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

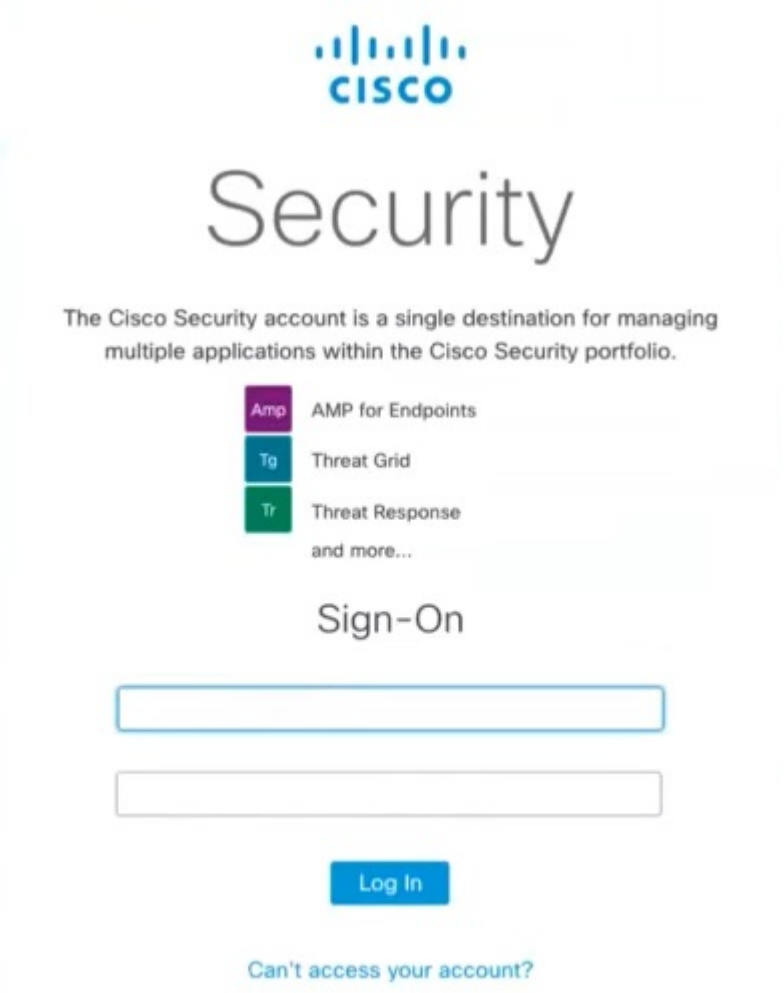
Before you begin

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:



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:

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:

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:

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.

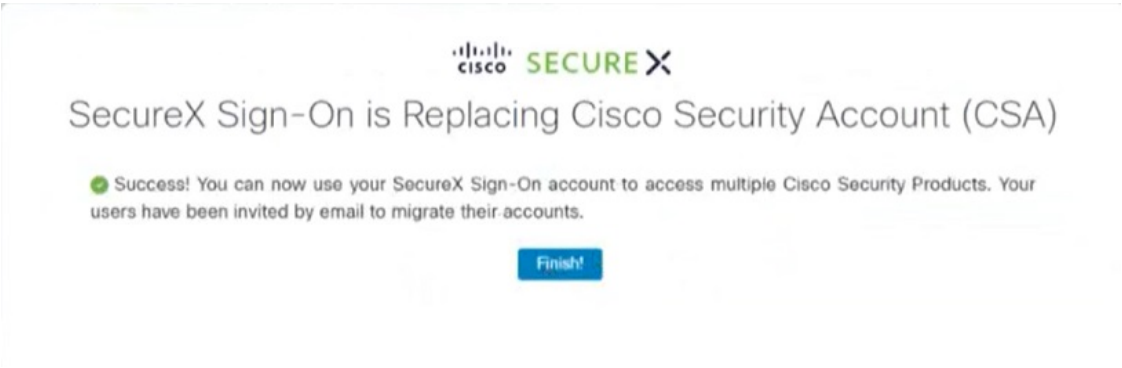
Note If you do not see the expected page, open a new browser session and restart the update process.

Figure 5:

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:



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

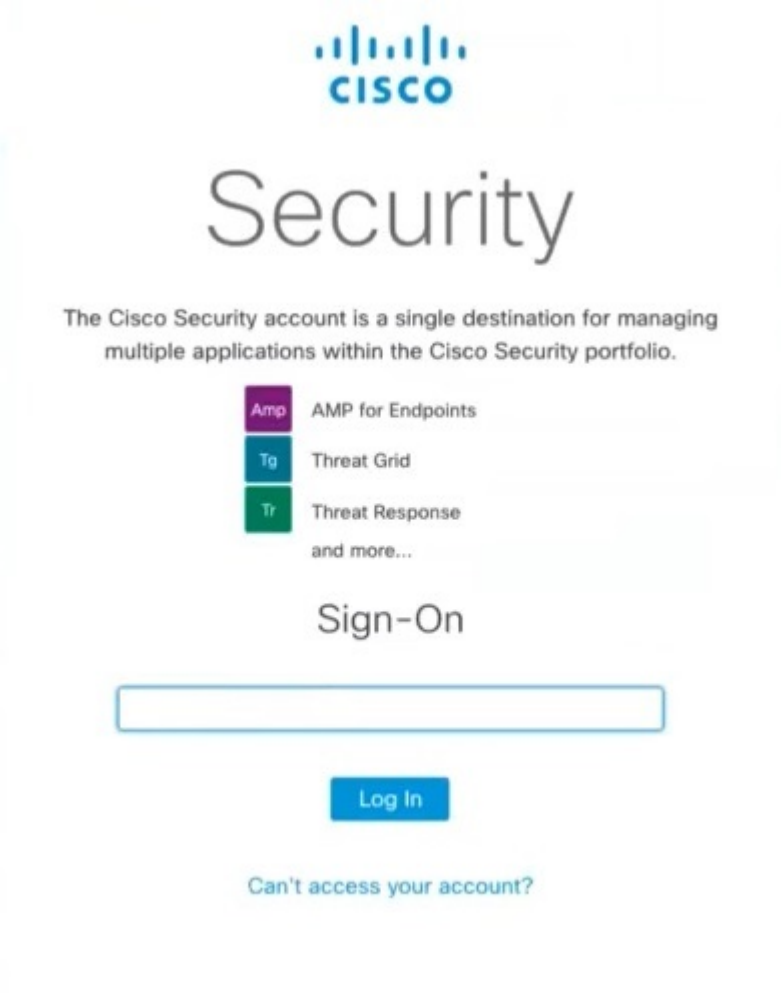
Before you begin

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:



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.

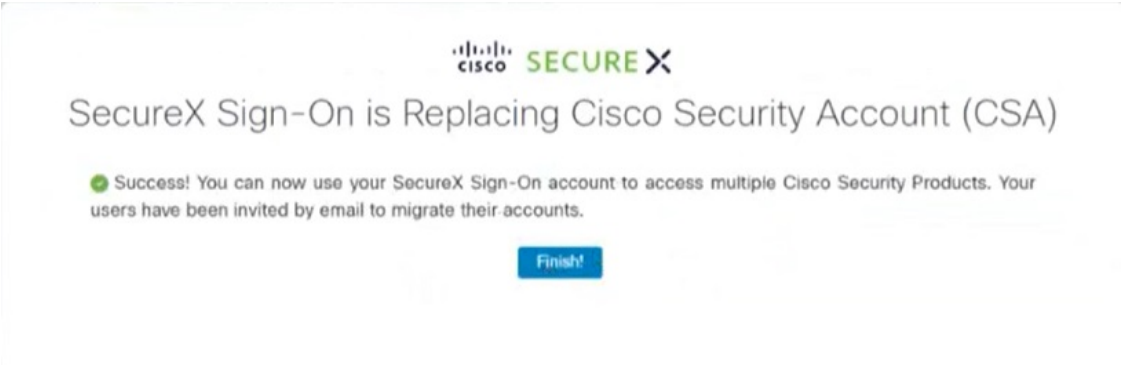
Note If you do not see the expected page, open a new browser session and restart the update process.

Figure 8:

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:



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.