Security Cloud Control Getting Started Guide

Cisco Security Cloud Control
Updated NaN,

1 SCC getting started

Topics:

- Security Cloud Control
- Getting started workflow
- Integrate existing products in Security Cloud Control

This section makes you to understand the new and existing deployment of security product's getting started workflow.

Security Cloud Control

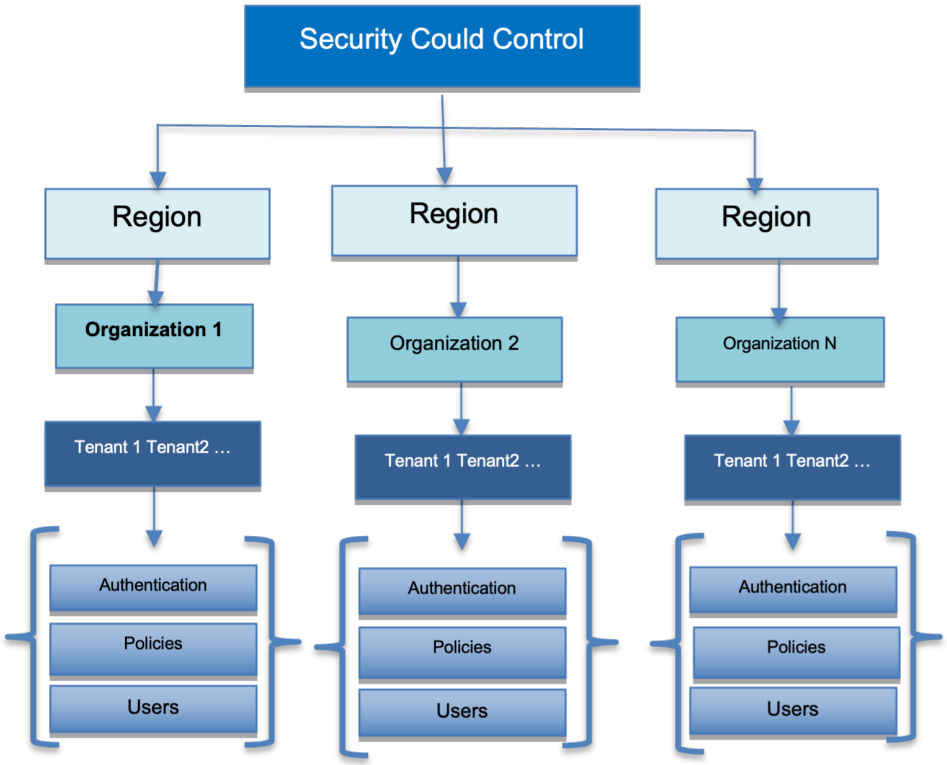
You can use a unified interface to manage security products and achieve consistent outcomes efficiently. It simplifies platform integration through a single claim code while providing centralized user and role management.

Security Cloud Control is a security platform that allows you to manage your security products and achieve security outcomes from a single integrated interface.

Integrating security products in the platform is a streamlined experience. After purchasing your subscriptions to Cisco security products, you receive a single email, with a single claim code for all the subscriptions you purchased. Entering the claim code in your new Security Cloud Control organization provisions all your products to Security Cloud Control simultaneously.

Within Security Cloud Control, user and group management occurs at the platform level. Roles are assigned to these users and groups to define their privileges for administering Security Cloud Control and the integrated products.

Figure 1: Security Cloud Control Hierarchical Flow

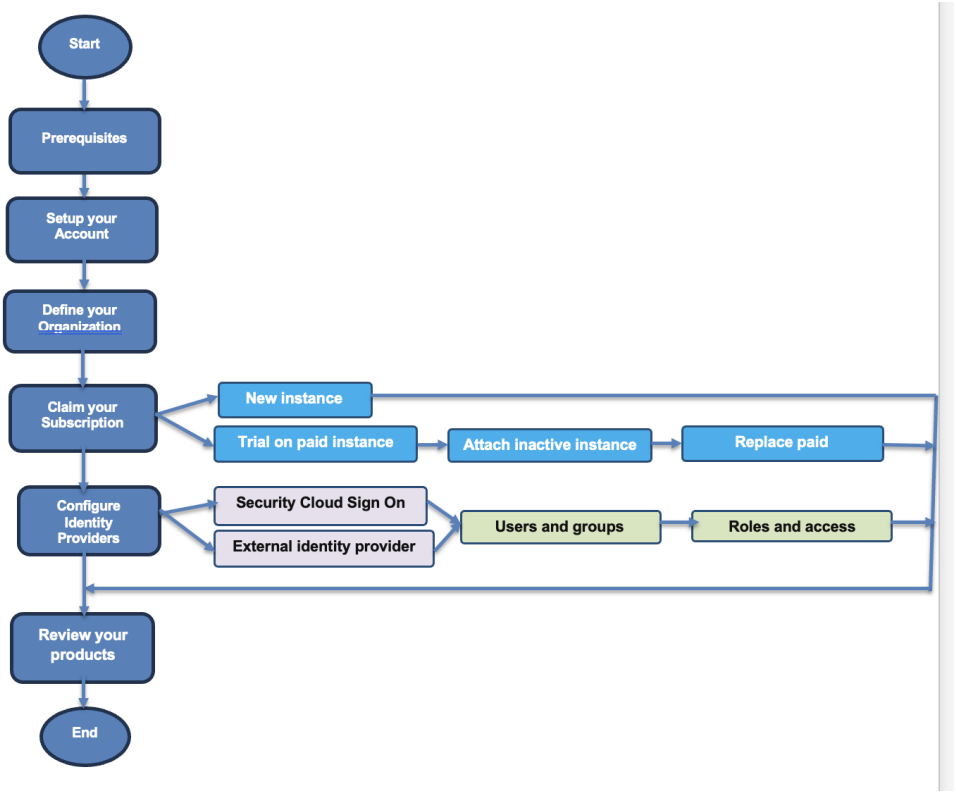


Level	Description
Region	The preferred geographic setting used to align deployment regions for products and their services.
Organization	The trust boundary for Cisco products, users, registered domains, identity providers, and organizatio
Tenant	The product-specific service environment or instance associated with the organization, including its configuration.
Authentication	The sign-in and identity-provider path used to verify users and provide access to the organization.
Policies	The product and security rules used to control how the associated services operate.
Users	The people associated with the organization who receive roles for administering SCC and integrated

Getting started workflow

Use this workflow to get started with Security Cloud Control.

Figure 2: Security Cloud Control flow chart



Onboarding Phase	New deployments	Migrated deployments
Prerequisited	1. Locate your welcome email: Retrieve the *Claim Your Cisco Security Cloud Subscription* email sent to the designated provisioning contact. It contains your unique subscription claim code and access link. **Note** Enterprise Agreement users must first explicitly request the email via the EA Workspace. 2. Verify your organization: Check with your team to see if an SCC organization already exists. Join as an administrator if it does to keep management centralized and avoid creating duplicates. 3. Attach before you claim Integrate existing products in Security Cloud Control. If you are changing order types or migrating (Example: Umbrella to Secure Access), you must attach your existing product instances during the claim process to apply the new license and prevent service gaps.	

Account Setup	Setup your Security Cloud Sign on account or sign in to Security Cloud Control. For more details refer to the Create your Security Cloud Sign On Account	Watch for a migration notification from Cisco once your product is migrated to Security Cloud Control. For more details, refer to the Security Cloud Sign On account and with organizations
Define your Organization	Create your organization and select your preferred region before you claim products. For more details, refer to the Organizations and Regions Video: Create an organization	Review the organization's region, which uses the existing product's region, and create another organization if necessary. For more details, refer to the Organizations and Regions Video: Create an organization
Claim your Subscription	Obtain your claim code, then choose a new, trial, inactive-instance, or paid-replacement path. Review the subscription details before you claim. For more details, refer to the claim Code Email for Subscription Video: Claim a Subscription	Migrated product is already active. You can deactivate an existing product subscription and replace with a new claim code. For more details, refer to the Deactivate a product instance Video: Claim a Subscription
Review	Review and manage your subscriptions. For more details refer to the Manage subscription and Services	Review and manage your subscriptions. For more details refer to the Manage subscription and Services
Users,Groups and Roles	Create new users, establish groups, and assign administrative roles. For more details refer to the Administrator access	Create new users, establish groups, and assign administrative roles. For more details refer to the Administrator access
Configure Identity providers	Choose Security Cloud Sign On or an external identity provider. Map groups only when you need federated role management. For more details refer to the Integrate Identity Providers You can also refer to the Invite Users, Import a User, Create Local Groups, or use Federated Groups. Video: Invite a User | Import Multiple Users You can assign product roles directly to users or through groups. **Video:** Add Users to Groups and Assign Group Roles For more details on Users, Identity settings, and activity log refer to https://securitydocs.cisco.com/docs/scc/admin/95952.dita	Add and verify enterprise domain and integrate IdentityProvider (IdP) if needed. Formore details, refer to the Organizations and Regions You can also refer to the Invite Users, Import a User, Create Local Groups, or use Federated Groups. **Video:** Invite a User | Import Multiple Users You can assign product roles directly to users or through groups. **Video:** Add Users to Groups and Assign Group Roles

Completion	View your product subscription details. For more details refer to the Product Configuration	View your product subscription details. For more details refer to the Product Configuration
Product Configuration	View your product configuration details. For details on product-specific configuration, refer to the AdditionalDocumentation and Support	View your product configuration details. For details on product-specific configuration, refer to the AdditionalDocumentation and Support
Support Information	CiscoCustomer Support	Cisco Customer Support
Reference	Additional reference: • Activity log • SCC API keys • FAQ	Additional reference: • Activity log • SCC API keys FAQ

Integrate existing products in Security Cloud Control

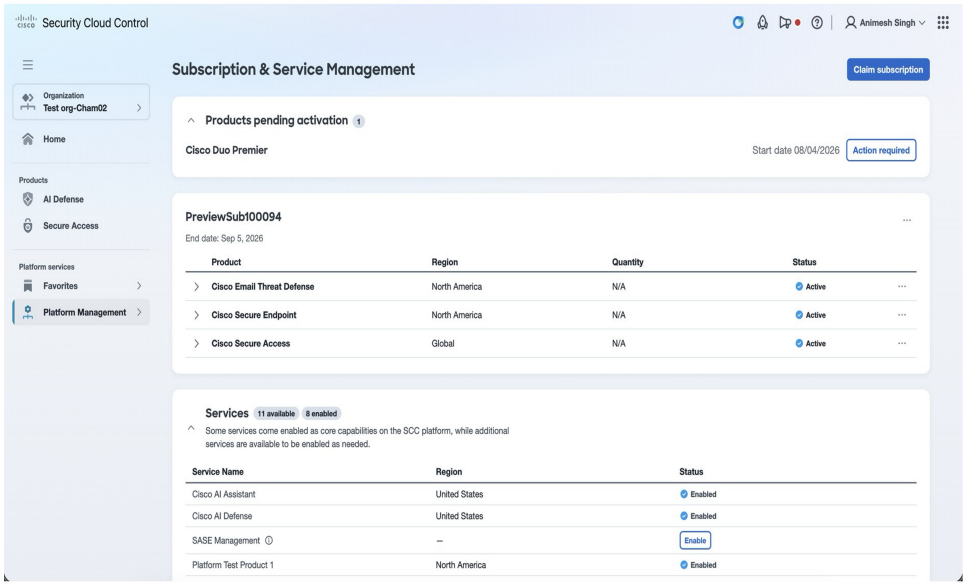
You can connect existing security deployments to the platform through guided activation workflows that simplify configuration. This process centralizes control, allowing you to manage licenses and service settings from a single unified dashboard.

Activate Cisco Duo Premier

Use these steps when **Cisco Duo Premier** appears under **Products pending activation** with an **Action required** status.

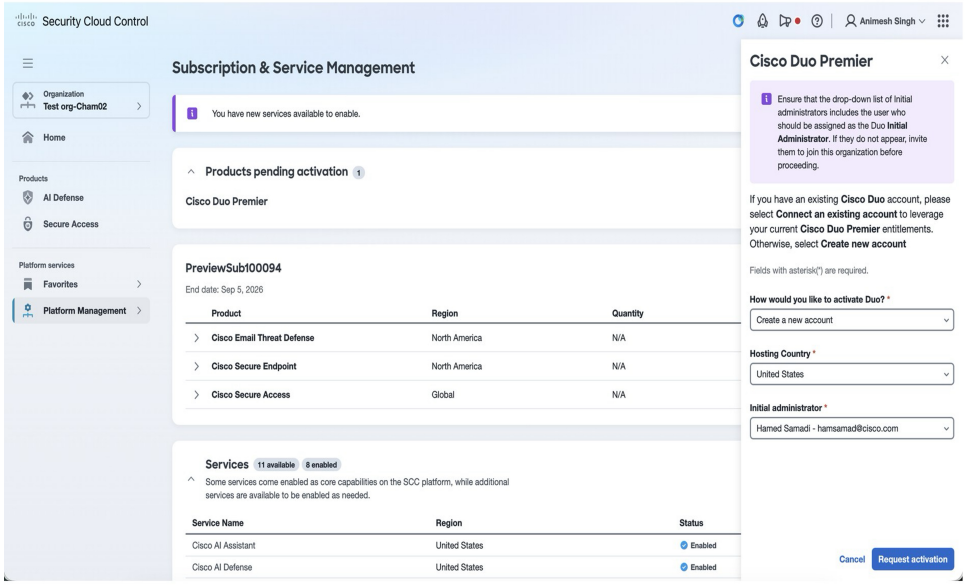
Open the Duo subscription

- Log in to Security Cloud Control.
- Select **Subscription & Service Management**.
- Find **Cisco Duo Premier** under **Products pending activation**.
- Select **Action required**.



Create a new Duo account

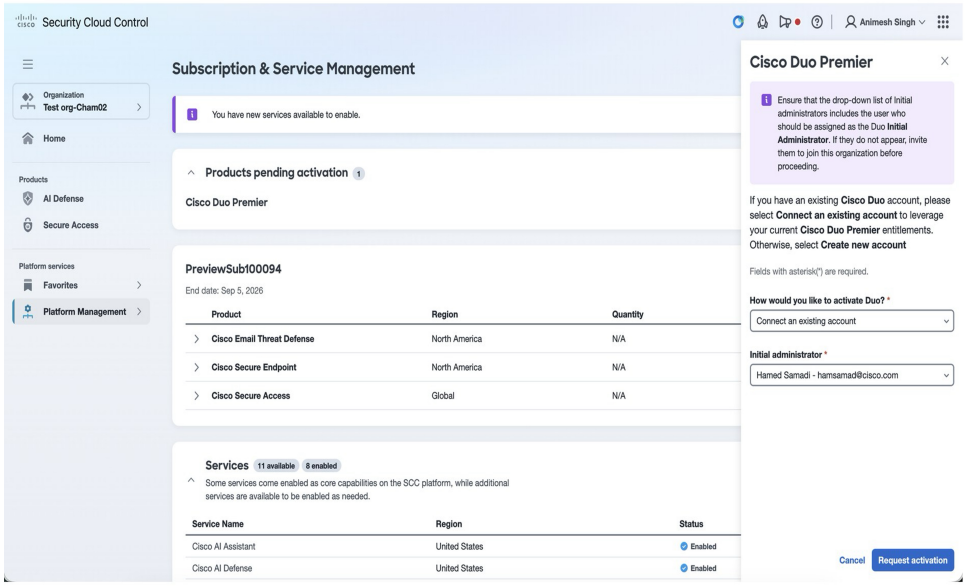
- Select **Create a new account**.
- Select a value for **Hosting Country**.
- Select the person from the **Initial administrator** list.
- Select **Request activation**.



Start the existing Duo account connection

- Select **Connect an existing account**.
- Select the person from the **Initial administrator** list.
- Invite the person to the Security Cloud Control organization if the name does not appear in the list and return to this step.

- Select **Request activation**.



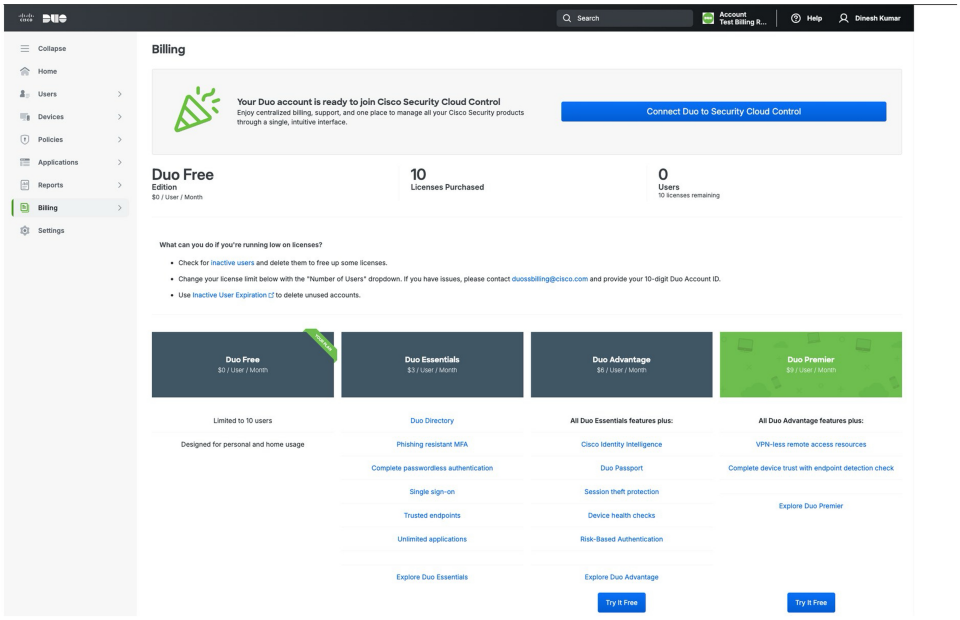
Connect the existing Duo account

- Open the connection invitation email for the initial administrator.
- Select **Connect accounts**.
- Sign in to the Duo account that you want to connect.
- Sign in as a Duo Owner. Ask a Duo Owner to complete the connection if you do not have that role.



Connect and authorize the existing account

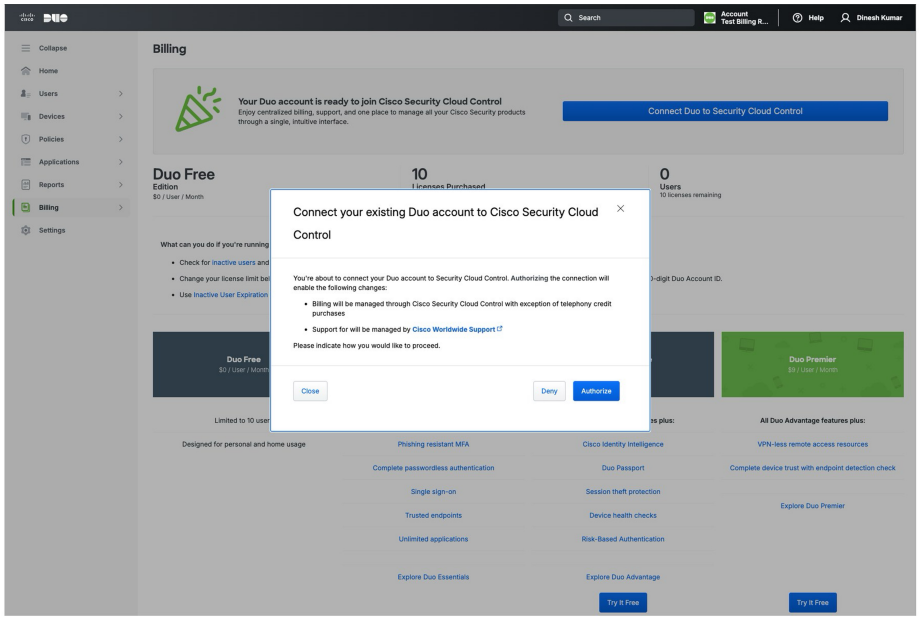
- Open Duo portal.
- Select **Billing** and select **Connect Duo to Security Cloud Control**.



Review the authorization before approving

Read the authorization details. The connection moves Duo Billing to Security Cloud Control, except for telephony credit purchases. Cisco worldwide Support handles billing support.

Select **Authorize** only after you review and accept these changes.



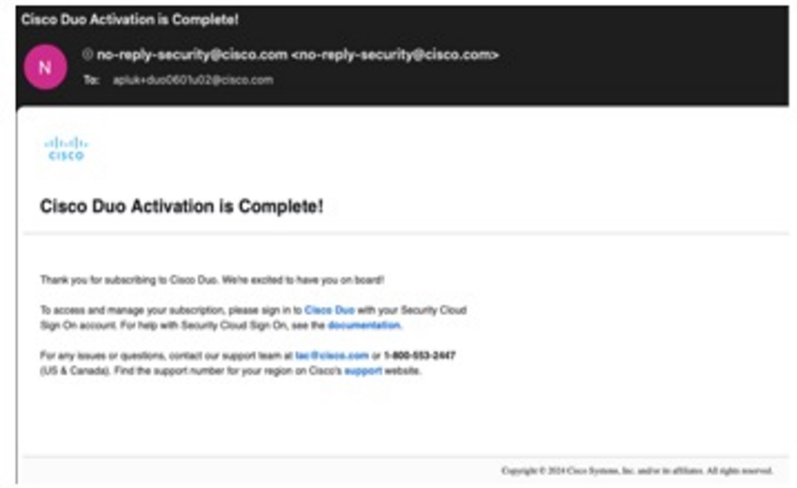
Confirm activation

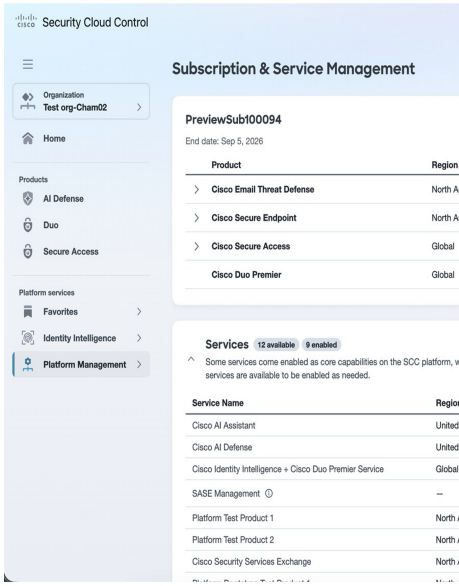
- Check email for the **Cisco Duo Activation is Complete** message.

  Sign in to Duo with your Security Cloud Sign On account.

  Return to **Subscription & Service Management**.

  Confirm **Cisco Duo Premier** shows **Active** and Duo appears in the product list.



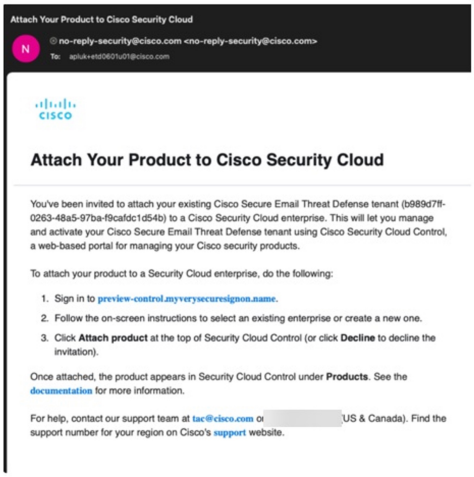


Activate Cisco Secure Email Threat Defense

Use this workflow to attach a Cisco Secure Email Threat Defense subscription to Security Cloud Control and activate a new or existing instance.

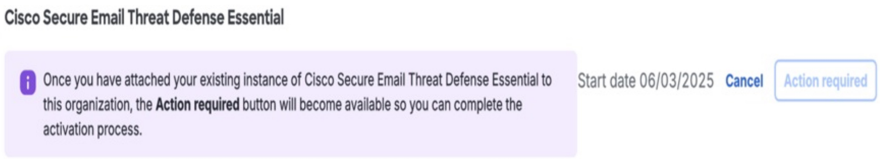
Accept the invitation and attach the product

- Open the **Attach Your Product to Cisco Security Cloud** invitation email.
- Select the sign-in link in the email and sign in to Security Cloud Control.
- Choose an existing enterprise or create a new enterprise.
- Select **Attach product** at the top of Security Cloud Control. The product then appears under **Products**.



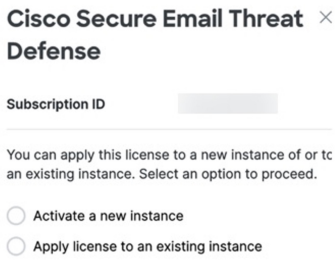
Start activation in Security Cloud Control

- Return to Security Cloud Control after the product is attached.
- Find Cisco Secure Email Threat Defense Essential. Select Action required to start activation.



Choose an instance

- Review the subscription ID in the **Cisco Secure Email Threat Defense** panel.
- Select **Activate a new instance** if you need a new instance. Follow the on-screen steps to complete setup.
- Select **Apply license to an existing instance** if you already have an instance. Continue to Step 4.



Apply the license to an existing instance

- Select the **Cisco Secure Email Threat Defense** instance that you want to use.

- Select **Apply license**



Confirm activation

- Check email for the **Cisco Secure Email Threat Defense** Activation is Complete message.
- Sign in to **Cisco Secure Email Threat Defense** with your **Security Cloud Sign On** account.



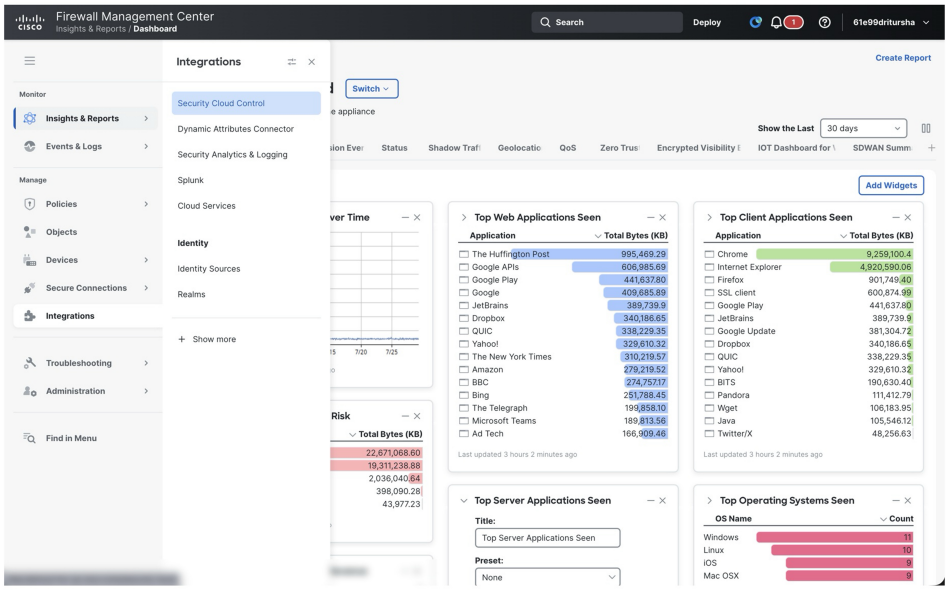
Connect Firewall Management Center

Use this workflow to register an existing Firewall Management Center (FMC) with Security Cloud Control, review its access, and save the integration settings. Optional sections cover cloud-delivered FMC and AIOps onboarding.

Open the Security Cloud Control integration in FMC

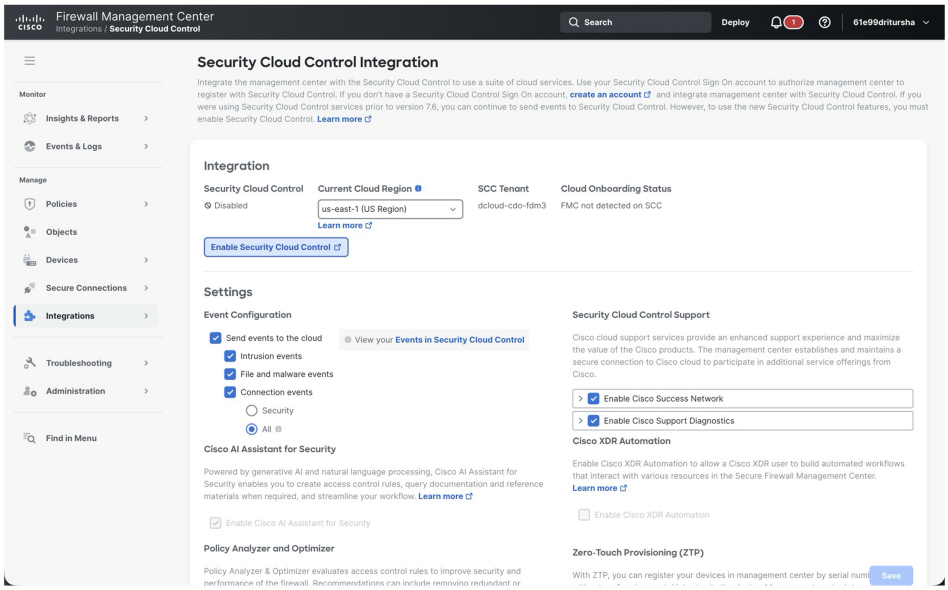
- Sign in to **Firewall Management Center**.

- Open **Integrations** and select **Security Cloud Control**.



Enable Security Cloud Control in FMC

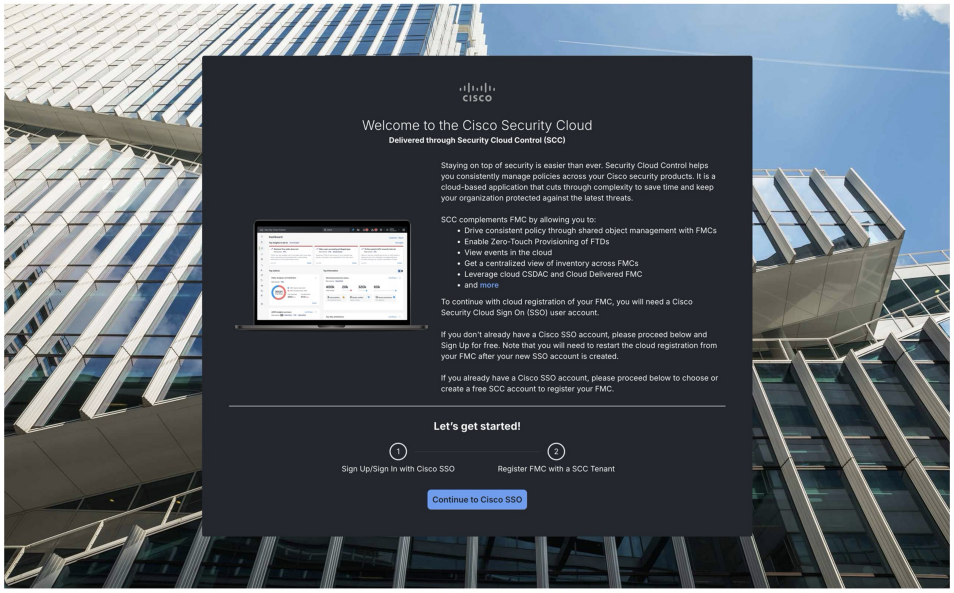
- Select the **Current Cloud Region** for your organization.
- Select **Enable Security Cloud Control**.
- Review the event settings. Choose the event types that you want **FMC** to send to the cloud, then select **Save** after registration.



Sign in with Cisco SSO

- On the welcome screen, select **Continue to Cisco SSO**.
- Sign in with your Cisco **Security Cloud Sign On** account. If you do not have an account, select Sign up now and create one.

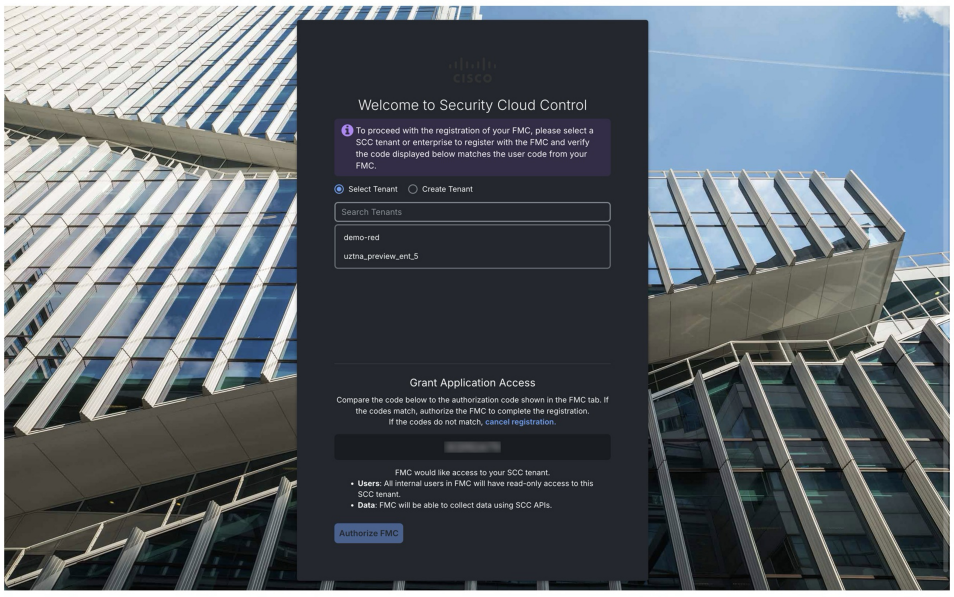
- Return to **FMC** and restart cloud registration after you create a new account.

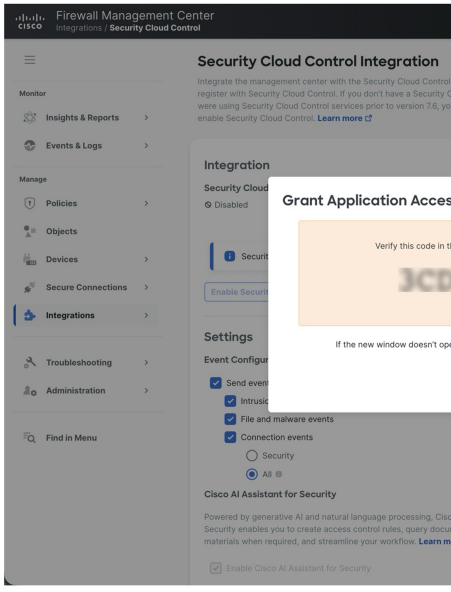




Select a tenant and verify the code

- In **Security Cloud Control**, select an existing tenant or select **Create Tenant**.
- If you select an existing tenant, choose the tenant that should connect to **FMC**.
- Compare the authorization code in **Security Cloud Control** with the user code in **FMC**. Continue only when the codes match.
- If a new window does not open, select **Click here** to continue.

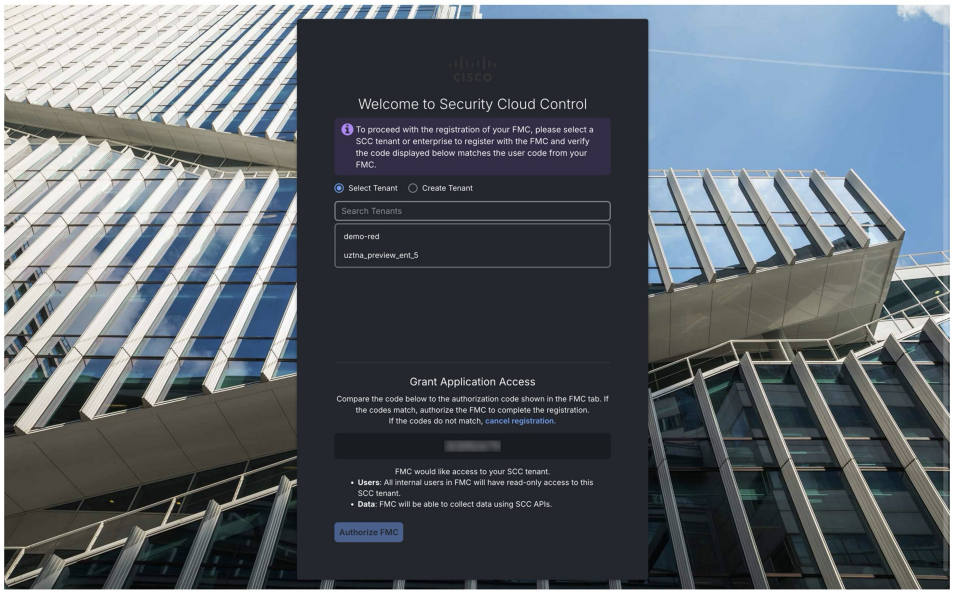




Review access and authorize FMC

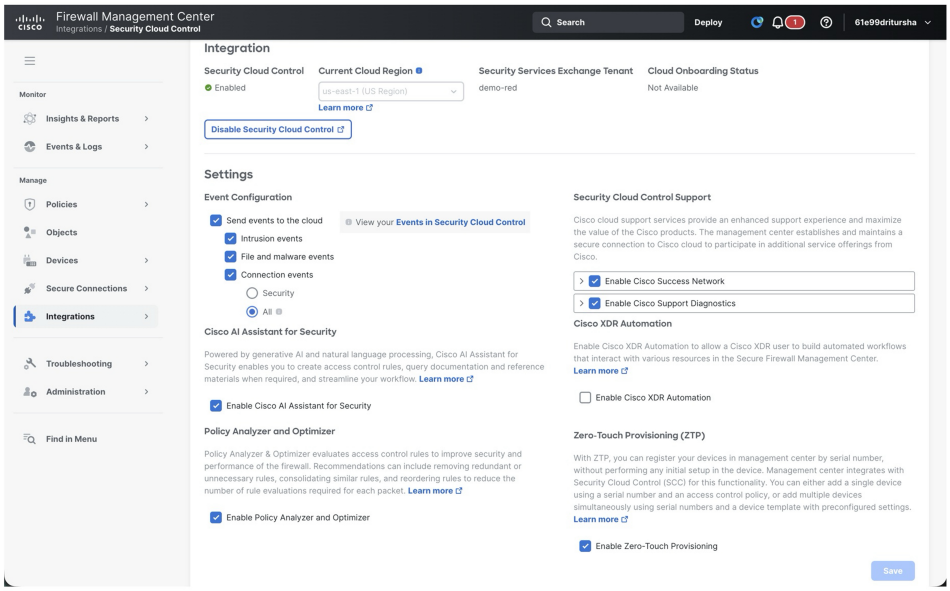
- Review the tenant name and the access details before you approve the connection.

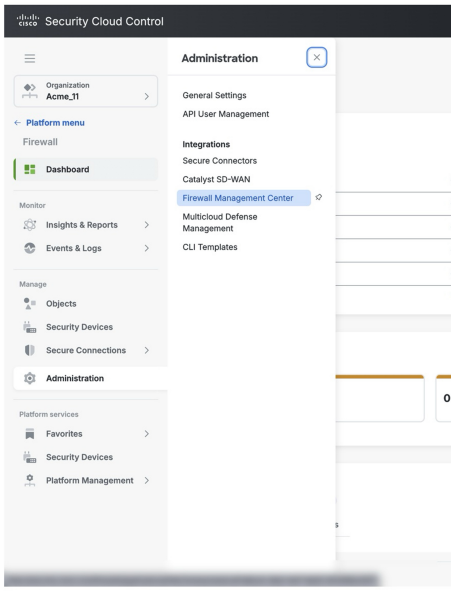
- Note that **FMC** can collect data from the tenant through **Security Cloud Control** APIs. Internal **FMC** users receive read-only access to the tenant.
- Select **Authorize FMC** to complete registration.



Confirm the FMC integration

- Return to the **Security Cloud Control Integration** page in **FMC** and confirm that the status shows Enabled.
- Review the event settings and select **Save**.
- In **Security Cloud Control**, open the Platform menu, then choose Administration, **Integrations**, and **Firewall Management Center** to view the **FMC** integration.

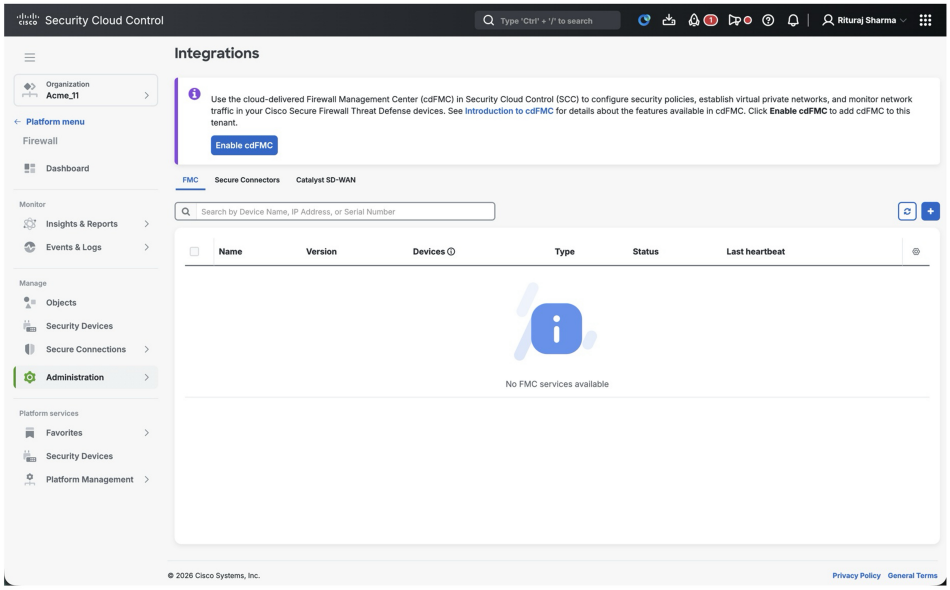


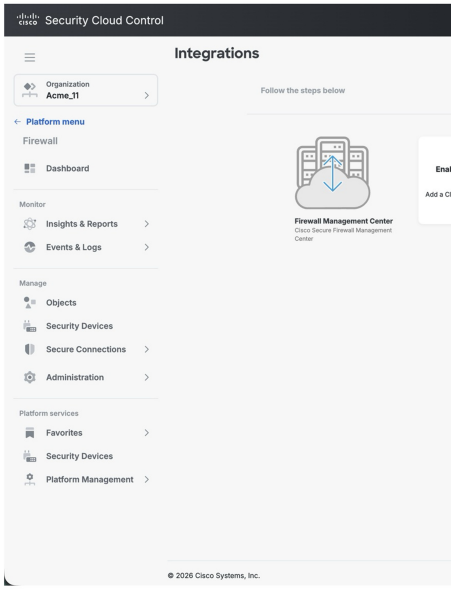


Optional: Set up cloud-delivered FMC

- In **Security Cloud Control**, open **Integrations** and select the **FMC** tab.

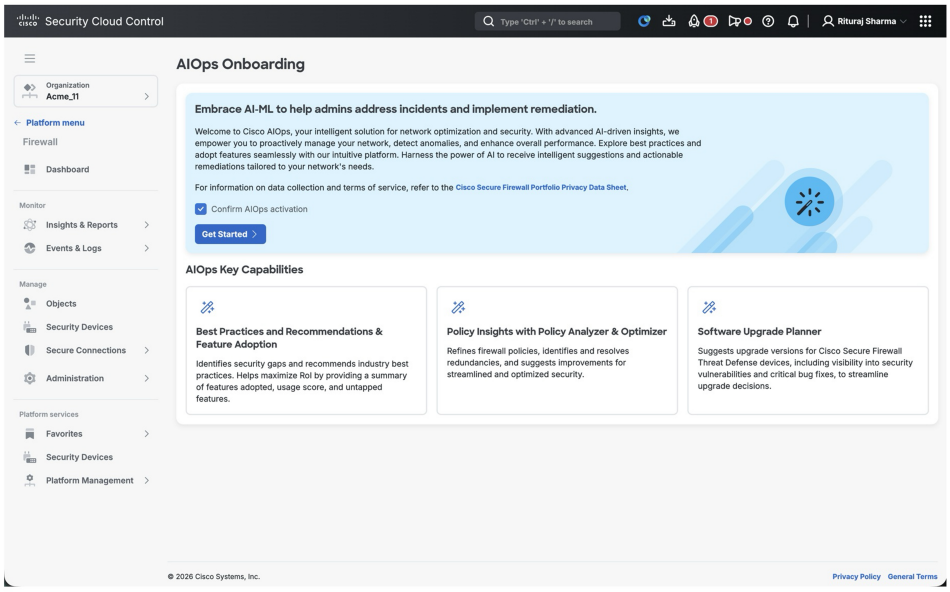
- To add cloud-delivered **FMC** to the tenant, select **Enable cdFMC**.
- To add or discover an **FMC**, select **Add** and choose **Enable Cloud-Delivered FMC**, **Auto discover from Cisco Security Cloud**, or **Use Credentials** based on your setup.





Optional: Start AIOps onboarding

- Open **AIOps Onboarding**.
- Select **Confirm AIOps activation**.
- Select **Get Started**.

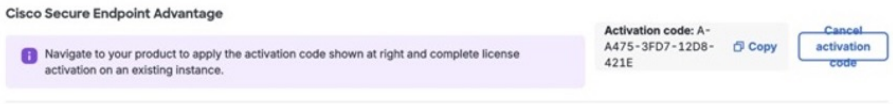


Activate Cisco Secure Endpoint

Use these steps to connect a Secure Endpoint instance to Security Cloud Control and confirm that Security Cloud Control manages its license. Use the activation code from your own account; the codes in the screenshots are examples.

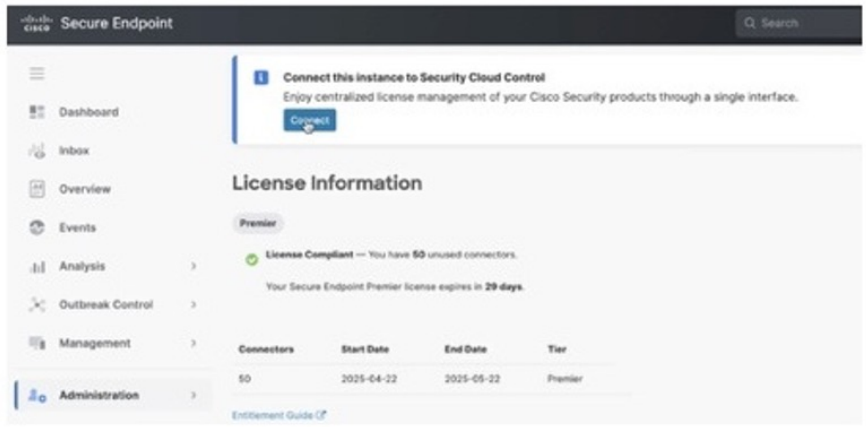
Copy the activation code

- Sign in to **Security Cloud Control**.
- Open the **Cisco Secure Endpoint Advantage** activation details and select **Copy** beside the activation code.



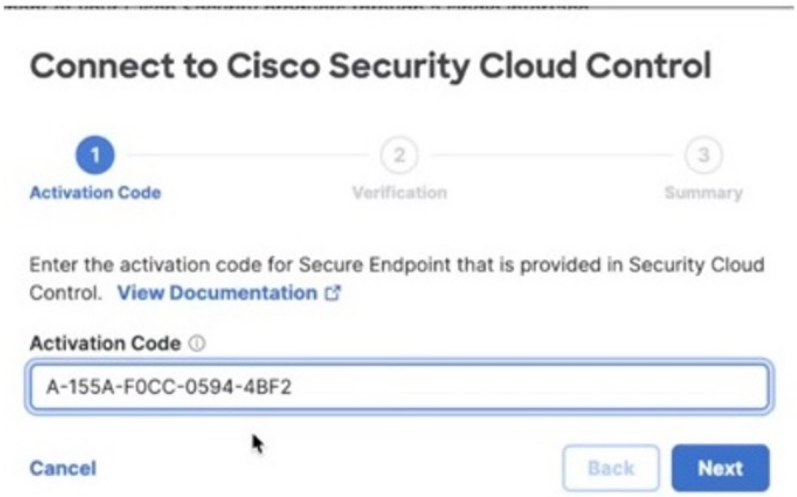
Open the connection setup in Secure Endpoint

- Sign in to Secure Endpoint.
- Open **Administration** and find **License Information**.
- Select **Connect** in the **Connect** this instance to **Security Cloud Control** message.



Enter the activation code

- In the **Connect to Cisco Security Cloud Control** wizard, enter the code that you copied from **Security Cloud Control** in **Activation Code**.
- Select **Next**.

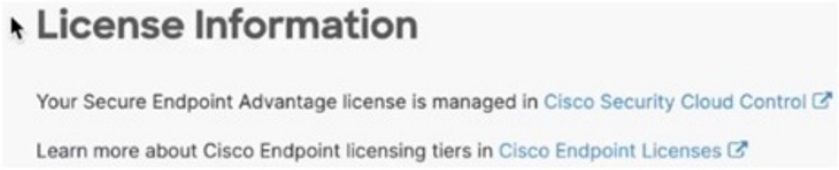


Verification and review the summary

Follow the on-screen steps for **Verification** and **Summary** to finish connecting the instance.

Confirm license management

- Return to **License Information**.
- Confirm that the page says **Security Cloud Control** manages your Secure Endpoint Advantage license.

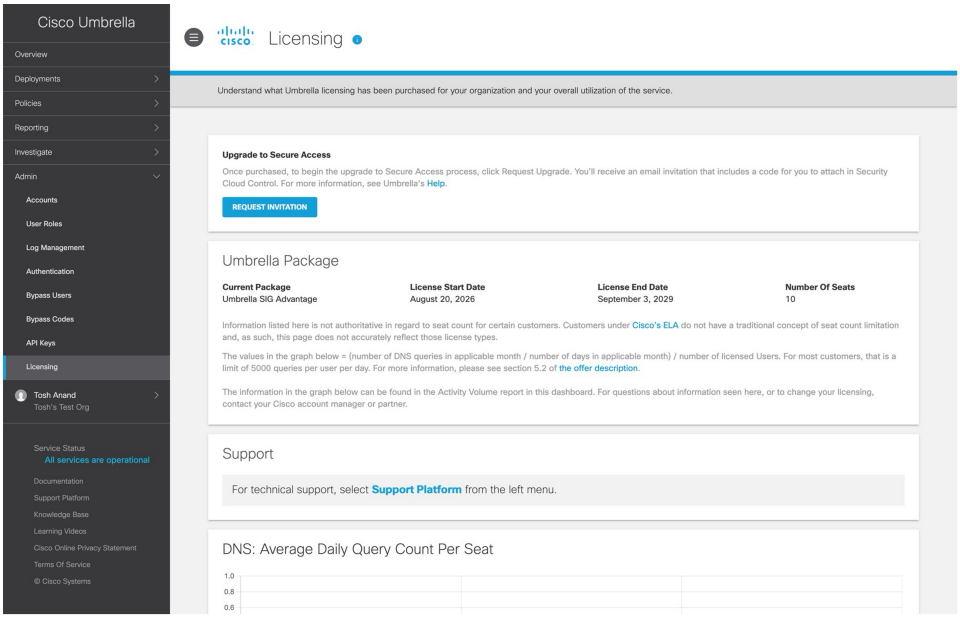


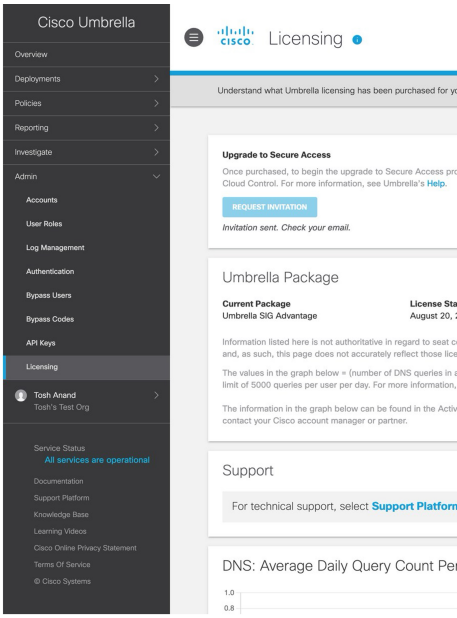
Upgrade Cisco Umbrella to Cisco Secure Access

This workflow requests the Secure Access upgrade, attaches an existing Cisco Secure Access instance to Security Cloud Control, and applies the subscription. Use the invitation and claim codes sent to your organization; codes shown in screenshots are examples.

Request the Secure Access upgrade

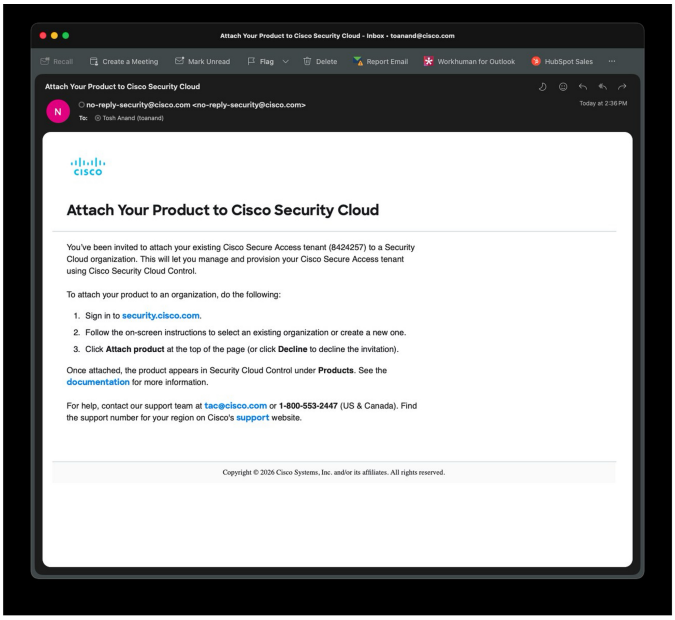
- Sign in to your Cisco Umbrella dashboard.
- Open **Admin** and select **Licensing**.
- Under **Upgrade to Secure Access**, select **Request Invitation**.
- When the page confirms that the invitation was sent, check the email account associated with your organization.

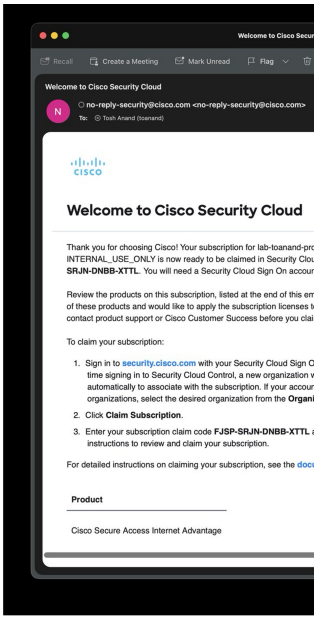




Review the invitation emails

- Open the **Attach Your Product to Cisco Security Cloud** email. It invites you to attach the existing Secure Access instance to a Security Cloud organization.
- Open the **Welcome to Cisco Security Cloud** email and keep the subscription claim code available for the claim step.
- Sign in to Security Cloud Control with your Security Cloud Sign On account. If you do not have one, create an account before continuing.
- If you need to apply these subscription licenses to an existing product, contact product support or Cisco Customer Success before claiming the subscription, as directed in the welcome email.

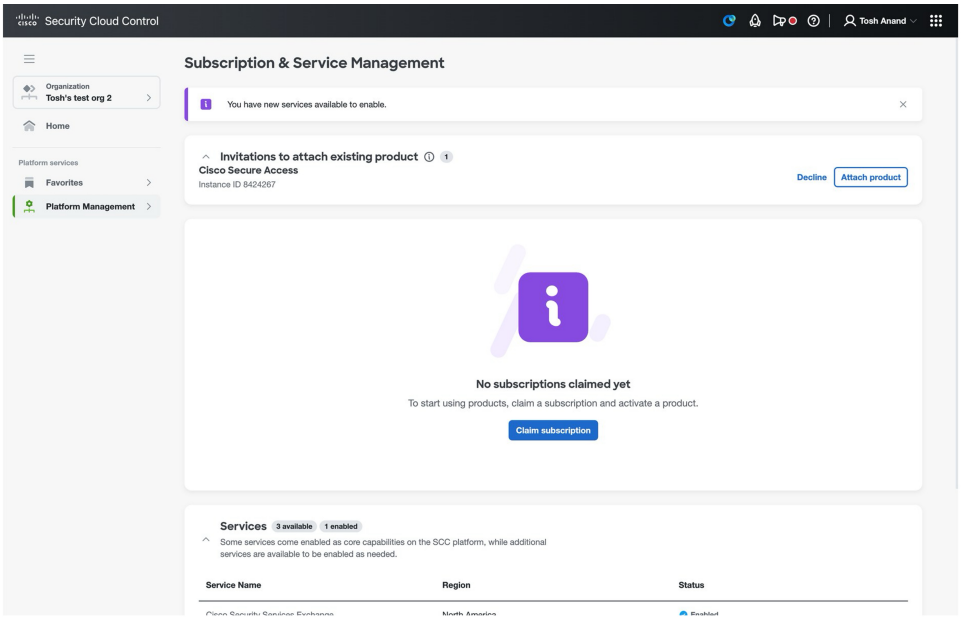


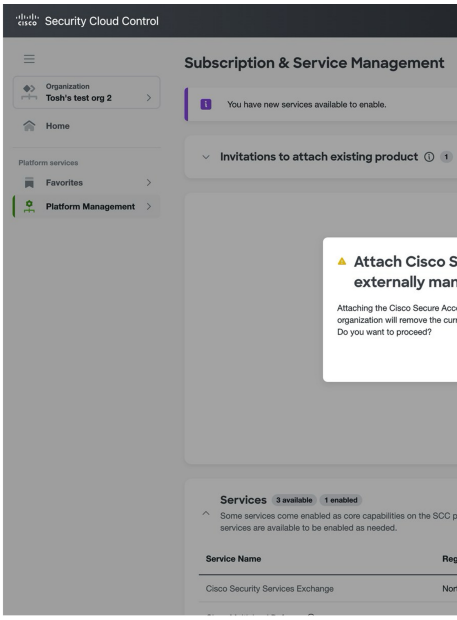


Attach the existing Secure Access instance

- In the attachment email, follow the link to **security.cisco.com** and sign in.

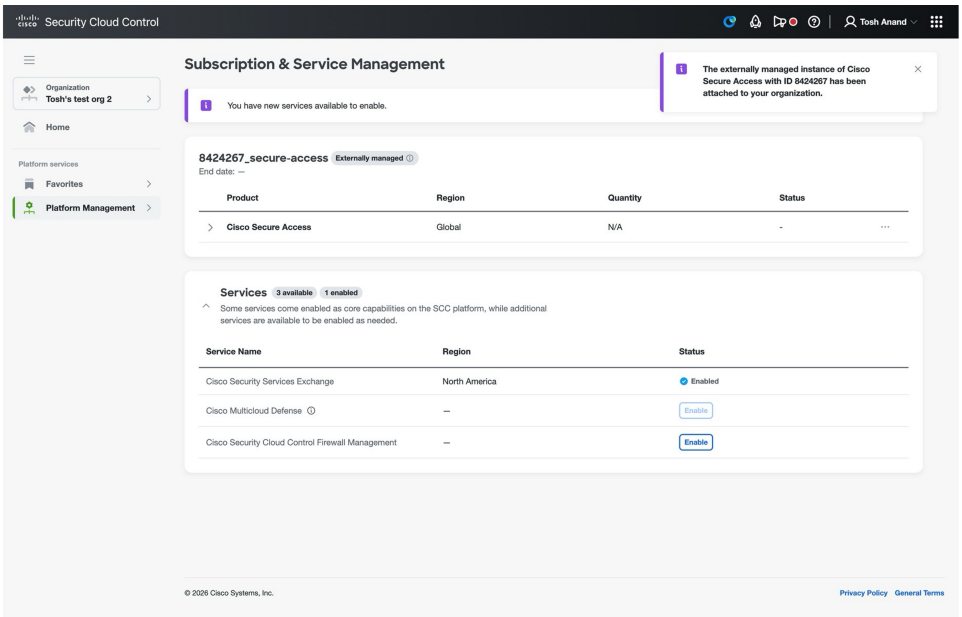
- Select the Security Cloud organization that should own the product, or create an organization if needed.
- In **Subscription & Service Management**, find the invitation to attach the existing Cisco Secure Access product and select **Attach product**.
- Review the confirmation. Attaching the externally managed instance removes the current inactive instance from the organization. Select **Attach** only if the organization and instance are correct.

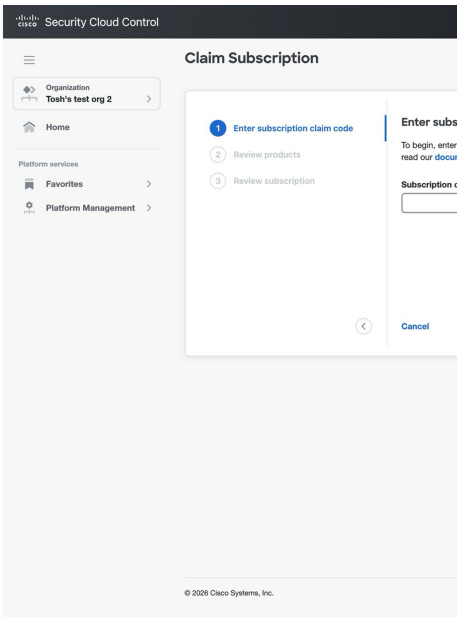




Confirm the attachment and open subscription claiming

- Confirm Security Cloud Control reports that the externally managed Cisco Secure Access instance is attached to your organization.
- Select **Claim subscription** to begin the subscription claim workflow.

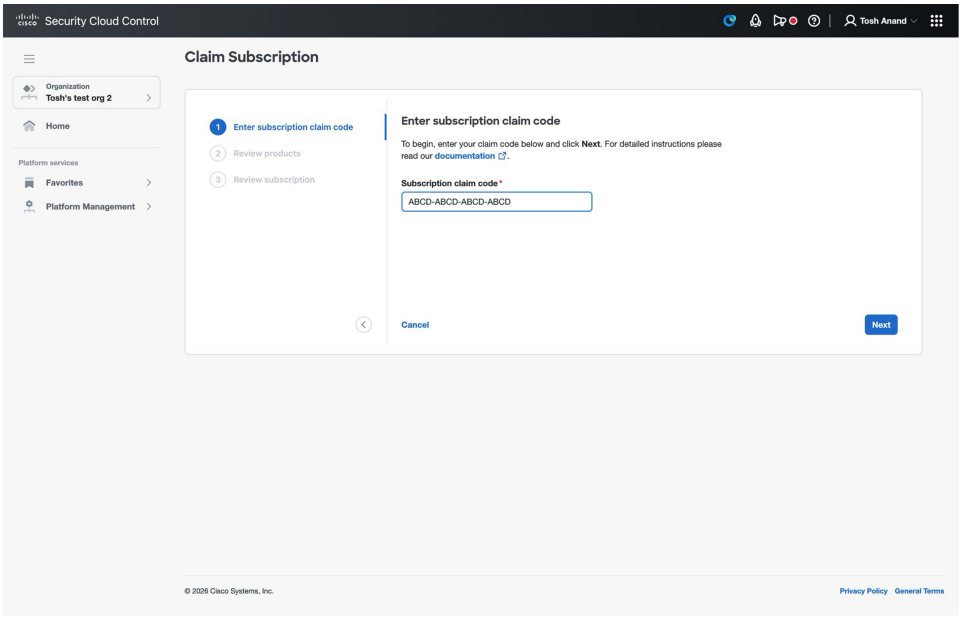




Enter the subscription claim code

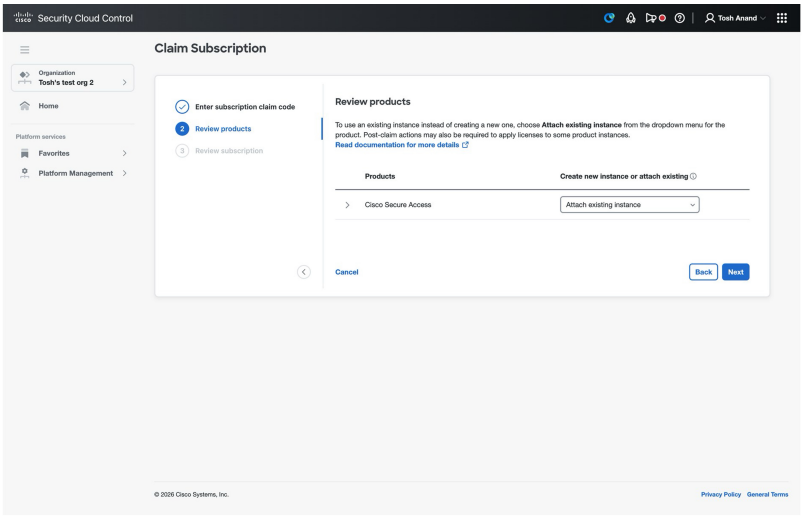
- On the **Claim Subscription** page, enter the claim code from the welcome email in **Subscription claim code**.
- 2. Select **Next**.

Use the complete code from your email. The code displayed in the screenshot is sample data.



Choose the existing instance

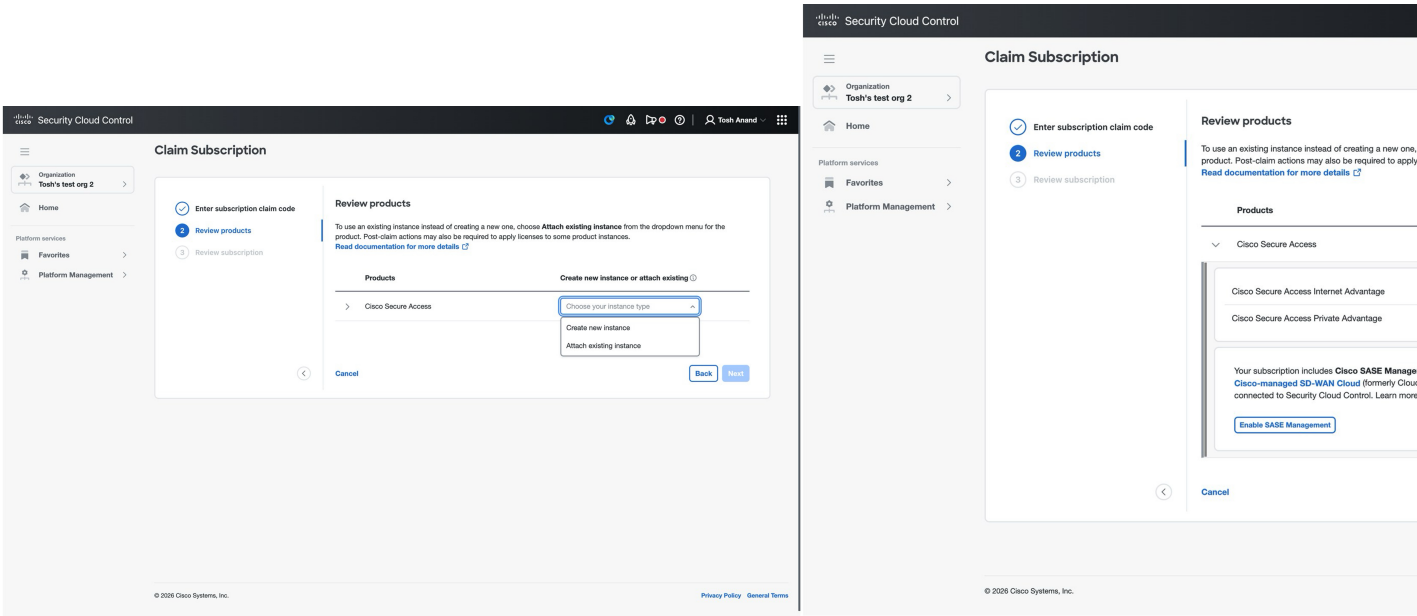
- On Review products, open the instance type menu for Cisco Secure Access.
- Select Attach existing instance to apply the subscription to the existing tenant. Select Create new instance only if you intend to provision a separate instance.



Review product options

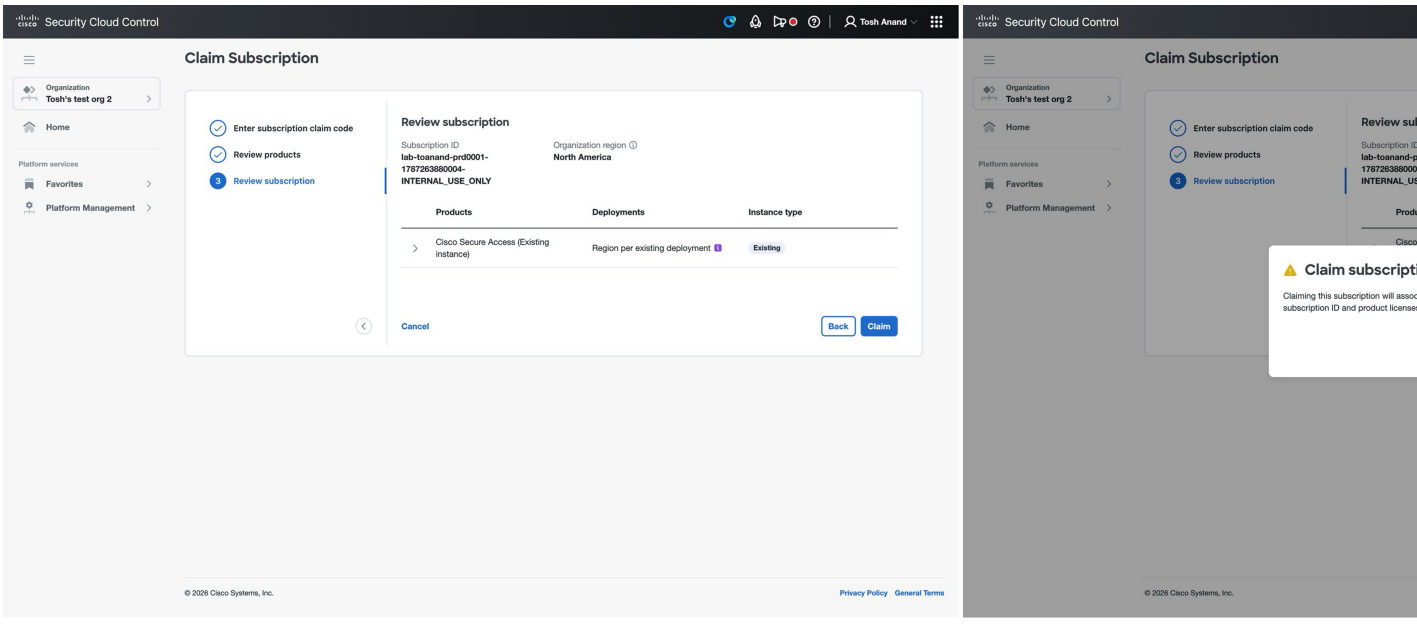
- Expand the **Cisco Secure Access** product row to review the included products and options.
- If the subscription includes Cisco SASE Management, connect the Cisco-managed SD-WAN Cloud fabric to Security Cloud Control as required. Select **Enable SASE Management** when you are ready to enable it.

Check that the selected product and instance match the organization where you want to use the subscription.



Review and claim the subscription

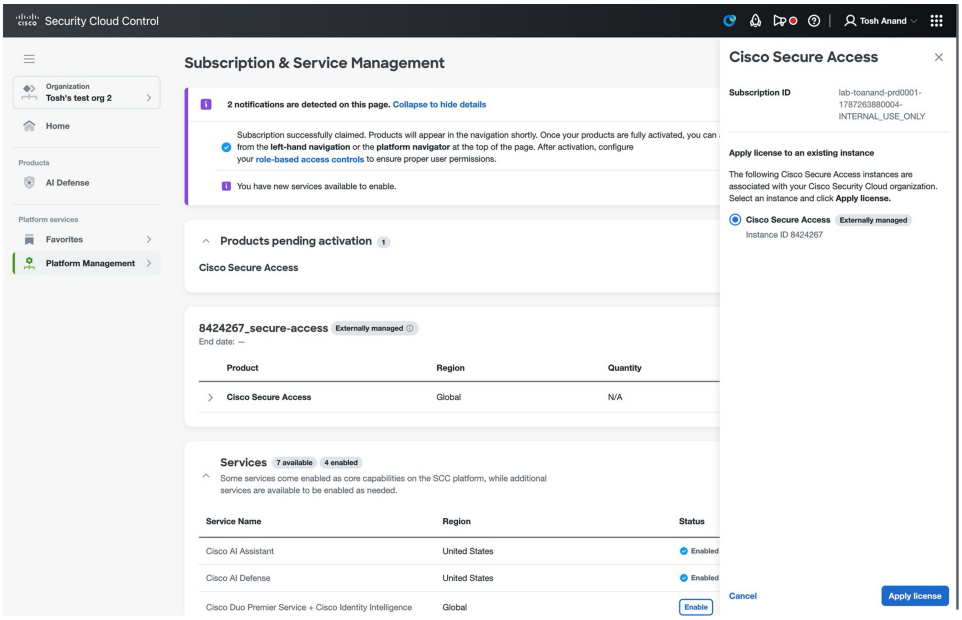
- On **Review subscription**, verify the organization region and confirm the product is shown as **Cisco Secure Access (Existing instance)**.
- Select **Claim**.
- Read the confirmation that the subscription ID and product licenses will be associated with the displayed organization.
- Select **Claim** to confirm.

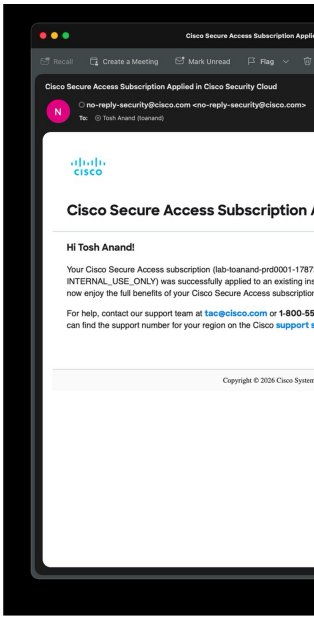


Apply the license and confirm completion

- After the subscription is claimed, open the **Cisco Secure Access** product panel.
- Under **Apply license to an existing instance**, select the existing Cisco Secure Access instance.

- Select **Apply license**.
- Check your email for **Cisco Secure Access Subscription Applied in Cisco Security Cloud**. The message confirms that the subscription was applied to the existing instance.





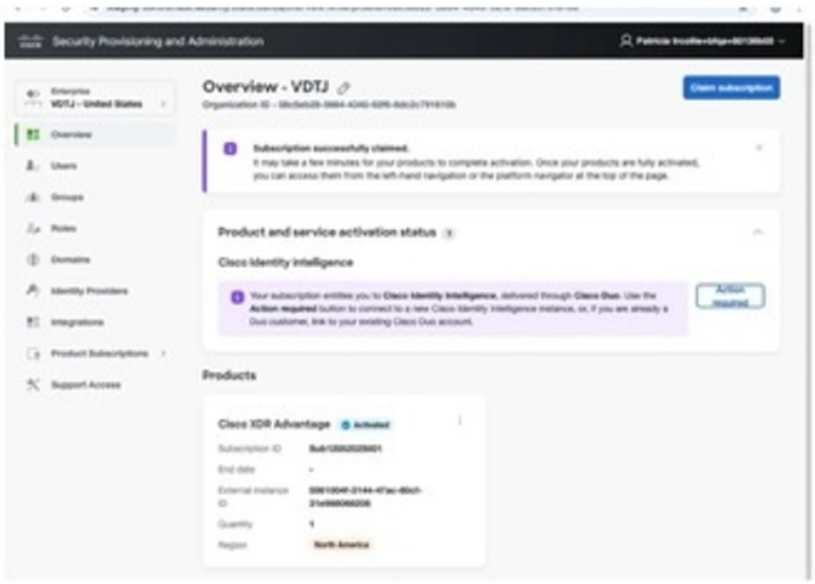
Activate Cisco XDR Advantage

Use this workflow after the Cisco XDR Advantage subscription is claimed in Security Cloud Control. It connects an existing Secure Client Cloud Management instance to your Security Cloud Control Enterprise and verifies the XDR activation.

Confirm the subscription and activation code

- In **Security Provisioning and Administration**, confirm the overview reports that the subscription was successfully claimed and **Cisco XDR Advantage** appears under Products.
- Locate the **Cisco XDR Advantage** activation code in Security Cloud Control and select **Copy** if you need to enter the code manually.

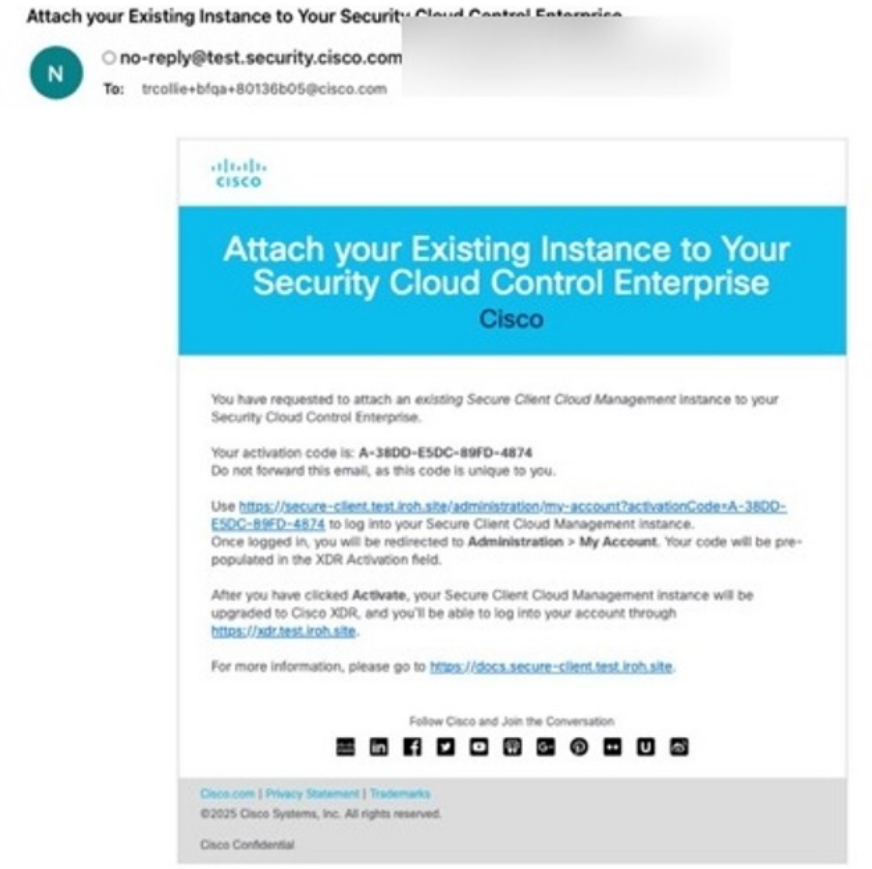
Use the activation email issued for your organization. Do not forward activation emails or codes.





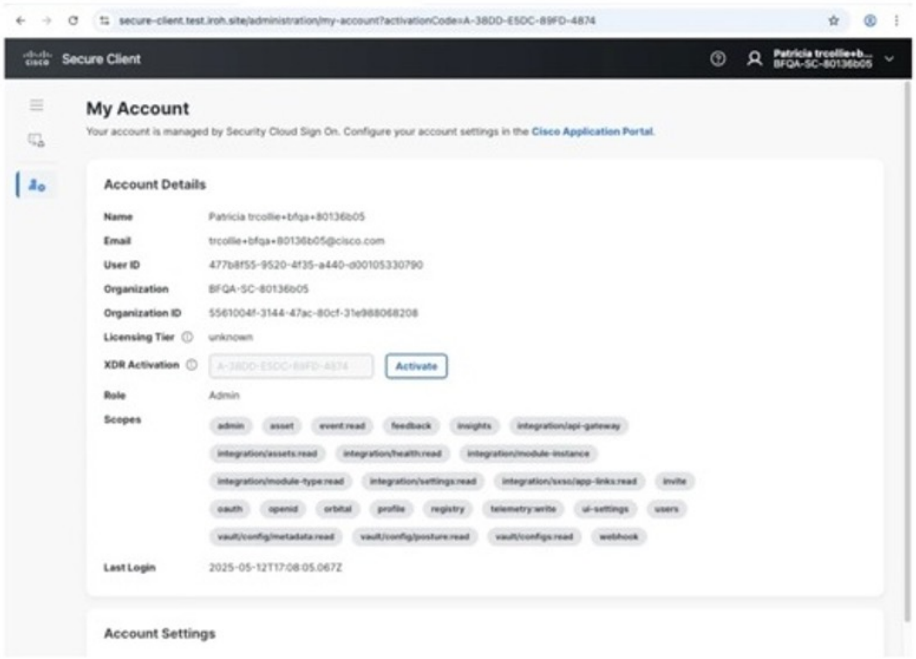
Open the instance attachment email

- Open the **Attach your Existing Instance to Your Security Cloud Control Enterprise** email.
- Select the Secure Client link in the email and sign in with your Cisco Security Cloud Sign On account.
- The email says its unique activation code is prepopulated in the **XDR Activation** field after sign-in. Do not forward the email.



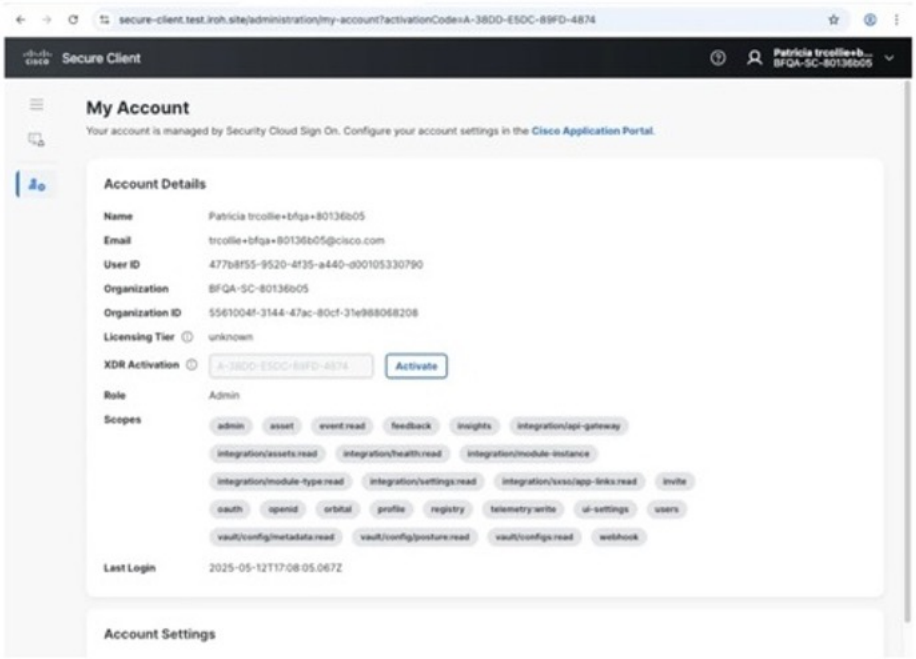
Activate the existing instance

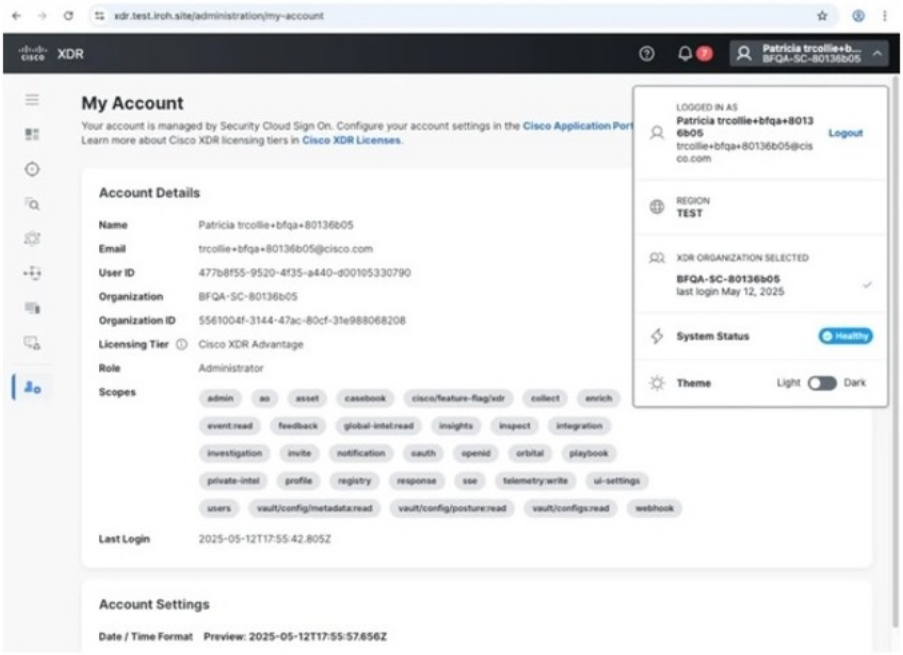
- In **Administration > My Account**, confirm the **XDR Activation** field contains the code from the invitation email.
- Select **Activate**. This upgrades the existing Secure Client Cloud Management instance to Cisco XDR.



Verify the XDR account

- Sign in to Cisco XDR and open **My Account**.
- Confirm the expected organization is selected and **Licensing Tier** shows **Cisco XDR Advantage**.
- Click **Activate**.




xdr.test.iroh.site/administration/my-account
XDR
Patricia trcollie+b...
BFQA-SC-80136b05
My Account
Your account is managed by Security Cloud Sign On. Configure your account settings in the Cisco Application Port
Learn more about Cisco XDR licensing tiers in Cisco XDR Licenses.
Account Details
Name
Patricia trcollie+bfqa+80136b05
Email
trcollie+bfqa+80136b05@cisco.com
User ID
477b8f55-9520-4f35-a440-d00105330790
Organization
BFQA-SC-80136b05
Organization ID
5561004f-3144-47ac-80cf-31e988068208
Licensing Tier
Cisco XDR Advantage
Role
Administrator
Scopes
admin
ao
asset
casebook
cisco/feature-flag/xdr
collect
enrich
event:read
feedback
global-intel:read
insights
inspect
integration
investigation
invite
notification
oauth
openid
orbital
playbook
private-intel
profile
registry
response
sse
telemetry:write
ui-settings
users
vault/config/metadata:read
vault/config/posture:read
vault/configs:read
webhook
Last Login
2025-05-12T17:55:42.805Z
Account Settings
Date / Time Format
Preview: 2025-05-12T17:55:57.656Z
LOGGED IN AS
Patricia trcollie+bfqa+80136b05
trcollie+bfqa+80136b05@cisco.com
Logout
REGION
TEST
XDR ORGANIZATION SELECTED
BFQA-SC-80136b05
last login May 12, 2025
System Status
Healthy
Theme
Light
Dark