How-To Library

Informatica

Setting up SCIM with Azure Active Directory

Abstract

Informatica Intelligent Cloud Services℠ user provisioning through SCIM 2.0 is available through Azure Active Directory (AD). This article provides instructions for setting up SCIM-based user and group sync for Azure AD.

Supported Versions

- Informatica Intelligent Cloud Services November 2024

Table of Contents

Overview

Informatica Intelligent Cloud Services℠ user provisioning through SCIM 2.0 is available through Azure Active Directory (AD). If you are an Informatica Intelligent Cloud Services organization administrator, you can set up SCIM-based user and group sync for Azure AD. To do this, you must create an Azure provisioning application to sync your Azure AD users and groups with Informatica Intelligent Cloud Services.

Note: If you do not use SCIM, follow the setup instructions in this Knowledge Base article instead.

To set up SCIM with Azure AD, complete the following tasks:

1. Create a provisioning app in Azure AD.
2. Set up SAML and enable SCIM in Informatica Intelligent Cloud Services.
3. Integrate the provisioning app with Informatica Intelligent Cloud Services.
4. Provision Azure AD users.
5. Provision Azure AD groups.
6. Start the provisioning cycle in Azure AD.
7. Map SAML roles and groups in Informatica Intelligent Cloud Services.
8. Verify provisioning in Informatica Intelligent Cloud Services.

Step 1. Create a provisioning app in Azure Active Directory

Create an app in Azure AD to provision users and groups in Informatica Intelligent Cloud Services.

1. Sign into Azure AD as an administrator and select **Azure services** > **Enterprise Applications**.
2. Select **New application** > **Create your own application**.
3. Enter a name for the app, select **Integrate any other application you don't find in the gallery**, and click **Create**.
4. In the left panel of the app, select **Single Sign On** and select **SAML**.
5. On the **Set up Single Sign-On with SAML** page, configure the following settings, and then click **Save**:

Set up Single Sign-On with SAML

Read the configuration guide ☐ for help integrating Test.

① Basic SAML Configuration   ✎ Edit

Identifier (Entity ID)	**Required**
Reply URL (Assertion Consumer Service URL)	**Required**
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

| Setting	Value
Identifier (Entity ID)	https://<organization ID>.<hostname> For example, `https://12a3b4cdef5gh67ijklm8n.dm-us.informaticacloud.com/`
Reply URL (Assertion Consumer Service URL)	<IICS base URL>/identity-service/acs/<organization ID> For example, `https://dm-us.informaticacloud.com/identity-service/acs/12a3b4cdef5gh67ijklm8n`
Sign on URL	<IICS base URL>/ma/sso/<organization ID> For example, `https://dm-us.informaticacloud.com/ma/sso/12a3b4cdef5gh67ijklm8n`

You do not need to configure the **Relay State** or **Logout Url** here.

6. On the **User Attributes & Claims** page, configure the attributes that you want to sync through the SAML token such as givenname, surname, and emailaddress.

② User Attributes & Claims   ✎ Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

7. If you want to sync groups, create a group claim which sends the group external ID in the SAML response.
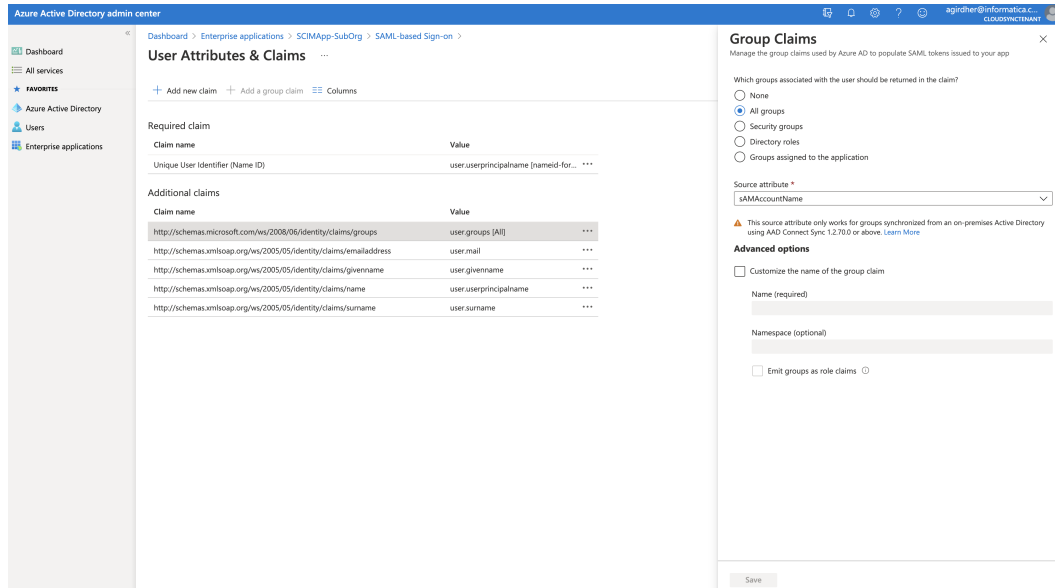
Note: App roles are sent in the SAML token by default, so you don't have to create a claim for roles.

8. On the **SAML Signing Certificate** page, download the service provider metadata file as an XML file.
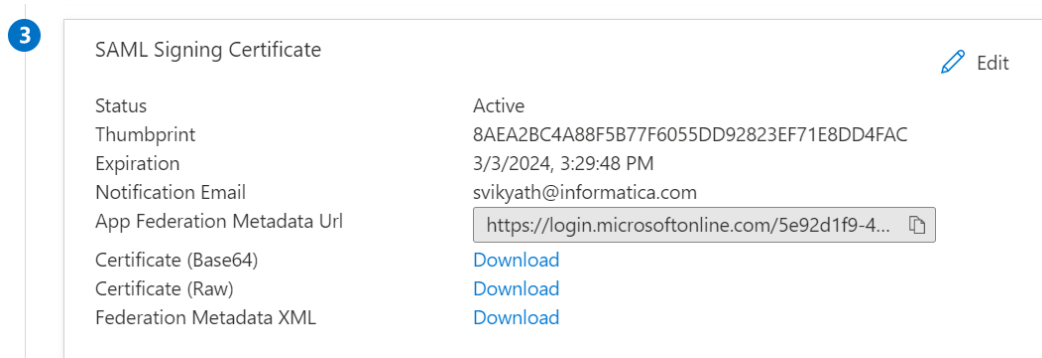
You will use this file to set up SAML in Informatica Intelligent Cloud Services.

Step 2. Set up SAML and enable SCIM in Informatica Intelligent Cloud Services

Set up SAML by uploading the metadata XML file that you generated in Azure AD. Then enable SCIM 2.0 and generate the token for the SCIM provisioning app.

1. Log in to Informatica Intelligent Cloud Services as a user with the Admin role.

    Note: If you are setting up SAML for a sub-organization, log in to the sub-organization as a native user with the Admin role. Do not log in to the parent organization and switch to the sub-organization from the parent organization.

2. In Administrator, open the **SAML Setup** page.
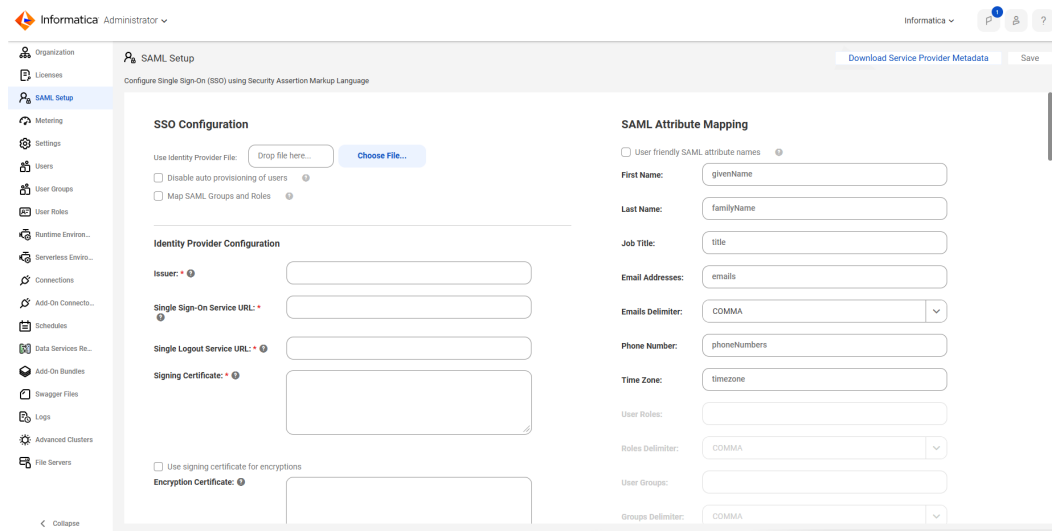
3. In the SSO Configuration area, click **Choose File** and upload the metadata XML file to define the identity provider properties.

4. Enable the **Map SAML Groups and Roles** option, and then enable the **Enable IdP to push users/groups using SCIM 2.0** option.
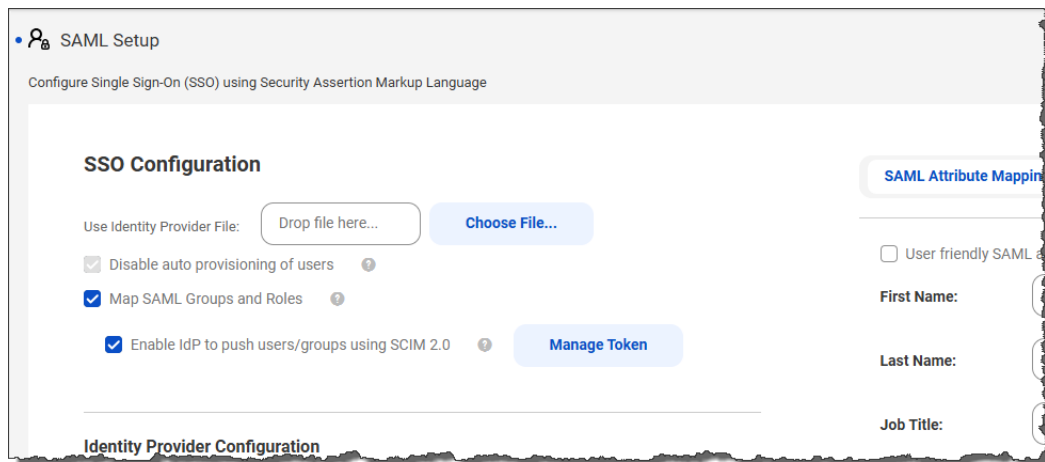
Note: When you enable the **Enable IdP to push users/groups using SCIM 2.0** option, auto-provisioning of users is disabled automatically because users are provisioned through the SCIM client.

5. Click **Manage Token**.
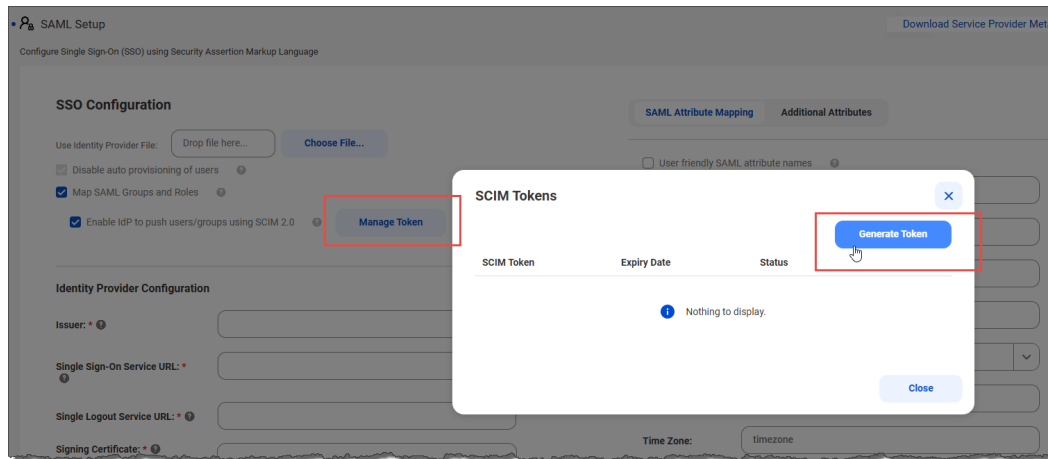
The **SCIM Tokens** dialog box displays the SCIM tokens that have been created for your organization along with the expiration date and status of each token. If two tokens are listed, you'll need to delete one before you can generate a new token.

6. Click **Generate Token** and copy the token to the clipboard.

You will need the SCIM token when you enable SCIM in the provisioning app.

The SCIM token is valid for 180 days from the time of generation. When the token expires, you'll need to generate a new one, even for an existing connection.

Tip: You can create two tokens on different days so that one token is always available. For example, you might want to generate a token on one day and a second token 90 days later. Informatica Intelligent Cloud Services notifies you when a token is about to expire.

7. Click **Save** to save the configuration.

You will map SAML roles and groups after you create the app roles and groups in Azure AD.

Step 3. Integrate the provisioning app with Informatica Intelligent Cloud Services

To integrate the provisioning app with Informatica Intelligent Cloud Services, configure the provisioning mode, map the required attributes, and create the app roles.

1. In Azure AD, open the provisioning app and select **Manage** > **Provisioning**.

2. Set the **Provisioning Mode** to **Automatic**.

3. In the Admin Credentials area, enter the tenant URL, for example, `https://dm-us.informaticacloud.com/scim-service`, and paste the SCIM token that you generated when you enabled SCIM in Informatica Intelligent Cloud Services.

4. Click **Test Connection** and verify that the connection is successful.

5. In the Mappings area, click **Azure Active Directory Users** and map only the following attributes:

   - externalId
   - username
   - displayName
   - title
   - preferredLanguage
   - locale

- timezone

- active

- addresses[type eq "work"].streetAddress

- addresses[type eq "work"].locality

- addresses[type eq "work"].region

- addresses[type eq "work"].postalCode

- addresses[type eq "work"].country

- roles

- employeeNumber

- organization

- department

- emails[type eq "work"]

- givenName

- familyName

- phoneNumbers[type eq "work"]

Note: The roles attribute must support multiple values.
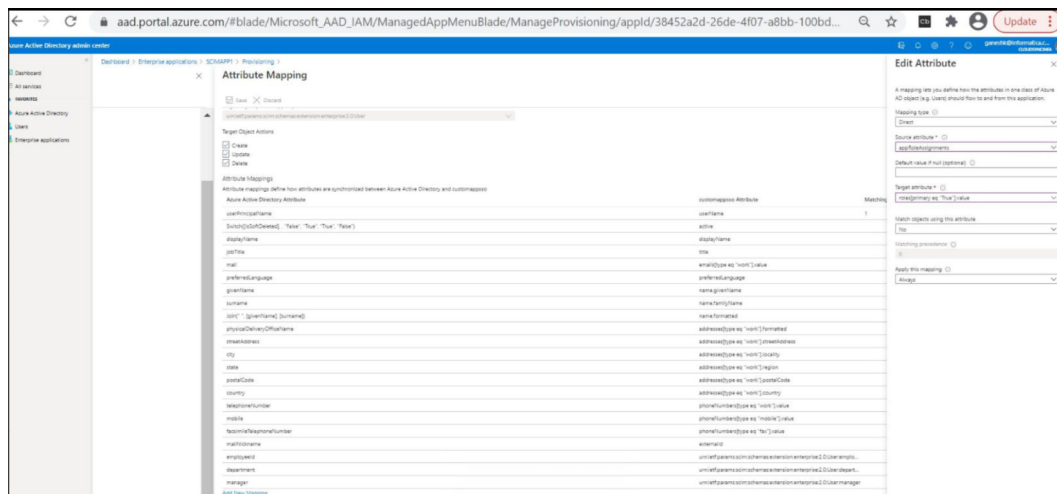
The following images show some constant attributes:

6. If you use role-based access control, add an expression for app roles to pass the roles to Informatica Intelligent Cloud Services.

7. In the Settings area, set the scope to **Sync only assigned users and groups**.

Warning: Do not set the scope to **Sync all** or the SAML response will contain no roles, and users won't be able to sign on to Informatica Intelligent Cloud Services.

8. Select **Manage** > **App roles** and create the app roles that you are mapping on the **SAML Setup** page in Administrator.
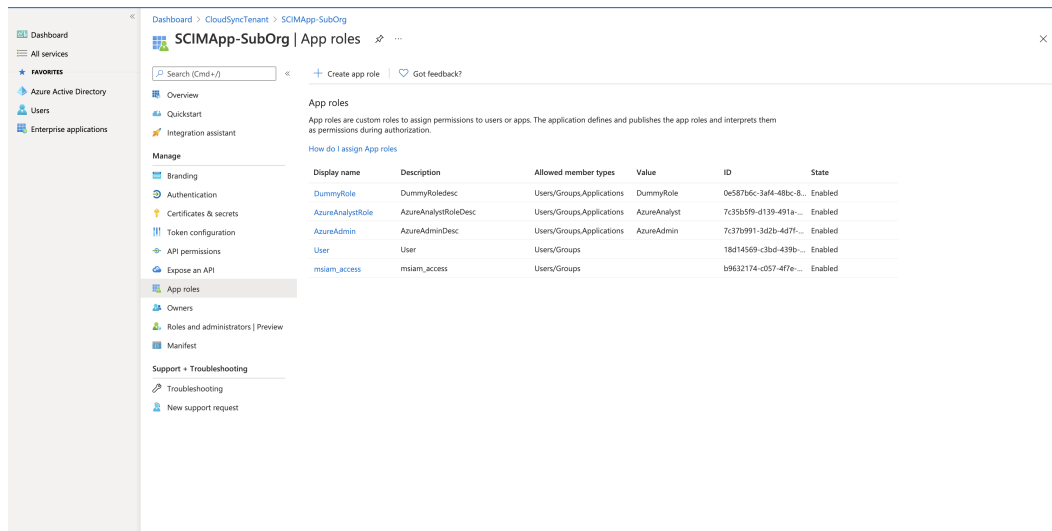
If you don't see this option, contact Microsoft Azure technical support.

9. If you want to provision groups, create a dummy role, but do not map this role on the **SAML Setup** page in Administrator.

This role is only used for assigning groups to the provisioning app.

You need to create the dummy role because a role is required for group provisioning. The dummy role is not used in Informatica Intelligent Cloud Services. Group to role mapping in Informatica Intelligent Cloud Services is based on the group external ID on the **SAML Setup** page.

10. Save the configuration.

Step 4. Provision Azure AD users

To provision users from Azure AD, assign users to the provisioning app and select the appropriate roles for each user.
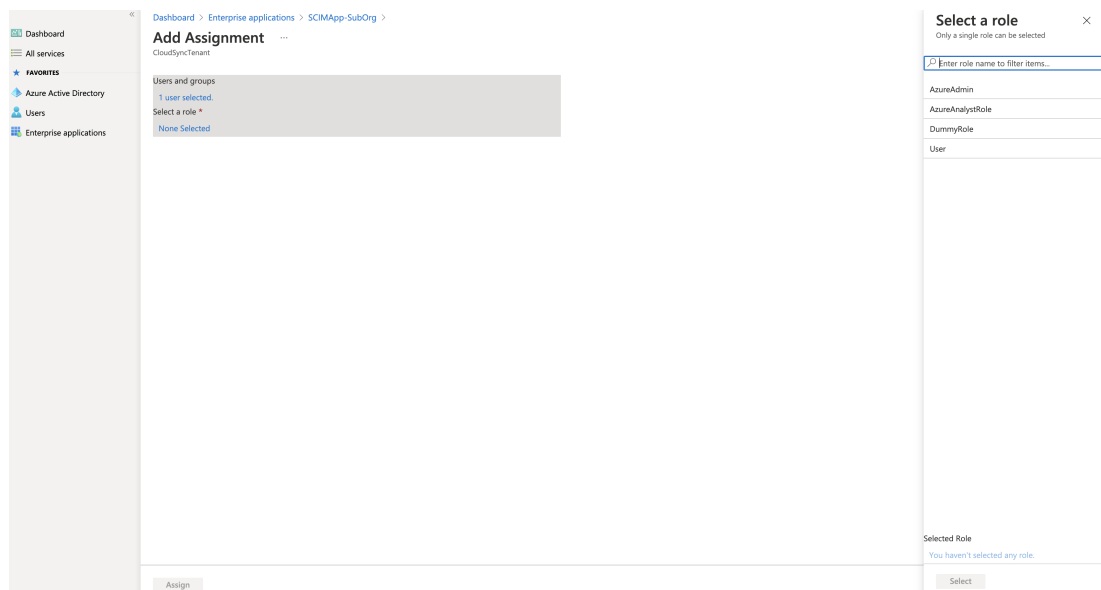
Users will be provisioned in Informatica Intelligent Cloud Services after the provisioning cycle completes. Each user will be provisioned with the Informatica Intelligent Cloud Services role that you map to the Azure AD role on the **SAML Setup** page in Administrator.

Step 5. Provision Azure AD groups

To provision groups from Azure AD, you assign groups to the provisioning app and select the dummy role you created when you integrated the provisioning app with Informatica Intelligent Cloud Services.
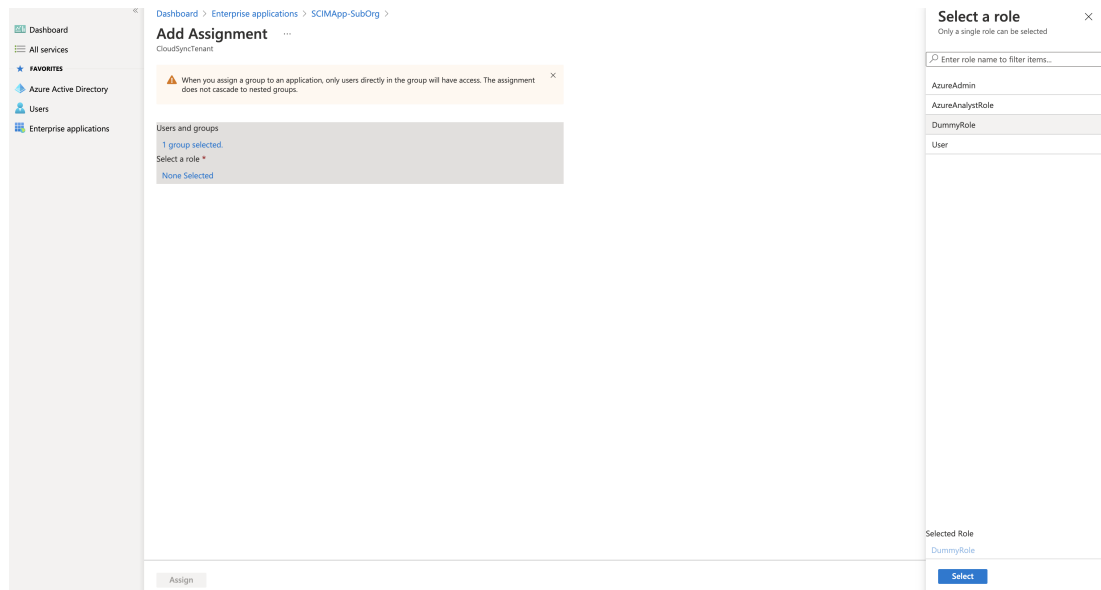
You can assign a role to all users in a group and to individual group members. To assign a role to all users in a group, map the SAML group object ID to an Informatica Intelligent Cloud Services role on the **SAML Setup** page. To provide an additional role to a group member, assign users to the provisioning app individually as explained in "Step 4. Provision Azure AD users" on page 11.

Step 6. Start the provisioning cycle in Azure AD

Start the provisioning cycle in the provisioning app in Azure AD.
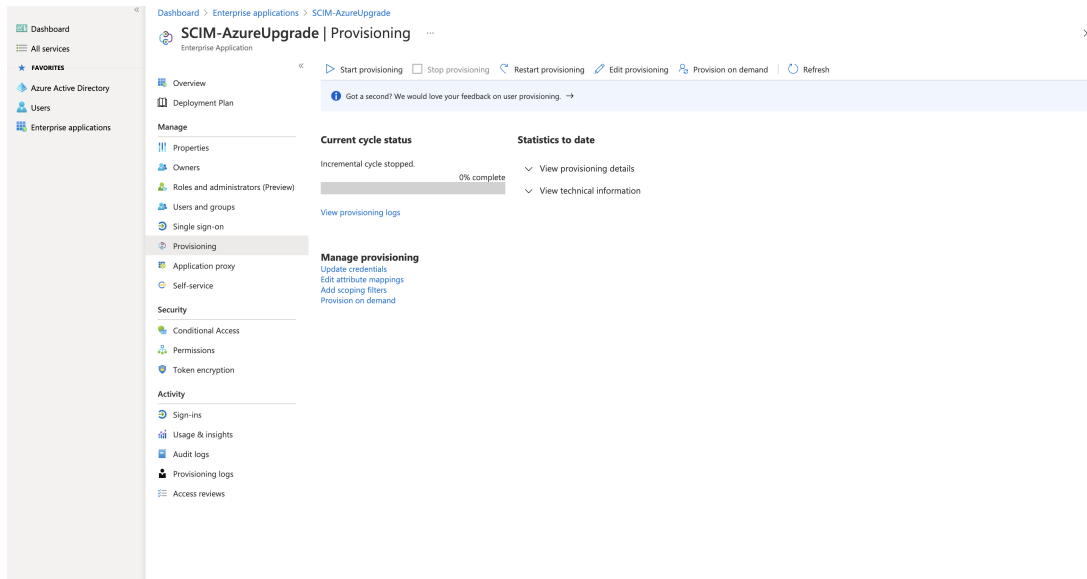
When you start provisioning, the initial provisioning cycle begins. It can take about 40 minutes to provision the assigned users and groups to Informatica Intelligent Cloud Services for the first time.

Incremental cycles run after the initial cycle to check for updates after the initial cycle. An incremental cycle also runs if there was an error in the previous provisioning cycle and the cycling needs to be retried.

After the initial provisioning cycle completes, verify that the group names have been provisioned in Informatica Intelligent Cloud Services. To do this, open the **User Groups** page in Administrator and verify that the group names appear in the **User Groups** list.
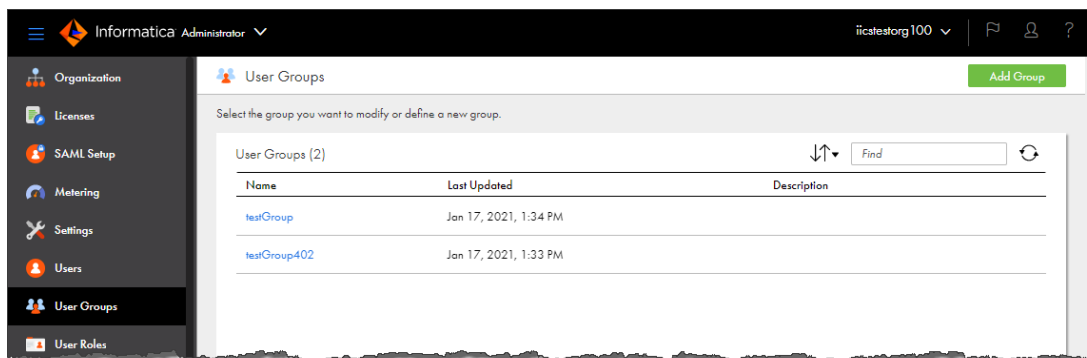
Step 7. Map SAML roles and groups in Informatica Intelligent Cloud Services

Map Azure AD groups to Informatica Intelligent Cloud Services roles on the **SAML Setup** page in Administrator.

1. In Administrator, open the **SAML Setup** page.
2. In the **SAML Attribute Mapping** area, set **User Groups** to the following URL to pass the assigned user groups:

```
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
```

Time Zone:	*timezone*
User Roles:	
Roles Delimiter:	COMMA ▼
User Groups:	http://schemas.microsoft.com/ws/2008/06/identity/claims/g
Groups Delimiter:	COMMA ▼

3. Optionally, on the **SAML Role Mapping** tab, map the Azure AD app roles to Informatica Intelligent Cloud Services roles.

SAML Role Mapping   SAML Group Mapping

Admin:	AzureAdmin
Customer 360 Analyst:	AzureAdmin
Customer 360 Data Steward:	AzureAnalyst
Customer 360 Manager:	AzureAnalyst;AzureAdmin
Data Integration Data Previewer:	role9, role10
Data Integration Task Executor:	role11, role12
Deployer:	role13, role14
Designer:	role15, role16
MDM Designer:	role17, role18
Monitor:	role19, role20
Operator:	role21, role22
Scheduleblackout Permission:	role23, role24
Service Consumer:	role25, role26

4. On the **SAML Group Mapping** tab, map the Azure AD groups to Informatica Intelligent Cloud Services roles.

SAML Role Mapping   SAML Group Mapping

Admin:	group1, group2
Customer 360 Analyst:	testGroup402
Customer 360 Data Steward:	group5, group6
Customer 360 Manager:	group7, group8
Data Integration Data Previewer:	group9, group10
Data Integration Task Executor:	group11, group12
Deployer:	group13, group14
Designer:	testGroup
MDM Designer:	group17, group18
Monitor:	group19, group20
Operator:	group21, group22
Scheduleblackout Permission:	group23, group24
Service Consumer:	testGroup

Note: The role or group mapping must be completed. If the mapping is not completed, users will be assigned no Informatica Intelligent Cloud Services roles, and single sign-on will fail.
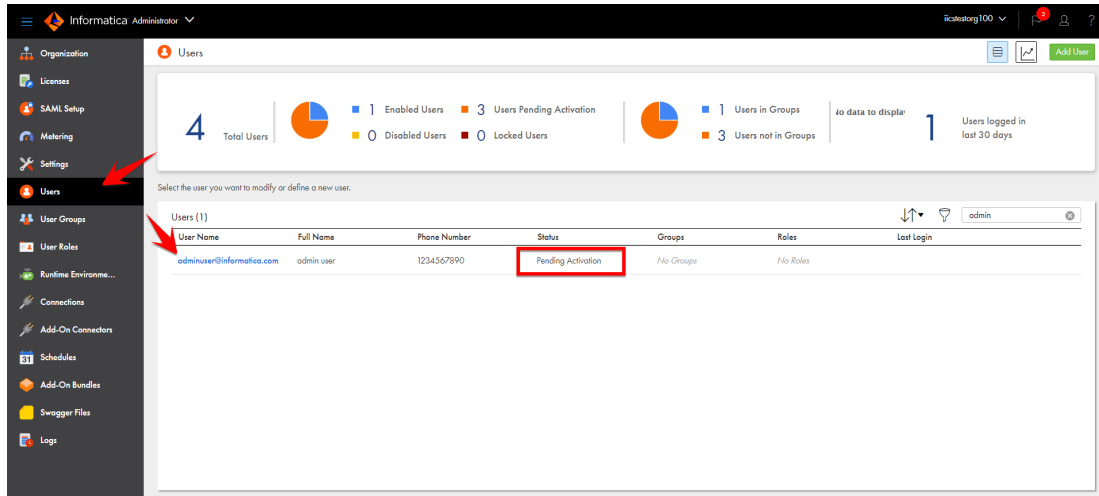
For more information about claims in SAML tokens see, SAML token claims reference in the Microsoft documentation.

5. Click **Save**.

Step 8. Verify provisioning in Informatica Intelligent Cloud Services

After the provisioning cycle completes, users and groups are provisioned in Informatica Intelligent Cloud Services. Users are listed on the **Users** page in Administrator, and user groups are listed on the **User Groups** page.

After the provisioning cycle completes, the users' status on the **Users** page will be "Pending Activation."

When a user signs on to Informatica Intelligent Cloud Services for the first time, the user's status changes to "Enabled."

Users are editable while in the Pending Activation state, but once they sign on and the status changes to Enabled, the user details become read-only. If you change the user details while the user is in the Pending Activation state, the changes are overwritten the first time the user signs on to Informatica Intelligent Cloud Services.

The user details page shows the mapped SCIM attributes on the **Extended User Attributes** tab.

You can view the SAML groups on the **User Groups** page. When you open a group, the **Mirrors the SAML group** field lists the SAML group that the Informatica Intelligent Cloud Services group is mapped to. SAML groups are read-only in Informatica Intelligent Cloud Services.
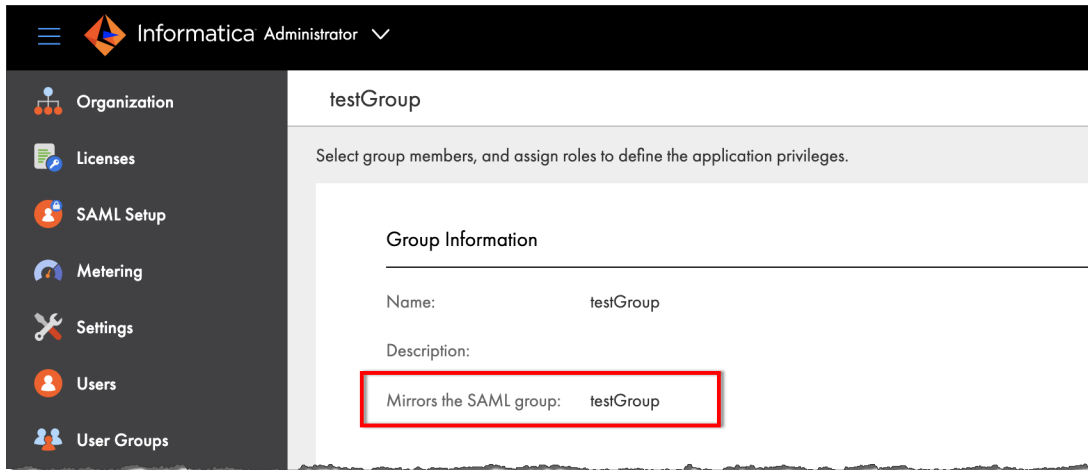
SAML group names vary based on when you complete the group mapping.

If you complete the SAML group mapping after the initial provisioning cycle (recommended), the Informatica Intelligent Cloud Services group names match the Azure AD group names, and the Informatica Intelligent Cloud Services roles are assigned as configured in the group mapping on the **SAML Setup** page.

The following image shows the group details for a SAML group when the group mapping is completed after the initial provisioning cycle:
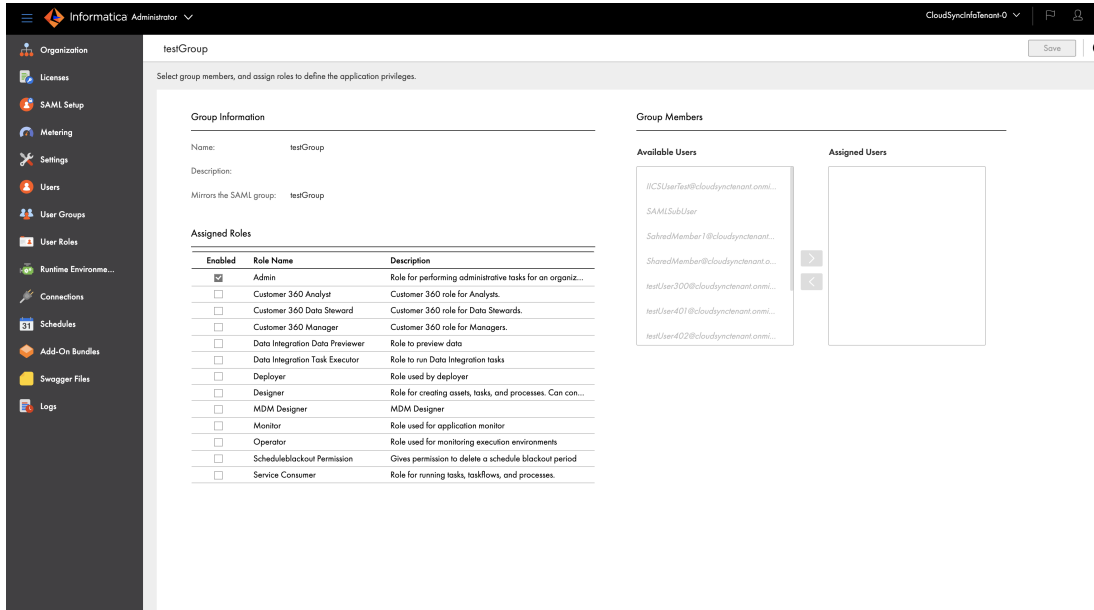
If you complete the SAML group mapping before the initial provisioning cycle, the Informatica Intelligent Cloud Services group name is the same as the group external ID in Azure AD. During provisioning, the Azure AD groups are merged with the Informatica Intelligent Cloud Services SAML groups that were created from the group and role mapping on the **SAML Setup** page.

The following image shows the group details for a SAML group when the group mapping is completed before the initial provisioning cycle:

Guidelines for working with users

Consider the following guidelines when you work with users:

- The user attributes "username" and "email" are required. If these attributes are not provided, provisioning of the user will fail.
- User email addresses must be in the format: `<local part>@<domain>`, for example, `jsmith@mycompany.com`.
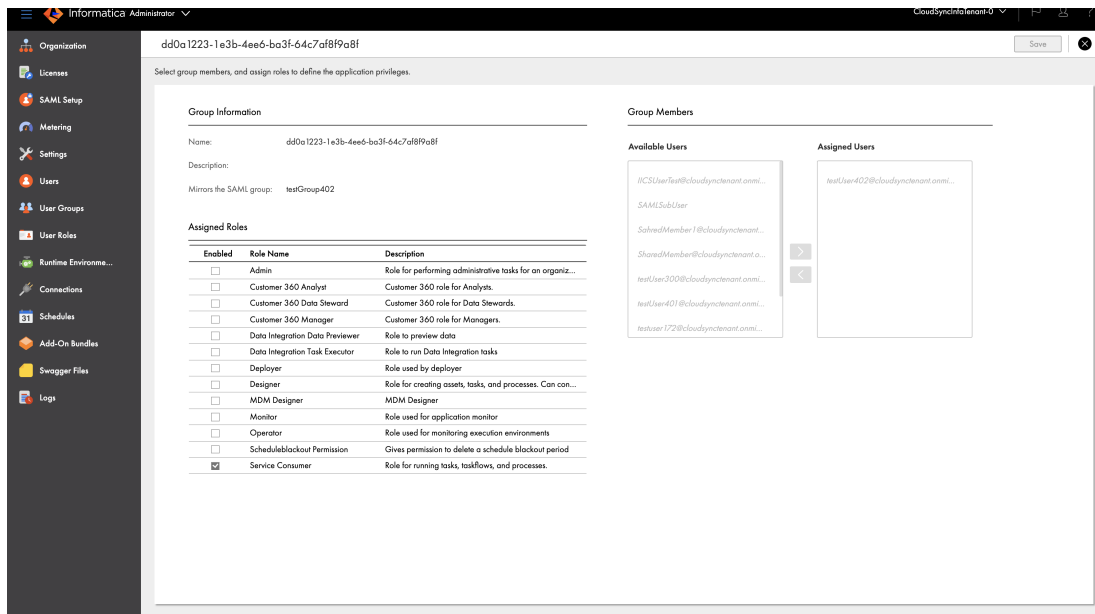- In Informatica Intelligent Cloud Services, user names are unique to each user. Therefore, if you edit a user name in Azure AD after provisioning, Informatica Intelligent Cloud Services creates two users: one with the old user name and one with the new user name.

  If you need to edit a user name after provisioning, delete the user in Azure AD, and then re-create the user with the new name.
- During provisioning, the user attribute "title" is truncated at 100 characters.
- User phone numbers must contain 10-25 characters. They can contain only numbers, spaces, parentheses, hyphens, periods, and a plus sign as the first character.
- If you update a user attribute and remove its value, the attribute value will not be removed in Informatica Intelligent Cloud Services. However, if you change its value, the attribute value will be updated in Informatica Intelligent Cloud Services.
- If you soft delete a user in Azure AD, the user will be disabled, not deleted, in Informatica Intelligent Cloud Services. Disabled users cannot sign on to Informatica Intelligent Cloud Services.

  To delete a user in Informatica Intelligent Cloud Services, first soft delete the user in Azure AD, then go to deleted users and permanently delete the user.
- If you remove a user from the provisioning app after users have been pushed, then add the user back to the app, the user's state in Informatica Intelligent Cloud Services will be Enabled instead of Pending Activation.

Guidelines for working with groups

Consider the following guidelines when you work with groups:

- Group display names in Informatica Intelligent Cloud Services vary based on when you complete the SAML group mapping. If you map groups after the SCIM push, the group names in Informatica Intelligent Cloud Services will match the Azure AD group names. If you map groups before the SCIM push, the group names in Informatica Intelligent Cloud Services will be the same as the group external IDs in Azure AD.

- If you change a group name in Azure AD, the group name is not updated in Informatica Intelligent Cloud Services. However, the **Mirrors the SAML group** field on the **User Groups** page displays the new Azure AD group name.

- If you delete a group in Azure AD, group members that were assigned to the app individually are removed from the group in Informatica Intelligent Cloud Services. Group members that were not assigned to the app directly are disabled, but not deleted, in Informatica Intelligent Cloud Services. Disabled users cannot sign on to Informatica Intelligent Cloud Services.

- Deleting a group does not delete the group members in Informatica Intelligent Cloud Services. If you want to delete group members, you must permanently delete the users in Azure AD.

Author

Astha Girdher
Principal SDET