

How to Set Up a SCIM Integration with Uniqkey and Azure AD

Introduction:

This guide explains how to set up a SCIM integration using Uniqkey and Azure Active Directory.

Requirements:

You need admin access to Uniqkey and permission to create enterprise applications in Azure Active Directory. Please note that assigning users to groups requires a paid version of Azure.

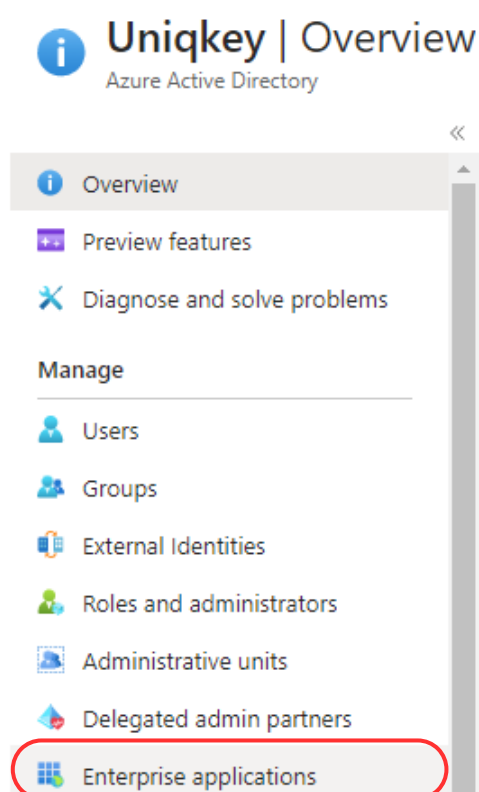
Instructions

1. Access Azure AD

- Log in to your Azure Active Directory (AD).

2. Navigate to Enterprise Applications

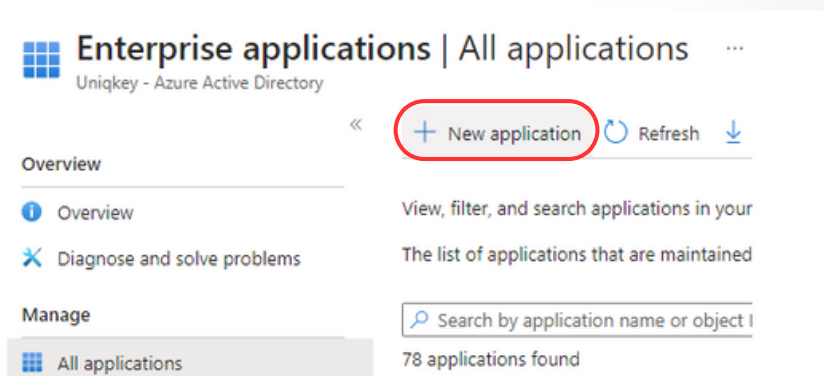
- Use the left-side menu to navigate to your "Enterprise Applications".



Instructions

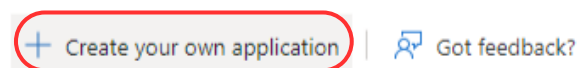
3. Create a New Application

- Click "New application".




- Select "Create your own application".

Browse Azure AD Gallery



- Provide a fitting name for the Enterprise Application and select the "Non-gallery" app option.

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?

Uniqkey 

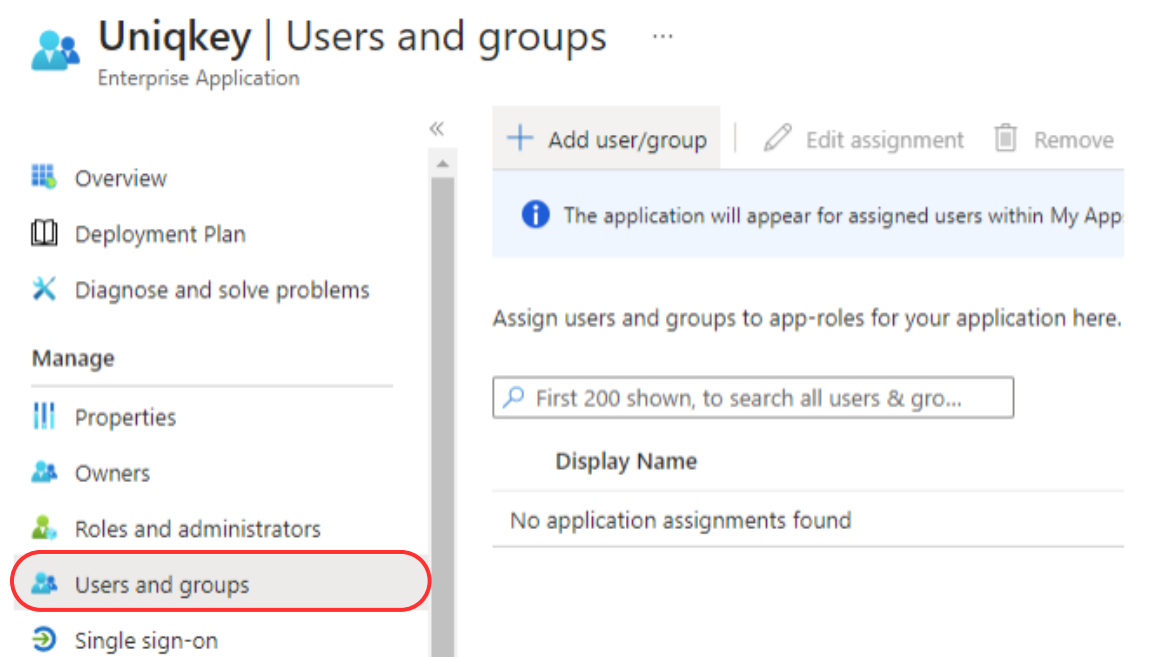
What are you looking to do with your application?

- 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)

Instructions

4. Manage Users and Groups

- After the application is created, go to the "users and groups" tab.
- From here, you can manage your users and groups. If you wish to assign users individually, simply add them directly



Things you need to know before continuing

- If using groups, only global security groups are supported by SCIM.
- Users in groups don't need to be directly assigned if they're members of an added security group.
- Group nesting is not supported.
- Users will be provisioned to Uniqkey if they have a connection to the Enterprise Application.
- If users are part of multiple groups assigned to the Enterprise App and get removed from one of them, they will still maintain their connection to the Uniqkey app.
- If you want to remove a user from Uniqkey, they must be removed from all the relevant security groups before they can be provisioned out of Uniqkey.

Instructions

5. Activate Provisioning

- Navigate to the "Provisioning" tab.

Manage

- ||| Properties
- 👤 Owners
- 👤 Roles and administrators
- 👤 Users and groups
- 🔄 Single sign-on
- ⚙️ Provisioning**

- Click the "Get started" button.



Automate identity lifecycle management with Azure Active Directory

Automatically create, update, and delete accounts when users join, leave, and move within your organization. [Learn more.](#)

Get started

6. Set Provisioning Mode

- Change the "Provisioning Mode" to automatic.

Provisioning ...

Save ✕ Discard

Provisioning Mode

Manual

Manual

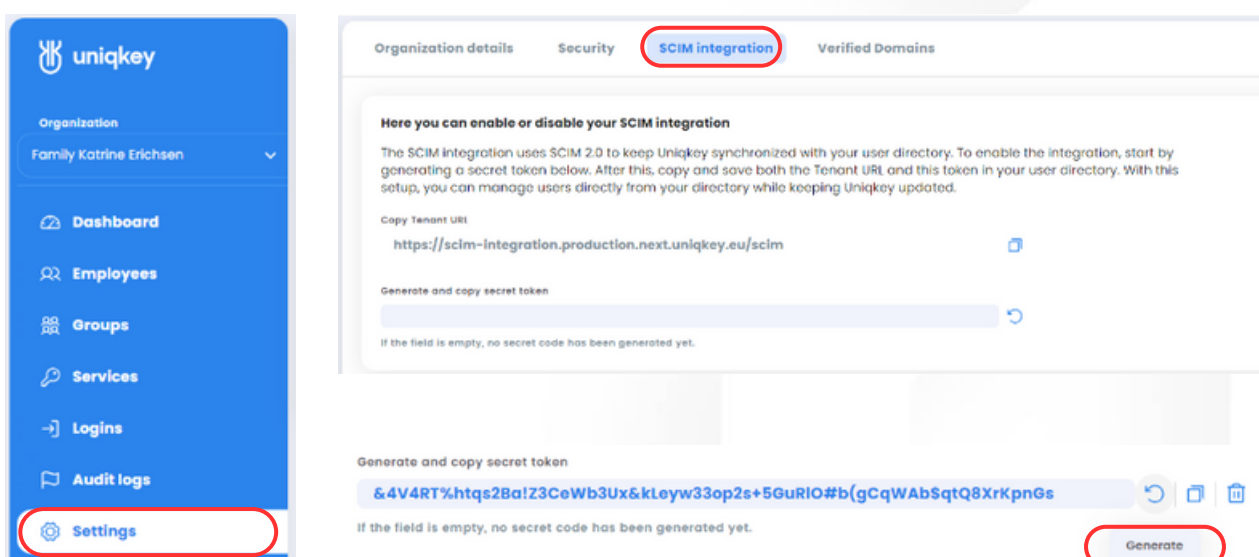
Automatic

user account

Instructions

7. Enter Tenant URL and secret token

- In the "Admin Credentials" panel, provide your tenant URL and secret token from your Uniqkey admin portal.
- To find these details, log in to your Uniqkey admin portal and go to the "Settings" page.



The screenshot shows the Uniqkey admin portal interface. On the left is a blue sidebar with navigation options: Organization (Family Katrine Erichsen), Dashboard, Employees, Groups, Services, Logins, Audit logs, and Settings (highlighted with a red circle). The main content area has tabs for Organization details, Security, SCIM integration (highlighted with a red circle), and Verified Domains. The SCIM integration page contains instructions on enabling/disabling the integration, a text input for the Tenant URL (containing `https://scim-integration.production.next.uniqkey.eu/scim`), and a section for generating a secret token. The secret token field contains a long alphanumeric string: `&4V4RT%.htqs2Ba!Z3CeWb3Ux&kleyw33op2s+5GuRIO#b(gCqWAb$qtQ8XrkpnGs`. A "Generate" button (highlighted with a red circle) is located at the bottom right of the secret token section.

- Copy the tenant URL and paste it into the corresponding field in Azure AD.
- To generate the secret token, click the "Generate" button.
- Add this token to the provisioning settings in Azure.



The screenshot shows the Azure AD provisioning settings form. It has two input fields: "Tenant URL" (with a red asterisk and help icon) containing `https://scim-integration.production.next.uniqkey.eu/scim` and a green checkmark, and "Secret Token" containing a masked token with dots. Below the fields is a "Test Connection" button.

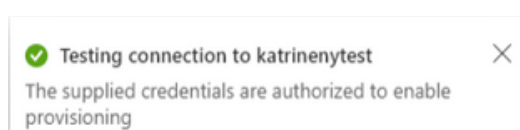
Instructions

8. Test Connection

- After adding the URL and token, click "Test Connection" to verify the link between your enterprise application and Uniqkey.

Test Connection

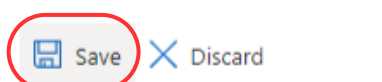
- A prompt will appear to confirm the connection.



9. Save Changes

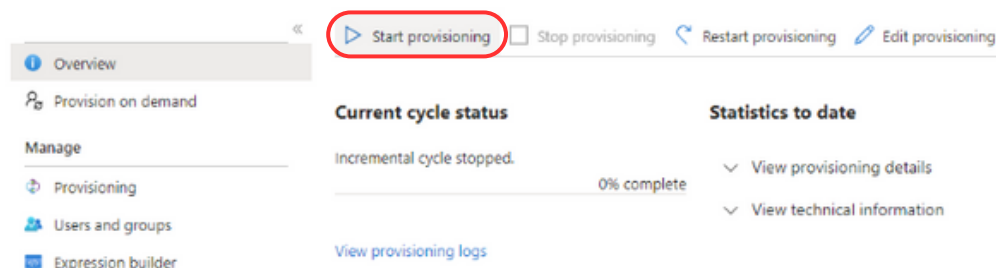
- Save the changes by clicking the button at the top of the screen.

Provisioning ...



10. Start Manual Provisioning

- Initially, manual start is required. Go back to the "Provisioning" tab and click "Start Provisioning."

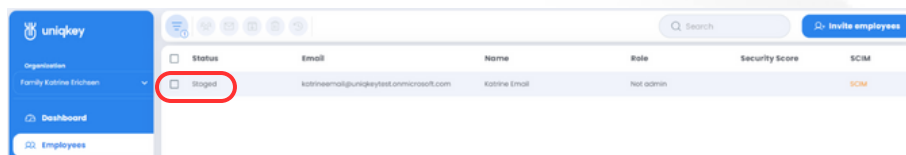


- A notification will appear indicating that provisioning will now run on a 45-minute schedule.

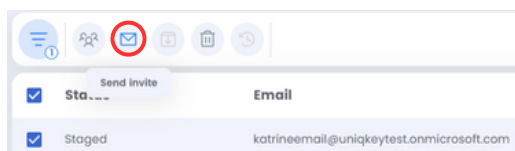


11. User Status and Invitations

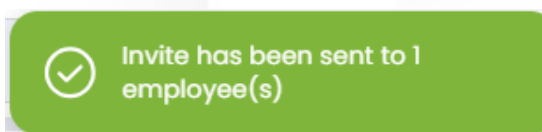
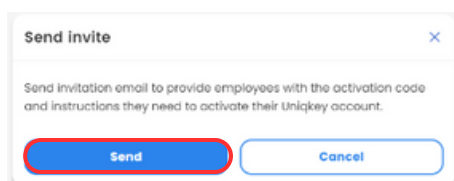
- Your assigned users and groups will now be provisioned to your Uniqkey admin portal.



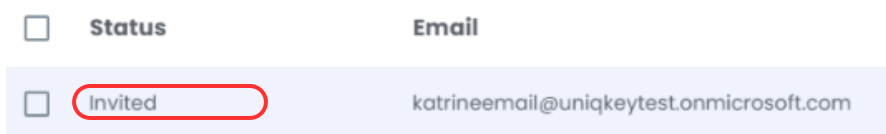
- They'll get the status "staged" which means they won't automatically receive an invitation email
- To send an invite, select the users and click the "Send Invite" button.



- Confirm the invitation by clicking "Send."



- Note: The email won't be sent until you've opened your Uniqkey mobile app. Upon doing so, the user's status will change to "Invited."



Troubleshooting:

If you're experiencing issues during this process, please refer to our Help Center or contact our support team at:

<https://uniqkey.zendesk.com/hc/en-gb> +45 71 96 99 67 support@uniqkey.eu