Enabling Cisco SecureX Sign-On for Secure Endpoint

A Cisco SecureX sign-on account is a new account for use across all Cisco security products. You can learn more about it at https://cisco.com/go/securesignon.

This document describes how to enable Cisco SecureX sign-on for use as your single sign-on provider for Cisco Secure Endpoint.

Caveats

Keep the following caveats in mind when enabling Cisco SecureX sign-on for Secure Endpoint:

- Using Cisco SecureX Sign-On as your SAML provider requires all accounts in your organization to have existing Cisco SecureX sign-on accounts. You can create Cisco SecureX sign-on accounts at https://sign-on.security.cisco.com. Users will receive an email and must activate their accounts within 7 days. Users without an account will not be able to sign in.

- All user passwords will be reset to prevent users from logging in using the standard username and password mechanism. Admin users will be able to create a one-time password.

- Two-factor authentication will be disabled for each user. You will need to re-enable two-factor authentication if you disable single sign-on.

Enable Cisco SecureX Sign-On for Secure Endpoint

To enable Cisco SecureX sign-on for your business:

1. Log in to your Secure Endpoint administrator account.

2. Go to Accounts > Organization Settings.


4. Select Cisco SecureX sign-on. This takes you to the SAML Configuration page.
5. Go to https://sign-on.security.cisco.com and click **Create a SecureX Sign-On** to create a Cisco SecureX sign-on account. For more information about creating this account, see Cisco SecureX Sign-On Quick Start Guide.

   **Note:** Using Cisco SecureX sign-on as your SAML provider requires all accounts in your organization to have existing Cisco SecureX sign-on accounts. You can create Cisco SecureX sign-on accounts at https://sign-on.security.cisco.com. Users without an account will not be able to sign in.

6. Once your account is created, return to the SAML Configuration screen, and click **Verify Configuration**.

7. Sign in with the credentials provided when you created the Cisco SecureX sign-on account. You are prompted to log in with Duo Security as a second authentication factor.

8. Once you have verified your configuration, note the caveats listed on the SAML configuration page then click **Enable Cisco SecureX Sign-On** to complete the setup.

9. An email is sent to each user with instructions on how to log in. Instead of entering their username and password, users must now log in by entering their email address, then clicking **Log In**, then signing in from the SecureX sign-on page. If the user has not already authenticated to the identity provider they are redirected to do so.