Configure Console integrations and services

NetApp Console local deployment

NetApp
August 10, 2026

Table of Contents

Configure Console integrations and services

Integrate NetApp Console local deployment with Active Directory

Integrate NetApp Console local deployment with Active Directory for directory-backed sign-in and user lookup. Use your directory service to authenticate users, then assign access to those users in NetApp Console local deployment.

Required access roles

Super admin or Organization admin. Learn about access roles.

When you integrate with Active Directory, Console local deployment authenticates users through your existing directory. After you add a directory user, assign Console access roles to control what that user can access.

Active Directory integration also helps you meet compliance requirements by applying your existing controls, audit trails, and policies to Console local deployment access.

- Active Directory integration does not create federated groups, does not synchronize directory-group assignments, and does not automatically grant access. Administrators still add directory users to the organization and assign roles in Console local deployment.
- Only one Active Directory integration is supported at a time. Once an integration is configured, the **Add integration** button is disabled. To switch to a different directory, disable or delete the existing integration first.
- Directory users do not configure or use multi-factor authentication (MFA). Console local deployment supports MFA only for local users. Learn how to manage member security settings.

Before you begin

Before you integrate with Active Directory, confirm that you have:

- An Active Directory domain and credentials that can query the directory
- The LDAP server address and the base distinguished name (DN) for the directory tree
- Network access from Console local deployment to your LDAP server on port 389 (LDAP) or 636 (LDAPS)
- SSL/TLS certificates, if you plan to use LDAPS

Steps

1. Select **Administration > Identity and access**.
2. Select **Directory services** to open the Federations page.
3. Select **Add integration**.
4. Enter the connection details for your Active Directory server:
   - A descriptive name for the integration.
   - The **LDAP host**: hostname or IP address of your LDAP server. For multiple servers, enter the primary.
   - The port: 389 for LDAP or 636 for LDAPS.

- The **Connection timeout** in milliseconds. The default is 1000 ms.

5. Select **Use SSL/TLS** to use LDAPS. Confirm that your LDAP server supports LDAPS and that the Console can access the required certificates.
6. Test the connection. If it fails, check the LDAP host, port, network connectivity, and SSL/TLS certificates.
7. After the test succeeds, enter the directory and user details:
   - **Base DN binding**: Enter the Bind DN for the LDAP/AD account this app will use to connect to the directory, and enter the Bind credential (password) for that account. Console uses these details to bind to LDAP and validate the connection.
   - **User DN**: a user account with permission to query the directory. For example, `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`.
8. Select **Add** to save the integration.

After you finish

After you save the integration, add directory users to your organization and assign roles. You must configure and enable at least one Active Directory integration before you can add directory users. Learn how to add directory users and assign roles.

Disable or enable an Active Directory integration

Disable an integration to temporarily suspend directory-backed authentication without deleting the configuration. When you disable a directory service, directory users cannot sign in through the directory.

Steps

1. Select **Administration > Identity and access**.
2. Select **Directory services** to open the Federations page.
3. In the integrations list, locate the integration and select the action menu for that row.
4. Select **Disable** to suspend the integration, or **Enable** to restore it.

Delete an Active Directory integration

Delete an integration to permanently remove the directory service configuration. Before deleting, review any warnings about directory users that are linked to the integration, as their access will be affected.

Steps

1. Select **Administration > Identity and access**.
2. Select **Directory services** to open the Federations page.
3. In the integrations list, locate the integration and select the action menu for that row.
4. Select **Delete** and confirm the deletion.

Connect your LLM and enable the NetApp Console assistant in NetApp Console local deployment

Connect your large language model (LLM) to NetApp Console local deployment to enable the Console assistant and AI-assisted storage management.

This documentation regarding connecting an LLM to the Console assistant to enable AI features is provided as a technology preview. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability.

Required access roles

Super admin or Organization admin. Learn about access roles.

After setup, users open the Console assistant from the dashboard and choose an access mode:

- In **Read only** mode, the assistant answers questions and provides guidance without making changes.
- In **Read/write** mode, the assistant can act on storage infrastructure. It shows details for review and confirmation before each change. For asynchronous operations, such as volume creation, it creates a job that users can check from the assistant.

To connect your LLM, select a provider path, enter endpoint details and API key, and then select a model in **Administration > AI Tools**. Assistant actions stay within your storage policies and role-based access controls.

Gather what you need before you connect an LLM

Before you connect your LLM, gather the following:

- Your provider type decision: OpenAI or OpenAI-compatible. Learn about provider choices.
- A valid API key for the provider path you select.
- The endpoint URL for your provider path.
- Your proxy or gateway URL, if your organization requires one.
- Your user name or single sign-on (SSO) ID for the LLM provider account, if required.
- Network access from Console local deployment to the selected endpoint.
- Storage classes and role-based access controls for the assistant actions you plan to allow.

For supported model details, see Learn about supported LLM providers and models in NetApp Console local deployment.

Connect an LLM to NetApp Console local deployment

Enter provider settings, API key, and model to connect your LLM to Console local deployment.

Steps

1. Log in to the NetApp Console local deployment.
2. Select **Administration > AI Tools**.
3. Select the menu, and then select **Edit**.
4. In **Provider type**, select a provider type.

   Learn about LLM integration in NetApp Console local deployment.

5. If prompted for a provider endpoint, enter the endpoint URL for the provider path you selected.
6. Enter the proxy or gateway URL and credentials.
7. In the **User name** field, enter your user name or SSO ID if your provider path requires it.

8. In the **API key** field, paste the API key from your selected provider path.
9. Select a model from the list.
10. Review the configuration, and then select **Save**.

    If save or test fails, verify the provider type, endpoint URL, API key, and selected model, and then try again.

Troubleshoot your LLM integration.

Verify that LLM integration works

After you save the configuration, verify assistant availability and behavior.

Steps

1. Confirm that the **Console assistant** button appears on the NetApp Console local deployment dashboard.
2. Open the assistant in **Read only** mode and run a basic query.
3. Open the assistant in **Read/write** mode and confirm that storage-changing actions require user confirmation before execution.
4. Verify that the users who need action workflows have the required role-based access controls.

After you complete validation, users can open the Console assistant from the dashboard and describe tasks in plain language. For usage examples and end-user workflows, see Use the NetApp Console assistant.

Protect credentials and monitor LLM usage

- Use a dedicated API key for Console local deployment integration when possible.
- Rotate API keys according to your organization policy.
- Restrict who can edit AI Tools settings to required admin roles only.
- Monitor provider-side API usage and alerts to track abnormal activity or cost spikes.

Troubleshoot LLM integration in NetApp Console local deployment

Use this quick triage flow to diagnose and resolve common LLM integration issues in NetApp Console local deployment.

> This documentation regarding connecting an LLM to the Console assistant to enable AI features is provided as a technology preview. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability.

If you have not completed setup, see Connect your LLM and enable the NetApp Console assistant.

Triage LLM integration issues quickly

1. Validate AI Tools configuration in **Administration > AI Tools**.

   Confirm provider type, endpoint URL, API key, selected model, and outbound network access.

2. Validate assistant availability on the dashboard.

   Confirm the **Console assistant** button appears for expected users and organizations.

3. Validate runtime behavior.

   Run a simple read-only request and confirm provider endpoint reachability, model availability, and provider service health.

Troubleshoot by symptom

Symptom	Likely cause	What to check	Next action
Save or test fails in AI Tools	Configuration or connectivity mismatch	Provider type, endpoint URL, API key format, selected model, and outbound access	Correct the value that fails validation and save again
Console assistant button is missing	Unhealthy integration status, org mismatch, or RBAC mismatch	Successful AI Tools save, integration status, current organization, and expected access role	Refresh the session and verify with a known-good admin account
Assistant opens but request fails	Provider or runtime path issue	Endpoint reachability, model availability on that endpoint, provider limits, and temporary provider status	Retry after fixing endpoint/model mismatch or provider-side limit issues
Assistant response is slow or inconsistent	Prompt size, endpoint performance, or network/proxy instability	Short prompt test, provider service health, and network/proxy stability	Use a shorter prompt, try another supported model, and stabilize network or proxy routing

Respond to LLM credential exposure or misuse

If you suspect API key exposure or unauthorized use:

1. Revoke the existing API key in your provider system.
2. Create a new API key.
3. Update the key in **Administration > AI Tools**.
4. Verify successful reconnection with a read-only assistant test.

Set up notification delivery channels in NetApp Console local deployment

In NetApp Console local deployment, you can set up multiple channels for alert notifications, including email and webhooks.

Required access roles

Super admin or Organization admin. Learn about access roles.

By default, Console local deployment displays notifications through its built-in notification system. Configuring additional delivery channels lets you receive notifications in the way that best fits your workflow.

You can send all notifications through the same channels or use different channels for different notification types. For example, you might send urgent storage alerts through email while routing other alert traffic to a third-party monitoring tool through a webhook.

After you set up notification delivery channels, you can configure notification rules and assign them to different channels. Learn how to configure notification rules.

Configure an email server

When you configure an email server, Console local deployment sends notifications, alerts, and user invitations through it. Console local deployment supports SMTP email servers, which can be your existing corporate email server or a third-party email service.

Steps

1. Select **Administration > Console**.
2. Select **Configuration** to open the System configurations page.
3. In the **Email server** section, select **Configure**.
4. Enter the connection details for your email server:
   - Add a sender name and a sender email address.
   - The **SMTP host**: hostname or IP address of your SMTP server. For multiple servers, enter the primary.
   - Select the connection protocol from the **Connection security** dropdown list. The port is configured for you and is read-only: 25 for SMTP with STARTTLS, or 465 for SMTPS.

     SMTPS (port 465) establishes an encrypted connection immediately and is recommended for security-sensitive environments. STARTTLS (port 25) upgrades from an unencrypted connection and may fall back to unencrypted transmission if the encryption negotiation fails.
5. Select **Test email** to send a test email to a recipient you specify.
6. After the test succeeds, select **Save** to save the configuration.

   If the test fails, re-verify the settings you entered and double-check that Console local deployment has network access to the email server.

Update an email server configuration

You can update an existing email server configuration if you want to use a different email server.

Steps

1. Select **Administration > Console**.
2. Select **Configuration** to open the System configurations page.
3. In the **Email server** section, select **Configure**.
4. Select **Clear fields** to clear the existing configuration.
5. Enter the new connection details for your email server.
6. Select **Test email** to send a test email to a recipient you specify.

7. After the test succeeds, select **Save** to save the new configuration.

   If the test fails, re-verify the settings you entered and double-check that Console local deployment has network access to the email server.

Remove an email server configuration

You can remove the email server configuration if you no longer want Console local deployment to send emails.

Steps

1. Select **Administration > Console**.
2. Select **Configuration** to open the Systems configuration page.
3. In the **Email server** section, select **Configure**.
4. Select **Clear fields** to clear the existing configuration.
5. Select **Save** to save the cleared configuration, which removes the email server configuration from Console local deployment.

Configure a webhook

Set up webhooks to send notifications from Console local deployment to other tools or services. You can configure multiple webhooks, each pointing to a different endpoint. For example, one for a SIEM and another for an on-call paging service.

After you create a webhook, users with the Storage admin role can assign it to specific alert rules. For example, they can send critical alerts to email while sending all alerts to a third-party monitoring tool through a webhook.

Console local deployment does not enforce access control on webhook endpoints. Any user or system that can reach the endpoint URL receives the alert data. Ensure that access to the receiving application is restricted to authorized users through that application's own access controls.

Before you begin

Confirm that Console local deployment can reach the receiving application over the network, and gather the endpoint URL, HTTP method, and any authentication or certificate details required by that application.

Steps

1. Select **Administration > Console**.
2. Select **Configuration** to open the System configurations page.
3. In the **Webhook integration** section, select **Configure**.
4. Enter the required details for the webhook:
   - A descriptive name for the webhook.
   - The Endpoint URL provided by the receiving application.
   - HTTP method
   - Optional: A self-signed certificate in PEM format.
   - Any required headers or secrets (authentication credentials).

- The format to use when sending the webhook. JSON and OTEL (OpenTelemetry) are supported.

  Use JSON for general-purpose webhooks and custom REST endpoints. Use OTEL for observability platforms that natively consume OpenTelemetry signals, such as Grafana or other OpenTelemetry-compatible collectors.

5. Select **Test webhook** to test the webhook connection and ensure that Console local deployment can successfully send messages to the receiving application.
6. After the test succeeds, select **Save** to create the webhook.

   After you save the webhook, it is available for users to select where webhooks are supported, such as Alert delivery options. Learn how to create alert rules and assign webhooks for alert delivery.

Copyright information

Trademark information