

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**.

Policies

 Create policy

 Copy policy

 Edit

 Delete policy

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

Create policy ✕

Priority*

996

Name*

Common Policy

Description

The common policy for all Indeed AM applications

Cancel

Create

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**.

Common Policy - Info

Info	✎ Edit 🗑 Delete policy				
Applications	Name Common Policy				
Scope	Description The common policy for all Indeed AM applications				
Administrators	Priority 996				
Authenticators	Number of applications in policy 0				
	<table border="1"><tr><td>Created by Emily Taylor</td><td>Creation time 2020.09.15 11:54</td></tr><tr><td>Last edited by Emily Taylor</td><td>Last edited time 2020.09.15 11:54</td></tr></table>	Created by Emily Taylor	Creation time 2020.09.15 11:54	Last edited by Emily Taylor	Last edited time 2020.09.15 11:54
Created by Emily Taylor	Creation time 2020.09.15 11:54				
Last edited by Emily Taylor	Last edited time 2020.09.15 11:54				

Applications

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

i 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**.

[MC](#) / [Policies](#) / [Common Policy](#) / [Applications](#)

Common Policy - Applications

Info	+ Add application	 Delete
Applications	No items found	
Scope		
Administrators		
Authenticators		

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.

Add application ×

Application*

Windows Logon ▼

Cancel

Add

- 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**.

Common Policy - Scope

Info

Applications

Scope

Administrators

Authenticators

+ Add Delete

No items found

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.

Common Policy - Scope

Info

Applications

Scope

Administrators

Authenticators

+ Add x Cancel

Name Object type

Admins User Group Unit

Location

Entire catalog Select

Search Reset

NAME	OBJECT TYPE	LOCATION
<input checked="" type="checkbox"/> AdminsIndeed	Group	indeed.local/Indeed/UsersIndeed/AdminsInde

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

Common Policy - Scope

Info

Applications

Scope

Administrators

Authenticators

+ Add Delete

NAME	OBJECT TYPE	LOCATION
<input type="checkbox"/> AdminsIndeed	Group	indeed.local/Indeed/UsersIndeed/AdminsInde

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**.

[MC](#) / [Policies](#) / [Common Policy](#) / Administrators

Common Policy - Administrators

Info **+ Add** **× Cancel**

Applications

Scope

Administrators

Authenticators

Name: Object type: **User** Group

Location: **Select**

Search Reset

NAME	OBJECT TYPE	LOCATION
<input checked="" type="checkbox"/> INDEED\emily.taylor	User	indeed.local/Indeed/UsersIndeed/Vilnius/Emily Taylor

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

Common Policy - Administrators

Info **+ Add** Delete

Applications

Scope

Administrators

Authenticators

NAME	SECURITY GROUP
Administrator	
<input type="checkbox"/> Emily Taylor	Administrator
Operator	
No items found	
Supervisor	
No items found	

Authenticators

This section shows information about available authenticators and additional settings.

MC / Policies / Common Policy / Authenticators

Common Policy - Authenticators

Info Save Cancel Allow use Deny use # Max count

AUTHENTICATOR TYPE	DEVICE	STATUS	MAX COUNT
<input type="checkbox"/> Fingerprint	Futronic	Allowed	1
<input type="checkbox"/> Hardware HOTP generator	Hardware HOTP generator	Allowed	1
<input type="checkbox"/> Multi-factor authentication	Windows Password + Futronic	Allowed	
<input type="checkbox"/> One-time password via SMS	Storage SMS	Allowed	1
<input type="checkbox"/> Palm Vein Pattern	Fujitsu PalmSecure Sensor	Allowed	1
<input type="checkbox"/> Passcode	Passcode	Allowed	1
<input type="checkbox"/> Push-authentication	Indeed AirKey	Allowed	1
<input type="checkbox"/> RFID card	HID OMNIKEY	Allowed	1
<input type="checkbox"/> Windows Password	Windows Password	Allowed	

Available actions for user

Register new authenticators	<input type="button" value="Allow"/> <input type="button" value="Deny"/>
Editing existing authenticators	<input type="button" value="Allow"/> <input type="button" value="Deny"/>
Delete existing authenticators	<input type="button" value="Allow"/> <input type="button" value="Deny"/>
Allow editing authenticator's comment	<input type="button" value="Always"/> <input type="button" value="New authenticator registration"/> <input type="button" value="Deny"/>

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**.

Save Cancel Allow use Deny use # Max count

AUTHENTICATOR TYPE	DEVICE	STATUS	MAX COUNT
<input checked="" type="checkbox"/> <u>Fingerprint</u>	Futronic	Allowed	1
<input type="checkbox"/> Hardware HOTP generator	Hardware HOTP generator	Allowed	1

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**.

Save Cancel Allow use Deny use **# Max count**

AUTHENTICATOR TYPE	DEVICE	STATUS	MAX COUNT
<input type="checkbox"/> Fingerprint	Futronic	Allowed	1
<input type="checkbox"/> Hardware HOTP generator	Hardware HOTP generator	Allowed	1
<input type="checkbox"/> Multi-factor authentication	Windows Password + Futronic	Allowed	
<input type="checkbox"/> One-time password via SMS	Storage SMS	Allowed	1
<input type="checkbox"/> Palm Vein Pattern	Fujitsu PalmSecure Sensor	Allowed	1
<input checked="" type="checkbox"/> Passcode	Passcode	Allowed	1
<input type="checkbox"/> Push-authentication	Indeed AirKey	Allowed	1
<input type="checkbox"/> RFID card	HID OMNIKEY	Allowed	1
<input type="checkbox"/> Windows Password	Windows Password	Allowed	

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

Max count ×

Max count*

Cancel

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