

Cisco Secure Endpoint (formerly AMP for Endpoints) Entitlement Guide

Table of Contents

Entitlement for your Product..... 2

Language Support 2

Cisco Security Account 2

SecureX Sign-On 2

New Secure Endpoint Organization 3

Existing Secure Endpoint Organization - POV conversion to Licensed/EA or License Renewal..... 5

Adding additional connectors to an existing Private Cloud Virtual Appliance 8

Troubleshooting 8

GLO Ticketing system..... 10

Entitlement for your Product

Secure Endpoint requires an entitlement license to be applied to have access to the dashboard. Although Secure Endpoint subscription has automatically renewed, you will still need to apply your license to your existing account. You can retrieve the entitlement license for your purchased product via links in either an eDelivery email or an entitlement email. If you do not have access to the eDelivery email, you may contact GLO (Page 11) to request an entitlement email for your order.

Language Support

We now support English, Japanese, Chinese and Korean on our Licensing portal when the Asia Pacific data center is selected. Users can select their preferred language from a drop-down menu (which is displayed in English by default). Buttons and important entries are then displayed in the selected language.

Only the APJC datacenter has the option to be presented in English, Japanese, Chinese or Korean. If you would like to move your organization to another datacenter (Americas, Europe, or Asia Pacific), contact your Cisco Sales representative.

Cisco Security Account

Existing Secure Endpoint customers are using a Cisco Security Account (CSA) credentials to logon and apply their license. In the future, you will be prompted to use SecureX Sign-On.

SecureX Sign-On

Cisco Security products are migrating to use SecureX sign-on. New Secure Endpoint (formerly AMP for Endpoints) trial and customers will be prompted to use this new authentication system.

Cisco SecureX sign-on Quick Start Guide <https://www.cisco.com/c/en/us/td/docs/security/secure-sign-on/sso-quick-start-guide/sso-qsg-procedure.html>

New Secure Endpoint Organization

Scenario: If the entitlement email has gone to the reseller, they must pass it onto the end customer to activate. The end customer does not have an existing Secure Endpoint Organization.

New POV trial or customers who have purchased without an evaluation account.

NOTE: THE 3 DATACENTERS ARE SEPARATE FROM EACH OTHER. IF YOU CHOOSE TO SPLIT UP YOUR LICENSES BETWEEN AMERICA, EUROPE, AND ASIA PACIFIC DATACENTERS, YOU WILL NOT BE ABLE TO MANAGE THEM AS ONE.

1. The end customer that will be administrating the Secure Endpoint organization, should click on the activation URL provided in the eDelivery email or Entitlement activation email.
2. Please follow the steps in order from 1 to 9. Only the End customer should apply the license and set up their credentials:
 1. Click on the license activation link
 2. Select datacenter
 3. Enter your email
 4. You will be directed to SecureX sign-on site. If you do not have a SecureX Sign-On account, follow these directions for your options. Proceed through the steps they lead you through [here](#)
 5. Once these steps are completed for signing up for a SecureX sign-on account, it will continue for you to claim your order and stand up a new Secure Endpoint Organization.
 6. You will be prompted to sign on with your credentials.
 7. A universal agreement window will pop up. Check the agree checkbox and select continue.
 8. You will be directed to your Secure Endpoint Dashboard. Bookmark this page to sign on directly to this dashboard for future use.
 9. You can check your licensing by selecting the drop down of Accounts – License Information.

If you did not bookmark the Secure Endpoint Dashboard, you can go to SecureX sign-on and select Secure Endpoint tile (picture below) for your regional datacenter. SecureX sign-on logon page is found here. <https://sign-on.security.cisco.com>

Existing Secure Endpoint Organization - POV conversion to Licensed/EA or License Renewal

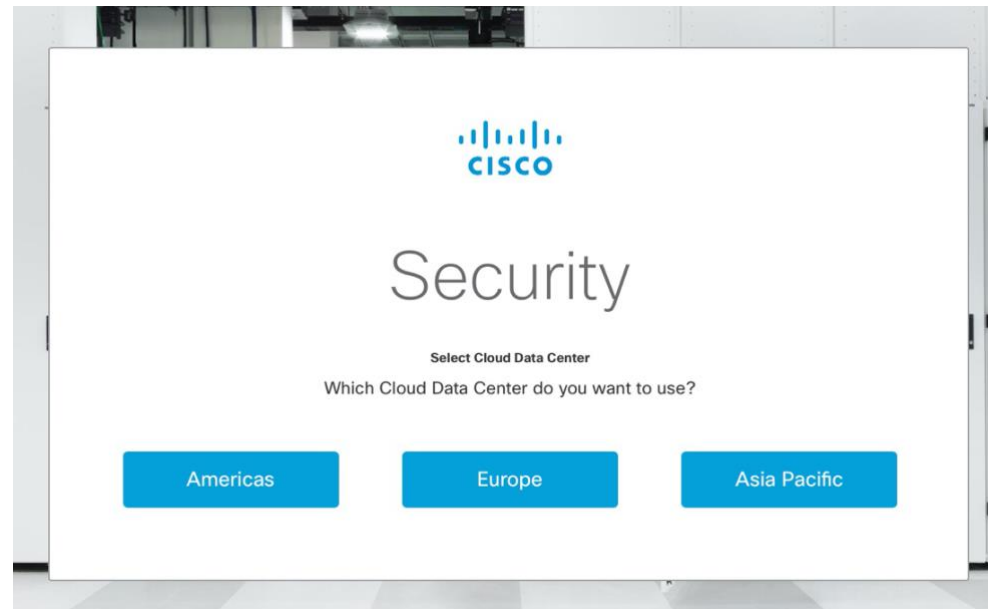
Scenario: If the entitlement email has gone to the reseller or to a user that does not have an existing Secure Endpoint Admin account for their organization, the email should be passed onto the admin. The admin is to use their CSA credentials to apply the license. The steps below are for POV conversions, license renewals or applying EA licenses to existing organizations.

NOTE: THE 3 DATACENTERS ARE SEPARATE FROM EACH OTHER. IF YOU CHOOSE TO SPLIT UP YOUR LICENSES BETWEEN AMERICA, EUROPE, AND ASIA PACIFIC DATACENTERS, YOU WILL NOT BE ABLE TO MANAGE THEM AS ONE.

1. The end customer with existing Secure Endpoint credentials must click the URL provided in the eDelivery email or Entitlement email.
2. Determine if the existing account is located in America, Europe, or Asia Pacific datacenter and click the corresponding button.

NOTE: To verify which datacenter the organization is located, look at the URL that shows in your dashboard.

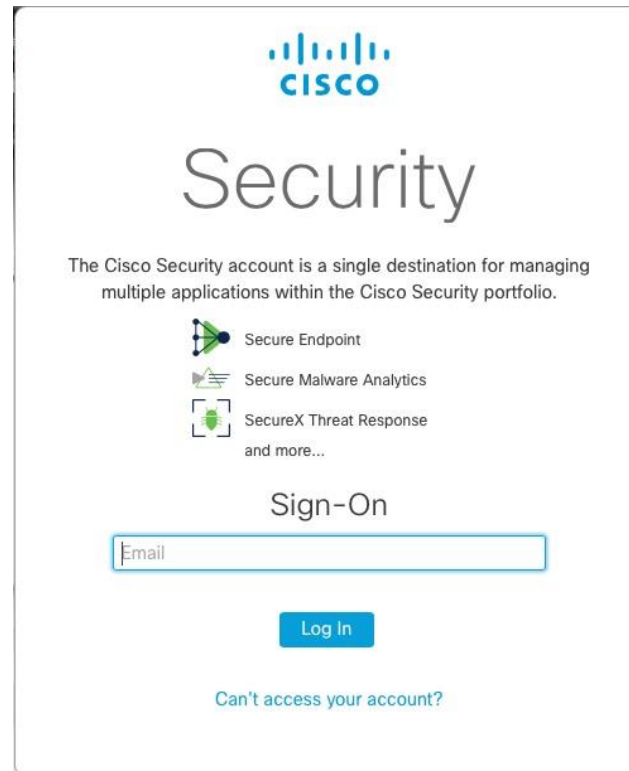
- a. Americas -
<https://console.amp.cisco.com/>
 - b. Europe-
<https://console.eu.amp.cisco.com/>
 - c. Asia Pacific-
<https://console.apjc.amp.cisco.com/>
- **Americas** - This datacenter can be used for all countries. There are no distance-related



issues with latency for countries that are far away.

- **Europe** - This datacenter complies with EU Privacy Laws.
- **Asia Pacific** - This datacenter has the capability to select English, Japanese, Chinese or Korean languages.

3. Enter your login email/login ID for your Secure Endpoint Org. Then you will be prompted for your password.




The image shows the Cisco Security Sign-On page. At the top is the Cisco logo. Below it is the word "Security" in a large, grey font. A paragraph states: "The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio." Below this are three icons with labels: "Secure Endpoint" (a green and blue icon), "Secure Malware Analytics" (a green and blue icon), and "SecureX Threat Response and more..." (a green and blue icon). Below these is a "Sign-On" section with a text input field labeled "Email" and a blue "Log In" button. At the bottom is a link that says "Can't access your account?"

4. Claim your order to apply your license to your existing Organization. SKUs and Sales order number will be unique to your business. For license renewals, you will want to apply it to your Existing account, a drop down is available if you have multiple Org using your same login email. If you select to apply it to a new organization, your license will not apply to your existing Organization and will stand up a separate instance.
5. A message will show on top that your order has been claimed and provisioning is currently in progress.
Note: Refresh your browser to see the Secure Endpoint Launch button.


Order: af55570ff2d840c6aeb8f7f30fd8582e
Datacenter: Americas


☐ Apply to a new organization

☒ Apply to an existing organization: Bobs Shake Business 

[AMP4E-ADV-CL-LIC] Claim 3434567 for Secure Endpoint.

[Claim Order](#)


✔ Your order has been claimed and provisioning is currently in progress. 



SecureX

Simplify your security with the broadest, most integrated platform

Connect Cisco's integrated security portfolio to your existing infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoints, cloud, and applications.

[Launch](#) [Learn More](#)






SecureX Threat Response

Advanced threat intelligence at your fingertips

Cisco SecureX Threat Response centralizes security events and alerts, and enriches them using data from other security services. It provides incident responders and SOC analysts with the data needed to detect, correlate, and prioritize security events.

[Launch](#) [Learn More](#)





Secure Endpoint

Visibility and control to defeat advanced attacks

Get global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches with Cisco Secure Endpoint. But because you can't rely on prevention alone, Secure Endpoint also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

[Launch](#) [Learn More](#)



Adding additional connectors to an existing Private Cloud Virtual Appliance

If you have purchased a virtual Private Cloud (vPC) or a HW Private cloud appliance and want to add additional connector licenses to your existing private cloud, follow directions in this help document [Private Cloud entitlement help doc.](#)

If you have any questions regarding provisioning your private cloud license, please open a GLO ticket (page 11).

Troubleshooting

My company renewed their license, but I don't see it listed under Licensing Information on my dashboard.

Secure Endpoint requires an entitlement license to be applied to have access to the dashboard. Although Secure Endpoint subscription has automatically renewed, you will still need to apply your license to your existing account. You can retrieve the entitlement license for your purchased product via links in either an eDelivery email or an entitlement email.

If you do not have access to the eDelivery email, you may contact GLO (Page 11) to request an entitlement email for your order.

When signing up for a SecureX sign-on account, I enter in my email in the default prompt, and received an error

You have not created a SecureX sign-on account yet. At the bottom of the page, you can select "Create a SecureX Sign-on" button. Or have the option to select on the right side [Cisco.com](#) or Microsoft to authenticate. Remember which authentication method you chose for future logins.

When signing up for a SecureX log in account. I can't remember if I chose to Create a SecureX Sign-On account or select Cisco.com, or Microsoft. When I enter in my email address to sign in, I get the error Unable to Sign in. Please verify you created your account.

If you select [Cisco.com](#) or Microsoft to authenticate then sign on that way. If you created a SecureX sign-on Login account manually, then authenticate by the prompt to sign in.

A new account was created for me or I'm expecting an email for SecureX Sign-On but it never came to my inbox

*If you are a O365 user, the **no-reply** email may have landed in your Other folder, under the Focused/Other Tab. For more information on how to change these to go to your Focused Tab, you can reference this Microsoft article [Focused Inbox for Outlook](#)*

I created a new SecureX sign-on account, but when I launch Secure Endpoint and enter my email, I receive "Invalid Account"

If you are an existing customer that uses the Cisco Security Account (CSA) continue to do so to login to Secure Endpoint Organization. Until you are prompted to change the authentication system, continue to use your CSA credentials.

I added users in the Secure Endpoint Dashboard, but they have not received their credentials email

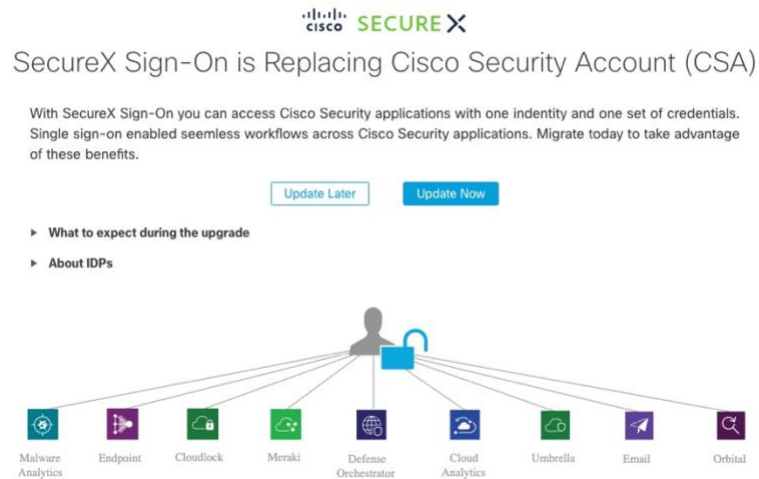
After you create user account, let the other person know and have them check their email. If they do not find the email, please have them check their spam folder, or for O365 users, your Focused/Other tab. If you do not find the email, please create a ticket with TAC.

I created a SecureX sign-on account, but didn't activate it within 7 days

If you didn't activate your account, it will be in provisioned state, but not active. Create a TAC ticket for support to resend with a new activation link or get the record removed.

How will I know when I'll be prompted to change to SecureX Sign-On?

Upon logging into Secure Endpoint you will come to this screen like this first.



GLO Ticketing system

In case you get an error message or if you haven't received confirmation within 48 hours of applying your license, contact GLO through their ticketing system.

Please open your case online using Support Case Manager (SCM) at: <https://mycase.cloudapps.cisco.com/case>

After selecting the Software Licensing – Security Related Licensing and sub-technology, select FireAMP/ThreatGrid. This is the preferred method and the most efficient method for customers to open severity 3 service requests. Please note, the selection maybe updated to refer to Secure Endpoint in the future.

We ask for the information to include the following:

Cisco.com ID:

Product Name:

Issue/Request Details:

Cisco Web Order ID #:

End Customer Business Name:

Customer Full Name:

Customer email address:

Please include as much information as possible. If you did not receive the entitlement email, the reason might be that the email address was not entered into the order, when the order was placed.