Integrate your identity provider

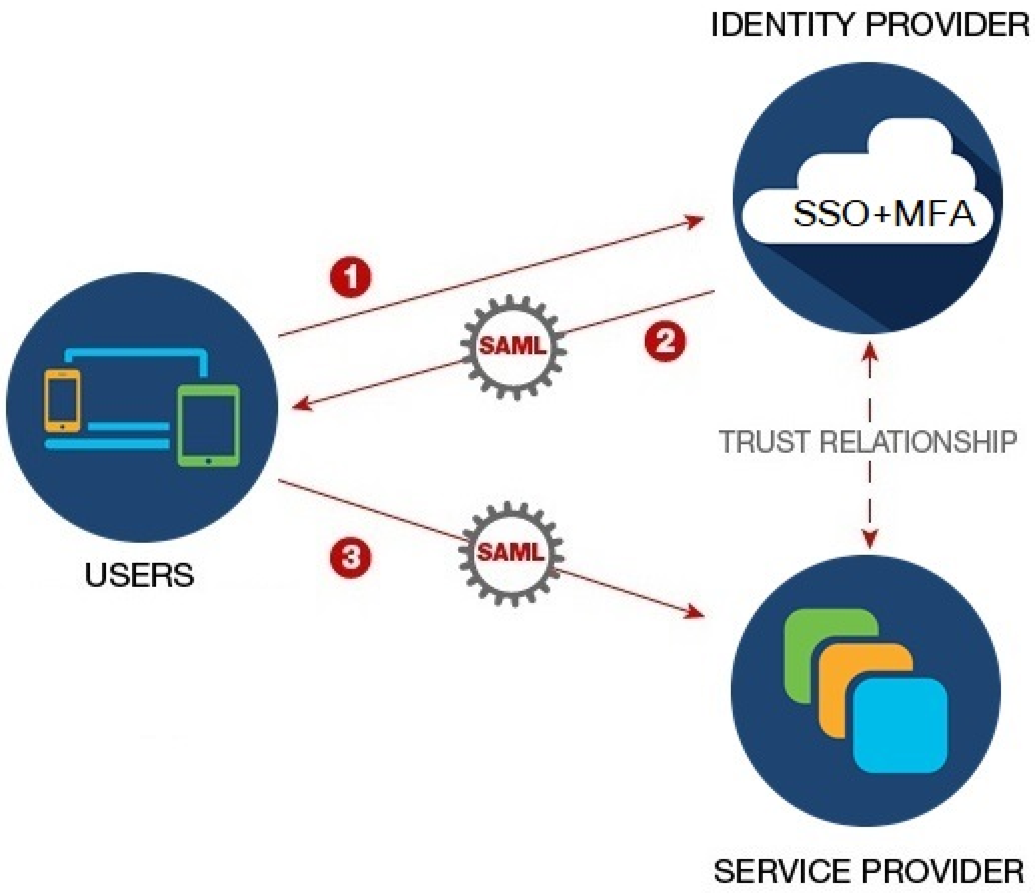
Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

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

Overview

You can integrate your own or third-party identity provider with Security Cloud Sign On using Security Assertion Markup Language (SAML). SAML is an XML-based open standard for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP), which in this case is Security Cloud Sign On. Once integrated, users can then their usual single sign on credentials to sign in to

Security Cloud Sign

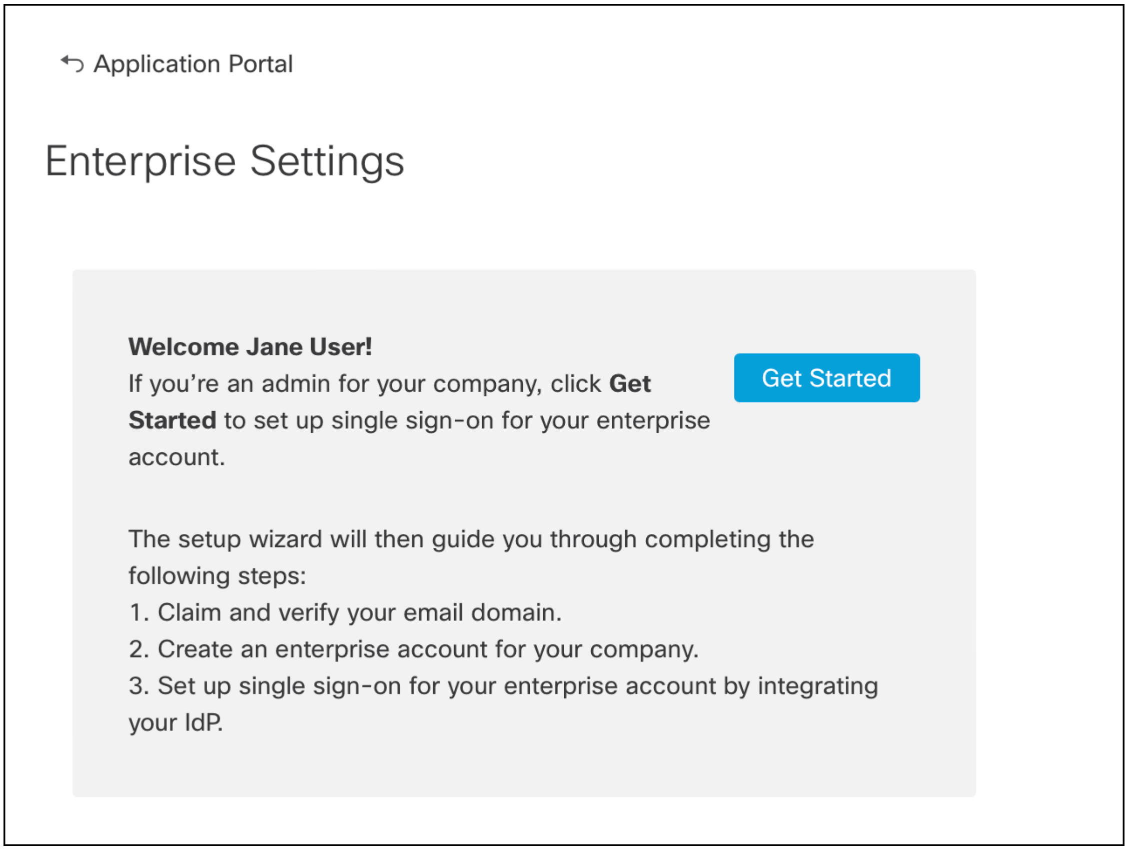


By default, Security Cloud Sign On enrolls all your IdP's users into Duo Multi-Factor Authentication (MFA) at no cost. If your organization already has MFA integrated with your IdP, you can optionally disable Duo-based MFA during the integration process.

Enterprise settings wizard

The Enterprise Settings setup wizard walks you multiple steps to integrate your own IdP with Security Cloud Sign On. The wizard saves your progress as you complete each step, so you can quit and return later to complete the process.

To open the Enterprise settings wizard, click your profile icon in the SecureX Application Portal, select **Enterprise Settings**, then click **Get Started**.



Enterprise Settings

Welcome Jane User!
If you're an admin for your company, click **Get Started** to set up single sign-on for your enterprise account.

The setup wizard will then guide you through completing the following steps:
1. Claim and verify your email domain.
2. Create an enterprise account for your company.
3. Set up single sign-on for your enterprise account by integrating your IdP.

The settings wizard lets you claim one email domain and configure one identity provider. You will need to open a case with Cisco TAC in the following cases:

- You need to configure more than one identity provider
- You need to claim more than one email domain
- You want to change your organization name or email domain after Step 2: Claim and verify your email domain

Note If you have an existing IdP integration that was **not** created with the Enterprise settings wizard, you can't use the wizard to modify your integration. See Customers with existing IdP integrations for details.

Step 1: Create an enterprise

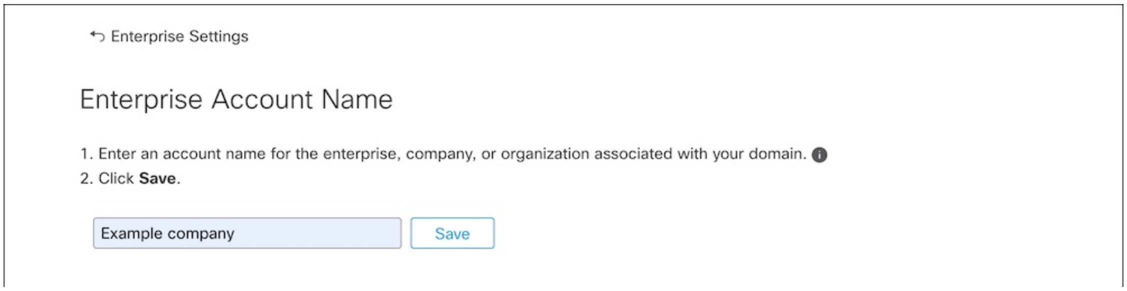
The first step is to create a named enterprise in Security Cloud Sign On. This enterprise will be associated with your claimed domain and identity provider configuration.

Step 1 Sign in to the SecureX Application Portal with a Security Cloud Sign On account.

Step 2 Click your profile icon in the upper right corner and select **Enterprise Settings**.

Step 3 Click **Get Started**.

Step 4 Enter a name for your enterprise account and click **Save**.



⮌ Enterprise Settings

Enterprise Account Name

1. Enter an account name for the enterprise, company, or organization associated with your domain.
2. Click **Save**.

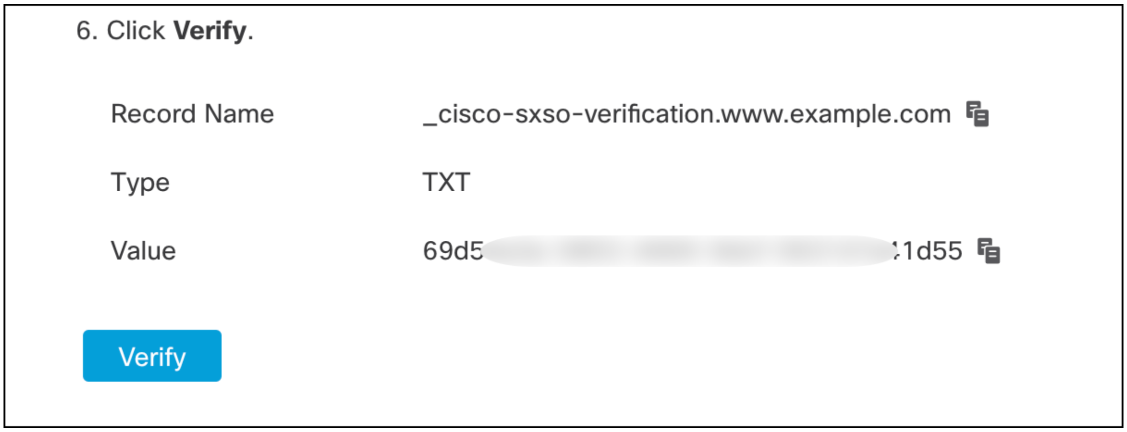
Example company

Step 2: Claim and verify your email domain

Next you'll claim and verify your enterprise's email domain. To complete this step you'll need to create a DNS record on your domain name registrar service portal. Once you've verified your domain you can delete the DNS record.

Step 1 Enter the domain you want to claim and click **Submit**.

The settings wizard displays a DNS TXT record name and value.



6. Click **Verify**.

Record Name _cisco-sxso-verification.www.example.com

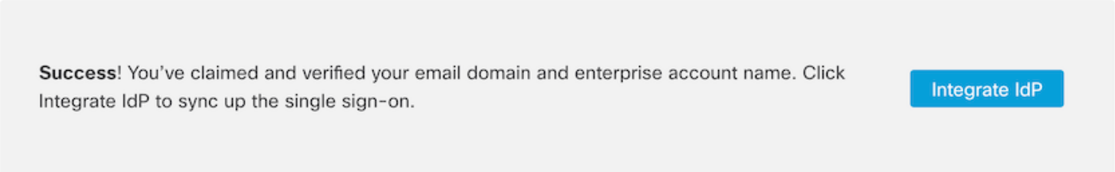
Type TXT

Value 69d5[redacted]1d55

Step 2 Sign in to your domain name registrar service and create a TXT record with the specified record name and value.

Step 3 Wait for the DNS record to propagate, then click **Verify**.

Step 4 If verification is successful, click **Integrate IdP** to begin integrating your identity provider.



Success! You've claimed and verified your email domain and enterprise account name. Click Integrate IdP to sync up the single sign-on.

Step 3: Exchange SAML metadata

In this step you'll exchange SAML metadata and signing certificates between your IdP and Security Cloud Sign On.

Before you begin

To complete this step you'll need the following information about the SAML integration you've created on your identity provider:

- **Single Sign-On Service URL** – The URL where Security Cloud Sign On will send a SAML Authentication Request via HTTP POST. The URL's domain must match the domain that you previously Step 2: Claim and verify your email domain.
- **Entity ID** – Uniquely identifies your identity provider to Security Cloud Sign On. In your IdP's SAML metadata it can be found in the `entityID` attribute of the `<EntityDescriptor>` element. It is called **Identity Provider Issuer** by some IdPs.
- **SAML signing certificate** – The x.509 signing certificate used by your IdP to sign SAML assertions.

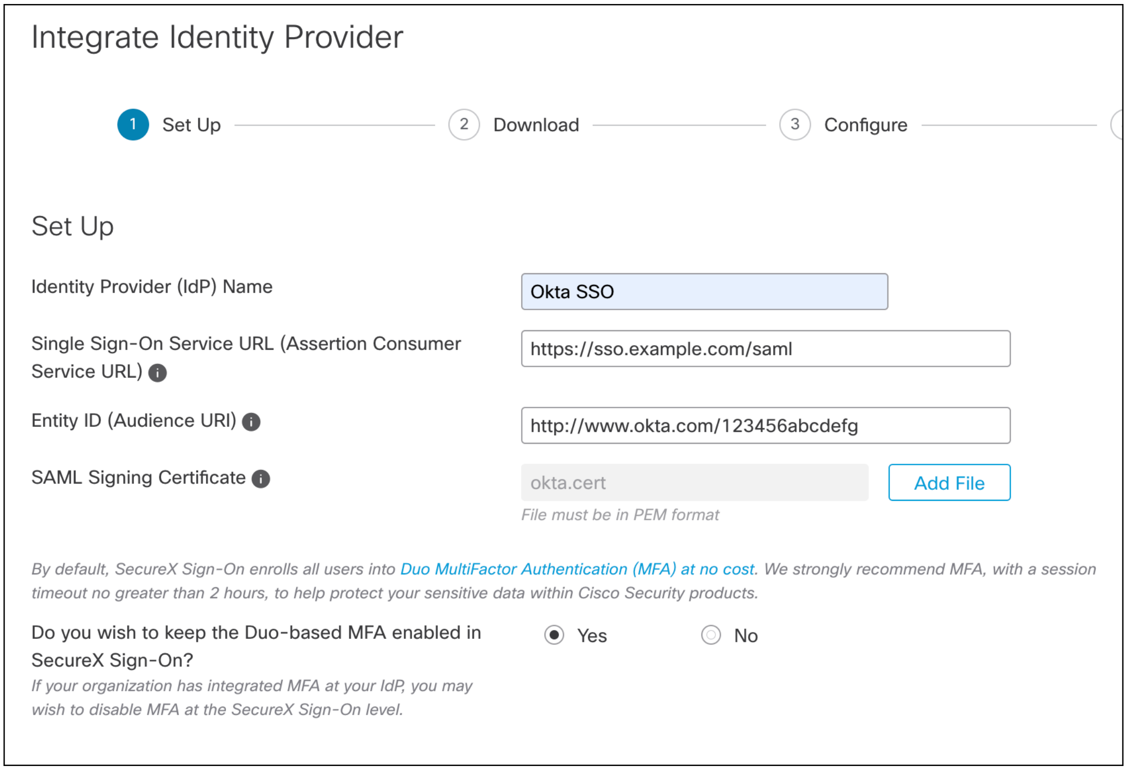
Note The certificate must be signed with the SHA-256 algorithm. Assertions signed with another algorithm are rejected with an HTTP 400 error.

Step 1 In the **Identity Provider Name** field enter a name for your IdP in the **Set Up** screen.

Step 2 Enter the values for **Single Sign-On Service URL** and **Entity ID** that you obtained from your IdP's SAML integration.

Step 3 Click **Add File** and select the SAML signing certificate you previously download from your IdP.

Step 4 If you don't want to automatically enroll your users in Duo MFA, select **No** for **Do you wish to keep the Duo-based MFA enabled in Security Cloud Sign On?**



Integrate Identity Provider

Set Up

Identity Provider (IdP) Name: Okta SSO

Single Sign-On Service URL (Assertion Consumer Service URL): https://sso.example.com/saml

Entity ID (Audience URI): http://www.okta.com/123456abcdefg

SAML Signing Certificate: okta.cert

File must be in PEM format

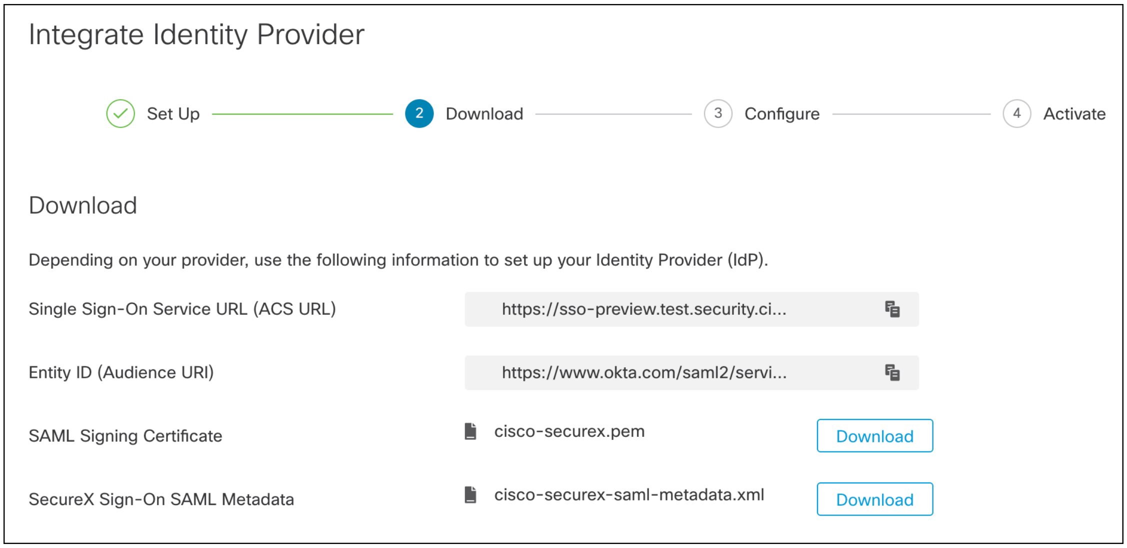
By default, SecureX Sign-On enrolls all users into Duo MultiFactor Authentication (MFA) at no cost. We strongly recommend MFA, with a session timeout no greater than 2 hours, to help protect your sensitive data within Cisco Security products.

Do you wish to keep the Duo-based MFA enabled in SecureX Sign-On? ● Yes ○ No

If your organization has integrated MFA at your IdP, you may wish to disable MFA at the SecureX Sign-On level.

Step 5 Click **Next** to advance to the **Download** screen.

Step 6 Copy the displayed **Single Sign-On Service (ACS URL)** and **Entity ID (Audience URL)**, and download the **SAML Signing Certificate**.



Integrate Identity Provider

Download

Depending on your provider, use the following information to set up your Identity Provider (IdP).

Single Sign-On Service URL (ACS URL): https://sso-preview.test.security.ci...

Entity ID (Audience URI): https://www.okta.com/saml2/servi...

SAML Signing Certificate: cisco-securex.pem

SecureX Sign-On SAML Metadata: cisco-securex-saml-metadata.xml

Step 7 7. Click **Next** to advance to the **Configure** screen.

Step 8 Open your the SAML application configuration page on your IdP management console and make the following changes:

a) Update the temporary values assigned to **ACS URL** and **Entity ID** with the values you obtained in the previous step.

b) Upload the SAML signing certificate provided by the settings wizard.

Note Some IdPs (Auth0, for example) require you to provide the contents of the certificate as a single-line JSON string (`-----BEGIN CERTIFICATE-----\n...\n...\n-----END CERTIFICATE-----\n`, for example).

c) Save the configuration changes to your SAML app configuration.

What to do next

Next, you'll test the IdP integration with your enterprise.

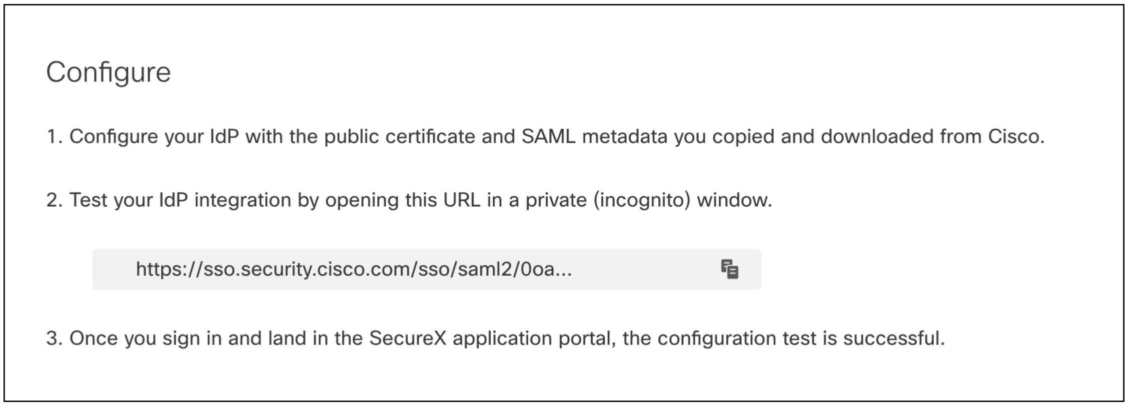
Step 4: Test the SSO integration

Next you'll test your IdP's integration by initiating an SSO request from the enterprise wizard to your IdP. If you land back in the SecureX Application Dashboard it means test was successful.

- Test the URL in a private (incognito) window.
- The email domain used to sign in must match the Step 2: Claim and verify your email domain you claimed previously.
- Test with new users (those without an existing Security Cloud Sign On account) as well as existing users.

Step 1 Return to the Enterprise settings wizard's **Configure** screen.

Step 2 Copy the SSO URL in **Step 2** to your clipboard and open it in a private (incognito) browser window.



Configure

1. Configure your IdP with the public certificate and SAML metadata you copied and downloaded from Cisco.

2. Test your IdP integration by opening this URL in a private (incognito) window.

https://sso.security.cisco.com/sso/saml2/0oa...

3. Once you sign in and land in the SecureX application portal, the configuration test is successful.

Step 3 Sign in to your identity provider.

- The email domain used to sign in must match the Step 2: Claim and verify your email domain you claimed previously.
- Test with an account other than the one you used to initially sign up with Secure Cloud Sign On. For instance, if you used the admin@example.com account to sign up and create the IdP integration, don't use that same email to test the integration.

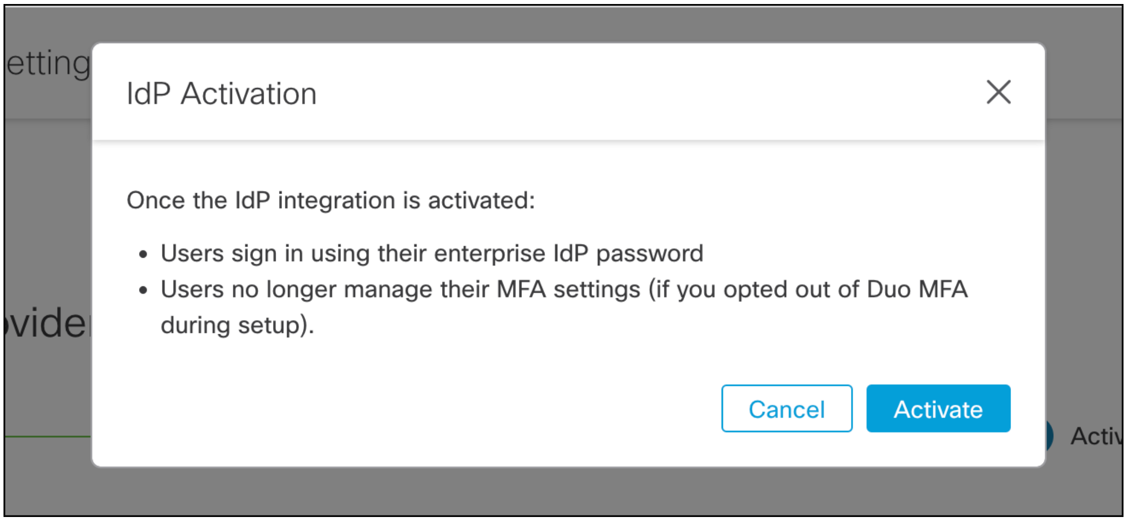
Once you land in the SecureX Application Portal, the configuration test is successful. See Troubleshooting if you encounter an error during the SSO process.

Step 4 Once you've tested the integration, click **Next** to advance to the **Activate** page.

Step 5: Activate IdP integration

Once you've Step 4: Test the SSO integration and are ready to to enable it for your organization, you can activate it. Once activated, users sign in using their enterprise (IdP) email address and password. If you opted out of free Duo MFA enrollment, your users will no longer manage their MFA settings.

To activate the integration with your IdP and Security Cloud Sign On click **Activate my IdP**, then click **Activate** in the confirmation dialog.



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).