Cisco User Defined Network Administration Portal

Overview of Cisco User Defined Network Administration Portal

As a Cisco User Defined Network administrator, you must have Cisco credentials to log in to the Cisco User Defined Network administration portal.

If you do not have Cisco credentials, click **Create A New Account** in the login window of the administrator portal. Follow the instructions displayed to create a Cisco account.

You can host Cisco User Defined Network services in multiple regions:

- US region: https://udn.cisco.com/
- EMEAR region: https://udn-de.cisco.com/

For information about configuring multiregion support, see the *Ciso User Defined Network Install and Upgrade Guide*.

Dashboard

The following features have been introduced in the Cisco User Defined Network Cloud dashboard:

- **Summary**
- **Sites View**
- **Invitation Status**

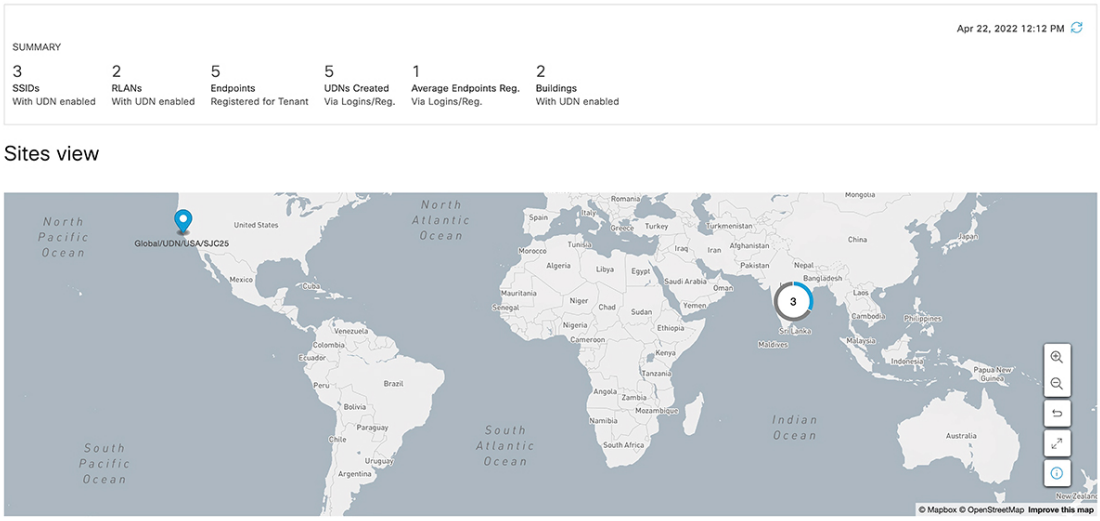
The **Summary** report lists the following statistics:

- Count of UDN-enabled SSIDs

- Count of UDN-enabled RLANs
- Count of devices and average number of devices per room
- Count of UDN rooms
- Count of UDN-enabled buildings

Note If stale data is displayed in the **Summary** report, refresh the report to fetch the latest data from the Cisco DNA Center.

Figure 1: UDN Dashboard - Summary and Sites View



Information about UDN-enabled (blue) and non-UDN-enabled (grey) buildings is displayed in the **Sites View** map.

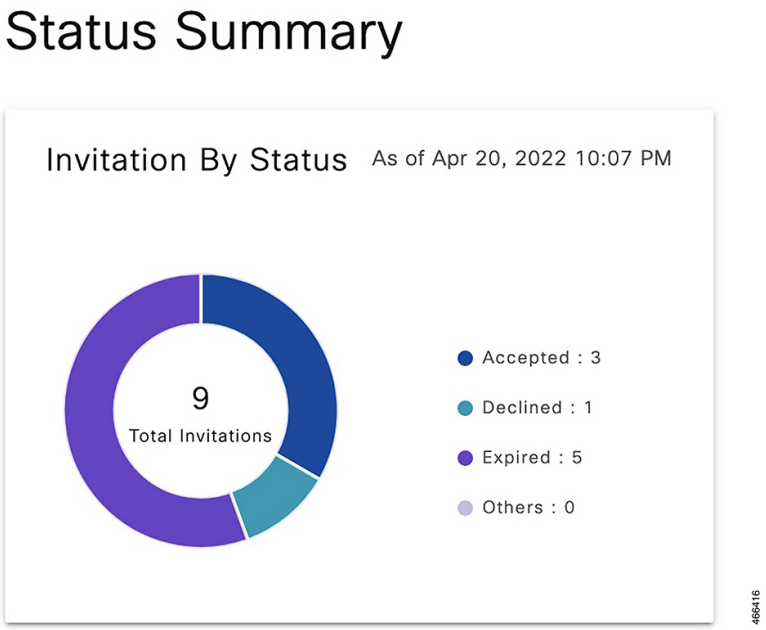
Note As information displayed in the **Sites View** map is at the building level, even if only one floor in the building is enabled for UDN, the entire building is listed as a UDN-enabled building in the map.

You can also view an overview of the invitations and the following statistics in the Dashboard:

- **Accepted**: Total number of invitations accepted by all guests
- **Declined**: Number of invitations rejected by a guest
- **Expired**: Number of invitations that have neither been accepted nor rejected

  Note that the expiry interval is set to 30 minutes.
- **Others**: Number of initiated invitations that have either failed or that do not fall under the **Accepted**, **Declined**, or **Expired** categories
- **Total**: The total number of invitations irrespective of the status

Figure 2: UDN Dashboard - Invitation Status



Note

- The invitation statistics are cumulative and are calculated since that specific Cisco User Defined Network was first deployed.
- If stale data is displayed in the **Invitation By Status** report, refresh the report to fetch the latest invitation statistics from the Cisco User Defined Network Cloud.

Customize Mobile Application

As a UDN admin, you can customize the Cisco User Defined Network mobile application accessed by users.

Step 1 Log in to the Cisco User Defined Network Cloud portal.

Step 2 Click the menu icon (☰) and go to **Manage** > **Mobile Customization**.
The **Mobile Customization** window is displayed with the following options:

- **Support Contacts**
- **Organization Logo**
- **SSID**

Step 3 To customize the support contact information, provide the following details:

- **Email Address**: Specify the email address of your organization's support team.
- **URL**: Specify the URL of your organization's support web page.
- **Phone Number**: Specify the phone number of your organization's support team.

Step 4 To customize the organization logo, upload a PNG file of the logo.

The logo file size should not exceed 1 MB.

Step 5 To customize the SSID, configure it in the on-premise Cisco DNA Center.

Note You can add up to three Cisco User Defined Network-enabled SSIDs.

When an Android device joins a Cisco User Defined Network-enabled SSID, Wi-Fi scanning on the mobile application is disabled. The Cisco User Defined Network mobile application otherwise has Wi-Fi scanning enabled to help consolidate MAC addresses for Cisco User Defined Network registration.

Some wireless devices are configured to use random MAC addresses for each SSID they connect to. Note that users can only add random MAC addresses when connected to the Cisco User Defined Network-enabled SSIDs specified in the **SSID** tab. By permitting device registration with random MAC addresses only through specific SSIDs, incorrect registration is avoided. Cisco User Defined Network is prevented from learning a device's random MAC address when the device is connected to an SSID that is not a part of the Cisco User Defined Network.

Endpoint Management

In the Cisco User Defined Network, a user's room name is set based on the username specified in the user's Active Directory profile. If the username is not available in the user's Active Directory profile, then the UDN room is named based on the UDN user's email ID.

For example, if the UDN user's Active Directory profile has the following details, the UDN room would be named *JDoe's room* based on the username. However, if the username is not available in the user's Active Directory profile, then the room would be named *janed's room* based on the email ID.

- First Name: Jane
- Last Name: Doe
- Username: JDoe
- Email ID: janed@example.com

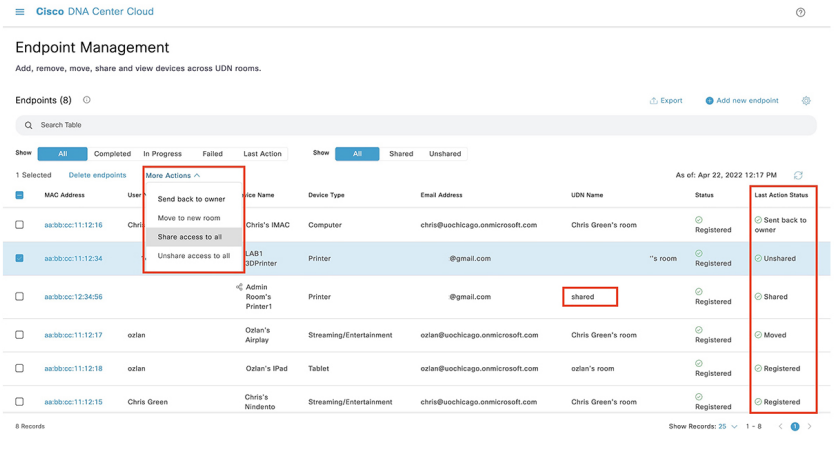
Both UDN administrators and users can add, delete, or move devices between UDN rooms. The users use the UDN mobile app to manage their devices while UDN admins use the Cisco User Defined Network Cloud portal both for managing user-owned and shared devices as well as to debug and fix user issues.

To manage endpoints as a UDN admin, follow these steps:

Step 1 Log in to the Cisco User Defined Network Cloud portal.

Step 2 Click the menu icon (☰) and choose **Manage** > **Endpoint Management**.
The **Endpoint Management** window is displayed with a table listing all the available endpoints.

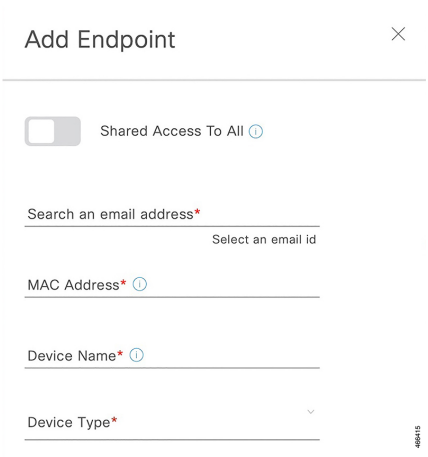
Step 3 In the **Endpoint Management** window, you can perform the following actions:



- Add a new endpoint: Click **Add New Endpoint**, then add the following details:
  - User's email address
  - Device MAC address
  - Device name
  - Device type

After these details are added, the device is listed in the **Endpoint Management** dashboard. While adding a new device, if you want it to be discovered by all users in the Cisco User Defined Network, enable **Shared Access to All** in the **Add Endpoint** window.

Figure 3: Add Endpoint



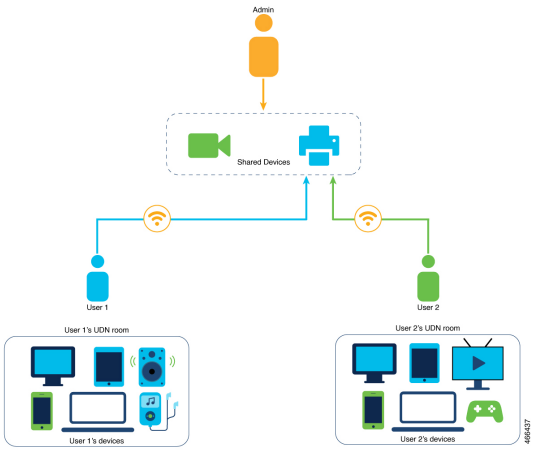
Note
- You cannot add a device whose MAC address is already registered.
- Only admins can add a shared device. A shared device is listed as **shared** under the **UDN Name** column in the **Endpoints** table.

- Move an endpoint
- Send an endpoint back to the original owner
- Share or unshare an endpoint
- Delete an existing endpoint
- Filter the endpoints based on the shared status or the following action statuses:
  - **Completed**
  - **In Progress**
  - **Failed**
  - **Last Action**

You can view the details of these actions in the **Last Action Status** column.

Share Device

Using the Cisco User Defined Network Cloud portal, as a UDN admin, you can add devices such as printers in a dormitory or projectors in an auditorium to be used as a shared resource and share or unshare these devices in the network. A shared device is discoverable by all UDN users in the network.



Note

- As a UDN admin, you can only share or unshare devices that are owned and added by you. User devices cannot be shared or unshared.
- Shared devices are not listed in the UDN mobile app.

Step 1 Log in to the Cisco User Defined Network Cloud portal.

Step 2 Click the menu icon (☰) and choose **Manage** > **Endpoint Management**.
The **Endpoint Management** window is displayed with a table listing all available endpoints.

Step 3 In the **Endpoint Management** window, select a device and click **More Actions** > **Share access to all**.

Note
- You can also make a device discoverable to all UDN users while adding it to the Cisco User Defined Network.
- To unshare a device, select **Unshare access to all** instead of **Share Access to all**.

A **Warning** message is displayed to check if the device is intended for sharing with all users in the Cisco User Defined Network.

Step 4 Click **Share**.
A window is displayed listing the details of the shared device such as its name, type, status, MAC address and the time at which the device sharing began.

Step 5 Click **Save**.
A success message is displayed confirming that the device is shared.

Configure UDN Room Settings

Prior to this release, only Cisco User Defined Network users could register devices on the network through the Cisco User Defined Network mobile app and the maximum number of devices was limited to 10 devices per user. Also, a limit on the number of devices per room could not be configured.

As a UDN administrator, you can now configure the maximum number of devices permitted per room and per user in a Cisco User Defined Network. You can also change this device limit through the Cisco User Defined Network portal. At the time of device registration through the Cisco User Defined Network mobile app, if the permitted device limit either for the user or the room is reached, then the user receives an error notification in the mobile app.

Note The device limit for a Cisco User Defined Network room does not apply to shared devices.

Step 1 Log in to the Cisco User Defined Network Cloud portal.

Step 2 Click the menu icon (☰) and choose **Manage** > **UDN Room Settings**
The **UDN Room Settings** window is displayed.

Step 3 In the **UDN Room Settings** window, you can specify the following limits:

- **UDN Room Limit**: Under **Devices per room**, specify the maximum number of devices permitted in a Cisco User Defined Network room. These devices include both the UDN room owner's devices and devices added by users invited to the room. The **UDN Room Limit** does not apply to shared devices.

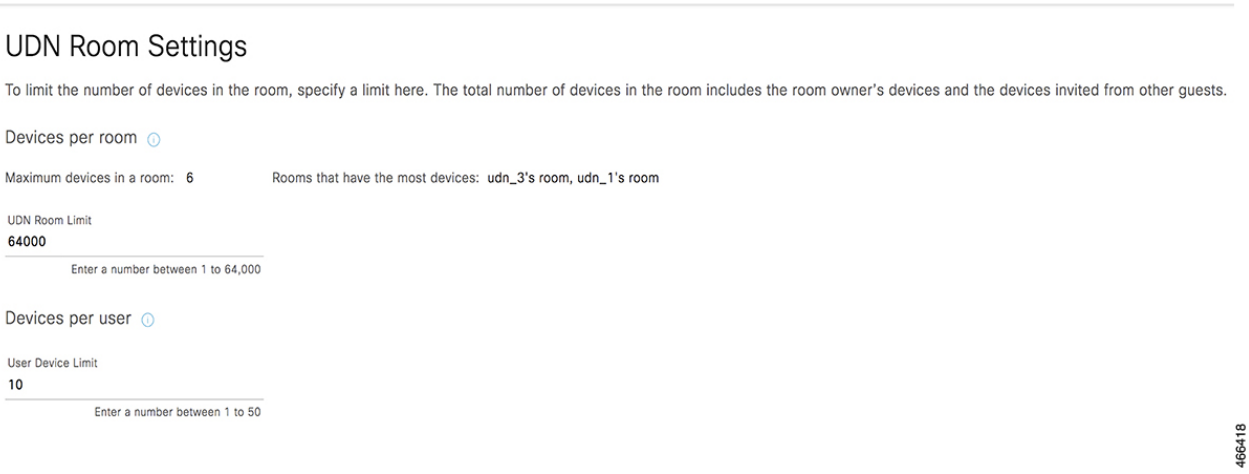
  The default value for the **UDN Room Limit** is 64,000.

  Note In the **Devices per room** section, the following data is displayed:
  - Maximum number of registered devices
  - Number of rooms that have the most devices

- **User Device Limit**: Under **Devices per user**, specify the maximum number of devices that a Cisco User Defined Network user can add to the network.

  The default value for the **User Device Limit** is 10.

  Note The number of devices per user cannot exceed the maximum number of devices per room.



Step 4 Click **Save**.
A **Success** message is displayed.

Configure System Settings

The **Users and Accounts** window of the Cisco User Defined Network administration portal allows a UDN administrator to configure and manage settings for that tenancy. Click the **Menu** icon (☰), choose **Users and Accounts**, and the following options are displayed in the left pane. Click the corresponding menu option to view the relevant window.

- **General**
- **User Management**
- **Cisco Support**
- **Single Sign-On**

General

Click the **Menu** icon (☰), and choose **Users and Accounts** > **General**.

The name of your Cisco User Defined Network Cloud account appears in the **General** window. Click **Delete Account** to delete your Cisco User Defined Network Cloud account.

User Management

To configure user management settings, click the **Menu** icon (☰), and choose **Users and Accounts** > **User Management**.

In the **User Management** window, all the users of a Cisco User Defined Network account are displayed. You can view, add, and edit user information in this window.

You can add users in two ways:

- **Add users manually**

  To add a user, in the **User Management** window, click **Add** and specify the user's email address and assign a role.

- **Attribute mapping for user enrollment**

  To automatically add the users of the Cisco User Defined Network mobile application, associate ID provider (IdP) groups with specific attributes, and map this information to a user role. Configure this attribute mapping in the **Single Sign-On** window (from the main menu, choose **Users and Accounts** > **Single Sign-On**). After authentication, a user is automatically added to the list of users in the **User Management** window.

The following user roles are available:

- **Account Admin**: A user with this role can function as a UDN administrator. Only users with this role can view and access all the options in the **System** menu and carry out configuration actions.
- **Observer**: A user with this role has read-only access to the Cisco User Defined Network administration portal, and to the **Mobile Customization** window (from the main menu, choose **Manage** > **Mobile Customization**). Note that an Observer user cannot view the **System** menu.
- **Network Admin**: A user with this role cannot view the **Users and Accounts** menu. A Network Admin user can only access the **Mobile Customization** window (from the main menu, choose **Manage** > **Mobile Customization**).
- **Account-User-Role**: A user with this role can access the Cisco User Defined Network mobile application. Users with this role have read-only access to the Cisco User Defined Network administration portal and can only view the home page.

Cisco Support

To configure the Cisco support feature, click the **Menu** icon (☰), and choose **Users and Accounts** > **Cisco Support**.

Here, you can allow Cisco support teams to access your account for information to enable quick troubleshooting and investigation of reported issues, if any.

The **Allow Cisco Support to access** toggle button is enabled by default. This allows Cisco support teams to access your account remotely and to troubleshoot specific issues that you have raised with the support team. You can disable this remote access at any time by clicking the toggle button.

Single Sign-On

Step 1 Click the **Menu** icon (☰), and choose **Users and Accounts** > **Single Sign-On**.

Step 2 Click the **Enable SSO Access** toggle button.
A new workflow is launched.

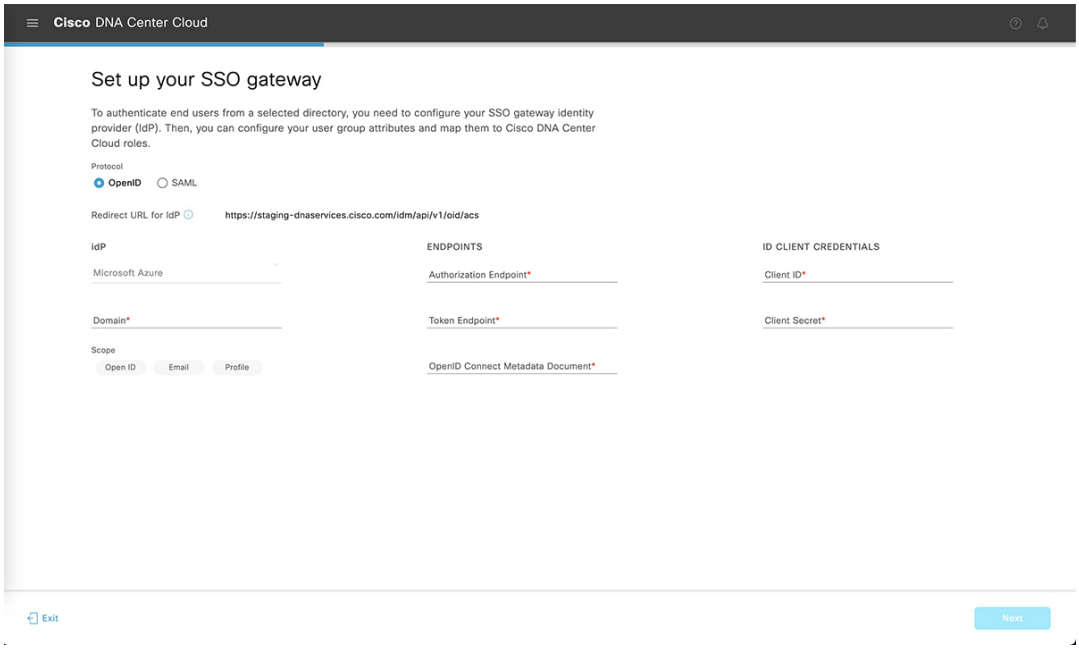
Step 3 In the **Set Up Single Sign-On (SSO)** window, click **Let's Do It**.

Step 4 In the **Set up your SSO gateway** window, choose the protocol and IdP, and perform the steps corresponding to your chosen protocol from the following options:

a) **OpenID**: Follow the instructions provided in the Set Up an OpenID SSO Gateway with Microsoft Azure Active Directory, on page 11 section.

b) **SAML**: Follow the instructions provided in the Set Up a SAML SSO Gateway with Microsoft Azure Active Directory, on page 11 section.

Figure 4: Set Up Your SSO Gateway - Cisco User Defined Network Cloud



What to do next

After configuring the SSO gateway as mentioned above, proceed to the next part of the workflow. The **Do You Want To Map Attributes From Active Directory** window is displayed. To map attributes from Active Directory to user roles in the Cisco User Defined Network, see Map Attributes from Active Directory, on page 12.

In the final part of the workflow, a summary window displays the SSO gateway configurations. Click the **Enable UI** button on this window to complete the SSO setup.

Set Up an OpenID SSO Gateway with Microsoft Azure Active Directory

Step 1 To configure an OpenID SSO Gateway, first log in to your Microsoft Azure Active Directory account.

Step 2 In the left pane, click **App Registrations**

Step 3 In the window that is displayed, click **+ New Registration**.

Step 4 In the **Register an Application** area, enter a name for the application to be used in the Cisco User Defined Network.

Step 5 In the **Redirect URI** section, select **Web**, and enter **https://dnaservices.cisco.com/idm/api/v1/oid/acs**.

Step 6 Click **Register**.

Microsoft Azure Active Directory assigns a unique application or client ID to your app.

The **Overview** window for your app is displayed.

Step 7 From the Microsoft Azure Active Directory, note down the values of the following fields for your registered app.

- From the **Overview** window, copy the **Application (Client) ID**.
- From the left menu pane, choose **Certificates and Secrets** > **+ New Client Secret**, select the expiry time from the list, enter a description, and click **Add**. Copy the client secret that is displayed.
- From the main left pane of the Microsoft Azure Active Directory, choose **App Registrations** > **Endpoints**. Copy the values in the following fields:
  - **OAuth 2.0 authorization endpoint**
  - **OAuth 2.0 token endpoint**
  - **OpenID Connect metadata document**

Step 8 In the Cisco User Defined Network administration portal, click the **Menu** icon (☰), and choose **Users and Accounts** > **Single Sign-On**.

Step 9 Click the **OpenID** radio button.

Step 10 Enter the information copied from the Microsoft Azure Active Directory in the corresponding fields:

- **Authorization Endpoint**
- **Token Endpoint**
- **OpenID Connect Metadata Document**
- **Client ID**
- **Client Secret**

Step 11 Click **Next**.

Set Up a SAML SSO Gateway with Microsoft Azure Active Directory

Step 1 Click the **Menu** (☰) icon, and choose **Users and Accounts** > **Single Sign-On**.

Step 2 Click the **SAML** radio button.

A **CDNA Metadata URL** for IdP is displayed. Keep this URL handy, or keep this window open because you need this value when configuring your SAML application in Microsoft Azure Active Directory.

Step 3 Log in to your Microsoft Azure Active Directory account to set up a SAML application.

Step 4 In the left pane, click **Enterprise Applications**.

Step 5 Click **New Application**, and then click **Non-Gallery Application**.

Step 6 In the **Name** field, enter your application's name.

Step 7 Click **Add**.

Step 8 In the **Overview** window that is displayed, click the **Set Up Single Sign On** option.

Step 9 In the **Set Up Single Sign-On With SAML** window that is displayed, click the **Edit** button for **Basic SAML Configuration**.

Step 10 In the **Identifier (Entity ID)** field, enter the **CDNA Metadata URL** value mentioned in Step 2.

Step 11 In the **Reply URL (Assertion Consumer Service URL)** field, append the IdM cluster name with */idm/api/v1/saml/acs*. This IdM cluster name is also part of your CDNA metadata. An example of a reply URL is *https://<IdMClusterName>/idm/api/v1/saml/acs*

Step 12 From the **SAML Signing Certificate** area, copy the value of **App Metadata Federation URL**. Keep this value handy, or leave this window open while you configure SAML SSO in the User Defined Network administrator account.

Step 13 In the Cisco User Defined Network administrator portal, follow the instructions provided in Step 1, on page 11 and Step 2, on page 11 for the **Single Sign-On** window.

Step 14 From the **IdP** drop-down list, choose **Microsoft Azure** .

Step 15 In the **Domain** field, enter the name of the organizational domain.

Step 16 In the **Metadata** field, enter the **App Metadata Federation URL** value captured in Step 12, on page 12.

Step 17 Click **Next**.

Map Attributes from Active Directory

You have the option to map user attributes from the user groups in your ID provider to specific Cisco User Defined Network user roles. To do so, in the **Do you want to map attributes from Active Directory?** window, click the **Yes** radio button. Configuring this option allows easy management of Cisco User Defined Network users, and automatically adds the required details of the users to the **User Management** window.

In Microsoft Azure Active Directory, add the required user attributes and claims. For more information, see https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-saml-claims-customization.

When configuring the claim names for the attributes email address, user ID, last name, and first name, use the corresponding claim names from the list below:

- **EmailAddress**
- **UserID**
- **LastName**
- **FirstName**

In the Cisco User Defined Network administrator portal, for each attribute-user group mapping that is to be created, enter the required values from the list below:

- **Attribute**: Enter the **Claim Name** value for the required attribute from Microsoft Azure Active Directory.

- **Value**: Enter the **Value** for the **Claim Name**, as specified in Microsoft Azure Active Directory.
- From the **Role** drop-down list, choose the user role to be mapped to the user attribute.
- From the **Regions** drop-down list, choose the region to be mapped.

Figure 5: Map Attributes from Active Directory - Cisco User Defined Network