Manage your account

Astra Control Center

NetApp
August 30, 2022

Table of Contents

Manage your account . . . 1
- Manage users . . . 1
- Manage roles . . . 3
- View and manage notifications . . . 5
- Add and remove credentials . . . 5
- Monitor account activity . . . 6
- Update an existing license . . . 7
- Manage repository connections . . . 7
- Manage software packages . . . 9

Manage your account

Manage users

You can invite, 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 users. At a high level, the configuration involves integrating Astra with LDAP and defining the Astra users and groups corresponding to the LDAP definitions. See LDAP authentication for more information.

Invite users

Account Owners and Admins can invite new users to Astra Control Center.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.
2. Select the **Users** tab.
3. Select **Invite User**.
4. Enter the user's name and email address.
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, see Manage roles.
7. Select **Invite users**.

   The user receives an email informing them that they've been invited to Astra Control Center. The email includes temporary password, which they'll need to change upon first login.

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, see Manage 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.

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

6. Select **Reset password**.

Change a user's role

Users with the Owner role can change the role of all users, while users with the Admin role can change the role of users who have the Admin, Member, or Viewer role.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.
2. Select the **Actions** drop-down list.
3. Select **Edit role**.
4. Select a new role.
5. To apply constraints to the role, enable the **Restrict role to constraints** check box and select a constraint from the list.

   If there are no constraints, you can add a constraint. For more information, see Manage roles.

6. Select **Confirm**.

Result

Astra Control Center updates the user's permissions based on the new role that you selected.

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.

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

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, see 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 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

Manage repository connections

You can connect repositories to Astra Control to use as a reference for software package installation images and artifacts. When you import software packages, Astra Control references installation images in the image repository and binaries and other artifacts in the artifact repository.

What you'll need

- Kubernetes cluster with Astra Control Center installed
- A running Docker repository that you can access
- A running artifact repository (such as Artifactory) that you can access

Connect a Docker image repository

You can connect a Docker image repository to hold package installation images, such as those for Astra Data Store. When you install packages, Astra Control imports the package image files from the image repository.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.
2. Select the **Connections** tab.
3. In the **Docker Image Repository** section, select the menu at the top right.
4. Select **Connect**.
5. Add the URL and port for the repository.

6. Enter the credentials for the repository.
7. Select **Connect**.

Result

The repository is connected. In the **Docker Image Repository** section, the repository should show a connected status.

Disconnect a Docker image repository

You can remove the connection to a Docker image repository if it is no longer needed.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.
2. Select the **Connections** tab.
3. In the **Docker Image Repository** section, select the menu at the top right.
4. Select **Disconnect**.
5. Select **Yes, disconnect Docker image repository**.

Result

The repository is disconnected. In the **Docker Image Repository** section, the repository should show a disconnected status.

Connect an artifact repository

You can connect an artifact repository to host artifacts such as software package binaries. When you install packages, Astra Control imports the artifacts for the software packages from the image repository.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.
2. Select the **Connections** tab.
3. In the **Artifact Repository** section, select the menu at the top right.
4. Select **Connect**.
5. Add the URL and port for the repository.
6. If authentication is required, enable the **Use authentication** check box and enter the credentials for the repository.
7. Select **Connect**.

Result

The repository is connected. In the **Artifact Repository** section, the repository should show a connected status.

Disconnect an artifact repository

You can remove the connection to an artifact repository if it is no longer needed.

Steps

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

2. Select the **Connections** tab.
3. In the **Artifact Repository** section, select the menu at the top right.
4. Select **Disconnect**.
5. Select **Yes, disconnect artifact repository**.

Result

The repository is disconnected. In the **Artifact Repository** section, the repository should show a connected status.

Find more information

- Manage software packages

Manage software packages

NetApp delivers additional capabilities for Astra Control Center with software packages that you can download from the NetApp Support Site. After you connect Docker and artifact repositories, you can upload and import packages to add this functionality to Astra Control Center. You can use the CLI or the Astra Control Center web UI to manage software packages.

What you'll need

- Kubernetes cluster with Astra Control Center installed
- A connected Docker image repository to hold software package images. For more information, see Manage repository connections.
- A connected artifact repository to hold software package binaries and artifacts. For more information, see Manage repository connections.
- A software package from the NetApp Support Site

Upload software package images to the repositories

Astra Control Center references package images and artifacts in connected repositories. You can upload images and artifacts to the repositories using the CLI.

Steps

1. Download the software package from the NetApp Support Site, and save it on a machine that has the `kubectl` utility installed.
2. Extract the compressed package file, and change directory to the location of the Astra Control bundle file (for example, `acc.manifest.bundle.yaml`).
3. Push the package images to the Docker repository. Make the following substitutions:
   - Replace BUNDLE_FILE with the name of the Astra Control bundle file (for example, `acc.manifest.bundle.yaml`).
   - Replace MY_REGISTRY with the URL of the Docker repository.
   - Replace MY_REGISTRY_USER and MY_REGISTRY_PASSWORD with the credentials for the repository.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY -u
MY_REGISTRY_USER -p MY_REGISTRY_PASSWORD
```

4. If the package has artifacts, copy the artifacts to the artifact repository. Replace BUNDLE_FILE with the name of the Astra Control bundle file, and NETWORK_LOCATION with the network location to copy the artifact files to:

```
kubectl astra packages copy-artifacts -m BUNDLE_FILE -n NETWORK_LOCATION
```

Add a software package

You can import software packages using an Astra Control Center bundle file. Doing this installs the package and makes the software available for Astra Control Center to use.

Add a software package using the Astra Control web UI

You can use the Astra Control Center web UI to add a software package that has been uploaded to the connected repositories.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.
2. Select the **Packages** tab.
3. Select the **Add** button.
4. In the file selection dialog, select the upload icon.
5. Choose an Astra Control bundle file, in `.yaml` format, to upload.
6. Select **Add**.

Result

If the bundle file is valid and the package images and artifacts are located in your connected repositories, the package is added to Astra Control Center. When the status in the **Status** column changes to **Available**, you can use the package. You can hover over the status for a package to get more information.

If one or more images or artifacts for a package are not found in your repository, an error message appears for that package.

Add a software package using the CLI

You can use the CLI to import a software package that you have uploaded to the connected repositories. To do this, you first need to record your Astra Control Center account ID and an API token.

Steps

1. Using a web browser, log in to the Astra Control Center web UI.
2. From the Dashboard, select the user icon at the top right.
3. Select **API access**.
4. Note the Account ID near the top of the screen.

5. Select **Generate API token**.
6. In the resulting dialog, select **Generate API token**.
7. Note the resulting token, and select **Close**.
   In the CLI, change directories to the location of the `.yaml` bundle file in the extracted package contents.
8. Import the package using the bundle file, making the following substitutions:
   - Replace BUNDLE_FILE with the name of the Astra Control bundle file.
   - Replace SERVER with the DNS name of the Astra Control instance.
   - Replace ACCOUNT_ID and TOKEN with the account ID and API token you recorded earlier.

   ```
   kubectl astra packages import -m BUNDLE_FILE -u SERVER -a ACCOUNT_ID
   -k TOKEN
   ```

Result

If the bundle file is valid and the package images and artifacts are located in your connected repositories, the package is added to Astra Control Center.

If one or more images or artifacts for a package are not found in your repository, an error message appears for that package.

Remove a software package

You can use the Astra Control Center web UI to remove a software package that you previously imported in Astra Control Center.

Steps

1. In the **Manage Your Account** navigation area, select **Account**.
2. Select the **Packages** tab.

   You can see the list of installed packages and their statuses on this page.
3. In the **Actions** column for the package, open the actions menu.
4. Select **Delete**.

Result

The package is deleted from Astra Control Center, but the images and artifacts for the package remain in your repositories.

Find more information

- Manage repository connections