

User Provisioning using SCIM in Azure

Table of Content

Customer.....	1
Prerequisites	1
Create enterprise application	1
Configure user provisioning	3
Initial connection	3
Mappings.....	4
Groups.....	5
Users	6
Settings.....	8
Assign groups	8
Start provisioning	8
Configure permissions	8
CERRIX	9
Prerequisites	9
Settings.....	9
Generate secret token	10

Customer

Prerequisites

To configure user provisioning the following information is required from CERRIX:

URL to SCIM endpoint	https://[customer short name].cerrix.com/api/scim
Secret token	A JWT to access the SCIM endpoint. This is a long-lived token which expires after a certain date and needs to be replaced. The date can be negotiated. (In future release of CERRIX the customer should be able to manage these tokens themselves)

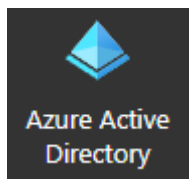
CERRIX requires the following information:

Default organization	Used to specify the default/fallback organization that new users are linked too. Or if an organization identifier is given through user provisioning when no match is found.
----------------------	--

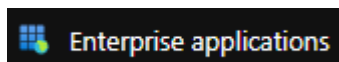
Create enterprise application

We need to create a non-gallery enterprise application in which we can configure user provisioning and configure which groups and users are synchronized.

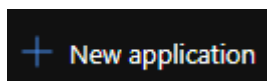
Go to “Azure Active Directory”:



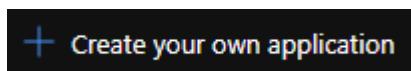
Select “Enterprise applications” in the side menu:



Select “New application” in the top menu under “All applications”:



Select “Create your own application” in the top menu to make a non-gallery application:



Fill in a name for the non-gallery application and make sure “non-gallery” is selected:

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

CERRIX SCIM

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises application

☐ Register an application to integrate with Azure AD (App you're developing)

☒ Integrate any other application you don't find in the gallery (Non-gallery)

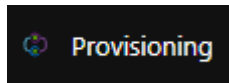
Select “Create” at the bottom:

Create

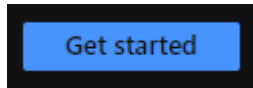
Configure user provisioning

Initial connection

Go to the created non-gallery enterprise application and select “Provisioning” in the side menu:



Select “Get started”:



Fill in the following values:


Provisioning Mode	Automatic
Tenant URL	https://[customer short name].cerrix.com/api/scim
Secret Token	JWT received from CERRIX to access the SCIM endpoint

Select “Test Connection” to validate the “Tenant URL” and “Secret Token” and when valid press “Save”:

A screenshot of the "Provisioning" configuration page. The page has a dark blue header with the title "Provisioning" and a menu icon. Below the header, there are "Save" and "Discard" buttons. The main content area has a light blue background. It starts with a "Provisioning Mode" dropdown menu set to "Automatic". Below this, there is a text box that says "Use Azure AD to manage the creation and synchronization of user accounts in CERRIX SCIM based on user and group assignment." Then, there is a section titled "Admin Credentials" with a sub-header "Admin Credentials" and a note "Azure AD needs the following information to connect to CERRIX SCIM's API and synchronize user data." Below this, there are two input fields: "Tenant URL" with a red asterisk and a help icon, containing the value "https://customer.cerrix.com/api/scim" with a green checkmark; and "Secret Token" with a masked input field. At the bottom, there is a "Test Connection" button.

Mappings

Extend "Mappings" in "Edit Provisioning" screen:

 **Mappings**

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

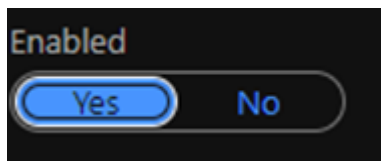
Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

☐ Restore default mappings

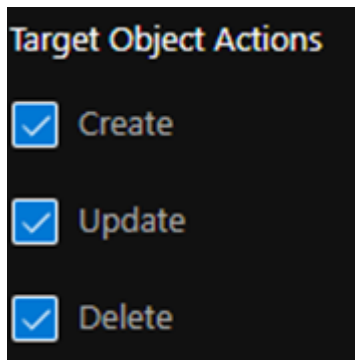
Groups

Select "Provision Azure Active Directory Groups" under "Mappings".

Set "Enabled" too "Yes":



Select "Create", "Update" and "Delete".



Make sure the following "Attribute Mappings" are configured and delete others if any:

displayName	displayName	Name for Role Group
objectId	externalId	Id to identifies role group in AD
members	members	Users connected to Role Group

Attribute Mappings			
Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso			
Azure Active Directory Attribute	customappsso Attri...	Matching preceden...	Remove
displayName	displayName	1	Delete
objectId	externalId		Delete
members	members		Delete
Add New Mapping			

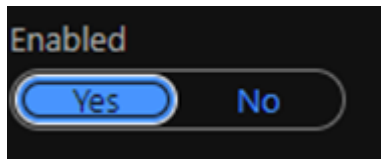
Select "Save" in the top menu:



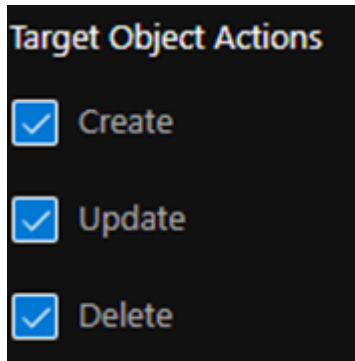
Users

Select “Provision Azure Active Directory Users” under “Mappings”.

Set “Enabled” too “Yes”:



Select “Create”, “Update” and “Delete”.



Make sure the following “Attribute Mappings” are configured and delete others if any:

userPrincipalName	username	Username
Switch([IsSoftDeleted], “False”, “True”, “True”, “False”)	active	Indicates if user may still access CERRIX. User gets deleted from CERRIX when user is also (permanently) deleted in Azure.
mail	emails[type eq “work”].value	Email address
givenName	name.givenName	First name
Surname	name.familyName	Last name
mailNickname	externalId	ID to identifies user in AD
When available a custom organization identifier	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:organization	(Optional) Custom organization identifier from customer.

Attribute Mappings			
Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso			
Azure Active Directory Attribute	customappsso Attri...	Matching preceden...	Remove
userPrincipalName	userName	1	Delete
Switch([IsSoftDeleted], , “False”, “True”, “True”, “False”)	active		Delete
mail	emails[type eq “work...		Delete
givenName	name.givenName		Delete
surname	name.familyName		Delete
mailNickname	externalId		Delete
?????	urn:ietf:params:scim:...		Delete
Add New Mapping			

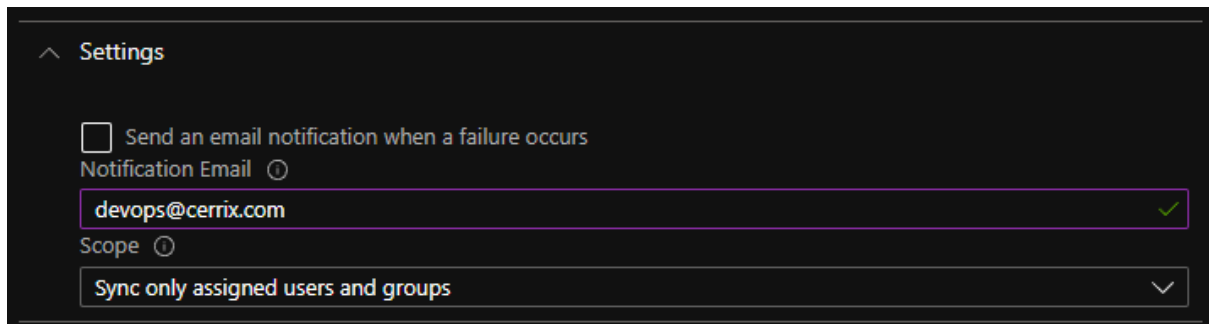
Select “Save” in the top menu:



Settings

Expand “Settings” in “Edit Provisioning”.

Make sure “Scope” is set to “Sync only assigned users and groups”:



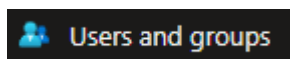
The screenshot shows a settings panel with a dark background. At the top, there is a header 'Settings' with an expand/collapse icon. Below it, there is a checkbox labeled 'Send an email notification when a failure occurs'. Under this checkbox is a field for 'Notification Email' with the value 'devops@cerrix.com' and a green checkmark icon. Below the email field is a dropdown menu for 'Scope' with the selected value 'Sync only assigned users and groups' and a downward arrow icon.

Optionally configure a “Notification Email” and select “Send an email notification when a failure occurs”.

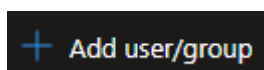
Assign groups

Normally only groups are assigned but users are also possible.

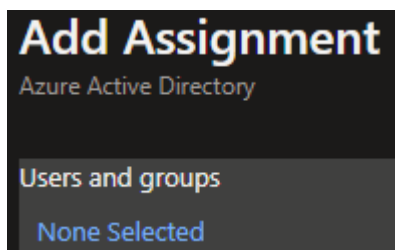
Select “Users and groups” in the left menu of the “Enterprise Application”:



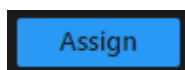
Select “Add user/group” in top menu:



Select “None Selected” under “Users and groups”:

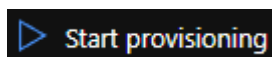


Select the groups (and users) that need to be assigned and select “Save” in bottom menu:



Start provisioning

Select “Start provisioning” at “Provisioning”:



Configure permissions

Permissions can be configured for the “Role Groups” in CERRIX after the groups are synchronized.

CERRIX

Prerequisites

Required information from customer:

Default organization id	Used to specify the default/fallback organization that new users are linked too. Or if an organization identifier is given through user provisioning when no match is found.
-------------------------	--

Required information from CERRIX:

Environment URL	Used for issuer in token
Environment Name	Used for audience in token
Security Key	Used to sign the token

Customer requires the following information:

URL to SCIM endpoint	https://[customer short name].cerrix.com/api/scim
Secret token	A JWT to access the SCIM endpoint. Use the "JWT Generator" to generate the long-lived token. (In future release of CERRIX the customer should be able to manage these tokens themselves)

Settings

Settings required to validate token:

JwtSecurityKey	Used to sign tokens
ApplicationRootUrl	Used for issuer in token
EnvironmentName	Used for audience in token

Settings required to use SCIM:

SCIM:ScimEnabled	Enable or disable user provisioning
SCIM:ScimDefaultOrganizationId	Configure default/fallback organization

Generate secret token

Use the “JWT Generator” to generate a long-lived token:



The screenshot shows a window titled "JWT Generator" with the following fields and values:

Field	Value
Security Key	X\z2oVBjN\$FSaVw#gCIEYuHRfABm%M
Environment URL	https://test-scim.cerrix.com/
Environment Name	testing-cerrix-scim-t
Username	CerrixScim
Scopes	scim.access
Valid For	2 years

Below the fields is a "Generate" button. The resulting token is displayed in a text area below the button:

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJqdGkiOiJkY2YyYmJhZC00YTU3LTQwMGEtOTNkMC02OTNiYyZmRkNWYiLCJ1bmlxdWVfbmFtZSI6IklncnJpeFNjaW0iLCJzY29wZSI6InNjaW0uYWNjZXRzIiwibmJmIjoxNjQ2NDAwNjI4LCJleHAiOiE3MDk1NTkwMjgsImh0bCI6MTY0NjQwMDYyOCwiaXNzIjoiaHR0cHM6Ly90ZXN0LXNjaW0uY2Vycml4LmNvbS8iLCJhdWQiOiJ0ZXN0aW5nLWNIcnJpeC1zY2ItLXQifQ.8PjOZR7-OXwIxlFuzzaaOjIaxhbD290-q2UT4RAHvxs
```