Manage your account

Astra Control Center

NetApp
August 11, 2025

Table of Contents

Manage your account

Manage local users and roles

You can add, remove, and edit users of your Astra Control Center installation using the Astra Control UI. You can use the Astra Control UI or the Astra Control API to manage users.

You can also use LDAP to perform authentication for selected users.

Use LDAP

LDAP is an industry standard protocol for accessing distributed directory information and a popular choice for enterprise authentication. You can connect Astra Control Center to an LDAP server to perform authentication for selected Astra Control users. At a high level, the configuration involves integrating Astra with LDAP and defining the Astra Control users and groups corresponding to the LDAP definitions. You can use the Astra Control API or web UI to configure LDAP authentication and LDAP users and groups. See the following documentation for more information:

- Use the Astra Control API to manage remote authentication and users
- Use the Astra Control UI to manage remote users and groups
- Use the Astra Control UI to manage remote authentication

Add users

Account Owners and Admins can add more users to the Astra Control Center installation.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.
2. Select the **Users** tab.
3. Select **Add User**.
4. Enter the user's name, email address, and a temporary password.

   The user will need to change the password upon first login.

5. Select a user role with the appropriate system permissions.

   Each role provides the following permissions:

   - A **Viewer** can view resources.
   - A **Member** has Viewer role permissions and can manage apps and clusters, unmanage apps, and delete snapshots and backups.
   - An **Admin** has Member role permissions and can add and remove any other users except the Owner.
   - An **Owner** has Admin role permissions and can add and remove any user accounts.

6. To add constraints to a user with a Member or Viewer role, enable the **Restrict role to constraints** check box.

   For more information on adding constraints, refer to Manage local users and roles.

7. Select **Add**.

Manage passwords

You can manage passwords for user accounts in Astra Control Center.

Change your password

You can change the password of your user account at any time.

Steps

1. Select the User icon at the top right of the screen.
2. Select **Profile**.
3. From the Options menu in the **Actions** column, and select **Change Password**.
4. Enter a password that conforms to the password requirements.
5. Enter the password again to confirm.
6. Select **Change password**.

Reset another user's password

If your account has Admin or Owner role permissions, you can reset passwords for other user accounts as well as your own. When you reset a password, you assign a temporary password that the user will have to change upon logging in.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.
2. Select the **Actions** drop-down list.
3. Select **Reset Password**.
4. Enter a temporary password that conforms to the password requirements.
5. Enter the password again to confirm.

   > ℹ️ The next time the user logs in, the user will be prompted to change the password.

6. Select **Reset password**.

Remove users

Users with the Owner or Admin role can remove other users from the account at any time.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.
2. In the **Users** tab, select the check box in the row of each user that you want to remove.
3. From the Options menu in the **Actions** column, select **Remove user/s**.
4. When you're prompted, confirm deletion by typing the word "remove" and then select **Yes, Remove User**.

Result

Astra Control Center removes the user from the account.

Manage roles

You can manage roles by adding namespace constraints and restricting user roles to those constraints. This enables you to control access to resources within your organization. You can use the Astra Control UI or the Astra Control API to manage roles.

Add a namespace constraint to a role

An Admin or Owner user can add namespace constraints to Member or Viewer roles.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.

2. Select the **Users** tab.

3. In the **Actions** column, select the menu button for a user with the Member or Viewer role.

4. Select **Edit role**.

5. Enable the **Restrict role to constraints** check box.

   The check box is only available for Member or Viewer roles. You can select a different role from the **Role** drop-down list.

6. Select **Add constraint**.

   You can view the list of available constraints by namespace or by namespace label.

7. In the **Constraint type** drop-down list, select either **Kubernetes namespace** or **Kubernetes namespace label** depending on how your namespaces are configured.

8. Select one or more namespaces or labels from the list to compose a constraint that restricts roles to those namespaces.

9. Select **Confirm**.

   The **Edit role** page displays the list of constraints you've chosen for this role.

10. Select **Confirm**.

    On the **Account** page, you can view the constraints for any Member or Viewer role in the **Role** column.

> If you enable constraints for a role and select **Confirm** without adding any constraints, the role is considered to have full restrictions (the role is denied access to any resources that are assigned to namespaces).

Remove a namespace constraint from a role

An Admin or Owner user can remove a namespace constraint from a role.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.

2. Select the **Users** tab.

3. In the **Actions** column, select the menu button for a user with the Member or Viewer role that has active constraints.

4. Select **Edit role**.

   The **Edit role** dialog displays the active constraints for the role.

5. Select the **X** to the right of the constraint you need to remove.

6. Select **Confirm**.

For more information

- User roles and namespaces

Manage remote authentication

LDAP is an industry standard protocol for accessing distributed directory information and a popular choice for enterprise authentication. You can connect Astra Control Center to an LDAP server to perform authentication for selected Astra Control users.

At a high level, the configuration involves integrating Astra with LDAP and defining the Astra Control users and groups corresponding to the LDAP definitions. You can use the Astra Control API or web UI to configure LDAP authentication and LDAP users and groups.

> ⓘ   Astra Control Center uses the email address in the LDAP "mail" attribute to search for and keep track of remote users. This attribute might be an optional or empty field in your directory. An email address must exist in this field for any remote users you wish to appear in Astra Control Center. This email address is used as the username in Astra Control Center for authentication.

Add a certificate for LDAPS authentication

Add the private TLS certificate for the LDAP server so that Astra Control Center can authenticate with the LDAP server when you use an LDAPS connection. You only need to do this once, or when the certificate you have installed expires.

Steps

1. Go to **Account**.

2. Select the **Certificates** tab.

3. Select **Add**.

4. Either upload the `.pem` file or paste the contents of the file from your clipboard.

5. Select the **Trusted** check box.

6. Select **Add certificate**.

Enable remote authentication

You can enable LDAP authentication and configure the connection between Astra Control and the remote LDAP server.

Before you begin

If you plan to use LDAPS, ensure that the private TLS certificate for the LDAP server is installed in Astra Control Center so that Astra Control Center can authenticate with the LDAP server. See Add a certificate for LDAPS authentication for instructions.

Steps

1. Go to **Account > Connections**.

2. In the **Remote Authentication** pane, select the configuration menu.

3. Select **Connect**.

4. Enter the server IP address, port, and preferred connection protocol (LDAP or LDAPS).

   (i) As a best practice, use LDAPS when connecting with the LDAP server. You need to install the LDAP server's private TLS certificate in Astra Control Center before you connect with LDAPS.

5. Enter the service account credentials in email format (administrator@example.com). Astra Control will use these credentials when connecting with the LDAP server.

6. In the **User Match** section, enter the base DN and an appropriate user search filter to use when retrieving user information from the LDAP server.

7. In the **Group Match** section, enter the group search base DN and an appropriate custom group search filter.

   (i) Be sure to use the correct base Distinguished Name (DN) and an appropriate search filter for **User Match** and **Group Match**. The base DN tells Astra Control at what level of the directory tree to start the search, and the search filter limits the parts of the directory tree Astra Control searches from.

8. Select **Submit**.

Result

The **Remote Authentication** pane status moves to **Pending**, and then to **Connected** when the connection to the LDAP server is established.

Disable remote authentication

You can temporarily disable an active connection to the LDAP server.

(i) When you disable a connection to an LDAP server, all settings are saved, and all remote users and groups that were added to Astra Control from that LDAP server are retained. You can reconnect to this LDAP server at any time.

Steps

1. Go to **Account > Connections**.

2. In the **Remote Authentication** pane, select the configuration menu.

3. Select **Disable**.

Result

The **Remote Authentication** pane status moves to **Disabled**. All remote authentication settings, remote users, and remote groups are preserved, and you can re-enable the connection at any time.

Edit remote authentication settings

If you have disabled the connection to the LDAP server or the **Remote Authentication** pane is in a

"Connection error" state, you can edit the configuration settings.

> ℹ️ You cannot edit the LDAP server URL or IP address when the **Remote Authentication** pane is in a "Disabled" state. You need to Disconnect remote authentication first.

Steps

1. Go to **Account > Connections**.

2. In the **Remote Authentication** pane, select the configuration menu.

3. Select **Edit**.

4. Make the necessary changes, and select **Edit**.

Disconnect remote authentication

You can disconnect from an LDAP server and remove the configuration settings from Astra Control.

> ⚠️ When you disconnect from the LDAP server, all configuration settings for that LDAP server are removed from Astra Control, as well as any remote users and groups that were added from that LDAP server.

Steps

1. Go to **Account > Connections**.

2. In the **Remote Authentication** pane, select the configuration menu.

3. Select **Disconnect**.

Result

The **Remote Authentication** pane status moves to **Disconnected**. Remote authentication settings, remote users, and remote groups are removed from Astra Control.

Manage remote users and groups

If you have enabled LDAP authentication on your Astra Control system, you can search for LDAP users and groups, and include them in the approved users of the system.

Add a remote user

Account Owners and Admins can add remote users to Astra Control.

> ℹ️ You cannot add remote user if a local user with the same email address already exists on the system. To add the user as a remote user, delete the local user from the system first.

> ℹ️ Astra Control Center uses the email address in the LDAP "mail" attribute to search for and keep track of remote users. This attribute might be an optional or empty field in your directory. An email address must exist in this field for any remote users you wish to appear in Astra Control Center. This email address is used as the username in Astra Control Center for authentication.

Steps

1. Go to the **Account** area.

2. Select the **Users & groups** tab.

3. At the far right of the page, select **Remote users**.

4. Select **Add**.

5. Optionally, search for an LDAP user by entering the user's email address in the **Filter by email** field.

6. Select one or more users from the list.

7. Assign a role to the user.

> ⓘ If you assign different roles to a user and the user's group, the more permissive role takes precedence.

8. Optionally, assign one or more namespace constraints to this user, and select **Restrict role to constraints** to enforce them. You can add a new namespace constraint by selecting **Add constraint**.

> ⓘ When a user is assigned multiple roles through LDAP group membership, the constraints in the most permissive role are the only ones that take effect. For example, if a user with a local Viewer role joins three groups that are bound to the Member role, the sum of the constraints from the Member roles take effect, and any constraints from the Viewer role are ignored.

9. Select **Add**.

Result

The new user appears in the list of remote users. In this list, you can see active constraints on the user as well as manage the user from the **Actions** menu.

Add a remote group

To add many remote users at once, account Owners and Admins can add remote groups to Astra Control. When you add a remote group, all remote users in that group are added to Astra Control and inherit the same role.

Steps

1. Go to the **Account** area.

2. Select the **Users & groups** tab.

3. At the far right of the page, select **Remote groups**.

4. Select **Add**.

   In this window, you can see a list of the common names and distinguished names of LDAP groups that Astra Control retrieved from the directory.

5. Optionally, search for an LDAP group by entering the group's common name in the **Filter by common name** field.

6. Select one or more groups from the list.

7. Assign a role to the groups.

> ⓘ The role you select is assigned to all users in this group. If you assign different roles to a user and the user's group, the more permissive role takes precedence.

8. Optionally, assign one or more namespace constraints to this group, and select **Restrict role to constraints** to enforce them. You can add a new namespace constraint by selecting **Add constraint**.

> ⓘ When a user is assigned multiple roles through LDAP group membership, the constraints in the most permissive role are the only ones that take effect. For example, if a user with a local Viewer role joins three groups that are bound to the Member role, the sum of the constraints from the Member roles take effect, and any constraints from the Viewer role are ignored.

9. Select **Add**.

Result

The new group appears in the list of remote groups, and all remote users in this group appear in the list of remote users. In this list, you can see details about the group as well as manage the group from the **Actions** menu.

View and manage notifications

Astra notifies you when actions have completed or failed. For example, you'll see a notification if a backup of an app completed successfully.

You can manage these notifications from the top right of the interface:

Steps

1. Select the number of unread notifications in the top right.

2. Review the notifications and then select **Mark as read** or **Show all notifications**.

   If you selected **Show all notifications**, the Notifications page loads.

3. On the **Notifications** page, view the notifications, select the ones that you want to mark as read, select **Action** and select **Mark as read**.

Add and remove credentials

Add and remove credentials for local private cloud providers such as ONTAP S3, Kubernetes clusters managed with OpenShift, or unmanaged Kubernetes clusters from your account at any time. Astra Control Center uses these credentials to discover Kubernetes clusters and the apps on the clusters, and to provision resources on your behalf.

Note that all users in Astra Control Center share the same sets of credentials.

Add credentials

You can add credentials to Astra Control Center when you manage clusters. To add credentials by adding a new cluster, refer to Add a Kubernetes cluster.

| | If you create your own `kubeconfig` file, you should define only **one** context element in it. See Kubernetes documentation for information about creating `kubeconfig` files. |

Remove credentials

Remove credentials from an account at any time. You should only remove credentials after unmanaging all associated clusters.

| | The first set of credentials that you add to Astra Control Center is always in use because Astra Control Center uses the credentials to authenticate to the backup bucket. It's best not to remove these credentials. |

Steps

1. Select **Account**.
2. Select the **Credentials** tab.
3. Select the Options menu in the **State** column for the credentials that you want to remove.
4. Select **Remove**.
5. Type the word "remove" to confirm deletion and then select **Yes, Remove Credential**.

Result

Astra Control Center removes the credentials from the account.

Monitor account activity

You can view details about the activities in your Astra Control account. For example, when new users were invited, when a cluster was added, or when a snapshot was taken. You also have the ability to export your account activity to a CSV file.

| | If you manage Kubernetes clusters from Astra Control and Astra Control is connected to Cloud Insights, Astra Control sends event logs to Cloud Insights. The log information, including information about pod deployment and PVC attachments, appears in the Astra Control Activity log. Use this information to identify any issues on the Kubernetes clusters you are managing. |

View all account activity in Astra Control

1. Select **Activity**.
2. Use the filters to narrow down the list of activities or use the search box to find exactly what you're looking for.
3. Select **Export to CSV** to download your account activity to a CSV file.

View account activity for a specific app

1. Select **Applications** and then select the name of an app.
2. Select **Activity**.

View account activity for clusters

1. Select **Clusters** and then select the name of the cluster.
2. Select **Activity**.

Take action to resolve events that require attention

1. Select **Activity**.

2. Select an event that requires attention.

3. Select the **Take action** drop-down option.

   From this list, you can view possible corrective actions that you can take, view documentation related to the issue, and get support to help resolve the issue.

Update an existing license

You can convert an evaluation license to a full license, or you can update an existing evaluation or full license with a new license. If you don't have a full license, work with your NetApp sales contact to obtain a full license and serial number. You can use the Astra Control Center UI or the Astra Control API to update an existing license.

Steps

1. Log in to the NetApp Support Site.

2. Access the Astra Control Center Download page, enter the serial number, and download the full NetApp license file (NLF).

3. Log in to the Astra Control Center UI.

4. From the left navigation, select **Account** > **License**.

5. In the **Account** > **License** page, select the status drop-down menu for the existing license and select **Replace**.

6. Browse to the license file that you downloaded.

7. Select **Add**.

The **Account** > **Licenses** page displays the license information, expiration date, license serial number, account ID, and CPU units used.

For more information

- Astra Control Center licensing