Configure Active IQ Unified Manager

Active IQ Unified Manager

NetApp
September 26, 2026

This PDF was generated from https://docs.netapp.com/us-en/active-iq-unified-manager/config/concept_configure_unified_manager.html on September 26, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Configure Active IQ Unified Manager . . . 1
- Learn about configuring Active IQ Unified Manager . . . 1
- Learn about the configuration sequence in Active IQ Unified Manager . . . 1
- Access the web UI in Active IQ Unified Manager . . . 1
- Perform the initial setup of the Active IQ Unified Manager web UI . . . 2
- Add clusters to Active IQ Unified Manager . . . 4
- Configure notifications . . . 6
  - Configure Active IQ Unified Manager to send alert notifications . . . 6
  - Configure event notification settings in Active IQ Unified Manager . . . 7
  - Enable remote authentication in Active IQ Unified Manager . . . 8
  - Disable nested groups from remote authentication in Active IQ Unified Manager . . . 9
  - Set up authentication services in Active IQ Unified Manager . . . 9
  - Add authentication servers to Active IQ Unified Manager . . . 10
  - Test the configuration of authentication servers in Active IQ Unified Manager . . . 12
  - Add alerts in Active IQ Unified Manager . . . 12
- Change the local user password in Active IQ Unified Manager . . . 14
- Set the session inactivity timeout in Active IQ Unified Manager . . . 14
- Set the session timeout using the CLI in Active IQ Unified Manager . . . 15
- Change the Unified Manager host name . . . 15
  - Change the Active IQ Unified Manager virtual appliance host name . . . 15
  - Generate a HTTPS security certificate in Active IQ Unified Manager . . . 16
  - Restart the Active IQ Unified Manager virtual machine . . . 18
  - Change the Active IQ Unified Manager host name on Linux systems . . . 18
- Enable and disable policy-based storage management in Active IQ Unified Manager . . . 19

Configure Active IQ Unified Manager

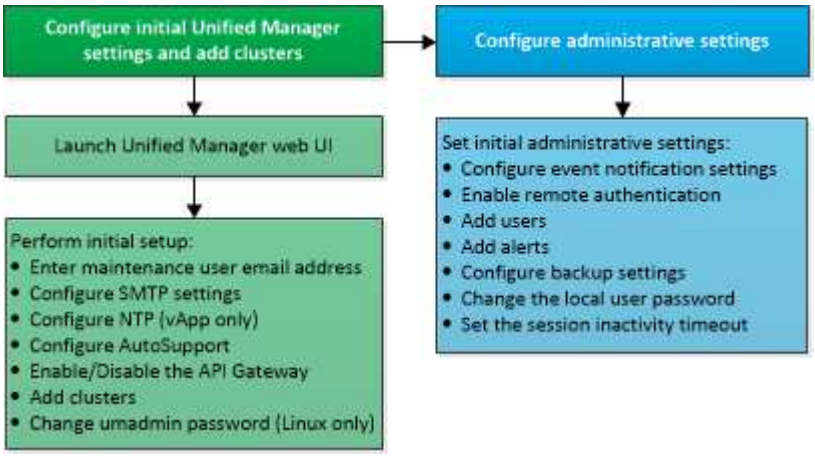
Learn about configuring Active IQ Unified Manager

After installing Active IQ Unified Manager (formerly OnCommand Unified Manager) you must complete the initial setup (also called the first experience wizard) to access the web UI. Then you can perform additional configuration tasks, such as adding clusters, configuring remote authentication, adding users, and adding alerts.

Some of the procedures described in this manual are required to complete the initial setup of your Unified Manager instance. Other procedures are recommended configuration settings that are helpful to set up on your new instance, or that are good to know about before you start the regular monitoring of your ONTAP systems.

Learn about the configuration sequence in Active IQ Unified Manager

The configuration workflow describes the tasks that you must perform before you can use Unified Manager.



Access the web UI in Active IQ Unified Manager

After you have installed Unified Manager, you can access the web UI to set up Unified Manager so that you can begin monitoring your ONTAP systems.

Before you begin

- If this is the first time you are accessing the web UI, you must log in as the maintenance user (or umadmin user for Linux installations).
- If you plan to allow users to access Unified Manager using the short name instead of using the fully qualified domain name (FQDN) or IP address, then your network configuration has to resolve this short name to a valid FQDN.
- If the server uses a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue the access or install a Certificate Authority (CA) signed digital certificate for server authentication.

Steps

1. Start the Unified Manager web UI from your browser by using the URL displayed at the end of the installation. The URL is the IP address or fully qualified domain name (FQDN) of the Unified Manager server.

   The link is in the following format: `https://URL`.

2. Log in to the Unified Manager web UI using your maintenance user credentials.

> If you make three consecutive unsuccessful attempts to log into the web UI within an hour, you will be locked out of the system, and will need to contact your system administrator. This is applicable for only local users.

Perform the initial setup of the Active IQ Unified Manager web UI

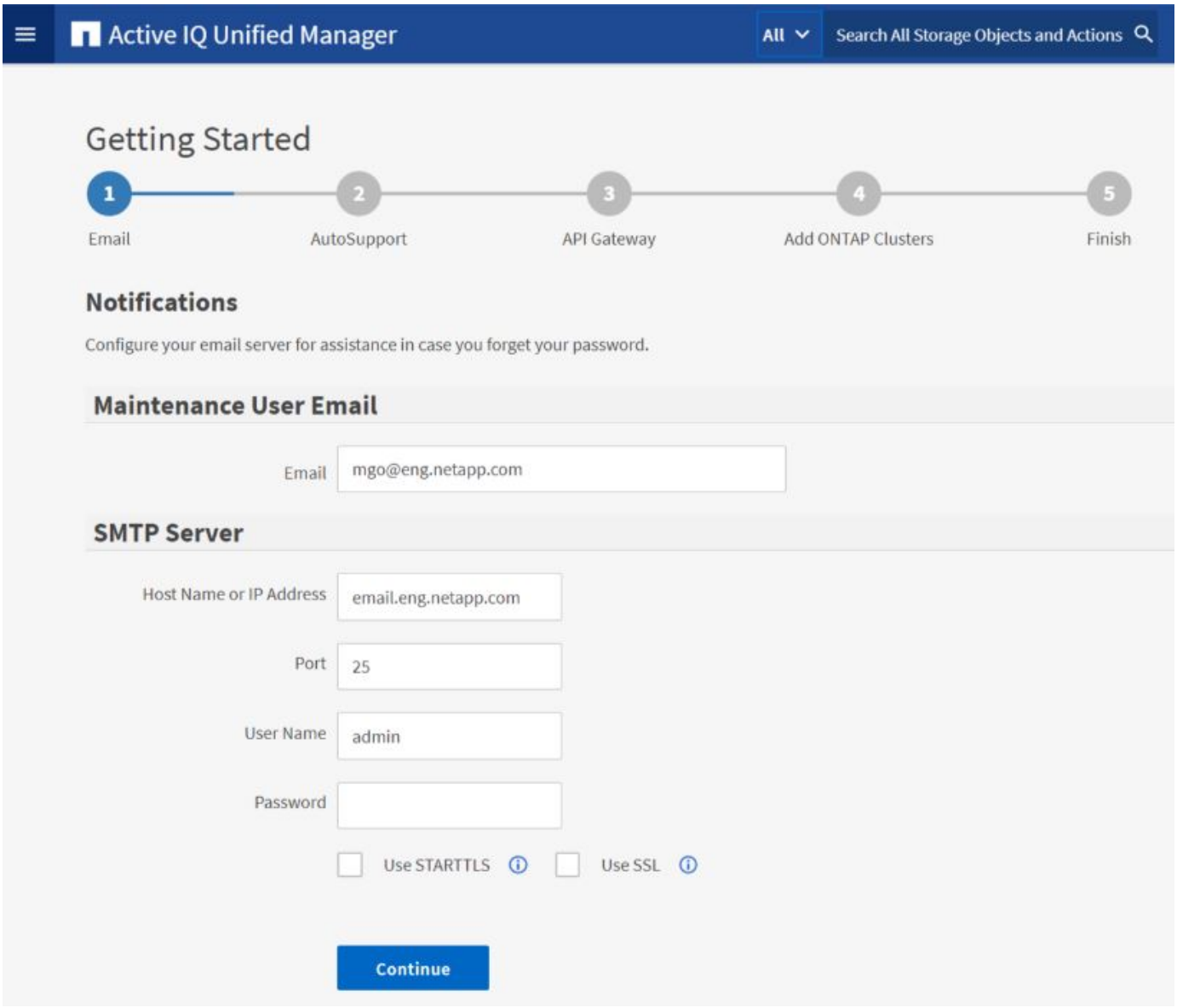
To use Unified Manager, you must first configure the initial setup options, including the NTP server, the maintenance user email address, the SMTP server host, and adding ONTAP clusters.

Before you begin

You must have performed the following operations:

- Launched the Unified Manager web UI using the URL provided after installation
- Logged in using the maintenance user name and password (umadmin user for Linux installations) created during installation

The Active IQ Unified ManagerGetting Started page appears only when you first access the web UI. The page below is from an installation on VMware.



If you want to change any of these options later, you can select your choice from the General options in the Unified Manager left-navigation pane. Note that the NTP setting is only for VMware installations, and it can be changed later using the Unified Manager maintenance console.

Steps

1. In the Active IQ Unified Manager Initial Setup page, enter the maintenance user email address, the SMTP server host name and any additional SMTP options, and the NTP server (VMware installations only). Then click **Continue**.

   If you have selected the **Use STARTTLS** or **Use SSL** option, a certificate page displays after you click the **Continue** button. Verify the certificate details and accept the certificate to continue with the initial setup settings of the web UI.

2. In the AutoSupport page click **Agree and Continue** to enable the sending of AutoSupport messages from Unified Manager to NetAppActive IQ.

   If you need to designate a proxy to provide internet access in order to send AutoSupport content, or if you want to disable AutoSupport, use the **General** > **AutoSupport** option from the web UI.

3. On Red Hat systems, change the umadmin user password from the default “admin” string to a personalized string.
4. In the Set up API Gateway page, select whether you want to use the API Gateway feature that allows Unified Manager to manage the ONTAP clusters you are planning to monitor using ONTAP REST APIs. Then click **Continue**.

   You can enable or disable this setting later in the web UI from **General** > **Feature Settings** > **API Gateway**. For more information about the APIs, see Getting started with Active IQ Unified Manager REST APIs.

5. Add the clusters that you want Unified Manager to manage, and then click **Next**. For each cluster you plan to manage, you must have the host name or cluster management IP address (IPv4 or IPv6) along with the user name and password credentials - the user must have the “admin” role.

   This step is optional. You can add clusters later in the web UI from **Storage Management** > **Cluster Setup**.

6. In the Summary page, verify that all the settings are correct and click **Finish**.

The Getting Started page closes and the Unified Manager Dashboard page is displayed.

Add clusters to Active IQ Unified Manager

You can add a cluster to Active IQ Unified Manager so that you can monitor the cluster. This includes the ability to obtain cluster information such as the health, capacity, performance, and configuration of the cluster so that you can find and resolve any issues that might occur.

Before you begin

- You must have the Application Administrator or Storage Administrator role.
- You must have the following information:
  - Unified Manager supports on-premises ONTAP clusters, ONTAP Select, Cloud Volumes ONTAP.
  - Host name or cluster-management IP address

    The host name is the FQDN or short name that Unified Manager uses to connect to the cluster. The host name must resolve to the cluster-management IP address.

    The cluster-management IP address must be the cluster-management LIF of the administrative storage virtual machine (SVM). If you use a node-management LIF, the operation fails.

  - The cluster must be running ONTAP version 9.1 software or greater.
  - ONTAP administrator user name and password

    This account must have the *admin* role with Application access set to *ontapi*, *amqp*, *console*, and *http*.

  - The port number to connect to the cluster using the HTTPS protocol (typically port 443)
  - You have the required certificates:

    SSL (HTTPS) certificate: This certificate is owned by Unified Manager. A default self-signed SSL (HTTPS) certificate is generated with a fresh installation of Unified Manager. NetApp recommends that you upgrade it to CA-signed certificate for better security. If the server certificate expires, you should

regenerate it and restart Unified Manager for the services to incorporate the new certificate. For more information about regenerating SSL certificate, see Generating an HTTPS security certificate.

EMS certificate: This certificate is owned by Unified Manager. It is used during authentication for EMS notifications received from ONTAP.

Certificates for Mutual TLS communication: Used during Mutual TLS communication between Unified Manager and ONTAP. The certificate-based authentication is enabled for a cluster, based on the ONTAP version. If the cluster running the ONTAP version is lower than the 9.5, certificate-based authentication is not enabled.

Certificate-based authentication is not enabled automatically for a cluster, if you are updating an older version of Unified Manager. However, you can enable it by modifying and saving the cluster details. If the certificate expires, you should regenerate it to incorporate the new certificate. For more information about viewing and regenerating the certificate, see Editing clusters.

- You can add a cluster from the web UI, and certificate-based authentication is automatically enabled.
- You can add a cluster through Unified Manager CLI, the certificate-based authentication is not enabled by default. If you add a cluster using Unified Manager CLI, it is required to edit the cluster using Unified Manager UI. You can see Supported Unified Manager CLI commands to add a cluster using Unified Manager CLI.
- If certificate-based authentication is enabled for a cluster, and you take the backup of Unified Manager from a server and restore to another Unified Manager server where hostname or IP address is changed, then monitoring of the cluster can fail. To avoid the failure, edit and save the cluster details. For more information about editing cluster details, see Editing clusters.

Cluster certificates: This certificate is owned by ONTAP. You cannot add a cluster to Unified Manager with an expired certificate and if the certificate has already expired, you should regenerate it before adding the cluster. For information about certificate generation, see the knowledge base (KB) article How to renew an ONTAP self-signed certificate in System Manager user interface.

- You must have adequate space on the Unified Manager server. You are prevented from adding a cluster to the server when greater than 90% of space in the database directory is already consumed.

For a MetroCluster configuration, you must add both the local and remote clusters, and the clusters must be configured correctly.

Steps

1. In the left navigation pane, click **Storage Management** > **Cluster Setup**.
2. On the Cluster Setup page, click **Add**.
3. In the Add Cluster dialog box, specify the required values, such as the host name or IP address of the cluster, user name, password, and port number.

   You can change the cluster-management IP address from IPv6 to IPv4 or from IPv4 to IPv6. The new IP address is reflected in the cluster grid and the cluster configuration page after the next monitoring cycle is complete.

4. Click **Submit**.
5. In the Authorize Host dialog box, click **View Certificate** to view the certificate information about the cluster.

6. Click **Yes**.

   After saving the cluster details, you can see the certificate for Mutual TLS communication for a cluster.

   If the certificate-based authentication is not enabled, Unified Manager checks the certificate only when the cluster is added initially. Unified Manager does not check the certificate for each API call to ONTAP.

After all the objects for a new cluster are discovered, Unified Manager starts to gather historical performance data for the previous 15 days. These statistics are collected using the data continuity collection functionality. This feature provides you with over two weeks of performance information for a cluster immediately after it is added. After the data continuity collection cycle is completed, real-time cluster performance data is collected, by default, every five minutes.

Because the collection of 15 days of performance data is CPU intensive, it is suggested that you stagger the addition of new clusters so that data continuity collection polls are not running on too many clusters at the same time. Additionally, if you restart Unified Manager during the data continuity collection period, the collection will be halted and you will see gaps in the performance charts for the missing timeframe.

If you receive an error message that you cannot add the cluster, check to see if the clocks on the two systems are not synchronized and the Unified Manager HTTPS certificate start date is later than the date on the cluster. You must ensure that the clocks are synchronized using NTP or a similar service.

Related information

Installing a CA signed and returned HTTPS certificate

Configure notifications

Configure Active IQ Unified Manager to send alert notifications

You can configure Unified Manager to send notifications that alert you about events in your environment. Before notifications can be sent, you must configure several other Unified Manager options.

Before you begin

You must have the Application Administrator role.

After deploying Unified Manager and completing the initial configuration, you should consider configuring your environment to trigger alerts and generate notification emails or SNMP traps based on the receipt of events.

Steps

1. Configure event notification settings.

   If you want alert notifications sent when certain events occur in your environment, you must configure an SMTP server and supply an email address from which the alert notification will be sent. If you want to use SNMP traps, you can select that option and provide the necessary information.

2. Enable remote authentication.

   If you want remote LDAP or Active Directory users to access the Unified Manager instance and receive

alert notifications, then you must enable remote authentication.

3. Add authentication servers.

   You can add authentication servers so that remote users within the authentication server can access Unified Manager.

4. Add users.

   You can add several different types of local or remote users and assign specific roles. When you create an alert, you assign a user to receive the alert notifications.

5. Add alerts.

   After you have added the email address for sending notifications, added users to receive the notifications, configured your network settings, and configured SMTP and SNMP options needed for your environment, then you can assign alerts.

Configure event notification settings in Active IQ Unified Manager

You can configure Unified Manager to send alert notifications when an event is generated or when an event is assigned to a user. You can configure the SMTP server that is used to send the alert, and you can set various notification mechanisms—for example, alert notifications can be sent as emails or SNMP traps.

Before you begin

You must have the following information:

- Email address from which the alert notification is sent

  The email address appears in the “From” field in sent alert notifications. If the email cannot be delivered for any reason, this email address is also used as the recipient for undeliverable mail.

- SMTP server host name, and the user name and password to access the server
- Host name or IP address for the trap destination host that will receive the SNMP trap, along with the SNMP version, outbound trap port, community, and other required SNMP configuration values

  To specify multiple trap destinations, separate each host with a comma. In this case, all other SNMP settings, such as version and outbound trap port, must be the same for all hosts in the list.

You must have the Application Administrator or Storage Administrator role.

Steps

1. In the left navigation pane, click **General** > **Notifications**.
2. In the Notifications page, configure the appropriate settings.

   Notes:

   - If the From Address is pre-filled with the address "ActiveIQUnifiedManager@localhost.com", you should change it to a real, working email address to make sure that all email notifications are delivered successfully.
   - If the host name of the SMTP server cannot be resolved, you can specify the IP address (IPv4 or IPv6)

of the SMTP server instead of the host name.

3. Click **Save**.
4. If you have selected the **Use STARTTLS** or **Use SSL** option, a certificate page displays after you click the **Save** button. Verify the certificate details and accept the certificate to save the notification settings.

   You can click the **View Certificate Details** button to view the certificate details. If the existing certificate is expired, uncheck the **Use STARTTLS** or **Use SSL** box, save the notification settings, and again check the **Use STARTTLS** or **Use SSL** box to view a new certificate.

Enable remote authentication in Active IQ Unified Manager

You can enable remote authentication so that the Unified Manager server can communicate with your authentication servers. The users of the authentication server can access the Unified Manager graphical interface to manage storage objects and data.

Before you begin

You must have the Application Administrator role.

> The Unified Manager server must be connected directly with the authentication server. You must disable any local LDAP clients such as SSSD (System Security Services Daemon) or NSLCD (Name Service LDAP Caching Daemon).

You can enable remote authentication using either Open LDAP or Active Directory. If remote authentication is disabled, remote users cannot access Unified Manager.

Remote authentication is supported over LDAP and LDAPS (Secure LDAP). Unified Manager uses 389 as the default port for non-secure communication, and 636 as the default port for secure communication.

> The certificate that is used to authenticate users must conform to the X.509 format.

Steps

1. In the left navigation pane, click **General** > **Remote Authentication**.
2. Check the box for **Enable remote authentication…**.
3. In the Authentication Service field, select the type of service and configure the authentication service.

For Authentication type…	Enter the following information…
Active Directory	• Authentication server administrator name in one of following formats: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (using the appropriate LDAP notation) • Administrator password • Base distinguished name (using the appropriate LDAP notation)

For Authentication type…	Enter the following information…
Open LDAP	• Bind distinguished name (in the appropriate LDAP notation) • Bind password • Base distinguished name

If the authentication of an Active Directory user takes a long time or times out, the authentication server is probably taking a long time to respond. Disabling support for nested groups in Unified Manager might reduce the authentication time.

If you select the Use Secure Connection option for the authentication server, then Unified Manager communicates with the authentication server using the Secure Sockets Layer (SSL) protocol.

4. **Optional:** Add authentication servers, and test the authentication.
5. Click **Save**.

Disable nested groups from remote authentication in Active IQ Unified Manager

If you have remote authentication enabled, you can disable nested group authentication so that only individual users, and not group members, can remotely authenticate to Unified Manager. You can disable nested groups when you want to improve Active Directory authentication response time.

Before you begin

- You must have the Application Administrator role.
- Disabling nested groups is only applicable when using Active Directory.

Disabling support for nested groups in Unified Manager might reduce the authentication time. If nested group support is disabled, and if a remote group is added to Unified Manager, individual users must be members of the remote group to authenticate to Unified Manager.

Steps

1. In the left navigation pane, click **General** > **Remote Authentication**.
2. Check the box for **Disable Nested Group Lookup**.
3. Click **Save**.

Set up authentication services in Active IQ Unified Manager

Authentication services enable the authentication of remote users or remote groups in an authentication server before providing them access to Unified Manager. You can authenticate users by using predefined authentication services (such as Active Directory or OpenLDAP), or by configuring your own authentication mechanism.

Before you begin

- You must have enabled remote authentication.
- You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **General** > **Remote Authentication**.
2. Select one of the following authentication services:

If you select…	Then do this…
Active Directory	a. Enter the administrator name and password. b. Specify the base distinguished name of the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Enter the bind distinguished name and bind password. b. Specify the base distinguished name of the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is **cn=ou,dc=domain,dc=com**.
Others	a. Enter the bind distinguished name and bind password. b. Specify the base distinguished name of the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is **cn=ou,dc=domain,dc=com**. c. Specify the LDAP protocol version that is supported by the authentication server. d. Enter the user name, group membership, user group, and member attributes.

If you want to modify the authentication service, you must delete any existing authentication servers, and then add new authentication servers.

3. Click **Save**.

Add authentication servers to Active IQ Unified Manager

You can add authentication servers and enable remote authentication on the management server so that remote users within the authentication server can access Unified Manager.

Before you begin

- The following information must be available:

- Host name or IP address of the authentication server
- Port number of the authentication server

- You must have enabled remote authentication and configured your authentication service so that the management server can authenticate remote users or groups in the authentication server.
- You must have the Application Administrator role.

If the authentication server that you are adding is part of a high-availability (HA) pair (using the same database), you can also add the partner authentication server. This enables the management server to communicate with the partner when one of the authentication servers is unreachable.

Steps

1. In the left navigation pane, click **General** > **Remote Authentication**.
2. Enable or disable the **Use secure connection** option:

If you want to…	Then do this…
Enable it	a. Select the **Use Secure Connection** option. b. In the Authentication Servers area, click **Add**. c. In the Add Authentication Server dialog box, enter the authentication name or IP address (IPv4 or IPv6) of the server. d. In the Authorize Host dialog box, click View Certificate. e. In the View Certificate dialog box, verify the certificate information, and then click **Close**. f. In the Authorize Host dialog box, click **Yes**. When you enable the **Use Secure Connection authentication** option, Unified Manager communicates with the authentication server and displays the certificate. Unified Manager uses 636 as default port for secure communication and port number 389 for non-secure communication.
Disable it	a. Clear the **Use Secure Connection** option. b. In the Authentication Servers area, click **Add**. c. In the Add Authentication Server dialog box, specify either the host name or IP address (IPv4 or IPv6) of the server, and the port details. d. Click **Add**.

   The authentication server that you added is displayed in the Servers area.

3. Perform a test authentication to confirm that you can authenticate users in the authentication server that you added.

Test the configuration of authentication servers in Active IQ Unified Manager

You can validate the configuration of your authentication servers to ensure that the management server is able to communicate with them. You can validate the configuration by searching for a remote user or remote group from your authentication servers, and authenticating them using the configured settings.

Before you begin

- You must have enabled remote authentication, and configured your authentication service so that the Unified Manager server can authenticate the remote user or remote group.
- You must have added your authentication servers so that the management server can search for the remote user or remote group from these servers and authenticate them.
- You must have the Application Administrator role.

If the authentication service is set to Active Directory, and if you are validating the authentication of remote users who belong to the primary group of the authentication server, information about the primary group is not displayed in the authentication results.

Steps

1. In the left navigation pane, click **General** > **Remote Authentication**.
2. Click **Test Authentication**.
3. In the Test User dialog box, specify the user name and password of the remote user or the user name of the remote group, and then click **Test**.

   If you are authenticating a remote group, you must not enter the password.

Add alerts in Active IQ Unified Manager

You can configure alerts to notify you when a particular event is generated. You can configure alerts for a single resource, for a group of resources, or for events of a particular severity type. You can specify the frequency with which you want to be notified and associate a script to the alert.

Before you begin

- You must have configured notification settings such as the user email address, SMTP server, and SNMP trap host to enable the Active IQ Unified Manager server to use these settings to send notifications to users when an event is generated.
- You must know the resources and events for which you want to trigger the alert, and the user names or email addresses of the users that you want to notify.
- If you want to have a script execute based on the event, you must have added the script to Unified Manager by using the Scripts page.
- You must have the Application Administrator or Storage Administrator role.

You can create an alert directly from the Event details page after receiving an event in addition to creating an alert from the Alert Setup page, as described here.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.

2. In the Alert Setup page, click **Add**.
3. In the Add Alert dialog box, click **Name**, and enter a name and description for the alert.
4. Click **Resources**, and select the resources to be included in or excluded from the alert.

   You can set a filter by specifying a text string in the **Name contains** field to select a group of resources. Based on the text string that you specify, the list of available resources displays only those resources that match the filter rule. The text string that you specify is case-sensitive.

   If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.

5. Click **Events**, and select the events based on the event name or event severity type for which you want to trigger an alert.

   To select more than one event, press the Ctrl key while you make your selections.

6. Click **Actions**, and select the users that you want to notify, choose the notification frequency, choose whether an SNMP trap will be sent to the trap receiver, and assign a script to be executed when an alert is generated.

   If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you modified the email address of the selected user from the Users page, the modified email address is not updated for the selected user.

   You can also choose to notify users through SNMP traps.

7. Click **Save**.

Example of adding an alert

This example shows how to create an alert that meets the following requirements:

- Alert name: HealthTest
- Resources: includes all volumes whose name contains “abc” and excludes all volumes whose name contains “xyz”
- Events: includes all critical health events
- Actions: includes "sample@domain.com", a “Test” script, and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

Steps

1. Click **Name**, and enter **HealthTest** in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
   a. Enter **abc** in the **Name contains** field to display the volumes whose name contains “abc”.
   b. Select **<<All Volumes whose name contains 'abc'>>** from the Available Resources area, and move it to the Selected Resources area.
   c. Click **Exclude**, and enter **xyz** in the **Name contains** field, and then click **Add**.

3. Click **Events**, and select **Critical** from the Event Severity field.
4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.
5. Click **Actions**, and enter **sample@domain.com** in the Alert these users field.
6. Select **Remind every 15 minutes** to notify the user every 15 minutes.

   You can configure an alert to repeatedly send notifications to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.

7. In the Select Script to Execute menu, select **Test** script.
8. Click **Save**.

Change the local user password in Active IQ Unified Manager

You can change your local user login password to prevent potential security risks.

Before you begin

You must be logged in as a local user.

The passwords for the maintenance user and for remote users cannot be changed using these steps. To change a remote user password, contact your password administrator. To change the maintenance user password, see Using the maintenance console.

Steps

1. Log in to Unified Manager.
2. From the top menu bar, click the user icon and then click **Change Password**.

   The **Change Password** option is not displayed if you are a remote user.

3. In the Change Password dialog box, enter the current password and the new password.
4. Click **Save**.

If Unified Manager is configured in a high-availability configuration, you must change the password on the second node of the setup. Both instances must have same password.

Set the session inactivity timeout in Active IQ Unified Manager

You can specify the inactivity timeout value for Unified Manager so that the session is terminated automatically after a certain period of inactivity. By default the timeout is set to 4,320 minutes (72 hours).

Before you begin

You must have the Application Administrator role.

This setting affects all logged in user sessions.

This option is not available if you have enabled Security Assertion Markup Language (SAML)

authentication.

Steps

1. In the left navigation pane, click **General** > **Feature Settings**.
2. In the **Feature Settings** page, specify the inactivity timeout by choosing one of the following options:

If you want to…	Then do this…
Have no timeout set so that the session is never closed automatically	In the **Inactivity Timeout** panel, move the slider button to the left (off) and click **Apply**.
Set a specific number of minutes as the time out value	In the **Inactivity Timeout** panel, move the slider button to the right (on), specify the inactivity timeout value in minutes, and click **Apply**.

Set the session timeout using the CLI in Active IQ Unified Manager

You can set a maximum session timeout value for Unified Manager using the CLI so that the session is terminated automatically after a certain period of time. By default, your session timeout is set to the maximum value, which is 4,320 minutes (72 hours). This means that your session ends automatically after 72 hours, even if you are logged in and actively using Unified Manager.

About this task

You must have the Application Administrator role.

The session timeout setting affects all logged in user sessions.

Steps

1. Log in to the Unified Manager CLI by entering the `um cli login` command. Use a valid username and password for authentication.
2. Enter the `um option set max.session.timeout.value=<in mins>` command to modify the session timeout value.

Change the Unified Manager host name

Change the Active IQ Unified Manager virtual appliance host name

The network host is assigned a name when the Unified Manager virtual appliance is first deployed. You can change the host name after deployment. If you change the host name, you must also regenerate the HTTPS certificate.

Before you begin

You must be logged in to Unified Manager as the maintenance user, or have the Application Administrator role assigned to you to perform these tasks.

You can use the host name (or the host IP address) to access the Unified Manager web UI. If you configured a static IP address for your network during deployment, then you would have designated a name for the network

host. If you configured the network using DHCP, the host name should be taken from the DNS. If DHCP or DNS is not properly configured, the host name “Unified Manager” is automatically assigned and associated with the security certificate.

Regardless of how the host name was assigned, if you change the host name, and intend to use the new host name to access the Unified Manager web UI, you must generate a new security certificate.

If you access the web UI by using the server’s IP address instead of the host name, you do not have to generate a new certificate if you change the host name. However, it is the best practice to update the certificate so that the host name in the certificate matches the actual host name.

If you change the host name in Unified Manager, you must manually update the host name in OnCommand Workflow Automation (WFA). The host name is not updated automatically in WFA.

The new certificate does not take effect until the Unified Manager virtual machine is restarted.

Steps

1. Generate an HTTPS security certificate

   If you want to use the new host name to access the Unified Manager web UI, you must regenerate the HTTPS certificate to associate it with the new host name.

2. Restart the Unified Manager virtual machine

   After you regenerate the HTTPS certificate, you must restart the Unified Manager virtual machine.

Generate a HTTPS security certificate in Active IQ Unified Manager

When Active IQ Unified Manager is installed for the first time, a default HTTPS certificate is installed. You might generate a new HTTPS security certificate that replaces the existing certificate.

Before you begin

You must have the Application Administrator role.

There can be multiple reasons to regenerate the certificate such as if you want to have better values for Distinguished Name (DN) or if you want a higher key size, or longer expiry period or if the current certificate has expired.

If you do not have access to the Unified Manager web UI, you can regenerate the HTTPS certificate with the same values using the maintenance console. While regenerating certificates, you can define the key size and the validity duration of the key. If you use the `Reset Server Certificate` option from the maintenance console, then a new HTTPS certificate is created which is valid for 397 days. This certificate will have an RSA key of size 2048 bits.

Steps

1. In the left navigation pane, click **General** > **HTTPS Certificate**.
2. Click **Regenerate HTTPS Certificate**.

   The Regenerate HTTPS Certificate dialog box is displayed.

3. Select one of the following options depending on how you want to generate the certificate:

If you want to…	Do this…
Regenerate the certificate with the current values	Click the **Regenerate Using Current Certificate Attributes** option.
Generate the certificate using different values	Click the **Update the Current Certificate Attributes** option. The Common Name and Alternative Names fields will use the values from the existing certificate if you do not enter new values. The “Common Name” should be set to the FQDN of the host. The other fields do not require values, but you can enter values, for example, for the EMAIL, COMPANY, DEPARTMENT, City, State, and Country if you want those values to be populated in the certificate. You can also select from the available KEY SIZE (The key algorithm is “RSA”.) and VALIDITY PERIOD. • The permitted values for key size are `2048`, `3072` and `4096`. • The validity periods are minimum 1 day to maximum 36500 days. Even though a validity period of 36500 days is permitted, it is recommended you use a validity period of not more than 397 days or 13 months. Because if you select a validity period of more than 397 days and plan to export a CSR for this certificate and get it signed by a well known CA, the validity of the signed certificate returned to you by the CA will be reduced to 397 days. • You can select the “Exclude local identifying information (e.g. localhost)” checkbox if you want to remove the local identifying information from the Alternative Names field in the certificate. When this checkbox is selected, only what you enter in the field is used in the Alternative Names field. When left blank the resulting certificate will not have an Alternative Names field at all.

4. Click **Yes** to regenerate the certificate.
5. Restart the Unified Manager server so that the new certificate takes effect.
6. Verify the new certificate information by viewing the HTTPS certificate.

Restart the Active IQ Unified Manager virtual machine

You can restart the virtual machine from the maintenance console of Unified Manager. You must restart after generating a new security certificate or if there is a problem with the virtual machine.

Before you begin

The virtual appliance is powered on.

You are logged in to the maintenance console as the maintenance user.

You can also restart the virtual machine from vSphere by using the **Restart Guest** option. See the VMware documentation for more information.

Steps

1. Access the maintenance console.
2. Select **System Configuration** > **Reboot Virtual Machine**.

Change the Active IQ Unified Manager host name on Linux systems

At some point, you might want to change the host name of the Red Hat Enterprise Linux machine on which you have installed Unified Manager. For example, you might want to rename the host to more easily identify your Unified Manager servers by type, workgroup, or monitored cluster group when you list your Linux machines.

Before you begin

You must have root user access to the Linux system on which Unified Manager is installed.

You can use the host name (or the host IP address) to access the Unified Manager web UI. If you configured a static IP address for your network during deployment, then you would have designated a name for the network host. If you configured the network using DHCP, the host name should be taken from the DNS server.

Regardless of how the host name was assigned, if you change the host name and intend to use the new host name to access the Unified Manager web UI, you must generate a new security certificate.

If you access the web UI by using the server's IP address instead of the host name, you do not have to generate a new certificate if you change the host name. However, it is the best practice to update the certificate, so that the host name in the certificate matches the actual host name. The new certificate does not take effect until the Linux machine is restarted.

If you change the host name in Unified Manager, you must manually update the host name in OnCommand Workflow Automation (WFA). The host name is not updated automatically in WFA.

Steps

1. Log in as the root user to the Unified Manager system that you want to modify.
2. Stop the Unified Manager software and the associated MySQL software by entering the following command:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Change the host name using the Linux `hostnamectl` command:

```
hostnamectl set-hostname new_FQDN

hostnamectl set-hostname nuhost.corp.widget.com
```

4. Regenerate the HTTPS certificate for the server:

```
/opt/netapp/essentials/bin/cert.sh create
```

5. Restart the network service:

```
systemctl restart NetworkManager.service
```

6. After the service is restarted, verify whether the new host name is able to ping itself:

```
ping new_hostname

ping nuhost
```

   This command should return the same IP address that was set earlier for the original host name.

7. After you complete and verify your host name change, restart Unified Manager by entering the following command:

```
systemctl start mysqld ocie ocieau
```

Enable and disable policy-based storage management in Active IQ Unified Manager

Starting with Unified Manager 9.7, you can provision storage workloads (volumes and LUNs) on your ONTAP clusters, and manage those workloads based on assigned performance service levels. This functionality is similar to creating workloads in ONTAP System Manager and attaching QoS policies, but when applied using Unified Manager you can provision and manage workloads across all clusters that your Unified Manager instance is monitoring.

You must have the Application Administrator role.

This option is enabled by default, but you can disable it if you do not want to provision and manage workloads using Unified Manager.

When enabled, this option provides many new items in the user interface:

New Content	Location
A page to provision new workloads	Available from **Common Tasks** > **Provisioning**
A page to create performance service level policies	Available from **Settings** > **Policies** > **Performance Service Levels**
A page to create performance storage efficiency policies	Available from **Settings** > **Policies** > **Storage Efficiency**

New Content	Location
Panels that describe your current Workload Performance and Workload IOPS	Available from the Dashboard

See the online help in the product for more information on these pages and on this functionality.

Steps

1. In the left navigation pane, click **General** > **Feature Settings**.
2. In the **Feature Settings** page, disable or enable policy-based storage management by choosing one of the following options:

If you want to…	Then do this…
Disable policy-based storage management	In the **Policy-based storage management** panel, move the slider button to the left.
Enable policy-based storage management	In the **Policy-based storage management** panel, move the slider button to the right.

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.