Connect Azure Active Directory via SCIM

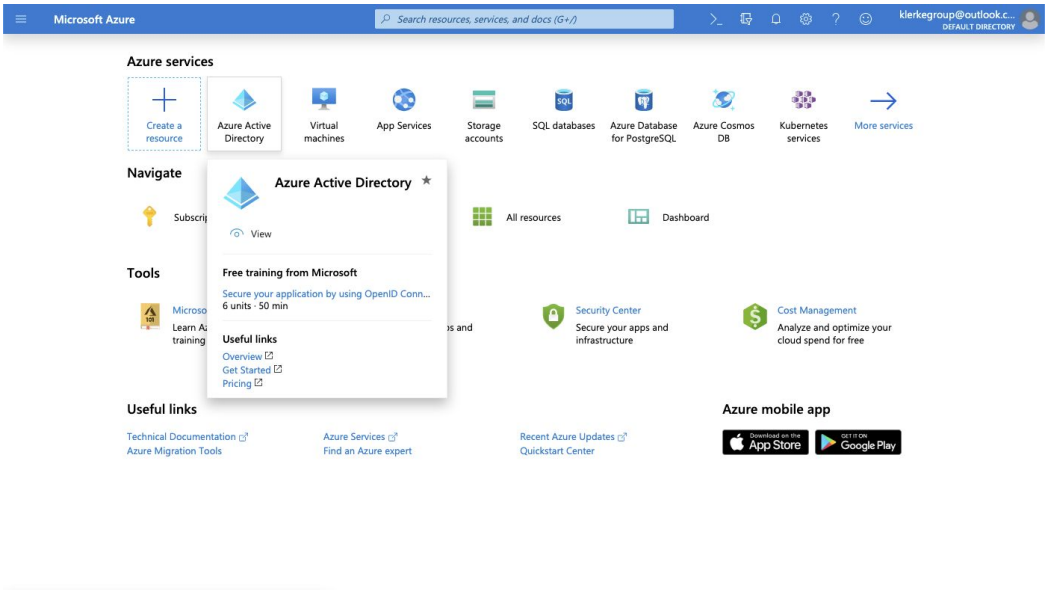
Uniqkey supports automatic provisioning of users using a SCIM connection between your user directory and Uniqkey. This guide shows how to connect Uniqkey and Azure Active Directory.

Preparation

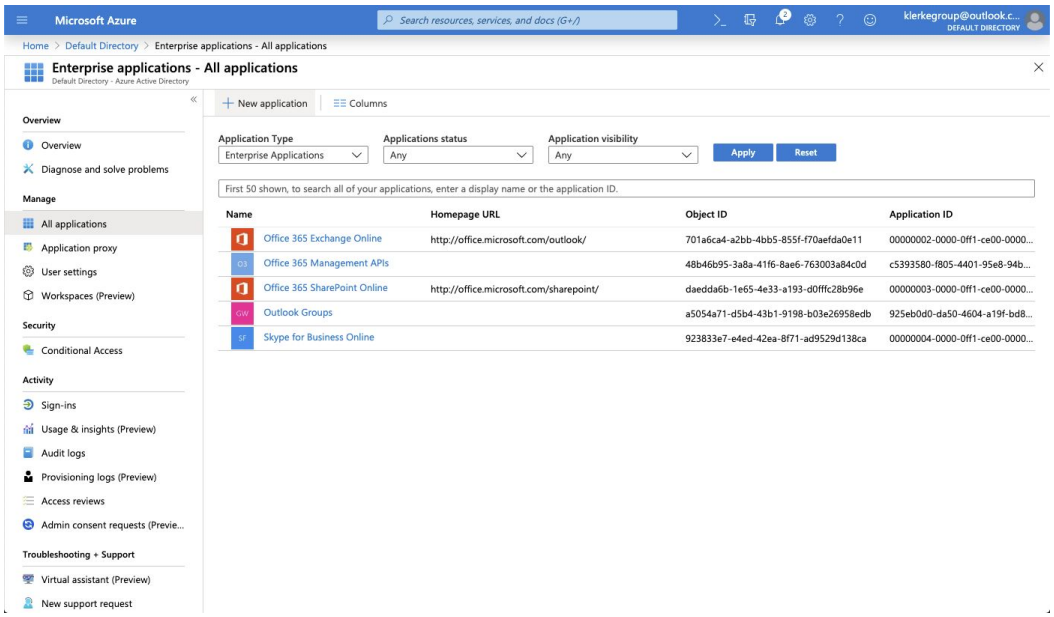
During your PoC period, you might have used groups in Uniqkey. Groups from Azure Active Directory can be synced with the correct mapping between users and groups to Uniqkey. The important part is that if you already created similar groups in Uniqkey, you need to make sure that the name of the group in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

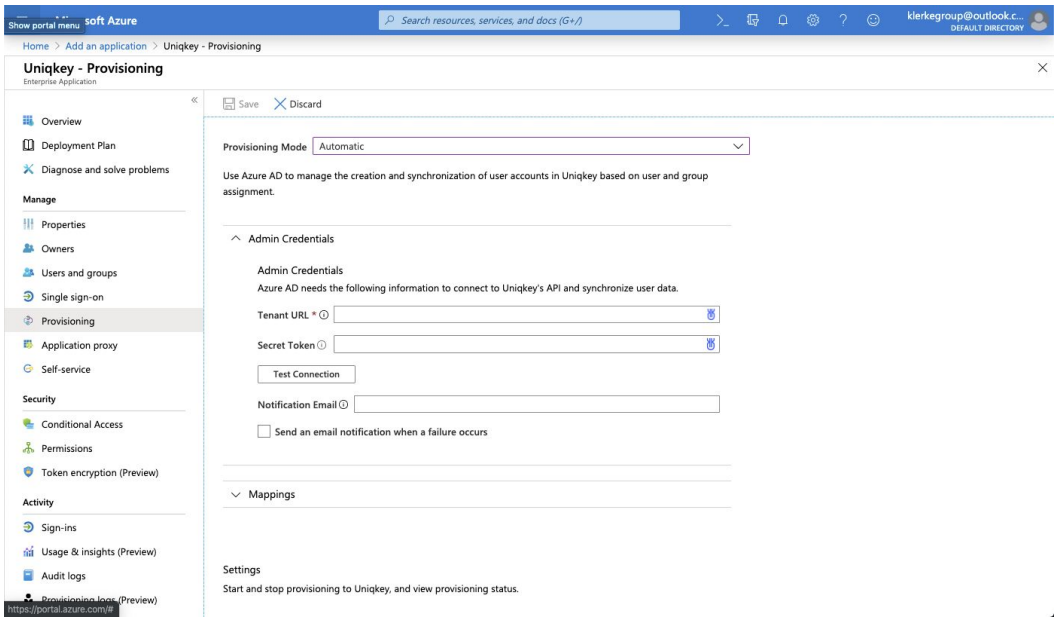
1. Log into your Azure Active Directory Portal
2. Select Azure Active Directory:



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

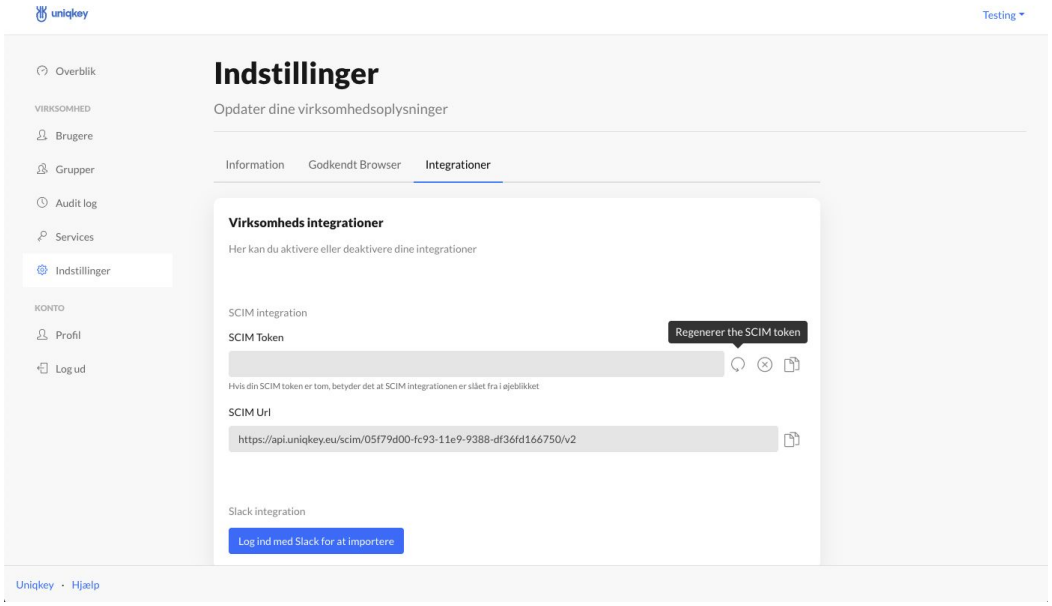


4. Select “Non-gallery” application, put in “Uniqkey” as application name and click “Add”
5. Now the Uniqkey application has been created, and we can click on “Provisioning”:

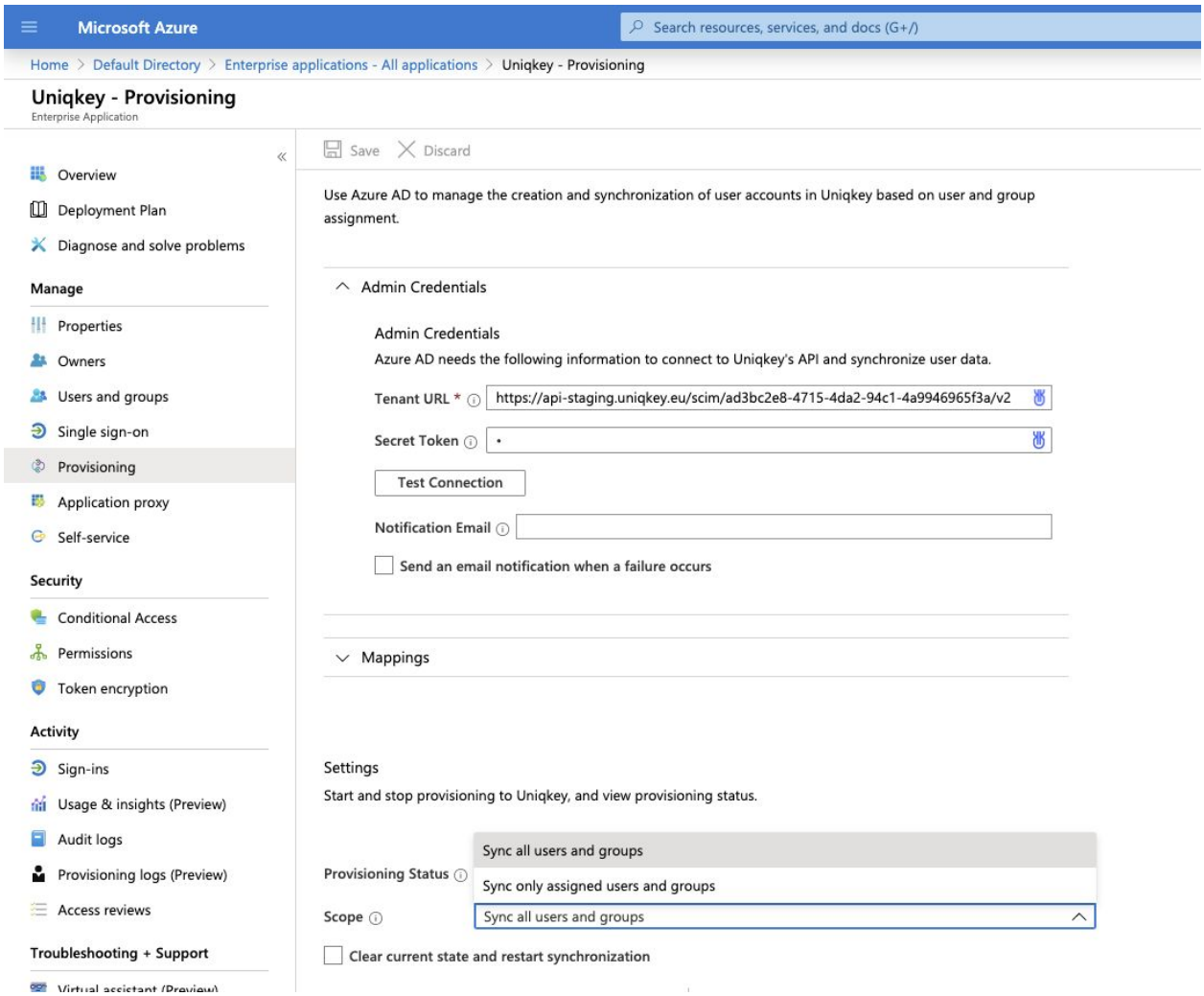


6. In here, we need to select “Automatic” in “Provisioning mode”, then we have to fill in a “Tenant URL” and a “Secret Token”. In order to get these for your company, you have to go to https://app.uniqkey.eu and scan the QR code with your Uniqkey app.

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



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



9. 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.