Cisco SecureX Sign-On Guide

First Published: 2020-06-09

Last Modified: 2022-09-29

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CHAPTER 1

Introduction

Overview

SecureX is a cloud-native, built-in platform experience that connects our Cisco Secure portfolio and your infrastructure. It is integrated and open for simplicity, unified in one location for visibility, and maximizes operational efficiency with automated workflows to secure your network, endpoints, cloud, and applications.

This document summarizes how to sign in to SecureX for the first time. The method you use is determined by the Cisco Secure product(s) you have purchased and whether you are a new or existing user of the product(s). To proceed, choose one of the following options:

- New to SecureX
- Invited to SecureX

CHAPTER 2

What's New

Check for Pending Invitations and Matched Domains

Starting on April 28, 2022, a new page is shown to new users during their first sign-on process. The new page shows:

- if you've been invited to join an existing organization activated in SecureX, so you may click to join
- if there are any existing organizations that match your email domain which are already activated in SecureX, so you may request to join
- a section to create a new organization that doesn't already exist in SecureX

Simplified Sign-On

Starting on November 24, 2021, the sign-on process has been simplified to improve the user experience.

Once you enter your email address or username, the sign-on system automatically detects and routes you to the appropriate IdP, where you can directly sign-on with your account:

- third-party IdP (including Cisco.com)
- SecureX Sign-On
- Cisco Customer Identity (CCI)
- Cisco Security Accounts (CSA)

If what you provided cannot be found, you are offered other login options, such as Secure Malware Analytics and Microsoft.

Update Cisco Security Accounts to SecureX Sign-On

Starting in August 2021, all users with a Cisco Security Accounts (CSA) account must be updated to use a SecureX sign-on account instead. This affects all users that sign in with CSA to access Cisco Security products such as:

- Cisco Secure Endpoint (formerly Advanced Malware Protection for Endpoints)
- Global Threat Alerts (formerly Cognitive Intelligence and Cognitive Threat Analytics)
- Orbital
- SecureX

CSA will be retired, so going forward, you'll use SecureX sign-on to access SecureX and other Cisco Security products. For instructions on how you'll need to update your account, see how to Update Cisco Security Accounts to SecureX Sign-On.

CHAPTER 3

New to SecureX

New to SecureX

This procedure describes the first-time SecureX sign-on experience for users new to SecureX.

Note Threat Response does not use a SecureX sign-on account. Instead, Threat Response uses either a Cisco Security Accounts (CSA) account or a Secure Malware Analytics (formerly Threat Grid) account. So, if you were to create and sign in with a SecureX sign-on account, the modules and users you have already set up in Threat Response would not appear in SecureX.

Therefore, if you’re already using Threat Response, use your same existing account for SecureX. If you don't have a Threat Response organization currently in use with modules already set up, then you can use a SecureX sign-on account and connect SecureX with your Cisco Security products.

Step 1 Go to https://security.cisco.com.

Step 2 Select your region of the world, and click **Next**.

Step 3 Enter your username email address, and click **Next**.

Note Alternatively, signing in with your third-party IdP account allows you to bypass setting up a SecureX sign-on account. Click **Other login options**.

Step 4 If you're an existing user of Secure Endpoint (formerly Advanced Malware Protection for Endpoints) or Threat Response and also have a Threat Response instance with existing modules, sign in with your CSA account email and password.

Step 5 If you're an existing user of Secure Malware Analytics (formerly Threat Grid), click **Secure Malware Analytics** and sign in with your Secure Malware Analytics account username and password.

Step 6 Don't have a SecureX sign-on account yet?

a) Create an account by completing Step 4 in the Quick Start Guide.

b) Select your region of the world, and click the respective SecureX launch tile.

Step 7 Sign in with your SecureX sign-on account password.

a) Are you a member of multiple organizations? If yes, you're prompted to choose which organization account to continue with. If you're not a member of any organization but have been invited, any pending invitations for you to join an organization are displayed here. Click **Join** to accept the pending invitation.

b) You may also be shown a list of existing organizations activated in SecureX that match your email domain. If so, click **Request Access** to send an email to the organization admin or admins asking to approve your request to join their organization. You have the option to request access to more than one organization.

- **Pending Access**—Once the request is sent, the organization admin or admins receive an email in which they can choose to grant you access as a user, grant you access as an admin, or reject your request.
- If your request is granted, you'll receive an email notifying you that you can now sign in to the organization in SecureX.
- **Access Rejected**—If your request is rejected, you'll be notified and not be given access to the organization. If needed, you can ask an admin user to send you an invitation in SecureX.

c) If you're the first in your organization to use SecureX or do not have any pending invitations and matched organizations, click **Create Organization** near the bottom of the page and enter your organization's details to create your new organization in SecureX.

Step 8 To start using SecureX, activate your account by enabling an integration module in the SecureX Demo. SecureX Demo is displayed to familiarize you with SecureX and assist you with activating your account. To get started, click **Enable SecureX**.

What to do next

Once you're signed in to SecureX with an activated account, you can customize your environment, including:

- configure additional product integration modules
- configure multiple dashboards
- configure dashboard tiles
- activate SecureX orchestration
- invite users to SecureX

For more information, see the FAQ in this guide and online help in SecureX.

CHAPTER 4

Invited to SecureX

Invited to SecureX

This procedure describes the first-time SecureX sign-on experience for users invited to SecureX.

Step 1 Are you an existing user of Secure Endpoint (formerly Advanced Malware Protection for Endpoints) or Threat Response? If yes, you received an email invitation with the subject "Welcome to Cisco Security" from your Cisco Security Accounts (CSA) administrator at no-reply@amp.cisco.com. Skip to Step 6.

Step 2 Are you an existing user of Secure Malware Analytics (formerly Threat Grid)? If yes, you received an email invitation from your Secure Malware Analytics administrator. Skip to Step 7.

Step 3 Click the secure link in your SecureX email invitation from no-reply@security.cisco.com.

Step 4 If you have a SecureX sign-on account:

a) Click and sign in with your SecureX sign-on account.

b) Click to join the organization. If you are a member of multiple organizations, choose your organization to launch into that SecureX dashboard.

c) Skip to Step 8.

Step 5 Create a SecureX sign-on account.

a) Complete Step 4 in the Quick Start Guide.

b) Select your region of the world, and click the respective SecureX launch tile.

c) Skip to Step 8.

Step 6 Click the secure link in your CSA email invitation.

Note If your CSA account is configured to delegate single sign-on to SecureX sign-on, click **Use Single Sign-On**, enter your username to **Log In**, and go to Step 4.

a) Create and validate your CSA account.

b) On the CSA portal page, click the SecureX launch tile.

c) Skip to Step 8.

Step 7 Click the secure link in your Secure Malware Analytics email invitation.

a) Create a password for your account.

b) Read the End User Agreement, and click **I Agree** to accept.

c) On the https://security.cisco.com page, sign in with your Secure Malware Analytics account.

Step 8 Are you the first in your organization to use SecureX? If yes, you'll be prompted to enter its details to create your organization in SecureX.

Important If you believe that you're a member of an existing organization in SecureX, do not create a new organization. Instead, request an invitation from the admin to join the existing organization.

Step 9 To start using SecureX, activate your account by enabling an integration module in the SecureX Demo. SecureX Demo is displayed to familiarize you with SecureX and assist you with activating your account. To get started, click **Enable SecureX**.

What to do next

Once you're signed in to SecureX with an activated account, you can customize your environment, including:

- configure additional product integration modules
- configure multiple dashboards
- configure dashboard tiles
- activate SecureX orchestration
- invite users to SecureX

For more information, see the FAQ in this guide and online help in SecureX.

CHAPTER 5

Frequently Asked Questions

Frequently Asked Questions

If I signed in with my CSA account, how do I invite users to SecureX?

If you're a CSA administrator, go to the appropriate URL for your regional cloud:

- North America: https://castle.amp.cisco.com
- Europe: https://castle.eu.amp.cisco.com
- Asia: https://castle.apjc.amp.cisco.com

Click **Users** to add or edit user access.

If I signed in with my Secure Malware Analytics account, how do I invite users to SecureX?

In Secure Malware Analytics, click **Help** > **Using Secure Malware Analytics Online Help** > **Managing Secure Malware Analytics Users**.

If I signed in with my SecureX account, how do I invite users to SecureX?

In SecureX, click **Administration** > **Manage Users** > **Invite Users**.

What if I'm not yet a Cisco Security customer?

You need to activate a Cisco Security product in order to use SecureX, which requires no purchase because it is built in. Try our products for free.

If I sign in with my Cisco Security Account, which I use with Secure Endpoint, does that mean I can't integrate SecureX with all my other products?

No matter how you sign in to SecureX, you can integrate it with all your products by connecting to their cloud APIs or onboarding connections to their on-prem devices. For example, if you're using Threat Response, keep using the same account to sign in to SecureX. All your Threat Response integrations will be there and waiting in SecureX. If you're not using Threat Response, you can use a SecureX sign-on account to sign in to your

SecureX, Secure Endpoint, Cisco Defense Orchestrator, Cloudlock, Meraki, Secure Cloud Analytics, and Umbrella dashboards (with more to come).

What if I have more questions?

Check out the SecureX support topics in Cisco Community, or open a support case.

Additional resources?

Please refer to these resources for additional information:

- Cisco SecureX Help Center
- Cisco SecureX product page
- Cisco SecureX support documentation

PART I

Appendix

CHAPTER 6

Update Cisco Security Accounts to SecureX Sign-On

Overview

Starting in August 2021, all users with a Cisco Security Accounts (CSA) account must be updated to use a SecureX sign-on account instead. This affects all users that sign in with CSA to access Cisco Security products such as:

- Cisco Secure Endpoint (formerly Advanced Malware Protection for Endpoints)
- Global Threat Alerts (formerly Cognitive Intelligence and Cognitive Threat Analytics)
- Orbital
- SecureX

CSA will be retired, so going forward, you'll use SecureX sign-on to access SecureX and other Cisco Security products. How you'll update your account depends on your account role in your organization and whether you already have a SecureX sign-on account delegated as your single sign-on for CSA. To proceed, choose one of the following options:

- Administrator Account
- Non-administrator Account
- Administrator with Delegated SecureX Sign-On Account
- Non-administrator with Delegated SecureX Sign-On Account

Administrator Account

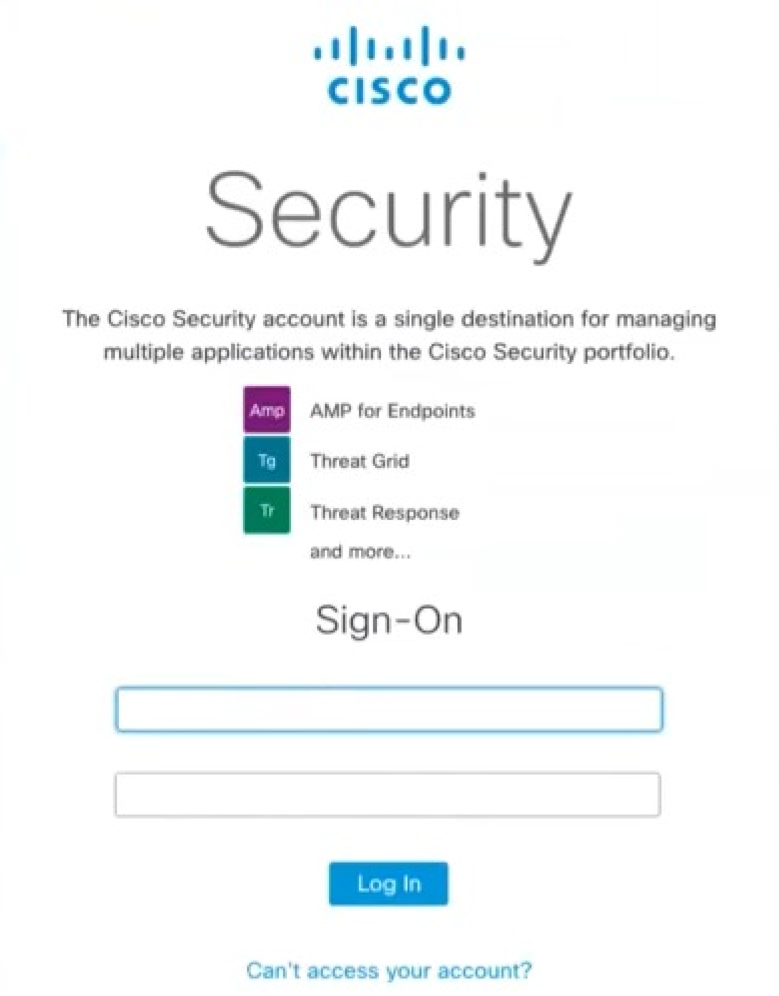
Before you begin

Important Only Castle users will be migrated. So prior to migration, review your users in Castle. Verify that all users under Castle are valid, accurate, and up-to-date, as only they'll receive the invite to create their SecureX sign-on account using their CSA email address.

- North America: https://castle.amp.cisco.com
- Europe: https://castle.eu.amp.cisco.com
- Asia: https://castle.apjc.amp.cisco.com

Step 1 As an account administrator, sign in using your CSA email and password, as you normally would. Click **Log In**.

Figure 1:

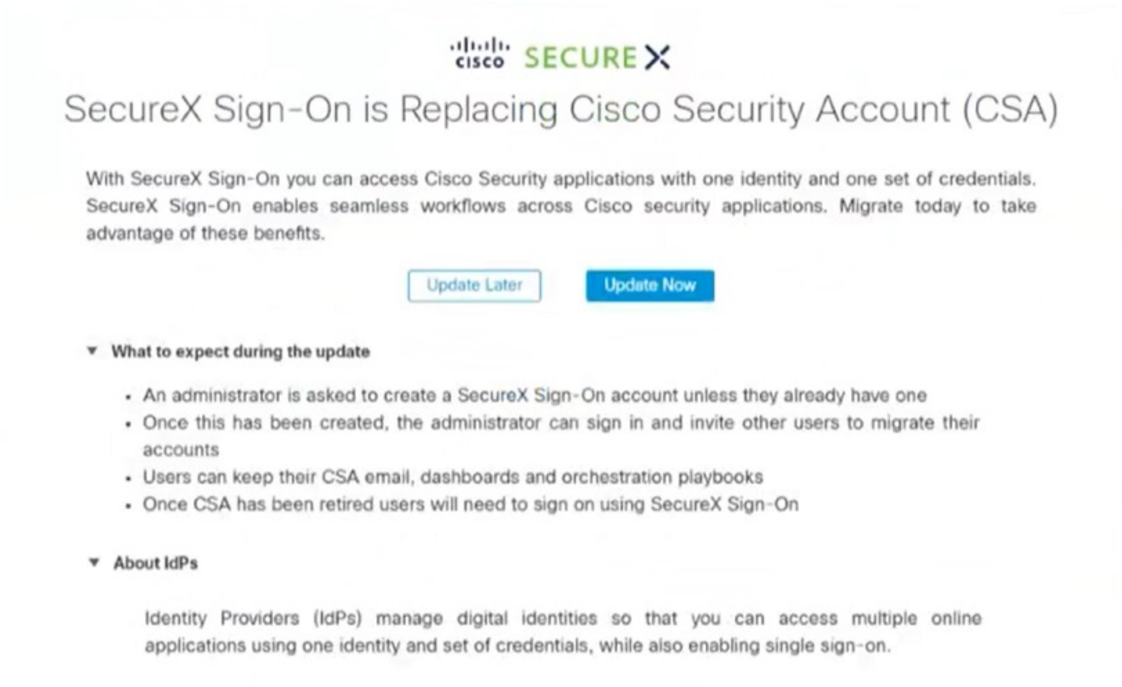


Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

Step 2 Once Cisco has enabled your organization for migration, you should see the **SecureX Sign-On is Replacing Cisco Security Account** page.

Figure 2:



SecureX Sign-On is Replacing Cisco Security Account (CSA)

With SecureX Sign-On you can access Cisco Security applications with one identity and one set of credentials. SecureX Sign-On enables seamless workflows across Cisco security applications. Migrate today to take advantage of these benefits.

▼ **What to expect during the update**

- An administrator is asked to create a SecureX Sign-On account unless they already have one
- Once this has been created, the administrator can sign in and invite other users to migrate their accounts
- Users can keep their CSA email, dashboards and orchestration playbooks
- Once CSA has been retired users will need to sign on using SecureX Sign-On

▼ **About IdPs**

Identity Providers (IdPs) manage digital identities so that you can access multiple online applications using one identity and set of credentials, while also enabling single sign-on.

a) If you're not ready to begin the migration, click **Update Later**. You will land in your respective Cisco Security product for now and can begin the migration the next time you sign in.

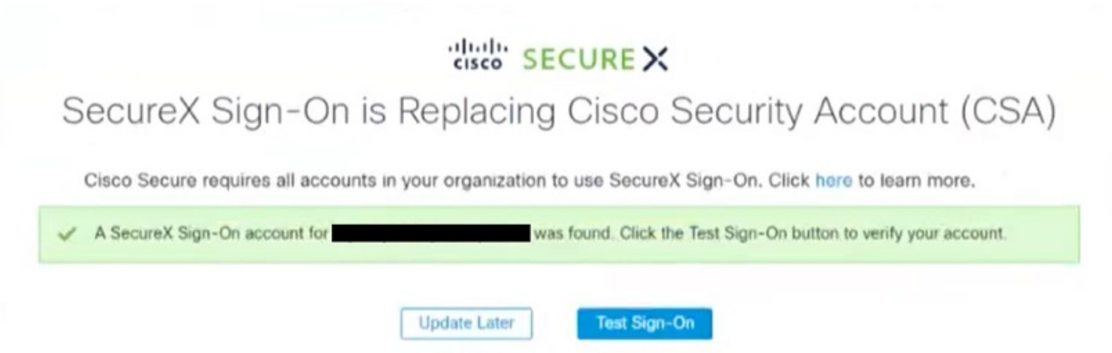
b) If you're ready to begin the migration, click **Update Now**.

Step 3 SecureX checks to see whether you have a SecureX sign-on account that has already been migrated.

a) If SecureX sees an account for you:

1. Looks like you have already set up your account. Click **Test Sign-On**.

Figure 3:



SecureX Sign-On is Replacing Cisco Security Account (CSA)

Cisco Secure requires all accounts in your organization to use SecureX Sign-On. Click here to learn more.

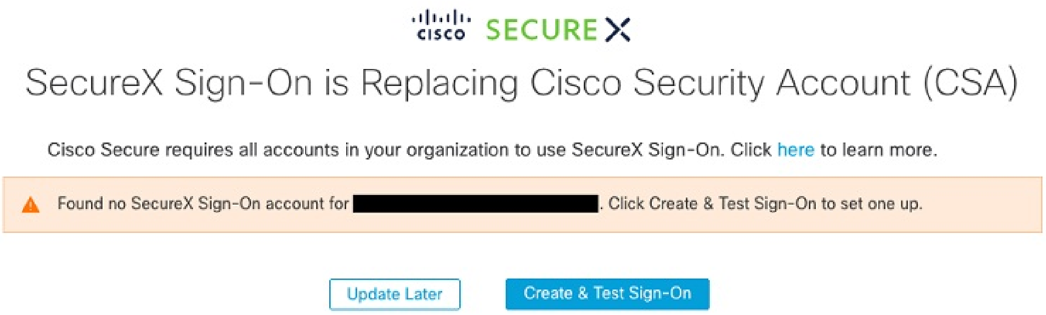
✓ A SecureX Sign-On account for [redacted] was found. Click the Test Sign-On button to verify your account.

2. On the SecureX Sign-On page, enter your SecureX username and password to sign in with your SecureX sign-on account.

b) If SecureX does not see an account for you:

1. You do not seem to have set up your account yet. Click **Create & Test Sign-On**.

   Figure 4:



SecureX Sign-On is Replacing Cisco Security Account (CSA)

Cisco Secure requires all accounts in your organization to use SecureX Sign-On. Click here to learn more.

⚠ Found no SecureX Sign-On account for [redacted]. Click Create & Test Sign-On to set one up.

2. On the SecureX Sign-On page, click **Sign up**.

   Note Or, you may click **Other login options** to continue by using an alternate account such as:

   - Sign in with Cisco if you're a Cisco employee or customer with a Cisco.com account used solely by you.
   - Sign in with Microsoft if your company maintains employee accounts in Microsoft Azure Active Directory.

3. Note that when you update your CSA to a SecureX sign-on account, the email address you use for your SecureX username *must match* your CSA email address, or you'll lose access to your tenant. Enter your account information, and click **Create Account**. Cisco will send you a verification email.

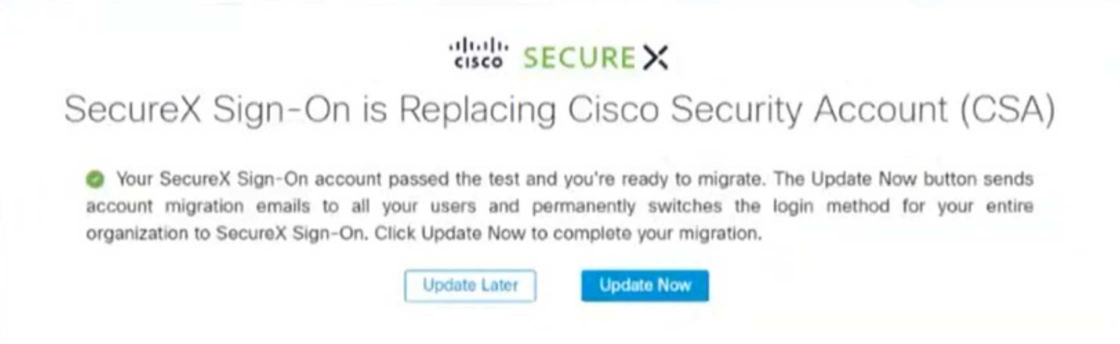
4. Find the no-reply email with the subject "Activate Account" from Cisco (@cisco.com, @external.cisco.com, or @security.cisco.com). Click the **Activate Account** button.

5. Follow the prompts to set up multifactor authentication by configuring Duo Security. For more information, see Step 4 in the Quick Start Guide.

Step 4 When you see the next **SecureX Sign-On is Replacing Cisco Security Account** page, your new SecureX sign-on account passed the test and you're ready to migrate the rest of your organization.

Note If you do not see the expected page, open a new browser session and restart the update process.

Figure 5:



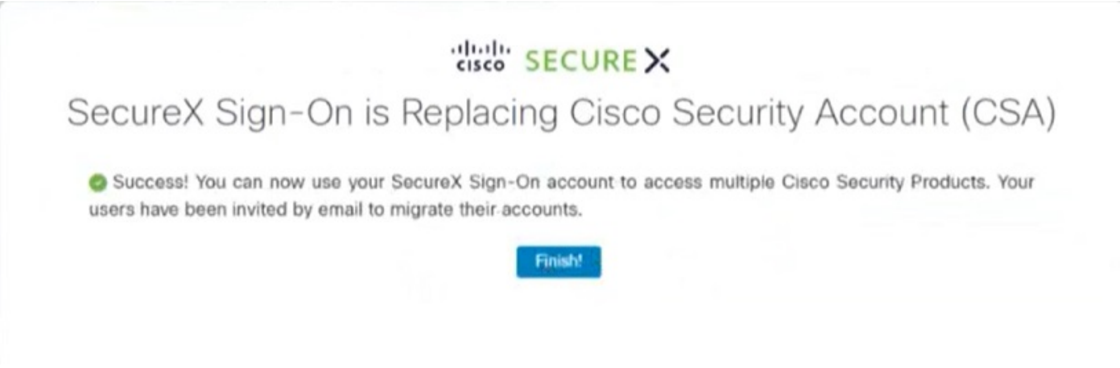
SecureX Sign-On is Replacing Cisco Security Account (CSA)

Your SecureX Sign-On account passed the test and you're ready to migrate. The Update Now button sends account migration emails to all your users and permanently switches the login method for your entire organization to SecureX Sign-On. Click Update Now to complete your migration.

a) If you're not ready to complete the migration, note the deadline and how many days remain. Then click **Update Later**. You will land in your respective Cisco Security product for now and can complete the migration the next time you sign in.
b) Note that all users in your organization will be signed out of the system during the migration. If you're ready to complete the migration, click **Update Now**.

Step 5 Success! The remaining users in your organization will now be invited by email to also create their SecureX sign-on accounts. Click **Finish!** to land in your respective Cisco Security product.

Figure 6:



SecureX Sign-On is Replacing Cisco Security Account (CSA)

Success! You can now use your SecureX Sign-On account to access multiple Cisco Security Products. Your users have been invited by email to migrate their accounts.

What to do next

From now on, when you try to sign in with CSA, once you enter your email address, Cisco will recognize that your account has been migrated to SecureX sign-on. So, when you then click **Log In**, you'll be redirected. When you land on the SecureX sign-on page, enter your SecureX username and password to sign in and access all your Cisco Security products. Once CSA has been retired, users must sign in using SecureX sign-on.

Non-administrator Account

Step 1 Once your administrator has updated your organization's authentication method, you should receive a notification email from no-reply@amp.cisco.com about the update to your account and your next action required. Click the **Create Account** link, and you'll be directed to the SecureX Sign-On page.

Step 2 If you cannot find the email in Step 1, try to sign in using CSA, as you normally would. You'll be directed to the SecureX Sign-On page. Click **Sign up**.

Note Or, you may click **Other login options** to continue by using an alternate account such as:

- Sign in with Cisco if you're a Cisco employee or customer with a Cisco.com account used solely by you.
- Sign in with Microsoft if your company maintains employee accounts in Microsoft Azure Active Directory.

Step 3 When you update your CSA to a SecureX sign-on account, the email address you use for your SecureX username *must match* your CSA email address, or you'll lose access to your tenant. Enter your account information, and click **Create Account**. Cisco will send you a verification email.

Step 4 Find the no-reply email with the subject "Activate Account" from Cisco (@cisco.com, @external.cisco.com, or @security.cisco.com). Click the **Activate Account** button.

Step 5 Follow the prompts to set up multifactor authentication by configuring Duo Security. For more information, see Step 4 in the Quick Start Guide.

Step 6 Success!

What to do next

From now on, when you try to sign in with CSA, once you enter your email address, Cisco will recognize that your account has been migrated to SecureX sign-on. So, when you then click **Log In**, you'll be redirected. When you land on the SecureX sign-on page, enter your SecureX username and password to sign in and access all your Cisco Security products. Once CSA has been retired, users must sign in using SecureX sign-on.

Administrator with Delegated SecureX Sign-On Account

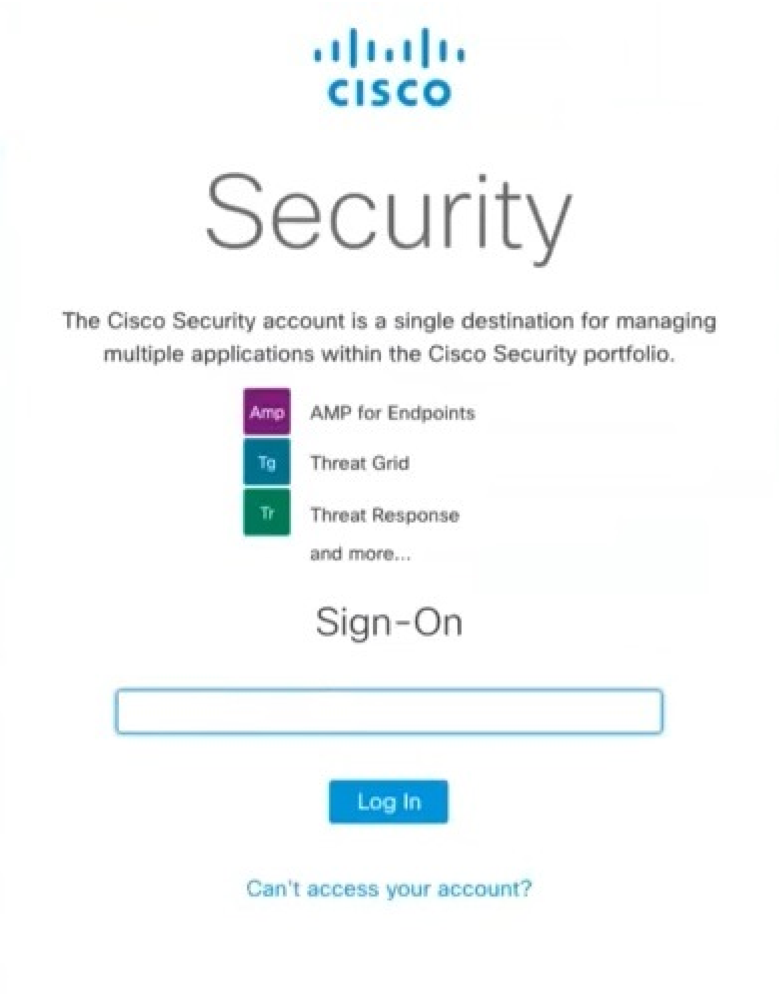
Before you begin

Important Only Castle users will be migrated. So prior to migration, review your users in Castle. Verify that all users under Castle are valid, accurate, and up-to-date, as only they'll receive the invite to create their SecureX sign-on account using their CSA email address.

- North America: https://castle.amp.cisco.com
- Europe: https://castle.eu.amp.cisco.com
- Asia: https://castle.apjc.amp.cisco.com

Step 1 As an account administrator, enter your CSA email, as you normally would. Click **Log In**.

Figure 7:



Security

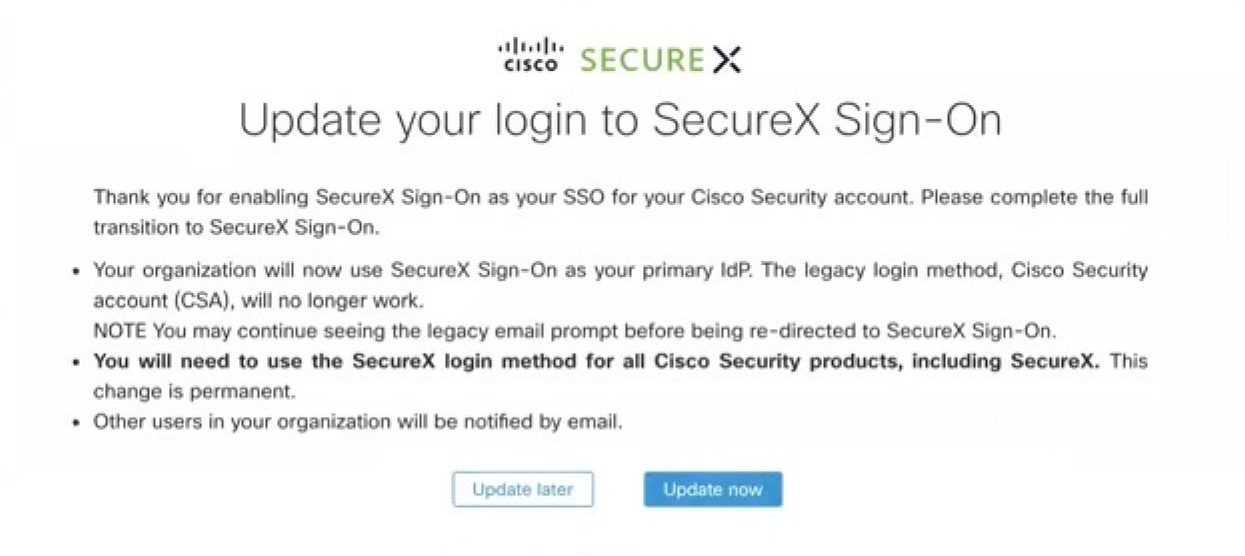
The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

Step 2 The system recognizes that you already have a SecureX sign-on account and directs you to the SecureX Sign-On page, where you'll enter your SecureX username and password to sign in with your SecureX sign-on account.

Step 3 You should see the **Update your login to SecureX Sign-On** page.

Note If you do not see the expected page, open a new browser session and restart the update process.

Figure 8:



cisco SECUREX

Update your login to SecureX Sign-On

Thank you for enabling SecureX Sign-On as your SSO for your Cisco Security account. Please complete the full transition to SecureX Sign-On.

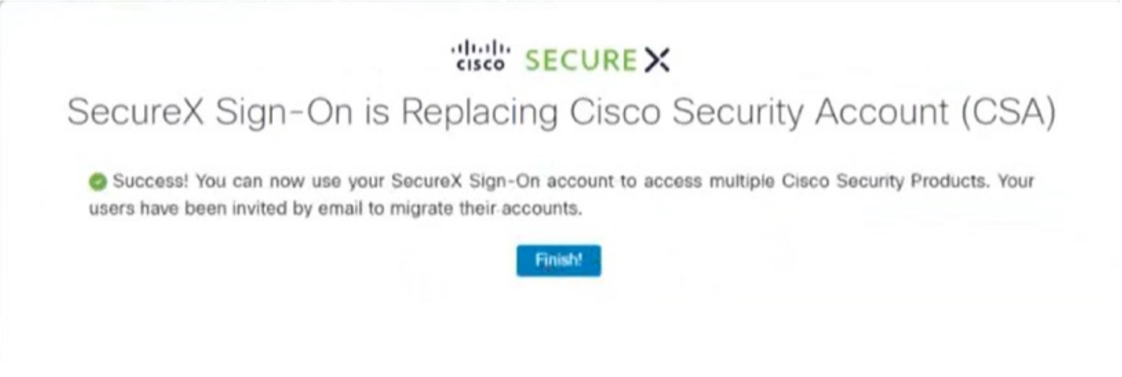
- Your organization will now use SecureX Sign-On as your primary IdP. The legacy login method, Cisco Security account (CSA), will no longer work.
  NOTE You may continue seeing the legacy email prompt before being re-directed to SecureX Sign-On.
- **You will need to use the SecureX login method for all Cisco Security products, including SecureX.** This change is permanent.
- Other users in your organization will be notified by email.

a) If you're not yet ready to complete the update, click **Update later**. You will land in your respective Cisco Security product for now and can complete the update the next time you sign in.

b) If you're ready to complete the update, click **Update now**.

Step 4 Success! Your SecureX sign-on account has been updated. The remaining users in your organization will now be invited by email to also update their SecureX sign-on accounts. Click **Finish!** to land in your respective Cisco Security product.

Figure 9:



cisco SECUREX

SecureX Sign-On is Replacing Cisco Security Account (CSA)

Success! You can now use your SecureX Sign-On account to access multiple Cisco Security Products. Your users have been invited by email to migrate their accounts.

What to do next

From now on, when you try to sign in with CSA, once you enter your email address, Cisco will recognize that your account has been migrated to SecureX sign-on. So, when you then click **Log In**, you'll be redirected. When you land on the SecureX sign-on page, enter your SecureX username and password to sign in and access all your Cisco Security products. Once CSA has been retired, users must sign in using SecureX sign-on.

Non-administrator with Delegated SecureX Sign-On Account

Step 1 Once your administrator has updated your organization's authentication method, you should receive a notification email from no-reply@amp.cisco.com about the update to your account.

Step 2 If you cannot find the email in Step 1, try to sign in using CSA, as your normally would. The system recognizes that you already have a SecureX sign-on account and directs you to the SecureX Sign-On page, where you'll enter your SecureX username and password to sign in with your SecureX sign-on account.

Note Or, you may click **Other login options** to continue by using an alternate account such as:

- Sign in with Cisco if you're a Cisco employee or customer with a Cisco.com account used solely by you.
- Sign in with Microsoft if your company maintains employee accounts in Microsoft Azure Active Directory.

Step 3 Success!

What to do next

From now on, when you try to sign in with CSA, once you enter your email address, Cisco will recognize that your account has been migrated to SecureX sign-on. So, when you then click **Log In**, you'll be redirected. When you land on the SecureX sign-on page, enter your SecureX username and password to sign in and access all your Cisco Security products. Once CSA has been retired, users must sign in using SecureX sign-on.

Frequently Asked Questions

In Cisco Secure Endpoint (formerly AMP), how do I tell if I have a SecureX sign-on account delegated as single sign-on for my organization?

In your Secure Endpoint console, navigate to **Accounts** > **Organization Settings**. Scroll down to the Features section. The Single Sign-On setting shows how single sign-on is configured for your organization.

My Secure Endpoint account was different in each region (North America, EU, and APJC) of the world. Will this new account also be regional?

Cisco SecureX sign-on accounts are global; you'll use the same password to sign in to any of those regions. Your account userid is added or removed to organizations in any region you access. You have one account, but you can use it to access multiple organizations in multiple regions.

Will I still add users to Secure Endpoint or Castle for accessing all of these products?

To add users, add them to each product and organization you want them to access. Add Secure Endpoint, Global Threat Alerts (formerly Cognitive Intelligence and Cognitive Threat Analytics), and Orbital users in the Secure Endpoint users console. Add SecureX users directly in SecureX. Manage users in SecureX, and give them write access. Users' permissions and access levels are also controlled and managed in each product.

Going forward, what will I need to create a Secure Endpoint account for a new user?

You'll need the user's email address in your organization. A user's first and last names are no longer needed. Once the user receives the email invite (from no-reply@amp.cisco.com) and signs in to Secure Endpoint using SecureX sign-on, their first and last names will automatically be retroactively populated into their account record. A user can go to My Account in the Secure Endpoint console and pivot to the SecureX User Identity Settings page to verify and edit their first and last names.

I'm logging into Secure Endpoint in EU. Is my new account stored in the EU?

No, it's currently stored globally in North America. To learn more, see our privacy data sheet.

I updated my account, but I'd rather go back to my old account? What do I do?

Your old account is no longer available. We have retired the old Cisco Security Accounts and are migrating to SecureX sign-on for all accounts. If you're having trouble with your new account, please open a support case.

I've already integrated Umbrella into Azure. Will this update to using SecureX sign-on impact the integration?

No, this update will not impact third-party IdP integrations with individual applications.