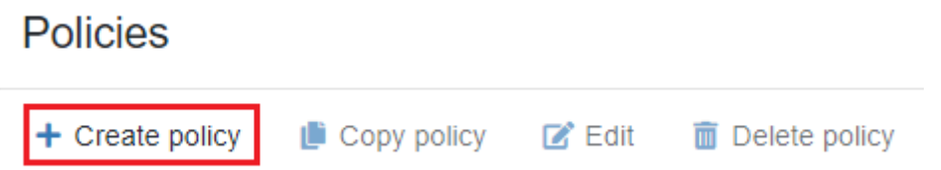
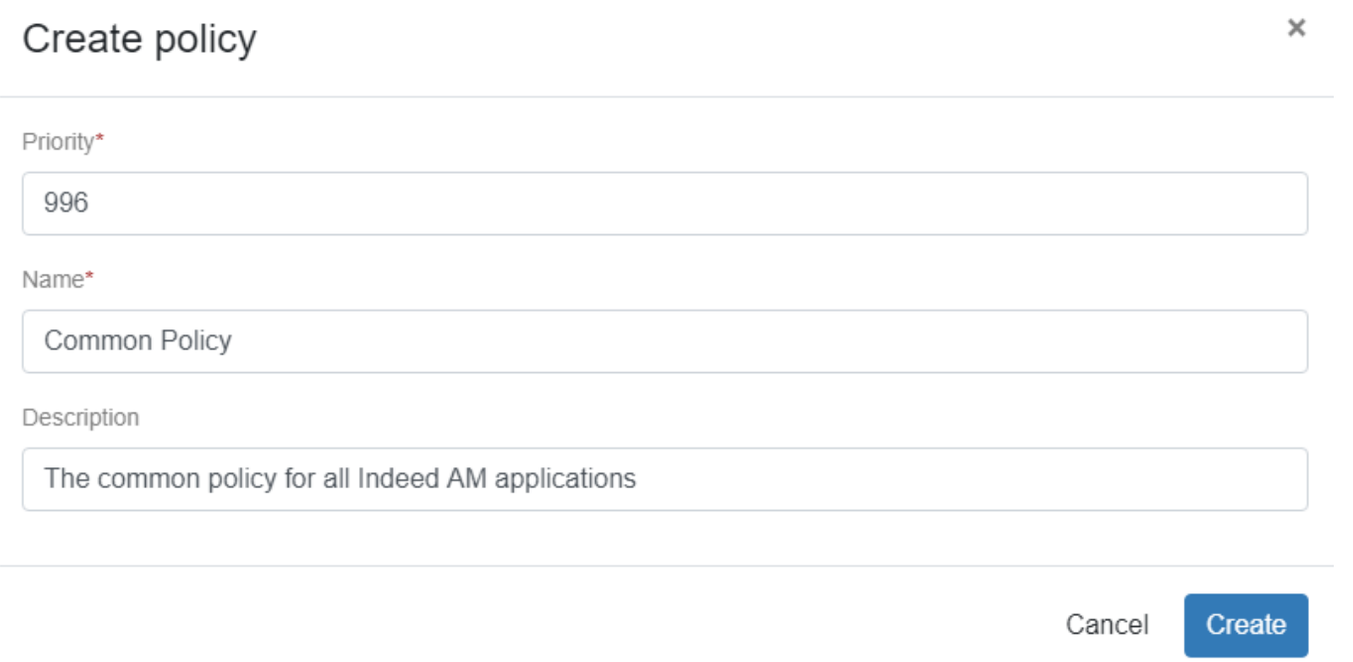
How to add and configure policies

How to add a new policy

1. Open your **Admin Console**.
2. In the left-side navigation bar, select **Policies**.
3. On the **Policies** page, click **Add**.



4. Indicate the priority status and name for a new policy, include its description (optional), and click Add.

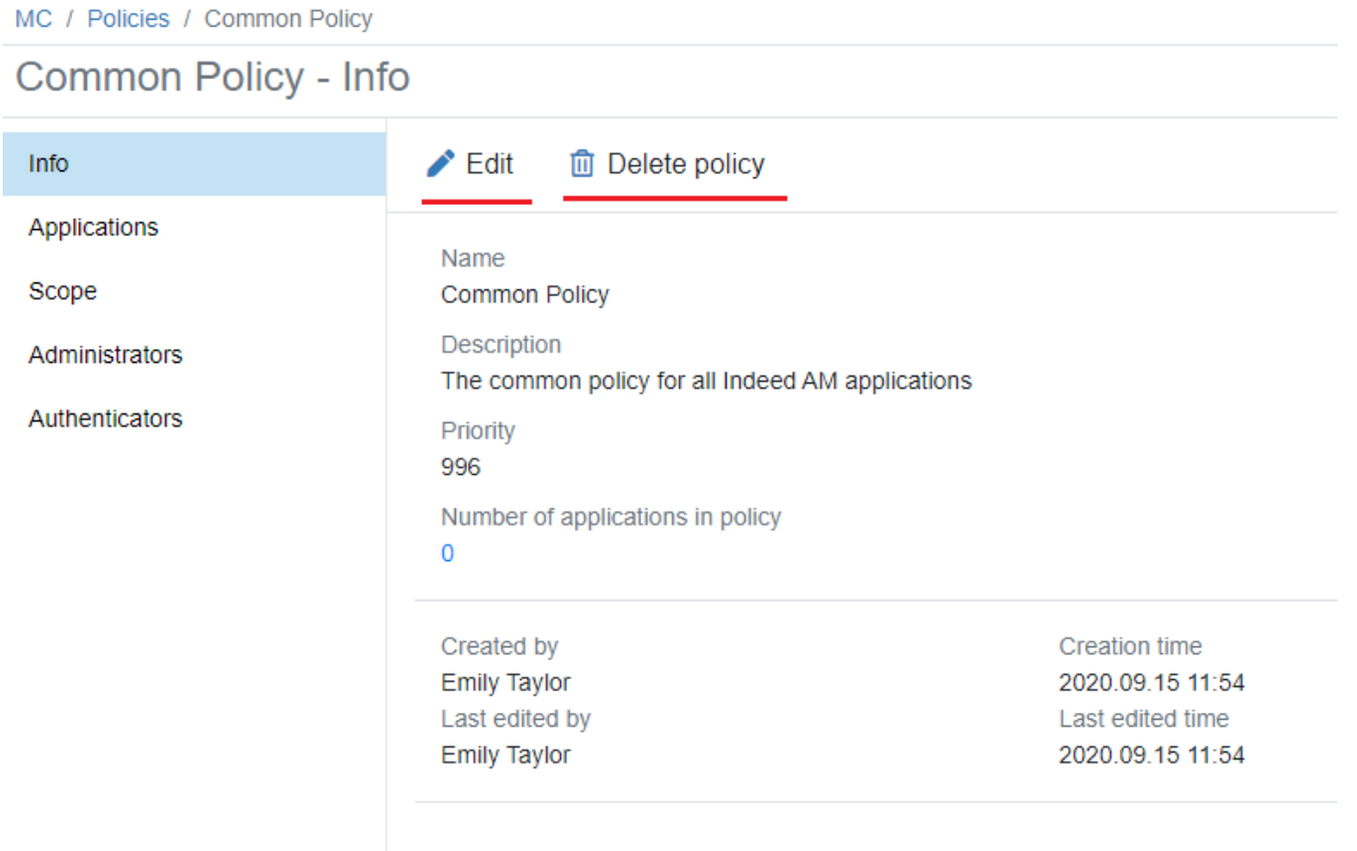


How to configure a policy

1. Open your **Admin Console**.
2. In the left-side navigation bar, select **Policies**.
3. Select the appropriate policy.

Information

This section contains basic information about the policy and its history. If you would like to edit the information, please click **Edit**. To delete a policy, click **Delete**.

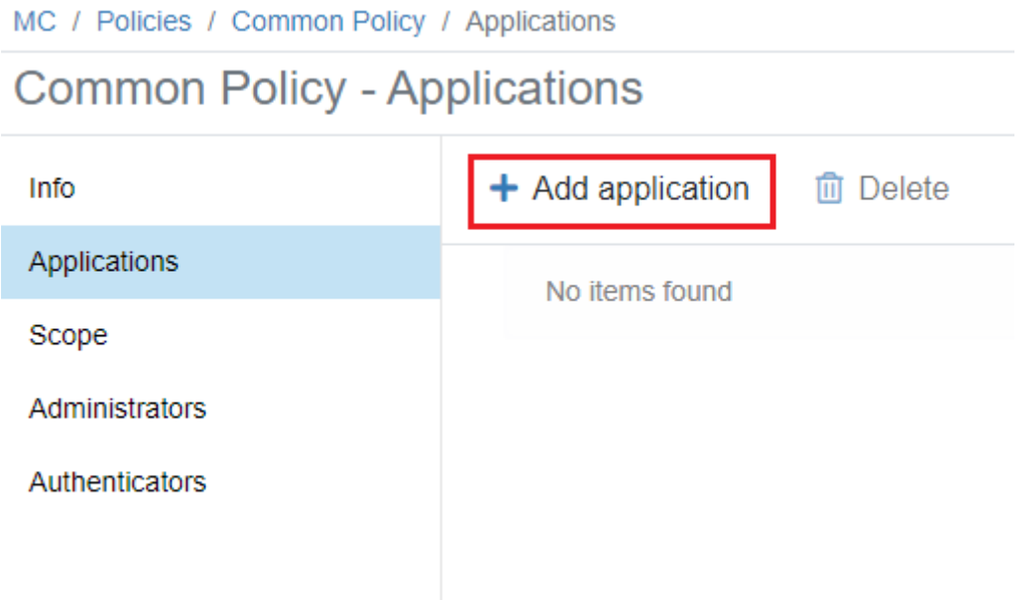


Applications

This section displays your policy apps. Please follow these steps to add an app:

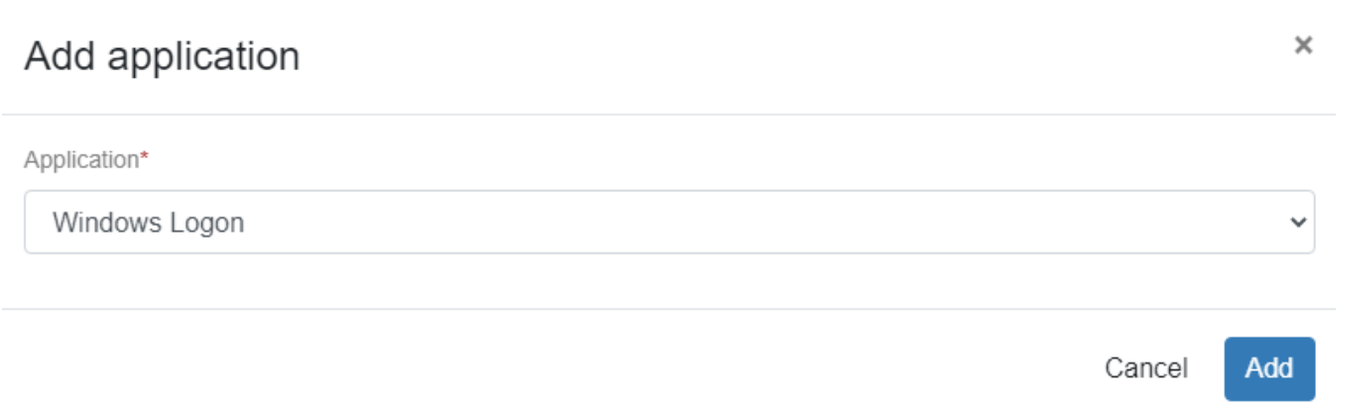
> The Indeed AM system apps include the Indeed AM ESSO Agent apps, as well as the Indeed AM integration modules (Indeed AM Windows Logon, Indeed AM NPS Radius, RDP Windows Logon, etc.).

1. Click **Add application**.



2. In the **Add a new application** window, select a relevant app and click **Add**. **Note.** You can only add an application if you have a registered license for this module.

> ⓘ You can only add an application if you have a registered license for this module.

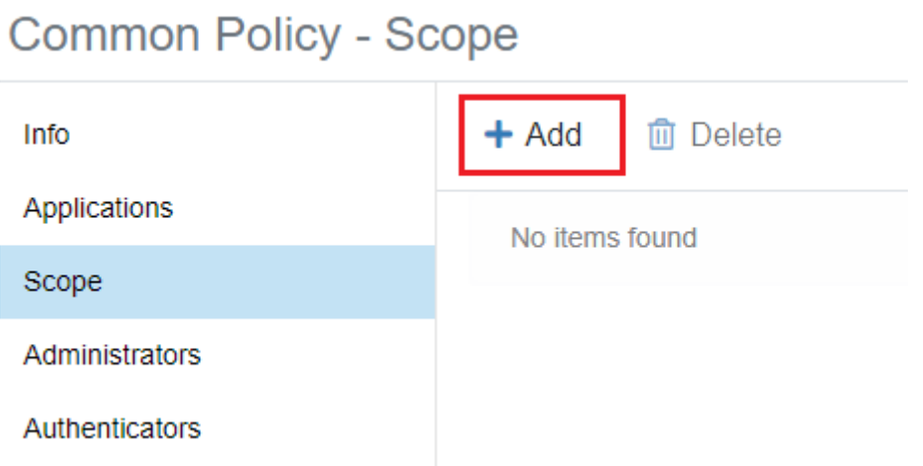


   a. To delete an app, select a relevant app and click **Delete**.

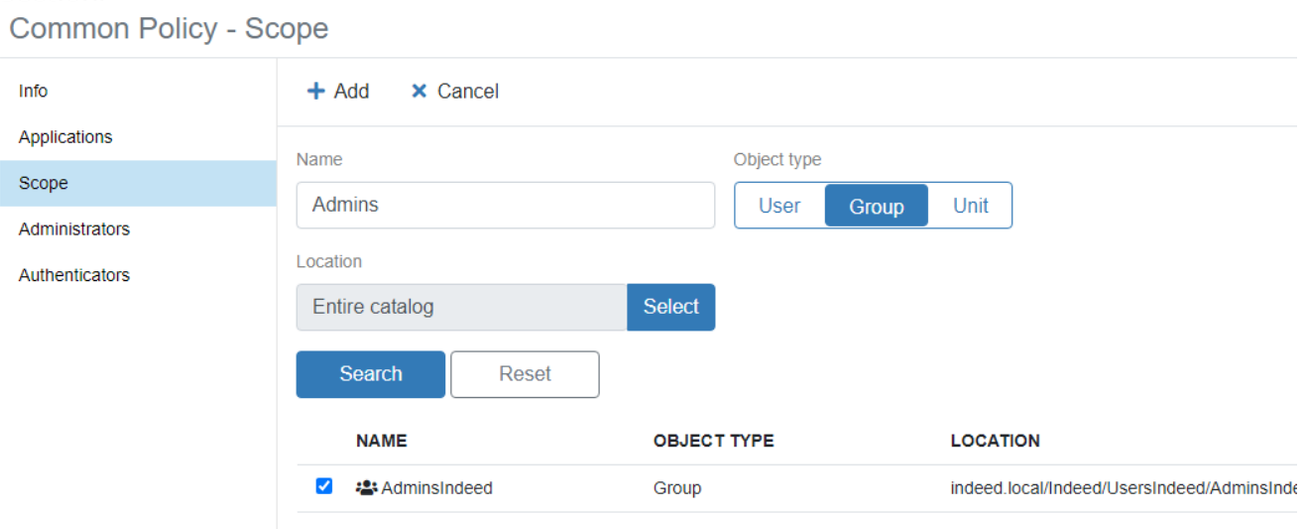
Scope

This section shows the list of objects covered by a given policy. Please follow these steps to add an object:

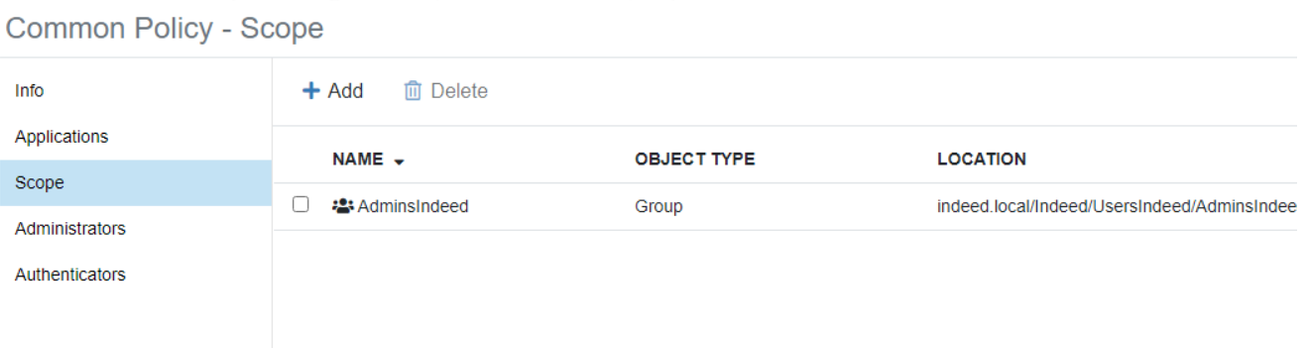
1. Click **Add**.



2. Select one option in the **Object type** field: User, Group or Container.
3. In the **Location** field, please select the object location – it may be an entire user folder or a separate container.
4. Please enter the object name or its part in the **Name** field and click **Search**. Select a relevant object and click **Add**. Once the object has been successfully added, it will be displayed in this section.



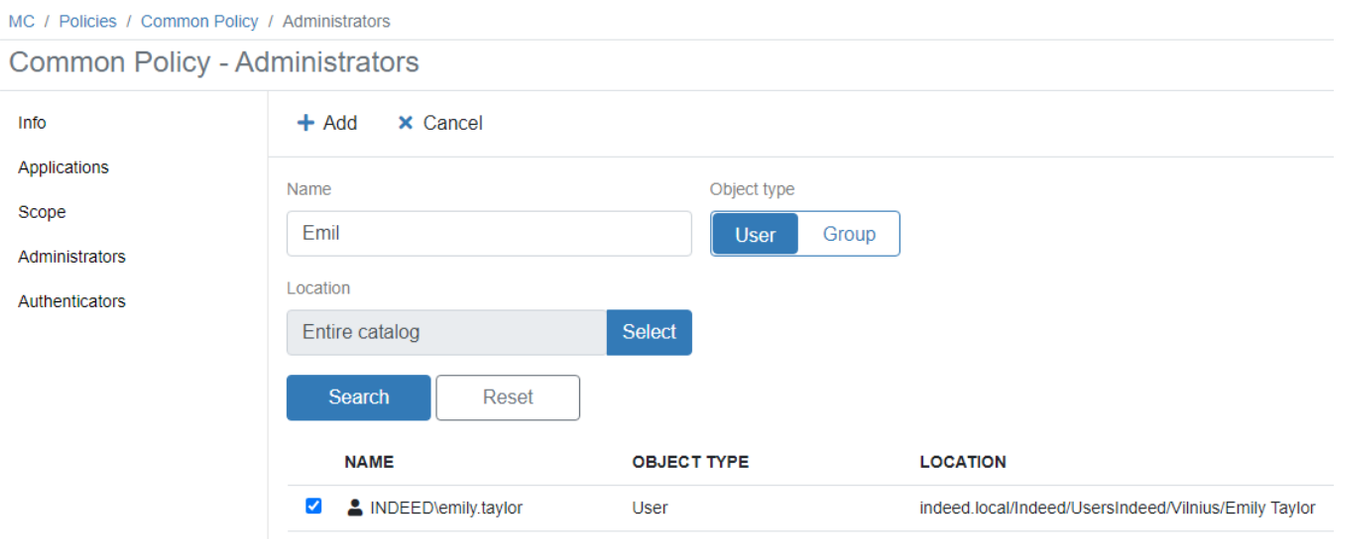
5. Select the found object and click **Add**.
6. After successfully adding the object will be displayed in the section.



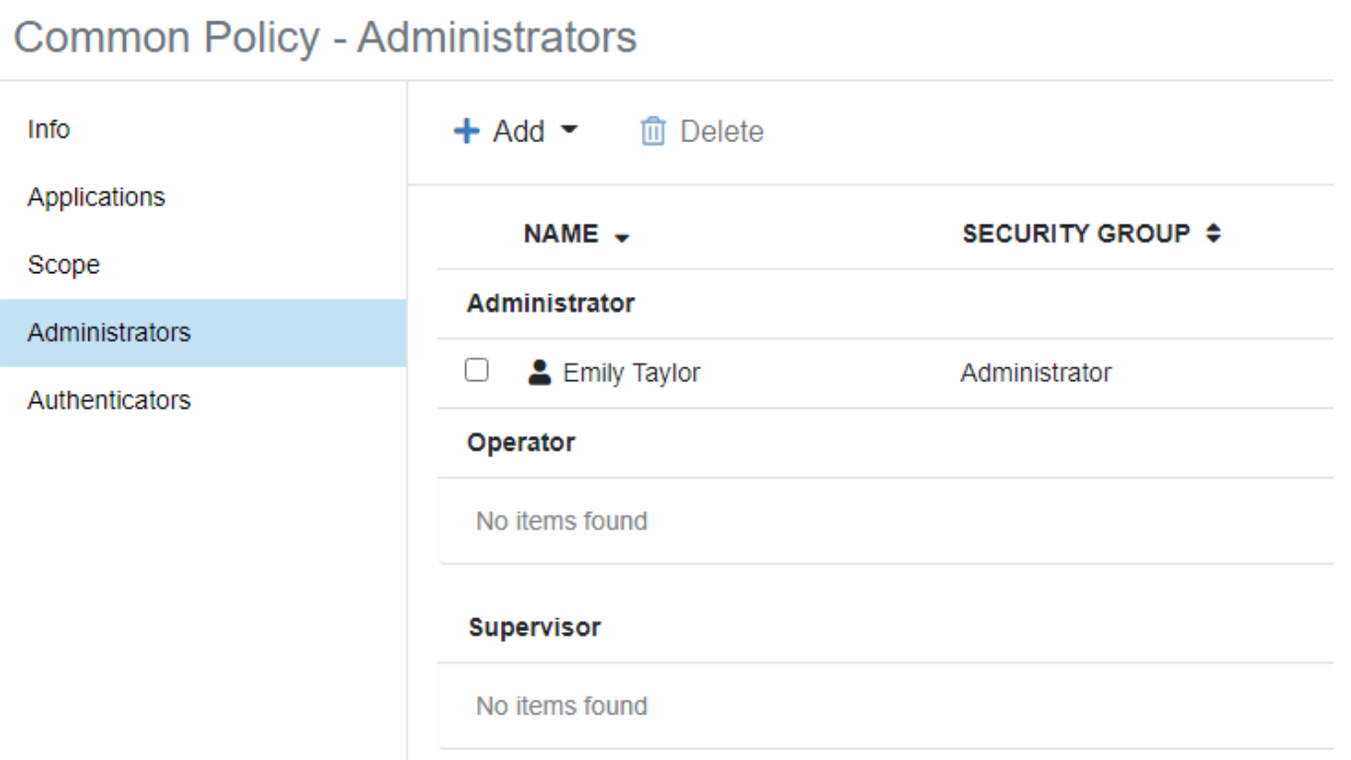
Administrators

This section shows the list of app administrators. Please follow these steps to add an administrator:

1. Click **Add** and select a relevant role: Administrator, Operator, Inspector.
2. In the **Object type** field, select one option: User or Group.
3. In the **Location** field, please select the object location – it may be an entire user folder or a separate container.
4. Please enter the object name or its part in the **Name** field and click **Search**.

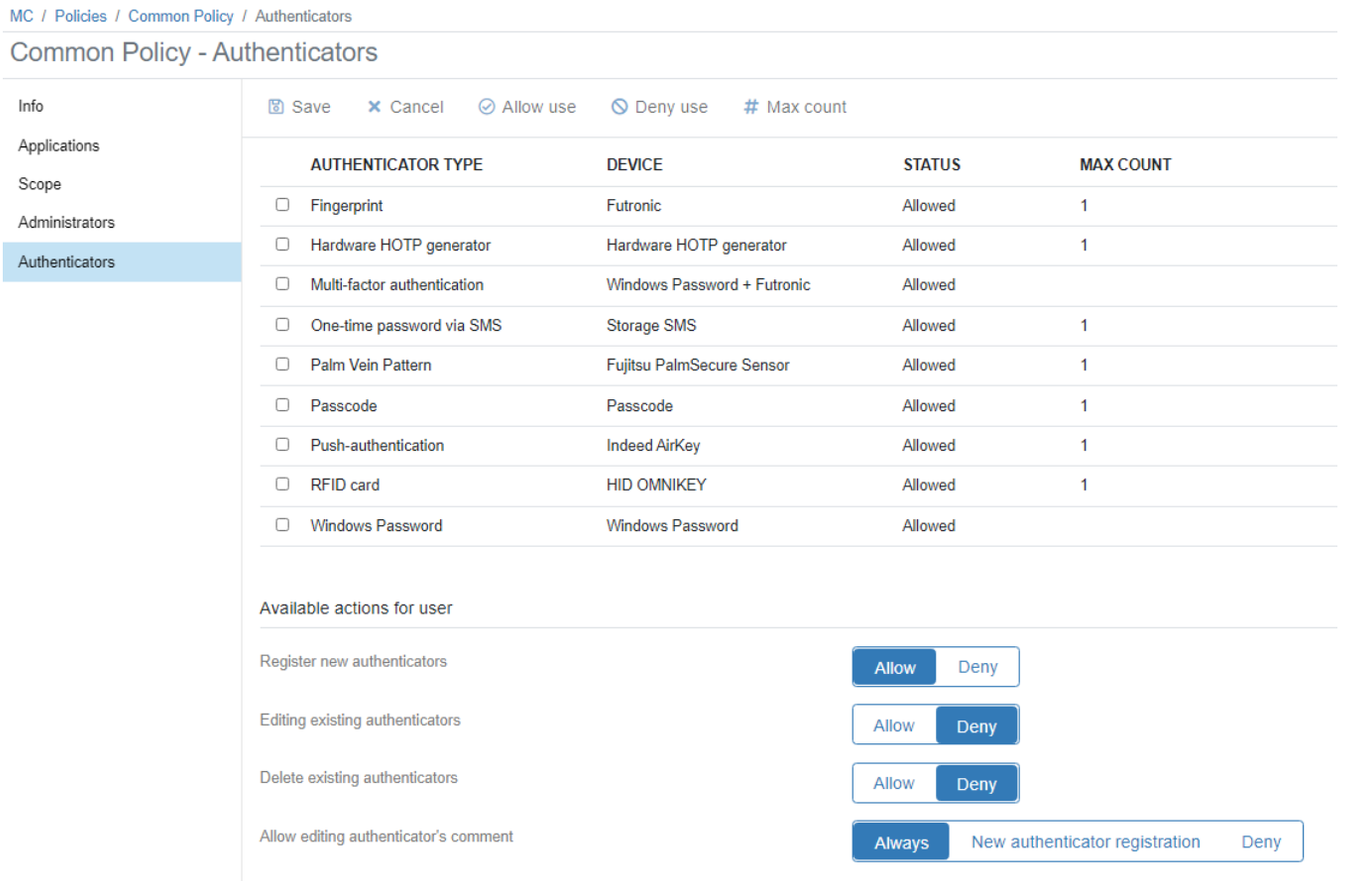


5. Select a relevant object and click **Add**.
6. Once the object has been successfully added, it will be displayed in this section.



Authenticators

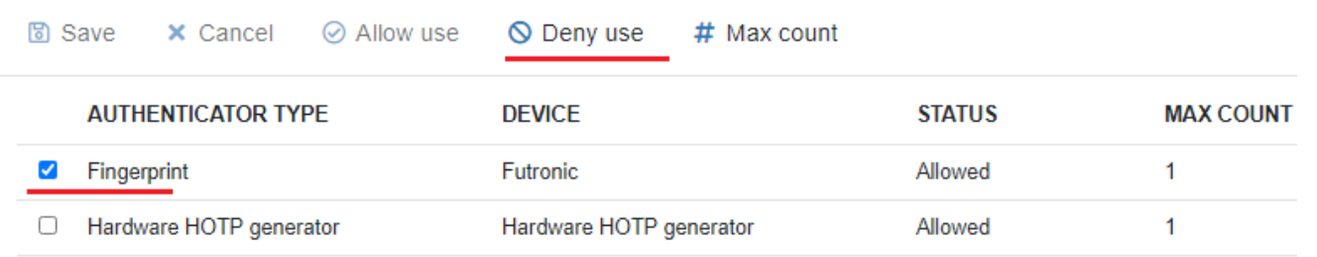
This section shows information about available authenticators and additional settings.



How to disable an authenticator

To disable an authenticator for all policy users, please follow these steps:

1. Select a relevant authenticator and click **Disable**.

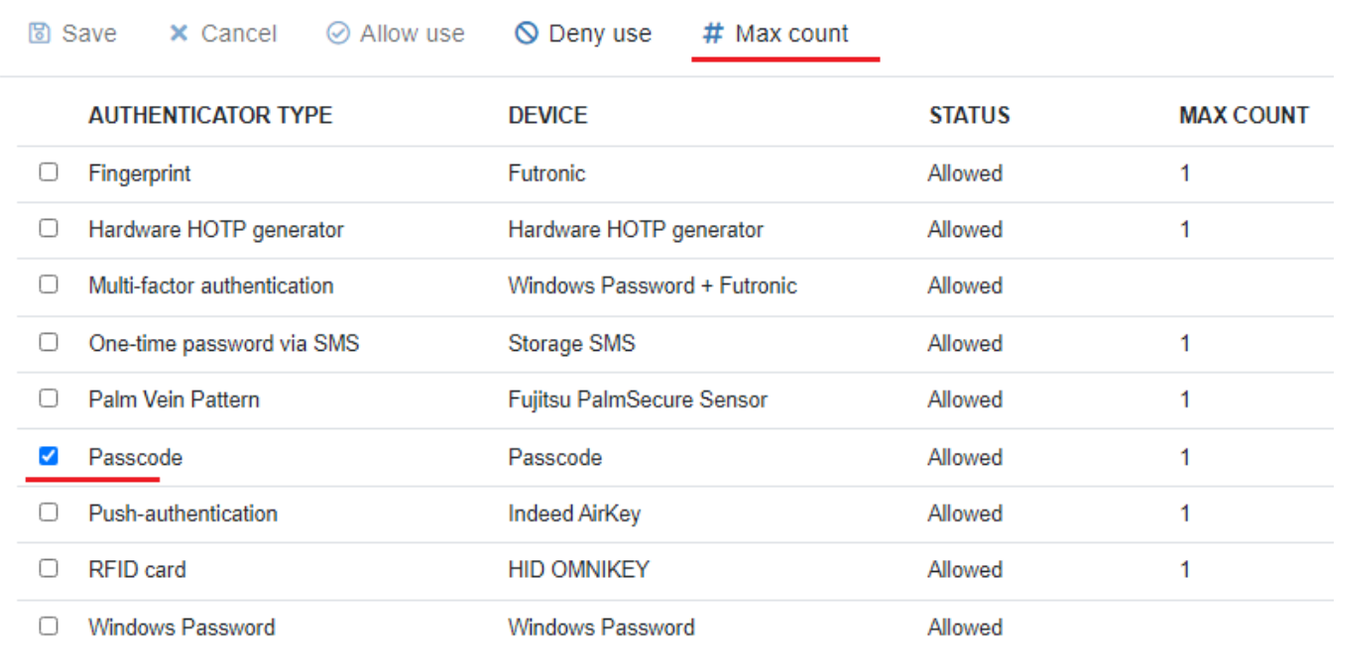


2. After that, the authenticator status will be changed to **Disabled**.

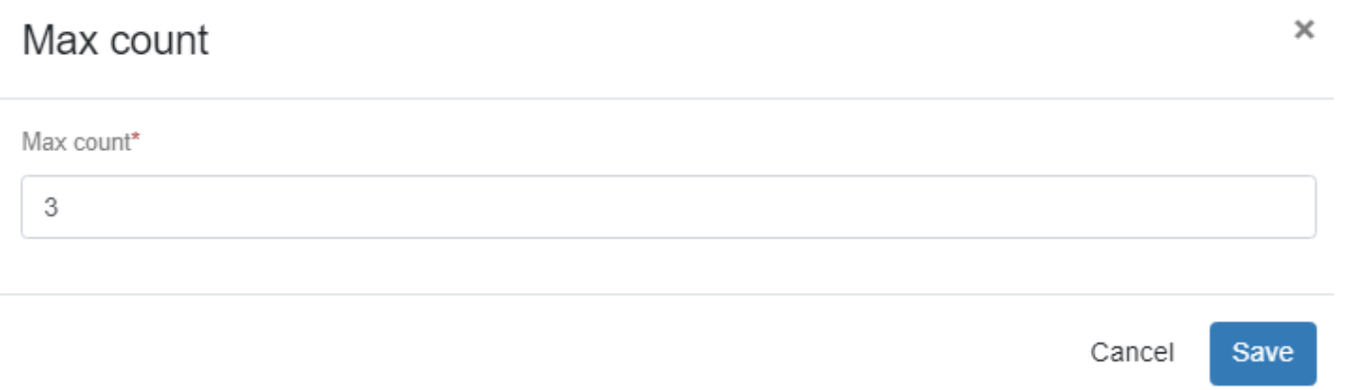
How to change authenticator limits

To change the maximum number of authenticators available for registration by a single user, please follow these steps:

1. Select a relevant authenticator and click **Max count**.



2. In the **Max count** window, please indicate a relevant value and click **Save**.



3. Upon successful completion, the authenticator limits will be changed.

Available actions for user

1. **Register new authenticators** – this parameter determines a user's permissions to train authenticators. Default value: **Enabled**
2. **Edit existing authenticators** – this parameter determines a user's permissions to edit the existing authenticators. Default value: **Disabled**
3. **Delete existing authenticators** – this parameter determines a user's permissions to delete the existing authenticators. Default value: **Disabled**
4. **Allow editing authenticator's comment** – this parameter determines a user's permissions to edit comments to the existing authenticators. Default value: **Always**

Available actions for user

Register new authenticators	**Allow** Deny
Editing existing authenticators	Allow **Deny**
Delete existing authenticators	Allow **Deny**
Allow editing authenticator's comment	**Always** New authenticator registration Deny