



Connect Azure Active Directory via SCIM

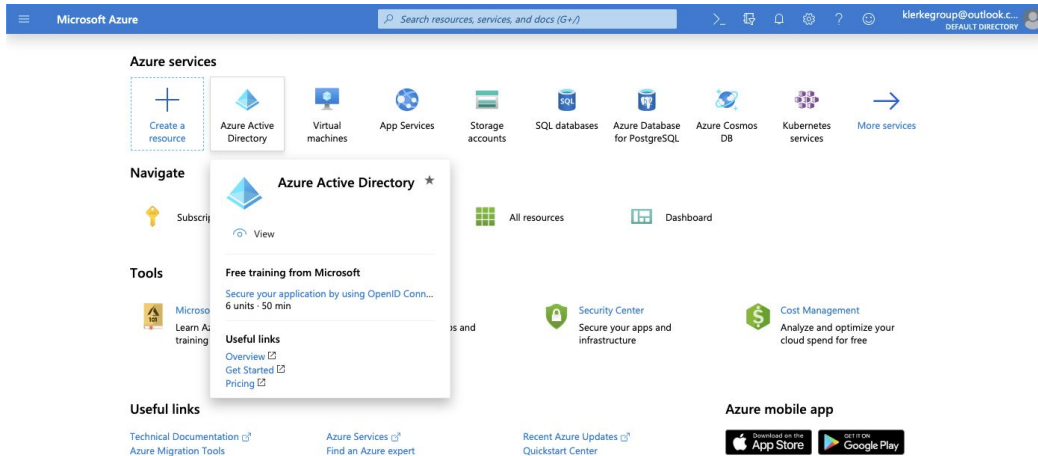
Uniqkey supports automatic provisioning of users using a SCIM connection between your user directory and Uniqkey. This guide shows how to connect Uniqkey and Azure Active Directory.

Preparation

During your PoC period, you might have used groups in Uniqkey. Groups from Azure Active Directory can be synced with the correct mapping between users and groups to Uniqkey. The important part is that if you already created similar groups in Uniqkey, you need to make sure that the name of the group in Uniqkey matches the group name in Azure Active Directory. When they match, users and groups will be synced and users will have access to any group accounts you have created during PoC.

Connecting Azure Active Directory and Uniqkey

1. Log into your Azure Active Directory Portal
2. Select Azure Active Directory:





3. Go to “Enterprise applications”, and click “New application”:

The screenshot shows the Microsoft Azure portal interface for "Enterprise applications - All applications". The left sidebar contains navigation options like Overview, Manage, Security, and Activity. The main content area shows a list of existing applications with columns for Name, Homepage URL, Object ID, and Application ID. A "New application" button is visible at the top left of the main area.

Name	Homepage URL	Object ID	Application ID
Office 365 Exchange Online	http://office.microsoft.com/outlook/	701a6ca4-a2bb-4bb5-855f-f70aefda0e11	00000002-0000-0ff1-ce00-0000...
Office 365 Management APIs		48b46b95-3a8a-41f6-8ae6-763003a84c0d	c5393580-f805-4401-95e8-94b...
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/	daedda6b-1e65-4e33-a193-d0fffc28b96e	00000003-0000-0ff1-ce00-0000...
Outlook Groups		a5054a71-d5b4-43b1-9198-b03e26958edb	925eb0d0-da50-4604-a19f-bd8...
Skype for Business Online		923833e7-e4ed-42ea-8f71-ad9529d138ca	00000004-0000-0ff1-ce00-0000...

4. Select “Non-gallery” application, put in “Uniqkey” as application name and click “Add”

5. Now the Uniqkey application has been created, and we can click on “Provisioning”:

The screenshot shows the "Uniqkey - Provisioning" page in the Microsoft Azure portal. The left sidebar shows navigation options like Overview, Deployment Plan, and Provisioning. The main content area shows the provisioning configuration for the Uniqkey application, including fields for Provisioning Mode, Admin Credentials (Tenant URL and Secret Token), and Mappings.

Provisioning Mode: Automatic

Admin Credentials

Tenant URL: [Input field]

Secret Token: [Input field]

Test Connection: [Button]

Notification Email: [Input field]

Send an email notification when a failure occurs:

Mappings

Settings

Start and stop provisioning to Uniqkey, and view provisioning status.

6. In here, we need to select “Automatic” in “Provisioning mode”, then we have to fill in a “Tenant URL” and a “Secret Token”. In order to get these for your company, you have to go to <https://app.uniqkey.eu> and scan the QR code with your Uniqkey app.



7. In the Uniqkey dashboard go to “Settings” and “Integrations”. In here you can generate and copy a SCIM token and a SCIM URL:

The screenshot shows the Uniqkey dashboard's 'Indstillinger' (Settings) page. The left sidebar contains navigation options: 'Overblik', 'VIRKSOMHED' (with sub-items 'Brugere', 'Grupper', 'Audit log', 'Services'), and 'KONTO' (with sub-items 'Profil', 'Log ud'). The 'Indstillinger' option is highlighted. The main content area is titled 'Indstillinger' and 'Opdater dine virksomhedsoplysninger'. It has three tabs: 'Information', 'Godkendt Browser', and 'Integrationer'. The 'Integrationer' tab is active, showing 'Virksomheds integrationer'. A sub-header reads 'Her kan du aktivere eller deaktivere dine integrationer'. Under 'SCIM integration', there is a 'SCIM Token' field with a 'Regenerer the SCIM token' button. Below the token field is a note: 'Hvis din SCIM token er tom, betyder det at SCIM integrationen er slået fra i øjeblikket'. The 'SCIM Uri' field contains the URL 'https://api.uniqkey.eu/scim/05f79d00-fc93-11e9-9388-df36fd166750/v2'. At the bottom, there is a 'Slack integration' section with a 'Log ind med Slack for at importere' button. The footer shows 'Uniqkey · Hjælp'.



- Go back to your Azure Active Directory from step 6 and insert the SCIM Token and SCIM URL and press save:

- Now Azure Active Directory is ready to sync, but we need to select who gets access. Under “Settings” select the users and groups that should get access and save.

After connecting Azure Active Directory and Uniqkey

Syncing from Azure Active Directory runs in 40 minutes intervals, so it might take a little time before users start showing up in the Uniqkey dashboard. Once synced, the Azure Active Directory users will receive an email with an activation code that should be entered in the Uniqkey app to finish setup of the Uniqkey account. Once activated and if the user is a member of a group, they will be awaiting the admins sending them an encryption key. This happens automatically in the background when an admin opens his Uniqkey app. Therefore we advise admins to open their app a couple of times a day so that the encryption key will be sent to awaiting users.