# Perform configuration and administrative tasks

## Active IQ Unified Manager

NetApp
December 23, 2021

# Table of Contents

# Perform configuration and administrative tasks

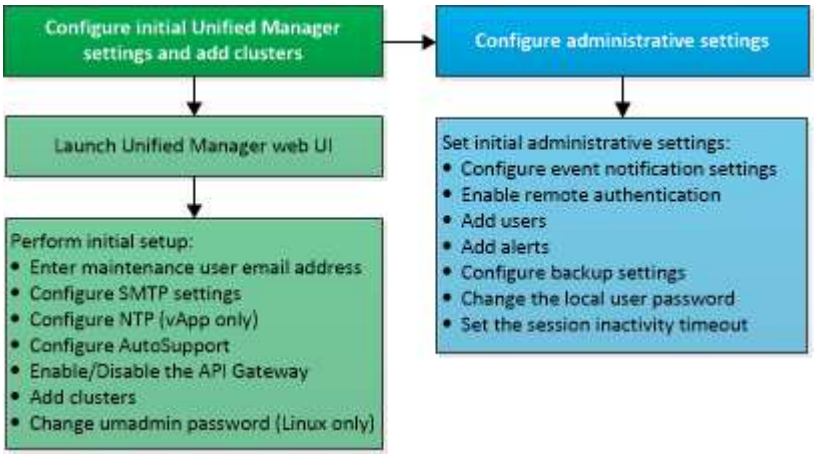
## Configuring Active IQ Unified Manager

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.

### Overview of the configuration sequence

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




### Accessing the Unified Manager web UI

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.

#### What you'll need

- 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.

## Performing the initial setup of the Unified Manager web UI

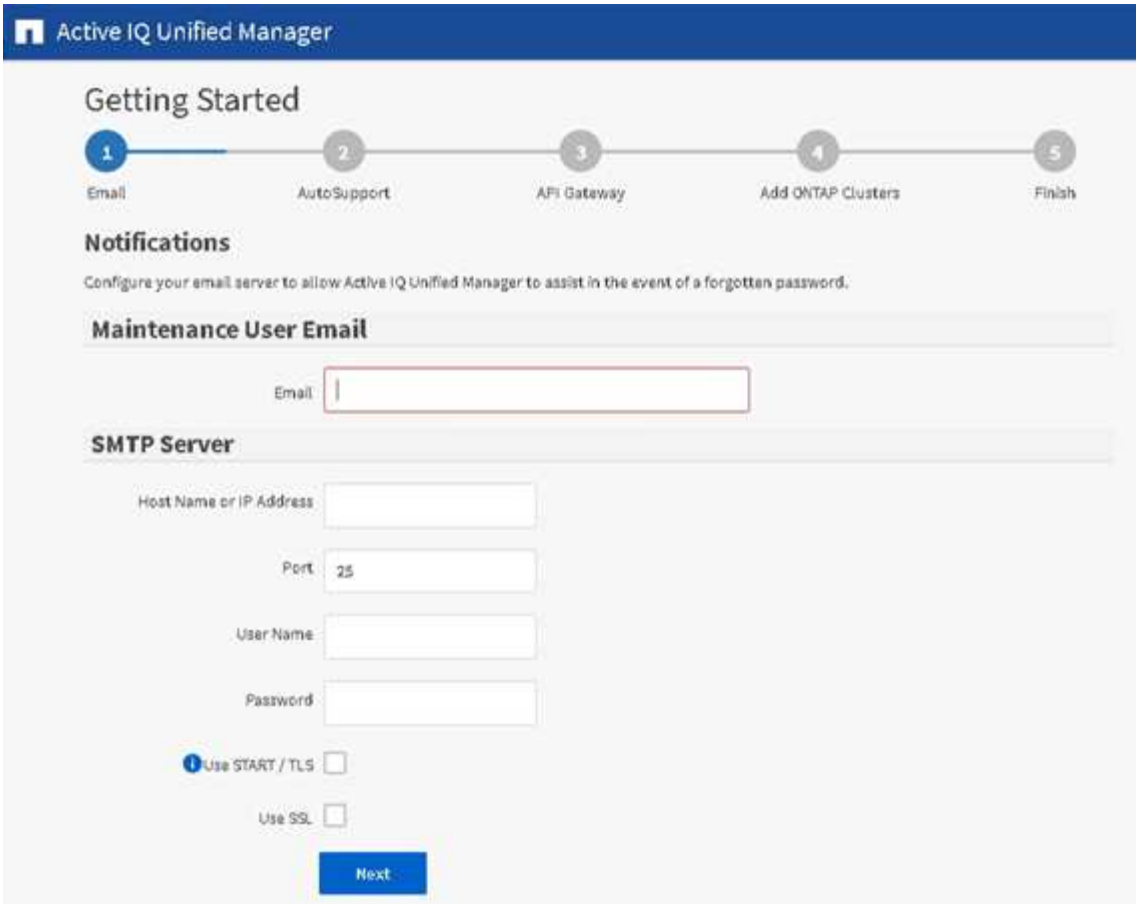
To use Unified Manager, you must first configure the initial setup options, including the NTP server, the maintenance user email address, the SMTP server host, and adding ONTAP clusters.

**What you'll need**

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**.
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 and CentOS systems you can 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 the Active IQ Unified Manager API Developer’s Guide.

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.

## Adding clusters

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.

**What you'll need**

- You must have the Application Administrator or Storage Administrator role.
- You must have the following information:
  - 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*, *ssh*, and *http*.

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

    **Server certificates**: Used for registration. A valid certificate is required for adding a cluster. If the server certificate expires, you should regenerate it and restart Unified Manager for the services to be automatically registered again. For information about certificate generation, see the knowledge base (KB) article: How to renew an SSL certificate in ONTAP 9

    **Client certificates**: Used for authentication. A valid certificate is required for adding a cluster. You cannot add a cluster to Unified Manager with an expired certificate and if the client certificate has already expired, you should regenerate it before adding the cluster. However, if this certificate expires for a cluster that is already added, and is being used by Unified Manager, EMS messaging continues to function with the expired certificate. You do not need to regenerate the client certificate.

    You can add clusters which are behind a NAT/firewall by using the Unified Manager NAT IP address. Any connected Workflow Automation or SnapProtect systems must also be behind the NAT/firewall, and SnapProtect API calls must use the NAT IP address to identify the cluster.

- 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.

You can monitor a single cluster by two instances of Unified Manager provided that you have configured a second cluster-management LIF on the cluster so that each instance of Unified Manager connects through a different LIF.

**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**.

   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.

## Configuring 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.

**What you'll need**

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.

### Configuring event notification settings

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.

**What you'll need**

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 and click **Save**.

   **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.

### Enabling remote authentication

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.

**What you'll need**

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:<br>◦ `domainname\username`<br>◦ `username@domainname`<br>◦ `Bind Distinguished Name` (using the appropriate LDAP notation)<br>• Administrator password<br>• Base distinguished name (using the appropriate LDAP notation) |
| Open LDAP | • Bind distinguished name (in the appropriate LDAP notation)<br>• Bind password<br>• 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**.

#### Disabling nested groups from remote authentication

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.

#### What you'll need

- 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**.

### Setting up authentication services

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.

#### What you'll need

- 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.<br>b. Specify the base distinguished name of the authentication server.<br><br>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.<br>b. Specify the base distinguished name of the authentication server.<br><br>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**. |

| If you select… | Then do this… |
| --- | --- |
| Others | a. Enter the bind distinguished name and bind password.<br>b. Specify the base distinguished name of the authentication server.<br>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**.<br>c. Specify the LDAP protocol version that is supported by the authentication server.<br>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**.

#### Adding authentication servers

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.

#### What you'll need

- 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.<br>b. In the Authentication Servers area, click **Add**.<br>c. In the Add Authentication Server dialog box, enter the authentication name or IP address (IPv4 or IPv6) of the server.<br>d. In the Authorize Host dialog box, click View Certificate.<br>e. In the View Certificate dialog box, verify the certificate information, and then click **Close**.<br>f. In the Authorize Host dialog box, click **Yes**.<br>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.<br>b. In the Authentication Servers area, click **Add**.<br>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.<br>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.

#### Testing the configuration of authentication servers

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.

#### What you'll need

- 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.

### Adding alerts

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.

**What you'll need**

- 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**.

## Changing the local user password

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

### What you'll need

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.

## Setting the session inactivity timeout

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

### What you'll need

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**. |

| If you want to… | Then do this… |
| --- | --- |
| 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**. |

## Changing the Unified Manager host name

At some point, you might want to change the host name of the system 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.

The steps required to change the host name are different depending on whether Unified Manager is running on a VMware ESXi server, on a Red Hat or CentOS Linux server, or on a Microsoft Windows server.

### Changing the 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.

#### What you'll need

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.

#### Generating an HTTPS security certificate

## 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.

**What you'll need**

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. |

| If you want to… | Do this… |
| --- | --- |
| Generate the certificate using different values | Click the **Update the Current Certificate Attributes** option.<br><br>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.<br><br>• The permitted values for key size are `2048`, `3072` and `4096`.<br>• The validity periods are minimum 1 day to maximum 36500 days.<br><br>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.<br><br>• 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.

Verify the new certificate information by viewing the HTTPS certificate.

#### Restarting the 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.

**What you'll need**

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**.

#### Changing the Unified Manager host name on Linux systems

At some point, you might want to change the host name of the Red Hat Enterprise Linux or CentOS 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.

**What you'll need**

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:

   ```
   service network restart
   ```

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
   ```

## Enabling and disabling policy-based storage management

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** |

| New Content | Location |
| --- | --- |
| A page to create performance storage efficiency policies | Available from **Settings** > **Policies** > **Storage Efficiency** |
| 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. |

# Configuring Unified Manager backup

You can configure the backup capability on Unified Manager through a set of configuration steps to be performed on the host systems and the through maintenance console.

For information about the configuration steps, see Managing backup and restore operations.

# Managing feature settings

The Feature Settings page allows you to enable and disable specific features in Active IQ Unified Manager. This includes creating and managing storage objects based on policies, enabling the API Gateway and Login Banner, uploading scripts for managing alerts, timing out a web UI session based on inactivity time, and disabling receipt of Active IQ platform events.

The Feature Settings page is only available for users with Application Administrator role.

For information about Scripts Upload, see Enabling and disabling scripts upload.

## Enabling policy-based storage management

The **Policy-based storage management** option allows storage management based on

service level objectives (SLOs). This option is enabled by default.

On activating this feature, you can provision storage workloads on the ONTAP clusters added to your Active IQ Unified Manager instance, and manage these workloads based on the assigned Performance Service Levels and Storage Efficiency Policies.

You can choose to activate or deactivate this feature from **General** > **Feature Settings** > **Policy-based storage management**. On activating this feature, the following pages are available for operation and monitoring:

- Provisioning (storage workload provisioning)
- **Policies** > **Performance Service Levels**
- **Policies** > **Storage Efficiency**
- Workloads Managed by Performance Service Level column on the Clusters Setup page
- Workload Performance panel on the **Dashboard**

You can use the screens to create Performance Service Levels and Storage Efficiency Policies, and provision storage workloads. You can also monitor the storage workloads that conform to the assigned Performance Service Levels, as well as the nonconforming ones. The Workload Performance and Workload IOPS panel also enables you to assess the total, available, and used capacity and performance (IOPS) of the clusters across your data center based on the storage workloads provisioned on them.

After activating this feature, you can run the Unified Manager REST APIs to perform some of these functions from **Menu Bar** > **Help button** > **API Documentation** > **storage-provider** category. Alternatively, you can enter the host name or IP address and the URL to access the REST API page in the format https://<hostname>/docs/api/

For more information about the APIs, see the *Active IQ Unified Manager API Developer's Guide*.

Active IQ Unified Manager API Developer's Guide

## Enabling API Gateway

The API Gateway feature allows Active IQ Unified Manager to be a single control plane from which you can manage multiple ONTAP clusters, without logging in to them individually.

You can enable this feature from the configuration pages that appear when you first log in to Unified Manager. Alternatively, you can enable or disable this feature from **General** > **Feature Settings** > **API Gateway**.

Unified Manager REST APIs are different from the ONTAP REST APIs, and not all the functionalities of ONTAP REST APIs can be availed by using the Unified Manager REST APIs. However, if you have a specific business requirement of accessing the ONTAP APIs for managing specific features that are not exposed to Unified Manager, you can enable the API Gateway feature and execute the ONTAP APIs. The gateway acts as a proxy to tunnel the API requests by maintaining the header and body requests in the same format as in the ONTAP APIs. You can use your Unified Manager credentials and execute the specific APIs to access and manage the ONTAP clusters without passing individual cluster credentials. Unified Manager performs as a single point of management for running the APIs across the ONTAP clusters managed by your Unified Manager instance. The response returned by the APIs is the same as the response returned by the respective ONTAP REST APIs executed directly from ONTAP.

After enabling this feature, you can execute the Unified Manager REST APIs from **Menu Bar** > **Help button** >

**API Documentation** > **gateway** category. Alternatively, you can enter the host name or IP address and the URL to access the REST API page in the format `https://<hostname>/docs/api/`

For more information about the APIs, see the *Active IQ Unified Manager API Developer's Guide*.

## Specifying inactivity timeout

You can specify the inactivity timeout value for Active IQ Unified Manager. After an inactivity of the specified time, the application is automatically logged out. This option is enabled by default.

You can deactivate this feature or modify the time from **General** > **Feature Settings** > **Inactivity Timeout**. Once you activate this feature, you should specify the time limit of inactivity (in minutes) in the **LOGOUT AFTER** field, after which the system automatically logs out. The default value is 4320 minutes (72 hours).

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

## Enabling Active IQ portal events

You can specify whether you want to enable or disable Active IQ portal events. This setting allows the Active IQ portal to discover and display additional events about system configuration, cabling, and so forth. This option is enabled by default.

On enabling this feature, Active IQ Unified Manager displays events discovered by the Active IQ portal. These events are created by running a set of rules against AutoSupport messages generated from all monitored storage systems. These events are different from the other Unified Manager events, and they identify incidents or risks related to system configuration, cabling, best practice, and availability issues.

You can choose to activate or deactivate this feature from **General** > **Feature Settings** > **Active IQ Portal Events**. In sites with no external network access, you must upload the rules manually from **Storage Management** > **Event Setup** > **Upload Rules**.

This feature is enabled by default. Disabling this feature stops the Active IQ events from being discovered or displayed on Unified Manager. When disabled, enabling this feature allows Unified Manager to receive the Active IQ events on a cluster at a predefined time of 00:15 for that cluster timezone.

## Enabling and disabling security settings for compliance

By using the **Customize** button on the **Security Dashboard** panel of the Features Settings page, you can enable or disable the security parameters for compliance monitoring on Unified Manager.

The settings that are enabled or disabled from this page govern the overall compliance status of the clusters and storage VMs on Unified Manager. Based on the selections, the corresponding columns are visible in the **Security: All Clusters** view of the Clusters inventory page and the **Security: All Storage VMs** view of the Storage VMs inventory page.

Only users with administrator role can edit these settings.

The security criteria for your ONTAP clusters, storage VMs, and volumes are evaluated against the

recommendations defined in the Security Hardening Guide for NetApp ONTAP 9. The Security panel on the dashboard and the Security page display the default security compliance status of your clusters, storage VMs, and volumes. Security events are also generated and management actions enabled for the clusters and storage VMs that have security violations.

### Customizing security settings

To customize the settings for compliance monitoring as applicable to your ONTAP environment, follow these steps:

#### Steps

1. Click **General > Feature Settings > Security Dashboard > Customize**. The **Customize Security Dashboard Settings** pop-up appears.

   The security compliance parameters that you enable or disable can directly affect the default security views, reports, and scheduled reports on the Clusters and Storage VMs screens. If you had uploaded an excel report from these screens before modifying the security parameters, the downloaded excel reports might be faulty.

2. To enable or disable the custom settings for your ONTAP clusters, select the required general setting under **Cluster**. For information on the options for customizing cluster compliance, see Cluster compliance categories
3. To enable or disable the custom settings for your storage VMs, select the required general setting under **Storage VM**. For information on the options for customizing storage VM compliance, see Storage VM compliance categories.

### Customizing AutoSupport and authentication settings

On the **AutoSupport Settings** section, you can specify whether HTTPS transport is to be used for sending AutoSupport messages from ONTAP.

From the **Authentication Settings** section, you can enable Unified Manager alerts to be raised for the default ONTAP administrator user.

## Enabling and disabling scripts upload

The ability to upload scripts to Unified Manager and run them is enabled by default. If your organization does not want to allow this activity because of security reasons, you can disable this functionality.

### What you'll need

You must have the Application Administrator role.

#### Steps

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

| If you want to… | Then do this… |
| --- | --- |
| Disable scripts | In the **Script Upload** panel, move the slider button to the left. |
| Enable scripts | In the **Script Upload** panel, move the slider button to the right. |

### Adding login banner

Adding a login banner enables your organization to display any information, such as, who is permitted access to the system and the terms and conditions of use during login and logout.

Any user, such as storage operators or administrators can view this login banner pop-up during login, logout, and session timeout.

# Using the maintenance console

You can use the maintenance console to configure network settings, to configure and manage the system on which Unified Manager is installed, and to perform other maintenance tasks that help you prevent and troubleshoot possible issues.

### What functionality the maintenance console provides

The Unified Manager maintenance console enables you to maintain the settings on your Unified Manager system and to make any necessary changes to prevent issues from occurring.

Depending on the operating system on which you have installed Unified Manager, the maintenance console provides the following functions:

- Troubleshoot any issues with your virtual appliance, especially if the Unified Manager web interface is not available
- Upgrade to newer versions of Unified Manager
- Generate support bundles to send to technical support
- Configure network settings
- Change the maintenance user password
- Connect to an external data provider to send performance statistics
- Change the performance data collection internal
- Restore the Unified Manager database and configuration settings from a previously backed up version.

### What the maintenance user does

The maintenance user is created during the installation of Unified Manager on a Red Hat Enterprise Linux or CentOS system. The maintenance user name is the “umadmin” user.

The maintenance user has the Application Administrator role in the web UI, and that user can create subsequent users and assign them roles.

The maintenance user, or umadmin user, can also access the Unified Manager maintenance console.

## Diagnostic user capabilities

The purpose of diagnostic access is to enable technical support to assist you in troubleshooting, and you should only use it when directed by technical support.

The diagnostic user can execute OS-level commands when directed by technical support, for troubleshooting purposes.

## Accessing the maintenance console

If the Unified Manager user interface is not in operation, or if you need to perform functions that are not available in the user interface, you can access the maintenance console to manage your Unified Manager system.

**What you'll need**

You must have installed and configured Unified Manager.

After 15 minutes of inactivity, the maintenance console logs you out.

When installed on VMware, if you have already logged in as the maintenance user through the VMware console, you cannot simultaneously log in using Secure Shell.

**Step**

1. Follow these steps to access the maintenance console:

| On this operating system… | Follow these steps… |
| --- | --- |
| VMware | a. Using Secure Shell, connect to the IP address or fully qualified domain name of the Unified Manager virtual appliance.<br>b. Log in to the maintenance console using your maintenance user name and password. |
| Linux | a. Using Secure Shell, connect to the IP address or fully qualified domain name of the Unified Manager system.<br>b. Log in to the system with the maintenance user (umadmin) name and password.<br>c. Enter the command `maintenance_console` and press Enter. |

| On this operating system… | Follow these steps… |
| --- | --- |
| Windows | a. Log in to the Unified Manager system with administrator credentials.<br>b. Launch PowerShell as a Windows administrator.<br>c. Enter the command `maintenance_console` and press Enter. |

The Unified Manager maintenance console menu is displayed.

## Accessing the maintenance console using the vSphere VM console

If the Unified Manager user interface is not in operation, or if you need to perform functions that are not available in the user interface, you can access the maintenance console to reconfigure your virtual appliance.

**What you'll need**

- You must be the maintenance user.
- The virtual appliance must be powered on to access the maintenance console.

**Steps**

1. In vSphere Client, locate the Unified Manager virtual appliance.
2. Click the **Console** tab.
3. Click inside the console window to log in.
4. Log in to the maintenance console using your user name and password.

   After 15 minutes of inactivity, the maintenance console logs you out.

## Maintenance console menus

The maintenance console consists of different menus that enable you to maintain and manage special features and configuration settings of the Unified Manager server.

Depending on the operating system on which you have installed Unified Manager, the maintenance console consists of the following menus:

- Upgrade Unified Manager (VMware only)
- Network Configuration (VMware only)
- System Configuration (VMware only)
- Support/ Diagnostics
- Reset Server Certificate
- External Data Provider
- Performance Polling Interval Configuration

### Network Configuration menu

The Network Configuration menu enables you to manage the network settings. You should use this menu when the Unified Manager user interface is not available.

> This menu is not available if Unified Manager is installed on Red Hat Enterprise Linux, CentOS, or on Microsoft Windows.

The following menu choices are available.

- **Display IP Address Settings**

  Displays the current network settings for the virtual appliance, including the IP address, network, broadcast address, netmask, gateway, and DNS servers.

- **Change IP Address Settings**

  Enables you to change any of the network settings for the virtual appliance, including the IP address, netmask, gateway, or DNS servers. If you switch your network settings from DHCP to static networking using the maintenance console, you cannot edit the host name. You must select **Commit Changes** for the changes to take place.

- **Display Domain Name Search Settings**

  Displays the domain name search list used for resolving host names.

- **Change Domain Name Search Settings**

  Enables you to change the domain names for which you want to search when resolving host names. You must select **Commit Changes** for the changes to take place.

- **Display Static Routes**

  Displays the current static network routes.

- **Change Static Routes**

  Enables you to add or delete static network routes. You must select **Commit Changes** for the changes to take place.

  - **Add Route**

    Enables you to add a static route.

  - **Delete Route**

    Enables you to delete a static route.

  - **Back**

    Takes you back to the **Main Menu**.

  - **Exit**

    Exits the maintenance console.

- **Disable Network Interface**

  Disables any available network interfaces. If only one network interface is available, you cannot disable it. You must select **Commit Changes** for the changes to take place.

- **Enable Network Interface**

  Enables available network interfaces. You must select **Commit Changes** for the changes to take place.

- **Commit Changes**

  Applies any changes made to the network settings for the virtual appliance. You must select this option to enact any changes made, or the changes do not occur.

- **Ping a Host**

  Pings a target host to confirm IP address changes or DNS configurations.

- **Restore to Default Settings**

  Resets all settings to the factory default. You must select **Commit Changes** for the changes to take place.

- **Back**

  Takes you back to the **Main Menu**.

- **Exit**

  Exits the maintenance console.

#### System Configuration menu

The System Configuration menu enables you to manage your virtual appliance by providing various options, such as viewing the server status, and rebooting and shutting down the virtual machine.

When Unified Manager is installed on a Linux or Microsoft Windows system, only the “Restore from a Unified Manager Backup” option is available from this menu.

The following menu choices are available:

- **Display Server Status**

  Displays the current server status. Status options include Running and Not Running.

  If the server is not running, you might need to contact technical support.

- **Reboot Virtual Machine**

  Reboots the virtual machine, stopping all services. After rebooting, the virtual machine and services restart.

- **Shut Down Virtual Machine**

  Shuts down the virtual machine, stopping all services.

You can select this option only from the virtual machine console.

- **Change <logged in user> User Password**

  Changes the password of the user that is currently logged in, which can only be the maintenance user.

- **Increase Data Disk Size**

  Increases the size of the data disk (disk 3) in the virtual machine.

- **Increase Swap Disk Size**

  Increases the size of the swap disk (disk 2) in the virtual machine.

- **Change Time Zone**

  Changes the time zone to your location.

- **Change NTP Server**

  Changes the NTP Server settings, such as IP address or fully qualified domain name (FQDN).

- **Change NTP Service**

  Switches between the `ntp` and `systemd-timesyncd` services.

- **Restore from a Unified Manager Backup**

  Restores the Unified Manager database and configuration settings from a previously backed up version.

- **Reset Server Certificate**

  Resets the server security certificate.

- **Change hostname**

  Changes the name of the host on which the virtual appliance is installed.

- **Back**

  Exits the System Configuration menu and returns to the Main Menu.

- **Exit**

  Exits the maintenance console menu.

#### Support and Diagnostics menu

The Support and Diagnostics menu enables you to generate a support bundle that you can send to technical support for troubleshooting assistance.

The following menu options are available:

- **Generate Light Support Bundle**

Enables you to produce a lightweight support bundle that contains just 30 days of logs and configuration database records — it excludes performance data, acquisition recording files, and server heap dump.

- **Generate Support Bundle**

  Enables you to create a full support bundle (7-Zip file) containing diagnostic information in the diagnostic user's home directory. If your system is connected to the internet you can also upload the support bundle to NetApp.

  The file includes information generated by an AutoSupport message, the contents of the Unified Manager database, detailed data about the Unified Manager server internals, and verbose-level logs not normally included in AutoSupport messages or in the lightweight support bundle.

#### Additional menu options

The following menu options enable you to perform various administrative tasks on the Unified Manager server.

The following menu choices are available:

- **Reset Server Certificate**

  Regenerates the HTTPS server certificate.

  You can regenerate the server certificate in the Unified Manager GUI by clicking **General** > **HTTPS Certificates** > **Regenerate HTTPS Certificate**.

- **Disable SAML authentication**

  Disables SAML authentication so that the identity provider (IdP) no longer provides sign-on authentication for users accessing the Unified Manager GUI. This console option is typically used when an issue with the IdP server or SAML configuration blocks users from accessing the Unified Manager GUI.

- **External Data Provider**

  Provides options for connecting Unified Manager to an external data provider. After you establish the connection, performance data is sent to an external server so that storage performance experts can chart the performance metrics using third-party software. The following options are displayed:

  - **Display Server Configuration**--Displays the current connection and configuration settings for an external data provider.
  - **Add / Modify Server Connection**--Enables you to enter new connection settings for an external data provider, or change existing settings.
  - **Modify Server Configuration**--Enables you to enter new configuration settings for an external data provider, or change existing settings.
  - **Delete Server Connection**--Deletes the connection to an external data provider.

    After the connection is deleted, Unified Manager loses its connection to the external server.

- **Performance Polling Interval Configuration**

  Provides an option for configuring how frequently Unified Manager collects performance statistical data from clusters. The default collection interval is 5 minutes.

You can change this interval to 10 or 15 minutes if you find that collections from large clusters are not completing on time.

- **View/Change Application Ports**

  Provides an option to change the default ports that Unified Manager uses for HTTP and HTTPS protocols, if required for security. The default ports are 80 for HTTP and 443 for HTTPS.

- **Exit**

  Exits the maintenance console menu.

## Changing the maintenance user password on Windows

You can change the Unified Manager maintenance user password when required.

**Steps**

1. From the Unified Manager web UI login page, click **Forgot Password**.

   A page is displayed that prompts for the name of the user whose password you want to reset.

2. Enter the user name and click **Submit**.

   An email with a link to reset the password is sent to the email address that is defined for that user name.

3. Click the **reset password link** in the email and define the new password.
4. Return to the web UI and log in to Unified Manager using the new password.

## Changing the umadmin password on Linux systems

For security reasons, you must change the default password for the Unified Manager umadmin user immediately after completing the installation process. If necessary, you can change the password again anytime later.

**What you'll need**

- Unified Manager must be installed on a Red Hat Enterprise Linux or CentOS Linux system.
- You must have the root user credentials for the Linux system on which Unified Manager is installed.

**Steps**

1. Log in as the root user to the Linux system on which Unified Manager is running.
2. Change the umadmin password:

   ```
   passwd umadmin
   ```

   The system prompts you to enter a new password for the umadmin user.

## Changing the ports Unified Manager uses for HTTP and HTTPS protocols

The default ports that Unified Manager uses for HTTP and HTTPS protocols can be

changed after installation if required for security. The default ports are 80 for HTTP and 443 for HTTPS.

**What you'll need**

You must have a user ID and password authorized to log in to the maintenance console of the Unified Manager server.

> There are some ports that are considered unsafe when using the Mozilla Firefox or Google Chrome browsers. Check with your browser before assigning a new port number for HTTP and HTTPS traffic. Selecting an unsafe port could make the system inaccessible, which would require that you contact customer support for a resolution.

The instance of Unified Manager is restarted automatically after you change the port, so make sure this is a good time to take the system down for a short amount of time.

1. Log in using SSH as the maintenance user to the Unified Manager host.

   The Unified Managermaintenance console prompts are displayed.

2. Type the number of the menu option labeled **View/Change Application Ports**, and then press Enter.
3. If prompted, enter the maintenance user password again.
4. Type the new port numbers for the HTTP and HTTPS ports, and then press Enter.

   Leaving a port number blank assigns the default port for the protocol.

   You are prompted whether you want to change the ports and restart Unified Manager now.

5. Type **y** to change the ports and restart Unified Manager.
6. Exit out of the maintenance console.

After this change, users must include the new port number in the URL to access the Unified Manager web UI, for example https://host.company.com:1234, https://12.13.14.15:1122, or https://[2001:db8:0:1]:2123.

## Adding network interfaces

You can add new network interfaces if you need to separate network traffic.

**What you'll need**

You must have added the network interface to the virtual appliance using vSphere.

The virtual appliance must be powered on.

> You cannot perform this operation if Unified Manager is installed on Red Hat Enterprise Linux or on Microsoft Windows.

**Steps**

1. In the vSphere console Main Menu, select **System Configuration** > **Reboot Operating System**.

   After rebooting, the maintenance console can detect the newly added network interface.

2. Access the maintenance console.
3. Select **Network Configuration** > **Enable Network Interface**.
4. Select the new network interface and press **Enter**.

   Select **eth1** and press **Enter**.

5. Type **y** to enable the network interface.
6. Enter the network settings.

   You are prompted to enter the network settings if using a static interface, or if DHCP is not detected.

   After entering the network settings, you automatically return to the **Network Configuration** menu.

7. Select **Commit Changes**.

   You must commit the changes to add the network interface.

## Adding disk space to the Unified Manager database directory

The Unified Manager database directory contains all of the health and performance data collected from ONTAP systems. Some circumstances may require that you increase the size of the database directory.

For example, the database directory may get full if Unified Manager is collecting data from a large number of clusters where each cluster has many nodes. You will receive a warning event when the database directory is 90% full, and a critical event when the directory is 95% full.

No additional data is collected from clusters after the directory reaches 95% full.

The steps required to add capacity to the data directory are different depending on whether Unified Manager is running on a VMware ESXi server, on a Red Hat or CentOS Linux server, or on a Microsoft Windows server.

### Adding space to the data directory of the Linux host

If you allotted insufficient disk space to the `/opt/netapp/data` directory to support Unified Manager when you originally set up the Linux host and then installed Unified Manager, you can add disk space after installation by increasing disk space on the `/opt/netapp/data` directory.

#### What you'll need

You must have root user access to the Red Hat Enterprise Linux or CentOS Linux machine on which Unified Manager is installed.

We recommend that you back up the Unified Manager database before increasing the size of the data directory.

#### Steps

1. Log in as root user to the Linux machine on which you want to add disk space.
2. Stop the Unified Manager service and the associated MySQL software in the order shown:

```
systemctl stop ocieau ocie mysqld
```

3. Create a temporary backup folder (for example, `/backup-data`) with sufficient disk space to contain the data in the current `/opt/netapp/data` directory.
4. Copy the content and privilege configuration of the existing `/opt/netapp/data` directory to the backup data directory:

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. If SE Linux is enabled:
   a. Get the SE Linux type for folders on existing `/opt/netapp/data` folder:

      ```
      se_type= `ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      The system returns a confirmation similar to the following:

      ```
      echo $se_type
      mysqld_db_t
      ```

   b. Run the chcon command to set the SE Linux type for the backup directory:

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. Remove the contents of the `/opt/netapp/data` directory:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Expand the size of the `/opt/netapp/data` directory to a minimum of 150 GB through LVM commands or by adding extra disks.

   > If you have created `/opt/netapp/data` from a disk, then you should not try to mount `/opt/netapp/data` as an NFS or CIFS share. Because, in this case, if you try to expand the disk space, some LVM commands, such as `resize` and `extend` might not work as expected.

8. Confirm that the `/opt/netapp/data` directory owner (mysql) and group (root) are unchanged:

   ```
   ls -ltr /opt/netapp/ | grep data
   ```

   The system returns a confirmation similar to the following:

   ```
   drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
   ```

9. If SE Linux is enabled, confirm that the context for the `/opt/netapp/data` directory is still set to mysqld_db_t:
   a. `touch /opt/netapp/data/abc`

b. `ls -Z /opt/netapp/data/abc`

   The system returns a confirmation similar to the following:

   ```
   -rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
   /opt/netapp/data/abc
   ```

10. Delete the file abc so that this extraneous file does not cause a database error in the future.
11. Copy the contents from backup-data back to the expanded `/opt/netapp/data` directory:

    ```
    cp -arp /backup-data/* /opt/netapp/data/
    ```

12. If SE Linux is enabled, run the following command:

    ```
    chcon -R --type=mysqld_db_t /opt/netapp/data
    ```

13. Start the MySQL service:

    ```
    systemctl start mysqld
    ```

14. After the MySQL service is started, start the ocie and ocieau services in the order shown:

    ```
    systemctl start ocie ocieau
    ```

15. After all of the services are started, delete the backup folder `/backup-data`:

    ```
    rm -rf /backup-data
    ```

#### Adding space to the data disk of the VMware virtual machine

If you need to increase the amount of space on the data disk for the Unified Manager database, you can add capacity after installation by increasing disk space using the Unified Manager maintenance console.

**What you'll need**

- You must have access to the vSphere Client.
- The virtual machine must have no snapshots stored locally.
- You must have the maintenance user credentials.

We recommend that you back up your virtual machine before increasing the size of virtual disks.

**Steps**

1. In the vSphere client, select the Unified Manager virtual machine, and then add more disk capacity to data `disk 3`. See the VMware documentation for details.

   In some rare cases the Unified Manager deployment uses "Hard Disk 2" for the data disk instead of "Hard Disk 3". If this has occurred in your deployment, increase the space of whichever disk is larger. The data disk will always have more space than the other disk.

2. In the vSphere client, select the Unified Manager virtual machine, and then select the **Console** tab.
3. Click in the console window, and then log in to the maintenance console using your user name and password.
4. In the Main Menu, enter the number for the **System Configuration** option.
5. In the System Configuration Menu, enter the number for the **Increase Data Disk Size** option.

#### Adding space to the logical drive of the Microsoft Windows server

If you need to increase the amount of disk space for the Unified Manager database, you can add capacity to the logical drive on which Unified Manager is installed.

#### What you'll need

You must have Windows administrator privileges.

We recommend that you back up the Unified Manager database before adding disk space.

#### Steps

1. Log in as administrator to the Windows server on which you want to add disk space.
2. Follow the step that corresponds to method you want to use to add more space:

| Option | Description |
|---|---|
| On a physical server, add capacity to the logical drive on which the Unified Manager server is installed. | Follow the steps in the Microsoft topic:<br><br>Extend a Basic Volume |
| On a physical server, add a hard disk drive. | Follow the steps in the Microsoft topic:<br><br>Adding Hard Disk Drives |
| On a virtual machine, increase the size of a disk partition. | Follow the steps in the VMware topic:<br><br>Increasing the size of a disk partition |

# Managing user access

You can create roles and assign capabilities to control user access to selected cluster objects. You can identify users who have the required capabilities to access selected objects within a cluster. Only these users are provided access to manage the cluster objects.

## Adding users

You can add local users or database users by using the Users page. You can also add remote users or groups that belong to an authentication server. You can assign roles to these users and, based on the privileges of the roles, users can manage the storage

objects and data with Unified Manager, or view the data in a database.

**What you'll need**

- You must have the Application Administrator role.
- To add a remote user or group, you must have enabled remote authentication and configured your authentication server.
- If you plan to configure SAML authentication so that an identity provider (IdP) authenticates users accessing the graphical interface, make sure these users are defined as "remote" users.

  Access to the UI is not allowed for users of type "local" or "maintenance" when SAML authentication is enabled.

If you add a group from Windows Active Directory, then all direct members and nested subgroups can authenticate to Unified Manager, unless nested subgroups are disabled. If you add a group from OpenLDAP or other authentication services, then only the direct members of that group can authenticate to Unified Manager.

**Steps**

1. In the left navigation pane, click **General** > **Users**.
2. On the Users page, click **Add**.
3. In the Add User dialog box, select the type of user that you want to add, and enter the required information.

   When entering the required user information, you must specify an email address that is unique to that user. You must avoid specifying email addresses that are shared by multiple users.

4. Click **Add**.

**Creating a database user**

To support a connection between Workflow Automation and Unified Manager, or to access database views, you must first create a database user with the Integration Schema or Report Schema role in the Unified Manager web UI.

**What you'll need**

You must have the Application Administrator role.

Database users provide integration with Workflow Automation and access to report-specific database views. Database users do not have access to the Unified Manager web UI or the maintenance console, and cannot execute API calls.

**Steps**

1. In the left navigation pane, click **General** > **Users**.
2. In the Users page, click **Add**.
3. In the Add User dialog box, select **Database User** in the **Type** drop-down list.
4. Type a name and password for the database user.
5. In the **Role** drop-down list, select the appropriate role.

| If you are… | Choose this role |
| --- | --- |
| Connecting Unified Manager with Workflow Automation | Integration Schema |
| Accessing reporting and other database views | Report Schema |

6. Click **Add**.

## Editing the user settings

You can edit user settings—such as the email address and role—that are specified each user. For example, you might want to change the role of a user who is a storage operator, and assign storage administrator privileges to the user.

**What you'll need**

You must have the Application Administrator role.

When you modify the role that is assigned to a user, the changes are applied when either of the following actions occur:

- The user logs out and logs back in to Unified Manager.
- Session timeout of 24 hours is reached.

**Steps**

1. In the left navigation pane, click **General** > **Users**.
2. In the Users page, select the user for which you want to edit settings, and click **Edit**.
3. In the Edit User dialog box, edit the appropriate settings that are specified for the user.
4. Click **Save**.

## Viewing users

You can use the Users page to view the list of users who manage storage objects and data using Unified Manager. You can view details about the users, such as the user name, type of user, email address, and the role that is assigned to the users.

**What you'll need**

You must have the Application Administrator role.

**Step**

1. In the left navigation pane, click **General** > **Users**.

## Deleting users or groups

You can delete one or more users from the management server database to prevent specific users from accessing Unified Manager. You can also delete groups so that all the

users in the group can no longer access the management server.

**What you'll need**

- When you are deleting remote groups, you must have reassigned the events that are assigned to the users of the remote groups.

  If you are deleting local users or remote users, the events that are assigned to these users are automatically unassigned.

- You must have the Application Administrator role.

**Steps**

1. In the left navigation pane, click **General** > **Users**.
2. In the Users page, select the users or groups that you want to delete, and then click **Delete**.
3. Click **Yes** to confirm the deletion.

## What RBAC is

RBAC (role-based access control) provides the ability to control who has access to various features and resources in the Active IQ Unified Manager server.

## What role-based access control does

Role-based access control (RBAC) enables administrators to manage groups of users by defining roles. If you need to restrict access for specific functionality to selected administrators, you must set up administrator accounts for them. If you want to restrict the information that administrators can view and the operations they can perform, you must apply roles to the administrator accounts you create.

The management server uses RBAC for user login and role permissions. If you have not changed the management server's default settings for administrative user access, you do not need to log in to view them.

When you initiate an operation that requires specific privileges, the management server prompts you to log in. For example, to create administrator accounts, you must log in with Application Administrator account access.

## Definitions of user types

A user type specifies the kind of account the user holds and includes remote users, remote groups, local users, database users, and maintenance users. Each of these types has its own role, which is assigned by a user with the role of Administrator.

Unified Manager user types are as follows:

- **Maintenance user**

  Created during the initial configuration of Unified Manager. The maintenance user then creates additional users and assigns roles. The maintenance user is also the only user with access to the maintenance console. When Unified Manager is installed on a Red Hat Enterprise Linux or CentOS system, the maintenance user is given the user name "umadmin."

- **Local user**

  Accesses the Unified Manager UI and performs functions based on the role given by the maintenance user or a user with the Application Administrator role.

- **Remote group**

  A group of users that access the Unified Manager UI using the credentials stored on the authentication server. The name of this account should match the name of a group stored on the authentication server. All users within the remote group are given access to the Unified Manager UI using their individual user credentials. Remote groups can perform functions according to their assigned roles.

- **Remote user**

  Accesses the Unified Manager UI using the credentials stored on the authentication server. A remote user performs functions based on the role given by the maintenance user or a user with the Application Administrator role.

- **Database user**

  Has read-only access to data in the Unified Manager database, has no access to the Unified Manager web interface or the maintenance console, and cannot execute API calls.

## Definitions of user roles

The maintenance user or Application Administrator assigns a role to every user. Each role contains certain privileges. The scope of activities that you can perform in Unified Manager depends on the role you are assigned and which privileges the role contains.

Unified Manager includes the following predefined user roles:

- **Operator**

  Views storage system information and other data collected by Unified Manager, including histories and capacity trends. This role enables the storage operator to view, assign, acknowledge, resolve, and add notes for the events.

- **Storage Administrator**

  Configures storage management operations within Unified Manager. This role enables the storage administrator to configure thresholds and to create alerts and other storage management-specific options and policies.

- **Application Administrator**

  Configures settings unrelated to storage management. This role enables the management of users, security certificates, database access, and administrative options, including authentication, SMTP, networking, and AutoSupport.

  When Unified Manager is installed on Linux systems, the initial user with the Application Administrator role is automatically named “umadmin”.

- **Integration Schema**

This role enables read-only access to Unified Manager database views for integrating Unified Manager with OnCommand Workflow Automation (WFA).

- **Report Schema**

  This role enables read-only access to reporting and other database views directly from the Unified Manager database. The databases that can be viewed include:

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

## Unified Manager user roles and capabilities

Based on your assigned user role, you can determine which operations you can perform in Unified Manager.

The following table displays the functions that each user role can perform:

| Function | Operator | Storage Administrator | Application Administrator | Integration Schema | Report Schema |
|---|---|---|---|---|---|
| View storage system information | • | • | • | • | • |
| View other data, such as histories and capacity trends | • | • | • | • | • |
| View, assign, and resolve events | • | • | • | | |
| View storage service objects, such as SVM associations and resource pools | • | • | • | | |
| View threshold policies | • | • | • | | |

| Function | Operator | Storage Administrator | Application Administrator | Integration Schema | Report Schema |
|---|---|---|---|---|---|
| Manage storage service objects, such as SVM associations and resource pools | | • | • | | |
| Define alerts | | • | • | | |
| Manage storage management options | | • | • | | |
| Manage storage management policies | | • | • | | |
| Manage users | | | • | | |
| Manage administrative options | | | • | | |
| Define threshold policies | | | • | | |
| Manage database access | | | • | | |
| Manage integration with WFA and provide access to the database views | | | | • | |
| Schedule and save reports | | • | • | | |
| Execute “Fix It” operations from Management Actions | | • | • | | |
| Provide read-only access to database views | | | | | • |

# Managing SAML authentication settings

After you have configured remote authentication settings, you can enable Security Assertion Markup Language (SAML) authentication so that remote users are authenticated by a secure identity provider (IdP) before they can access the Unified Manager web UI.

Note that only remote users will have access to the Unified Manager graphical user interface after SAML authentication has been enabled. Local users and Maintenance users will not be able to access the UI. This configuration does not impact users who access the maintenance console.

## Identity provider requirements

When configuring Unified Manager to use an identity provider (IdP) to perform SAML authentication for all remote users, you need to be aware of some required configuration settings so that the connection to Unified Manager is successful.

You must enter the Unified Manager URI and metadata into the IdP server. You can copy this information from the Unified ManagerSAML Authentication page. Unified Manager is considered the service provider (SP) in the Security Assertion Markup Language (SAML) standard.

### Supported encryption standards

- Advanced Encryption Standard (AES): AES-128 and AES-256
- Secure Hash Algorithm (SHA): SHA-1 and SHA-256

### Validated identity providers

- Shibboleth
- Active Directory Federation Services (ADFS)

### ADFS configuration requirements

- You must define three claim rules in the following order that are required for Unified Manager to parse ADFS SAML responses for this relying party trust entry.

| Claim rule | Value |
| --- | --- |
| SAM-account-name | Name ID |
| SAM-account-name | urn:oid:0.9.2342.19200300.100.1.1 |
| Token groups — Unqualified Name | urn:oid:1.3.6.1.4.1.5923.1.5.1.1 |

- You must set the authentication method to “Forms Authentication” or users may receive an error when logging out of Unified Manager . Follow these steps:
  a. Open the ADFS Management Console.
  b. Click on the Authentication Policies folder on the left tree view.

c. Under Actions on the right, click Edit Global Primary Authentication Policy.

d. Set the Intranet Authentication Method to “Forms Authentication” instead of the default “Windows Authentication”.

- In some cases login through the IdP is rejected when the Unified Manager security certificate is CA-signed. There are two workarounds to resolve this issue:
  - Follow the instructions identified in the link to disable the revocation check on the ADFS server for chained CA cert associated relying party:

    Disable Revocation Check per Relying Party Trust

  - Have the CA server reside within the ADFS server to sign the Unified Manager server cert request.

**Other configuration requirements**

- The Unified Manager clock skew is set to 5 minutes, so the time difference between the IdP server and the Unified Manager server cannot be more than 5 minutes or authentication will fail.

## Enabling SAML authentication

You can enable Security Assertion Markup Language (SAML) authentication so that remote users are authenticated by a secure identity provider (IdP) before they can access the Unified Manager web UI.

**What you’ll need**

- You must have configured remote authentication and verified that it is successful.
- You must have created at least one Remote User, or a Remote Group, with the Application Administrator role.
- The Identity provider (IdP) must be supported by Unified Manager and it must be configured.
- You must have the IdP URL and metadata.
- You must have access to the IdP server.

After you have enabled SAML authentication from Unified Manager, users cannot access the graphical user interface until the IdP has been configured with the Unified Manager server host information. So you must be prepared to complete both parts of the connection before starting the configuration process. The IdP can be configured before or after configuring Unified Manager.

Only remote users will have access to the Unified Manager graphical user interface after SAML authentication has been enabled. Local users and Maintenance users will not be able to access the UI. This configuration does not impact users who access the maintenance console, the Unified Manager commands, or ZAPIs.

Unified Manager is restarted automatically after you complete the SAML configuration on this page.

**Steps**

1. In the left navigation pane, click **General** > **SAML Authentication**.
2. Select the **Enable SAML authentication** checkbox.

   The fields required to configure the IdP connection are displayed.

3. Enter the IdP URI and the IdP metadata required to connect the Unified Manager server to the IdP server.

   If the IdP server is accessible directly from the Unified Manager server, you can click the **Fetch IdP Metadata** button after entering the IdP URI to populate the IdP Metadata field automatically.

4. Copy the Unified Manager host metadata URI, or save the host metadata to an XML text file.

   You can configure the IdP server with this information at this time.

5. Click **Save**.

   A message box displays to confirm that you want to complete the configuration and restart Unified Manager.

6. Click **Confirm and Logout** and Unified Manager is restarted.

The next time authorized remote users attempt to access the Unified Manager graphical interface they will enter their credentials in the IdP login page instead of the Unified Manager login page.

If not already completed, access your IdP and enter the Unified Manager server URI and metadata to complete the configuration.

> When using ADFS as your identity provider, the Unified Manager GUI does not honor the ADFS timeout and will continue to work until the Unified Manager session timeout is reached. You can change the GUI session timeout by clicking **General** > **Feature Settings** > **Inactivity Timeout**.

## Changing the identity provider used for SAML authentication

You can change the identity provider (IdP) that Unified Manager uses to authenticate remote users.

### What you'll need

- You must have the IdP URL and metadata.
- You must have access to the IdP.

The new IdP can be configured before or after configuring Unified Manager.

### Steps

1. In the left navigation pane, click **General** > **SAML Authentication**.
2. Enter the new IdP URI and the IdP metadata required to connect the Unified Manager server to the IdP.

   If the IdP is accessible directly from the Unified Manager server, you can click the **Fetch IdP Metadata** button after entering the IdP URL to populate the IdP Metadata field automatically.

3. Copy the Unified Manager metadata URI, or save the metadata to an XML text file.
4. Click **Save Configuration**.

   A message box displays to confirm that you want to change the configuration.

5. Click **OK**.

Access the new IdP and enter the Unified Manager server URI and metadata to complete the configuration.

The next time authorized remote users attempt to access the Unified Manager graphical interface they will enter their credentials in the new IdP login page instead of the old IdP login page.

## Updating SAML authentication settings after Unified Manager security certificate change

Any change to the HTTPS security certificate installed on the Unified Manager server requires that you update the SAML authentication configuration settings. The certificate is updated if you rename the host system, assign a new IP address for the host system, or manually change the security certificate for the system.

After the security certificate is changed and the Unified Manager server is restarted, SAML authentication will not function and users will not be able to access the Unified Manager graphical interface. You must update the SAML authentication settings on both the IdP server and on the Unified Manager server to re-enable access to the user interface.

**Steps**

1. Log into the maintenance console.
2. In the **Main Menu**, enter the number for the **Disable SAML authentication** option.

   A message displays to confirm that you want to disable SAML authentication and restart Unified Manager.
3. Launch the Unified Manager user interface using the updated FQDN or IP address, accept the updated server certificate into your browser, and log in using the maintenance user credentials.
4. In the **Setup/Authentication** page, select the **SAML Authentication** tab and configure the IdP connection.
5. Copy the Unified Manager host metadata URI, or save the host metadata to an XML text file.
6. Click **Save**.

   A message box displays to confirm that you want to complete the configuration and restart Unified Manager.
7. Click **Confirm and Logout** and Unified Manager is restarted.
8. Access your IdP server and enter the Unified Manager server URI and metadata to complete the configuration.

| Identity provider | Configuration steps |
| --- | --- |
| ADFS | a. Delete the existing relying party trust entry in the ADFS management GUI.<br>b. Add a new relying party trust entry using the `saml_sp_metadata.xml` from the updated Unified Manager server.<br>c. Define the three claim rules that are required for Unified Manager to parse ADFS SAML responses for this relying party trust entry.<br>d. Restart the ADFS Windows service. |

| Identity provider | Configuration steps |
| --- | --- |
| Shibboleth | a. Update the new FQDN of Unified Manager server into the `attribute-filter.xml` and `relying-party.xml` files.<br>b. Restart the Apache Tomcat web server and wait for port 8005 to come online. |

9. Log in to Unified Manager and verify that SAML authentication works as expected through your IdP.

## Disabling SAML authentication

You can disable SAML authentication when you want to stop authenticating remote users through a secure identity provider (IdP) before they can log into the Unified Manager web UI. When SAML authentication is disabled, the configured directory service providers, such as Active Directory or LDAP, perform sign-on authentication.

After you disable SAML authentication, Local users and Maintenance users will be able to access the graphical user interface in addition to configured Remote users.

You can also disable SAML authentication using the Unified Manager maintenance console if you do not have access to the graphical user interface.

Unified Manager is restarted automatically after SAML authentication is disabled.

**Steps**

1. In the left navigation pane, click **General** > **SAML Authentication**.
2. Uncheck the **Enable SAML authentication** checkbox.
3. Click **Save**.

   A message box displays to confirm that you want to complete the configuration and restart Unified Manager.

4. Click **Confirm and Logout** and Unified Manager is restarted.

The next time remote users attempt to access the Unified Manager graphical interface they will enter their credentials in the Unified Manager login page instead of the IdP login page.

Access your IdP and delete the Unified Manager server URI and metadata.

## Disabling SAML authentication from the maintenance console

You may need to disable SAML authentication from the maintenance console when there is no access to the Unified Manager GUI. This could happen in cases of misconfiguration or if the IdP is not accessible.

**What you'll need**

You must have access to the maintenance console as the maintenance user.

When SAML authentication is disabled, the configured directory service providers, such as Active Directory or LDAP, perform sign-on authentication. Local users and Maintenance users will be able to access the graphical user interface in addition to configured Remote users.

You can also disable SAML authentication from the Setup/Authentication page in the UI.

Unified Manager is restarted automatically after SAML authentication is disabled.

**Steps**

1. Log into the maintenance console.
2. In the **Main Menu**, enter the number for the **Disable SAML authentication** option.

   A message displays to confirm that you want to disable SAML authentication and restart Unified Manager.

3. Type **y**, and then press Enter and Unified Manager is restarted.

The next time remote users attempt to access the Unified Manager graphical interface they will enter their credentials in the Unified Manager login page instead of the IdP login page.

If required, access your IdP and delete the Unified Manager server URL and metadata.

## SAML Authentication page

You can use the SAML Authentication page to configure Unified Manager to authenticate remote users using SAML though a secure identity provider (IdP) before they can to log in to the Unified Manager web UI.

- You must have the Application Administrator role to create or modify the SAML configuration.
- You must have configured remote authentication.
- You must have configured at least one remote user or remote group.

After remote authentication and remote users have been configured, you can select the Enable SAML authentication checkbox to enable authentication using a secure identity provider.

- **IdP URI**

  The URI to access the IdP from the Unified Manager server. Example URIs are listed below.

  ADFS example URI:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Shibboleth example URI:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **IdP Metadata**

  The IdP metadata in XML format.

  If the IdP URL is accessible from the Unified Manager server, you can click the **Fetch IdP Metadata** button

to populate this field.

- **Host System (FQDN)**

  The FQDN of the Unified Manager host system as defined during installation. You can change this value if necessary.

- **Host URI**

  The URI to access the Unified Manager host system from the IdP.

- **Host Metadata**

  The host system metadata in XML format.

# Managing authentication

You can enable authentication using either LDAP or Active Directory on the Unified Manager server and configure it to work with your servers to authenticate remote users.

For enabling remote authentication, setting up authentication services, and adding authentication severs, see the previous section on **Configuring Unified Manager to send alert notifications**.

## Editing authentication servers

You can change the port that the Unified Manager server uses to communicate with your authentication server.

#### What you'll need

You must have the Application Administrator role.

#### Steps

1. In the left navigation pane, click **General** > **Remote Authentication**.
2. Check the **Disable Nested Group Lookup** box.
3. In the **Authentication Servers** area, select the authentication server that you want to edit, and then click **Edit**.
4. In the **Edit Authentication Server** dialog box, edit the port details.
5. Click **Save**.

## Deleting authentication servers

You can delete an authentication server if you want to prevent the Unified Manager server from communicating with the authentication server. For example, if you want to change an authentication server that the management server is communicating with, you can delete the authentication server and add a new authentication server.

#### What you'll need

You must have the Application Administrator role.

When you delete an authentication server, remote users or groups of the authentication server will no longer be able to access Unified Manager.

**Steps**

1. In the left navigation pane, click **General** > **Remote Authentication**.
2. Select one or more authentication servers that you want to delete, and then click **Delete**.
3. Click **Yes** to confirm the delete request.

   If the **Use Secure Connection** option is enabled, then the certificates associated with the authentication server are deleted along with the authentication server.

## Authentication with Active Directory or OpenLDAP

You can enable remote authentication on the management server and configure the management server to communicate with your authentication servers so that users within the authentication servers can access Unified Manager.

You can use one of the following predefined authentication services or specify your own authentication service:

- Microsoft Active Directory

  You cannot use Microsoft Lightweight Directory Services.

- OpenLDAP

You can select the required authentication service and add the appropriate authentication servers to enable the remote users in the authentication server to access Unified Manager. The credentials for remote users or groups are maintained by the authentication server. The management server uses the Lightweight Directory Access Protocol (LDAP) to authenticate remote users within the configured authentication server.

For local users who are created in Unified Manager, the management server maintains its own database of user names and passwords. The management server performs the authentication and does not use Active Directory or OpenLDAP for authentication.

## Audit Logging

You can detect whether the audit logs have been compromised with using Audit Logs. All the activities performed by a user are monitored and logged in the Audit Logs. The audits are performed for all user interface and publicly exposed APIs' functionalities of Active IQ Unified Manager.

You can use the Audit Log: File View to view and access all the audit log files available in your Active IQ Unified Manager. The files in the Audit Log: File View are listed based on their creation date. This view displays information of all the audit log that are captured from the installation or upgrade to the present in the system. Whenever you perform an action in Unified Manager, the information is updated and is available in the logs. The status of each log file is captured using the "File Integrity Status" attribute which gets actively monitored to detect tampering or deletion of the log file. The audit logs can have one of the following states when the audit logs are available in the system:

| State | Description |
| --- | --- |
| ACTIVE | File in which logs are being currently logged. |
| NORMAL | File which is inactive, compressed and stored in the system. |
| TAMPERED | File which has been compromised by a user who has manually edited the file. |
| MANUAL_DELETE | File which got deleted by an authorized user. |
| ROLLOVER_DELETE | File which got deleted due to Rolling off based on Rolling Configuration Policy. |
| UNEXPECTED_DELETE | File which got deleted due to unknown reasons. |

The Audit Log page includes the following command buttons:

- Configure
- Delete
- Download

The **DELETE** button enables you to delete any of the audit logs listed in the Audit Logs view. You can delete an audit log and optionally provide a reason to delete the file which helps in future to determine a valid delete. The REASON column lists the reason along with the name of the user who performed the delete operation.

Deleting a log file will cause deletion of file from the system but the entry in the DB table will not be deleted.

You can download the audit logs from Active IQ Unified Manager using the **DOWNLOAD** button in the Audit Logs section and export the audit log files. The files that are marked “NORMAL” or “TAMPERED” are downloaded in a compressed `.gzip` format.

When a full Autosupport bundle is generated, the support bundle includes both archived and active audit log files. But when a light support bundle is generated, it includes only the active audit logs. The archived audit logs are not included.

#### Configuring audit logs

You can use the **Configure** button in the Audit Logs section to configure rolling policy for Audit Log files and to also enable remote logging for the Audit Logs.

You can set the values in the **MAX FILE SIZE** and **AUDIT LOG RETENTION DAYS** as per the desired amount and frequency of data that you want to store in the system. The value in the field **TOTAL AUDIT LOG SIZE** is the size of the total audit log data present in the system. The roll over policy is determined by the values in the field **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE**, and **TOTAL AUDIT LOG SIZE**. When the size of the audit log backup reaches the value configured in **TOTAL AUDIT LOG SIZE**, then the file that was archived first is deleted. This means that the oldest file is deleted. But the file entry continues to be available in the database and is marked as “Rollover Delete”. The **AUDIT LOG RETENTION DAYS** value is for the number of the days

the audit log files are preserved. Any file older than the value set in this field is rolled over.

**Steps**

1. Click **Audit Logs** > > **Configure**.
2. Enter values in the **MAX FILE SIZE**, **TOTAL AUDIT LOG SIZE**, and **AUDIT LOG RETENTION DAYS**.

   If you want to enable remote logging, then you should select the **Enable Remote Logging**.

### Enabling remote logging of audit logs

You can select the **Enable Remote Logging** checkbox on the Configure Audit Logs dialog box to enable remote audit logging. You can use this feature to transfer audit logs to a remote Syslog server. This will enable you to manage your audit logs when there are space constraints.

The remote logging of audit logs provides a tamper-proof backup in case the audit log files on the Active IQ Unified Manager server are tampered.

**Steps**

1. In the **Configure Audit Logs** dialog box, select the **Enable Remote Logging** checkbox.

   Additional fields to configure remote logging are displayed.

2. Enter the **HOSTNAME** and **PORT** of the remote server you want to connect to.
3. In the **SERVER CA CERTIFICATE** field, click **BROWSE** to select a public certificate of the target server.

   The certificate should be uploaded in `.pem` format. This certificate should be obtained from the target Syslog server and should not have expired. The certificate should contain the selected “hostname” as part of the `SubjectAltName` (SAN) attribute.

4. Enter the values for the following fields: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   The values should be in milliseconds for these fields.

5. Select the required Syslog format and TLS protocol version in the **FORMAT** and **PROTOCOL** fields.
6. Select the **Enable Client Authentication** checkbox if the target Syslog server requires certificate based authentication.

   You will need to download client authentication certificate and upload it to the Syslog server before saving the Audit Log configuration, otherwise the connection will fail. Depending on the type of Syslog server, you might need to create a hash of the client authentication certificate.

   Example: syslog-ng requires a <hash> of the certificate to be created using the command `openssl x509 -noout -hash -in cert.pem`, and then you should symbolically link the client authentication certificate to a file named after the <hash> .0.

7. Click **Save** to configure the connection with your server and enable remote logging.

   You will be redirected to the Audit Logs page.

## Remote Authentication page

You can use the Remote Authentication page to configure Unified Manager to communicate with your authentication server to authenticate remote users who attempt to log into the Unified Manager web UI.

You must have the Application Administrator or Storage Administrator role.

After you select the Enable remote authentication checkbox, you can enable remote authentication using an authentication server.

- **Authentication Service**

  Enables you to configure the management server to authenticate users in directory service providers, such as Active Directory, OpenLDAP, or specify your own authentication mechanism. You can specify an authentication service only if you have enabled remote authentication.

  - **Active Directory**
    - Administrator Name

      Specifies the administrator name of the authentication server.

    - Password

      Specifies the password to access the authentication server.

    - Base Distinguished Name

      Specifies the location of the remote users in 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**.

    - Disable Nested Group Lookup

      Specifies whether to enable or disable the nested group lookup option. By default this option is disabled. If you use Active Directory, you can speed up authentication by disabling support for nested groups.

    - Use Secure Connection

      Specifies the authentication service used for communicating with authentication servers.

  - **OpenLDAP**
    - Bind Distinguished Name

      Specifies the bind distinguished name that is used along with the base distinguished name to find remote users in the authentication server.

    - Bind Password

      Specifies the password to access the authentication server.

    - Base Distinguished Name

Specifies the location of the remote users in 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**.

- Use Secure Connection

  Specifies that Secure LDAP is used for communicating with LDAPS authentication servers.

- **Others**
  - Bind Distinguished Name

    Specifies the bind distinguished name that is used along with the base distinguished name to find remote users in the authentication server that you have configured.

  - Bind Password

    Specifies the password to access the authentication server.

  - Base Distinguished Name

    Specifies the location of the remote users in 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**.

  - Protocol Version

    Specifies the Lightweight Directory Access Protocol (LDAP) version that is supported by your authentication server. You can specify whether the protocol version must be automatically detected or set the version to 2 or 3.

  - User Name Attribute

    Specifies the name of the attribute in the authentication server that contains user login names to be authenticated by the management server.

  - Group Membership Attribute

    Specifies a value that assigns the management server group membership to remote users based on an attribute and value specified in the user’s authentication server.

  - UGID

    If the remote users are included as members of a GroupOfUniqueNames object in the authentication server, this option enables you to assign the management server group membership to the remote users based on a specified attribute in that GroupOfUniqueNames object.

  - Disable Nested Group Lookup

    Specifies whether to enable or disable the nested group lookup option. By default this option is disabled. If you use Active Directory, you can speed up authentication by disabling support for nested groups.

  - Member

    Specifies the attribute name that your authentication server uses to store information about the

individual members of a group.

- User Object Class

  Specifies the object class of a user in the remote authentication server.

- Group Object Class

  Specifies the object class of all groups in the remote authentication server.

- Use Secure Connection

  Specifies the authentication service used for communicating with authentication servers.

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

**Authentication Servers area**

The Authentication Servers area displays the authentication servers that the management server communicates with to find and authenticate remote users. The credentials for remote users or groups are maintained by the authentication server.

- **Command buttons**

  Enables you to add, edit, or delete authentication servers.

  - Add

    Enables you to add an authentication server.

    If the authentication server that you are adding is part of a high-availability 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.

  - Edit

    Enables you to edit the settings for a selected authentication server.

  - Delete

    Deletes the selected authentication servers.

- **Name or IP Address**

  Displays the host name or IP address of the authentication server that is used to authenticate the user on the management server.

- **Port**

  Displays the port number of the authentication server.

- **Test Authentication**

  This button validates the configuration of your authentication server by authenticating a remote user or

group.

While testing, if you specify only the user name, the management server searches for the remote user in the authentication server, but does not authenticate the user. If you specify both the user name and password, the management server searches and authenticates the remote user.

You cannot test the authentication if remote authentication is disabled.

# Managing security certificates

You can configure HTTPS in the Unified Manager server to monitor and manage your clusters over a secure connection.

## Viewing the HTTPS security certificate

You can compare the HTTPS certificate details to the retrieved certificate in your browser to ensure that your browser's encrypted connection to Unified Manager is not being intercepted.

**What you'll need**

You must have the Operator, Application Administrator, or Storage Administrator role.

Viewing the certificate enables you to verify the content of a regenerated certificate, or to view Subject Alt Names (SAN) from which you can access Unified Manager.

**Step**

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

   The HTTPS certificate is displayed at the top of the page

If you need to view more detailed information about the security certificate than what is displayed on the HTTPS Certificate page, you can view the connection certificate in your browser.

## Downloading an HTTPS certificate signing request

You can download a certification signing request for the current HTTPS security certificate so that you can provide the file to a Certificate Authority to sign. A CA-signed certificate helps prevent man-in-the-middle attacks and provides better security protection than a self-signed certificate.

**What you'll need**

You must have the Application Administrator role.

**Steps**

1. In the left navigation pane, click **General** > **HTTPS Certificate**.
2. Click **Download HTTPS Certificate Signing Request**.
3. Save the `<hostname>.csr` file.

You can provide the file to a Certificate Authority to sign, and then install the signed certificate.

## Installing a CA signed and returned HTTPS certificate

You can upload and install a security certificate after a Certificate Authority has signed and returned it. The file that you upload and install must be a signed version of the existing self-signed certificate. A CA-signed certificate helps prevent man-in-the middle attacks and provides better security protection than a self-signed certificate.

### What you'll need

You must have completed the following actions:

- Downloaded the Certificate Signing Request file and had it signed by a Certificate Authority
- Saved the certificate chain in PEM format
- Included all certificates in the chain, from the Unified Manager server certificate to the root signing certificate, including any intermediate certificates present

You must have the Application Administrator role.

If the validity of certificate for which a CSR was created is more than 397 days, then the validity will be reduced to 397 days by the CA before signing and returning the certificate

### Steps

1. In the left navigation pane, click **General** > **HTTPS Certificate**.
2. Click **Install HTTPS Certificate**.
3. In the dialog box that is displayed, click **Choose file…** to locate the file to upload.
4. Select the file, and then click **Install** to install the file.

Installing a HTTPS certificate generated using external tools

### Example certificate chain

The following example shows how the certificate chain file might appear:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

## Installing a HTTPS certificate generated using external tools

You can install certificates that are self signed or CA signed and are generated using an external tool like OpenSSL, BoringSSL, LetsEncrypt.

You should load the private key along with the certificate chain because these certificates are externally generated public-private key pair. The permitted key-pair algorithms are “RSA” and “EC”. The **Install HTTPS Certificate** option is available in the HTTPS Certificates page under the General section. The file you upload should be in the following input format.

1. Private Key of the server that belongs to the Active IQ UM host
2. Certificate of the server that matches with the private key
3. Certificate of the CAs in reverse till the root, which are used to sign the above certificate

#### Format for loading a certificate with an EC key pair

The permitted curves are “prime256v1” and “secp384r1”. Sample of certificate with an externally generated EC pair:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

**Format for loading a certificate with an RSA key pair**

The allowed key sizes for the RSA key-pair belonging to the host certificate are 2048, 3072, and 4096. certificate with an externally generated **RSA key pair**:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

After the certificate is uploaded, you should restart the Active IQ Unified Manager instance for the changes to take effect.

**Checks while uploading externally generated certificates**

The system performs checks while uploading a certificate generated using external tools. If any of the checks fail, then the certificate is rejected. There are also validation included for the certificates that are generated from the CSR within the product and for certificates that are generated using external tools.

- The private key in the input is validated against the host certificate in the input.
- The Common Name (CN) in the host certificate is checked against the FQDN of the host.

- The Common Name (CN) of the host certificate should not be empty or blank and should not be set to localhost.
- The validity start date should not be in future and the validity expiry date of the certificate should not be in the past.
- If Intermediate CA or CA exists the validity start date of certificate should not be in future and the validity expiry date should not be in the past.

The private key in the input should not be encrypted. If there are any private keys that are encrypted, then they are rejected by the system.

Example 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Example 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Example 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

## Page descriptions for certificate management

You can use the HTTPS Certificate page to view the current security certificates and to generate new HTTPS certificates.

#### HTTPS Certificate page

The HTTPS Certificate page enables you to view the current security certificate, download a certificate signing request, generate a new HTTPS certificate, or install a new HTTPS certificate.

If you have not generated a new HTTPS certificate, the certificate that appears on this page is the certificate that was generated during installation.

#### Command buttons

The command buttons enable you to perform the following operations:

- **Download HTTPS Certificate Signing Request**

  Downloads a certification request for the currently installed HTTPS certificate. Your browser prompts you to save the <hostname>.csr file so that you can provide the file to a Certificate Authority to sign.

- **Install HTTPS Certificate**

  Enables you to upload and install a security certificate after a Certificate Authority has signed and returned it. The new certificate is in effect after you restart the management server.

- **Regenerate HTTPS Certificate**

  Enables you to generate an HTTPS certificate, which replaces the current security certificate. The new certificate is in effect after you restart Unified Manager.

### Regenerate HTTPS Certificate dialog box

The Regenerate HTTPS Certificate dialog box enables you to customize the security information and then generate a new HTTPS certificate with that information.

The current certificate information appears on this page.

The “Regenerate Using Current Certificate Attributes” and “Update the Current Certificate Attributes” selection enables you to regenerate the certificate with the current information or generate a certificate with new information.

- **Common Name**

  Required. The fully qualified domain name (FQDN) that you wish to secure.

  In Unified Manager high availability configurations, use the virtual IP address.

- **Email**

  Optional. An email address to contact your organization; typically the email address of the certificate administrator or IT department.

- **Company**

  Optional. Typically the incorporated name of your company.

- **Department**

  Optional. The name of the department in your company.

- **City**

  Optional. The city location of your company.

- **State**

Optional. The state or province location, not abbreviated, of your company.

- **Country**

  Optional. The country location of your company. This is typically a two-letter ISO code of the country.

- **Alternative Names**

  Required. Additional, non-primary domain names that can be used to access this server in addition to the existing localhost or other network addresses. Separate each alternate name with a comma.

  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.

- **KEY SIZE (KEY ALGORITHM: RSA)**

  The key algorithm is set to RSA. You can select from one of the key sizes: 2048, 3072 or 4096 bits. The default key size is set to 2048 bits.

- **VALIDITY PERIOD**

  The default validity period is 397 days. If you have upgraded from a previous version, you might see the previous certificate validity unchanged.