

Auto Provisioning with ZoomInfo and Microsoft Entra ID Integration Guide

For administrators setting up ZoomInfo SCIM auto provisioning using Microsoft Entra ID

Prerequisites	2
Configuration Overview	3
Step 1: Configure Groups in Microsoft Entra ID	3
Step 2: Create Subscription Sets in the ZoomInfo Admin Portal	5
Troubleshooting	8

This guide describes how to configure **System for Cross-domain Identity Management (SCIM) 2.0** auto provisioning for ZoomInfo applications using **Microsoft Entra ID**.

- **About Microsoft Entra ID**

Microsoft Entra ID, formerly known as **Azure Active Directory (Azure AD)**, is a cloud-based identity and access management (IAM) solution that helps organizations secure and manage identities for both cloud and on-premises resources.

- **About SCIM 2.0**

SCIM 2.0 is an Internet Task Engineering Force (IETF) standard for transmitting digital identity data between domains.

Prerequisites

Set Up Single Sign-On (SSO) Using Entra ID

SCIM auto provisioning requires an existing Single Sign-On (SSO) configuration using Microsoft Entra ID as the Identity Provider (IdP). See [Single Sign-On Setup for Common Identity Providers](#) for details on setting up a ZoomInfo SSO configuration with Microsoft Entra ID.

Assign Responsibility for Refreshing API Tokens

ZoomInfo's auto provisioning configuration requires that the API token used to authenticate the SCIM connection be periodically refreshed by a ZoomInfo admin.

- When setting up or refreshing your API token, you'll need to choose a token expiration option (90 days, 180 days, or 1 year).
- All configured ZoomInfo admins for your organization will receive notifications (email and in-app) starting approximately 1 month before expiration.
- An admin can choose to refresh the token proactively at any time.
- The expiration of the token will not impact existing provisioned users. However, new subscription groups cannot be created, and provisioning activities cannot occur until the token is refreshed.

Configuration Overview

Auto provisioning in Entra ID involves two main steps:

1. Create Group(s) in Entra ID: In Microsoft Entra ID, create one or more groups that align with how you plan to allocate ZoomInfo product seats. This process follows the standard group configuration for user management in Entra ID.

2. Create Subscription Sets in the ZoomInfo Admin Portal: Select Entra ID (Azure) as your IdP in the Admin Portal and configure one or more subscription sets linked to the Entra ID groups created.

After the initial sync, ZoomInfo product seats will be automatically provisioned as users are added or removed from the designated Entra ID groups.

Step 1: Configure Groups in Microsoft Entra ID

A Microsoft admin establishes one or more groups in Entra ID that contain members that correspond to ZoomInfo product seats.

Microsoft Documentation

Our auto provisioning setup uses standard Entra ID groups that contain users to be provisioned for one or more ZoomInfo products. For important concepts and step-by-step configuration details refer to the [Microsoft documentation](#). Additional ZoomInfo-specific considerations are noted in this guide.

In this guide, we'll include any additional information specific to the ZoomInfo configuration (for example, [Attribute Mappings](#)).

Group Naming Convention

To set up this solution, a group name in Entra ID must meet the following criteria:

Facet	Description
Minimum length	3
Maximum length	35
Allowed characters	[a-zA-Z0-9\.\-\s]+\$

Example Scenarios

Important: Before you create groups, note that a user cannot exist in more than one group. If a user needs to be licensed across multiple products, create groups that accommodate the situation as described in the examples below.

Single product scenario: If your organization has one ZoomInfo product (for example, ZoomInfo Sales) you could create two groups:

- *Sales Team* containing your Sales users.
- *ZoomInfo-Admins* containing admins that need access to the ZoomInfo Admin Portal and the Sales product.

Multiple product scenario: If your organization has both ZoomInfo Sales and ZoomInfo Marketing, you could set up two groups:

- *Sales Team* for your Sales users, and *Marketing Team* for Marketing users.
- If you have users of both products, you could set up a third group called *Sales-Marketing-Team*.
- You could also set up a fourth group called *ZoomInfo-Admins* containing admins that need access to the ZoomInfo Admin Portal and multiple products.

User Attribute Mappings

Attribute mappings define how user attributes are synchronized between Microsoft Entra ID and ZoomInfo.

Microsoft Documentation

Refer to the following Microsoft documentation:

- [Conceptual information on mapping attributes](#)
- [Customize user provisioning attribute-mappings for SaaS applications in Microsoft Entra ID](#)

Customize User Provisioning Attribute Mappings

There is a preconfigured set of attributes and attribute mappings between Microsoft Entra user objects and a SaaS app's user objects. You only need a subset of these mappings for the auto provisioning to function for ZoomInfo.

Here are the attribute mappings needed for ZoomInfo:

Attribute Mappings	
customappsso Attribute	Microsoft Entra ID Attribute
userName	userPrincipalName
active	Switch([IsSoftDeleted], , "False", "True", "True", "False")
emails[type eq "work"].value	mail
name.givenName	givenName
name.familyName	surname
externalId	objectId
Add New Mapping	

To customize the attribute mappings for ZoomInfo:

1. Remove any attribute mappings not shown in the image above.
2. By default, the *externalId* attribute is mapped to *mailNickname*. Update the mapping so that the *externalId* attribute is mapped to *objectId*.

Once your group(s) and attribute mappings are in place, you can create corresponding subscription set(s) in the ZoomInfo Admin Portal.

Step 2: Create Subscription Sets in the ZoomInfo Admin Portal

Create subscription sets in the ZoomInfo Admin Portal to link the members of a group with a specific ZoomInfo product license type.

Using the example above, you would create four subscription sets: *Sales Team*, *Marketing Team*, *Sales-Marketing Team*, and *ZoomInfo Admins*.

To create a subscription set:

1. In the ZoomInfo Admin Portal, go to **User Management > Users > Auto Provisioning**.
2. Select the **IdP** tab.

CRM IdP

IdP Auto Provisioning

Auto Provisioning allows user management via your identity provider (IdP). Once set up, you can see user provisioning status on the [User Management](#) page. See the [instruction guide](#) to learn more.

Note: Okta and Azure are currently the only IdPs supported for Auto Provisioning

IdP Type

Connect your IdP

API Token

Base URL

Create Subscription Groups

You must assign subscription groups for users you are auto provisioning using Azure.

Manage Users through IdP ☐

When turned on, ZoomInfo users are then managed through your IdP. User Management within ZoomInfo will then only show user sync status. You can choose to turn Auto Provisioning off or on at any time.

Once SCIM client app successfully connects to SCIM service, user Auto Provisioning will automatically turn on for the first time.

- For **IdP Type**, select **Azure** and click **Select**.
- Select a token expiration option (**90 days**, **180 days**, **1 year**) and click **Generate New API Token**. All admins configured for your organization will receive reminders to generate a new token as the expiration date approaches.

Generate New API Token

For improved security, this provisioning method requires setting an expiration for the API token expiration. You'll receive reminders to extend this about 1 month prior to expiration.

API Token will expire in:

☐ 90 days ☐ 180 days ☒ 1 year

Generating a new API Token will invalidate the previous Token. If you delete this API Token, you will have to add a new API Token to your IdP settings again.

☐ I understand and would like to proceed anyway

The **API Token** and **Base URL** for your Microsoft Entra ID Provisioning (SCIM) configuration is auto-populated on the page.

- Under **Create Subscription Sets**, click **Create Set**. Provide the following:

- Subscription Set Name
- Description
- Select one or more products

- Optionally, select **Give Admin role permissions to all users in this set**. This is a useful option if you're creating an admin-only group.

- Click **Save Set**.

Each subscription set that you configure will undergo some processing to ensure that the users are sync'd between Entra ID and ZoomInfo.


The 'Create Subscription Set' dialog box contains the following fields and options:

- Subscription Set Name (35 characters max):** NA Sales Team
- Description (45 characters max):** North American Sales Team
- Select the subscriptions you would like to provision for this set:**
 - ☐ Marketing
 - ☒ Sales
 - ☐ Talent
- ☐ Give Admin role permissions to all users in this set

Buttons: Cancel, Save Set

Create Subscription Sets					
Subscription Sets 1		Search subscription sets		+ Create Set	
Name	Description	Last Synced	Created	Modified	Actions
NA Sales Team	North American Sales Team	UnSynced	PA Nov 8, 2024		...

- Once processing is complete, ensure that auto-provisioning through Entra ID for your organization is enabled by the **Manage Users through IdP** toggle.

Manage Users through IdP ☒ 

When turned on, ZoomInfo users are then managed through your IdP. User Management within ZoomInfo will then only show user sync status. You can choose to turn Auto Provisioning off or on at any time.

Once IdP is processed and subscription sets are created, user Auto Provisioning will automatically turn on for the first time

As users are added to or removed from Entra ID groups, our system automatically assigns or revokes seats based on the changes.

Troubleshooting

- **Provisioning errors:** If you encounter any issues during provisioning, the system will display error messages that identify why users may not have been provisioned successfully. These error messages can help you troubleshoot any problems with the provisioning process.
- **Subscription group naming:** Subscription group names in ZoomInfo must exactly match the subscription group created within the SCIM client to ensure proper syncing
- **Available seats:** You must have sufficient available seats for the users you're attempting to provision
- **Token refresh requirement:** The API token must remain active to ensure proper provisioning and de-provisioning capabilities