Configure notifications

Active IQ Unified Manager

NetApp
September 26, 2026

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

Table of Contents

Configure notifications . . . 1
- Configure Active IQ Unified Manager to send alert notifications . . . 1
- Configure event notification settings in Active IQ Unified Manager . . . 1
- Enable remote authentication in Active IQ Unified Manager . . . 2
- Disable nested groups from remote authentication in Active IQ Unified Manager . . . 3
- Set up authentication services in Active IQ Unified Manager . . . 4
- Add authentication servers to Active IQ Unified Manager . . . 5
- Test the configuration of authentication servers in Active IQ Unified Manager . . . 6
- Add alerts in Active IQ Unified Manager . . . 7
  - Example of adding an alert . . . 8

Configure notifications

Configure Active IQ Unified Manager to send alert notifications

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

Before you begin

You must have the Application Administrator role.

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

Steps

1. Configure event notification settings.

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

2. Enable remote authentication.

   If you want remote LDAP or Active Directory users to access the Unified Manager instance and receive alert notifications, then you must enable remote authentication.

3. Add authentication servers.

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

4. Add users.

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

5. Add alerts.

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

Configure event notification settings in Active IQ Unified Manager

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

Before you begin

You must have the following information:

- Email address from which the alert notification is sent

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

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

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

You must have the Application Administrator or Storage Administrator role.

Steps

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

   Notes:

   - If the From Address is pre-filled with the address "ActiveIQUnifiedManager@localhost.com", you should change it to a real, working email address to make sure that all email notifications are delivered successfully.
   - If the host name of the SMTP server cannot be resolved, you can specify the IP address (IPv4 or IPv6) of the SMTP server instead of the host name.
3. Click **Save**.
4. If you have selected the **Use STARTTLS** or **Use SSL** option, a certificate page displays after you click the **Save** button. Verify the certificate details and accept the certificate to save the notification settings.

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

Enable remote authentication in Active IQ Unified Manager

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

Before you begin

You must have the Application Administrator role.

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

You can enable remote authentication using either Open LDAP or Active Directory. If remote authentication is

disabled, remote users cannot access Unified Manager.

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

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

Steps

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

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

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

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

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

Disable nested groups from remote authentication in Active IQ Unified Manager

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

Before you begin

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

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

Steps

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

Set up authentication services in Active IQ Unified Manager

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

Before you begin

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

Steps

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

If you select…	Then do this…
Active Directory	a. Enter the administrator name and password. b. Specify the base distinguished name of the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Enter the bind distinguished name and bind password. b. Specify the base distinguished name of the authentication server. For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is **cn=ou,dc=domain,dc=com**.

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

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

3. Click **Save**.

Add authentication servers to Active IQ Unified Manager

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

Before you begin

- The following information must be available:
  - Host name or IP address of the authentication server
  - Port number of the authentication server
- You must have enabled remote authentication and configured your authentication service so that the management server can authenticate remote users or groups in the authentication server.
- You must have the Application Administrator role.

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

Steps

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

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

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

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

Test the configuration of authentication servers in Active IQ Unified Manager

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

Before you begin

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

remote user or remote group from these servers and authenticate them.

- You must have the Application Administrator role.

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

Steps

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

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

Add alerts in Active IQ Unified Manager

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

Before you begin

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

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

Steps

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

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

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

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

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

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

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

   You can also choose to notify users through SNMP traps.

7. Click **Save**.

Example of adding an alert

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

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

Perform the following steps in the Add Alert dialog box:

Steps

1. Click **Name**, and enter **HealthTest** in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
   a. Enter **abc** in the **Name contains** field to display the volumes whose name contains “abc”.
   b. Select **<<All Volumes whose name contains 'abc'>>** from the Available Resources area, and move it to the Selected Resources area.
   c. Click **Exclude**, and enter **xyz** in the **Name contains** field, and then click **Add**.
3. Click **Events**, and select **Critical** from the Event Severity field.
4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.
5. Click **Actions**, and enter **sample@domain.com** in the Alert these users field.
6. Select **Remind every 15 minutes** to notify the user every 15 minutes.

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

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

Copyright information

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

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

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

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

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

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

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

Trademark information

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