Set up account provisioning (SCIM)

Let your identity provider add people to Ovation, keep their details current, and turn off their access when they leave.

For organization administrators and the identity team that manages your directory. You need the organization administrator role in Ovation and an administrator for your identity provider.

What provisioning does

SCIM is the standard identity providers use to keep other services' accounts in step with their directory. Once you connect it, your provider tells Ovation whenever something changes:

You assign someone	Ovation adds them to your organization, or links the member who already has that email. New members get the **Default** role, **Full** access, and every Ovation app, which you can change in Ovation. Ovation doesn't email them.
You change their details	Ovation updates their first name, last name, and sign-in email to match.
You unassign or deactivate them	Ovation turns off their access right away, ending any open session, and keeps their recordings and reports. Assigning them again brings back the same account and work.
You push a group	With **Provision groups** on, Ovation creates a group with the same name and keeps its members in step. Groups don't grant roles.

SCIM doesn't sign anyone in. People it adds usually sign in through single sign-on (SSO); see Set up single sign-on (SSO). Unless you require SSO, they can also sign in with a one-time email link or create a password.

BEFORE YOU BEGIN

Before you start

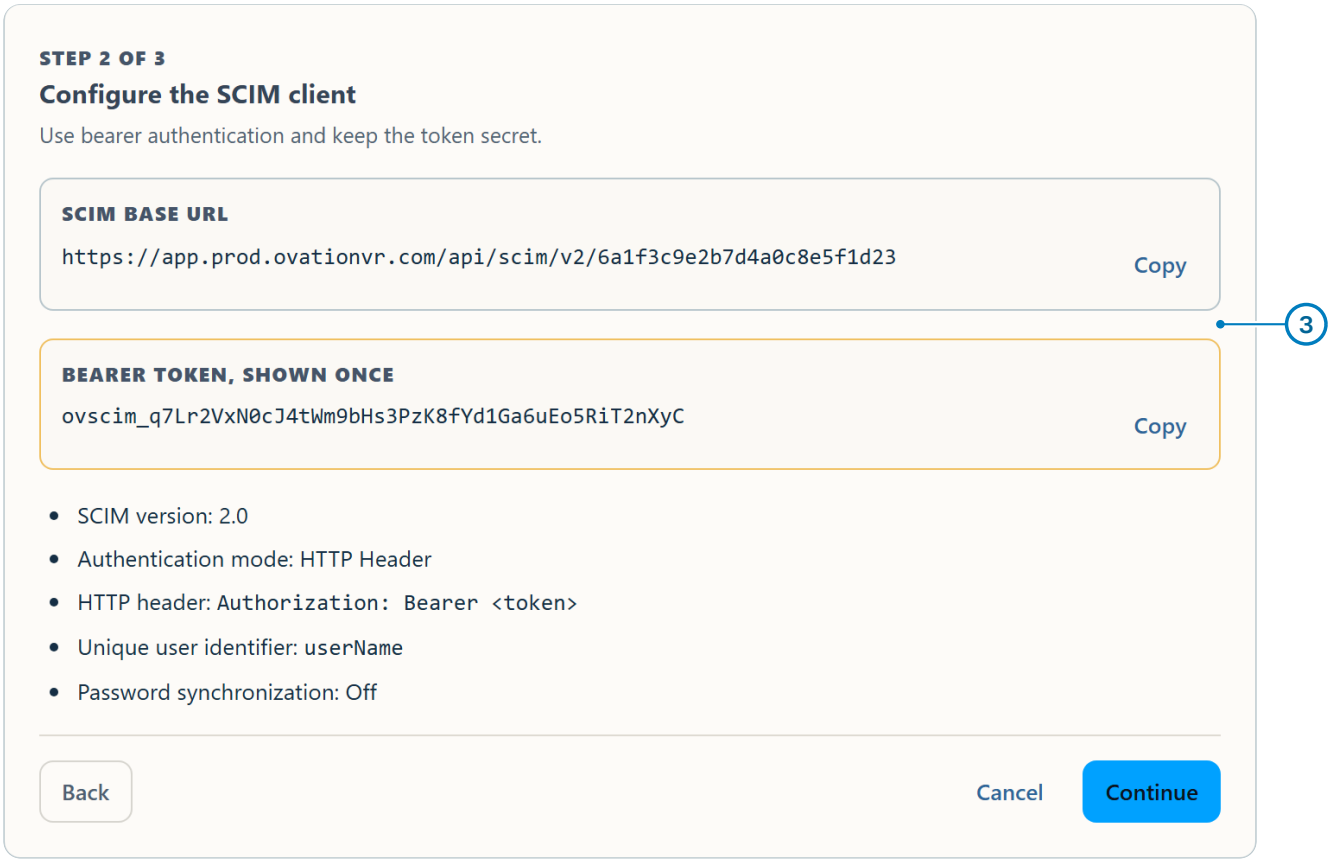
- [ ] You can sign in as your organization's administrator, the only account that can open the **Provisioning** tab.
- [ ] Someone on your identity team can set up SCIM provisioning in your provider. Any SCIM 2.0 client works, including one that isn't your SSO provider.
- [ ] Each person's SCIM **userName** is their work email, the same address your SSO provider sends. Ovation matches people by it.
- [ ] One pilot person is ready to assign, plus a small test group if you'll provision groups.

STEP 1

Add the SCIM connection

Go to **Organization › Settings › Provisioning**

1. Select **Add SCIM**. Enter a **Connection name** that identifies the system sending changes, such as your directory's name.
2. Select **Provision groups** if your directory should also create groups in Ovation and keep their members in step. Then select **Continue**.
3. Copy the **SCIM base URL** and the bearer token into your provider's provisioning settings, described below. Ovation shows the token only this once, so also save it in your password manager.



4. Select **Continue**, check the settings, and select **Finish** to turn the connection on. Its card shows **Waiting for request** until your provider sends its first request.

The token works like a password for this connection: anyone who has it can add, change, or turn off your members. If it is ever exposed, select **Replace token** on the connection card.

STEP 2

Set up your provider

Enter these settings in the provisioning setup of the Ovation application in your provider. Step 2 in Ovation lists them too.

Setting	Value
SCIM version	2.0
Base URL	The **SCIM base URL** from Ovation. Okta calls it **SCIM connector base URL**; Entra calls it **Tenant URL**.
Authentication	HTTP header **Authorization: Bearer** followed by the token. If your provider already shows the word Bearer, paste only the token.
Unique user identifier	**userName**, set to each person's work email. If your provider also sends a work email address, it must be the same address.
What to send	Create users, update user attributes, and deactivate users. Push groups only if **Provision groups** is on.
Password sync	Off. Ovation doesn't accept passwords from your provider.

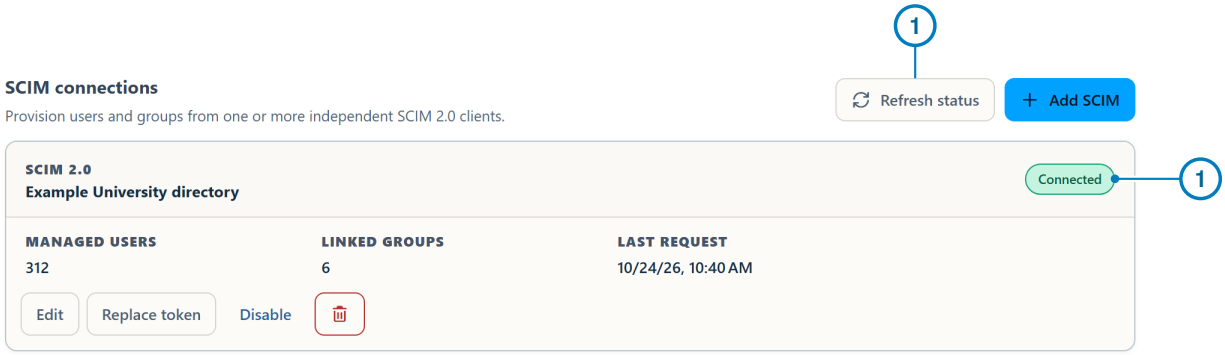
Provider	Where the settings go
Okta	In the Ovation app integration, on **General** > **App Settings**, set **Provisioning** to **SCIM** and save. On **Provisioning** > **Integration**, enter the settings, choose **Push New Users**, **Push Profile Updates**, and for groups **Push Groups**, then select **Test Connector Configuration** and save. Under **To App**, turn on **Create Users**, **Update User Attributes**, and **Deactivate Users**.
Microsoft Entra ID	In the enterprise app, open **Provisioning**, start a new configuration, and choose **Automatic**. Enter the base URL as **Tenant URL** and the token as **Secret Token**, then select **Test Connection**. Under **Attribute Mapping** > **Users**, map both userName and emails[type eq "work"].value to userPrincipalName, or to mail if that is the person's Ovation email. Set the scope to **Sync only assigned users and groups** and start provisioning.
Others	Use the same settings, and send one test person before scheduling regular syncs.

Entra sends changes on a schedule, about every 40 minutes, and its first cycle can take longer. To check one person right away, use **Provision on demand**.

STEP 3

Test with a pilot person

1. Send a test request from your provider, such as Okta's connector test or Entra's **Test Connection**. In Ovation, select **Refresh status**. The card shows **Connected** once a request arrives with the current token.



Connected means a request arrived; it doesn't show that anyone was created. Check each of these with your pilot person before you assign everyone. The **SCIM provisioning** column on the Members page shows **Active**, **Inactive**, or **Not managed** for each member.

In your provider	What you should see in Ovation
Assign the pilot person	They appear on **Members** with their work email and **Active** under **SCIM provisioning**. If they were already a member, it's the same member with the same role and work, not a second account.
Change their name	The new name shows in Ovation after your provider's next update.
Push a test group	A group with the same name and members appears on the Groups page, marked **Directory managed**.
Unassign them	**SCIM provisioning** shows **Inactive**. If they try to sign in, Ovation tells them your organization has deactivated the account, and the Web App shows **Your access has been turned off**.
Assign them again	**Active** again. They can sign in and practice, and their earlier work is still there.

If a check fails, correct the mapping in your provider and run that check again before you assign more people.

Working with provisioned members

Removing someone	Ovation won't remove a member SCIM manages while they're **Active**. Unassign them in your provider; once they show **Inactive**, remove them on the Members page as usual.
Keeping someone	To keep an **Inactive** person but manage them in Ovation instead, choose **Release from SCIM** in their row's menu on **Members**. They can then sign in with the methods your organization allows.
Pausing access	Your provider's updates can clear pause and removal dates you set in Ovation for a member SCIM manages. Turn their access off in your provider instead.
Administrators	SCIM can deactivate your administrator account too, which locks it out of Ovation. Keep the administrator assigned in your provider.
Groups	Change the name and members of a **Directory managed** group in your provider. You can still assign work to it, but people who join the group later don't receive work you assigned earlier. Deleting the group in your provider archives it in Ovation.

Manage the connection

Go to **Organization › Settings › Provisioning**

Refresh status	Updates the card's status: **Waiting for request**, **Connected**, or **Disabled**.
Replace token	Creates a new token and stops the old one immediately. Copy the new token into your provider and send a test request; the card shows **Waiting for request** until one arrives.
Edit	Rename the connection, or turn **Provision groups** on or off.
Disable	Stops accepting requests from your provider and turns **Provision groups** off. Members keep their current status, so people SCIM turned off stay off. After you select **Enable**, turn groups back on with **Edit**.
Delete	Deletes the token and Ovation's record of which members and groups SCIM manages. Accounts and work stay, but every member it managed becomes a regular member: people it had turned off can sign in again, and its groups become editable.
Add another	You can add a connection for each system that sends changes. Each person can be managed by only one connection at a time.

If something goes wrong

What's happening	Likely cause and what to do
There is no **Provisioning** tab	Only your organization's administrator can open **Settings**. If that's you, contact Ovation.
The card stays on **Waiting for request**, or your provider reports a bearer token error	No request has arrived with the current token. Check the base URL and the token after **Authorization: Bearer**, send a test request, and select **Refresh status**.
Your provider reports that SCIM or group sync is not enabled	The connection is disabled, or **Provision groups** is off. Select **Enable**, or turn on **Provision groups** with **Edit**, then send the change again.
A user with this email already exists	The email belongs to someone in another Ovation organization or to a personal Ovation account. Contact Ovation to resolve it.
A group push fails because an Ovation group already uses the name	Ovation never takes over a group you created in Ovation. Rename one of the two groups, then push again.
Connected, but people don't appear	Check that they're assigned to the application and in your provider's provisioning scope, and that provisioning has started.
A provisioned person can't sign in through SSO	The email your SSO provider sends must match their SCIM **userName** exactly. Check both mappings use the same directory field.

Need help?

For setup help, contact Ovation support with your organization, the connection name, your provisioning system, the affected person's email, and when the request failed. Never send the bearer token.