ManageEngine
ADAudit Plus

EMC Isilon
Auditing Guide

www.adauditplus.com

Table of contents

Overview of EMC Isilon auditing

Isilon is a network-attached storage platform from Dell EMC, running the proprietary OneFS operating system. ADAudit Plus can track file accesses and modifications made in Dell EMC Isilon storage in real time, and detect anomalous activity using its user behavior analytics (UBA) engine.

Benefits of auditing EMC Isilon storage using ADAudit Plus

ManageEngine ADAudit Plus offers several advantages over native tools when auditing EMC file clusters. It can:

- Track successful and failed file read, write, create, delete, modify, move, rename, and delete events.
- Provide information on who made the change, to which file, when, and from where on a user-friendly interface unlike native tools, which rely on command-line interface.
- List the Access Control List (ACL) values before and after a permission change.
- Maintain a unified audit trail of all file activities across multiple servers.
- Trigger instant alerts when anomalous file activities are detected.
- Deliver detailed, out-of-the-box audit reports for regulatory compliances such as HIPAA, SOX, GDPR, PCI DSS, ISO 27001, FISMA, GLBA, and more.

Supported versions
OneFS OS versions 7.0 and above.

Audited events
ADAudit Plus audits every successful and failed attempt to perform these file activities:

- Create
- Read
- Modify
- Write
- Delete
- Change file permissions (with information on the permission settings before and after the change)

This guide provides steps on configuring real-time change auditing for your EMC Isilon cluster using ADAudit Plus.

Privileges required for effective EMC Isilon auditing

Certain minimum privileges are required to ensure the effective functioning of ADAudit Plus while auditing your EMC Isilon nodes. Create a dedicated ADAudit Plus Isilon user account and provide it with the below privileges.

1. For discovering zones:

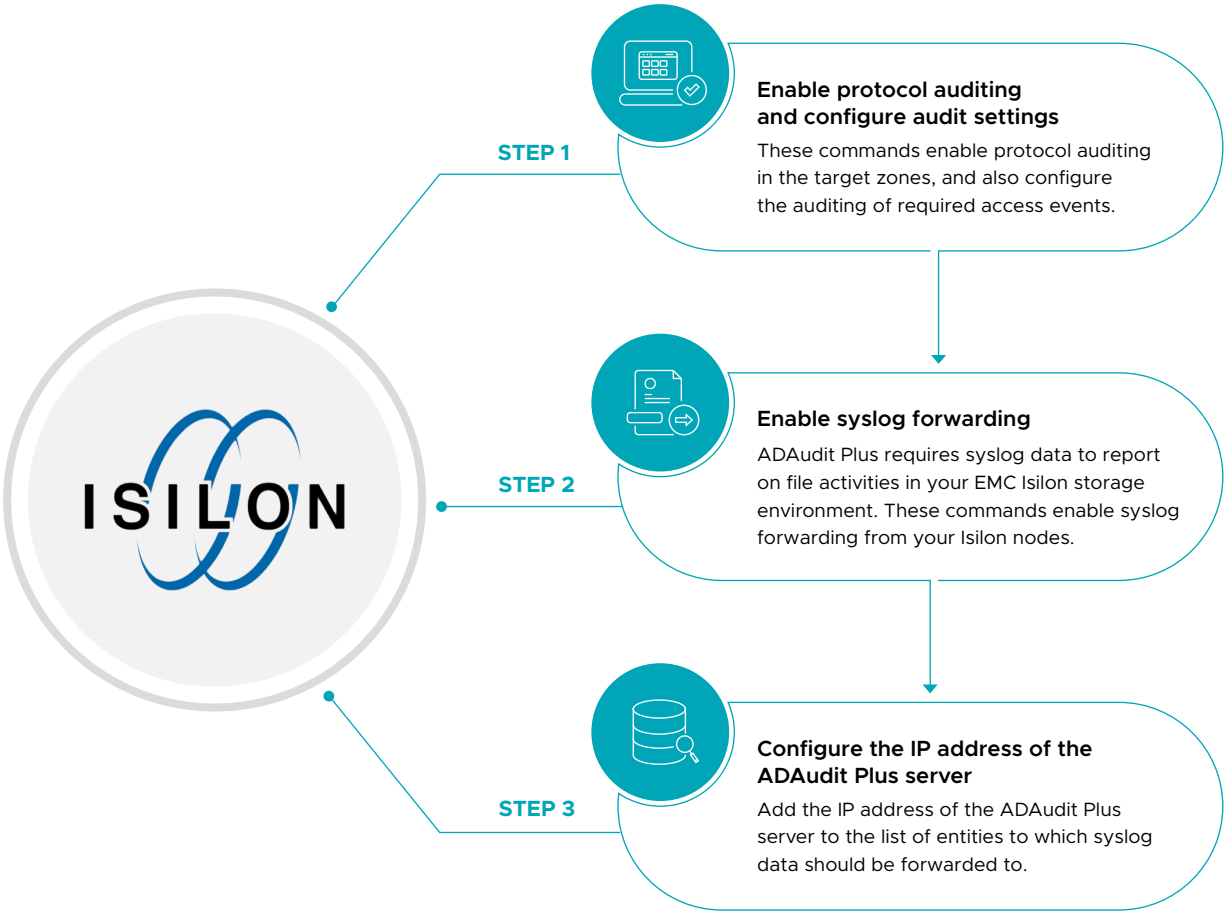
- Provide these privileges with read-only access:
  - ID: ISI_PRIV_LOGIN_SSH
  - ID: ISI_PRIV_AUTH
  - ID: ISI_PRIV_NETWORK
- Ensure that Smart Connect Zone (SC Zone) is configured for all the zones to be audited.
  The domain must be the **Authentication Provider (lsa-activedirectory-provider)** for the zone.
- Verify that the cluster name or cluster DNS name is mapped to the node's IP address.
- Secure Shell (SSH) must be enabled on port 22 on the Isilon cluster to be audited.

2. For discovering shares in a zone:

The user configured under domain settings for the authentication provider must have Read permission to the shares.

Configuring EMC Isilon auditing

This section outlines the steps to configure audit settings in EMC Isilon nodes, and to forward event data to ADAudit Plus. The commands to configure the required settings vary based on the OneFS version, but they all involve three steps:



Follow the steps listed under your OneFS version to configure EMC Isilon auditing.

For OneFS Version 7.x:

1. Execute these commands to enable protocol auditing and configure audit settings:
   - isi audit settings modify --protocol-auditing-enabled yes --audited-zones <zone_names>
   - isi zone zones modify <zone_name> --audit-success create,delete,read,rename,set_security,write
   - isi zone zones modify <zone_name> --audit-failure create,delete,read,rename,set_security,write
   - isi zone zones modify <zone_name> --syslog-audit-events create,delete,read,rename,set _security,write

2. To enable syslog forwarding, execute this command:
   - isi zone zones modify <zone_name> --syslog-forwarding-enabled=yes

3. To configure the IP address of the ADAudit Plus server, follow these steps:
   - Connect to any one of your Isilon nodes using an SSH client.
   - Open the **syslog.conf** file, which can be found at the **/etc/mcp/templates** directory.
   - Locate the **!audit_protocol** line and add the below entry, providing the correct value in place of hostname or IP address:

     . @<hostname/IP Address of the ADAuditPlus server>
   - Save the **syslog.conf** file.

For OneFS Versions 8.0 and 8.1:

1. Execute these commands to enable protocol auditing and configure audit settings:
   - isi audit settings global modify --protocol-auditing-enabled yes --audited-zones <zone_names>
   - isi audit settings modify --zone <zone_name> --audit-success create,delete,read,rename, set_security,write
   - isi audit settings modify --zone <zone_name> --audit-failure create,delete,read,rename, set_security,write
   - isi audit settings modify --zone <zone_name> --syslog-audit-events create,delete,read, rename,set_security,write

2. To enable syslog forwarding, execute this command:
   - isi audit settings modify --syslog-forwarding-enabled=yes --zone=<zone_name>

3. To configure the IP address of the ADAudit Plus server, follow these steps:
   - Connect to any one of your Isilon nodes using an SSH client.
   - Open the **syslog.conf** file, which can be found at the **/etc/mcp/templates** directory.
   - Locate the **!audit_protocol** line and add the below entry, providing the correct value in place of hostname or IP address:

     . @<hostname/IP Address of the ADAuditPlus server>
   - Save the **syslog.conf** file.

For OneFS Versions 8.2 to 9.4

1. To enable protocol auditing, configure audit settings, and configure the IP address of the ADAudit Plus server, execute this command:
   - isi audit settings global modify --protocol-auditing-enabled yes --audited-zones <zone_name> --protocol-syslog-servers <IP_of_ADAuditPlus_server>
   - isi audit settings modify --zone <zone_name> --audit-success create,delete,read,renam ,set_security,write

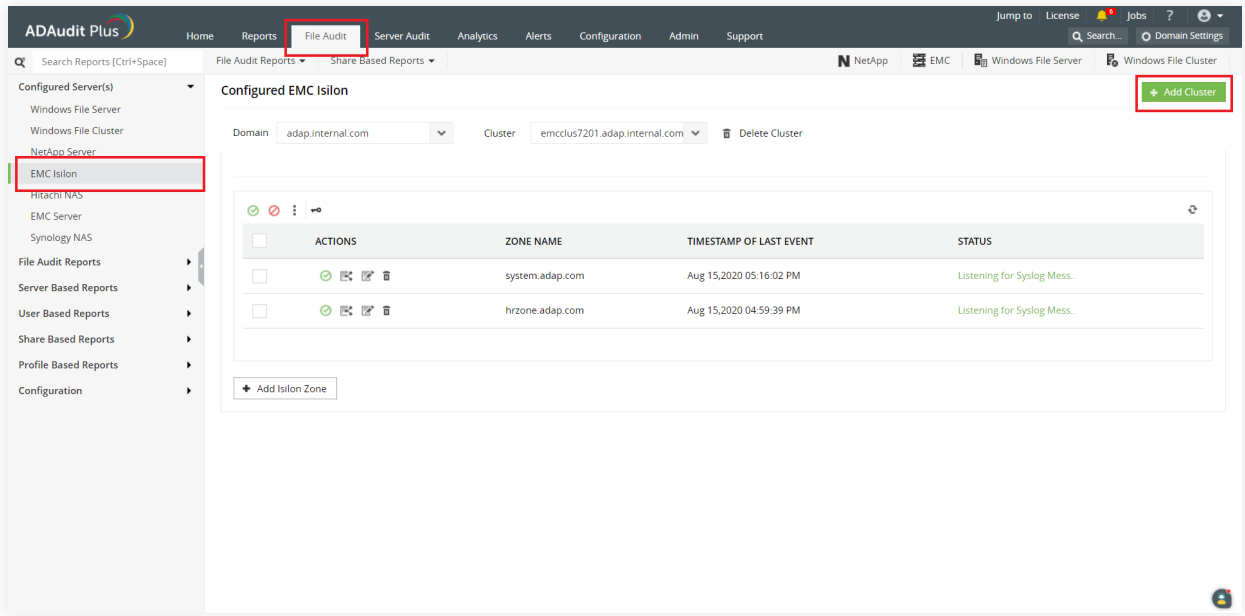
- isi audit settings modify --zone <zone_name> --audit-failure create,delete,read,rename, set_security,write
- isi audit settings modify --zone <zone_name> --syslog-audit-events create,delete,read, rename,set_security,write

2. To enable syslog forwarding, execute this command:
   - isi audit settings modify --syslog-forwarding-enabled yes --zone <zone_name>

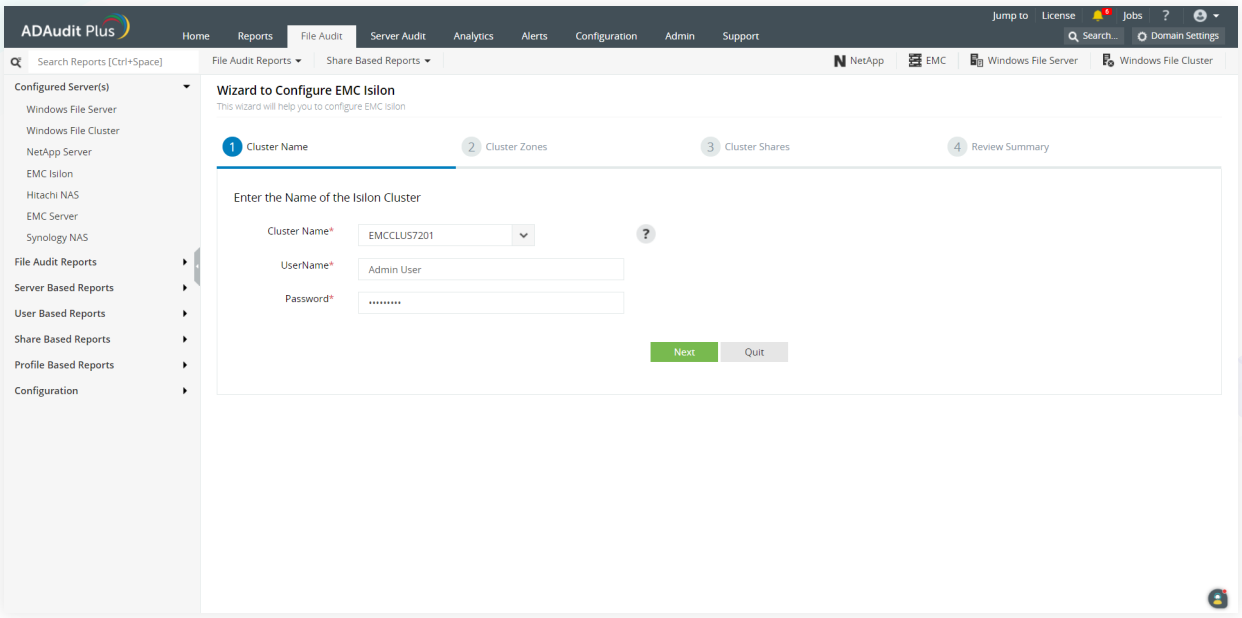
Adding EMC Isilon clusters in ADAudit Plus

To add an EMC Isilon device to the ADAudit Plus console, follow these steps:

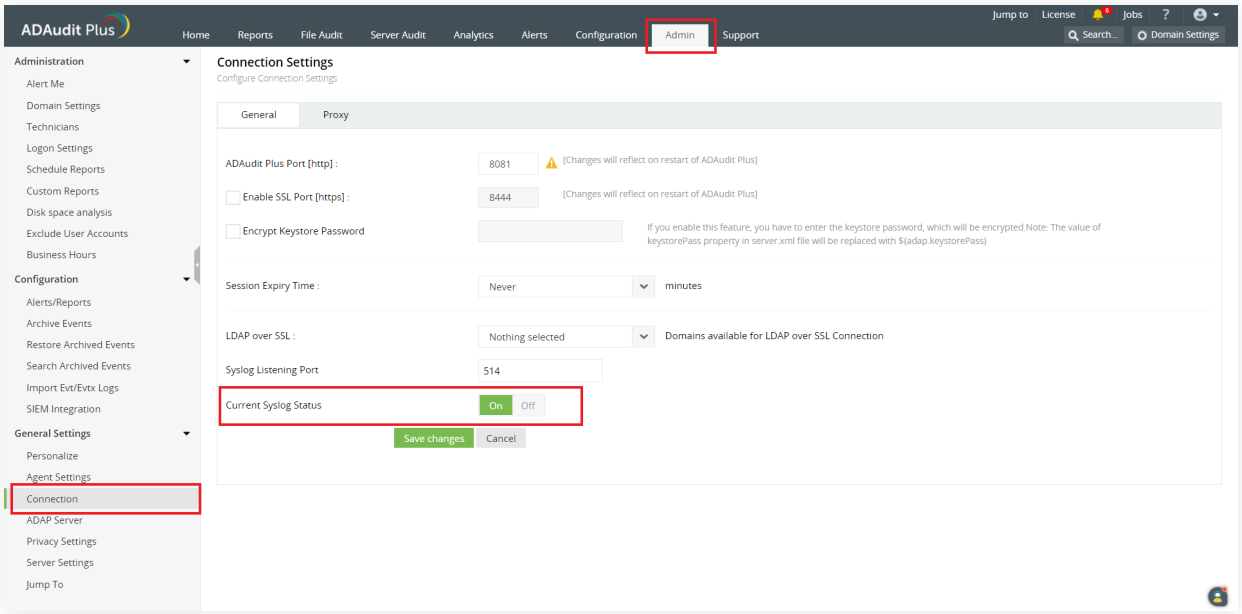
1. Log in to the ADAudit Plus web console. Navigate to the **File Audit** tab > **Configured Server(s)** > **EMC Isilon.** Click **Add Cluster** in the top right corner.



2. Provide the required information in the Wizard to Configure EMC Isilon to add the clusters you wish to audit, and click **Save.**



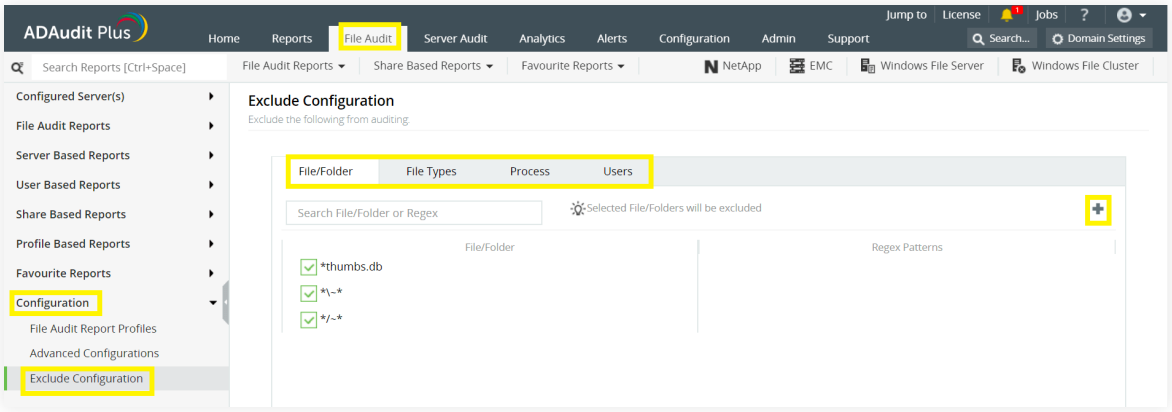
3. Then, navigate to **Admin** > **General Settings** > **Connection.**
4. Verify that **Current Syslog Status** is set to **On.** If it is set to Off, turn on Syslog Listening Status and click **Save Changes.**



Exclude configuration

Files/folders can be excluded based on File/folder local path, file type, process name, and user name by using the **Exclude Configuration** setting.

Log in to ADAudit Plus' web console ⟶ Go to the **File Audit** tab, navigate to the left pane, click on **Configuration** and then on **Exclude Configuration** ⟶ Choose to exclude by **File/Folder** local path, **File Type, Process Name,** or Users ⟶ Click on '+', and configure the necessary settings.



Example scenarios, to exclude by File/Folder local path:

Objective	To exclude a folder and all of its subfolders and files	
Share configured	**Share path**	**Local path**
	\\SERVER_NAME\share_name	C:\sharefolder
Path of folder that is to be excluded	C:\sharefolder\excludefolder	
File/Folder or Regex Patterns	File/Folder Patterns	
Syntax	• C:\sharefolder\excludefolder • C:\sharefolder\excludefolder*	
What will get excluded	• C:\sharefolder\excludefolder • C:\sharefolder\excludefolder\folder • C:\sharefolder\excludefolder\files.txt • C:\sharefolder\excludefolder\folder\files.txt	
What won't get excluded		

Objective	To exclude "AppData" folder for every user profile
Share and folder path	\\SERVER_NAME\Users C:\Users
Path of folder that is to be excluded	C:\Users\user1\AppData
File/Folder or Regex Patterns	Regex Patterns
Syntax	C:\\Users\\[^\\]*\\AppData
What will get excluded	• C:\Users\user1\AppData • C:\Users\user2\AppData • C:\Users\user1\AppData\subfolder • C:\Users\user2\AppData\subfolder
What won't get excluded	• C:\Users\user1\subfolder\AppData • C:\Users\user2\subfolder\AppData

Objective	**To exclude files from a specific folder but audit all subfolders and its contents**
Share and folder path	\\SERVER_NAME\share_name C:\sharefolder
Path of folder that is to be excluded	C:\sharefolder\excludefolder
File/Folder or Regex Patterns	Regex Patterns
Syntax	^C:\\sharefolder\\excludefolder\\[^\\]*\.[^\\]*$
What will get excluded	• C:\sharefolder\excludefolder\file.txt • C:\sharefolder\excludefolder\folder.withDot
What won't get excluded	• C:\sharefolder\excludefolder • C:\sharefolder\excludefolder\folderWithoutDot • C:\sharefolder\excludefolder\folderWithoutDot\subfolder • C:\sharefolder\excludefolder\folderWithoutDot\testfile.txt • C:\sharefolder\excludefolder\folder.withDot\subfolder • C:\sharefolder\excludefolder\folder.withDot\testfile.txt

Troubleshooting

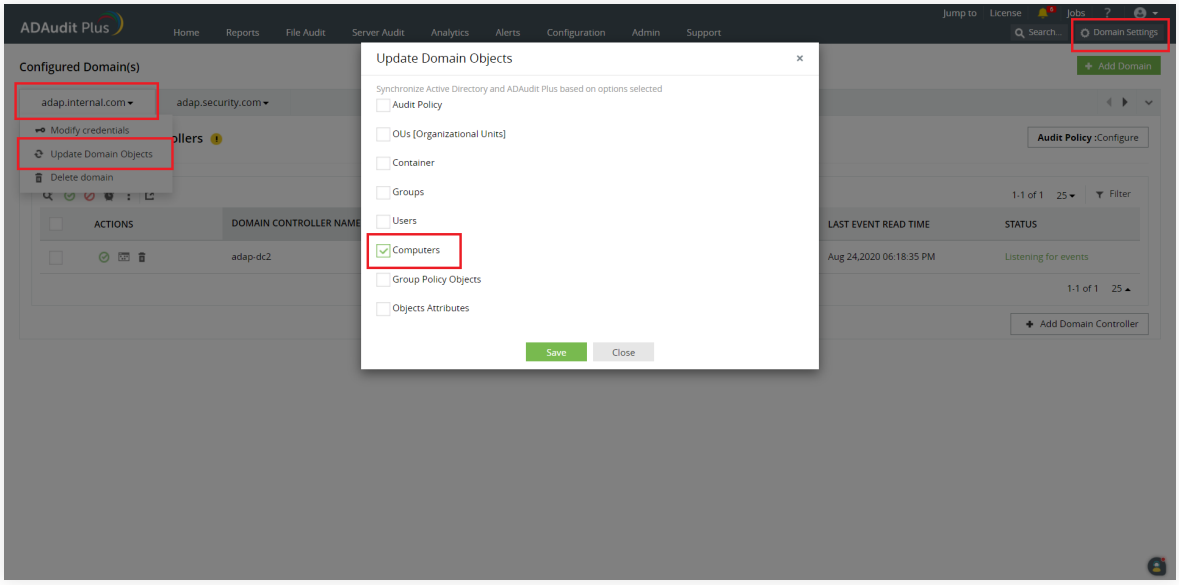
To learn about the common issues faced in EMC Isilon auditing using ADAudit Plus, review these steps.

1. Error messages and solutions:

i. **The selected Domain must be an Authentication Provider for the Cluster.**

Verify that the cluster is a part of the selected domain, and try adding the cluster again. If the issue persists, update the computer objects by following the steps below:

- On the ADAudit Plus console, go to **Domain Settings** at the top right corner.
- From the domain drop-down menu, select **Update Domain Objects** to open the corresponding pop-up screen.
- Choose **Computers** on the list and click **Save.**



ii. **Isilon Zone(s) not found.**

Ensure that the ADAudit Plus Isilon user has permission to read the Isilon configuration.

Verify that the minimum required permissions are provided to the user.

iii. **Error in getting shares/Access is denied.**

- Ensure that the user configured under Domain Settings has permission to read the shares in the configured zone.
- Add the Domain Settings user to the LOCAL: System provider's Administrators group to provide read access to files.

iv. **The Timestamp is not updated/No data is received.**

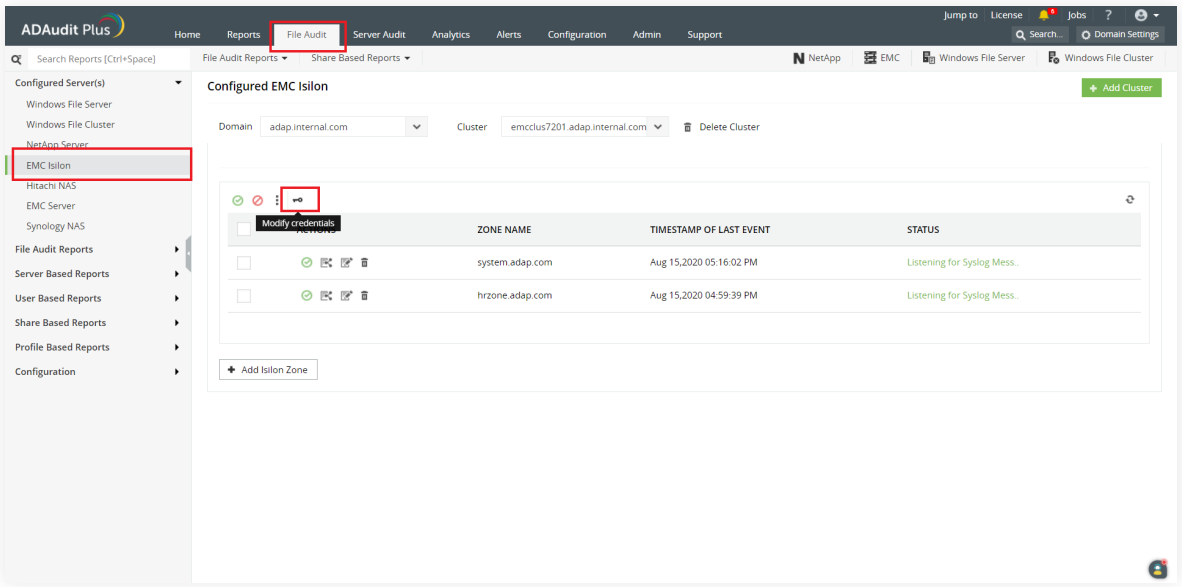
Verify that the cluster is a part of the selected domain, and try adding the cluster again. If the issue persists, update the computer objects by following the steps below:

- Check if the forwarded syslog data is received by the ADAudit Plus server by installing ManageEngine Free Syslog Forwarder.
- Navigate to **Admin** > **General Settings** > **Connection**, and set **Current Syslog Status** to **Off**. Alternatively, you can stop the ADAudit Plus Service.
- In the free syslog forwarder tool, click **Start** to receive syslog data.
- If no data is shown, check the syslog configuration once again. If the issue persists, contact the support team at support@adauditplus.com.

v. **Configured credentials are expired. Click on the key icon to update.**

This error occurs when the user account provided during cluster configuration has been updated or deleted. To resolve this,

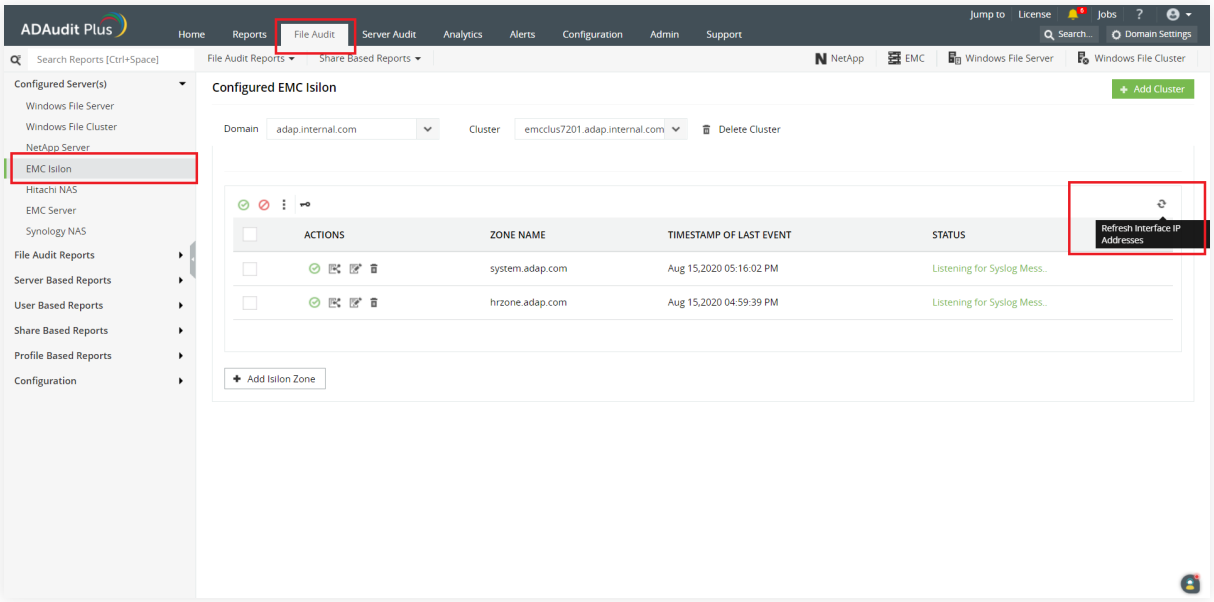
- On the ADAudit Plus web console, navigate to **File Audit** > **Configured Servers** > **EMC Isilon.**
- Click the key icon to provide fresh credentials for the Isilon user.
- Click **OK** to save the changes.



vi. Refresh Interface IP Address

This message is shown when there are no configured IP addresses to receive data from.

- On the ADAudit Plus web console, navigate to **File Audit > Configured Servers > EMC Isilon.**
- Click the **Refresh icon** at the top right corner of the table listing the configured zones.
- If the issue persists, contact the support team at support@adauditplus.com.



vii. Syslog Listening Stopped

Ensure that the port configured under the **Syslog Listening Port (Admin > General Settings > Connection)** is free to use.

2. If the target cluster is not listed in the Cluster Name drop down during configuration:

- Ensure that the correct domain is selected.
- Check if the cluster's domain is the authentication provider.
- Update the computer objects for the domain **(Domain Settings** > select **Update Domain Objects** from the domain drop down > choose **Computers** on the resulting pop-up and click **OK)** and retry the configuration.