menu

   - Provide your Email address

   - Add a comment

   - Attach the saved support info file from the stored location

   - Click on Upload

How to manually create and send Information

1. Go to the Log360 installation folder.

2. Open the bin folder.

3. Double click on **compressLogFiles.bat** file.

4. Go back to the installation folder and open **logs\archive** folder to find a zip file named in the format **ssmmHHddMMyyyy**.

5. Attach the zip file and mail it to log360-support@manageengine.com.

6. Alternatively if the file size is very large, you can upload the saved file to our server by following the below steps.

   - Type **https://bonitas2.zohocorp.com/** on a web browser.

   - Select **Log360** from the product drop down menu.

   - Provide your email address.

   - Add a comment.

   - Attach the saved support info file from the stored location.

   - Click on **Upload**.

9.1. Knowledge Base

- How do I reset the password of the admin account?
- How do I change the password of the admin account?
- How do I install Log360 as a Windows service?
- How to I manually backup and restore the database in Log360?
- How do I move Log360 to a new server?
- How do I change the port number of Log360?

9.2. Reset Admin Password

How do I reset the password of the admin account?

To reset your admin password,

- Navigate to **<Installation_Dir>\bin** folder. By default, the path is set as **C:\ManageEngine\Log360\bin**.
- Find and run the **resetADSPassword.bat** file.
- Your password will now be reset to the default password "admin".

> **Note**: This process will reset both the default admin password and the two-factor authentication (2FA) settings.

9.3. Change Admin Password

How do I change the password of the admin account?

To change the password of your admin account,

- Click the ▼ icon located at the top right corner of Log360 window and click **Change Password.**
- In the change password page, enter the old password. Then, enter the new password and confirm it by keying in the new password in the **Confirm Password** field.
- Click **Change Password.**

Alternatively, you can also:

- Click the **Admin** tab.
- Navigate to **Administration → Logon Settings → Change Password**.
- Enter the old and new passwords. Confirm the new password by keying in the new password in the **Confirm Password** field.
- Click **Change Password.**

9.4. Install Log360 as a Windows service

How do I install Log360 as a Windows service?

After installing Log360, follow these steps to install the product as a service:

- Navigate to **Start menu → All Programs**.

- Select **Log360**.

- Click on **NT Service folder**.

- Click on **Install Log360 as a Service**.

When Log360 is installed as a service, it runs with the privileges of the system account.

9.5. Manually Backup and Restore Database

How to manually backup and restore the database in Log360?

To backup the Log360 database,

- Start command prompt as an administrator (right-click command prompt and select **Run as Administrator**)
- Navigate to **<Installation_Dir>\bin** folder by using the **cd** command. By default, the path to installation directory is **C:\ManageEngine\Log360**.
- Now, execute the command **app_ctl.bat backupDB** to backup the database.
- A folder named "Backup" will be created at Log360 installation directory (By default: **C:\ManageEngine\Log360**) and it will contain the DB backup in compressed file format.

To restore a Log360 database

- Start command prompt as an administrator (right-click command prompt and select **Run as Administrator**)
- Navigate to **<Installation_Dir>\bin** folder by using the **cd** command. By default, the path to installation directory is **C:\ManageEngine\Log360**.
- Now, execute the command **app_ctl.bat restoreDB backupzip <Installation_Dir>\Backup\ <compressed_file_name>.zip** to restore the database.

9.6. Migrate Server

How do I move Log360 to a new server?

To migrate Log360 to a new server, it is recommended to copy the Log360 folder, the EventLog Analyzer folder, and the Elasticsearch folder to the new server. The following steps describe how to do the same.

Step 1) Stop the services - Log360 and EventLog Analyzer.

- Open Command Prompt as the administrator. Navigate to **<Home> Log360/bin** and execute
    - Shutdown.bat
    - app_ctl.bat stopDB
- Open Command Prompt as the administrator. Navigate to **<Home> EventLog Analyzer/ bin** and execute
    - Shutdown.bat
    - app_ctl.bat stopDB
    - StopSEC.bat
- Open Command Prompt as the administrator. Navigate to **<Home> elasticsearch/ES/bin** and execute
    - stopES.bat

Open Task Manager and end all tasks related to Log360 and EventLog Analyzer.

2) Copy the following folders to the new server

- Log360
- EventLog Analyzer
- elasticsearch

> **Note**: Ensure that the new path is the same as the path in the old server.

After Log360 and elasticsearch folders are moved along with EventLog Analyzer, if the new path is not the same as the previous path, then **path.data** and **path.repo** should be updated accordingly in the following files:

- **<ManageEngine Home>\elasticsearch\ES\config\elasticsearch.yml** (as shown in the image below).
- **<EventLog Analyzer Home>\ES\config\elasticsearch.yml**

```
elasticsearch.yml - Notepad
File  Edit  Format  View  Help
# ---- sample paths for index location ---
# for windows os,
# path.data : ["C:\\ManageEngine\\EventLog Analyzer\\ES\\data"]
# path.data : ["D:\\NewIndexStorage\\data"]
# for linux os,
# path.data : ["/opt/ManageEngine/EventLog Analyzer/ES/data"]
# path.data : ["/NewIndexStorage/data"]
# path.data : ["//remote machine name/shared folder/data"] //for shared locations
# NOTE:
# parent path should be a valid folder, since adjacent folders will be used for archives and others

cluster.name: LOG360-CLUSTER
indices.query.bool.max_clause_count: 10240
indices.fielddata.cache.size: 50%
node.master: true
node.data: true
path.logs: D:\ManageEngine\EventLog Analyzer\ES\logs
path.data:
- D:\ManageEngine\EventLog Analyzer\ES\data
path.repo: D:\ManageEngine\EventLog Analyzer\ES\repo
script.inline: true
script.stored: true
indices.store.throttle.max_bytes_per_sec: 100mb
discovery.zen.minimum_master_nodes: 1
bootstrap.system_call_filter: false
cluster.indices.tombstones.size: 0
searchguard.disabled: false
searchguard.ssl.transport.pemcert_filepath: certificates/localnode.pem
searchguard.ssl.transport.pemkey_filepath: certificates/localnode.key
searchguard.ssl.transport.pemtrustedcas_filepath: certificates/root_ca.pem
searchguard.ssl.transport.enforce_hostname_verification: "false"
searchguard.ssl.transport.resolve_hostname: "false"
searchguard.ssl.http.enabled: false
http.enabled: false
searchguard.ssl.http.pemcert_filepath: certificates/localnode.pem
```

3) Installing services on the new server.

- Open Command Prompt as the administrator. Navigate to **<Home> Log360/bin** and execute
  - InstalNT service.bat
- Open Command Prompt as the administrator. Navigate to **<Home> EventLog Analyzer/ bin** and execute
  - service.bat -i

4) Start Log360

Start → All Programs → Log360 → Start Log360

> **Note:**
>
> - If you have enabled log forwarding from any Linux, Unix, router, switch, firewall, or syslog devices to EventLog Analyzer, you would need to re-point them to the new server.
>
> - If an agent has been configured for any device, check if it has been modified appropriately.
>
> - Do not delete the previous installation until you ensure the migration is successful. Verify the migration by checking the log collection after 30 minutes.

Eventlog Analyzer distributed migration

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 are changed now.
6. Restart the Admin Server.

7. Now, start the Managed Server.

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 needs to be success.

Check the below links for other components of Log360:

- ADAudit Plus
- M365 Manager Plus
- Exchange Reporter Plus
- Log360 UEBA
- DataSecurity Plus
- ADManager Plus
- PAM360

> **Note**: This applies for Eventlog Analyzer MSSP edition as well.

9.7. Change Port

How do I change the port number of Log360?

To change the port number in Log360,

- Go to the **Admin** tab.
- Navigate to **General Settings → Product Settings**.
- If you wish to use HTTP, select the **HTTP** field under **Connection Type** and enter the new port number.
- If you wish to enable secure socket layer, select **HTTPS** and enter the appropriate port number.
- Click **Save**.
- Restart Log360 for the changes to take effect.

9.8. NTLMv2 SSO configuration

Log360 uses Jespa to provide NTLMv2 SSO. To enable NTLMv2 SSO in Log360 and all integrated components in builds 5282 and above, follow the steps listed below.

> **Note for customers who are on build 5281 or lower**: If you have already enabled NTLMv2 SSO, you can continue using the feature without having to perform the following steps.

1. Download the latest Jespa JAR file.

2. Add the downloaded file to the <log360_install_directory>/lib folder. <log360_install_directory> is the location where Log360 is installed.

> **Note**: If you have integrated components such as ADManager Plus and ADAudit Plus with Log360, ensure you've added the Jespa JAR file in the respective component's lib folder as well.

3. Restart Log360 and all the other integrated components for the changes to take effect.

Please contact log360-support@manageengine.com if you require any assistance in configuring NTLMv2 SSO for your users.

10.1. Troubleshooting Tips

Log360 Integration

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.

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.

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 belongs to the selected component and try again.

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**.

Communication Failure

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

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 still persists, contact log360-support@manageengine.com

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 click **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.

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**.

Log360 and child components won't automatically start after server reboot

Choose the "Automatic (Delayed Start)" option instead of "Automatic" in product service startup type.

Dashboard

Unable to view one or more of the components' dashboard.

Following are the list of situations that may hinder the dashboard view of the components:

- **Component Setup:** To view the dashboard of Log360, you must first download and install its components. Only when a component is installed and integrated with Log360, you can view its dashboard. If you have already installed the component, make sure that any change made to the hostname and port number of a component is reflected under the Log360 integration tab in Administration settings of Log360. Click here to learn more about installing and integrating the components with Log360.
- **Domain Selection:** It is possible to configure different domains with different components. As you switch between the dashboard views of different components, make sure that the domain that you have configured with that component is selected. Also, make sure that you have logged in with the appropriate credentials to view the dashboard of the domain you have selected.

Product Settings

Please enter a HTTP port number that is not used by other applications.

Description:

This error may occur when you are trying to enable HTTPS. When you try to enable HTTPS, Log360 will automatically assign a port number for HTTP based on the HTTPS port number you've chosen. And if that new HTTP port number is used by some other application, then this error occurs.

Solution:

- Once you get the error, select **HTTP**.
- Change the port number to something that is not in use by another application.
- Now, select **HTTPS**.
- Click **Save**.

Increasing Log360 heap size.

An effective way to enhance Log360 responsiveness and efficiency is by increasing the heap size.

- Navigate to the Log360 installation directory and find the Log360 configuration file in <Log360>/conf/ directory.
- Open the configuration file named wrapper.conf for editing.
- In the configuration file, you will find the initial and maximum heap size settings. Modify them as follows:
  - Initial Java Heap Size:
    - Find wrapper.java.initmemory=1024.
    - Change this value to the required size in MB for your system.
  - Maximum Java Heap Size:
    - Find wrapper.java.maxmemory=1024.
    - Change this value to the required size in MB for your system.
- After modifying the heap size, save the changes made to the configuration file.
- To apply the new heap size settings, restart Log360.

> **Note:** Administrator privileges are required if Log360 is installed in the C:\Program Files\ directory. Otherwise, a local account with write permissions for the relevant files is sufficient to change the heap size.

Product Start-up

Log360 and child components won't automatically start after server reboot

Product Start-up

Log360 and child components won't automatically start after server reboot even though they are installed as service.

Cause:

This might be due to certain configurations or performance issues that might happen during the server startup.

Try this solution:

Choose the "Automatic (Delayed Start)" option instead of "Automatic" in product service startup type.

Search Engine Management

- Check the bootstrap settings provided.
- **JRE version**: Supported JRE version is 1.8 and above, JRE should be a server JVM.
- **Increase file descriptors**: Make sure to increase the limit on the number of open files descriptors for the user running Elasticsearch to 65,536 or higher. For the .zip and .tar.gz packages, set **ulimit -n 65536** as root before starting Elasticsearch, or set **nofile** to **65536 in /etc/security/limits.conf**.This is applicable only for Linux and macOS.
- **Ensure sufficient virtual memory**: Elasticsearch uses a mmapfs directory by default to store its indices. The default operating system limits on mmap counts is likely to be too low, which may result in out of memory exceptions. You can increase the limits by running the following command as root in Linux: **sysctl -w vm.max_map_count=262144**
- **Disable swapping**: Usually Elasticsearch is the only service running on a box, and its memory usage is controlled by the JVM options. There should be no need to have swap enabled. On Linux systems, you can disable swap temporarily by running: **sudo swapoff -a** and on Windows, the equivalent can be achieved by disabling the paging file entirely by going to **System Properties → Advanced → Performance → Advanced → Virtual memory**.
- **Ensure sufficient threads**: Elasticsearch uses many thread pools for different types of operations. It is important that it can create new threads whenever needed. Make sure that the number of threads that the Elasticsearch user can create is at least 4096. This can be done by setting **ulimit -u 4096** as root before starting Elasticsearch, or by setting **nprocto 4096 in /etc/security/limits.conf**.
- **JVM DNS cache settings**: Elasticsearch runs with a security manager in place. With a security manager in place, the JVM defaults to caching positive host name resolutions indefinitely. If your Elasticsearch nodes rely on DNS in an environment where DNS resolutions vary with time, then you might want to modify the default JVM behavior. This can be modified by adding **networkaddress.cache.ttl=<timeout>** to your Java security policy.
- **Port availability**: Ensure that **port 9322** is available on the machine that will run Elasticsearch.
- **Sharing of <Installation Dir>/EventLog Analyzer/ES/repo**: Ensure that the folder **<Installation Dir>/EventLog Analyzer/ES/repo** is shared with the service account of the Log360 server. This folder will be used to create snapshot from Elasticserch to save archives. If the Log360 server is not in AD, it will be an open share or else make sure that the user has the permission to share the folder and follow the steps below.
  - Share the folder **<Installation Dir>/EventLog Analyzer/ES/repo** manually with the Log360 server.
  - Copy the shared path of **<Installation Dir>/EventLog Analyzer/ES/repo** directory.
  - Navigate to **<Installation Dir>/EventLog Analyzer/ES/config/dae.properties** file and specify the copied path as the value for **node.repo.sharedlocation**.
  - Restart the EventLog Analyzer server.

- **Check IP address configuration**
- Open command prompt and run ipconfig/ifconfig. This will return the current IP address
- Open the file stored at **<Log360 Installation Dir>/../elasticsearch/ES/config/dae.properties**". Check the value of the following paramater **node.local.ip.** If it is not the same IP address from the previous step then update the paramater **allow_restart_on_ip_change** to true. This will restart Elasticsearch with a new IP address.
- **Check if Elasticsearch is running**

- You can use the following command to see if Elasticsearch is running or not: **netstat -aon|findstr 9322| findstr LISTENING**

EventLog Analyzer's Elasticsearch is not connected

- Check if EventLog Analyzer is running.
- Update EventLog Analyzer from the Integration page.
- Check if firewall is blocking ports (9300-9400).

JRE version is not compatible

- Java version should be higher than 1.8 and it should be a server JVM.

Installation Failed

- **Restart required**: The Elastiscsearch service is marked for deletion, the system will delete the service after restart.

Server network not accessible or incorrect credentials

- Make sure that the Log360 server is able to access the admin share of the target host. Refer: https://www.wintips.org/how-to-enable-admin-shares-windows-7/

Shared path is not accessible

- Ensure that the machine in which EventLog Analyzer is installed is accessible from the Log360 machine.
- Please make sure the user starting EventLog Analyzer has the proper permission to share the folder.
- To share the folder manually follow the steps below.
    - Share the folder **<Installation Dir>/EventLog Analyzer/ES/repo** manually with the Log360 server.
    - Copy the shared path of **<Installation Dir>/EventLog Analyzer/ES/repo** directory.
    - Navigate to **<Installation Dir>/EventLog Analyzer/ES/config/dae.properties** file and specify the copied path as the value for **node.repo.sharedlocation**.
    - Restart the EventLog Analyzer server.

Deletion of node failed

- Ensure that all the nodes are connected, as deletion can fail if another node is not connected.

Data Path Not Accessible

- **What is Elasticsearch Data Path?**

  Elasticsearch writes the data you index to indices, and data streams to a data directory which is available in elasticsearch.yml. Search and indexing won't work if the data path is not accessible.

  If the data path is not accessible to write, the following notification will be shown.
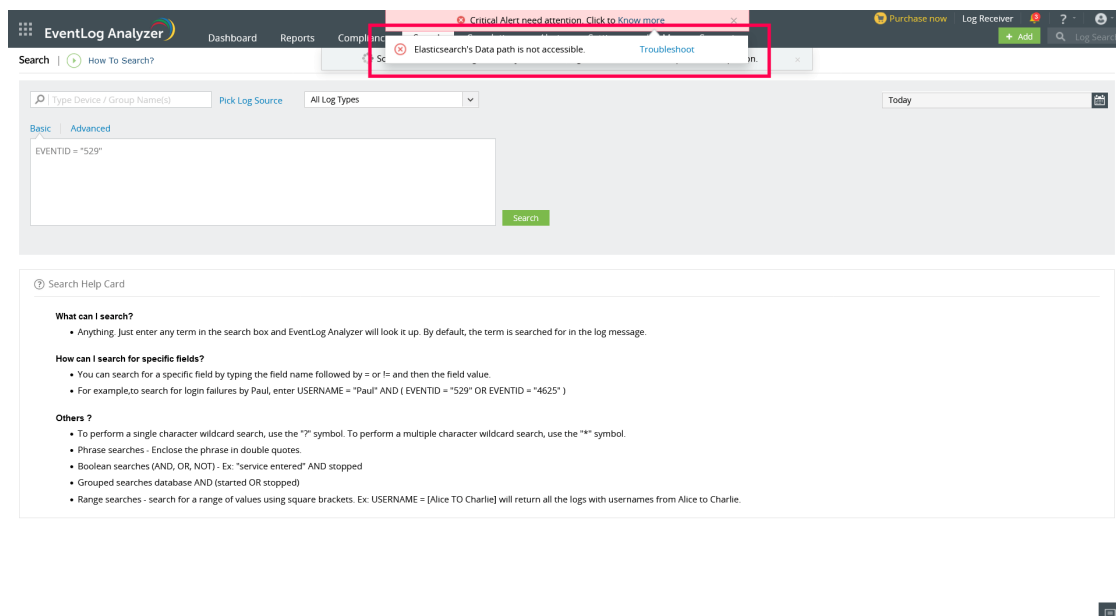
Troubleshooting steps

- Open elasticsearch.yml file,search for **path.data** and find its value. **elasticsearch.yml** file can be found in the locations given below.
    - <Log360 Installation Dir>/../elasticsearch/ES/config/elasticsearch.yml if the notification is from **ManageEngine Log360**
    - <Installation Dir>/EventLog Analyzer/ES/config/elasticsearch.yml if the notification is from **ManageEngine EventLog Analyzer**
- Make sure that both read and write permissions are enabled for the service account running EventLog Analyzer/Log360.
- If the path is a network location, then ensure connectivity and that the network path is accessible from the machine running EventLog Analyzer/Log360. Verify that there are no latency issues between the server and remote data path.
- If there is a need to change the data path of Elasticsearch, kindly follow this guide.

10.2. SSL Troubleshooting Tips

This section will help you to troubleshoot any SSL server certificate related issues that you might encounter in the product.

Error Messages

Blocked Content

Description:

This problem arises when Log360 is configured to use HTTPS under connection settings and integrated component is configured to use HTTP. As a result, you will not be able to access the component from the apps pane.

Resolution:

If Log360 is configured with HTTPS, then you must configure the integrated components to use HTTPS (SSL) to successfully access the components from the apps pane.

Certificate Name mismatch

Description:

This error occurs when the common name of the SSL Certificate doesn't exactly match the hostname of the server in which the component is installed.

Resolution:

Please get a new SSL certificate for the current hostname of the server in which the component is installed.

Hostname mismatch

Description:

This error occurs when the component's SSL certificate is issued for a hostname that is different from the Log360's hostname. For example, Log360 could be installed on a parent domain and the component could be running on a child domain.

Resolution:

In this scenario, you can configure a valid SSL wildcard certificate and apply it to both the component and Log360.

Invalid Certificate

Description:

This error occurs when the SSL certificate you have configured with the component is invalid. A certificate can become invalid if it has expired or other reasons.

Resolution:

Please configure the component to use a valid SSL certificate.

Problem in trusting the security certificate

Description:

This error occurs when any component integrated with Log360 is of an older build.

Resolution:

Upgrade all integrated components to the latest build to resolve this issue.

For certificates signed by Public Certificate Authority

If the certificate is signed by Public Certificate Authority, follow the steps below:

- Open browser settings
- Open Privacy / Privacy and Security Tab
- Under Security Tab, click on Manage Certificates.
- Please make sure the CA certificate is not under Untrusted Publishers.
- If the certificate is not under Untrusted Publishers, open the Trusted Root Certification Authorities tab to check if the Public Certification Authority you signed is available.
- If it is not available, please import the Certification Authority certificate and restart the browser.

For certificates signed by a Local Certificate Authority or it is self signed

If the web client is accessed under Domain machine, Please follow the below steps.

- Start the Group Policy Management snap-in.
- Right-click the respective GPO, and then click Edit.
- Open Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies, right-click Trusted Root Certification Authorities, and then click Import.
- On the Welcome to the Certificate Import Wizard page, click Next.
- On the File to Import page, choose the certificates, and then click Next.
- On the Certificate Store page, click Place all certificates in the following store, and then click Next.
- On the Completing the Certificate Import Wizard page, verify that the information you provided is accurate, and then click Finish.

If the web client is accessed under a Non-domain machine, Please follow the below steps.

- Open Browser settings
- Open Privacy / Privacy and Security Tab
- Under Security Tab, click on Manage Certificates.
- In the Certificates popup, open Trusted Root Certification Authorities.
- Please import the Certification Authority certificate and restart the browser.

11. Frequently Asked Questions

General product information

1. What is Log360?

Log360 is a comprehensive SIEM solution that integrates log management and AD auditing components into a single dashboard. With this web-based solution you can,

- **Manage log data:** Collect, monitor, analyze, correlate, and archive log data from sources across the network.

- **Monitor privileged users:** Track all activities including logon and logoff activities of privileged users. Get detailed session monitoring reports as well.

- **Comply to IT mandates:** Be 100% compliant to various regulatory mandates including PCI DSS, HIPAA, FISMA, GLBA, ISO 27001, SOX, and more.

- **Audit AD in real-time:** Audit all critical changes to Active Directory objects and get notified via email or SMS in real-time.

- **Protect confidential data:** Monitor and track critical changes including creation, deletion, modification, and more happening to sensitive information on files/folders.

- **Track GPO and OU changes:** Audit critical changes to your AD GPOs and OUs in real-time and get instant alerts.

- **Perform database auditing:** Monitor all database activities, database server logons and logoffs, database server account changes, and more.

2. Is it necessary for Log360 and its integrated products to be installed on a domain-joined device?

No, Log360 can be installed on any device, whether it's domain-joined or part of a workgroup, as long as the system meets the necessary prerequisites. It will function properly in either case.

3. I have already deployed ADAudit Plus in my environment. Why should I get Log360 now?

Your ADAudit Plus deployment would've simplified your Active Directory monitoring and auditing challenges. However, when it comes to securing the entire organization's network, you need a complimentary solution that can manage, monitor, and audit other aspects of your network.

You need to go for Log360 as it brings both ADAudit Plus and the comprehensive log management solution viz., EventLog Analyzer together in a single console.

The EventLog Analyzer component complements the functionality of ADAudit Plus and also helps you to continuously monitor the entire network including network devices, Linux/Unix servers, IBM AS400 servers,

applications, databases, Hyper Vs, and cloud environments such as Amazon AWS EC2 instances.

4. I have already deployed EventLog Analyzer in my environment. Why should I get Log360 now?

Your EventLog Analyzer deployment would've simplified your log management and compliance challenges. However, when it comes to SIEM, you need in-depth auditing of the Identity Access and Management (IAM) suite so as to mitigate internal security threats.

You need to go for Log360 as it brings both EventLog Analyzer and the real-time Active Directory auditing, monitoring, and alerting solution viz., ADAudit Plus together in a single console.

The ADAudit Plus component, complements the functionality of EventLog Analyzer and in addition to that provides detailed reports and real-time alerts that help in monitoring and auditing critical changes to Active Directory environment, track user behavior, auditing file servers and more.

5. What are the requirements that are needed for installing Log360?

Hardware requirements

Hardware	Minimum requirements	Recommended System
Processor	Dual Core	8+ Core
RAM	4 GB	8+ GB
Disk Space	40 GB	Depends on the log flow rate

Software requirements

ManageEngine Log360 supports the following Microsoft Windows operating system versions:

- Windows 2003
- Windows 2008, 2008R2
- Windows 2012, 2012R2
- Windows XP
- Windows Vista
- Windows 7,8, and 10

Supported Browsers

ManageEngine Log360 requires one of the following browsers to be installed on the system to access the Log360 web client.

- Microsoft Edge
- Firefox
- Chrome

- Safari 5 and above

6. Can I access Log360 over internet?

Yes. Once Log360 has been deployed and started, the web client can be accessed from anywhere.

7. Do I need any prerequisite software to be installed before using Log360?

No, Log360 does not require any prerequisite software to be installed.

Licensing

1. How is Log360 licensed?

Log360 is licensed based on the number of devices that you add for monitoring. The solution has two components viz.,

- EventLog Analyzer, the log management component wherein you can add any device including,
    - Linux/Unix servers
    - IBM AS400 machine
    - Network devices such as routers, switches, firewalls, and IDS/IPS
    - Application log sources such as IIS & Apache web servers, DHCP Linux/Unix servers, databases including Oracle and MS SQL, vulnerability scanners, and threat intelligence solutions
    - Windows servers and workstations

    Click here to view the entire list of supported devies.
- ADAudit Plus, the active directory auditing component wherein you can add the following servers for auditing,
    - Domain controller
    - Member servers
    - File servers
    - NetApp servers, EMC servers

Log360 license is based on both the number of devices that you need to monitor and the number of servers that you wish to audit.

2. If I had bought member server license in ADAudit Plus component, will I be able to monitor the same server in EventLog Analyzer component too? Or do I need to get the separate license ?

When you buy the auditing license for member server in ADAudit Plus component, you will be able to monitor the same server in EventLog Analyzer component too.

The member servers added for auditing will be automatically synchronized with EventLog Analyzer without any additional license.

3. If I choose not to buy auditing component of Log360, can I do so? Will the log management component function alone?

Yes. You can choose to disintegrate any of the components from Log360. To remove any of the components,

- Go to **Admin tab > Corresponding component**
- Click on the **Remove** button to remove the corresponding component

Integration

1. What are synced hosts?

Any device or server added in one of the components of Log360 will be automatically synchronized with the other component. Such devices or servers are termed as synced hosts.

For instance, when you add a member server in ADAudit Plus component of Log360, the server will be automatically synchronized with EventLog Analyzer components as well. In this case, that particular member server is a synced host.

2. I'm running Log360. However, I haven't purchased auditing component yet. Now I want to try it out. How do I purchase and integrate it with Log360?

Once you have Log360 in place, at any point of time you can purchase and integrate the ADAudit Plus component to audit the servers.

All you need to do is, get the corresponding license of ADAudit Plus by contacting us. Once you have purchased the license, follow the below steps:

- Apply the license file in the product.
- Go to **Admin tab > ADAudit Plus** .
- Click on **Update**.

The ADAudit Plus component will now be integrated.

3. How do I synchronize ADAudit Plus hosts with that of EventLog Analyzer?

All the hosts between ADAudit Plus and EventLog Analyzer will be automatically synchronized everyday at 12.00am. In case need to sync the host manually, follow the below steps

- Click on the **Admin** tab.
- Go to Log360 Integration window.
- Click on the **Sync Now** button in the top right corner of the window.

The hosts will now be integrated automatically.

Uninstallation

1. Can I remove any one of the components alone from Log360? Will the solution be still functional?

Yes. At any point of time, you can remove any one of the components from Log360. To do so, follow the below steps:

Steps for disintegration:

1. Open the Log360 web console with admin account.
2. In the Log360 overview tab, click Admin> Administration> Log360 integration to view all integrated components.
3. From the list of components, identify the component you wish to disintegrate. For example, if you need to disintegrate the EventLog Analyzer integration, click on the **Modify** button next to it.
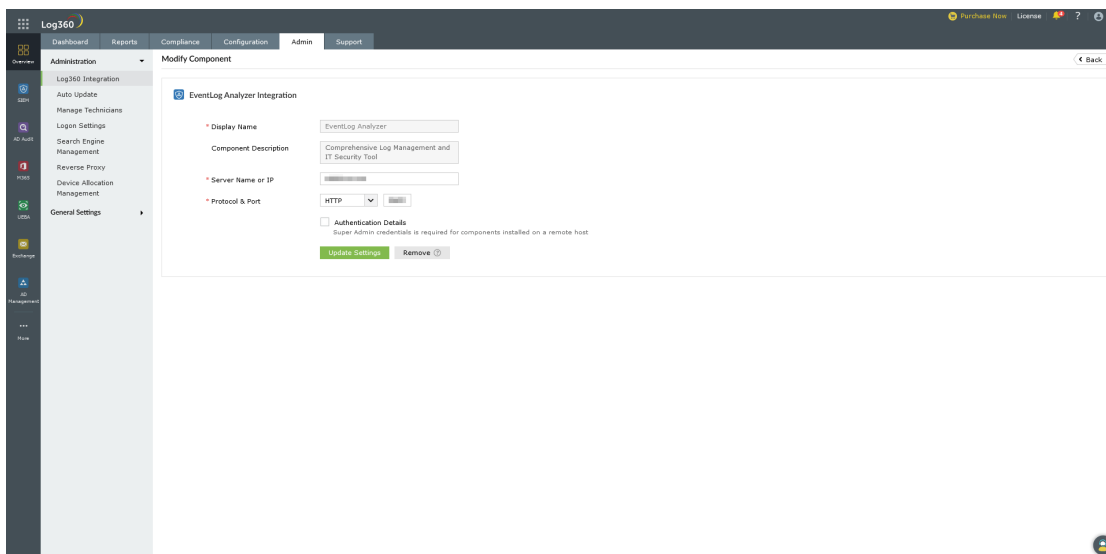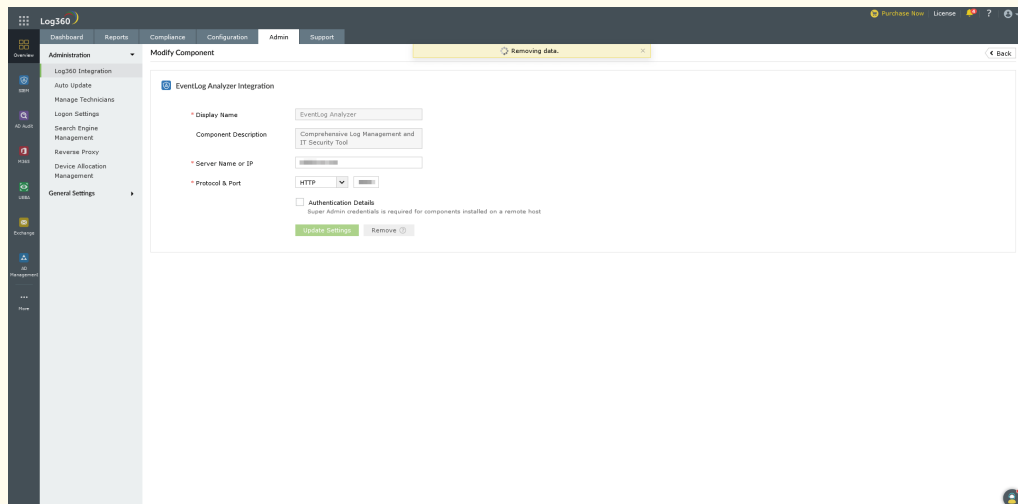

4. Initiate disintegration:
   - For the selected component, verify details such as **Display Name, Component Description, Server Name or IP**, and **Protocol & Port**.
   - Then click on **Remove**.
   - Click **OK** to confirm removal in the confirmation dialog box.
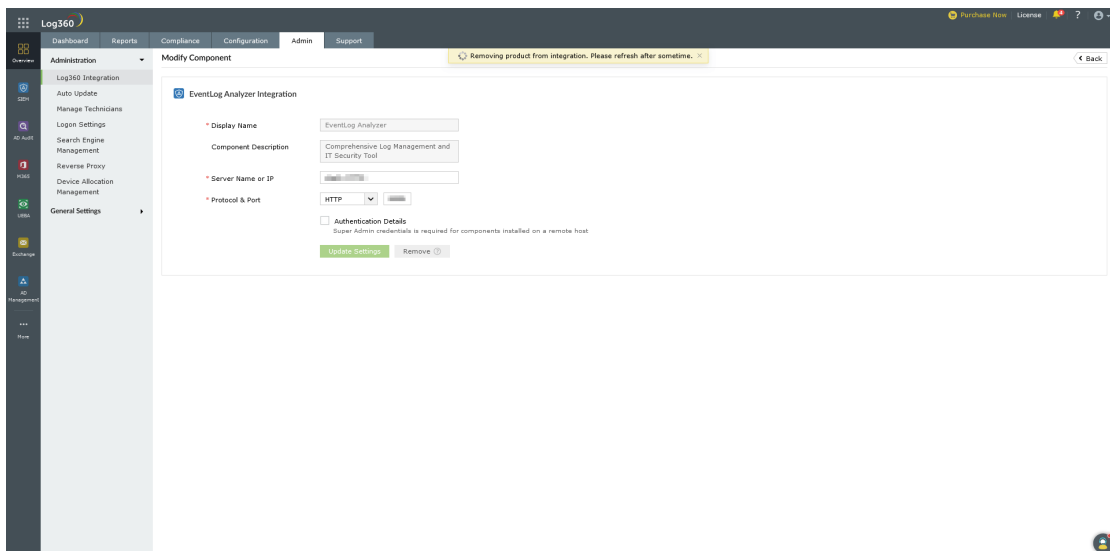
Note:

- Please do not stop the service of the component you are disintegrating. For instance, the EventLog Analyzer service should remain active throughout the disintegration process. This is essential as it ensures that any data in the common ES is seamlessly migrated to the internal ES during disintegration.
- Removing integration of Eventlog Analyzer may require considerable time depending on the size of your data. Users must wait until the notification as in the screenshot below disappears, before proceeding.

- Restart EventLog Analyzer once disintegration is successful.

2. How do I uninstall Log360?

To uninstall Log360, follow the below steps:

- Go to **Control Panel**
- Click on **Log360** and click uninstall
- Select **EventLog Analyzer** and/or **ADAudit Plus**. Whichever component is selected will be uninstalled. If you select both the components, then Log360 will be completely uninstalled.