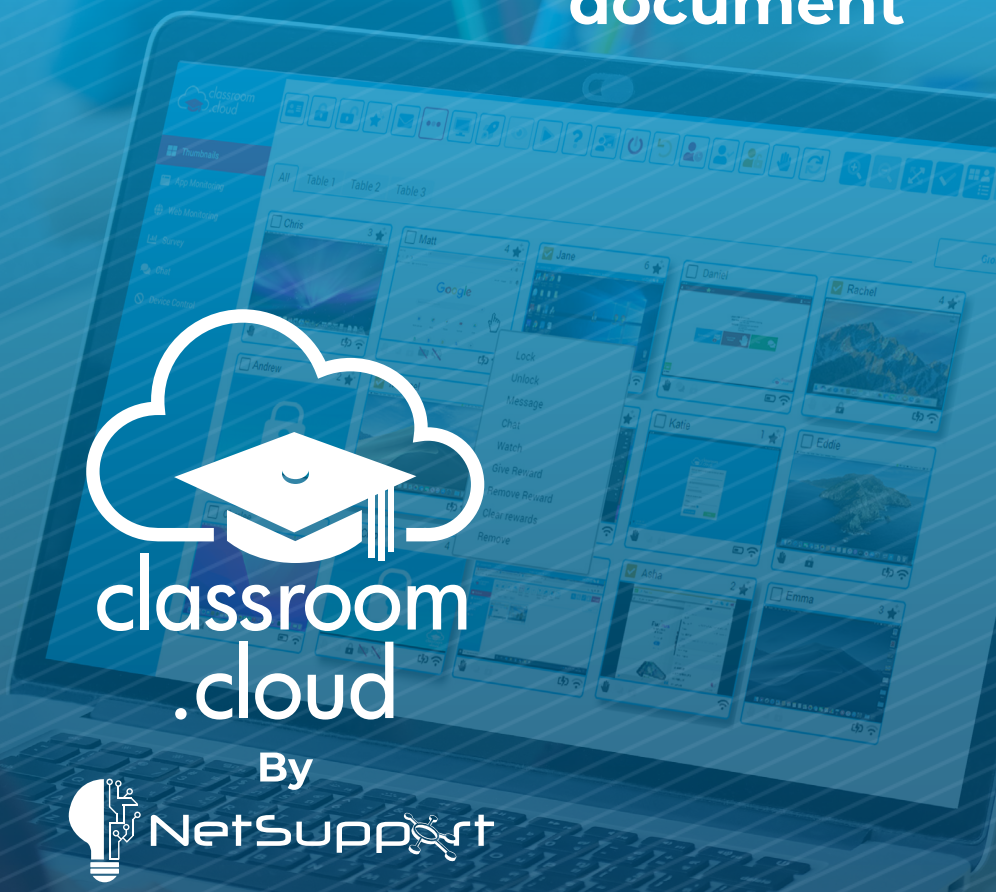
Technical document



classroom.cloud

By NetSupport

Setting up Entra User Provisioning (SCIM)

Guide to setting up Entra user provisioning (SCIM)

Thanks to the various ways **classroom.cloud** can be configured to integrate with third-party user management/SIS systems, enrolling users into **classroom.cloud** to mirror your existing environment is a quick and seamless process.

This includes the ability to use the SCIM (System for Cross-domain Identity Management) capabilities of Microsoft Entra to auto-provision users into **classroom.cloud**.

We hope this guide gets you up and running with user provisioning without any problems, but if you do need any additional assistance, our Support team are on hand to help. Email support@classroom.cloud.

1. Ensure you have a **classroom.cloud** account with Organization Admin rights and a Microsoft tenant where you have the permissions to create and edit enterprise apps in Entra.
2. Go to https://portal.azure.com/, navigate to **Microsoft Entra ID** and then **Enterprise applications**.
3. Click **New application** and then click **Create your own application**. A menu will appear, enter a name for the new application (for example, **classroom.cloud** test environment user provisioning, this is just for your Microsoft tenant, so it doesn't affect anything outside of your tenant) and make sure the bottom option (**Non-gallery**) is selected. Click **Create**. This will create a new enterprise application for you (it may take a minute).
4. Once your enterprise application has been created, navigate to it (if it hasn't done so automatically) and click the **Provisioning** option on the left-hand side. Click the **Get Started** button.
5. Change the Provisioning Mode to **Automatic** and enter the details below:
    a. Tenant URL https://userprovisioning-uksouth.classroom.cloud/scim/

    Note: The trailing slash is important! (Substitute UKSouth for your region, the URL can be found in the Microsoft Integrations tab within **classroom.cloud**.)

    b. Navigate to **classroom.cloud** and sign in as an Organization Admin. Go to **Settings** > **Integrations** > **Microsoft** and select the User Provisioning tab.
    c. Click **Generate**.
    d. Click **Copy** to copy the token to your clipboard.

Note: The secret token may expire while you are testing the Provision on Demand feature within Entra. If this does happen, you will get an unauthorized error. This can be rectified by generating a new token in **classroom.cloud**.

e. Return to portal.azure.com and paste the token into the correct box.

6. Click **Test Connection** and you should be advised that the provided details were accepted – it may take a moment or two. Click **Save** at the top of the page.
7. Once you have clicked **Save**, the screen will update with more options. Click the **Mappings** drop-down menu and select **Provision Entra ID Users**.
8. Scroll down to the bottom of the page and check the **Show advanced options** button. At the bottom of the options, click the **Review your schema here** link.
9. Download the schema from **classroom.cloud Settings** > **Integrations** > **Microsoft** > **User Provisioning**.
10. Select all the text in the Schema editor in Entra and delete it. Then, open the schema for **classroom.cloud** that you downloaded and copy and paste the text into the Schema editor.
11. Click the **Save** button at the top of the screen. At this point, it may be best to press CTRL and F5, as this refreshes the page and any cache associated with it.
12. You now need to go back to the top level of Entra (you can click the Home breadcrumb at the top of the page) and navigate back to the app (**Entra ID** > **Enterprise applications** > [**App name**] > **Provisioning**).
13. This screen will now look different to when you initially started provisioning. Click on **Edit Provisioning** at the top and navigate to **Mappings** > **Provision Entra ID Users**.
14. The new mapping of fields will be completed and should look like this:

Attribute Mappings

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

Azure Active Directory Attribute	customappsso Attribute	Matching precedence	Remove
mail	emails[type eq "work"].value	1	Delete
objectId	externalId		Delete
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active		Delete
givenName	name.givenName		Delete
surname	name.familyName		Delete
jobTitle	title		Delete
en-GB	locale		Delete
telephoneNumber	phoneNumbers[type eq "work"].value		Delete

15. Go back one level (clicking **Provisioning** on the breadcrumb will take you to the correct place). Under the Settings area, feel free to add an email for notifications. See below if you want to set up Entra Groups to assign users to the app. Otherwise, change the Scope setting here to **Sync all users and groups**. Click **Save** once you have made any changes here.

    Setting up groups

    a. Go to the top level of Entra ID and click **Groups** on the left-hand side.

    b. Click **New group**. Keep the group as a Security group and give the group a name. You can also assign any members to the group at this point. Once you have done this, click **Create** at the bottom of the page. You can create as many groups as you would like.

    c. Once your groups have been set up, go to the top level of Entra ID and navigate back to your enterprise app. Here, click **Users and groups** on the left-hand side. Click the **Add user/group** button and find the group(s) that you created. This will now allow any users within groups here to be provisioned.

16. Navigate back to the Provisioning top menu (clicking the [**App name**] | **Provisioning** part of the breadcrumb will take you to the correct place). Don’t worry if your browser warns you of unsaved changes.

17. Click **Provision on demand**. Here, select any user (not your Organization Admin at the current time) and click **Provision** at the bottom of the screen. If everything has

worked, this will come back successful. If you want to provision more users, we recommend using the Groups feature mentioned in step 15. Once this is set up, you can navigate to the Provisioning top menu and click **Start provisioning**.

18. Before your provisioned users can sign in to **classroom.cloud**, you need to create rule (s) within the **classroom.cloud** portal for site/role assignment. You can have different rules for different groups of users, e.g. to provide access to different sites or roles.

    a. In the **classroom.cloud** Web Portal, select **Organization** > **Settings** > **User Provisioning**.

    b. Select **Add user assignment rule**.

    c. Give the rule a name.

    d. Select the site(s) that you want to give the user access to.

    e. Select the role(s) that you want to assign to the users.

    f. Select whether "all" or "any" of the following conditions need to apply to match the users to the rule.

    g. Add a condition, for example, "Microsoft Entra Group ID" "Equals" and enter the Group Object ID from Entra or "Microsoft Entra User ID" "Equals" and enter the user's Entra Object ID to target an individual user.

    h. If required, you can add additional conditions to the rule.

    i. Click **Save**.

19. Provisioned users can now sign in to **classroom.cloud**.

Note: Provisioned users will initially appear in the **classroom.cloud** Web Portal without their user role or site specified. It is not until they sign in to **classroom.cloud** for the first time that your provisioning rules will be evaluated and the appropriate access granted.