Azure AD

Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

Overview

This guide shows how to create an Azure AD SAML application and integrate with it with Security Cloud Sign On .

Note

- Keep in mind that the user principal name (UPN) of an Azure AD user is not always the same as the user's email address.
- The `<NameID>` element and the `email` user attribute in the SAML response **must** contain the user's email address. See SAML response requirements for details.
- The specified email address should match the one used in existing product access controls. If they do not match you will need to update your product access controls.

Getting started

Before you begin

- You must be able to sign in to the Azure portal with admin privileges.
- You need to have completed Step 1: Create an enterprise and Step 2: Claim and verify your email domain of the enterprise settings wizard.

Step 1 Sign in to https://portal.azure.com.

If your account gives you access to more than one tenant, select your account in the upper right corner. Set your portal session to the Azure AD tenant that you want.

a) Click **Azure Active Directory**.
b) Click **Enterprise Applications** in the left sidebar.
c) Click **+ New Application** and search for `Azure AD SAML Toolkit`.
d) Click **Azure AD SAML Toolkit**.
e) In the **Name** field enter `SecureX Sign On` or other value then click **Create**.
f) On the Overview page click **Single Sign On** under **Manage** in the left sidebar.
g) Select **SAML** for the select single sign on method.
h) In the **Basic SAML Configuration** panel click **Edit**.

- Under **Identifier (Entity ID)** click **Add Identifier** and enter a temporary value of `https://example.com` or other valid URL. You'll replace this temporary value later.
- Under **Reply URL (Assertion Consumer Service URL)** click **Add reply URL** and enter a temporary value of `https://example.com` or other valid URL. You'll replace this temporary value later.
- In the **Sign on URL** field enter `https://sign-on.security.cisco.com/`.
- Click **Save** and close the **Basic SAML Configuration** panel.

i) Under **Required claim**, click the **Unique User Identifier (Name ID)** claim to edit it.
j) Set the **Source** attribute field to `user.userprincipalname`.

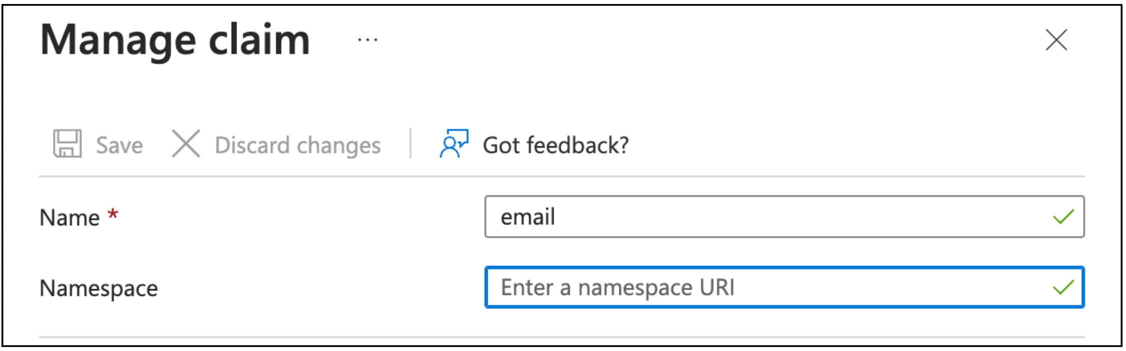
This assumes that the value of **user.userprincipalname** represents a valid email address. Otherwise, set **Source** to use **user.primaryauthoritativeemail**.

k) Under **Additional Claims** panel click **Edit** and create the following mappings between Azure AD user properties and SAML attributes.

This assumes that the value of **user.userprincipalname** represents a valid email address. Otherwise, set **Source attribute** for the **email** claim to use **user.primaryauthoritativeemail**.

Name	Namespace	Source attribute
`email`	No value	`user.userprincipalname`
`firstName`	No value	`user.givenname`
`lastName`	No value	`user.surname`

Be sure to clear the **Namespace** field for each claim.



Name * email

Namespace Enter a namespace URI

l) In the **SAML Certificates** panel click **Download** for the **Certificate (Base64)** certificate.

m) In the **Set up Single Sign-On with SAML** section copy the value of **Login URL** and **Azure AD Identifier** for use later in this procedure.

Step 2 In a new browser tab, open the Enterprise settings wizard. You should be on the **Integrate Identity Provider** > **Set Up** screen (Step 3: Exchange SAML metadata).

a) In the **Identity Provider (IdP) Name** field enter `Azure SSO` or other name for the integration.

b) In the **Single Sign-On Service URL** field enter the value of the **Login URL** field you copied from Azure.

c) In the **Entity ID (Audience URI)** field enter the value of the **Azure AD Identifier** you copied from Azure.

d) Click **Add File** and upload the SAML signing certificate you downloaded from the Azure portal.

e) Opt out of free Duo MFA for your users, if desired.

f) On the **Download** screen click **Next**.

g) Copy the values of **Single Sign-On Service URL (ACS URL)** and **Entity ID (Audience URI)** for use later in this procedure.

h) Click **Next**.

Step 3 Return to the Azure console browser tab.

a) In the **Basic SAML Configuration** section click **Edit**.

b) In the **Identifier (Entity ID)** field replace the temporary identity provider you entered with the value of the **Entity ID (Audience URI)** field you copied from the Enterprise settings wizard.

c) In the **Reply URL (Assertion Consumer Service URL)** field replace the temporary identity provider you entered with the value of the **Single Sign-On Service URL (ACS URL)** field you copied from the Enterprise settings wizard.

d) Click **Save** and close the **Basic SAML Configuration** panel.

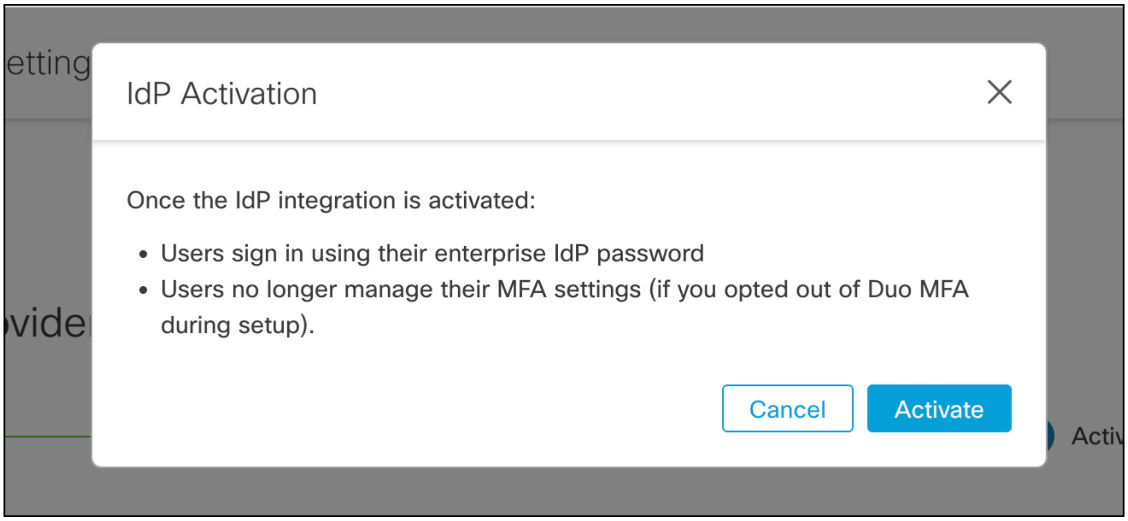
Step 4 Return to the Enterprise settings wizard to test the integration. You should be on the **Configure** screen (Step 4: Test the SSO integration) and do the following:

a) Copy the provided URL and open it a private (incognito) window.

b) Sign in with an Azure AD account associated with the SAML application.
If you land back in the SecureX Application Portal then the test was successful. If you encounter an error see Troubleshooting.

c) Click **Next** to advance to the **Activate** screen.

d) When you're ready click **Activate my IdP** and then confirm your choice in the dialog box.



IdP Activation

Once the IdP integration is activated:

- Users sign in using their enterprise IdP password
- Users no longer manage their MFA settings (if you opted out of Duo MFA during setup).