

Configuring Corporate Sign In with Azure

This page provides information on how to configure Corporate Sign in in Chaos services with Azure.

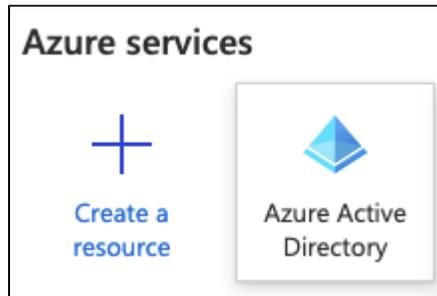
Overview

In this section we explore how you to integrate your Azure identity provider with Chaos, so that your employees benefit from the **Corporate Sign In** functionality.

Before doing the steps in this section, make sure to [reach out to Chaos](#) first to request the Corporate Sign In feature.

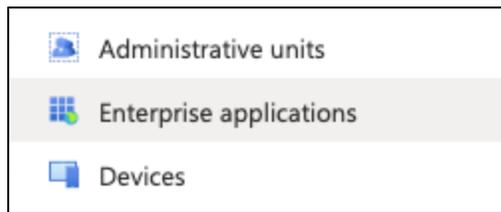
Adding Chaos application from Azure Gallery

1. Log in to your **Azure** portal and navigate to the **Azure Active Directory** service.

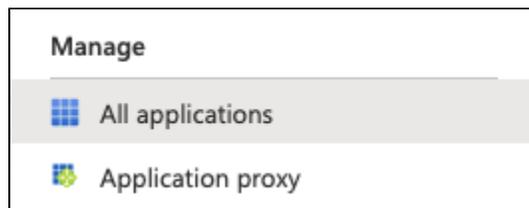


Your Portal may look different due to a number of factors ranging from theme selection, changes on Azure side, etc.

2. Navigate to the **Enterprise applications** menu on the left.



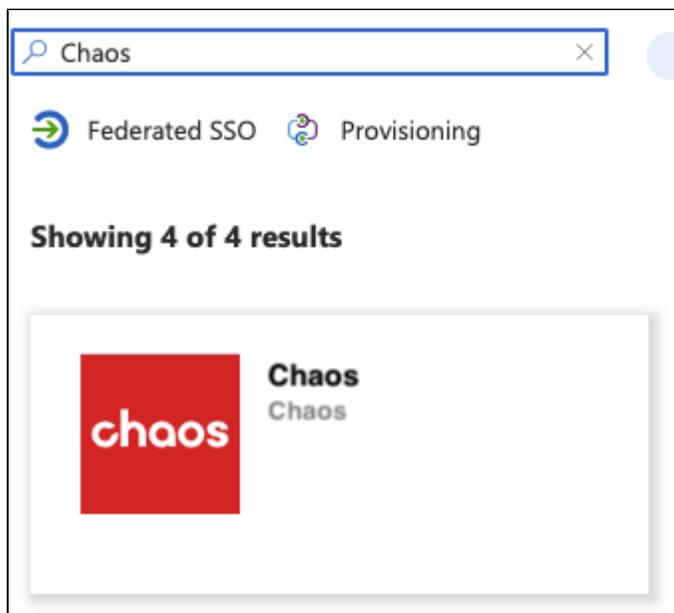
3. Navigate to the **All applications** menu on the left.



4. Use the **New application button** at the top.



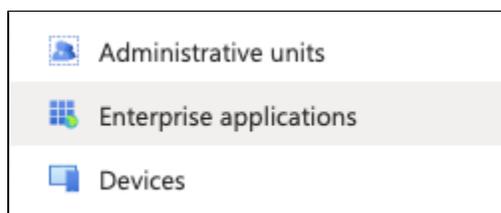
5. Search for the **Chaos application** and select it.



6. Once selected, click the **Create** button on the right-hand side.

Configuring access to the Chaos application

1. Navigate to the **Enterprise applications** menu in **Azure Active Directory**.



2. Find and select the **Chaos application** in the list.

If it does not show, try waiting a minute or so and refresh the page.

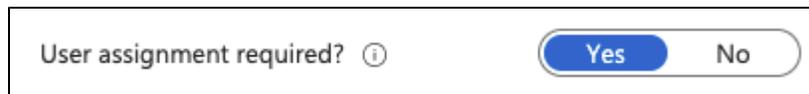
3. Navigate to the **Properties** menu.



4. Ensure that **Enabled for users to sign-in** is set to **Yes**.

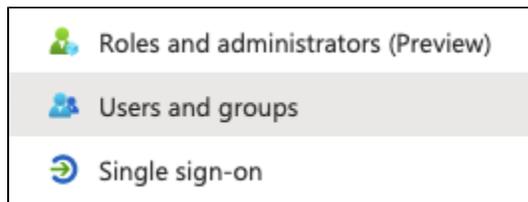


5. Change **User assignment required?** to **Yes**.



You can leave this option to **No** but that means all employees in your Azure tenant will be able to access Chaos with their user credentials. Normally, you would want to keep this setting aligned to the provisioning settings (explored later) which means that if you leave it as is, you would also need to provision all users to Chaos.

6. Navigate to the **Users and Groups** menu.



7. Use the **Add user/group** button to add users and groups to the Chaos application. Users and groups added to this application are able to login to Chaos using the Corporate Sign In functionality. This setting is also important when provisioning is configured.

Make sure to add your administrator to this list.

If you selected **No** in the User assignment required option, then you don't need to add any users or groups here.

Accessing Chaos through Corporate Sign In

The following steps need to be followed by the Administrator of your Azure tenant.

1. Navigate to the Chaos accounts page: <https://accounts.chaosgroup.com/>
2. Log in [using Corporate Sign In](#)
3. Confirm the consent dialog.



john.doe@chaosgroup.com

Permissions requested



This application is not published by Microsoft or your organisation.

This app would like to:

- View your basic profile
- Maintain access to data you have given it access to
- Consent on behalf of your organisation

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

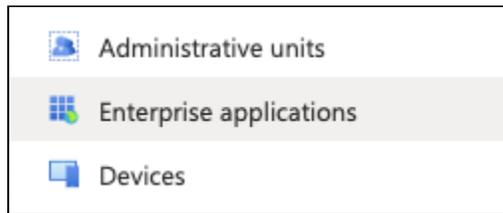
Does this app look suspicious? [Report it here](#)

Make sure to enable the **Consent on behalf of your organization** checkbox. This prevents the dialog from appearing to every non-administrator user that tries to log in.

- 4. Verify that you are logged in successfully to the Chaos web page.

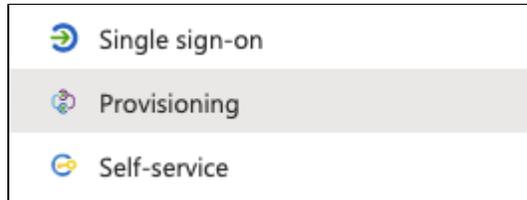
Enabling provisioning

- 1. Navigate to the **Enterprise applications** menu in Azure Active Directory.



2. Find and select the **Chaos application** in the list.

3. Navigate to the **Provisioning** menu.



4. Press the **Get started** button.

Automate identity lifecycle management with Azure Active Directo

Automatically create, update, and delete accounts when users join, leave, and move within your c

[Get started](#)

5. Select **Automatic provisioning** mode.

Provisioning Mode

Automatic ▼

6. Configure **Tenant URL** and **Secret Token**.

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to Custom Integration 2's API and synchronize user data.

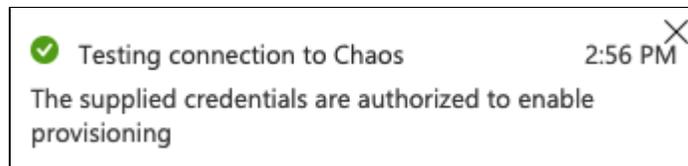
Tenant URL * ⓘ

Secret Token

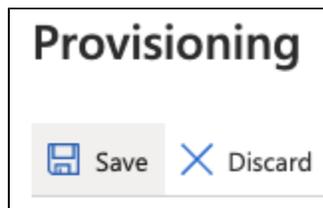
The URL has the following pattern: <https://scim.chaos.com/<chaos-tenant-id>/v2>

The **chaos-tenant-id** and **secret token** are received as part of the [onboarding process](#).

7. Verify the configuration with the **Test Connection** button.



8. Use the **Save** button to save the configuration.



Once you save the configuration, additional **Mappings and Settings** sections appear. These are configured next.

9. Expand the **Mappings** section.

^ Mappings

Mappings

Mappings allow you to define how data should flow between Azure Active Directory and customappsso.

Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

Restore default mappings

10. By default the Group mapping function is not visible. However if it is visible on your end, here is how to disable it.

a. Click on the **Provision Azure Active Directory Groups** link.

b. **Disable** the Group mapping.



Chaos does not process Groups, as such this mapping is unnecessary. Even when disabled, it is still possible to assign Groups in the **Users and Groups** setting of the Application and use them to control access and provisioning.

c. Save the changes to the Group mapping.



11. Return to the **Mappings** section and select the **Provision Azure Active Directory Users** link.

12. Make sure the **Attribute Mappings** table looks as it follows.

Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

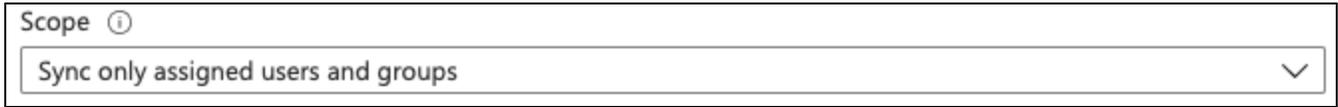
Azure Active Directory Attribute	customappsso Attribute	Matching preceden...	Remove
userPrincipalName	userName	1	Delete
Not([IsSoftDeleted])	active		Delete
userPrincipalName	emails[type eq "work"].value		Delete
givenName	name.givenName		Delete
surname	name.familyName		Delete

[Add New Mapping](#)

13. Save the changes to the User mapping. If no changes were performed, navigate back to the previous screen.



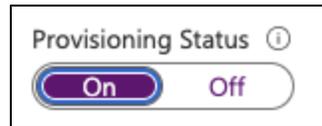
- Expand the **Settings** section.
- Ensure the **Scope** is set to **Sync only assigned users and groups**.



A screenshot of a dropdown menu titled "Scope" with an information icon. The selected option is "Sync only assigned users and groups".

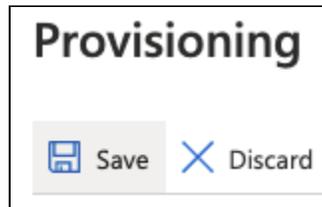
When configuring the Application, if you decide to allow all Azure users in your tenant to be able to log in to Chaos, set the Scope to **Sync all users and groups** to get a consistent experience.

- Set **Provisioning Status** to **On**.



A screenshot of a toggle switch labeled "Provisioning Status" with an information icon. The "On" option is selected and highlighted in purple.

- Save the provisioning settings.



A screenshot of a dialog box titled "Provisioning". It contains two buttons: "Save" (with a floppy disk icon) and "Discard" (with an 'X' icon).

Provisioning is now enabled. You can check whether it is working successfully through the **Application's Provisioning** menu.

Currently, Azure performs provisioning on regular intervals of 40 minutes. Most likely, you will need to wait that much to see if it works successfully. This also means that it takes at least 40 minutes when a user is disabled in your Azure directory to take effect in the Chaos system.