

Cisco Secure Endpoint Entitlement Guide

Table of Contents

Entitlement for your Product..... 2

Cisco Security Cloud Sign On (Formerly SecureX Sign-On)..... 2

New Secure Endpoint Organization 3

Existing Secure Endpoint Organization – Trial conversion to Licensed/EA or License Renewal..... 4

Adding additional connectors to an existing Private Cloud Virtual Appliance 6

Troubleshooting 6

GLO Ticketing system..... 7

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 request to resend your activation link for your license through contacting Global Licensing (GLO) (Page 11)

Cisco Security Cloud Sign On (Formerly SecureX Sign-On)

Cisco Security products are using Security Cloud Sign On to authenticate to their security products. This was formally called SecureX Sign-On and has been rebranded, no action is required by existing users, they will continue to sign on as they did before. New Secure Endpoint trial and customers will be prompted to sign up with this new authentication system.

Security Cloud 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 license 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 trials 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 license 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 Security Cloud Sign On site. If you do not have a Security Cloud 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 Security Cloud 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 Security Cloud Sign On and select Secure Endpoint tile for your regional datacenter. Security Cloud Sign On logon page is found here. <https://sign-on.security.cisco.com>

Existing Secure Endpoint Organization – Trial conversion to Licensed/EA or License Renewal

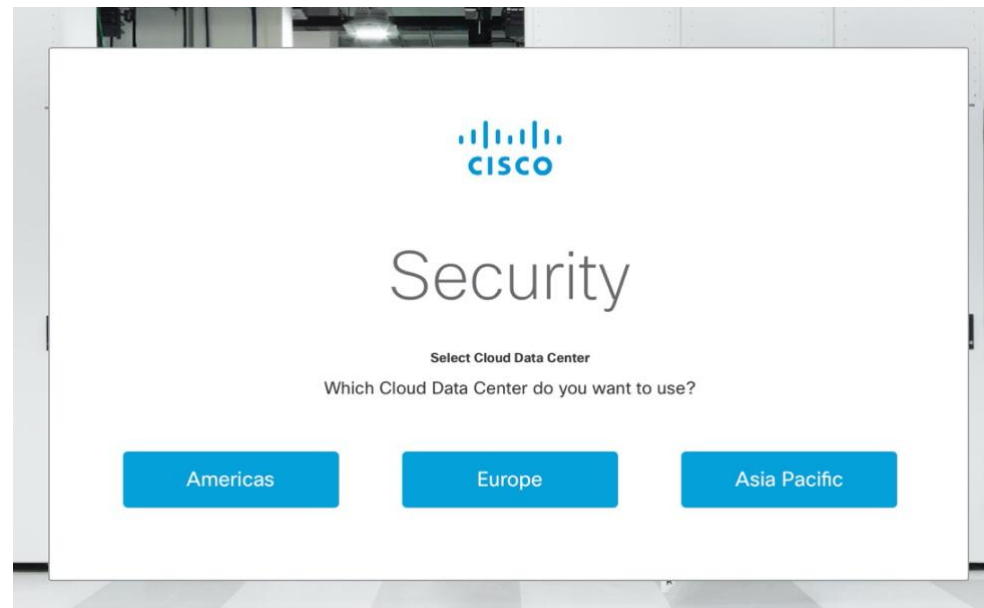
Scenario: If the entitlement email has gone to the reseller or to a user that does not have an existing Secure Endpoint Admin account for their organization, the email should be passed onto the admin. The admin is to use their credentials to apply the license. The steps below are for POV conversions,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

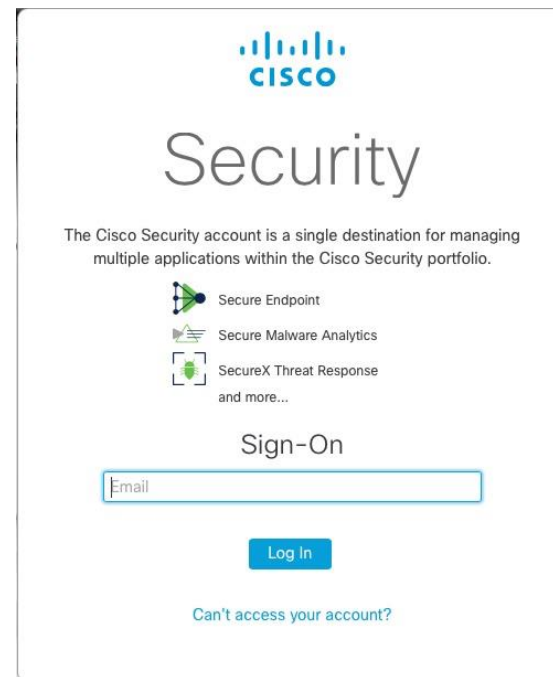
- a. Americas -
<https://console.amp.cisco.com/>
 - b. Europe-
<https://console.eu.amp.cisco.com/>
 - c. Asia Pacific-
<https://console.apjc.amp.cisco.com/>
- **Americas** - This datacenter can be used for all countries. There are no distance-related



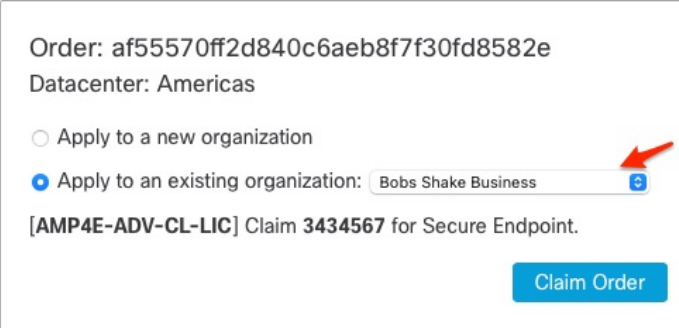
issues with latency for countries that are far away.

- **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 Organization. Then you will be prompted for your password.



4. Claim your order to apply your license to your existing Organization.
 - a. For license renewals, apply it to your existing organization, a drop down is available if you have multiple Organizations using your same login email. If your organization's license had expired after the grace period given, it will have a prefix of *Expired_* appended at the beginning of the Organization name. Once you apply the license, the organization will be renamed back, and you will gain access again.
 - b. 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.



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

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 Security Cloud Sign On account, I enter in my email in the default prompt, and received an error Unable to sign in. Please verify that you have created your account and try resetting your password. Too many failed password attempts will lock your account. Select Don't have an account? *Sign up now* to create an account.

A new account was created for me or I'm expecting an email for Security Cloud 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](#)*

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