ManageEngine
Log360

ManageEngine Log360

Admin Guide

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
- Logon Settings
- Device allocation management
- Auto Update
- Manage Technicians
- Search Engine Management Securing your SEM nodes
- Reverse Proxy

Log360 Integration

Log360 contains seven 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

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 two 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.
- 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 .

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 easily switch between two components by using the **Jump to** link provided at the top right corner of the Log360 Web Client. Simply place your mouse pointer over the **Jump to** link and select the component to which you want to jump.

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.

Logon Setting

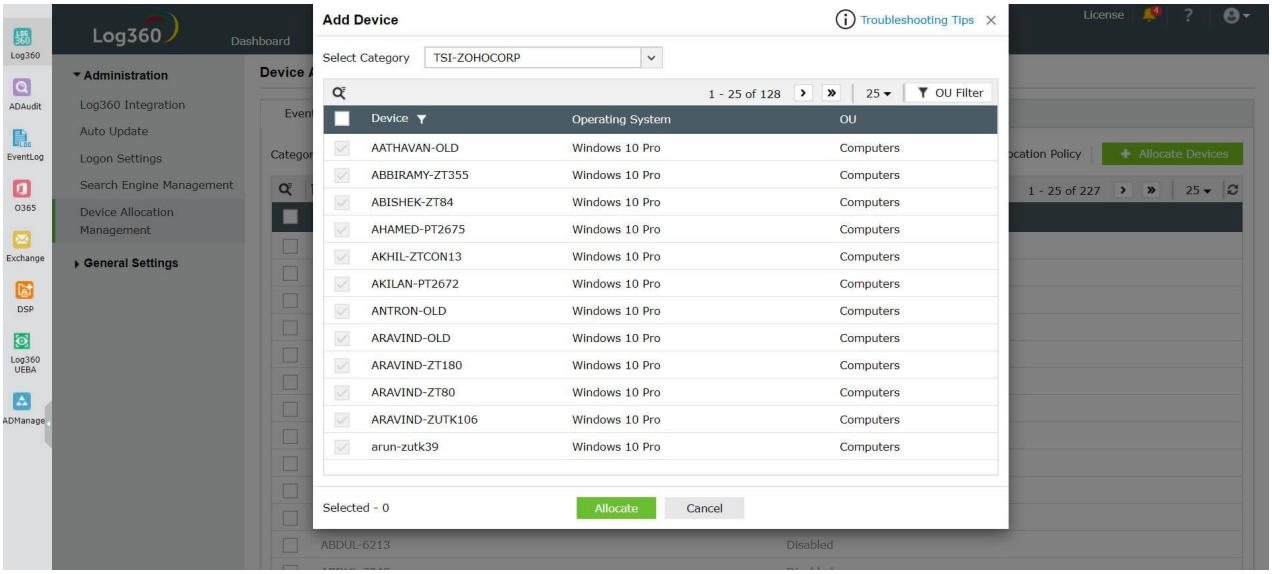
Learn how to configure the following logon settings.

- 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.

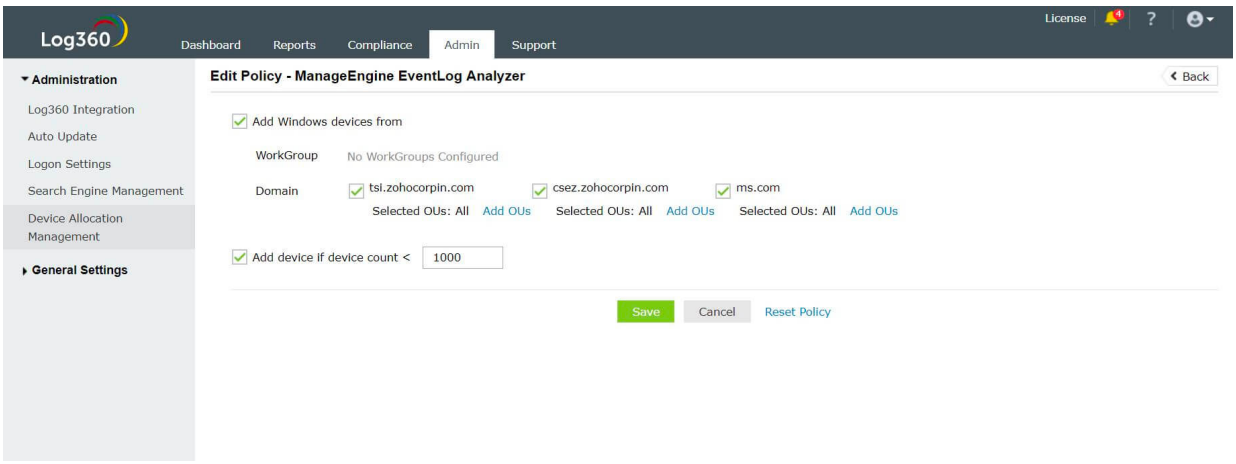
Device allocation module

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 category from the drop down and select the devices from the **Add Devices** window and click **Allocate.**



- 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.

Auto Update

Auto Updated

- Navigate to **Admin** → **Administration** → **Auto 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.**

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.

> **Note:** Limited license of ADManager Plus, Exchange Reporter Plus, and M365 Manager Plus does not include the centralized technician feature.

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

Admin

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

Operator

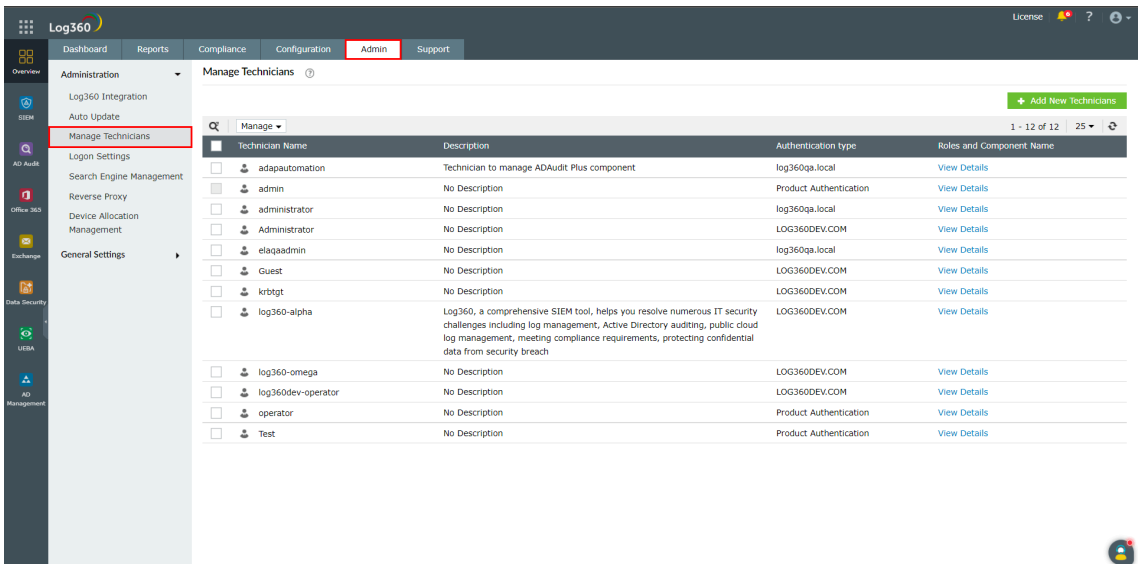
An operator can audit the operations taking place in the application.

How to add a new centralized technician?

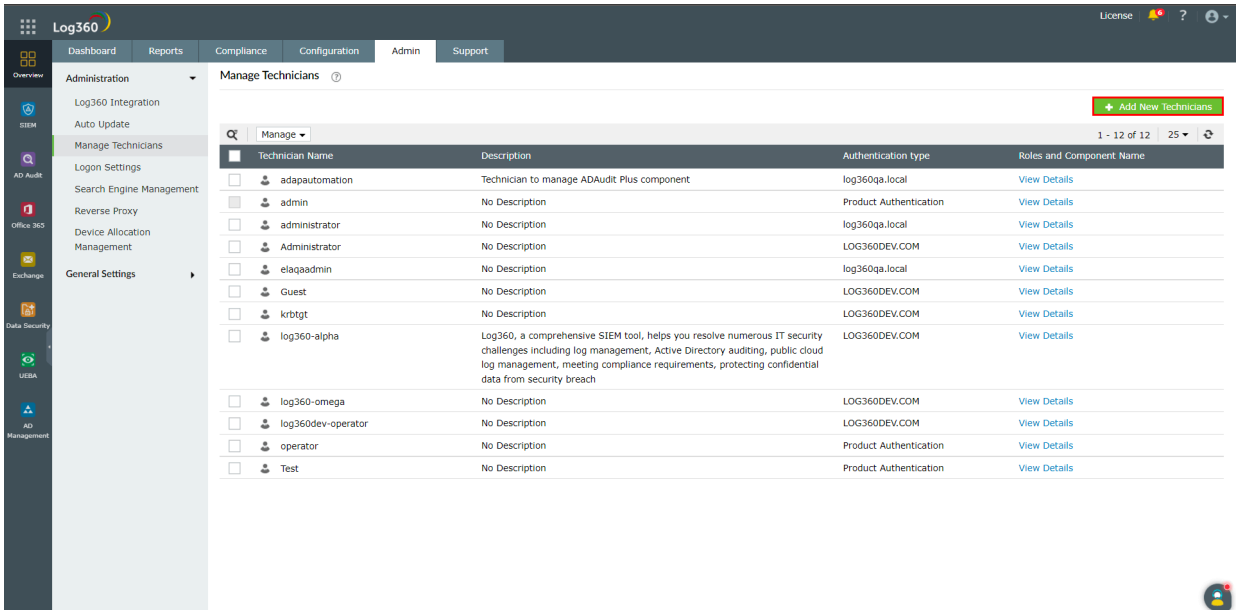
A new centralized technician can be added with authentication by two methods - product authentication and Active Directory authentication.

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

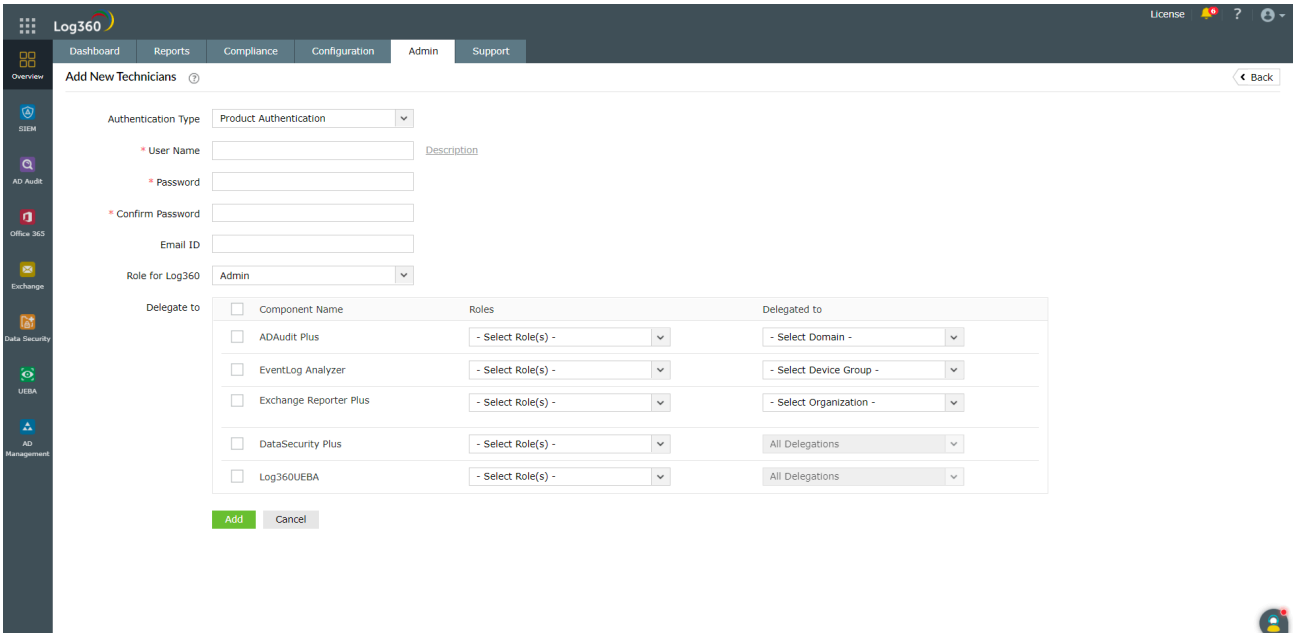
- Under the **Admin** tab, navigate to **Administration → Manage Technicians.**



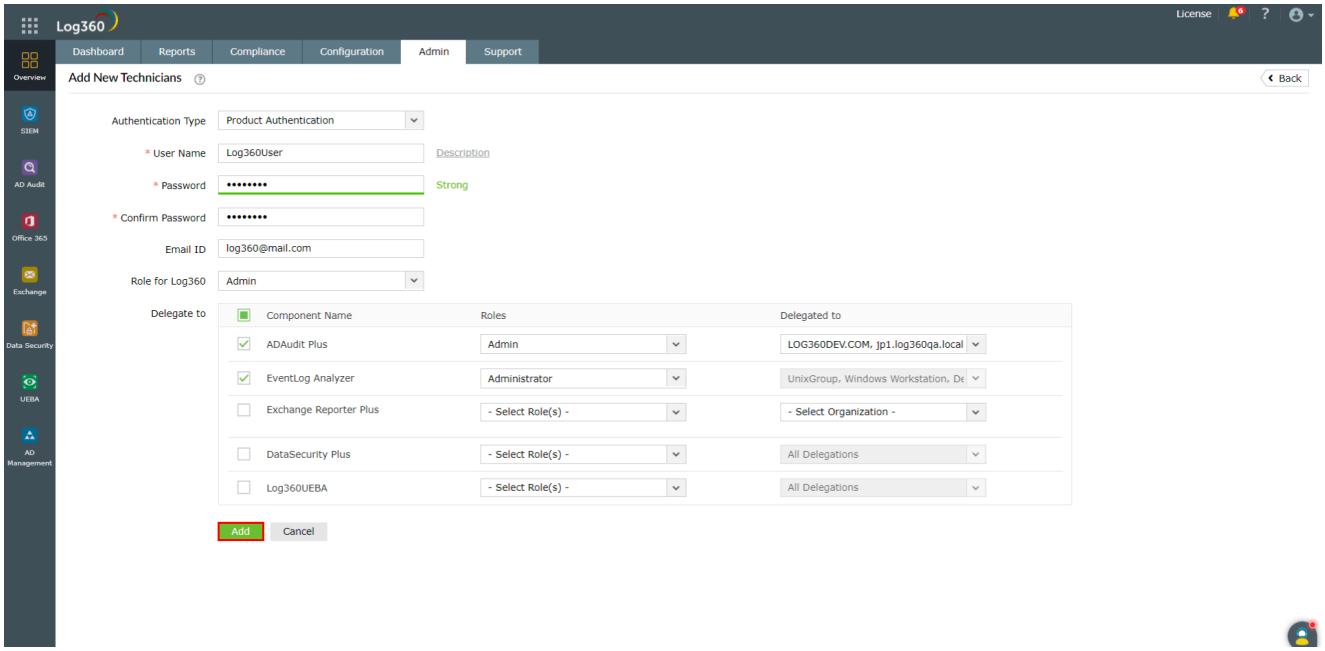
- Then click on the **+ Add New Technicians** button on the top-right corner.



- Enter a name for the technician in the **User Name** field. You can additionally add a description by clicking on the **Description** button.

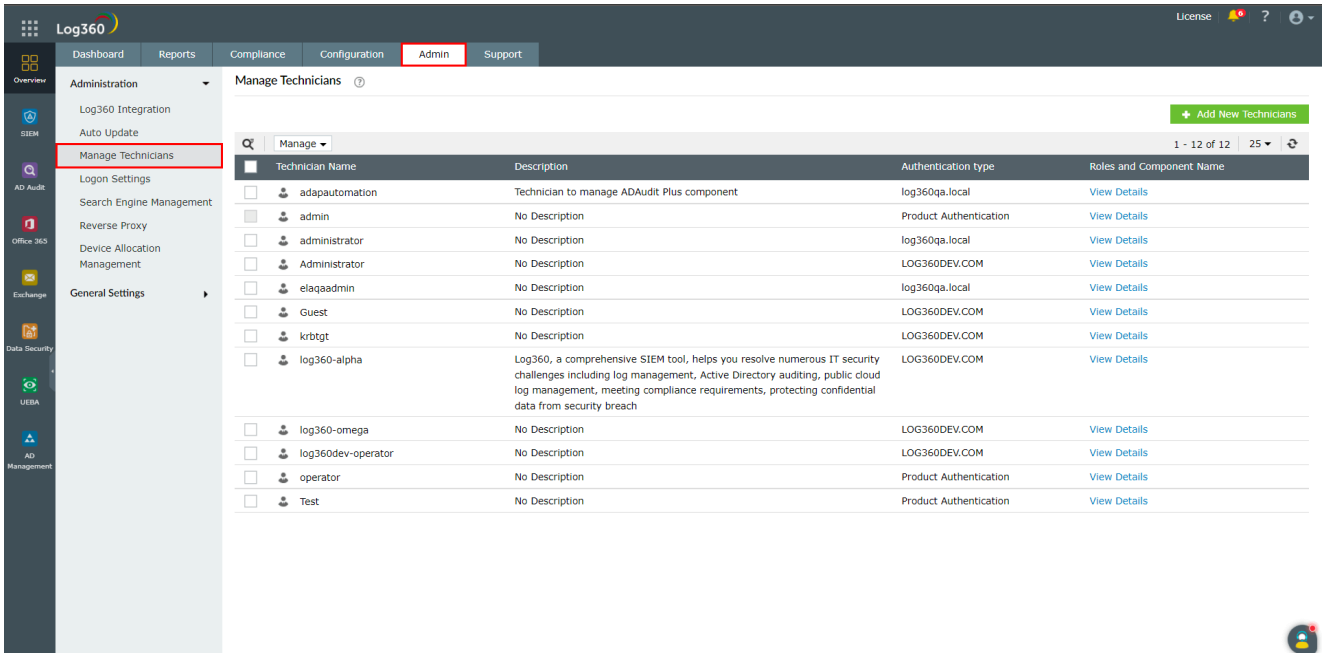


- Enter a new password and confirm it in the respective fields.
- Enter the email address of the technician in the **Email ID** field.
- In the **Roles** drop-down box, choose the role(s) you want to assign to the technician. The permissions applicable to the selected role will be assigned to the technician.
- 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.

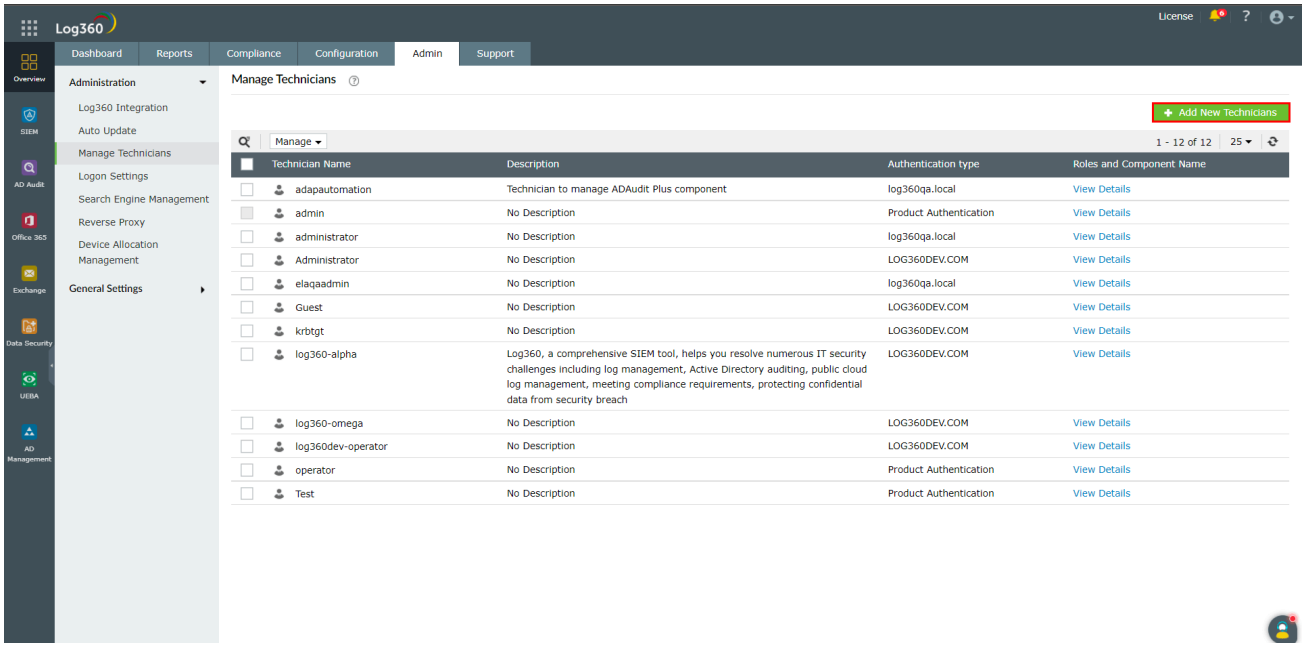


To add new users with authentication by Active Directory, follow the steps given below:

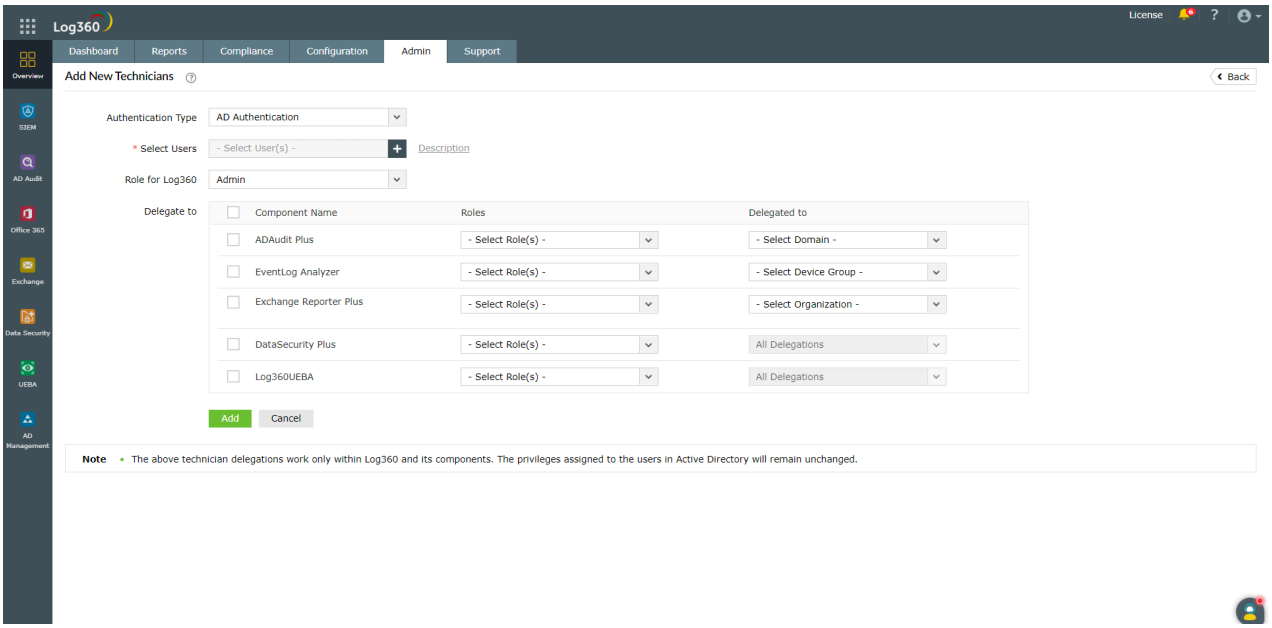
- Under the **Admin** tab, navigate to **Administration** → **Manage Technicians.**



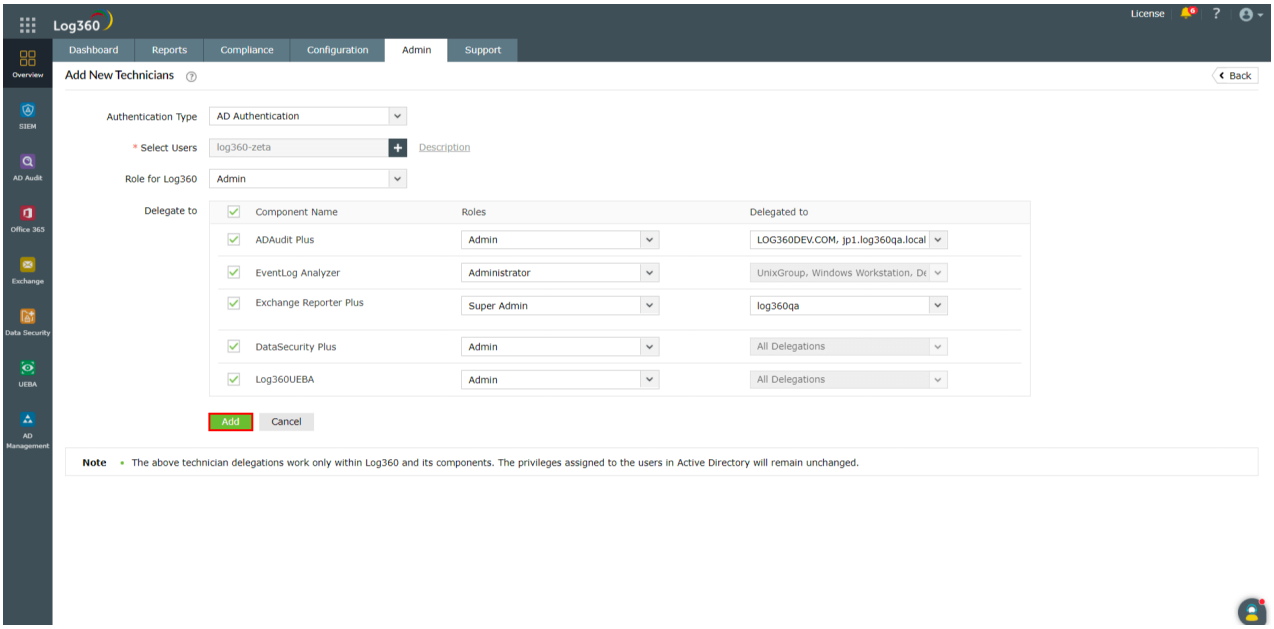
- Then click on the **+ Add New Technicians** button on the top-right corner.



- 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.

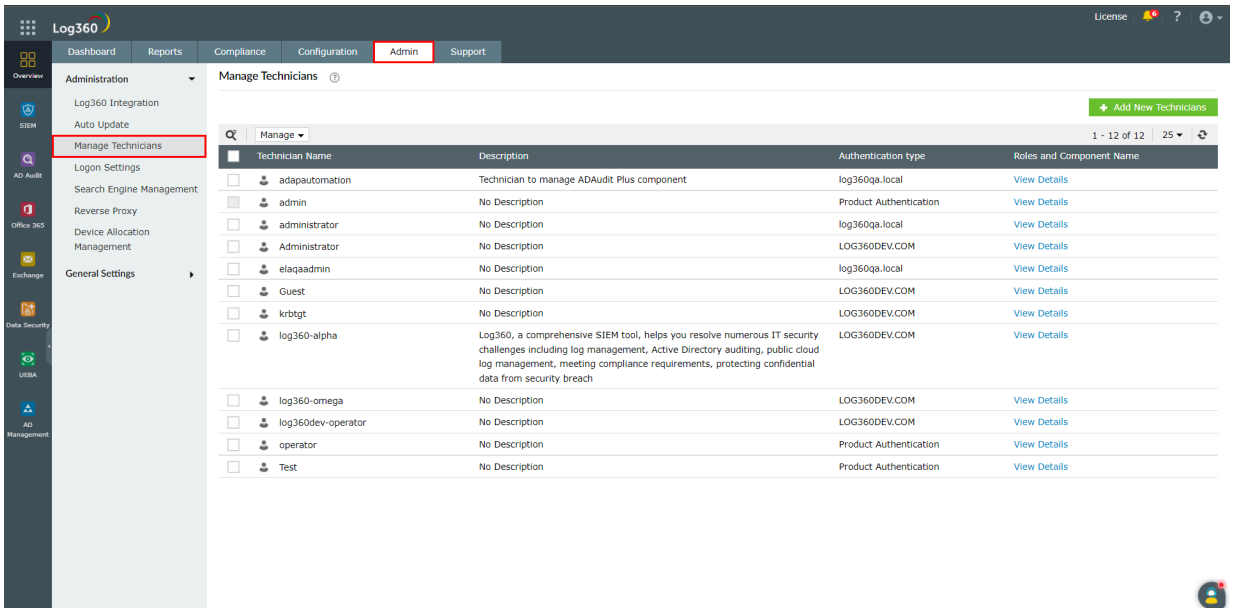


Note: Previously, auto addition of domain technicians in Exchange Reporter Plus and M365 Manager Plus was initiated when the user logs into Log360 using their AD credentials. Now, users are required to create domain technicians separately in each component, or from the centralized technician dashboard.

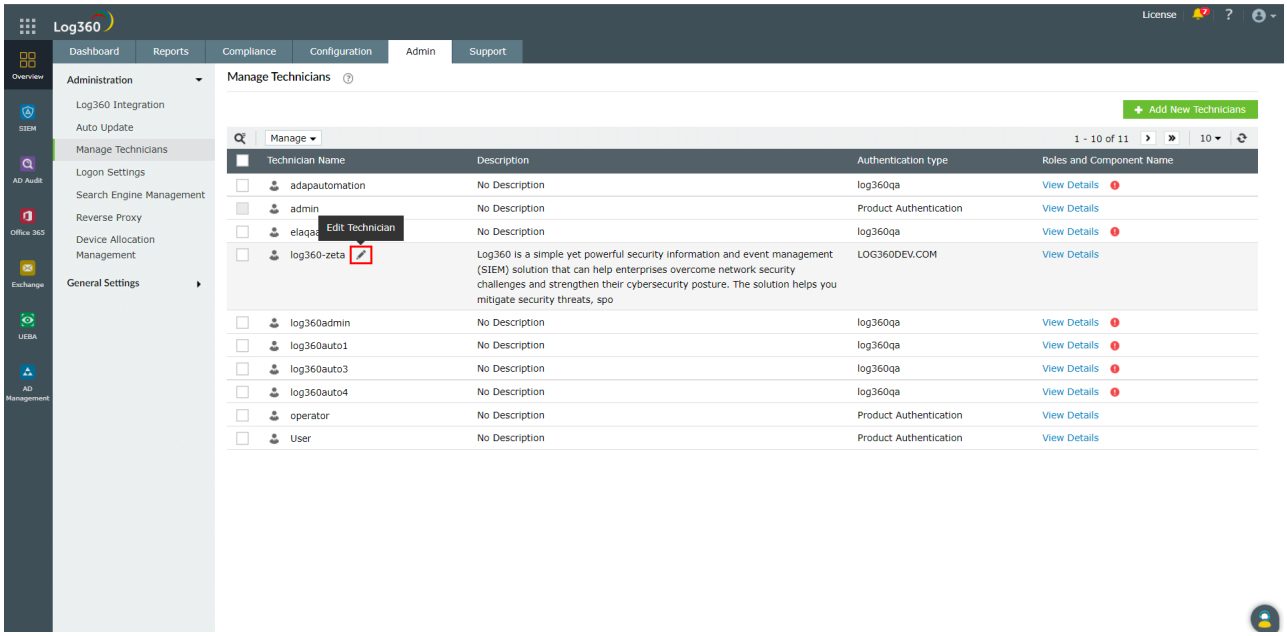
How to modify an existing technician from the centralized dashboard?

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

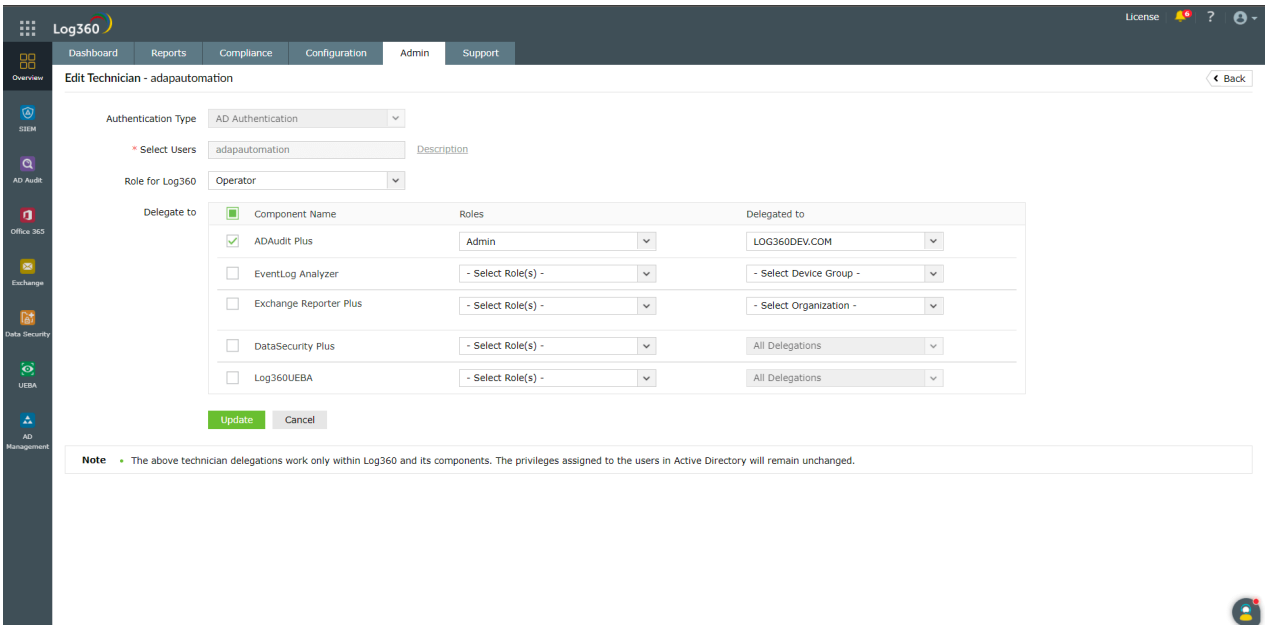
- Under the **Admin** tab, navigate to **Administration** → **Manage Technicians.**



- Click the edit icon 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.



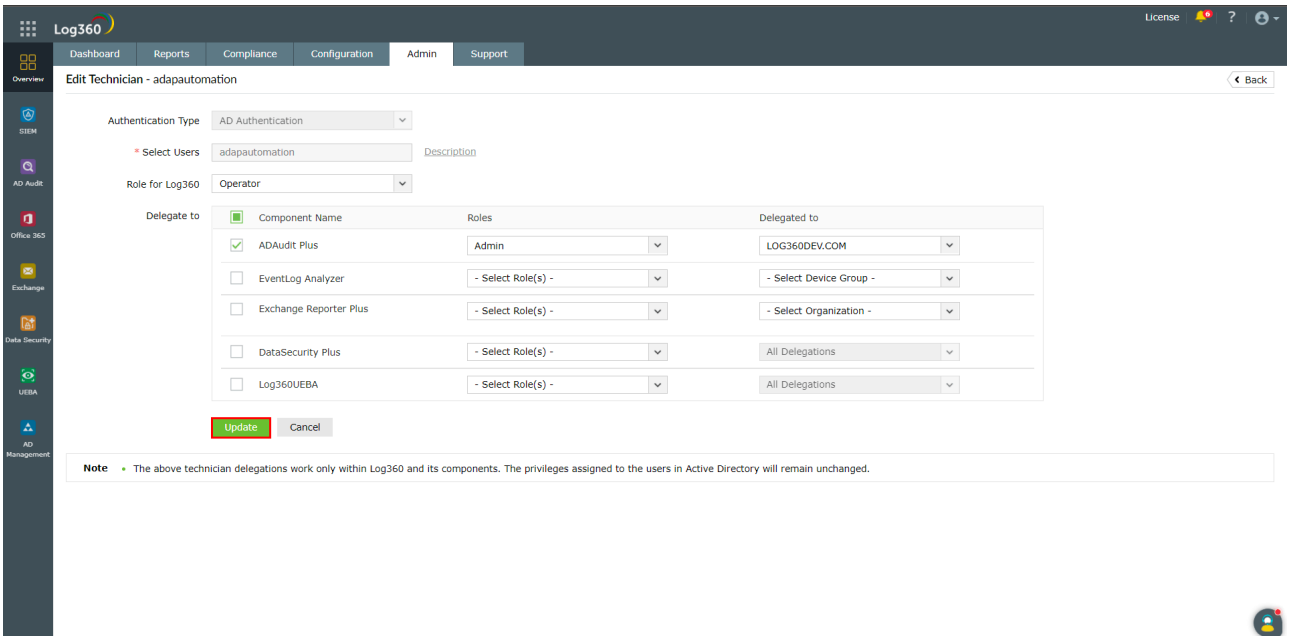
- Edit the information in the various fields as required.



- 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.

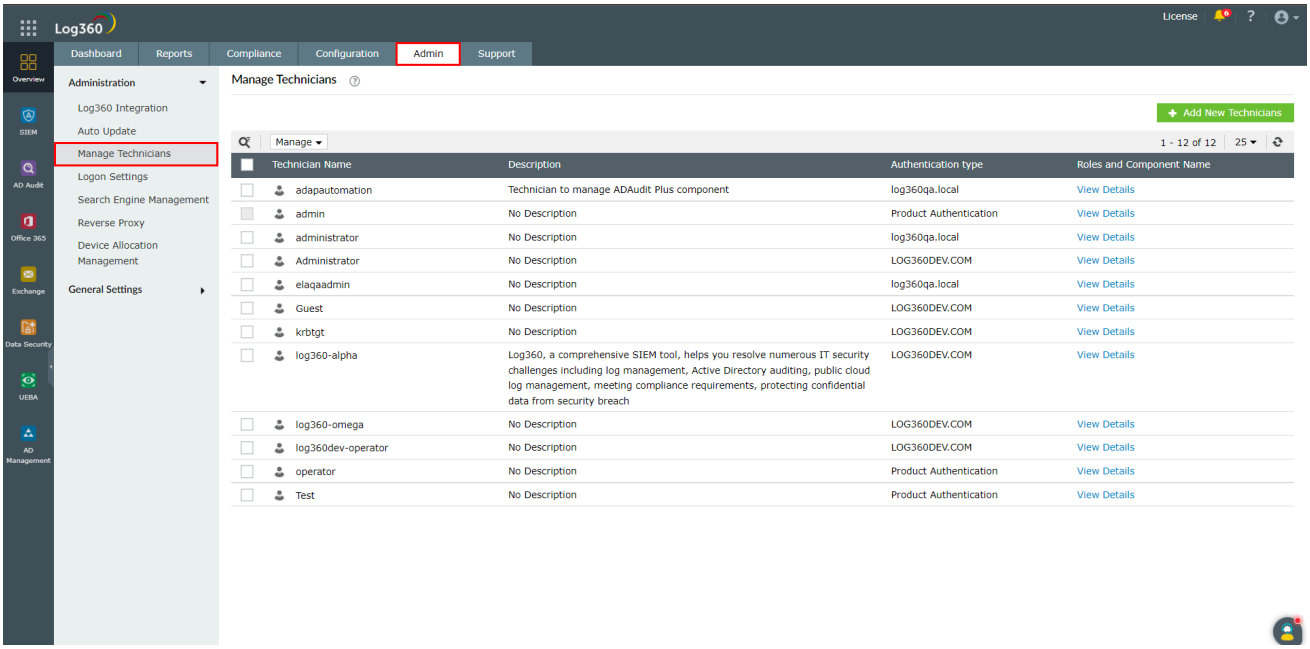
- To modify the roles and delegations associated with the technician, choose the required role and delegation from the drop-down for the respective component under the **Delegate to** section.
- Click on the **Update** button to save the changes.



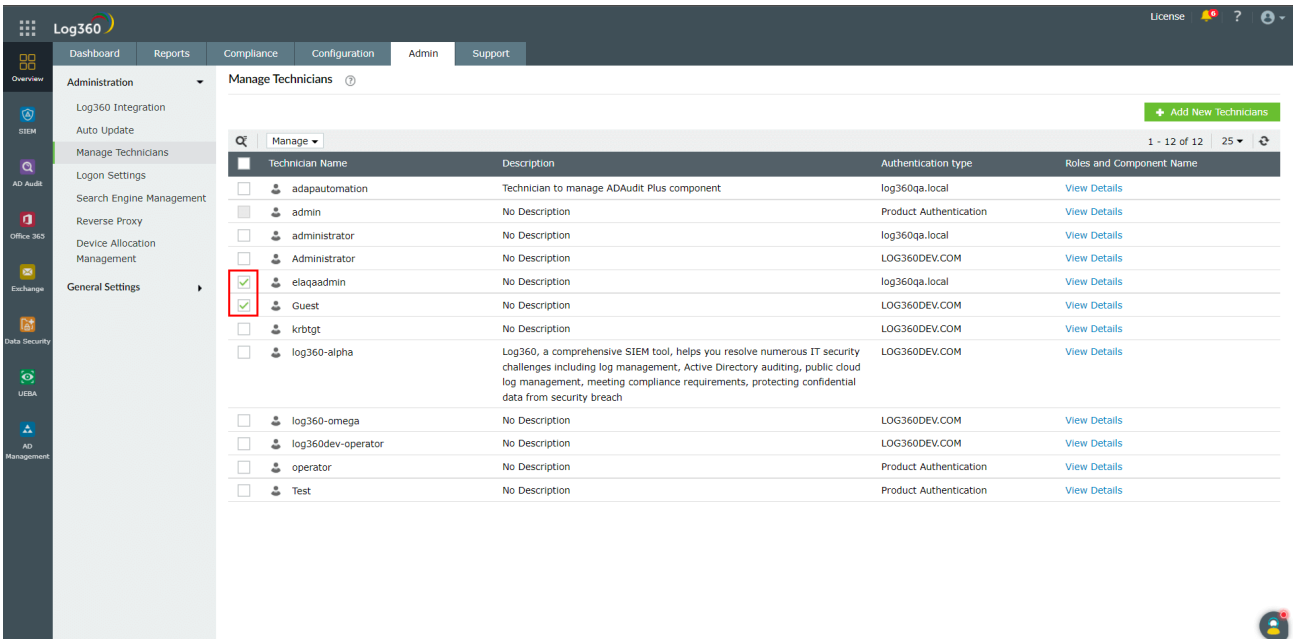
How to delete an existing technician from the centralized dashboard?

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

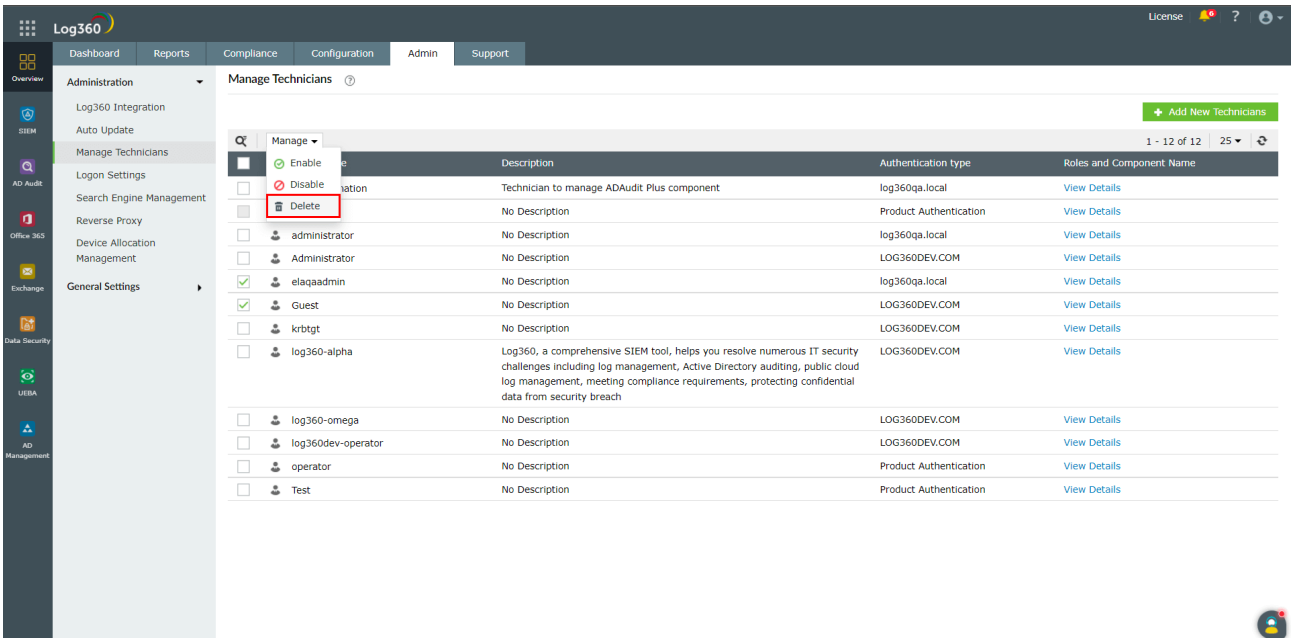
- Under the **Admin** tab, navigate to **Administration** → **Manage Technicians.**



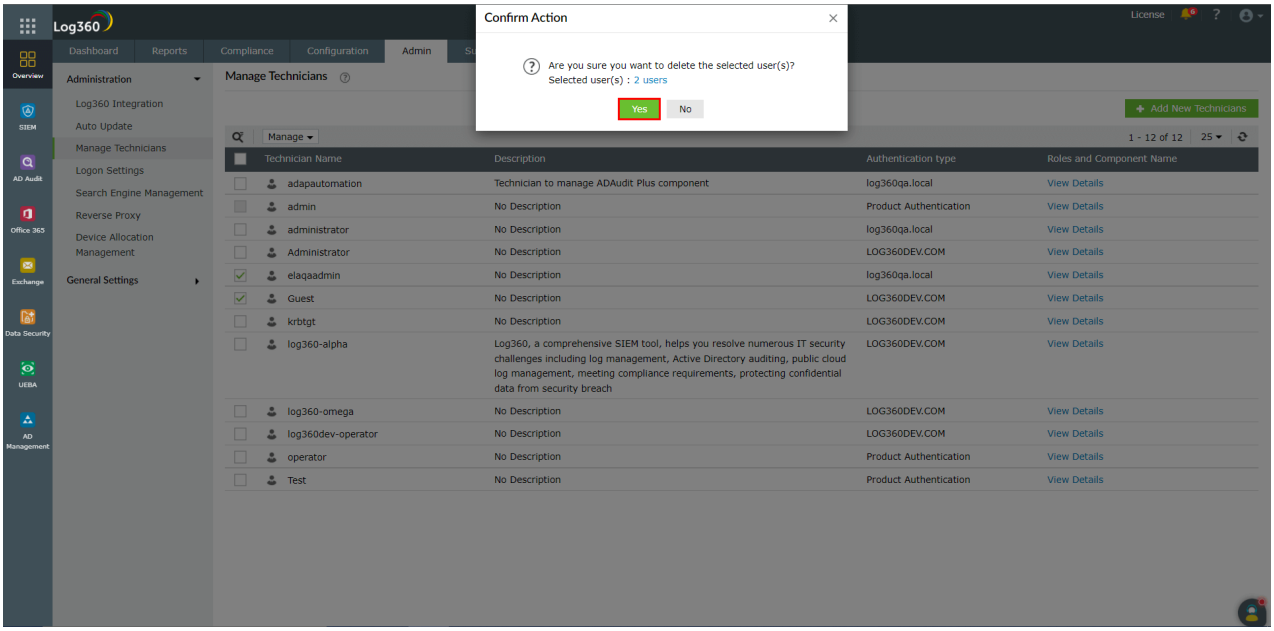
- Choose the technicians to be deleted by ticking the checkbox corresponding to the technician's name.



- 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.

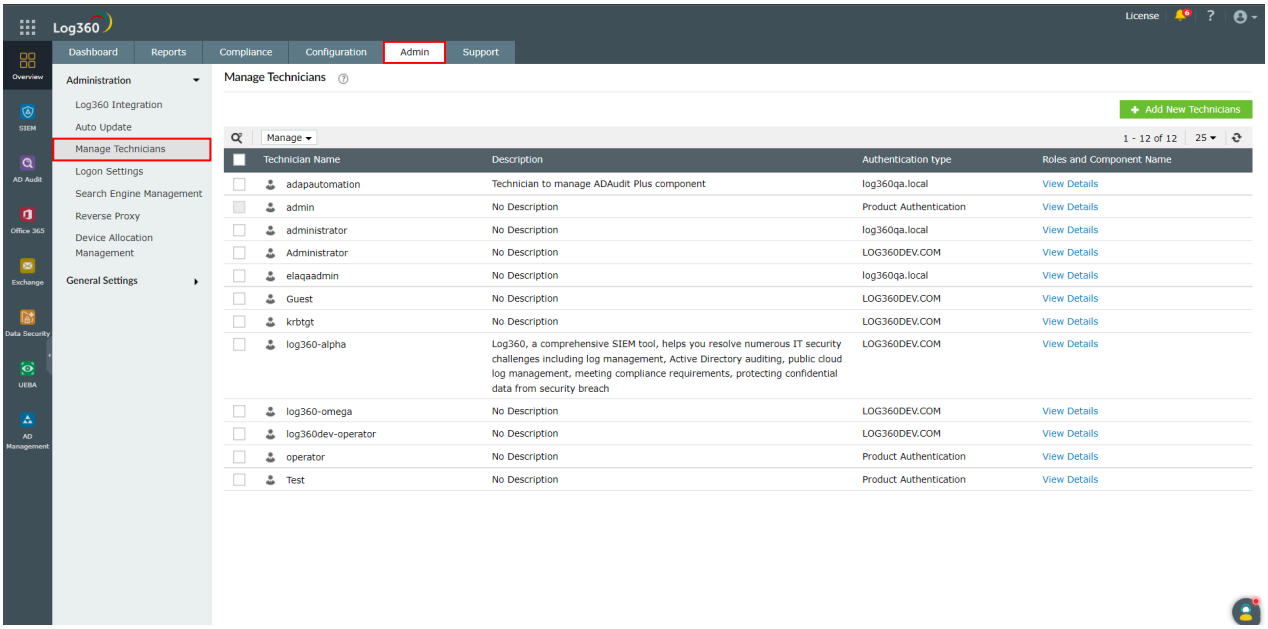


- The technician is now deleted.

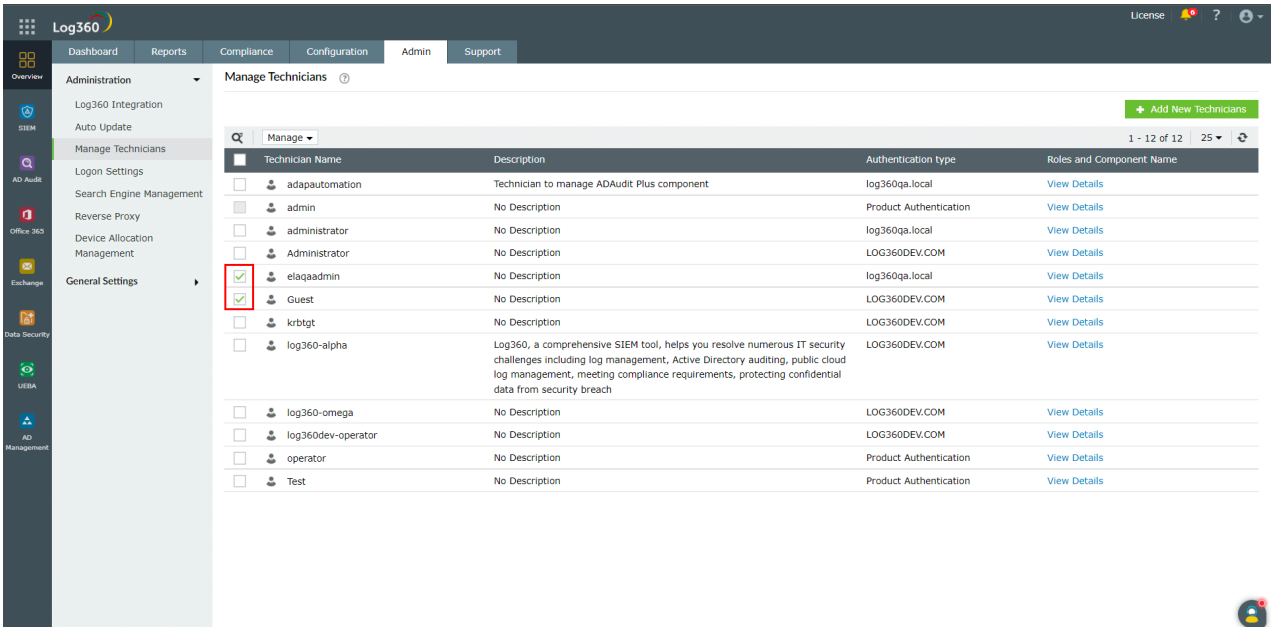
How to enable or disable an existing technician?

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

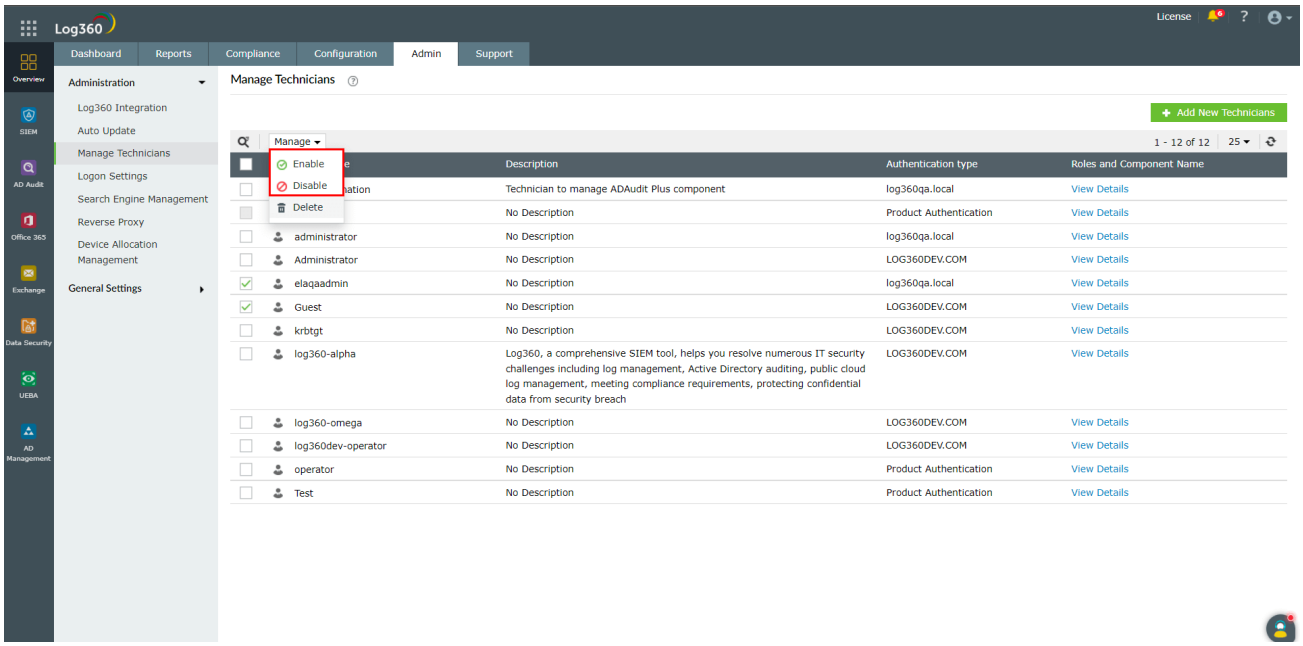
- Under the **Admin** tab, navigate to **Administration** → **Manage Technicians.**



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



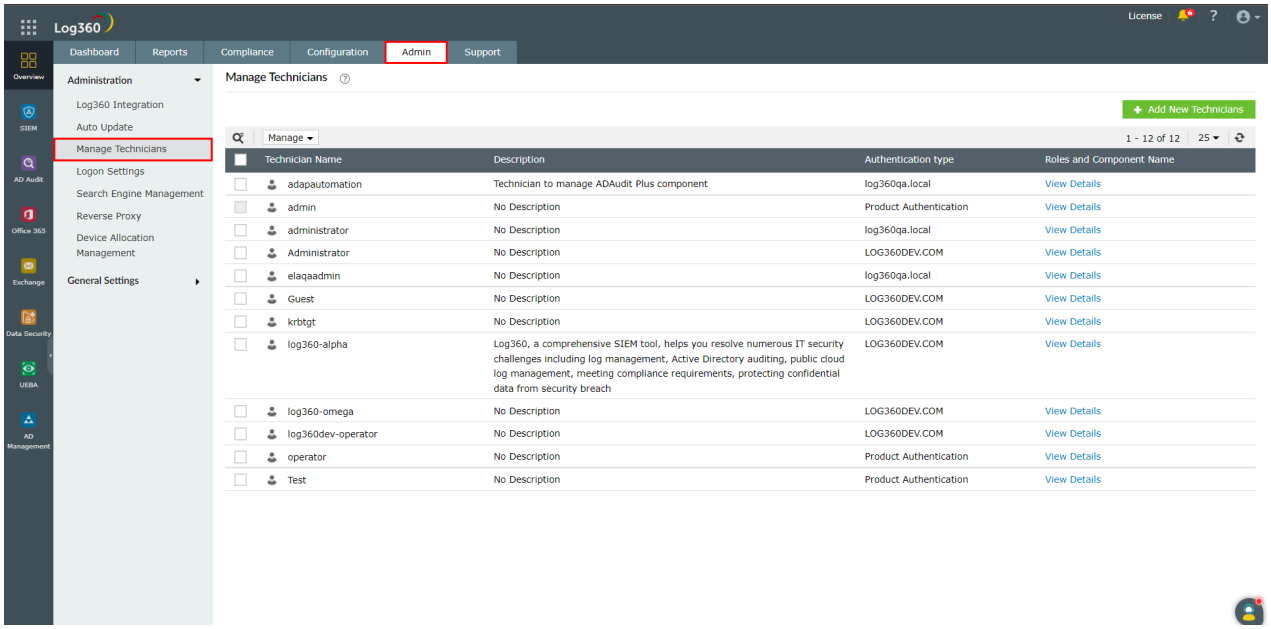
- Click on the **Manage** button above the table and select **Enable** or **Disable** from the drop-down menu.



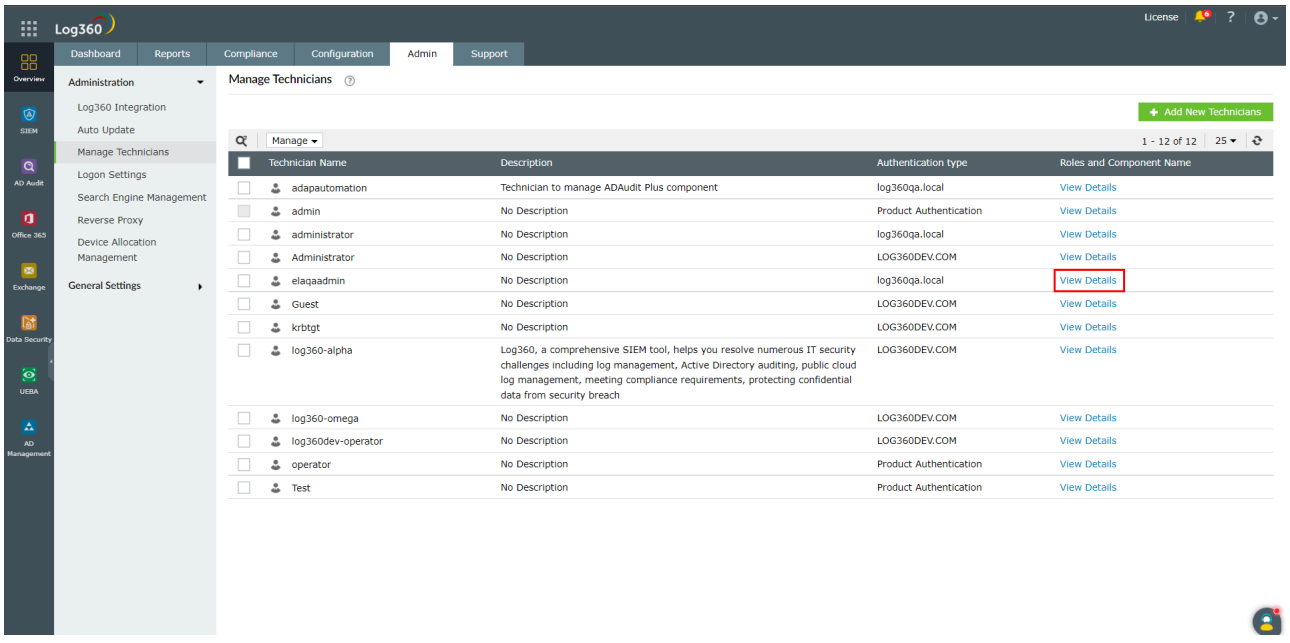
- The technician is now enabled/disabled.

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

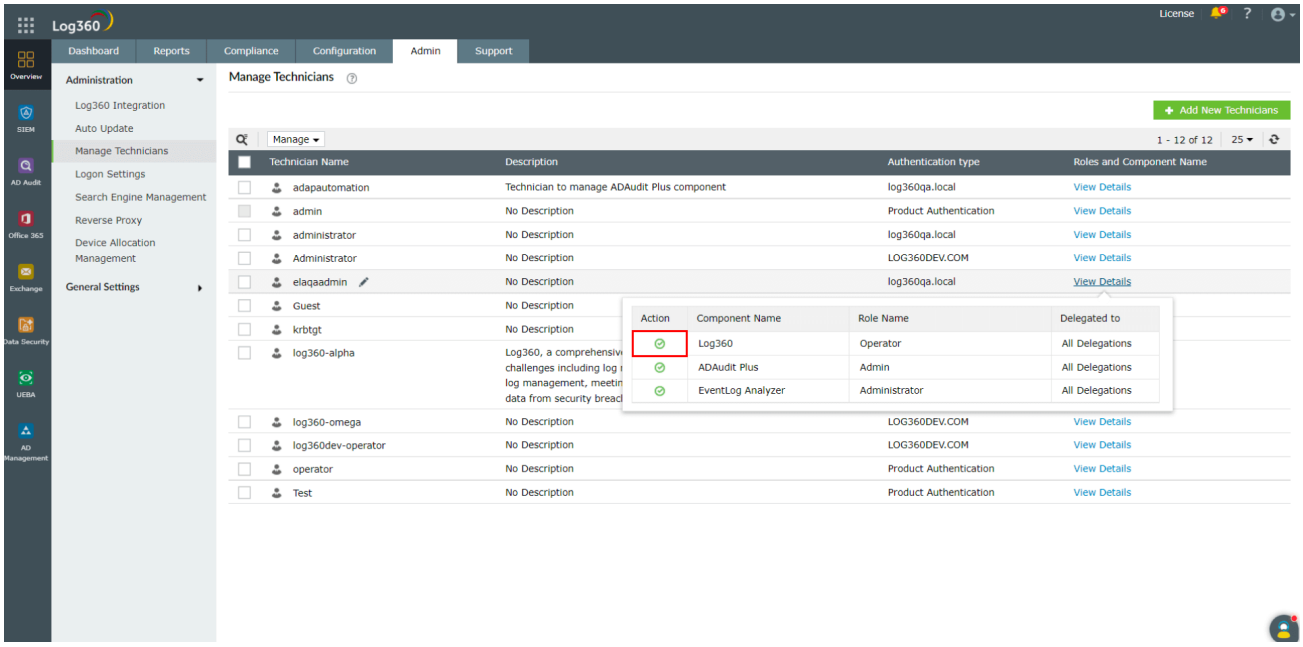
- Under the **Admin** tab, navigate to **Administration** → **Manage Technicians.**



- 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)

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.

3. Why are Active Directory Manager Plus (ADMP), M365 Manager Plus (M365) and Exchange Reporter Plus (ERP) not supported?

In order to use ADMP, M365 and ERP, you need to have the full versions of the products. You can upgrade to the full version here:

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

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.

Troubleshooting

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

Solution:

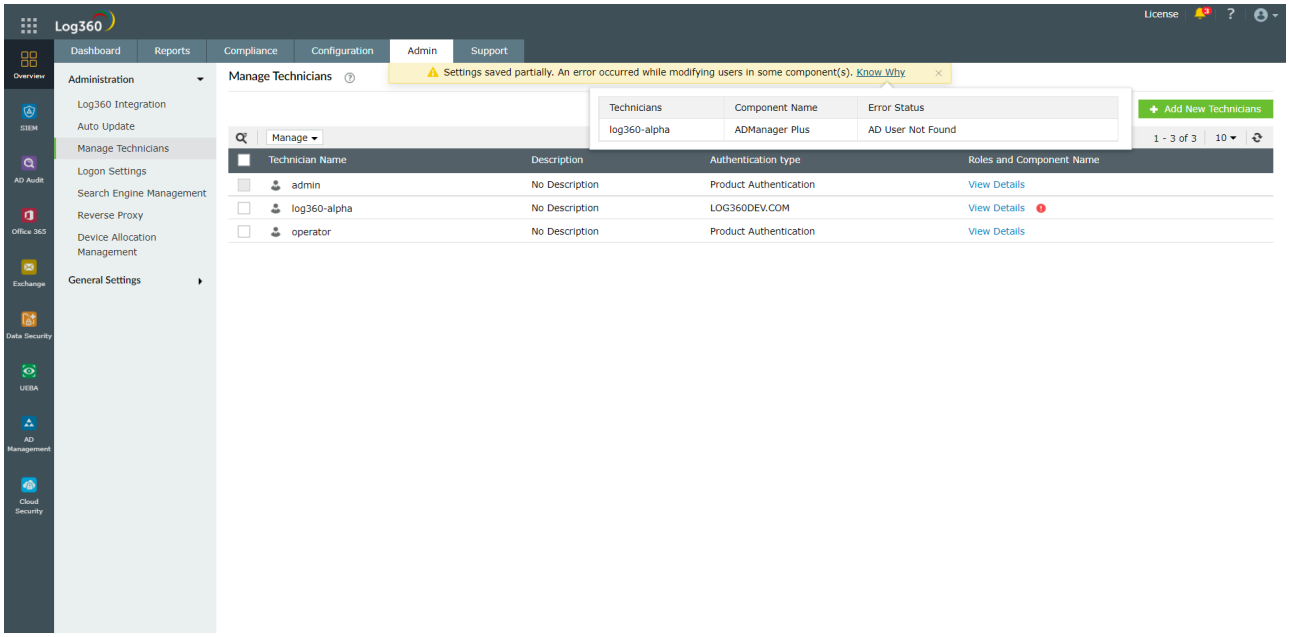
- Under the **Admin** tab, navigate to **Administration → Log360 Integrations.**
- Update the integration settings for the required component.

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

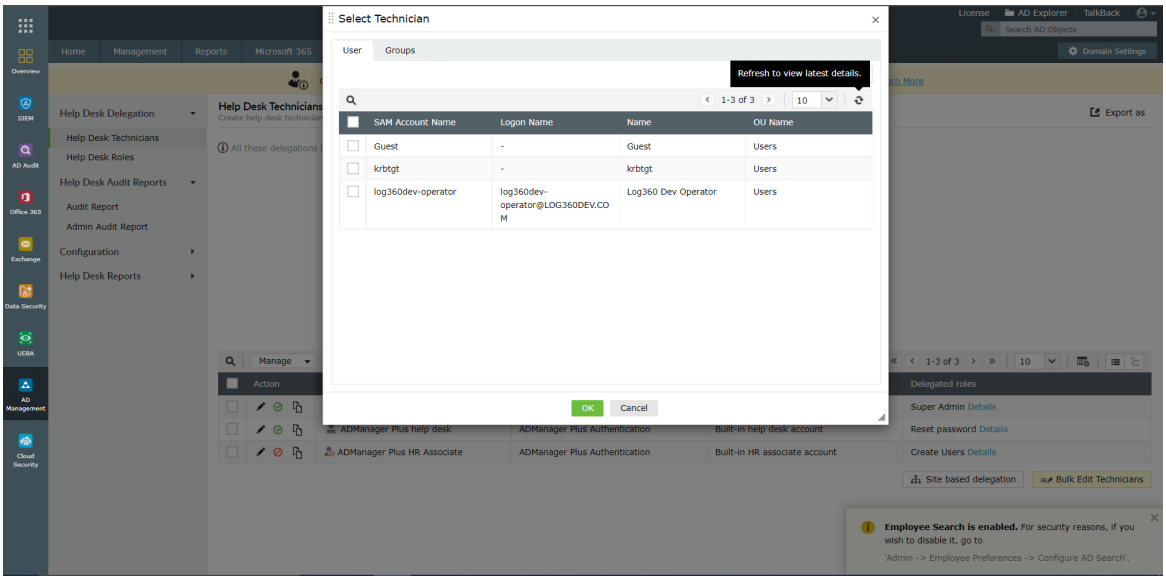
Solution:

- 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'

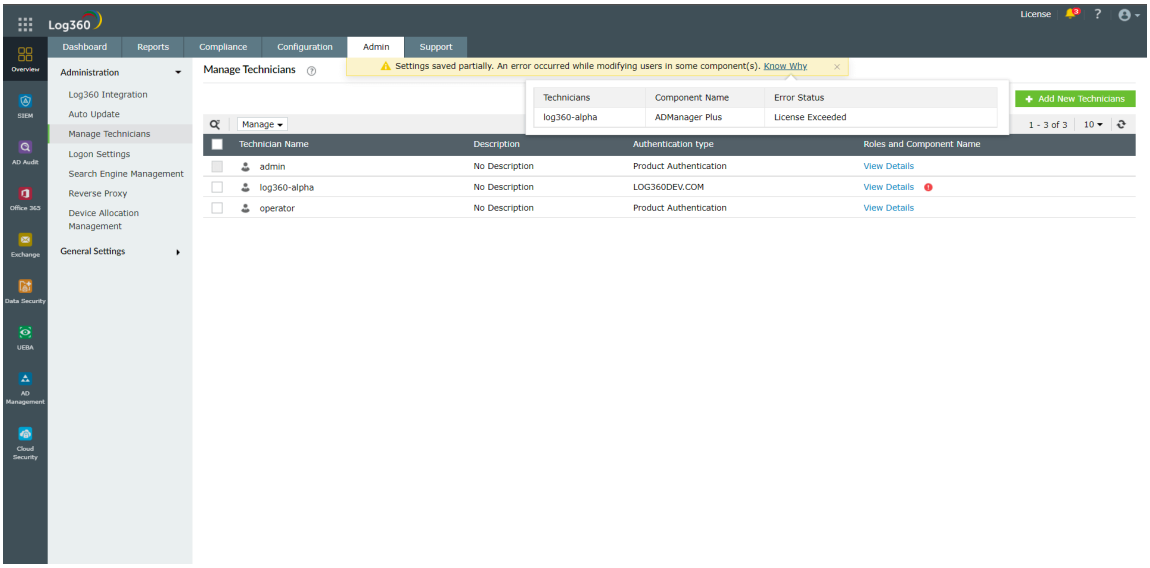


Solution:



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

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



Solution:

- Upgrade your license to add more technicians

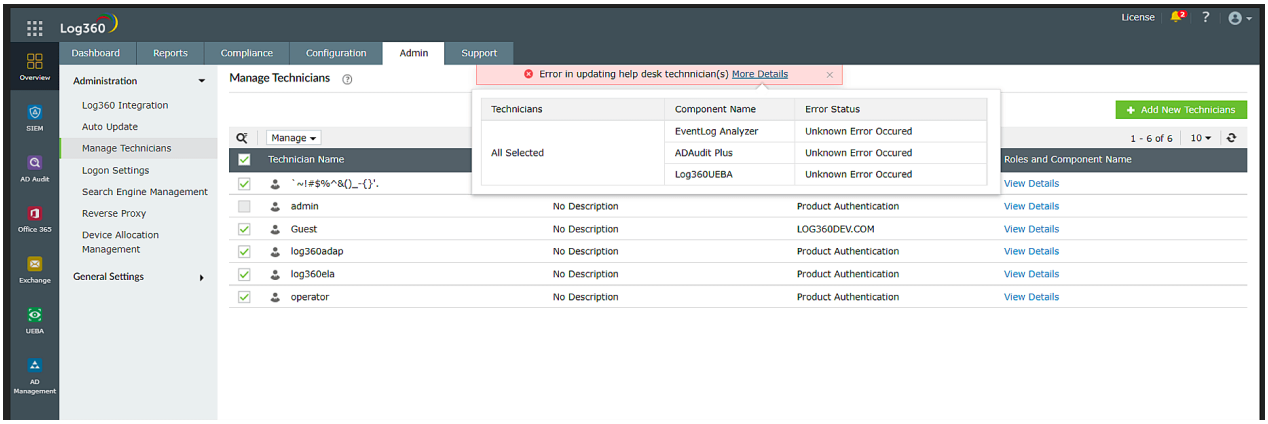
  You can upgrade your license here:
- M365 Manager Plus
- Active Directory Manager Plus
- Exchange Reporter Plus

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

Solution:

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

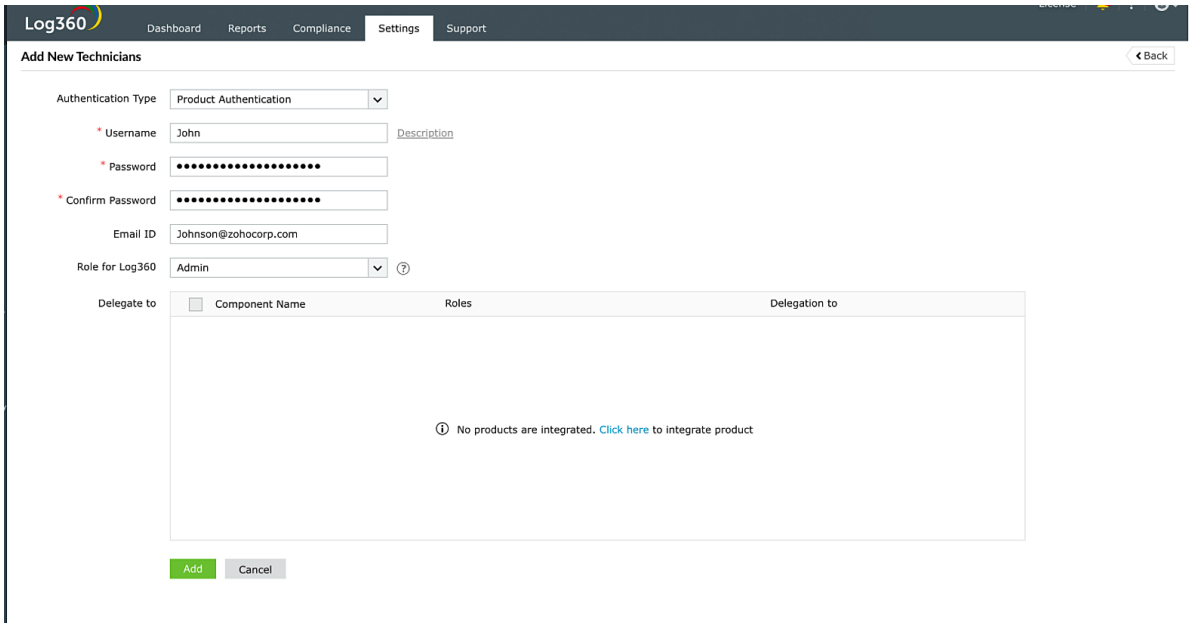
6. Error status returns 'Unknown Error Occurred'



Solution:

- Contact Log360 support in case this error occurs.

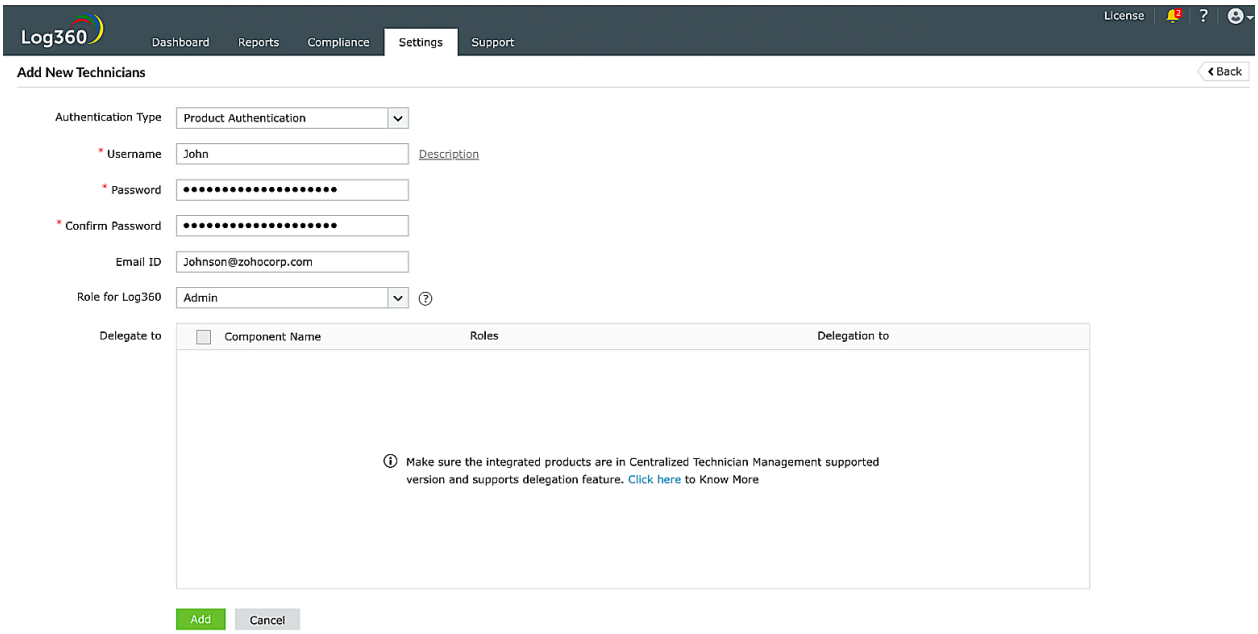
7. Error returns 'No products are integrated'.



Solution:

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

8. Error returns 'No products are supported'.



Solution:

- Check if the integrated product is in its latest/supported version.
- Next, check if the integrated product belongs to the following build numbers.
  - EventLog Analyzer - 12214
  - Log360 UEBA - 4033
  - ADAudit Plus - 7009
  - M365 Manager Plus - 4502
  - DataSecurity Plus - 6061
  - Exchange Reporter Plus - 5615
  - Cloud Security Plus - 4130

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.

- **Actions on nodes**
- **Prerequisites**
- **Setting up Elasticsearch**
- **Configuring Elasticsearch in Log360**

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 elasticsarch service by opening the **taskmanager>services.**
- Move the certificates to **<INSTALLAITON DIR>\ES\config\certificate**
- 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.

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.

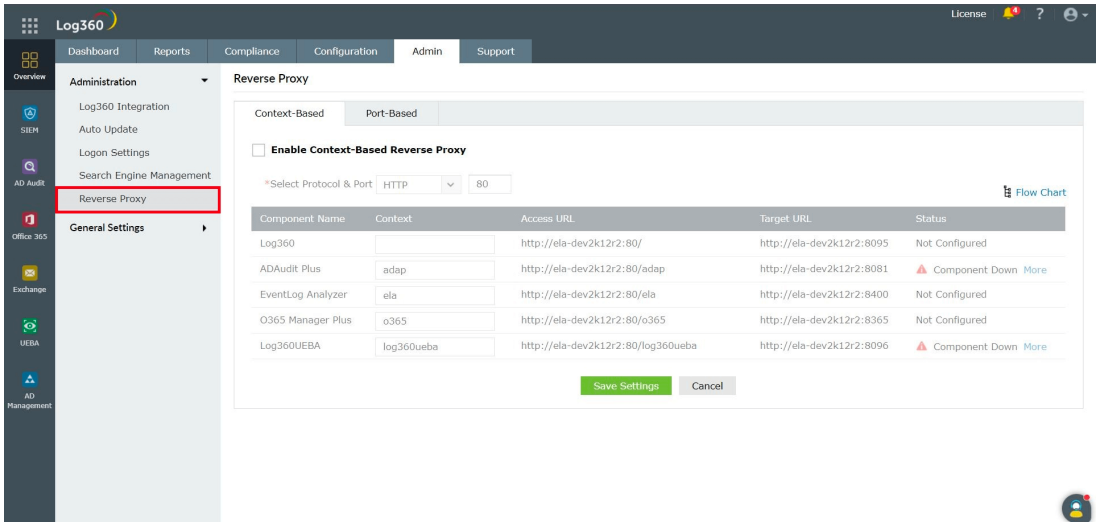
If you want to enable the port-based reverse proxy, you need to choose a unique port number and protocol, for Log360 and its components' servers. In this case, a unique port number for the servers is mandatory whereas specifying a unique protocol is optional. The hostname remains the same for all the 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

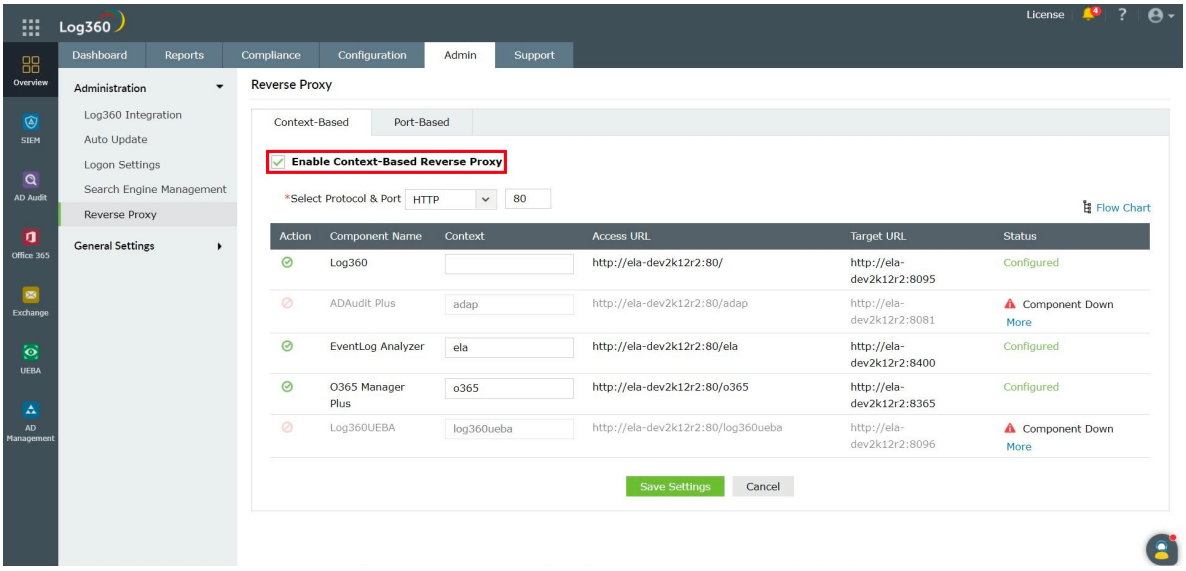
To enable context-based reverse proxy, please follow the steps given below.

- 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.

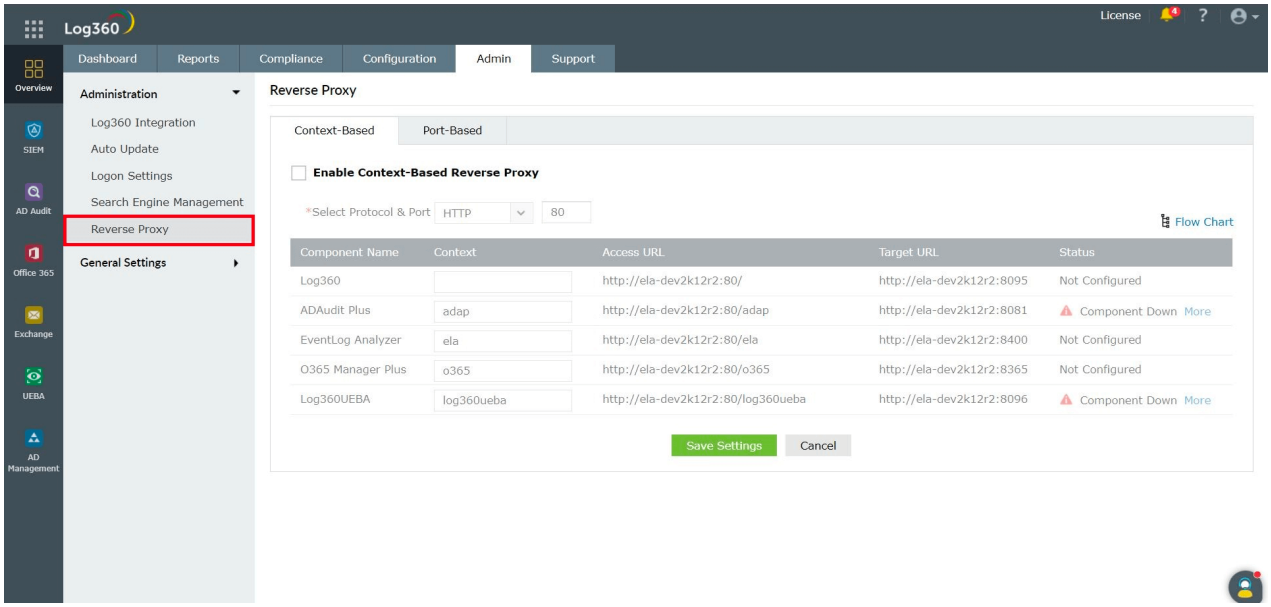
- Under the **Context-Based** tab, **Enable Context-Based Reverse Proxy** by ticking the check box.



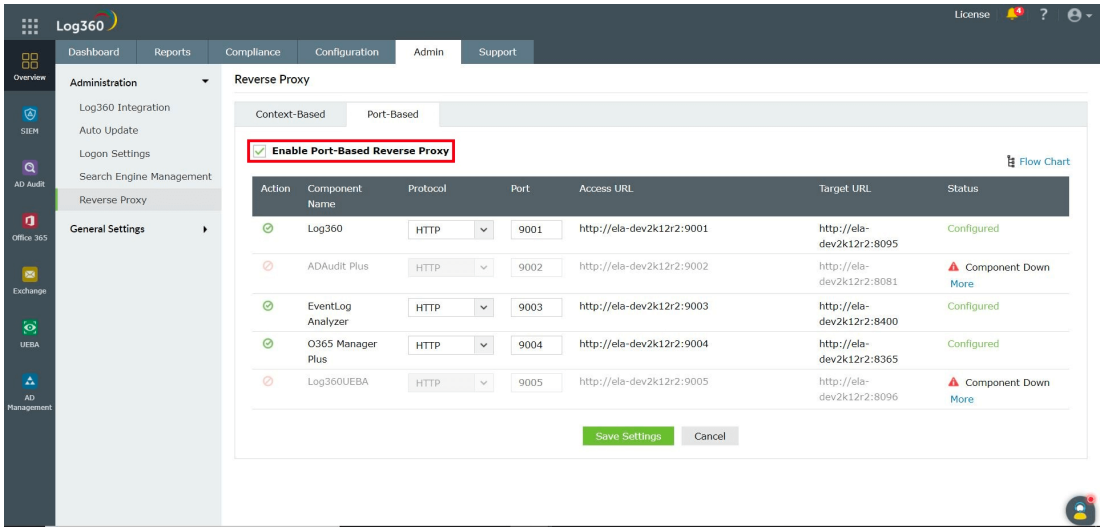
- In the **Protocol & Port** fields, select the required protocol and port number. Make sure the port number is not used by other applications.
- Now, for Log360 and each of the integrated components, enter a context path under the **Context** column. The context path must be unique to each component.
- 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.