Cisco Security Cloud Control: On-Premises Firewall Management Center Integration

Cisco Security Cloud Control
Updated NaN,

© 2021-2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

1 Introduction

Topics:

- Overview of Security Cloud Control Firewall Management
- Manage On-Premises Firewall Management Center with Security Cloud Control
- Security Cloud Control Firewall Management dashboard

Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator) is a cloud-based platform that unifies and simplifies security policy management across Cisco firewalls and devices. It streamlines policy consistency, offers intuitive and advanced interfaces, and reconciles configuration changes across multiple device managers.

Overview of Security Cloud Control Firewall Management

An overview of Security Cloud Control Firewall Management for managing firewall devices, policies, objects, and configuration consistency.

Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator or CDO) is a cloud-based security policy manager that helps simplify and unify security policies across your Cisco firewalls and other devices such as Cisco IOS and SSH. The firewalls and devices can be managed from **Firewall**, which is listed under **Products** in the Security Cloud Control dashboard.

Security Cloud Control Firewall Management helps you optimize your security policies by identifying inconsistencies within them and by providing with the tools to fix them. It provides you with ways to share objects and policies, as well as create configuration templates, to promote policy consistency across devices.

Because Security Cloud Control Firewall Management coexists with Adaptive Security Device Manager (ASDM), it keeps track of configuration changes made by ASDM and reconciles the differences.

You can manage a wide range of devices in one place. Advanced users will also find their traditional CLI interface with some new enhancements to make management even more efficient for them.

Security Cloud Control Firewall Management also provides a guided "Day 0" experience, helping you to quickly onboard Threat Defense devices to your on-premises or Cloud-Delivered Firewall Management Center. It also presents you with other key features that you may benefit from and helps you enable and configure them.

Device onboarding requirements

Before you onboard a device, complete these prerequisites:

- Complete the installation wizard.
- License the device.

After you complete those prerequisites, use the Security Cloud Control Firewall Management onboarding wizard to onboard the device.

Keep these restrictions in mind:

- After you onboard devices to a Security Cloud Control Firewall Management associated with an organization, you cannot migrate those devices to another organization.
- To move devices to a new organization, you must re-onboard them to the new organization.

Cisco Online Privacy Statement

Cisco Systems, Inc. and its subsidiaries (collectively referred to as "Cisco") are committed to protecting your privacy and providing you with a positive experience on Cisco websites and while using Cisco products and services ("Solutions"). Read the Cisco Online Privacy Statement carefully to get a clear understanding of how Cisco collects, uses, shares, and protects your personal information.

Manage On-Premises Firewall Management Center with Security Cloud Control

Learn how to onboard, view, manage, and cross-launch to on-premises Firewall Management Center in Security Cloud Control. You can manage devices, monitor status, and handle network objects.

About On-Premises Firewall Management Center

On-Premises Firewall Management Center is a centralized management console with graphical user interface. You can use it to perform administrative, management, analysis, and reporting tasks. This console is similar to ASDM and FDM, but provides different features.

On-Premises Firewall Management Center support is limited to onboarding, viewing its managed devices, viewing, managing network objects, and cross-launching to the on-premises Firewall Management Center UI for managing associated devices and objects. Additional features will be available soon.

If a feature is not supported by Security Cloud Control at this time, use the on-premises Firewall Management Center console. To learn more about the features provided by on-premises Firewall Management Center, see Cisco Secure Firewall Management Center Configuration Guide for your system's version.

For a list of on-premises Firewall Management Center devices and software versions that Security Cloud Control supports, see Software and Hardware support by Security Cloud Control.

Version Support

Security Cloud Control supports version 6.4 and later. On-Premises Firewall Management Center can manage older devices, typically a few major versions back. For example, devices running version 6.6.0 can manage devices running version 6.4.0. If an on-premises Firewall Management Center manages a device that is running a version earlier than 6.4, the device may be displayed in the **Security Devices** page, but cannot be deployed to or its policies modified from Security Cloud Control. You must make changes and deploy from the on-premises Firewall Management Center UI.

> **Note**
>
> If a managed device is disabled, or unreachable, Security Cloud Control may display the device in the **Security Devices** page, but cannot successfully send requests or view device information.

How does Security Cloud Control Communicate with an FMC

Security Cloud Control acts as a REST API client to send requests to on-premises Firewall Management Center, and then on-premises Firewall Management Center uses its designated client to channel the requests to its managed devices.

As the device does not allow multiple logins with the same credentials, you must create a new user on the on-premises Firewall Management Center specifically for Security Cloud Control communication. This user must have administrator-level permissions. This new user will have to be replicated on Security Cloud Control, as either a Security Cloud Control-provided Administrator or a custom user role with **system** and **devices** permissions. Without an admin login, Security Cloud Control cannot use REST API commands to modify or create policies, rules, or objects.

Onboard or Remove an On-Premises Firewall Management Center

You can onboard or remove an on-premises Firewall Management Center at any time. On-Premises Firewall Management Center and its registered devices must be running at least version 6.4 to be read by Security Cloud Control. To onboard an on-premises Firewall Management Center and its registered devices, see Onboard an FMC.

Once an on-premises Firewall Management Center is onboarded, select the on-premises Firewall Management Center from **Administration** > **Integrations** > **Firewall Management Center** and click **Devices** under **Management** or any actions on the right pane to open up the **Verify FMC Cross Launch URL** wizard, which allows you to enter the public IP address or the FQDN and the port number of your management center. Click **Continue** to cross-launch to the selected on-premises Firewall Management Center web UI in a new tab using the IP address you entered. You can also add external links manually using the **Add External Links** option under **External Links** on the right pane.

Removing an on-premises Firewall Management Center from your Security Cloud Control tenant also removes the devices registered to that on-premises Firewall Management Center. See Remove an FMC from Security Cloud Control for more information.

If an on-premises Firewall Management Center experiences an "Invalid Credentials" status after onboarding, you can **reconnect** the appliance. See Troubleshoot Invalid Credentials for more information.

> **Note**
>
> Devices running Firewall 6.6 do not support the **reconnect** feature. If you have to reconnect the appliance, we recommend removing the on-premises Firewall Management Center and re-onboarding the appliance.

Devices Managed by an On-Premises Firewall Management Center

Once you onboard an on-premises Firewall Management Center to Security Cloud Control, all the devices registered to that on-premises Firewall Management Center are also imported into Security Cloud Control. On the **Security Devices** page, you can view device information such as name, IP address, device type, software version, and state.

> **Note**
>
> Your on-premises Firewall Management Center is displayed on the **Services** page, and the devices it manages are listed on the **Security Devices** page.

In the **Services** page, you can see information such as version, devices managed, device type, and status. Clicking the devices icon on the **Services** page, which shows the number of devices your FMC manages, directs you to the **Security Devices** page with a filter applied to display all devices managed by the selected on-premises Firewall Management Center.

You can perform actions using options in the **Device Actions**, **Monitoring**, **Device Management**, and **Policies** panels available from the **Security Devices** page. If you select a device that is currently managed by an FMC and click these options, Security Cloud Control automatically launches the on-premises Firewall Management Center console that manages the devices using the cross-launch URL you had entered.

Use the filter icon to further organize the **Security Devices** page. From this page, you can view all the devices managed by the onboarded on-premises Firewall Management Center and other supported device types. In addition, you can expand or collapse devices in a cluster and select them individually or as a group to perform actions.

Device Health Status

Security Cloud Control displays the health status of threat defense devices on the **Security Devices** page, such as **Normal**, **Error**, **Warning**, and **Disabled**. You can click the status of a device to navigate to the **Health Monitoring** page that corresponds to the device in the on-premises Firewall Management Center UI.

> **Note**
>
> Security Cloud Control automatically updates the device health status every 10 minutes. You can also do this manually by selecting the device and clicking **Check for Changes**.

Objects

After you onboard an on-premises Firewall Management Center to Security Cloud Control, you can choose to discover objects from on-premises Firewall Management Center and manage them in Security Cloud Control. You can do this by

choosing **Administration** > **Integrations** > **Firewall Management Center**, selecting the desired on-premises Firewall Management Center, and clicking **Settings**. You can enable the **Discover & Manage Network Objects** toggle button. When this option is enabled, Security Cloud Control automatically imports all the objects from the On-Premises Firewall Management Center-managed devices into Security Cloud Control. Once imported, the objects can be managed from Security Cloud Control.

> **Note**
>
> You must have the super-admin or admin user role to use the **Settings** button.

When you change an object configuration in Security Cloud Control, Security Cloud Control stages the change. After you review it in **Pending Changes**, you can manually push the change to on-premises Firewall Management Center. When you make a configuration change to an object from the on-premises Firewall Management Center UI, Security Cloud Control detects that change as an out-of-band change that can be synchronized later. If you want your changes to be automatically synchronized with on-premises Firewall Management Center and not staged for review, enable the **Enable automatic sync of network objects** toggle button.

If you have existing objects in Security Cloud Control that you want to assign to your on-premises Firewall Management Center, select the on-premises Firewall Management Center from the **Services** page and choose **Assign Objects** on the right pane. Security Cloud Control displays all the existing objects and allows you to select the ones that you want to associate with the on-premises Firewall Management Center that you selected. Use this to ensure that network object definitions are consistent across all platforms you manage with Security Cloud Control. You can use the **Assign Objects** button only if **Discover & Manage Network Objects** is enabled for the selected on-premises Firewall Management Center.

> **Note**
>
> - You cannot enable the **Discover & Manage Network Objects** toggle button if the on-premises Firewall Management Center that you have selected has one or more child domains or has the Change Management workflow enabled on it.
> - You cannot enable the **Enable automatic sync of network objects** toggle button if the **Discover & Manage Network Objects** toggle button is disabled.

On-Premises Firewall Management Center supports the following object types:

- Network Objects
- Network Group Objects

Object Issues

Security Cloud Control identifies duplicate, inconsistent, or unused objects, and you can filter the issues based on their issue states. However, Security Cloud Control cannot resolve object issues.

Eventing

Searching and filtering the historical and live event tables for specific events works the same way as it does for other information in Security Cloud Control. For more information, see Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide.

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging allows you to capture connection, intrusion, file, malware, and security intelligence events from all your devices and view them in a single location in Security Cloud Control.

You can view events stored in the Cisco cloud on the Event Logging page in Security Cloud Control. Use filters to review which security rules are triggered in your network. The **Logging and Troubleshooting** package gives you these capabilities.

With the **Firewall Analytics and Monitoring** package, the system can apply Secure Cloud Analytics dynamic entity modeling to your events and use behavioral modeling analytics to generate Secure Cloud Analytics observations and alerts. If you obtain a **Total Network Analytics and Monitoring** package, the system applies dynamic entity modeling to both your device events and your network traffic and generates observations and alerts. You can cross-launch from Security Cloud Control to a Secure Cloud Analytics portal provisioned for you, using Cisco Single Sign-On.

Security Cloud Control Firewall Management dashboard

Learn about the Security Cloud Control Firewall Management dashboard for organization-level visibility, insights, actions, and customizable widgets.

The Security Cloud Control Firewall Management dashboard is your central hub for monitoring and managing organization-level details across various categories. Upon logging in, you can access a customizable dashboard that offers critical insights and actions to optimize security and operational efficiency.

Customize your dashboard

Make your dashboard fit your specific needs by customizing the visible widgets:

1. On the **Home** page, click **Customize**.
2. Select or deselect dashboard widgets and drag and drop them to arrange in your preferred order.

Top Information

This section provides detailed insights into various tenant-level metrics. If enabled, you can view the following widgets:

- **Configuration States**: Indicates the discrepancies between the configurations on your devices and those maintained by Security Cloud Control. This comparison helps identify any inconsistencies or conflicts that may exist.

  For more information, see Device Management.

- **Change Log Management**: Helps you manage the change logs for precise operational control. The widget displays **Completed** and **Pending** change logs.

  For more information, see Change Logs.

- **RA VPN Sessions**: Helps you monitor your Remote Access VPN sessions.

  For more information, see RA VPN Sessions.

- **Overall Inventory**: Helps you monitor the health and status of all devices. The widget displays the total number of devices, categorized into **Issues**, **Pending Actions**, **Other**, **Online** and devices that are nearing or have already reached their last day of hardware support.

  For more information, see All Devices.

- **Site-to-Site VPN**: Helps you manage and assess your site-to-site VPN connections. The widget displays the total number of VPN tunnels and the percentage that are **Active** and **Idle**.

  For more information, see Site-to-site VPN.

- **Accounts and Assets**:

  - Helps you track and manage your multicloud accounts and resources effectively. You can launch the Multicloud Defense Controller from here.
  - Click **+Add Account** to add a new account.

  For more information, see Multicloud Defense Controller.

- **Top Risky Destinations**: Helps you identify and monitor the top risky destinations that are granted access. The widget lists Applications and URL Categories and allows you to filter data for the last 90, 60, or 30 days. You can filter between **Allowed** (default) and **Blocked** traffic.
- **Top Intrusion and Malware Events**: Helps you monitor and respond to top intrusion and malware events. The widget displays intrusion events and malware events and allows you to filter data for the last 90, 60, and 30 days. You can filter between **Allowed** (default) and **Blocked** events.

Announcements

Click the **Announcements** icon to view the most recent Security Cloud Control features and updates. Links to related documentation are provided if you need more information on any of the items listed.

2 Configure basic settings

Topics:

- Overview of Security Cloud Control Firewall Management
- Overview of Cloud-Delivered Firewall Management Center

Security Cloud Control provides a unique view of policy management through a clear and concise interface. Below are topics that cover the basics of using Security Cloud Control for the first time.

Overview of Security Cloud Control Firewall Management

An overview of Security Cloud Control Firewall Management for managing firewall devices, policies, objects, and configuration consistency.

Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator or CDO) is a cloud-based security policy manager that helps simplify and unify security policies across your Cisco firewalls and other devices such as Cisco IOS and SSH. The firewalls and devices can be managed from **Firewall**, which is listed under **Products** in the Security Cloud Control dashboard.

Security Cloud Control Firewall Management helps you optimize your security policies by identifying inconsistencies within them and by providing with the tools to fix them. It provides you with ways to share objects and policies, as well as create configuration templates, to promote policy consistency across devices.

Because Security Cloud Control Firewall Management coexists with Adaptive Security Device Manager (ASDM), it keeps track of configuration changes made by ASDM and reconciles the differences.

You can manage a wide range of devices in one place. Advanced users will also find their traditional CLI interface with some new enhancements to make management even more efficient for them.

Security Cloud Control Firewall Management also provides a guided "Day 0" experience, helping you to quickly onboard Threat Defense devices to your on-premises or Cloud-Delivered Firewall Management Center. It also presents you with other key features that you may benefit from and helps you enable and configure them.

Device onboarding requirements

Before you onboard a device, complete these prerequisites:

- Complete the installation wizard.
- License the device.

After you complete those prerequisites, use the Security Cloud Control Firewall Management onboarding wizard to onboard the device.

Keep these restrictions in mind:

- After you onboard devices to a Security Cloud Control Firewall Management associated with an organization, you cannot migrate those devices to another organization.
- To move devices to a new organization, you must re-onboard them to the new organization.

Cisco Online Privacy Statement

Cisco Systems, Inc. and its subsidiaries (collectively referred to as "Cisco") are committed to protecting your privacy and providing you with a positive experience on Cisco websites and while using Cisco products and services ("Solutions"). Read the Cisco Online Privacy Statement carefully to get a clear understanding of how Cisco collects, uses, shares, and protects your personal information.

Security Cloud Control Firewall Management Platform Maintenance Schedule

Security Cloud Control Firewall Management receives weekly platform updates every Thursday from 09:00 to 12:00 UTC, delivering new features and quality improvements. Access remains available during maintenance, but avoid deploying configuration changes to ensure uninterrupted policy enforcement and stable device management.

Security Cloud Control Firewall Management updates its platform every week with new features and quality improvements. Updates are made during a 3-hour period according to this schedule:

Day of the week	Time of day (24-hour time, UTC)
Thursday	09:00 UTC - 12:00 UTC

During the Security Cloud Control Firewall Management upgrade period, you can still access your organization and the Cloud-Delivered Firewall Management Center. Additionally, the devices that you have onboarded to Security Cloud Control Firewall Management continue to enforce their security policies.

Note

- During the maintenance period of the Security Cloud Control Firewall Management, refrain from creating or deploying configurations to the devices it manages.
- If there is any issue that stops Security Cloud Control Firewall Management from communicating, Cisco addresses that issue in all the affected tenants as quickly as possible, even if it is outside the maintenance window.

Security Cloud Control Firewall Management licenses

Security Cloud Control Firewall Management requires a base subscription and device licenses to manage firewalls and supported devices. Choose term-based plans to match your deployment needs, access software updates, and receive Cisco TAC support. Catalyst SD-WAN doesn't require an additional license; customers using Cisco Digital Network Architecture (DNA) or WAN Essentials license can integrate with Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management requires a base subscription for organization entitlement and device licenses for managing devices. You can buy one or more Security Cloud Control Firewall Management base subscriptions based on the number of tenants you require and device licenses based on the device model number and the quantity. In other words, purchasing the base subscription provides you with a Security Cloud Control Firewall Management organization. For every device you choose to manage using Security Cloud Control Firewall Management, you need separate device licenses.

To onboard and manage devices from Security Cloud Control Firewall Management, you must purchase a base subscription and device-specific, term-based subscriptions based on the devices you want to manage.

Subscriptions

Security Cloud Control Firewall Management subscriptions are term-based:

- **Base**: Offers subscriptions for one, three, and five years, and provides entitlement to access the Security Cloud Control Firewall Management organization and onboard adequately licensed devices.
- **Device License**: Offers subscriptions for one, three, and five years for any supported device you choose to manage. For example, you can choose to manage a Cisco Firepower 1010 device using Security Cloud Control Firewall Management for three years if you purchase a three-year software subscription for the Cisco Firepower 1010 device.

See Software and Hardware Supported by Security Cloud Control Firewall Management for more information on Cisco security devices that Security Cloud Control Firewall Management supports.

Important

You do not require two separate device licenses to manage a high-availability device pair in Security Cloud Control Firewall Management. If you have a high-availability pair, purchasing one device license is sufficient because Security Cloud Control Firewall Management considers the pair of high-availability devices as one single device.

Note

- Catalyst SD-WAN does not require an additional license for integration with Security Cloud Control Firewall Management. Customers with Cisco Digital Network Architecture (DNA) or WAN Essentials licenses can use these existing licenses for integration without needing any other license.
-

Note

You cannot manage Security Cloud Control Firewall Management licensing through the Cisco Smart Licensing portal.

Software Subscription Support

The Security Cloud Control Firewall Management base subscription includes software subscription support that is valid for the term of the subscription and provides access to software updates, major upgrades, and Cisco Technical Assistance Center (TAC) at no extra cost. While software support is selected by default, you can also leverage Security Cloud Control Firewall Management solution support based on your requirement.

More Supported Devices and Licenses

In addition to supporting Secure Firewall Threat Defense devices through the Cloud-Delivered Firewall Management Center, Security Cloud Control also manages these devices:

- Cisco Secure Firewall ASA
- On-premises Cisco Secure Firewall Management Center
- Cisco Meraki Security Appliance
- Cisco IOS devices
- Devices accessible using SSH
- Amazon Web Services (AWS) virtual private cloud (VPC)
- Umbrella Organization

You will need a Security Cloud Control base entitlement license and a license specific to the device you want to manage.

Overview of Cloud-Delivered Firewall Management Center

An overview of Cloud-Delivered Firewall Management Center, including Threat Defense management, migration, onboarding, high availability, security analytics, and licensing.

Cloud-Delivered Firewall Management Center is a software-as-a-service product that manages Secure Firewall Threat Defense devices through Security Cloud Control Firewall Management. It provides many of the same functions as an On-Premises Firewall Management Center.

Cloud-Delivered Firewall Management Center has the same appearance and behavior as an On-Premises Firewall Management Center and uses the same FMC API.

Because it is a SaaS product, the Security Cloud Control Firewall Management operations team deploys and maintains the Cloud-Delivered Firewall Management Center software. As new features are introduced, the operations team updates the Cloud-Delivered Firewall Management Center in your Security Cloud Control Firewall Management organization.

Migration and onboarding details

A migration wizard is available to help you migrate Threat Defense devices from an On-Premises Firewall Management Center to Cloud-Delivered Firewall Management Center.

Devices must run one of these Threat Defense software releases before you migrate them:

- Minimum On-Premises Firewall Management Center: 7.2
- Minimum Threat Defense: 7.2.x (not supported for Version 7.1)

Threat Defense 7.1 releases are not supported for migration.

You onboard Threat Defense devices in Security Cloud Control Firewall Management by using familiar methods, such as entering the serial number or using a CLI command that includes a registration key.

After onboarding:

- The device appears in both Security Cloud Control Firewall Management and Cloud-Delivered Firewall Management Center.
- You configure the device in Cloud-Delivered Firewall Management Center.
- In Security Cloud Control Firewall Management, you can review device information such as version, configuration status, connectivity, health status, and node status.
- When you click the health status in Security Cloud Control Firewall Management, the platform opens the device health monitoring page in the Cloud-Delivered Firewall Management Center user interface.

Availability and Security Analytics

Security Cloud Control Firewall Management supports high availability for the Threat Defense devices that it manages through the data interface. This feature is supported for devices that run software version 7.2 or later.

You can analyze security events from onboarded threat defense devices by using either Security Analytics and Logging (SaaS) or Security Analytics and Logging (On-Premises):

- Security Analytics and Logging (SaaS) stores events in the cloud, and you view those events in Security Cloud Control Firewall Management.
- Security Analytics and Logging (On-Premises) stores events on an on-premises Secure Network Analytics appliance, and analysis occurs in the On-Premises Firewall Management Center.

In both cases, you can still send logs directly from firewalls to a log collector of your choice.

Licenses

The license for Cloud-Delivered Firewall Management Center is a per-device-managed license and there is no license required for the Cloud-Delivered Firewall Management Center itself. Existing Secure Firewall Threat Defense devices re-use their existing smart licenses and new Secure Firewall Threat Defense devices provision new smart licenses for each feature implemented on the Secure Firewall Threat Defense For more information, see Cloud-Delivered Firewall Management Center license.

Existing customers can continue to use Security Cloud Control for managing other device types like, the Secure Firewall ASA, Meraki, Cisco IOS devices, Umbrella, and AWS virtual private clouds. If you use Security Cloud Control to manage a Secure Firewall Threat Defense device configured for local management with Firepower Device Manager, you can continue to manage them with Security Cloud Control as well.

To learn how to have a Cloud-Delivered Firewall Management Center provisioned on your tenant, see Enable Cloud-delivered Firewall Management Center on Your Security Cloud Control Tenant.

See Managing Cisco Secure Firewall Threat Defense with Cloud-delivered Firewall Management Center for the complete administrator guide to the Cloud-Delivered Firewall Management Center.

Enable Cloud-Delivered Firewall Management Center

Learn how to enable Cloud-Delivered Firewall Management Center for a Security Cloud Control tenant, track provisioning status, receive readiness notifications, and prepare for licensing and device onboarding.

If you want to manage your Secure Firewall Threat Defense devices, you can enable the Cloud-Delivered Firewall Management Center on your tenant. You need to have an admin or a super admin user role to perform this task.

Procedure

From the Security Cloud Control menu, click **Administration** > **Integrations** > **Firewall Management Center** and click **Enable Cloud-Delivered FMC**.

Security Cloud Control starts provisioning a Cloud-Delivered Firewall Management Center instance in the background; it typically takes 15 to 30 minutes for this to be complete. You can track the provisioning progress on the **Status** column of **Cloud-Delivered FMC**.

After the provisioning is complete, the status changes to **Active**. In addition, you get a **Cloud-Delivered Firewall Management Center is Ready** notification on the Security Cloud Control notifications panel and on the applications on which you have configured incoming webhooks. See Notification Settings for more information.

> **Note**
>
> After you receive the **Cloud-Delivered Firewall Management Center is Ready** notification, ensure that you log out of and log in back to your tenant once, to see the **Cloud-Delivered FMC** right pane options, such as **Actions**, **Management**, and **System**.

What to do next:

a. Register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager (CSSM) to activate smart license. For detailed steps, refer to Register the Cloud-Delivered Firewall Management Center with the Smart Software Manager.

b. Onboard your Firewall Threat Defense devices to the Cloud-Delivered Firewall Management Center and manage them.

Determine the Cloud-Delivered Firewall Management Center Version in Security Cloud Control Firewall Management

Information about the Cloud-Delivered Firewall Management Center version is required primarily for migration planning, feature support verification, troubleshooting, licensing, and operational management.

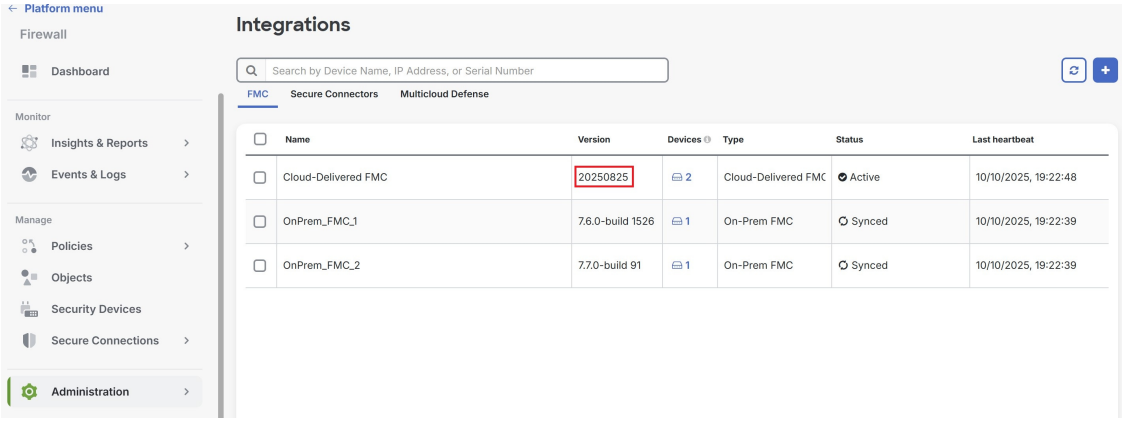
Use this procedure to determine the current version of your Cloud-Delivered Firewall Management Center in Security Cloud Control Firewall Management.

Before you begin

Enable Enable Cloud-Delivered Firewall Management Center in your organzation.

Procedure

1. In the left pane, click **Administration** > **Integrations** > **Firewall Management Center**.
2. Under the **FMC** tab, the version is displayed under the **Version** column.



For more information about Cloud-Delivered Firewall Management Center versions, see Release Notes for Cloud-Delivered Firewall Management Center.

Cloud-Delivered Firewall Management Center licensing and registration

Learn how to register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager for Smart Licensing. Registration enables export-controlled features and helps avoid deployment interruptions after the evaluation period.

Register Cloud-Delivered Firewall Management Center with Cisco Smart Licensing the same way you would for On-Premises Firewall Management Center.

Overview

Cloud-Delivered Firewall Management Center is included with the base subscription and trial for Security Cloud Control Firewall Management. You do not need to purchase a separate license for Cloud-Delivered Firewall Management Center. The base subscription or trial covers Cloud-Delivered Firewall Management Center, enabling you to manage Firewall Threat Defense devices through the cloud.

Cloud-Delivered Firewall Management Center is provisioned with a 90-day evaluation license upon deployment.

Important

We strongly recommend registering Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager immediately after deployment to access all features, including those requiring export encryption such as RAVPN and SSL VPN. Early registration prevents feature limitations and deployment interruptions.

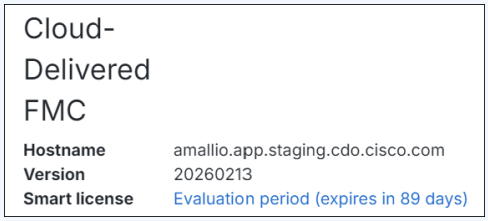
Evaluation license

- Features requiring export encryption, such as Remote Access VPN, SSL VPN, and other encryption-dependent options, remain disabled until you register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager (CSSM).

- After the 90-day evaluation period ends, you can continue onboarding Firewall Threat Defense devices, but manually triggered or scheduled deployments are blocked until registration with CSSM is completed.
- Security Cloud Control Firewall Management sends alert notifications as the evaluation license nears expiration.

Note

The **Smart license** field displays a warning when the evaluation license is expiration.



When the evaluation period ends, Cloud-Delivered Firewall Management Center is unregistered. Registering Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager converts from evaluation mode to a fully licensed state.

Click the evaluation warning link to open the smart licensing registration page and register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager.

Registration with Cisco Smart Software Manager (CSSM)

- Connect Cloud-Delivered Firewall Management Center to your smart licensing account, following the same process as On-Premises Firewall Management Center. The high-level procedure is provided in this section.
- No separate license purchase is needed for Cloud-Delivered Firewall Management Center; the license is automatically applied upon registration.
- Registering with smart licensing enables encryption export features.
- Registration ensures compliance and prevents deployment issues.

To learn how to get a Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant, see Request a Cloud-Delivered Firewall Management Center for your Security Cloud Control Tenant.

Licensing for Firewall Threat Defense devices

- No separate license purchase is needed for Cloud-Delivered Firewall Management Center.
- Each Firewall Threat Defense device managed by Cloud-Delivered Firewall Management Center requires an individual license.
- After registering Cloud-Delivered Firewall Management Center with CSSM, an administrator may apply feature licenses to security devices.

Step-by-step registration

A high-level procedure is provided here. For detailed steps, see Register the Management Center with the Smart Software Manager.

1. Create or Access Your Smart Account:

   Ensure you have a Cisco Smart Software Manager account. If you do not have one, create it at Smart Software Manager.

2. Generate a Registration Token or Use a Registration Token:

   In the Smart Software Manager, use an existing valid registration token or generate a registration token for the virtual account to which you want to register the Cloud-Delivered Firewall Management Center.

   a. Navigate to **Inventory > New Token**.

   b. Enter a description and set an expiration (Cisco recommends 30 days).

   c. Create and copy the token.

3. Register Cloud-Delivered Firewall Management Center with the Token:

   a. Log in to the Cloud-Delivered Firewall Management Center interface.

   b. Navigate to **System > Licenses > Smart Licenses**.

   c. Click **Register** and paste the registration token into the **Product Instance Registration Token** field.

   d. Ensure there are no extra spaces or blank lines before or after the token.

   e. Click **Apply Changes**.

4. Verify Registration:

   After registration, verify the license status under **System > Licenses > Smart Licenses** to confirm successful registration, license application, and that “Export-Controlled Features” are enabled.

Cloud-Delivered Firewall Management Center Maintenance Schedule

Find details about Cloud-Delivered Firewall Management Center maintenance schedule, including Customers who have a Cloud-Delivered Firewall Management Center deployed on their organization are notified approximately 1 week before Security Cloud Control updates the Cloud-Delivered.

Customers who have a Cloud-Delivered Firewall Management Center deployed on their organization are notified approximately 1 week before Security Cloud Control updates the Cloud-Delivered Firewall Management Center environment.

Super Admin and Admin users of the tenant are notified by email. Security Cloud Control also displays a banner on its home page notifying all users of upcoming updates.

Note

- During the maintenance period of the Cloud-Delivered Firewall Management Center, refrain from creating or deploying configurations to the devices it manages.
- If there is any issue that stops Security Cloud Control or Cloud-Delivered Firewall Management Center from communicating, that failure is addressed on all affected tenants as quickly as possible, even if it is outside the maintenance window.

3 Manage Firewall administration in Security Cloud Control Firewall Management

Topics:

- Configure general settings
- Manage users and groups within Security Cloud Control organization
- Manage API-Only users for Security Cloud Control Firewall Management
- View Security Cloud Control notifications
- View logging settings
- Understand user roles in Security Cloud Control Firewall Management
- Filters on security devices, policies, and objects page

Learn how Firewall administration settings apply across the managed organization and can affect multiple devices and users.

Use this chapter if you administer Security Cloud Control Firewall Management for your organization. It explains how to manage organization-wide firewall settings, user access, notifications, logging visibility, and role permissions.

This section provides the following information:

- General Settings
- API User Management
- Logging Settings

What firewall administration settings control

Firewall administration settings apply across the managed organization and can affect multiple devices and users. Some toggle buttons appear only when the related feature is enabled for your managed organization.

Configure general settings

Learn how to configure organization-wide settings that affect multiple managed devices and users in Security Cloud Control Firewall Management.

Use **Administration** > **General Settings** to manage organization-wide settings that affect multiple managed devices and users in your managed organization.

> **Note**
>
> You do not see toggle buttons for features that are not enabled for your managed organization.

Enable Change Request Tracking

Enabling Change Request Tracking lets you monitor and manage configuration changes across the tenant. Use this feature to implement formal change management workflows that maintain a comprehensive audit trail for all system modifications.

Enabling change request tracking affects all users of your tenant. To enable change request tracking, perform these steps:

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn on the **Change Request Tracking** toggle button.

   Once confirmed, you see the Change Request toolbar appear in the lower left corner of the interface and the Change Request drop-down menu in the Change Log.

Enable AI Assistant for Firewall

The AI Assistant provides contextual guidance for managing security policies, troubleshooting, and optimizing configurations to enhance operational efficiency. Tenant administrators should manage this setting within General Settings to control access for their entire organization.

AI Assistant is an AI-driven virtual companion that provides contextual guidance and insights to manage security policies, troubleshooting issues, and optimizing configurations. For more information, refer to Onboard with Cisco AI Assistant.

By default, the AI Assistant is enabled. When you enable or disable the AI Assistant, the change affects all users in your tenant .

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn off the **Enable AI Assistant for Firewall** toggle button to disable the AI Assistant.

Enable the option to auto-accept device changes

Enable auto-accept for device changes to streamline configuration management by automatically syncing updates, eliminating the need for manual conflict reviews. This task should be performed when you want to automate change synchronization across your managed devices.

When this setting is enabled, Security Cloud Control Firewall Management automatically accepts changes that users make directly on the device. If you leave this setting disabled, or disable it later, you must review each device conflict before you accept it.

Follow these steps to enable automatic acceptance of device changes:

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn on the **Enable the option to auto-accept device changes** toggle button.

Enable Multicloud Defense SCC features

Use the Enable Multicloud Defense SCC features option to integrate specific platform capabilities directly into your Security Cloud Control Firewall Management environment. Perform this task whenever you need to leverage advanced Multicloud Defense functionalities within your existing security management workflow.

When you enable this feature, you can configure site-to-site IPsec VPN tunnels between Multicloud Defense and your ASA and Firewall Threat Defense devices that are managed by Security Cloud Control Firewall Management. After you enable the feature, you can establish and deploy VPN configurations between these managed devices to improve secure connectivity across your multicloud infrastructure.

Follow these steps to enable Multicloud Defense Security Cloud Control Firewall Management features:

Procedure

1. Choose **Settings** > **General Settings**.
2. Turn on the **Enable Multicloud Defense SCC features** toggle button.

Enable object sharing with Multicloud Defense

Use the Enable object sharing with Multicloud Defense option to synchronize network objects seamlessly, ensuring policy consistency across platforms. This task should be performed when you need to integrate security objects between Security Cloud Control Firewall Management and Multicloud Defense for improved operational efficiency.

Enable this setting to share Multicloud Defense network objects from Security Cloud Control Firewall Management.

Follow these steps to enable object sharing with Multicloud Defense:

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn on the **Enable object sharing with Multicloud Defense** toggle button.

Enable ASA health monitoring

Enable ASA Health Monitoring to collect and analyze device health data within the dashboard. You must perform this task at the tenant level to ensure comprehensive monitoring of ASA devices managed by the system.

You must enable Device Health Metrics at the tenant level. For ASA devices managed by Secure Device Connector, you must also enable the feature at the individual device level. These steps ensure health data is collected and made available for analysis within the dashboard.

You must have the **Super Admin** user role to enable this feature.

Follow these steps to enable ASA health monitoring for the managed organization:

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn on the **Enable ASA Health Monitoring** toggle button to enable the Device Health Metrics feature for your tenant.

   Device Type Considerations

   - For ASA devices managed by Cloud Device Gateway (CDG), health metrics are enabled when the **Enable Device Health Metrics** toggle in **General Settings** is enabled.
   - For ASA devices managed by Secure Device Connector (SDC), manually enable health metrics for each device:
     a. Choose **Security Devices**.
     b. Select the SDC-managed ASA device.
     c. In the **Device Actions** pane, choose **Opt-in to Health Metrics**.

        If the device is already opted in, you will see the option to **Opt-out of Health Metrics** instead.

> **Note**
>
> Each SDC can support health metrics collection for up to 50 ASA devices.

Set the default conflict detection interval

Configure the default conflict detection interval to determine how often the system polls onboarded devices for configuration changes. This task should be performed whenever you need to adjust the frequency of automated monitoring across your tenant to optimize system performance and visibility.

This interval determines the frequency at which Security Cloud Control polls onboarded devices for changes. The selection applies to all devices managed in this tenant. You can change this option at any time.

> **Note**
>
> This selection can be overridden via the **Conflict Detection** option available from the **Security Devices** page after you have selected one or multiple devices.

Follow these steps to set the default conflict detection interval:

Procedure

1. Choose **Administration** > **General Settings**.
2. From the **Default conflict detection interval** drop-down list, select a time value.

Manage web analytics

You can enable or disable web analytics to share anonymous product usage data with Cisco, helping to improve the platform's features and performance. Adjust your privacy preferences regarding the collection of anonymous usage information by completing this task as needed.

Web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, and device hostname. This data helps Cisco determine feature usage patterns and improve the product. All usage data is anonymous and no sensitive data is transmitted.

Web analytics is enabled by default. To disable web analytics or re-enable it in the future, complete these steps:

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn on the **Web Analytics** toggle button to enable it.

Auto onboard On-Prem FMCs from Cisco Security Cloud

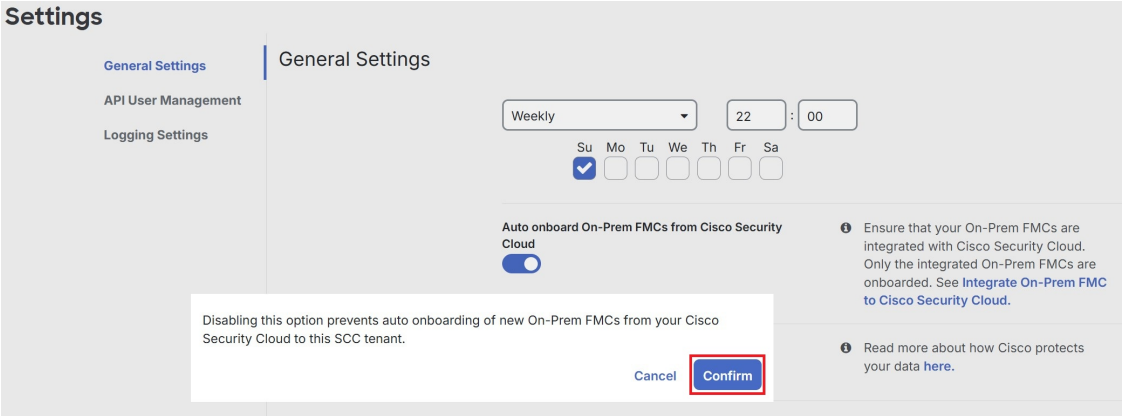
Learn how to disable the auto-onboarding of on-premises Firewall Management Centers from your Cisco Security Cloud to your Security Cloud Control tenant, ensuring only authorized devices are added. This procedure is available to Super Admins and Admins.

Disabling the auto-onboarding functionality stops new on-premises Firewall Management Centers from being automatically added from your Cisco Security Cloud tenant.

> **Note**
>
> Only a Super Admin or Admin can enable or disable this functionality on Security Cloud Control.

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn off the **Auto onboard On-Prem FMCs from Cisco Security Cloud** toggle button to disable the auto-onboarding of on-premises Firewall Management Center.
3. Click **Confirm**.



Enable event data sharing with Talos

Manage Talos event data sharing to contribute to Cisco's threat intelligence and enhance your organization's protection against new security threats. You can opt in or out of anonymous event data sharing at any time depending on your organization's policy.

Share malicious event data from your device with Talos, Cisco's threat intelligence organization. Sharing event data allows Talos to improve threat detection and response capabilities, provide more targeted security updates for your network, and deliver better protection against emerging threats.

For more information about Talos, see the Cisco Talos product page.

> **Note**
>
> The **Enable event data sharing with Talos** setting in Security Cloud Control and the **Talos Threat Hunting Telemetry** option in Cloud-Delivered Firewall Management Center are separate settings. The setting in Security Cloud Control shares malicious event data from your devices with Talos.
>
> To add threat-hunting rules to the global intrusion policy and send events from those rules to Talos, enable **Talos Threat Hunting Telemetry** in Cloud-Delivered Firewall Management Center at **Administration > Configuration > Intrusion Policy Preferences**.

Enabling the **Enable event data sharing with Talos** toggle button does not automatically activate the **Talos Threat Hunting Telemetry** feature in Cloud-Delivered Firewall Management Center. For the best results with this feature, also enable the **Talos Threat Hunting Telemetry** in Cloud-Delivered Firewall Management Center. For more information, see Set Intrusion Policy Preferences.

Sharing event data with Talos is enabled by default. To opt out, follow this procedure:

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn off the **Enable event data sharing with Talos** toggle button to disable this setting.

> **Note**
>
> Sharing event data enables Talos to provide relevant security insights for your network. Disabling this setting might limit your ability to fully leverage Talos's capabilities and could affect your network's defense against evolving threats.

View firewall management instance details

Tenant details are helpful if you need to contact the Cisco Technical Assistance Center (TAC). Examples include tenant ID, enterprise ID, Secure Services Exchange tenant ID, and tenant name.

Firewall Management Instance Details are helpful if you need to contact the Cisco Technical Assistance Center (TAC). You can copy these tenant details by clicking the copy icon.

- **Firewall Management Instance Name**: The display name of the firewall management instance.
- **Firewall Management Instance ID**: The system-generated unique identifier for the firewall management instance in Cisco Security Cloud Control.
- **Secure Services Exchange ID**: The unique identifier for the firewall management instance in the Secure Services Exchange environment. Cisco uses this value for service integration and backend correlation across cloud services.
- **Security Cloud Control Organization ID**: The unique identifier of the Security Cloud Control organization associated with the firewall management instance.

Use the Security Cloud Control Firewall Management platform navigator

The platform navigator is a nine-block launcher that provides users with quick, centralized access to various Cisco networking and security applications. This tool allows users to seamlessly transition between integrated Cisco platforms to manage their infrastructure and security operations.

The platform navigator is a nine-block applications cross-launcher () that appears on the top-right corner of Security Cloud Control. You can readily cross-launch to these Cisco networking and security applications:

Networking applications

- **Catalyst**: Cisco Catalyst products include a wide variety of network switches, wireless controllers, wireless access points, and edge platforms and routers, supporting enterprise-class business needs to heavy-duty and rugged networking environments.
- **Intersight**: Cisco Intersight is a cloud operations platform that consists of optional, modular capabilities of advanced infrastructure, workload optimization, and Kubernetes services. Cisco Intersight infrastructure services include the deployment, monitoring, management, and support of your physical and virtual infrastructure. It supports Cisco Unified Computing System (Cisco UCS), Cisco HyperFlex hyperconverged infrastructure (HCI), and other third-party Intersight-connected targets.
- **IoT Operations Dashboard**: Cisco IoT Operations Dashboard is a cloud-based IoT services platform that empowers operations teams to securely connect, maintain, and gain insights from industrial networking devices and connected industrial assets at massive scale. With one comprehensive view of all their connected industrial assets, operations teams can uncover valuable insights that help them streamline operations and drive business continuity.
- **Meraki**: Cisco Meraki is an IT and IoT cloud-managed platform that provides a centralized management platform for Cisco Meraki devices.
- **Spaces**: Cisco Spaces is a cloud-based location services platform through which organizations can gain insights into how people and things move throughout their physical spaces. With these insights, they can deliver contextual engagements that are valuable and relevant. Besides looking at where people go, organizations can also drive operational efficiencies by monitoring the location, movement, and utilization of assets.
- **ThousandEyes**: Cisco ThousandEyes is a cloud service suite that helps monitor and measure the availability and performance of web applications, services, and networks. It provides end-to-end visibility from any user to any application over any network, enabling enterprises to swiftly get to the source of issues, resolve them faster, and manage performance effectively.
- **Workflows**: Cisco Workflows is a cloud-hosted automation application that is part of the larger Cisco Networking Cloud vision. It provides an entitlement to cross-domain automation capabilities for Cisco customers. It streamlines repetitive and error-prone tasks across both Cisco and third-party applications using custom and premade automation templates, as well as various adapter options that can be provided by Cisco or built independently, reaching targets in the cloud or on-premises.

Security applications

- **Duo Security**: Cisco Duo is a user-centric zero-trust security platform with two-factor authentication to protect access to sensitive data for all users, devices, and applications. It offers features such as adaptive policies, single sign-on (SSO), and advanced endpoint visibility, making it a comprehensive solution for securing remote access and maintaining business continuity.
- **Secure Access**: Cisco Secure Access simplifies IT operations through a single, cloud-managed console, unified client, centralized policy creation, and aggregated reporting. Extensive security capabilities converged in one solution (ZTNA, SWG, CASB, FWaaS, DNS security, RBI, and more) mitigate security risk by applying zero trust principles and enforcing granular security policies. Market leading Talos threat intelligence fuels unmatched threat blocking to mitigate risk and speed investigations.

- **Secure Endpoint**: Cisco Secure Endpoint, formerly known as Cisco AMP for Endpoints, is a cloud-managed endpoint security solution designed to prevent breaches and rapidly detect, contain, and remediate threats. It instantly checks your files against a cloud-based scanner with advanced tracking features. These features enable security analysts to identify and isolate initial outbreak sources. The solution also provides retrospective quarantine for files found to be malicious.
- **Cisco Security Provisioning and Administration**: Cisco Security Provisioning and Administration is a web application that provides centralized management of Cisco Secure product instances, user identity, and user access management across Cisco Security Cloud. Security Cloud Control administrators can create new Security Cloud enterprises, manage users in an enterprise, claim domains, and integrate their organization's SSO identity provider, among other tasks.
- **XDR**: Cisco Extended Detection and Response (XDR) is a cloud-based solution designed to simplify security operations and empower security teams to detect, prioritize, and respond to sophisticated threats. By integrating both Cisco and third-party security solutions into a unified platform, Cisco XDR offers a comprehensive approach to threat management. Integrated with the threat intelligence provided by Talos, Cisco XDR enriches incident data with additional context and asset insights, reducing false positives and enhancing overall threat detection, response, and forensic capabilities.

Manage users and groups within Security Cloud Control organization

Learn how to manage organization users and groups through centralized access management in Security Cloud Control.

The purpose of this task is to provide centralized and automated management of user access across Cisco security products through role-based access control (RBAC).

Security Cloud Control supports role-based access control (RBAC) to automate access management across the organization. A role defines the level of user access to functions within a product. With Security Cloud Control, you can centralize the management of user roles within an organization, allowing organization users to switch seamlessly between products without the need to log in repeatedly.

Additionally, you can create API-only users for Security Cloud Control Firewall Management. API-only users allow systems to interact with Security Cloud Control using APIs, eliminating the need for a user interface.

Procedure

1. From the Security Cloud Control Home page, click **Platform Management**.
2. Choose **Platform Management** > **Access Management** > **Administrator Access**

   For more information, see Managing users in the Security Cloud Control platform services documentation.

Manage API-Only users for Security Cloud Control Firewall Management

Learn how to create API-only users and generate API tokens for programmatic access to Security Cloud Control Firewall Management.

Developers use Security Cloud Control Firewall Management API tokens when making Security Cloud Control Firewall Management REST API calls. The API token must be included in the REST API authorization header for a successful call. API-only users can generate API tokens. Regular users cannot create API tokens for themselves or others.

The purpose of creating an API-only user in Security Cloud Control Firewall Management is to enable secure, programmatic access to the system using API tokens.

An API-only user role allows a user to interact with Security Cloud Control Firewall Management using APIs, eliminating the need for a user interface. API-only users cannot log in to the Security Cloud Control interface directly. The role benefits organizations -only user role is useful in organizations that need automated processes and integrations.

Only API-only users can generate API tokens; regular users cannot create API tokens for themselves or others.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, choose **Administration** > **API User Management**.
3. Click the **Add a new user** () icon to add a new user to your tenant.
4. In the **Username** field, enter a name for the API-only user.
5. From the **Role** drop-down list, choose a role for the API-only user and click **Add**.
6. In the **Token** column for the new API Only user, click **Generate API Token** to obtain an API token. Save the token in a secure location in accordance with your enterprise's best practices for maintaining sensitive data.

> **Note**
>
> Click edit to change the role of the existing API-only user.

View Security Cloud Control notifications

Learn how to view, search, dismiss, and review Security Cloud Control notifications for device events, alerts, and reports.

Click the notifications icon  to view the most recent alerts that have occurred or affected the devices that you onboarded to your tenant. The settings that you choose on the Notification Settings page determine the notification types that appear in Security Cloud Control Firewall Management.

This drop-down page is grouped into three tabs: Overview, All, and Dismissed.

Overview tab

The **Overview** tab displays a combination of the most recent high-priority alerts and events to which you are subscribed. High priority events are the following:

- Deployment Failed
- Backup Failed
- Upgrade Failed
- Migrate FTD to Cloud-Delivered Firewall Management Center Failed
- Device went offline
- Device HA state changed
- Device certificates expiring

You can configure which alerts you want to receive by clicking the Notification Settings in the Notifications window or by selecting **UserID** > **User Preferences** page. The User ID button in the upper right corner of the dashboard.

All tab

Displays all notifications, regardless of priority, including email subscription notifications and all high-priority items.

Dismissed tab

Displays notifications that you dismissed. You can dismiss individual notifications by clicking the "**x**" of the notification.

Opting to **Dismiss** notifications from the drop-down menu dismisses notifications from **both** the "Overview" and "All" tabs. They will remain in the **Dismiss** tab for 30 days, after which they will be removed from Security Cloud Control.

Search notifications

When viewing the notifications drop-down window, for any of the tabs mentioned above, you can use the search bar at the top of the drop-down to query for key words or alerts.

Manage user notification preferences

Security Cloud Control Firewall Management generates notifications whenever a device linked to your tenant encounters a specific event. This includes actions taken by the device, expiring or expired device certificates, or the start, completion, or failure of a report generation task. By default, these notifications are enabled and visible to all users associated with the tenant, regardless of their role. You have the option to customize your personal notification preferences to display only the alerts that interest you. These preferences are unique to you and do not impact other users connected to the tenant.

> **Note**
>
> Changes made to the notifications listed below are automatically updated in real time and do not require deployment.

View your personal preferences in the **Username ID** > **Preferences** > **Notification Preferences** page. Your Username ID is always located in the upper right corner of Security Cloud Control across all pages. From this page you can configure the following "**Notify Me in Security Cloud Control When**" alerts.

Device workflow alerts

- **Deployments** - This action does not include integration instances for SSH or IOS devices.
- **Backups** - This action is only applicable for FDM-managed devices.
- **Upgrades** - This action is only applicable for ASA and FDM-managed devices.
- **Migrate Firewall Threat Defense to cloud** - This action is applicable when changing the Firewall Threat Defense device manager from Firewall Management Center to Security Cloud Control.

Device event alerts

- **Went offline** - Applies to all devices associated with your tenant.
- **Back online** - Applies to all the devices associated with your tenant.
- **Conflict detected** - Applies to all the devices associated with your tenant.
- **HA state changed** - Indicates the device within an HA or failover pair, the current state, and the state it changed from. This action applies to all HA and failover configurations associated with your tenant.

- **Site-to-Site session disconnected** - Applies to all site-to-site VPN configurations configured in your tenant.

Event search report alerts

- **Report generation started**: Notifies you when a report generation task starts. This applies to both immediate and scheduled search reports.
- **Report generation completed**: Notifies you when a report generation task ends. This applies to both immediate and scheduled search reports.
- **Report generation failed**: Notifies you when a report generation task fails. This applies to both immediate and scheduled search reports. Check the parameters or query and try again.

Application insights alerts

- **Application available**: Notifies you when a monitored application becomes available.
- **Application unavailable**: Notifies you when a monitored application becomes unavailable.

Opt out of notifications

By default, all notification types are enabled. To stop receiving a notification type, clear that notification and click **Save**.

Manage email notifications

Enable the `Email notifications` toggle button to receive email for the alerts that you select.

By default, **Use Security Cloud Control notification settings above** is selected. When this option is selected, email notifications match the same notifications and events that you selected in the **Notify Me in Security Cloud Control When** sections.

If you want email notifications for only some alerts, clear **Use Security Cloud Control notification settings above**, select the alert types that you want to receive by email, and then click **Save**.

View logging settings

Learn how to review tenant logging usage, monthly limits, reset timing, historical usage, and storage options.

Use **Logging Settings** to check current logging usage for your tenant.

The page shows:

- Your monthly event logging limit.
- The number of days until the limit resets.
- Stored logging usage, which represents the compressed event data that the Cisco cloud received.

Click **View Historical Usage** to review the logs that your tenant received during the last 12 months.

The page also includes links that you can use to request additional storage.

Understand user roles in Security Cloud Control Firewall Management

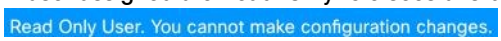
Learn how user roles define permissions for each Security Cloud Control Firewall Management organization.

Security Cloud Control Firewall Management assigns roles per user and per organization. If a user has access to more than one tenant, that user can have the same user ID but different roles on different organizations. For example, a user can have the `Read-Only` role on one organization and the `Super Admin` role on another.

When the interface or documentation refers to a `Read-Only` user, `Admin` user, or `Super Admin` user, it describes that user's permission level on a specific organization.

Read-only role

A user assigned the Read-Only role sees this blue banner on every page:



Users with the `Read-Only` role can:

- View any page or any setting in Security Cloud Control.
- View all device configuration details including sensitive values in device configurations, such as certificates, PSKs, and credentials.

  Note

  Note: For ASA devices, we recommend enabling password encryption as a best practice. Password encryption helps prevent PSKs and credentials from being visible in clear text in the configuration.

- Compare device configurations, view the change log, and see VPN mappings.
- Search and filter the contents of any page.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. Note that if a read-only user revokes their own token, they cannot recreate it.
- Contact support through our interface and can export a change log.

Users with the `Read-Only` role cannot:

- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

Edit-Only role

Users with the Edit-Only role can:

- Edit and save device configurations, including but not limited to objects, policies, rulesets, interfaces, VPN, etc.
- Allow configuration changes that are made through the **Read Configuration** action.
- Utilize the Change Request Management action.

Users with the Edit-Only role cannot:

- Deploy changes to a device or to multiple devices.
- Discard staged changes or changes that are detected through OOB.
- Upload AnyConnect Packages, or configure these settings.
- Schedule or manually start image upgrades for devices.
- Schedule or manually start a security database upgrade.
- Manually switch between Snort 2 and Snort 3 versions.
- Create a template.
- Change the existing OOB Change settings.
- Edit System Management settings.
- Onboard devices.
- Delete devices.
- Delete VPN sessions or user sessions.
- Create Security Cloud Control user records.
- Change user role.

Deploy-Only role

Users with the Deploy-Only role can:

- Deploy staged changes to a device, or to multiple devices.
- Revert or restore configuration changes for ASA devices.
- Schedule or manually start image upgrades for devices.
- Schedule or manually start a security database upgrade.
- Utilize the Change Request Management action.

Users with the `Deploy-Only` role cannot:

- Manually switch between Snort 2 and Snort 3 versions.
- Create a template.
- Change the existing OOB Change settings.
- Edit System Management settings.
- Onboard devices.
- Delete devices.
- Delete VPN sessions or user sessions.
- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.

- Attach or detach access rules to a policy.

VPN Sessions Manager role

The `VPN Sessions Manager` role is intended for administrators who monitor remote access VPN connections, not site-to-site VPN connections.

Users with the VPN Sessions Manager role can:

- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see RA VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. Note that if a VPN Sessions Manager user revokes their own token, they cannot recreate it.
- Contact support through our interface and export a change log.
- Terminate existing RA VPN sessions.

Users with the VPN Sessions Manager role cannot:

- Create, update, configure, or delete anything on any page.
- Onboard devices.
- Step-through the tasks needed to create something like an object or a policy, but not be able to save it.
- Create Security Cloud Control user records.
- Change user role.
- Attach or detach access rules to a policy.

Admin role

Users with the `Admin` role have complete access to most areas of Security Cloud Control Firewall Management.

- Create, read, update, and delete any object or policy in Security Cloud Control Firewall Management and configure any setting.
- Onboard devices.
- View any page or any setting in Security Cloud Control.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. If their token is revoked, they can contact support through our interface and can export a change log.

Admin users **cannot** do the following:

- Create Security Cloud Control user records.
- Change user role.

Super Admin role

Users with the Super Admin role have complete access to all areas of Security Cloud Control Firewall Management.

Users with the Super Admin role can:

- Change user roles.
- Create user records.
- Create, read, update, and delete any object or policy in Security Cloud Control Firewall Management and configure any setting.
- Onboard devices.
- View any page or any setting in Security Cloud Control Firewall Management.
- Search and filter the contents of any page.
- Compare device configurations, view the change log, and see VPN mappings.
- View every warning regarding any setting or object on any page.
- Generate, refresh, and revoke their own API tokens. If their token is revoked, they can
- Contact support through our interface and can export a change log.

Filters on security devices, policies, and objects page

Learn how to filter devices, policies, and objects by attributes such as device type, status, version, connector, management application, and labels.

Use filters on the **Security Devices**, **Policies**, and **Objects** pages to find devices and objects. To filter, select the filter icon in the left pane.

On the **Security Devices** page, the filter panel lets you filter devices by criteria such as device type, hardware version, software version, Snort version, configuration status, connection state, conflict detection, Secure Device Connector, and labels. You can apply filters within the selected device type tab.

When the **FTD** tab is open, the filter panel also lets you filter FTD devices by the management application that Security Cloud Control uses to access them.

To filter, click  in the left-hand pane of the Security Devices, Policies, and Objects tabs.

> **Note**
>
> When the **FTD** tab is opened, the filter pane provides filters to show FDM-managed devices based on the management application through which the devices are accessed from Security Cloud Control.
>
> - FDM: Devices managed using FTD API or Firewall Device Manager.
> - FMC-FTD: Devices managed using Firepower Management Center.
> - FTD: Devices managed using FTD Management.

4 Firewall models and software supported

Topics:

- Manage security devices
- Supported devices, software, and hardware for Security Cloud Control Firewall Management

Manage security devices

Learn how to manage security devices in Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management provides the ability to view, manage, filter, and evaluate your onboarded devices on the **Security Devices** page.

From the **Security Devices** page you can:

- Onboard devices and services for Security Cloud Control management.
- View the configuration state and connectivity state of managed devices and services.
- View onboarded devices and templates categorized in separate tabs. See Security devices overview on page 92.
- Evaluate and take action on individual devices and services.
- View device and service specific information and resolve issues.
- View device health status for threat defense devices managed by:
  - Cloud-Delivered Firewall Management Center
  - on-premises Firewall Management Center

  For Firewall Threat Defense devices managed by the Cloud-Delivered Firewall Management Center, you can also see the node status for devices in a cluster.
- Search for a device or template by name, type, IP address, model name, serial number, or labels. Search is not case-sensitive. Providing multiple search terms brings up devices and services that match at least one of the terms. See Page Level Search on page 94.
- Filter for a device or template filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. See Filters.
- Delete a device

Supported devices, software, and hardware for Security Cloud Control Firewall Management

An overview of devices supported by Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management is a cloud-based management solution enabling the management of security policies and device configurations across multiple security platforms.

This section describes the supported device types, software, hardware, and constraints for managing firewall, cloud, SD-WAN, Cisco IOS, Cisco Umbrella, and management center integrations in Security Cloud Control Firewall Management.

Support scope

Security Cloud Control Firewall Management is a cloud-based management solution for security policies and device configurations across multiple security platforms. The source identifies support for these management areas:

- Cisco Secure Firewall ASA, both on-premises and virtual
- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Catalyst SD-WAN Manager
- Cisco Secure Firewall Management Center, on-premises

- Cisco Meraki MX
- Cisco IOS devices
- Cisco Umbrella
- AWS Security Groups

Security Cloud Control Firewall Management documentation identifies the devices, software, and hardware that Security Cloud Control Firewall Management supports. If the documentation does not explicitly claim support for a software version or device type, Security Cloud Control Firewall Management does not support it.

Cisco Secure Firewall ASA

Cisco Adaptive Security Appliance (ASA) is a security device that integrates firewall, VPN, and intrusion prevention capabilities. Security Cloud Control supports ASA device management to streamline configuration management and support regulatory compliance across the network infrastructure.

Cisco Secure Firewall Threat Defense

Cisco Secure Firewall Threat Defense integrates traditional firewall features with advanced threat protection capabilities. It includes security functions such as intrusion prevention, application control, URL filtering, and advanced malware protection.

A Secure Firewall Threat Defense device can be deployed on ASA hardware appliances, Cisco firewall hardware appliances, and virtual environments. You can manage threat defense devices through management interfaces such as Cisco Firewall Management Center, Security Cloud Control, and Firewall Device Manager.

Firewall Threat Defense integrates traditional firewall features with advanced threat protection capabilities. It offers comprehensive security functions, including intrusion prevention, application control, URL filtering, advanced malware protection, and so on. An FTD can be deployed on ASA hardware appliances, and Cisco firewall hardware appliances, and in virtual environments. Managing threat defense devices is possible through various management interfaces, such as Cisco Firewall Management Center, Security Cloud Control Firewall Management, and Firewall Device Manager.

For more information on software and hardware compatibility, see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Firewall Device Manager is a web-based management interface explicitly designed for threat defense device management. It provides a simplified approach for configuring and monitoring threat defense devices, making it ideal for smaller-scale deployments or organizations preferring an intuitive interface.

FDM offers basic configuration capabilities for network settings, access control policies, NAT rules, VPN configuration, monitoring, and basic troubleshooting. Typically accessed through a web browser, FDM is directly available on the FTD device, eliminating the need for additional management servers or appliances.

Cisco Catalyst SD-WAN Manager

Security Cloud Control offers centralized management for Catalyst SD-WAN and Branch WAN environments, allowing organizations to efficiently configure, monitor, and enforce security policies across their networks. This integration also facilitates advanced troubleshooting, rule optimization, and change management on the Catalyst SD-WAN Manager.

For more information on software and hardware compatibility, see Cisco Catalyst SD-WAN Device Compatibility.

Cisco Secure Firewall Management Center

Security Cloud Control Firewall Management simplifies the management of on-premises Firewall Management Center by establishing a secure integration, discovering security devices, and enabling centralized policy management. Security policies such as firewall rules, VPN settings, and intrusion prevention policies can be efficiently managed and deployed across all devices under FMC.

Cisco Meraki MX

The Cisco Meraki MX appliance is an enterprise-grade security and SD-WAN next-generation firewall appliance for decentralized deployments. Security Cloud Control Firewall Management supports management of layer 3 network rules on Meraki MX devices.

When you onboard a Meraki device to Security Cloud Control Firewall Management, Security Cloud Control Firewall Management communicates with the Meraki dashboard to manage that device. Security Cloud Control Firewall Management transfers configuration requests to the Meraki dashboard, and the Meraki dashboard applies the new configuration to the device.

Security Cloud Control Firewall Management support for Cisco Meraki MX includes centralized policy management, backup and restore, monitoring and reporting, compliance checking, and automation capabilities.

Cisco IOS devices

Cisco IOS software manages network functions such as routing, switching, and other networking protocols. Cisco IOS includes features and commands to configure and maintain Cisco network devices.

Cisco Umbrella

Security Cloud Control Firewall Management manages Cisco Umbrella through integrations such as the Umbrella ASA Integration. This integration lets administrators include Cisco Adaptive Security Appliance (ASA) devices in their Umbrella configuration by using per-interface policies.

The integration enables ASA devices to redirect DNS queries to Umbrella and use Umbrella DNS security, web filtering, and threat intelligence capabilities.

AWS Security Groups

Security Cloud Control Firewall Management provides a simplified management interface for Amazon Web Services (AWS) Virtual Private Clouds (VPCs). Source-backed capabilities include monitoring AWS Site-to-Site VPN connections, tracking changes to AWS devices, and viewing AWS Site-to-Site VPN tunnels.

5 Deploy and manage Secure Connectors for device onboarding

Topics:

- Introduction to Secure Connectors

Introduction to Secure Connectors

Learn how secure connectors support communication between Security Cloud Control Firewall Management and managed resources in your network or cloud environment.

A secure connector is a connector instance that runs in your network or supported cloud environment and provides a secure communication path between Security Cloud Control Firewall Management and managed resources. Secure connectors help Security Cloud Control Firewall Management manage devices that are not directly reachable from the internet and support event forwarding for logging and analytics workflows.

Use the **Secure Connectors** page to view, deploy, and manage connector instances for your tenant.

Secure connector types

The **Secure Connectors** page can include these connector types.

- Secure Device Connector (SDC): Provides a secure communication path between Security Cloud Control Firewall Management and supported managed devices.
- Secure Event Connectors (SEC): Receives events from supported devices and forwards the events to the Cisco cloud for logging and analytics.

About Secure Device Connector

A Secure Device Connector (SDC) is an intelligent proxy that lets Cisco devices communicate with Security Cloud Control Firewall Management when the devices are not directly reachable from the internet. When you onboard a device by using device credentials, you can deploy an SDC in your network to proxy communication between the device and Security Cloud Control Firewall Management.If the device is directly reachable from the internet, you can allow direct communication through the device's outside interface instead of using an SDC. The SDC performs these functions:

- Monitors Security Cloud Control Firewall Management for commands and messages for your managed devices.
- Executes commands on behalf of Security Cloud Control Firewall Management.
- Relays messages to your managed devices.
- Returns device responses.

Communication between the SDC and Security Cloud Control Firewall Management uses HTTPS with TLS 1.3 and AES-128-GCM. Credentials for onboarded devices and services are encrypted from the browser to the SDC and are encrypted at rest by using AES-128-GCM. Only the SDC has access to those credentials.

A user with the Super Administrator role is required to create a Secure Device Connector or a Secure Event Connector (SEC).

You can onboard these devices to Secure Device Connector through an SDC:

- On-Premises Firewall Management Center using credentials method
- Meraki MX devices
- Generic SSH devices
- Cisco IOS devices

Secure Firewall Threat Defense devices that are managed by Cloud-Delivered Firewall Management Center do not require an SDC and do not support onboarding through proxies. Ensure that these devices have proper DNS settings and outbound internet connectivity so they can connect to Cloud-Delivered Firewall Management Center.

See Allow inbound access for direct cloud connectivity on page 44 for information explaining how to allow communication between an SDC and Security Cloud Control.

For more information, refer to Deploy a VM for Running the Secure Device Connector and Secure Event Connector on page 45.

Plan device connectivity

Security Cloud Control Firewall Management connects to managed devices either through the cloud connector or through an SDC.

Table 1:

Connection method	Use when	Required network access
Direct cloud connector	The device is directly reachable from the internet.	Allow inbound access from the Security Cloud Control Firewall Management IP addresses for your cloud region on port 443, or on the port that you use for device management.
SDC	The device is not directly reachable from the internet, or the source explicitly requires an on-premises SDC.	Allow full inbound access from the SDC host on port 443, or on the port that you use for device management. Ensure that the SDC VM can reach the device management interface.

An FDM-managed device can be onboarded to Security Cloud Control Firewall Management by using device credentials, a registration key, or its serial number whether it is directly accessible from the internet. If the device does not have direct internet access, but it resides on a network that does, the Security Services Exchange connector that is delivered as part of the device can reach the Security Services Exchange cloud and allow the FDM-managed device to be onboarded.

The source explicitly states that you need an on-premises SDC to onboard the following:

- An ASA device that is not accessible from the cloud
- An FDM-managed device that is not accessible from the cloud when you use the credentials onboarding method
- A Cisco IOS device
- A device with SSH access

All other devices and services do not require an on-premises SDC because Security Cloud Control Firewall Management connects by using its cloud connector.

Docker network considerations for the SDC

SDC runs as a Docker container. Docker commonly uses the `172.17.0.0/16` subnet for the default bridge network, docker0.

If `172.17.0.0/16`, or any part of the Docker-assigned network space, overlaps with your existing network IP space, change the Docker network defaults before deploying the SDC. To use alternate networks, edit /etc/docker/daemon.json configuration.

For example, Use the supernet `10.198.0.1/24` for Docker networking address pools and use IP address `10.198.128.0/17` as the default docker bridge interface, docker0, from the subnet `10.198.0.0/24`.

```
sudo vi /etc/docker/daemon.json

{
  "log-driver": "json-file",
  "log-opts": {
```

```
    "max-size": "100m",
    "max-file": "5"
  },
    "bip": "10.198.0.1/24",
    "default-address-pools": [
        {
            "base": "10.198.128.0/17",
            "size": 24
        }
    ]
}

(save and exit)

sudo reboot (required)
```

For more information, see Networking overview.

Allow inbound access for direct cloud connectivity

Security Cloud Control connects to the devices that it manages through the cloud connector or through an (SDC).

When you connect Security Cloud Control Firewall Management directly to a device through the cloud connector, allow inbound access on port 443, or on the port that you have configured for device management, from the IP addresses for your region.

Table 2:

Region	URL	Allow inbound access from
Asia-Pacific-Japan (APJ)	https://security.cisco.com	54.199.195.111, 52.199.243.0
Australia (AUS)	https://security.cisco.com	13.55.73.159, 13.238.226.118
Europe, Middle East, and Africa (EMEA)	https://security.cisco.com	35.157.12.126, 35.157.12.15
India (IN)	https://security.cisco.com	35.154.115.175 13.201.213.99
United States (US)	https://security.cisco.com	52.34.234.2 52.36.70.147

Plan SDC capacity and host requirements

Each Security Cloud Control Firewall Management organization can have an unlimited number of SDCs. An SDC belongs to one organization only and is not shared across organizations.For deployment planning, one SDC is expected to support approximately 500 devices. Actual capacity depends on the features enabled on those devices and the size of their configuration files.

Deploying more than one SDC lets you:

- Scale device management without performance degradation.

- Place SDCs in isolated network segments while keeping the devices in the same Security Cloud Control Firewall Management organization.
- Run multiple SDCs on one host by following the bootstrap procedure for each additional SDC.

The first SDC name includes the tenant name and the number 1. Each additional SDC is numbered in sequence.

Deploy a VM for Running the Secure Device Connector and Secure Event Connector

When using device credentials to connect Security Cloud Control to a device, it is a best practice to download and deploy an SDC in your network to manage the communication between Security Cloud Control and the device. Typically, these devices are nonperimeter based and do not have a public IP address, or have an open port to the outside interface.

The SDC monitors Security Cloud Control for commands that need to be executed on your managed devices, and messages that need to be sent to your managed devices. The SDC executes the commands on behalf of Security Cloud Control, sends messages to Security Cloud Control on behalf of the managed devices, and returns replies from the managed devices to Security Cloud Control.

The number of devices a single SDC can manage depends on the features that are implemented on those devices and the size of their configuration files. To plan your deployment, however, we expect one SDC to support approximately 500 devices. For more information, see Using Multiple SDCs on a Single Security Cloud Control Tenant.

This procedure describes how to install an SDC in your network, using Security Cloud Control's VM image. This is the recommended and most reliable way to create an SDC.

Before you begin

- Security Cloud Control requires strict certificate checking and does not support Web or Content Proxy inspection between the Secure Device Connector (SDC) and the internet. If using a proxy server, disable inspection for traffic between the SDC and Security Cloud Control.
- The SDC must have full outbound access to the internet on TCP port 443, or the port you have configured for device management.
- The devices that are managed by Security Cloud Control must allow inbound traffic from the SDC VM's IP address.
- Review Connect Allow inbound access for direct cloud connectivity on page 44 to the Secure Device Connector to ensure proper network access.
- If you are using a proxy on your network, ensure that you have all the required details before running the host setup command. Most of the issues are related to incorrect proxy configurations. Important details are:
  - The IP/hostname of your proxy.
  - Whether or not your proxy intercepts traffic and reencrypts it using its own cert. This detail is the cause of most of the complications with the SDC VM setup.
    - If your proxy does intercept traffic, have the root certificate ready when configuring the VM. You can paste it in when prompted so that the host and the SDC know to trust the certificates generated by your proxy.
    - If your proxy does not intercept traffic, then nothing else is required here.
  - The following items are most likely the same for proxied HTTP and HTTPS connections. However, if you use a different proxy for each protocol, you would need all of the following for each:
    - The IP address of your proxy
    - The port your proxy uses
    - Whether your proxy requires that the connection to the proxy itself be over HTTPS (typically not the case). For example, if the address of your proxy is listed as https://proxy.corp.com:80 then you would answer yes. If the listed address is http://proxy.corp.com:80 then you would answer no. Note that both URLs use port 80, but the protocol is different.

- The authentication details of your proxy including:
  - Whether your proxy requires auth (most do not)
  - If yes, then you'll need the username and password available when you configure the host.

Supported Installations

- Security Cloud Control supports installing its SDC VM OVF image using the vSphere web client or the ESXi web client.
- Security Cloud Control does not support installing the SDC VM OVF image using the vSphere desktop client.
- Security Cloud Control supports installing the SDC on your own Ubuntu instance. Versions 20LTS – 24LTS are currently supported.
- ESXi 5.1 hypervisor.

System Requirements

- System requirements for a VM with one SDC:
  - 2 vCPUs
  - 2 GB of memory
  - 64 GB of disk space
- Each SDC you add to your host requires an additional 1 vCPU and 1 GB of RAM.
- System requirements for a VM with one SEC (a component that is used in Cisco Security Analytics and Logging):
  - 4 vCPUs minimum
  - 8 GB of memory
- Each SEC you add to the host requires doubling its resources, therefore, these are the requirements for a VMware ESXi host with one SDC and one SEC:
  - 6 vCPUs
  - 10 GB memory
  - 64 GB of disk space

Prepare for Installation

- To configure networking manually on the host, gather the following information:
  - The static IP address that you want to use for your VM
  - The passwords to use for the `cdo`user (or whichever user has sudo access) and the sdc user (the user under which Docker runs)
  - The IP address of the DNS server your organization uses
  - The gateway IP address of the network the SDC address is on
  - The FQDN or IP address of your time/NTP server
- The SDC virtual machine is configured to install security patches regularly and to do this, opening port 80 outbound is required.

If your network is using allow/deny lists for outbound connections, you need to allow connections to ubuntu.com so those security updates can be applied.

> **Note**
>
> Ubuntu secures its updates with checksums and only uses HTTP, not HTTPS. To pull security updates, you must allow HTTP connections to ubuntu.com.

Deploy the VM

There are two options for deploying the VM used to run the SDC and SEC.

1. Follow the steps below to download the VMware image provided by Security Cloud Control.
2. To deploy Ubuntu 20, 22, or 24 yourself. If deploying your own Ubuntu instance, you may skip the following section and proceed to the Configure the VM section.

Procedure

1. In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.
2. Select the **Secure Connectors** tab on the **Services** page, click the blue plus button, and select **Secure Device Connector**.
3. Click **Download the SDC VM** image. This opens in a new tab.
4. Extract all the files from the .zip file. They look similar to these:
   - CDO-SDC-VM-ddd50fa.ovf
   - CDO-SDC-VM-ddd50fa.mf
   - CDO-SDC-VM-ddd50fa-disk1.vmdk
5. Log in to your VMware server as an administrator using the vSphere Web Client.

   > **Note**
   >
   > Do not use the ESXi Web Client.

   Deploy the Secure Device Connector virtual machine from the OVF template by following the prompts.
6. When the setup is complete, power on the SDC VM.
7. Open the console for your new SDC VM.
8. Log in with the `cdo` username. The default password is `adm123`.

Configure the VM

Now you are able to bring up the console for the VM image you deployed (or SSH into it if you rolled your own and enabled SSH), you should run the configuration script to get your host ready to run the SDC or SEC Docker container(s).

1. If you downloaded the Security Cloud Control-provided VM, the CLI is already installed, and you can proceed to step 2. If you have deployed your own VM, SSH into it and run the command to install the CLI:

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
 && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh &&
./install.sh
```

2. Start the host configuration by running the command:

```
sudo sdc host configure
```

3. When prompted for the password, enter adm123 for the Security Cloud Control-provided VM or whatever admin password you chose for your own VM.
4. Follow the prompts to configure the `sdc` user.
5. When prompted for the networking configuration, choose one of the following:
   - Manually configure this host with a static IP: If you want to specify the IP, gateway, DNS server, and so on, for this host and write it to the system config on the VM.
   - DHCP: If you have a DHCP server assigning static IPs to your VMs.
   - Static IP is already configured and I don't want to change my networking now.
6. When prompted, answer the questions about your proxy configuration. Review the detailed list at the top of this topic for all the prerequisites and potential proxy configuration options.
7. If you have configured a proxy, you will be prompted to reboot the VM for all the proxy settings to take effect. If you did not, you will not be prompted to reboot and you can move on to step 8.
8. Set a custom internet access test URL. You only need to do this if you deny all outbound connections by default. If you do, then specify a publicly accessible web url such at https://google.com that is on your allow list.
9. Install the latest security patches, some requires os tools and Docker server.
10. When prompted, indicate whether you want to have the script harden your SSH configuration.

    If using our VM, proceed. If you are using your own VM and configuring SSH yourself, you may want to skip this step to avoid changing your current configuration.
11. When prompted to enable automatic updates for the SDC or SEC and the CLI itself, it is recommended that you do this to stay up to date with bug fixes, patches, and new features. If your policies prevent you from allowing automatic updates, see Update your Secure Device Connector.

Deploy a Secure Device Connector On Your VM

When using device credentials to connect Security Cloud Control to a device, it is a best practice to download and deploy a Secure Device Connector (SDC) in your network to manage the communication between Security Cloud Control and the device. Typically, these devices are non-perimeter based, do not have a public IP address, or have an open port to the outside interface. Adaptive Security Appliances (ASAs), FDM-managed devices, and Firepower Management Centers (FMCs) devices can all be onboarded to Security Cloud Control using device credentials.

The SDC monitors Security Cloud Control for commands that need to be executed on your managed devices, and messages that need to be sent to your managed devices. The SDC executes the commands on behalf of Security Cloud Control, sends messages to Security Cloud Control on behalf of the managed devices, and returns replies from the managed devices to Security Cloud Control.

The number of devices a single SDC can manage depends on the features implemented on those devices and the size of their configuration files. For the purposes of planning your deployment, however, we expect one SDC to support approximately 500 devices. See Use multiple Secure Device Connectors on one tenant on page 62 for more information.

This procedure describes how to install an SDC in your network by using your own virtual machine image.

> **Note**
>
> The preferred, easiest, and most reliable way to install an SDC is to download Security Cloud Control's SDC OVA image and install it.

Before you begin

- Security Cloud Control requires strict certificate checking and does not support a Web/Content Proxy between the SDC and the Internet.
- The SDC must have full outbound access to the Internecdot on TCP port 443 in order for it to communicate with Security Cloud Control.
- Devices that reach Security Cloud Control through the SDC must allow inbound access from the SDC on port 443.
- Review Connect to Security Cloud Control using Secure Device Connector for networking guidelines.
- VMware ESXi host installed with vCenter web client or ESXi web client.

  > **Note**
  >
  > We do not support installation using the vSphere desktop client.

- ESXi 5.1 hypervisor.
- Ubuntu 22.04 and Ubuntu 24.04 operating system.
- System requirements for a VM with only an SDC:
  - VMware ESXi host needs 2 CPUs.
  - VMware ESXi host needs a minimum of 2 GB of memory.
  - VMware ESXi requires 64 GB disk space to support the virtual machine depending on your provisioning choice. This value assumes you are using Logical Volume Management (LVM) with the partition so you can expand required disk space as needed.
- After you have updated the CPU and memory on the VM, power on the VM and ensure that the Secure Connectors page indicates that the SDC is in the "Active" state.
- Users performing this procedure should be comfortable working in a Linux environment and using the vi visual editor for editing files.
- If you are installing your on-premise SDC on a CentOS virtual machine, we recommend you install Yum security patches on a regular basis. Depending on your Yum configuration, to acquire Yum updates, you may need to open outbound access on port 80 as well as 443. You will also need to configure yum-cron or crontab to schedule the updates. Work with your security-operations team to determine if any security policies need to change to allow you to get the Yum updates.

> **Note**
>
> **Before you get started**: Do not copy and paste the commands in the procedure into your terminal window, type them instead. Some commands include an "n-dash" and in the cut and paste process, these commands can be applied as an "m-dash" and that may cause the command to fail.

Procedure

1. Log on to the Security Cloud Control tenant you are creating the SDC for.
2. In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.
3. On the **Services** page, select the **Secure Connectors** tab, click the blue plus button, and select **Secure Device Connector**.
4. Copy the bootstrap data in step 2 on the window to a notepad.
5. Install a **CentOS 7 virtual machine** with at least the following RAM and disk space allotted to the SDC:
   - 8GB of RAM
   - 10GB disk space
6. Once installed, configure basic networking such as specifying the IP address for the SDC, the subnet mask, and gateway.
7. Configure a DNS (Domain Name Server) server.
8. Configure a NTP (Network Time Protocol) server.
9. Install an SSH server on CentOS for easy interaction with SDC's CLI.
10. Run a Yum update and then install the packages: **open-vm-tools**, **nettools**, and **bind-utils**

```
[root@sdc-vm ~]# yum update -y
                [root@sdc-vm ~]# yum install -y open-vm-tools net-tools
bind-utils
```

11. Install the AWS CLI package; see https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html.

> **Note**
>
> Do not use the **--user** flag.

12. Install the Docker CE packages; see https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce

> **Note**
>
> Use the "Install using the repository" method.

13. Start the Docker service and enable it to start on boot:

```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service
to
    /usr/lib/systemd/system/docker.service.
```

14. Create two users: `cdo` and `sdc`. Use the `cdo` user to perform administrative tasks without directly accessing the root user. The `sdc` user will be designated for running the SDC docker container.

```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

15. Set a password for the `sdc` user.

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

16. Add the `sdc` user to the `wheel` group to give it administrative (sudo) privileges.

```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

17. When Docker is installed, there is a user group created. Depending on the version of CentOS/Docker, this may be called either "docker" or "dockerroot". Check the /etc/group file to see which group was created, and then add the sdc user to this group.

```
[root@sdc-vm ~]# grep docker /etc/group
 docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

18. If the /etc/docker/daemon.json file does not exist, create it, and populate with the contents below. Once created, restart the docker daemon.

> **Note**
>
> Make sure that the group name entered in the "group" key matches the group you found in the /etc/group file the previous step.

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
         {
            "live-restore": true,
            "group": "docker"
         }
         [root@sdc-vm ~]# systemctl restart docker
         [root@sdc-vm ~]#
```

19. If you are currently using a vSphere console session, switch over to SSH and log in with the `cdo` user. Once logged in, change to the `sdc` user. When prompted for a password, enter the password for the `cdo` user.

```
[CDO@sdc-vm ~]$ sudo su sdc
               [sudo] password for cdo: <type password for cdo user>
               [sdc@sdc-vm ~]$
```

20. Change directories to **/usr/local/CDO**.
21. Create a new file called `bootstrapdata` and paste the bootstrap data from Step 2 of the **Deploy an On-Premises Secure Device Connector** wizard into this file. **Save** the file. You can use `vi` or `nano` to create the file.
22. The bootstrap data comes encoded in base64. Decode it and export it to a file called `extractedbootstrapdata`

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/ CDO/bootstrapdata >
/usr/local/CDO/extractedbootstrapdata
              [sdc@sdc-vm ~]$
```

Run the cat command to view the decoded data. The command and decoded data should look similar to this:

```
[sdc@sdc-vm ~]$ cat /usr/local/ CDO/extractedbootstrapdata
               CDO_TOKEN="<token string>"
               CDO_DOMAIN="www.defenseorchestrator.com"
               CDO_TENANT="<tenant-name>"

CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
```

23. Run the following command to export the sections of the decoded bootstrap data to environment variables.

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv &&
source sdcenv
              [sdc@sdc-vm ~]$
```

24. Download the bootstrap bundle from Security Cloud Control.

```
[sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN"
"$CDO_BOOTSTRAP_URL"
               100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:--
10654
```

```
               [sdc@sdc-vm ~]$ ls -l /usr/local/ CDO/*SDC
               -rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48
/usr/local/CDO/tenant-name-SDC
```

25. Extract the SDC tarball, and run the `bootstrap.sh` file to install the SDC package.

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/CDO/tenant-name-SDC
               <snipped – extracted files>
               [sdc@sdc-vm ~]$
               [sdc@sdc-vm ~]$ /usr/local/ CDO/bootstrap/bootstrap.sh
               [2018-07-23 13:54:02] environment properly configured
               download: s3://onprem-sdc/toolkit/prod/toolkit.tar to
toolkit/toolkit.tar
               toolkit.sh
               common.sh
               [2018-07-23 13:54:04] startup new container
             Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest'
 locally

sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458:
Pulling from
               ciscodefenseorchestrator/sdc_prod
               08d48e6f1cff: Pull complete
               ebbd10b629b1: Pull complete
               d14d580ef2ed: Pull complete
               45421d451ab8: Pull complete
               <snipped – downloads>
               no crontab for sdc
```

The SDC should now show "Active" in Security Cloud Control.

Bootstrap a Secure Device Connector on the Deployed Host

Procedure

---

1. In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.
2. On the **Services** page, select the **Secure Connectors** tab, click the + icon, and select **Secure Device Connector**.
3. Copy the bootstrap data in step 2 on the window to a notepad.
4. SSH into your VM using the admin user, typically `cdo`, and your chosen password.
5. Switch to the `sdc` user using the command:

```
sudo su - sdc
```

6. Bootstrap your new SDC using the command:

```
sdc bootstrap <paste-your-bootstrap-data-here>
```

7. Select the version of the SDC you want to use.

   We have three options for the SDC version:

   - SDC 2024- This is the version that most will want to run.
   - SDC 2024 with FIPS enabled- Choose this version if you are subject to FedRamp compliance.

- SDC Legacy- This version is no longer receiving feature updates and it is recommended to run SDC 2024 instead.

8. The CLI pulls the container image and starts the SDC and you can validate that your SDC is active and operational on the user interface, and also on the host by running:

```
sdc show running
```

You should now see an SDC for your tenant.

Deploy a Secure Device Connector to vSphere Using Terraform

Before you begin

This procedure details how you can use the Security Cloud Control SDC Terraform module for vSphere in conjunction with the Security Cloud Control Terraform Provider to deploy an SDC to your vSphere. Ensure you review the following prerequisites before attempting to perform this task procedure:

- You have vSphere datacenter version 7 and above
- You have an admin account on the datacenter with permissions to do the following:
  - Create VMs
  - Create folders
  - Create content libraries
  - Upload files to content libraries
- Terraform knowledge

Procedure

---

1. Create an API-only user in Security Cloud Control and copy the API token. To know how to create an API-only user, see Create API Only Users.
2. Configure the Security Cloud Control Terraform provider in your Terraform repository by following the instructions in Security Cloud Control Terraform Provider.

   Example

```
terraform {
  required_providers {
    cdo = {
      source = "CiscoDevNet/cdo"
      version = "0.7.0"
    }
  }
}

provider "cdo" {
  base_url = "<the CDO URL you use to access CDO>"
  api_token = "<the API Token generated in step 1>"
}
```

3. Write Terraform code to create a `cdo_sdc` resource using the Security Cloud Control Terraform provider. See the Terraform registry for Security Cloud Control-sdc resource for more information.

Example

```
Resource "cdo_sdc" "my-sdc" {
  name = "my-sdc-in-vsphere"
}
```

The `bootstrap_data` attribute of this resource is populated with the value of the Security Cloud Control bootstrap data and is provided to the `cdo_sdc` Terraform module in the next step.

4. Write Terraform code to create the SDC in vSphere using Security Cloud Control_sdc Terraform module.

   Example

```
data "cdo_tenant" "current" {}

module "vsphere-cdo-sdc" {
  source               = "CiscoDevNet/cdo-sdc/vsphere"
  version              = "1.0.0"
  vsphere_username     = "<replace-with-username-with-admin-privileges>"
  vsphere_password     = "<super-secure-password>"
  vsphere_server       = "<replace-with-address-of-vsphere-server>"
  datacenter           = "<replace-with-datacenter-name>"
  resource_pool        = "<replace-with-resource-pool-name>"
  cdo_tenant_name      = data.cdo_tenant.current.human_readable_name
  datastore           = "<replace-with-name-of-datastore-to-deploy-vm-in>"

  network              = "<replace-with-name-of-network-to-deploy-vm-in>"
  host                 = "<replace-with-esxi-host-address>"
  allow_unverified_ssl = <boolean; set to true if your vsphere server does
not have a valid SSL certificate>
  ip_address           = "<sdc-vm-ip-address; must be in the subnet of the
assigned network for the VM>"
  gateway              = "<replace-with-network-gateway-address>"
  cdo_user_password    = "<replace-with-password-for-cdo-user-in-sdc-vm>"
  root_user_password   = "<replace-with-password-for-root-user-in-sdc-vm>"
  cdo_bootstrap_data   = cdo_sdc.sdc-in-vsphere.bootstrap_data
}
```

   Note that the VM created has two users–a `root` user and a user called `cdo`–and the IP Address of the VM is configured statically. The `cdo_bootstrap_data` attribute is given the value of the `bootstrap_data` attribute generated when the `cdo_sdc` resource is created.

5. Plan and apply your Terraform using `terraform plan` and `terraform apply`, as you would normally.

   See the Security Cloud Control Automation Repository in the CiscoDevNet for a complete example.

If your SDC stays in the onboarding state, connect to the vSphere VM using remote console, log in as the `cdo` user, and execute the following command:

```
sdc host status
```

Depending on the readout, you may need to manually run:

```
sdc host configure
```

Note

The Security Cloud Control Terraform modules are published as Open Source Software under the Apache 2.0 license. You can file issues on GitHub if you require support.

Deploy a Secure Device Connector on an AWS VPC Using a Terraform Module

This procedure details the steps involved in deploying a secure device connector on an AWS VPC using a Terraform module.

Before you begin

Review these prerequisites before attempting to deploy an SDC on your AWS VPC:

- Security Cloud Control requires strict certificate checking and does not support Web/Content Proxy inspection between the SDC and the Internet. If using a proxy server, disable inspection for traffic between the Secure Device Connector (SDC) andSecurity Cloud Control.
- See Connect Security Cloud Control to the Secure Device Connector to ensure proper network access.
- You require an AWS account, an AWS VPC with at least one subnet, and an AWS Route53-hosted zone.
- Ensure you have the Security Cloud Control bootstrap data, your AWS VPC ID, and its subnet ID handy.
- Ensure that the private subnet to which you deploy the SDC has a NAT gateway attached.
- Open traffic on the port on which your firewall management HTTP interface is running, from your firewalls to the Elastic IP attached to the NAT gateway.

Procedure

1. Add the following lines of code in your Terraform file; make sure you manually enter inputs for variables:

```
module "example-sdc" {
  source              =
"git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"

  env                 = "example-env-ci"
  instance_name       = "example-instance-name"
  instance_size       = "r5a.xlarge"
  cdo_bootstrap_data  = "<replace-with-cdo-bootstrap-data>"
  vpc_id              = <replace-with-vpc-id>
  subnet_id           = <replace-with-private-subnet-id>
}
```

   See the Secure Device Connector Terraform module for a list of input variables and descriptions.

2. Register `instance_id` as an output in your Terraform code:

```
output "example_sdc_instance_id" {
  value = module. example-sdc.instance_id
}
```

   You can use the `instance_id` to connect to the SDC instance for troubleshooting using the AWS Systems Manager Session Manager (SSM). See Outputs in the Secure Device Connector Terraform module for a list of available outputs.

What to do next:

For any troubleshooting of your SDC, you need to connect to the SDC instance using AWS SSM. See AWS Systems Manager Session Manager to know more about how to connect to your instance. Note that the ports to connect to the SDC instance using SSH are not exposed because of security reasons.

> **Note**
>
> The Security Cloud Control Terraform modules are published as Open Source Software under the Apache 2.0 license. You can file issues on GitHub if you require support.

Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine

Security Cloud Control's on-premises Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to this point. Since CentOS 7 is now end-of-life and has been deprecated by Security Cloud Control, we have created this migration process to help you migrate all SDCs from CentOS 7 to an Ubuntu virtual machine.

Before You Migrate

- The SDC must have full outbound access to the internet on TCP port 443.
- The Ubuntu virtual machine running the SDC must have network access to the management interfaces of the devices it communicates with, such as ASAs and Cisco IOS devices.
- Any networking rules created for the IP address or FQDN of the old SDC VM to reach your devices should be recreated with the IP address or FQDN of the new SDC VM.
- The migration will take 10 to 15 minutes. During this time, your device will continue to enforce security policy and route network traffic, but you will not be able to communicate with it through the SDC.

Prerequisites

Deploy a new host by following the instructions on Deploy a VM for Running the Secure Device Connector and Secure Event Connector.

Host Configuration

Follow this procedure if you are migrating the SDC and/or SEC:

1. Download the new VM image here.
2. Unzip the CDO-SDC_VM.zip file. You should see three VM files named similarly to the following:
   - CDO-SDC-VM-708cd33-2024-05-30-2031-disk1.vmdk
   - CDO-SDC-VM-708cd33-2024-05-30-2031.mf
   - CDO-SDC-VM-708cd33-2024-05-30-2031.ovf
3. Deploy the VM you just downloaded.
4. Note the static IP address or FQDN you assigned to the new VM.
5. Using SSH, log in to the new VM as the `cdo` user.

6. At the prompt, enter the command:

```
sudo sdc host configure
```

> **Note**
>
> - Follow the prompts in the migration script closely. The script is well-documented and will guide you through the migration process, explaining each step.
> - At the end of the migration script, you will receive a message indicating that your SDC has been migrated to the new VM. The SDC will retain its name after the migration.

SDC Migration

Procedure:

1. Using SSH, log in to the old (CentOS) SDC as the `cdo` user.
2. Install the CLI using the command:

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
 && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh &&
./install.sh
```

3. Run the following command and follow the prompts:

```
sudo sdc migrate now
```

Verification:

1. Log in to your Security Cloud Control tenant.
2. Select the SDC you migrated, and in the **Actions** pane, click **Request Heartbeat**.

> **Note**
>
> Ensure that the SDC is in the **Active** state.

SEC Migration

Procedure:

1. Using SSH, log in to the old (CentOS) SDC as the `cdo` user.
2. Install the CLI using the command:

```
curl -O
https://s3.us-west-2.amazonaws.com/download.defenseorchestrator.com/sdc-cli/sdc-cli-package-latest.tgz
```

```
 && tar -xvf sdc-cli-package-latest.tgz && chmod +x ./install.sh &&
./install.sh
```

3. Run the following command and follow the prompts:

```
sudo sdc eventing migrate
```

4. You can configure your devices to point to the new IP address of the SEC or you can shut down the old host and assign the new host the same IP address that the old host had so that the devices do not need to be updated.

Verification:

For information on the state of the SEC, see Use Health Check to Learn the State of your Secure Event Connector.

Additional Instructions

Do Not Restart Your Old SDC

After the migration is complete, do not restart your old SDC on the original virtual machine.

Revert Failed Migration

If the migration fails for any reason, or the result is not what you are expecting and you want to revert to the old SDC, follow the instructions below:

1. Log in to the new VM and switch to the **SDC** user.
2. Ensure the SDC is not currently running on the new VM using the command:

```
docker ps
```

3. If the SDC is running, run the command:

```
sdc stop
```

4. Confirm that the SDC has stopped running by executing `docker ps` again.
5. Log in to the old VM and run the command:

```
sdc migrate revert
```

6. When the old SDC is active and visible in the UI, return to the new VM and execute the command:

```
sdc delete <your-tenant-name-here>
```

7. Refresh the browser completely, click on the SDC, and verify that the IP of the old host appears in the sidebar.

   If the new IP still appears despite following these steps, request a new health check, refresh the browser, and check again.

8. To revert the SEC migration,run the command:

```
sdc eventing revert
```

Change the IP Address of a Secure Device Connector

When you are using a Secure Device Connector (SDC) deployed on your own VM, you might need to change the IP address of your SDC for several reasons, such as migrating your VMs to a different data center. Use this procedure to assign a new IP address to your SDC.

Before you begin

- You must be an admin to perform this task.
- The SDC must have full outbound access to the Internet on TCP port 443, or the port you have configured for device management.

> **Note**
>
> You will not be required to re-onboard any devices to Security Cloud Control after changing the SDC's IP address.

Procedure

1. Create an SSH connection to your SDC or open your virtual machine's console, and log in as the **CDO** user.
2. To view your SDC VM's network interface configuration information before changing the IP address, use the command:

```
[cdo@localhost ~]$ ip addr
```

3. To change the IP address of the interface, re-initiate the host configuration using the command:

```
[cdo@localhost ~]$ sdc host configure network
```

4. Enter your password at the prompt.
5. The configure script will then ask you about your networking configuration, write the new config file with the new IP and apply that configuration.

> **Note**
>
> You will lose your SSH connection at this time.

6. Create an SSH connection using the new IP address you assigned to your SDC and log in.
7. Your SDC should start automatically, but if it does not, run the following commands:

```
[cdo@localhost ~]$ sudo su - sdc
```

```
[cdo@localhost ~]$ sdc start
```

> **Note**
>
> If you are performing this procedure in the VM's console, when you confirm the values are correct, the connectivity status test is automatically run and the status is shown.

8. You can also check your SDC's connectivity through the Security Cloud Control user interface. To do that, open the Security Cloud Control application and navigate to **Administration** > **Integrations** > **Secure Connectors** page.
9. Refresh the page once and select the secure connector whose IP address you changed.
10. On the **Actions** pane, click **Request Heartbeat**. You should see the **Heartbeat** requested successfully message, and the **Last Heartbeat** should display the current date and time.

Move an ASA from one Secure Device Connector to Another

Security Cloud Control Firewall Management supports the use of more than one SDC per tenant. You can move a managed ASA from one SDC to another using this procedure:

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **ASA** tab.
3. Select the ASA or ASAs you want to move to a different SDC.
4. In the **Device Actions** pane, click **Update Credentials**.
5. Click the Secure Device Connector button and select the SDC you want to move the device to.
6. Enter the administrator username and password Security Cloud Control uses to log into the device and click **Update**. Unless they were changed, the administrator username and password are the same credentials you used to onboard the ASA. You do not have to deploy these changes to the device.

> **Note**
>
> If all the ASAs use the same credentials, you can move ASAs in bulk from one SDC to another. If the ASAs have different credentials, you have to move them from one SDC to another one at a time.

Rename a Secure Device Connector

Procedure

1. In the left pane, choose **Administration** > **Integrations** > **Secure Connectors**.
2. Select the SDC you want to rename.
3. In the Details pane, click the edit icon next to the name of the SDC.

4. Rename the SDC.

This new name will appear wherever the SDC name appears in the Security Cloud Control interface including the Secure Device Connectors filter of the **Security Devices** pane.

Update a Secure Device Connector manually

Use this task as a troubleshooting tool. The source says that the SDC is usually updated automatically and that you should not need to perform a manual update unless errors occur.

Procedure

1. Connect to your SDC. You can connect using SSH or use the console view in your Hypervisor.
2. Log in to the SDC as the admin user, typically **cdo**.
3. Switch to the SDC user to update the SDC docker container:

```
[cdo@sdc-vm ~]$ sudo su sdc
                [sudo] password for cdo: <type password for cdo user>
                [sdc@sdc-vm ~]$
```

4. Upgrade the SDC:

```
sdc upgrade
```

> **Note**
>
> **Recommended updates and maintenance on the SDC Virtual Machine**
>
> Ensure that you monitor and apply updates to the SDC VM running on Ubuntu Linux following your organisation's internal IT security and patch management policies. We highly recommend regularly reviewing and applying relevant security patches to ensure that the SDC VM remains secure and functions optimally within your network environment.

Use multiple Secure Device Connectors on one tenant

You can install an unlimited number of SDCs on a tenant. Multiple SDCs let you manage more devices and place connectors in different network segments while keeping those devices in the same Security Cloud Control Firewall Management tenant.The procedure for deploying a second or later SDC is the same as the procedure for the first SDC.The first SDC name includes the tenant name and the number `1`. Each additional SDC is numbered in order.

- The procedure for deploying a second or subsequent SDC is the same for deploying your first SDC.
- The initial SDC for your tenant incorporates the name of your tenant and the number 1. Each additional SDC is numbered in order.

Find devices that sse the same Secure Device Connector

Follow this procedure to find devices that connect through the same SDC:

Procedure

1. In the left pane, **Security Devices**.
2. Click the **Devices** tab to locate the device.
3. Click the appropriate device type tab.
4. If there is any filter criteria already specified, click the **clear** button at the top of the **Security Devices** page to show all the devices and services you manage with Security Cloud Control.
5. Click the filter button to expand the filter menu.
6. In the **Secure Device Connectors** section of the filter, check the name of the SDC(s) you're interested in. The **Security Devices** page displays only the devices that connect to Security Cloud Control through the SDC you checked in the filter.
7. (Optional) Check additional filters in the filter menu to refine your search further.
8. (Optional) When you're done, click the **clear** button at the top of the **Security Devices** page to show all devices and services you manage with Security Cloud Control.

Remove a Secure Device Connector

Deleting an SDC is not reversible. After you remove it, you cannot manage the devices that were connected to that SDC until you install a new SDC and reconnect the devices. Reconnecting devices can require you to enter administrator credentials again.

Before you remove an SDC, move the connected devices to another SDC or remove them from Security Cloud Control Firewall Management.

Procedure

1. Remove any devices connected to the SDC you want to delete.
   - a. See Find all Devices that Connect to Security Cloud Control Using the Same SDC to identify all the devices used by the SDC.
   - b. In the **Security Devices** page, select all the devices you identified.
   - c. In the Device Actions pane, click **Remove** and click **OK** to confirm your action.
2. In the left pane, click **Administration** > **Integrations** > **Secure Connectors**.
3. On the **Services** page with the **Secure Connectors** tab selected, click the blue plus button and select **Secure Device Connector**.
4. In the Secure Connectors table, select the SDC you want to remove. Its device count should now be zero.
5. In the Actions pane, click **Remove**. You receive this warning:

> **Warning**
>
> You are about to delete <sdc_name>. Deleting the SDC is not reversible. Deleting the SDC will require you to create and onboard a new SDC before you can onboard, or re-onboard, your devices.

Because you currently have onboarded devices, removing the SDC will require you to reconnect those devices and provide credentials again after setting up a new SDC.

- If you have any questions or concerns, click **Cancel** and contact Security Cloud Control support.
- If you wish to proceed, enter <sdc_name> in the text box below and click **OK**.

6. In the confirmation dialog box, if you wish to proceed, enter your SDC's name as it is stated in the warning message.
7. Click **OK** to confirm the SDC removal.

Open source and third-party license in SDC

An overview of open-source and third-party license attributions for components included in the Cisco Secure Device Connector (SDC).

==========

*** amqplib ***

amqplib copyright (c) 2013, 2014

Michael Bridgen <mikeb@squaremobius.net>

This package, "amqplib", is licensed under the MIT License. A copy maybe found in the file LICENSE-MIT in this directory, or downloaded from

http://opensource.org/licenses/MIT

==========

*** async ***

Copyright (c) 2010-2016 Caolan McMahon

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** bluebird ***

The MIT License (MIT)

Copyright (c) 2013-2015 Petka Antonov

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** cheerio ***

Copyright (c) 2012 Matt Mueller <mattmuelle@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the 'Software'), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED 'AS IS', WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** command-line-args ***

The MIT License (MIT)

Copyright (c) 2015 Lloyd Brookes <75pound@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** ip ***

This software is licensed under the MIT License.

Copyright Fedor Indutny, 2012.

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** json-buffer ***

Copyright (c) 2013 Dominic Tarr

Permission is hereby granted, free of charge,to any person obtaining a copy of this software andassociated documentation files (the "Software"), todeal in the Software without restriction, includingwithout limitation the rights to use, copy, modify,merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whomthe Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission noticeshall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIESOF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FORANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THESOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stable-stringify ***

This software is released under the MIT license:

Permission is hereby granted, free of charge, to any person obtaining a copy ofthis software and associated documentation files (the "Software"), to deal inthe Software without restriction, including without limitation the rights touse, copy, modify, merge, publish, distribute, sublicense, and/or sell copies ofthe Software, and to permit persons to whom the Software is furnished to do so,subject to the following conditions:

The above copyright notice and this permission notice shall be included in allcopies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESSFOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS ORCOPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHERIN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR INCONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** json-stringify-safe ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** lodash ***

Copyright JS Foundation and other contributors <https://js.foundation/**>**

Based on Underscore.js, copyright Jeremy Ashkenas,

DocumentCloud and Investigative Reporters & Editors<http://underscorejs.org/**>**

This software consists of voluntary contributions made by manyindividuals. For exact contribution history, see the revision historyavailable at https://github.com/lodash/lodash

The following license applies to all parts of this software except as

documented below:

====

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

Copyright and related rights for sample code are waived via CC0. Samplecode is defined as all source code displayed within the prose of thedocumentation.

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

Files located in the node_modules and vendor directories are externallymaintained libraries used by this software which have their ownlicenses; we recommend you read them, as their terms may differ from theterms above.

==========

*** log4js ***

Copyright 2015 Gareth Jones (with contributions from many other people)

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions andlimitations under the License.

==========

*** mkdirp ***

Copyright 2010 James Halliday (mail@substack.net)

This project is free software released under the MIT/X11 license:

Permission is hereby granted, free of charge, to any person obtaining a copyof this software and associated documentation files (the "Software"), to dealin the Software without restriction, including without limitation the rightsto use, copy, modify, merge, publish, distribute, sublicense, and/or sellcopies of the Software, and to permit persons to whom the Software isfurnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included inall copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

==========

*** node-forge ***

New BSD License (3-clause)

Copyright (c) 2010, Digital Bazaar, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or withoutmodification, are permitted provided that the following conditions are met:

*** Redistributions of source code must retain the above copyrightnotice, this list of conditions and the following disclaimer.**

*** Redistributions in binary form must reproduce the above copyrightnotice, this list of conditions and the following disclaimer in thedocumentation and/or other materials provided with the distribution.**

*** Neither the name of Digital Bazaar, Inc. nor thenames of its contributors may be used to endorse or promote productsderived from this software without specific prior written permission.**

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" ANDANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIEDWARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AREDISCLAIMED. IN NO EVENT SHALL DIGITAL BAZAAR BE LIABLE FOR ANYDIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED ANDON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THISSOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

*** request ***

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their

Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to

indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

==========

*** rimraf ***

The ISC License

Copyright (c) Isaac Z. Schlueter and Contributors

Permission to use, copy, modify, and/or distribute this software for anypurpose with or without fee is hereby granted, provided that the abovecopyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIESWITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OFMERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FORANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGESWHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN ANACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF ORIN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==========

*** uuid ***

Copyright (c) 2010-2012 Robert Kieffer

MIT License - http://opensource.org/licenses/mit-license.php

==========

*** validator ***

Copyright (c) 2016 Chris O'Hara <cohara87@gmail.com>

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==========

*** when ***

Open Source Initiative OSI - The MIT License

http://www.opensource.org/licenses/mit-license.php

Copyright (c) 2011 Brian Cavalier

Permission is hereby granted, free of charge, to any person obtaininga copy of this software and associated documentation files (the"Software"), to deal in the Software without restriction, includingwithout limitation the

rights to use, copy, modify, merge, publish,distribute, sublicense, and/or sell copies of the Software, and topermit persons to whom the Software is furnished to do so, subject tothe following conditions:

The above copyright notice and this permission notice shall beincluded in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OFMERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE ANDNONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BELIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTIONOF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTIONWITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.==========

6 Onboard devices in Security Cloud Control Firewall Management

Topics:

- Onboard an On-Premises Firewall Management Center to Security Cloud Control Firewall Management
- Remove an On-Premises Firewall Management Center from Security Cloud Control

Learn how to onboard devices in Security Cloud Control Firewall Management, including prerequisites, connector selection, credentials, labels, and inventory results.

You can onboard both live devices and model devices to Security Cloud Control Firewall Management. Model devices are uploaded configuration files that you can view and edit using Security Cloud Control Firewall Management.

Most live devices and services require an open HTTPS connection so that the Secure Device Connector can connect Security Cloud Control Firewall Management to the device or service.

This chapter covers the following sections:

Onboard an On-Premises Firewall Management Center to Security Cloud Control Firewall Management

This concept explains how to onboard an On-Premises Firewall Management Center to Security Cloud Control Firewall Management, enabling centralized device visibility, shared policy management, and streamlined provisioning using recommended integration methods and best practices. It also outlines important limitations and configuration guidelines for a successful onboarding process.

Security Cloud Control Firewall Management provides two methods to onboard on-premises Firewall Management Centers.

- Preferred method (direct onboarding without Secure Device Connector): Auto discover and onboard on-premises Firewall Management Center integrated with Cisco Security Cloud. This direct method is recommended because most cloud assist features are supported only when on-premises Firewall Management Center is onboarded directly without using Secure Device Connector (SDC). Direct onboarding provides full access to cloud assist capabilities, such as zero-touch provisioning, centralized device visibility, and policy optimization. This is the preferred method for most use cases. For more information about integrating on-premises Firewall Management Center with Cisco Security Cloud, refer to Integrate an On-Premises Firewall Management Center With Cisco Security Cloud on page 75.

  > **Attention**
  >
  > This method is not available to Government customers. Government customers must use the credentials method to onboard an On-Premises Firewall Management Center to Security Cloud Control.

- Alternative method (using SDC): Use on-premises Firewall Management Center credentials with SDC is supported but intended only for very rare use cases. Onboarding with SDC limits access to many cloud assist features available with direct onboarding. Choose SDC if direct onboarding is not possible.

  For more information, see Allow inbound access for direct cloud connectivity on page 44.

Security Cloud Control complements FMC by enabling:

- Consistent policy enforcement through shared object management with FMCs.

  For more information, see the **Objects** section in Managing On-Prem Firewall Management Center with Security Cloud Control.

- Zero-touch provisioning of Firewall Threat Defense devices. For more information, refer to Onboard a Device to On-Premises Firewall Management Center with Zero-Touch Provisioning.
- Centralized visibility and management of security devices. For more information, refer to Device and Service Management.
- Integration with cloud Cisco Secure Dynamic Attributes Connector (CSDC) and Cloud-Delivered Firewall Management Center. For more information, refer to Cisco Secure Dynamic Attributes Connector.

Limitations and Guidelines

- Onboarding an on-premises Firewall Management Center also onboards all devices registered to it. Disabled or unreachable devices may appear in the **Security Devices** page in Security Cloud Control but cannot be managed or queried.
- Onboarding does **not** cascade policies from on-premises Firewall Management Center to Security Cloud Control or Cloud-Delivered Firewall Management Center. To migrate Firewall Threat Defense devices to Cloud-Delivered Firewall Management Center, use the built-in **Migrate FTD to** Cloud-Delivered Firewall Management Center feature. For more information, refer to Migrate Threat Defense to Cloud-delivered Firewall Management Center.

- We recommend creating a dedicated user on the on-premises Firewall Management Center with administrator-level permissions specifically for Security Cloud Control communication. If you log in to on-premises Firewall Management Center with the same credentials during onboarding, the process will fail. This recommendation applies only to credentials-based onboarding, not to direct integration.
- For this dedicated user, set the **Maximum Number of Failed Logins** to zero.
- For on-premises Firewall Management Centers version 7.4 or later, if a switchover causes a loss of cloud connectivity, disable and then re-enable **SecureX**, **Security Cloud Control**, or **Cisco Security Cloud** (depending on your version) to restore the connection.

Auto onboard an On-Premises Firewall Management Center integrated with Cisco Security Cloud

Automatically onboard an On-Premises Firewall Management Center integrated with Cisco Security Cloud, ensuring seamless discovery and enrollment of both the management center and its associated devices for centralized security management.

> **Attention**
>
> This method is not available to Government customers. Government customers must use the credentials method to onboard an On-Premises Firewall Management Center to Security Cloud Control.

The auto-discovery and onboarding feature is enabled by default in Security Cloud Control. All on-premises Firewall Management Centers running version 7.2 or later and integrated with Cisco Security Cloud are automatically discovered and onboarded to Security Cloud Control. The associated Firewall Threat Defense devices are onboarded to Security Cloud Control.

Security Cloud Control also onboards the on-premises Firewall Management Center high-availability (HA) pair.

Before you begin

Ensure that outbound traffic is allowed from port 443 on the on-premises Firewall Management Center.

Procedure

1. Integrate the on-premises Firewall Management Center you want to onboard with Cisco Security Cloud and register it with a Security Cloud Control tenant. For more information, see Integrate an On-Premises Firewall Management Center With Cisco Security Cloud on page 75.
2. Log in to the Security Cloud Control tenant that was registered with the on-premises Firewall Management Center.
3. Choose **Administration** > **Integrations** > **Firewall Management Center**.

   All on-premises Firewall Management Centers associated with your tenant are displayed in the **FMC** tab. For more information, see View Onboarded On-Premises Firewall Management Center.

Integrate an On-Premises Firewall Management Center With Cisco Security Cloud

Integrate an on-premises Firewall Management Center with Cisco Security Cloud to enable seamless registration, tenant selection or creation, and centralized management of your firewall devices using a guided integration process.

This procedure describes how to integrate the On-Premises Firewall Management Center with Cisco Security Cloud. By enabling Cisco Security Cloud integration, your management center gets registered to the Cisco cloud tenancy.

Before you begin

When onboarding an on-premises Firewall Management Center:

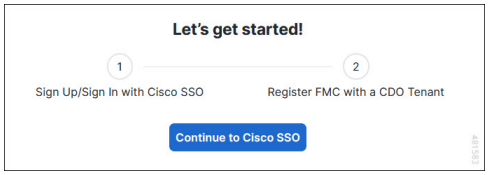
- If you already have a Security Cloud Control tenant, you will be prompted to confirm whether you want to attach the on-premises Firewall Management Center to that existing tenant.
- If you do not have a tenant or account, the on-premises Firewall Management Center integration wizard will automatically create a new tenant for you during the registration task the onboarding process. This tenant is a free tier provided exclusively for on-premises Firewall Management Center AI Assist enablement. Allow the wizard to manage tenant creation so that you do not receive a trial tenant that would later require conversion. The wizard manages this process to provide a seamless experience.
- If you intend to use the Cloud-Delivered Firewall Management Center or manage firewalls using the Security Cloud Control, you must purchase a base license and device entitlements. For detailed licensing information and product options, refer to the Security Cloud Control Licensing Overview.

Procedure

1. Based on your on-premises Firewall Management Center version, do the following:
   - For on-premises Firewall Management Center version between 7.2 and 7.4.x, click **Enable Secure X**.
   - For on-premises Firewall Management Center version 7.6 or later, click **Cisco Security Cloud**.
   - For on-premises Firewall Management Center version 10.0 or later, click **Security Cloud Control**.

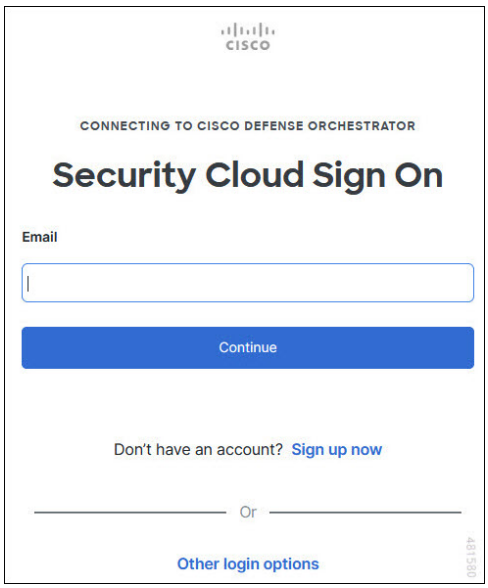
   A separate browser tab opens to log you in to your Security Cloud Control account. Make sure this page is not blocked by a pop-up blocker.
2. Click **Continue to Cisco SSO**.

   Figure 1: Cisco Security Cloud Welcome Page



3. Log in to your Security Cloud Control account.

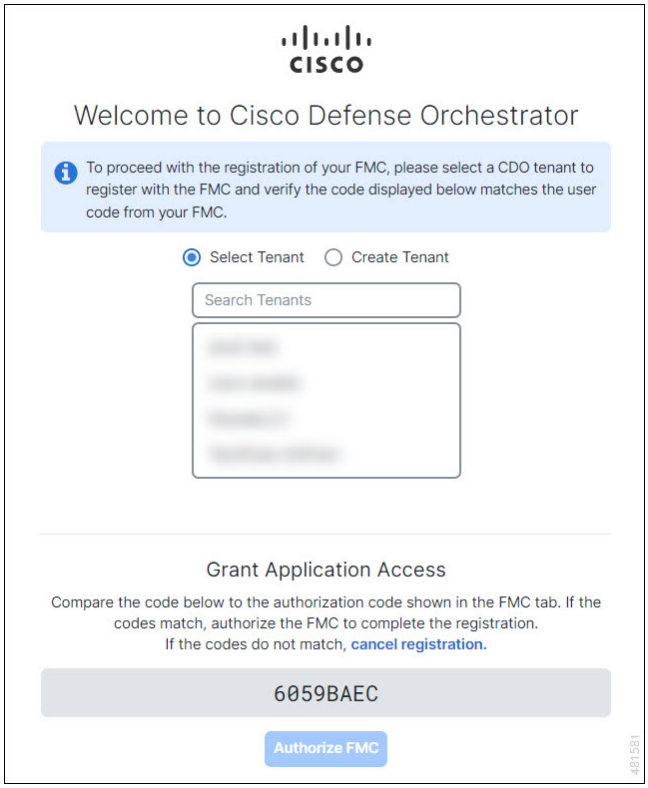
   Figure 2: Cisco Security Cloud Sign On



If you do not have a security cloud sign on account to log in to Security Cloud Control and you want to create one, click **Sign up now** in the **Security Cloud Sign On** page. See Create a New Cisco Security Cloud Sign On Account.

4. Choose a Security Cloud Control tenant that you want to use for this integration. The on-premises Firewall Management Center and the managed devices get onboarded to the Security Cloud Control tenant that you choose here.

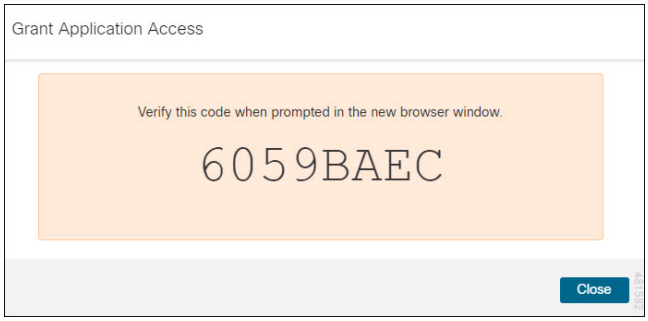
Figure 3: Choose the Security Cloud Control Tenant



If you do not already have a Security Cloud Control tenant or if you want to use a new tenant for this integration, create a new tenant.

5. Verify that the code displayed in the Security Cloud Control login page matches the code provided by the on-premises Firewall Management Center.

   Figure 4: Verification Code in the on-premises Firewall Management Center



6. Click **Authorize FMC**.
7. In the on-premises Firewall Management Center UI, click **Save** to save the configuration.

   You can view the task progress under **Notifications** > **Tasks**.

   The registration task can take up to 90 seconds to complete. If you must use on-premises Firewall Management Center while the registration task is in progress, open the on-premises Firewall Management Center in a new window.

Auto onboard On-Prem FMCs from Cisco Security Cloud

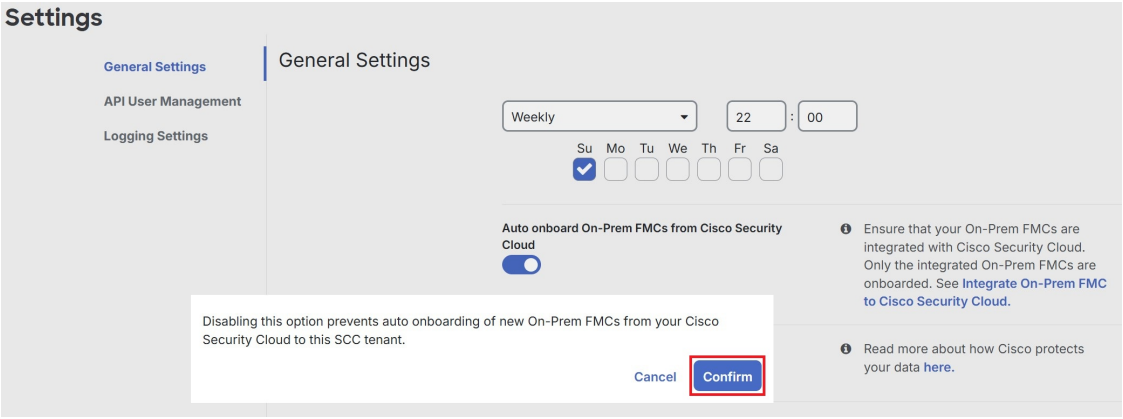
Learn how to disable the auto-onboarding of on-premises Firewall Management Centers from your Cisco Security Cloud to your Security Cloud Control tenant, ensuring only authorized devices are added. This procedure is available to Super Admins and Admins.

Disabling the auto-onboarding functionality stops new on-premises Firewall Management Centers from being automatically added from your Cisco Security Cloud tenant.

> **Note**
>
> Only a Super Admin or Admin can enable or disable this functionality on Security Cloud Control.

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn off the **Auto onboard On-Prem FMCs from Cisco Security Cloud** toggle button to disable the auto-onboarding of on-premises Firewall Management Center.
3. Click **Confirm**.



Onboard an On-Premises Firewall Management Center to Security Cloud Control with Credentials

Learn how to onboard an on-premises Firewall Management Center to Security Cloud Control using credentials, ensuring proper connectivity and secure access through either a Secure Device Connector or Cloud Connector, with options to label and manage your devices after onboarding.

To onboard an on-premises Firewall Management Center to Security Cloud Control with credentials, follow this procedure:

Before you begin

These prerequisites must be met:

- **For Cloud Secure Device Connector (SDC)**: Allow inbound traffic on port 443 of the on-premises Firewall Management Center.

  The SDC reaches the on-premises Firewall Management Center by allowing inbound traffic on port 443.



  Both the Security Cloud Control and the SDC are hosted in the cloud.

- **For On-Premises Secure Device Connector (SDC)**: Allow outbound connectivity on port 443 of the SDC.

  The SDC requires connectivity to the Security Cloud Control, making it imperative to permit outbound traffic from the SDC to the Security Cloud Control. No additional port configuration is required on on-premises Firewall Management Center.



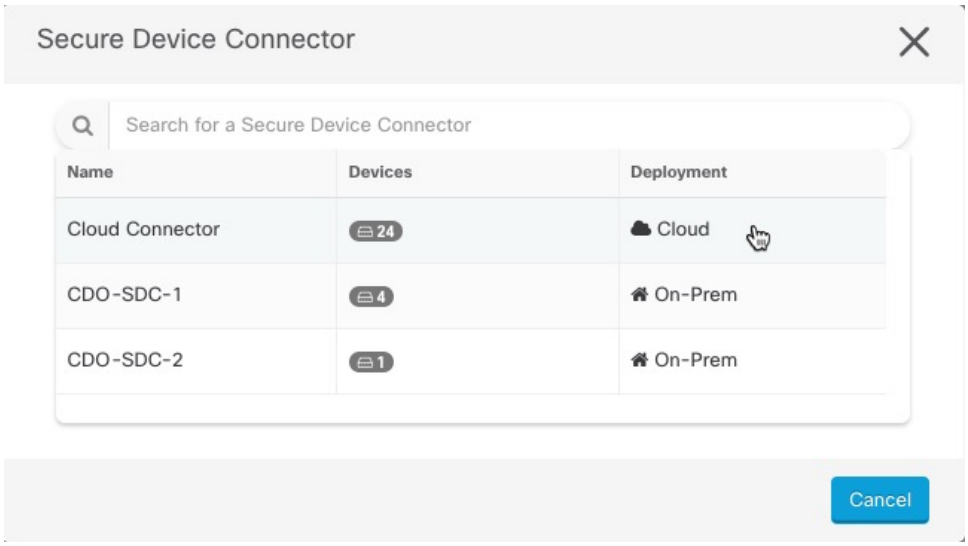
Procedure

1. Choose **Administration** > **General Settings**.

2. Click + to onboard an on-premises Firewall Management Center.
3. Click **Firewall Management Center**.
4. Select the **Use Credentials** card.
5. Click the **Secure Device Connector** button and select an SDC installed in your network.

   If you would rather not use an SDC, Security Cloud Control can connect to your on-premises Firewall Management Center using the Cloud Connector. Your choice depends on how you connect Security Cloud Control to your managed devices.

   Figure 5: Choose a Secure Device Connector



6. Enter the device name and location and click **Next**.
7. Enter the **Username** and **Password** of the account credentials you want to use to access the on-premises Firewall Management Center. Click **Next**.
8. After you onboard the device, you can add labels to your on-premises Firewall Management Center, or you can click **Go to Services** to view the page of onboarded devices. If the device is healthy, the FMC displays a **Synced** status.

> **Note**
>
> Devices managed by on-premises Firewall Management Center are automatically named as " *<fmcname>_<manageddevicename>*."

Redirect Security Cloud Control to an On-Premises Firewall Management Center

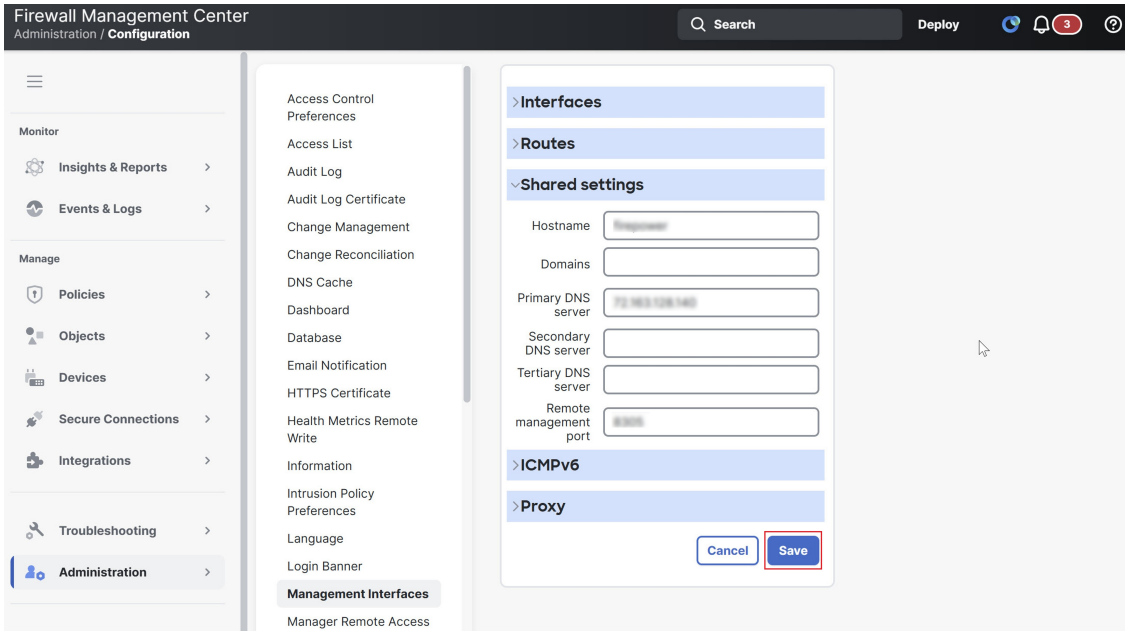
Learn how to update the management interface hostname to include the FQDN in your on-premises Firewall Management Center, enabling seamless cross-launch from Security Cloud Control to the device UI.

After you onboard an on-premises Firewall Management Center to Security Cloud Control, update the management interface's hostname in the on-premises Firewall Management Center UI so that it contains the FQDN. If you do not update the management interface's hostname, you cannot cross-launch from Security Cloud Control.

Use this procedure to update the management interface hostname and redirect from Security Cloud Control to on-premises Firewall Management Center:

Procedure

1. Log in to the On-Premises Firewall Management Center UI.
2. Choose **Administration** > **Configuration**.
3. Click the **Management Interfaces** tab.
4. Under **Shared Settings**, locate the **Hostname** field and enter the Firewall Management Center's FQDN.
5. Click **Save**.



> **Note**
>
> You may have to log out of Security Cloud Control before you can click **Manage Devices in Firepower Management Center** and cross-launch to the on-premises Firewall Management Center UI.

Remove an On-Premises Firewall Management Center from Security Cloud Control

Learn how to remove an on-premises Firewall Management Center and its managed devices from Security Cloud Control by disabling auto-onboarding and following the device removal steps in the **Administration** settings.

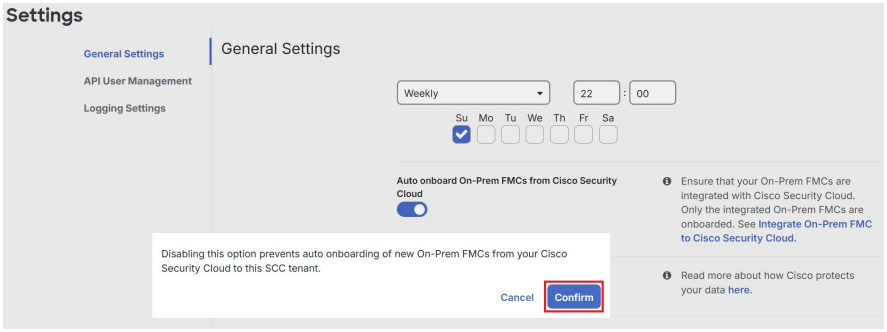
If you remove an on-premises Firewall Management Center from Security Cloud Control, all devices managed by that on-premises Firewall Management Center will also be removed.

Before you begin

To remove one or more on-premises Firewall Management Centers that were onboarded using auto-onboarding, first disable the auto-onboarding option.

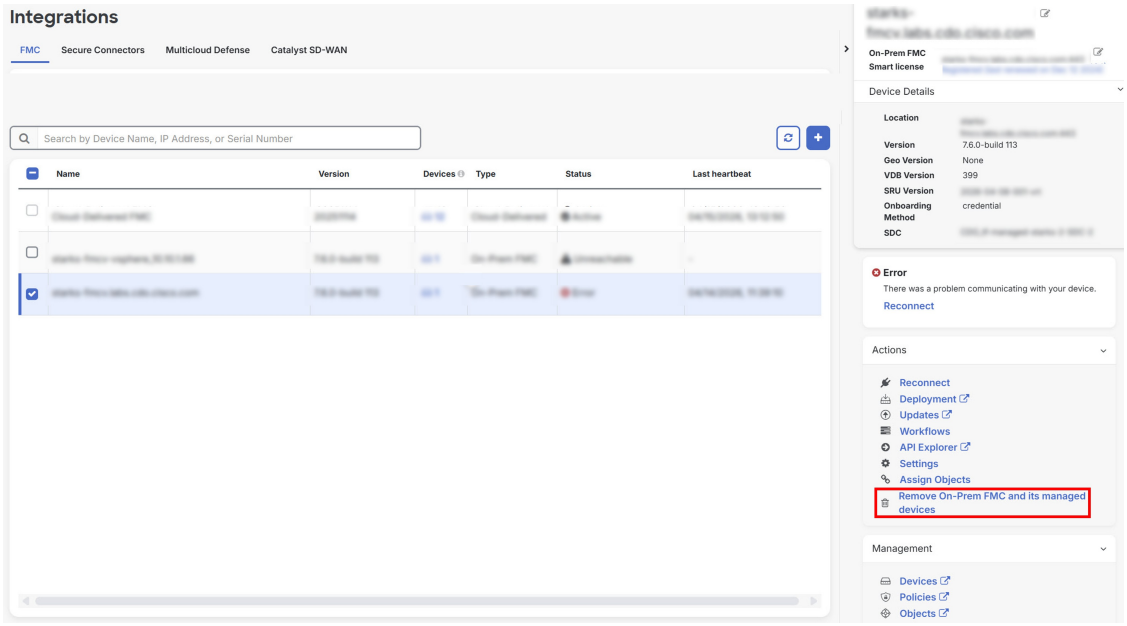
1. Choose **Administration** > **General Settings**.

2. In the **Tenant Settings** section, disable **Auto onboard On-Prem FMCs integrated to Cisco Security Cloud**.



Procedure

1. Choose **Administration** > **Integrations** > **Firewall Management Center**.
2. Click the **FMC** tab.
3. Choose the on-premises Firewall Management Center you want to remove.
4. In the **Device Actions** pane, click **Remove On-Prem FMC and its managed devices**.



5. Click **OK** to confirm that you want to remove on-premises Firewall Management Center and its managed devices from your tenant.
6. Refresh your browser to see an updated list of devices.

7 Manage onboarded device settings

Topics:

- Changing a device's IP address in Security Cloud Control Firewall Management
- Changing a device's name in Security Cloud Control Firewall Management
- Export a list of devices and services
- Export device configuration
- External links for devices
- Bulk reconnect devices to Security Cloud Control Firewall Management
- Moving devices between organizations
- Device certificate expiry detection
- Write a device note
- Delete a device from Security Cloud Control Firewall Management
- Back up Firewall Threat Defense devices
- Manage Firewall Threat Defense devices through Security Cloud Control Firewall Management
- Security devices overview
- Security Cloud Control Firewall Management labels and filtering
- Use Security Cloud Control Firewall Management search functionality

This chapter provides guidance on managing the device settings of the onboarded device.

Changing a device's IP address in Security Cloud Control Firewall Management

Learn how to use changing a device's IP address in Security Cloud Control Firewall Management.

When you onboard an device to Security Cloud Control Firewall Management using an IP address, Security Cloud Control Firewall Management stores that IP address in its database and communicates with the device using that IP address. If the IP address of the device changes, you can update the IP address stored in Security Cloud Control Firewall Management to match the new address. Changing the device's IP address on Security Cloud Control Firewall Management does not change device's configuration.

To change the IP address, Security Cloud Control uses to communicate with a device, follow this procedure:

Procedure

1. Choose **Security Devices**
2. Click the **Devices** tab to locate the device.
3. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required device.
4. Select the device whose IP address it is you want to change.
5. Above the **Device Details** pane, click the edit button next to the device's IP address.

6. Enter the new IP address in the field and click the blue check button.

   No change is made to the device itself, so the device's Configuration Status will continue to show that it is Synced.

Changing a device's name in Security Cloud Control Firewall Management

Learn how to use changing a device's IP address in Security Cloud Control Firewall Management.

All devices, models, templates, and services are given a name when they are onboarded or created in Security Cloud Control Firewall Management. You can change that name without changing the configuration of the device itself.

Procedure

1. Choose **Security Devices**.
2. Click the **Device** tab to locate the device.
3. Select the device whose name it is you want to change.
4. Above the **Device Details** pane, click the edit button next to the device's name.

5. Enter the new name in the field and click the blue check button.

   No change is made to the device itself, so the device's Configuration Status will continue to show that it is Synced.

Export a list of devices and services

Learn how to export a list of devices and services in Security Cloud Control Firewall Management.

This article explains how to export your list of devices and services to a comma-separated value (.csv) file. Once in that format, you can open the file in a spreadsheet application such as Microsoft Excel to sort and filter the items in your list.

The export button is available in both the Devices and Templates tab. You can also export details from devices under the selected device type tab.

Before you export your list of devices and services, look at the filter pane and determine if the **Security Devices** page is displaying the information you want to export. Clear all filters to view all managed devices and services, or apply filters to display a subset of your devices and services. The export function includes only the information currently displayed in the **Security Devices** page.

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab to export details from devices under that tab or click **All** to export details from all devices.

   You can use the filter and search functionalities to find the required device.
4. Click **Export list to CSV**.



5. If prompted, save the .csv file.
6. Open the .csv file in a spreadsheet application to sort and filter the results.

Export device configuration

Learn how to export device configuration in Security Cloud Control Firewall Management.

You can only export one device configuration at a time. Use the following procedure to export a device's configuration to a JSON file:

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.

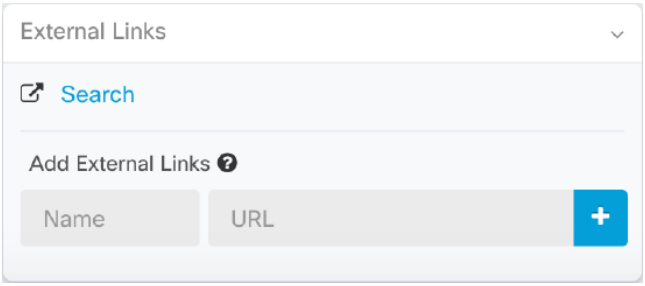
   You can use the filter and search functionalities to find the required device.
4. Select the device you want so it is highlighted.
5. In the **Actions** pane, select **Export Configuration**.

6. Select **Confirm** to save the configuration as a JSON file.

External links for devices

Learn about external links for devices in Security Cloud Control Firewall Management.

You can create a hyperlink to an external resource and associate it with a device you manage with Security Cloud Control. You could use this feature to create a convenient link to the local manager of one of your devices (). You could also use it to link to a search engine, documentation resource, a corporate wiki, or any other URL that you choose. You can associate as many external links with a device as you want. You can also associate the same link with multiple devices at the same time.



The links you create can reach anywhere, but your company's security requirements do not change. For example, if you ordinarily need to be connected to your corporate network, by being on-premises or through a VPN connection to reach a particular URL, those requirements remain. If your company blocks specific URLs, those URLs continue to be blocked. URLs that are not restricted continue to not be restricted.

Location Variable

We have created the {location} variable that you can incorporate in your URLs. This variable will be populated with the IP address of your device. For example,

```
https://{location}
```

.

Create an External Link from your Device

Learn how to create an external link from your device for the related settings, requirements, and user workflow.

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.
4. Select a device or model.

   You can use the filter and search functionalities to find the required device.
5. Enter a name for the link in the details pane under the **External Links** section.
6. Enter the URL for the link in the URL field. You need to specify the full URL. For example, for Cisco, enter http://www.cisco.com.

7. Click + to associate the link with the device.

Create an External Link to

Learn how to create an external link to asdm FDM. Here is a convenient way to open the Adaptive Security Device Manager (ASDM) of your ASA the Firepower Device Manager (FDM) of your FDM-managed.

Here is a convenient way to open , directly from Security Cloud Control.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required device.
4. Select a device or model.
5. In the details pane, on the right, go to the **External Links** section.
6. Enter a name for the link such as .
7. Enter https://{location} in the URL field. The {location} variable will be populated with the IP address of your device.
8. Click the + box.

Create an External Link for Multiple Devices

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required devices.
4. Select multiple devices or models.
5. In the details pane, on the right, go to the **External Links** section.
6. Enter a name for the link.
7. Enter the URL you want to reach using one of these methods:
   - Enter

     ```
     https://{location}
     ```

     in the URL field. The {location} variable will be populated with the IP address of your device. This creates an automatic link to the ASDM for your device.
   - Enter the URL for the link in the URL field. You need to specify the full URL, for example, for Cisco enter http://www.cisco.com.
8. Click + to associate the link with the device.

Edit or Delete External Links

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required device.

4. Select a device or model.
5. In the details pane, go to the **External Links** section.
6. Mouse-over the name of the link to reveal the edit and delete icons.
7. Click the appropriate icon to edit or delete the external link and confirm your action.

Edit or Delete External Links for Multiple Devices

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.

   You can use the filter and search functionalities to find the required devices.

4. Select multiple devices or models.
5. In the details pane, on the right, go to the **External Links** section.
6. Mouse-over the name of the link to reveal the edit and delete icons.
7. Click the appropriate icon to edit or delete the external link and confirm your action.

Bulk reconnect devices to Security Cloud Control Firewall Management

Learn how to bulk reconnect devices to Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management allows an administrator to attempt to reconnect more than one managed device to Security Cloud Control Firewall Management at the same time. When a device Security Cloud Control Firewall Management manages is marked "unreachable," Security Cloud Control Firewall Management can no longer detect out of band configuration changes or manage the device. There could be many different reasons for the disconnect. Attempting to reconnect the devices is a simple first step in restoring Security Cloud Control Firewall Management's management of the device.

> **Note**
>
> If you are reconnecting devices having new certificates, Security Cloud Control Firewall Management automatically reviews and accepts the new certificates on the devices and continues to reconnect with them. However, if you are reconnecting with only one device, Security Cloud Control Firewall Management prompts you to review and accept the certificate manually to continue to reconnect with it.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate devices.
3. Click the appropriate device type tab.

   Use the filter to look for devices whose connectivity status is "unreachable."
4. From the filtered results, select the devices you want to attempt to reconnect.
5. Click **Reconnect** . Notice that Security Cloud Control only provides command buttons for actions that can be applied to all the selected devices.
6. Look at the **notifications** tab for the progress of the bulk device reconnect action.

> **Tip**
>
> If a reconnect failure was caused because the device's certificate or credentials have changed, you will have to reconnect to those devices individually to add the new credentials and accept the new certificate.

Moving devices between organizations

Learn about moving devices between organizations in Security Cloud Control Firewall Management.

After onboarding devices to a Security Cloud Control Firewall Management organization, you cannot migrate the devices from one Security Cloud Control Firewall Management organization to another. If you want to move your devices to a new organization, you need to remove the devices from the old tenant and re-onboard them to the new organization.

Device certificate expiry detection

Learn about device certificate expiry detection in Security Cloud Control Firewall Management.

The management certificate is used for accessing FDM-managed and ASA devices from Security Cloud Control Firewall Management, while the Cisco Secure Client (formerly AnyConnect) is necessary for using virtual private network features on ASA, FDM-managed, and FTD devices from Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management actively monitors the expiration status of these certificates and notifies the user when these certificates are nearing their expiration date or have expired. This prevents any disruptions in device operations due to certificate expiry. You should renew the corresponding certificate to address this issue.

The management certificate expiry check applies to ASA and FDM-managed devices, while the Secure Client certificate expiry check applies to ASA, FDM-managed, and FTD devices.

View Certificate Expiry Notification

In the top right corner, click the **Notifications** () icon to view the most recent alerts that have occurred or affected the devices you have onboarded to your tenant. The **High Priority** section displays the certificate expiration notifications.

These notifications are sent 30, 14, and 7 days before the certificate expiration date and then every day thereafter until the certificate either expires or is renewed with a valid certificate. You can also subscribe to receive these notifications by email on the **Notification Settings** section of the user preferences page. For more information, see User Notification Preferences.

Write a device note

Learn how to write a device note in Security Cloud Control Firewall Management.

Use this procedure to create a single, plain-text, note file for a device.

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.
4. Select the device or model you want to create a note for.
5. In the **Management** pane on the right, click **Notes**. Notes.
6. Click the editor button on the right and select the Default text editor, Vim, or Emacs text editors.
7. Edit the Notes page.
8. Click **Save**.
   The note is saved in the tab.

Delete a device from Security Cloud Control Firewall Management

Learn how to delete a device from Security Cloud Control Firewall Management.

Follow these steps to delete a device from Security Cloud Control Firewall Management:

Procedure

1. Choose **Security Devices**.
2. Select the device you want to delete.
3. Click **Remove** in the **Device Actions** pane.
4. To confirm device removal, click **OK**.
   To keep the device onboarded, click **Cancel**.

Back up Firewall Threat Defense devices

Learn about backing up Firewall Threat Defense devices managed by Security Cloud Control Firewall Management.

To know how to back up Security Cloud Control-managed Firewall Threat Defense device types, use the following references:

Back Up Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center

- In the Security Cloud Control left pane, choose **Administration** > **Firewall Management Center**.
- Choose **Cloud-delivered FMC** under the **FMC** tab.
- Click **Devices** on the right pane to navigate to the Cloud-Delivered Firewall Management Center.
- Continue to follow the steps in Back Up a Threat Defense Device from Cloud-delivered Firewall Management Center.

Back Up Firewall Threat Defense devices managed by On-Premises Firewall Management Center onboarded to Security Cloud Control Firewall Management

- In the Security Cloud Control left pane, choose **Administration** > **Firewall Management Center**.
- Choose the On-Premises Firewall Management Center whose Firewall Threat Defense devices you want to back up.
- Click **FMC Cross Launch URL** on the right pane to navigate to the on-premises Firewall Management Center or manually log in to the on-premises Firewall Management Center.
- Continue to follow the steps in *Back up a Device from the Management Center* in the Cisco Secure Firewall Management Center Administration Guide.

Back up Firewall Threat Defense devices managed by Firewall Device Managers onboarded to Security Cloud Control Firewall Management

Follow the steps in Back up an FDM-managed Device.

Manage Firewall Threat Defense devices through Security Cloud Control Firewall Management

Learn how to manage Firewall Threat Defense devices through Security Cloud Control Firewall Management.

Before you begin

Security Cloud Control Firewall Management provides a unified interface to manage Firewall Threat Defense devices, both in hardware and virtual formats.

Firewall Threat Defense devices associated with these three management applications can be managed on the Security Cloud Control platform:

- Secure Firewall Device Manager
- Secure Firewall Management Center
- Secure Cloud-Delivered Firewall Management Center

Procedure

1. Log in to the Security Cloud Control platform.
2. In the left pane, click **Security Devices**.
3. Click the **FTD** tab.
4. Click  at the top-left corner.

   Under **Devices/Services**, the filter pane provides filters that display Firewall Threat Defense devices based on the management application through which they are accessed from Security Cloud Control.

   - **FDM**: Firewall Threat Defense device managed by Firewall Device Manager
   - **FMC-FTD**: Firewall Threat Defense devices managed by Firewall Management Center
   - **FTD**: Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center
5. To view the Firewall Threat Defense devices under a management application, check the corresponding check box.

Security devices overview

Learn how to view onboarded devices and templates on the Security Devices page in Security Cloud Control, apply filters, and identify devices nearing hardware end-of-life for support planning and reporting.

The **Security Devices** page displays all the physical and virtual onboarded devices and the templates created from the onboarded devices. The page classifies devices and templates based on their type and displays them in the corresponding tabs dedicated to each device type.

You can view the following details on the **Security Devices** page:

- The **Devices** tab displays all the live devices that are onboarded to Security Cloud Control.
- The **Templates** tab displays all the template devices created from live devices or configuration files imported to Security Cloud Control.

Filters in security devices

The **Filter** panel on the **Security Devices** page provides multiple options to narrow down results and find devices based on specific attributes, including **Devices/Services, Hardware Versions, Device End-of-Life, Software Versions, Snort Version, Configuration Status, Connectivity States, Conflict Detection, Health Status, Secure Device Connectors, and Labels**.

The Hardware End-of-Life (EoL) Filter

The **Hardware End-of-Life (EoL) filter** allows you to identify devices that are nearing or have reached their last day of hardware support. Running unsupported hardware may pose operational and security risks because Cisco no longer provides software updates, security patches, or technical support after the EoL date.

> **Note**
>
> The Hardware EoL filter currently supports Firewall Threat Defense devices managed by on-premises Firewall Management Center and Cloud-Delivered Firewall Management Center, and ASA devices.

Procedure

1. In the **Devices** tab, click the filter icon.
2. From the list of available filters, under **Device End-of-Life**, select **Hardware End-of-Life**.

   The list now displays all devices that are approaching or have reached their hardware end-of-life.
3. Select a device to view more information on the right pane.
4. Scroll down to the **Device End of Life** section to view the following details:
   - The exact end-of-life date.
   - Remaining time until the last day of support.
5. Click **Know more**.

   You can view a detailed page that provides the following information:
   - Cisco's recommended replacement devices with product specifications, along with links to view the official data sheets.
   - Guidance on submitting a request through the Contact Cisco page and options to connect directly with Cisco experts.
   - Information on Cisco's product recycling program.
6. Click **Export** to download the device report in CSV format for offline analysis.

Security Cloud Control Firewall Management labels and filtering

Learn how to use Security Cloud Control Firewall Management labels to group devices and objects, create label groups, and filter device or object tables by assigned labels.

Labels are used for grouping devices or objects. You can apply labels to one or more devices during onboarding or any time after onboarding. You can apply labels to objects after creating them. Once you apply labels to devices and objects, you can filter the contents of the device table or objects table using the corresponding label.

> **Note**
>
> A label that is applied to a device is not extended to its associated objects, and a label applied to a shared object is not extended to its associated objects.

You can create a label group by using the syntax group name:label, for example, Region:East or Region:West. If you create these two labels, the group label would be Region and you could choose from East or West in that group.

Apply Labels to Devices and Objects

To apply a label to devices, perform these steps:

Procedure

1. In the left pane, click **Security Devices**.
2. In the left pane, click **Objects**.
3. Click the **Devices** tab to locate a device or the **Templates** tab to locate the model device.

4. Click the appropriate device type tab.
5. Select one or more devices.
6. In the **Add Groups and Labels** field on the right, specify a label for the devices.
7. Click the + icon.

Filters on security devices, policies, and objects page

Learn how to filter devices, policies, and objects by attributes such as device type, status, version, connector, management application, and labels.

Use filters on the **Security Devices**, **Policies**, and **Objects** pages to find devices and objects. To filter, select the filter icon in the left pane.

On the **Security Devices** page, the filter panel lets you filter devices by criteria such as device type, hardware version, software version, Snort version, configuration status, connection state, conflict detection, Secure Device Connector, and labels. You can apply filters within the selected device type tab.

When the **FTD** tab is open, the filter panel also lets you filter FTD devices by the management application that Security Cloud Control uses to access them.

To filter, click in the left-hand pane of the Security Devices, Policies, and Objects tabs.

Note

When the **FTD** tab is opened, the filter pane provides filters to show FDM-managed devices based on the management application through which the devices are accessed from Security Cloud Control.

- FDM: Devices managed using FTD API or Firewall Device Manager.
- FMC-FTD: Devices managed using Firepower Management Center.
- FTD: Devices managed using FTD Management.

Use Security Cloud Control Firewall Management search functionality

Learn how to search in Security Cloud Control Firewall Management using page-level search and global search to find devices, policies, objects, VPN entries, change logs, and jobs across your tenant.

The Security Cloud Control Firewall Management platform has a highly efficient search function that makes it easy to find anything you need. The search bar on each page is tailored to the content of that page, while the global search allows for a comprehensive search across the entire tenant. This saves time and effort, as you can quickly locate the necessary information.

Page Level Search

The page-level search enables you to search specific items on the Security Devices, Policies, Objects, VPN, Change Log, and Jobs pages.

- In the **Security Devices** space, you can simply start typing in the search bar, and devices that fit the search criteria will be displayed. You can type any partial part name of the device, IP address, or the serial number of the physical device to find the device.

- In the **Policies** space, you can search policies by their name, components or objects used in them.
- In the **Objects** space, you can search for an object by typing any partial part of the name of the object, or partial IP Address, port, or protocols.
- In the **VPN** space, you can search by tunnel name, device name, and IP address used in the VPN policies.
- In the **Change log** space, you can search logs based on events, device names, or actions.

Procedure

1. Navigate to the search bar near the top of the interface.
2. Type the search criteria into the Search Bar and the corresponding results will be displayed.

Global Search

Global search in Security Cloud Control provides a centralized way to quickly locate and navigate to onboarded devices, objects, and policies.

The global search feature allows you to quickly locate and navigate to devices managed by Security Cloud Control.

All search results are based on the indexing option you choose. These are the indexing options:

- Full Indexing–Requires that you invoke the full indexing process. This process scans all the devices and objects in the system and displays them in the search index only after you invoke the indexing. To invoke full indexing, you must have administrative privileges.

  For more information, see Initiate Full Indexing on page 96.
- Incremental Indexing–An event-based indexing process where the search index automatically updates each time that a device or an object is added, modified, or deleted.

The information that you enter in the search field is not case-sensitive. You can perform a global search using these entities:

- Device Name–Supports partial device names, URL, IP address, or range.
- Object Types–Supports object name, object descriptions, and configured values.
- Policy Types–Supports policy name, policy description, rule name, and rule comments.

  Cloud-Delivered Firewall Management Center and on-premises Firewall Management Center managed in Security Cloud Control support the following policy types:

  - Access Control Policy
  - Prefilter Policy
  - Threat Defense NAT Policy

When you type a search expression, the interface begins to display search results and you do not need to press *Enter* to execute a search.

The search results display all devices and objects that match your search terms. If your search term matches more than one device or object, the results appear under categories such as devices, objects, and connected_fmc.

By default, the first item in the search result is highlighted and the related information for that item appears in the right pane. You can scroll through the search results and click any item to view the corresponding information. You can click the arrow icon besides the item to navigate to the corresponding page.

Note

- Global search does not display duplicate search results. For objects, the unique identifier of the shared object is used to navigate to the Object view.
- If you delete a device from Security Cloud Control, all associated objects are removed from the global search index.
- If you delete an object from the policy and retain the device before you initiate full indexing, the object remains in the global search index because it is associated with the device.

Initiate Full Indexing

Procedure to initiate full indexing for global search.

Procedure

1. In the left pane, click **Administration** > **General Settings**.
2. In Global Search, click **Initiate Full Indexing** to trigger indexing.



Note

Initiating full indexing clears existing indexing of the Security Cloud Control tenant.

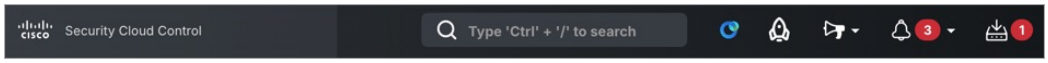
3. Click **here** to view the global search workflow.

Perform a Global Search

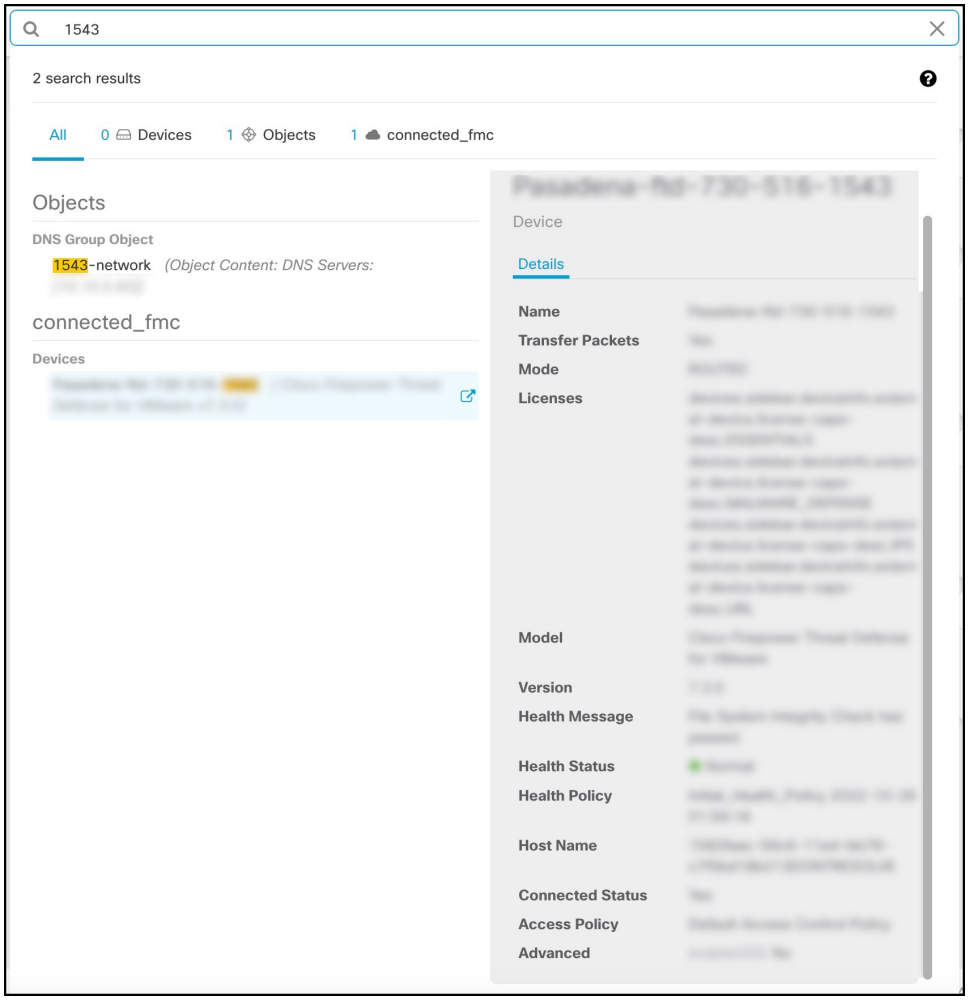
Procedure

1. Log into Security Cloud Control.
2. Click the search icon in the Security Cloud Control page and enter the search strings in the search field that appears.

   Alternatively, you can press and hold the **Ctrl** key and the **/** key simultaneously on Windows, or the **Command** key and **/** key on Mac, to open the search bar.



   The search results display a list of possible items as you begin entering the search strings. The search results appear under four categories: All, Devices, Objects, Policies, and Cloud-Delivered Firewall Management Center. The right pane displays information for a selected search result.



3. From the search result, select a device or an object, and click the arrow icon to navigate from the search results to the corresponding device and object page. From the search result, select an item, and click the arrow icon to navigate from the search results to the corresponding page.

> **Note**
>
> Selecting a search result for devices in the Cloud-Delivered Firewall Management Center, allows you to navigate to the Cloud-Delivered Firewall Management Center user interface within Security Cloud Control.
>
> For information on Cloud-Delivered Firewall Management Center, see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control.

4. Click **X** to close the search bar.

8 Configuring On-Premises Firewall Management Center Devices

Topics:

- View onboarded On-Premises Firewall Management Center
- Troubleshoot cloud region synchronization issue in On-Premises Firewall Management Center high availability
- Discover and manage On-Premises Firewall Management Center network objects
- Object filters
- Enable AgenticOps insights

This chapter covers the following sections:

View onboarded On-Premises Firewall Management Center

This concept explains how to view and manage onboarded On-Premises Firewall Management Centers, including high-availability pairs, and cross-launch directly to the active or specific management center node using customizable URLs in Security Cloud Control Firewall Management.

To view onboarded On-Premises Firewall Management Centers, perform these steps:

1. Choose **Administration** > **Integrations** > **Firewall Management Center**.
2. Click the **FMC** tab.

View On-Premises Firewall Management Center high-availability pair

The high-availability pair is displayed in the **Services** page. When you expand the pair, you can see the primary and secondary on-premises Firewall Management Center nodes and their current statuses.

To cross-launch the active on-premises Firewall Management Center, perform these steps:

1. In the **Services** page, check the corresponding high-availability pair.
2. Click the option you want to open in on-premises Firewall Management Center.

   The **Verify FMC Cross Launch URL** window is displayed. By default, the public IP address or FQDN of the currently active on-premises Firewall Management Center is shown and will be used to open on-premises Firewall Management Center. If necessary, specify the URL of the standby on-premises Firewall Management Center to launch it.

Add cross-launch URLs to each on-premises Firewall Management Center node. When you launch from the pair, only the active node is launches. Verifying which node is currently active is not necessary.

To cross-launch to a specific on-premises Firewall Management Center node, perform these steps:

1. Expand the high-availability pair and click primary or secondary on-premises Firewall Management Center node you want to launch.
2. In the **External Links** pane, click **FMC Cross Launch URL** to cross-launch the selected on-premises Firewall Management Center.

   To update the public IP address or the FQDN and the port number of your on-premises Firewall Management Center hover over the **FMC Cross Launch URL** and click the edit icon.

> **Note**
>
> If high availability is broken or roles are switched on on-premises Firewall Management Center (version 7.4.x or earlier), disable the SecureX integration, then enable it again on the secondary on-premises Firewall Management Center. To complete this task, navigate to the secondary on-premises Firewall Management Center and choose the appropriate option.
>
> If you break a high-availability on-premises Firewall Management Center pair, the participating management centers become two standalone on-premises Firewall Management Centers.

Troubleshoot cloud region synchronization issue in On-Premises Firewall Management Center high availability

This collection guides users in resolving On-Premises Firewall Management Center cloud integration issues after high availability (HA) switchover, helping identify symptoms, understand applicability, and restore connectivity for non-U.S. region integrations without affecting device configurations or policies.

Issue

When an On-Premises Firewall Management Center high-availability (HA) pair that is integrated with Security Cloud Control in a non-US region experiences a switchover, cloud connectivity issues occur:

- The newly active On-Premises Firewall Management Center automatically connects to the U.S. Region (default) instead of the originally configured non-US region.
- The **Tenant** field displays **None** instead of showing the configured tenant.
- Cloud integration errors prevent proper connectivity to Security Cloud Control.

Example scenario

Initial configuration

- On-Premises Firewall Management Center HA pair configured to connect to Security Cloud Control in the EU (Europe) region
- On-Premises Firewall Management Center primary: Active
- On-Premises Firewall Management Center secondary: Standby

After switchover event

- On-Premises Firewall Management Center primary experiences a failure
- On-Premises Firewall Management Center secondary becomes the new active unit
- On-Premises Firewall Management Center secondary (now active) automatically connects to the U.S. region (default) instead of the EU region
- **Tenant** field displays **None**

Note

- If the On-Premises Firewall Management Center HA pair is integrated with the U.S. region in Security Cloud Control, this procedure is not required.
- The switchover does not affect Firewall Threat Defense device configurations, security policies, or any other On-Premises Firewall Management Center settings.
- This procedure only restores cloud connectivity and does not require redeployment of policies to managed devices.

Problem cause

Cloud region and tenant configuration settings do not automatically synchronize from the active On-Premises Firewall Management Center to the standby On-Premises Firewall Management Center in an HA pair. During a switchover, the standby unit becomes active. However, it resets to the default (U.S. region) rather than retaining your previously configured region.

Solution

To restore cloud connectivity after failover, complete these steps on the newly active On-Premises Firewall Management Center:

1. Log in to the On-Premises Firewall Management Center that is active after a switchover.
2. Choose **Integrations > Security Cloud Control**.

   The **Current Cloud Region** drop-down list is configured to the **US Region**.
3. Click **Disable Security Cloud Control**.
4. Click **Save**.
5. From the **Current Cloud Region** drop-down list, choose the same region that was configured in the previous active On-Premises Firewall Management Center.
6. Click **Enable Security Cloud Control**.
7. Click **Save**.

Discover and manage On-Premises Firewall Management Center network objects

This topic helps you enable the discover and manage objects feature for on-premises Firewall Management Centers managed by Security Cloud Control.

If you have an on-premises Firewall Management Center that you manage using Security Cloud Control and you want to share and manage its objects, perform this procedure:

Procedure

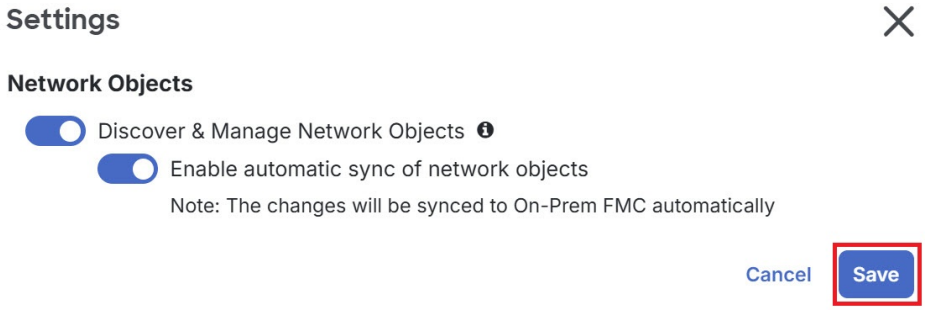
1. Choose **Administration** > **Integrations** > **Firewall Management Center** to view the **Services** page.
2. If you have already onboarded an on-premises Firewall Management Center to Security Cloud Control, select it.

   If you want to onboard a new on-premises Firewall Management Center, see Onboard an On-Prem Firewall Management Center.

3. Choose **Settings** from the **Actions** pane. The **Actions** pane does not appear when you select more than one on-premises Firewall Management Center.

> **Note**
>
> You must be an admin or super admin to use **Settings**.

4. Enable the **Discover & Manage Network Objects** toggle button. To automatically synchronize your changes with on-premises Firewall Management Center instead of staging them for review, turn on the **Enable automatic sync of network objects** toggle button. Then, click **Save**.



> **Note**
>
> - You cannot enable the **Discover & Manage Network Objects** toggle button if the selected on-premises Firewall Management Center has one or more child domains or if it has the Change Management workflow enabled.
> - You cannot enable the **Enable automatic sync of network objects** toggle button if the **Discover & Manage Network Objects** toggle button is disabled.

For every new on-premises Firewall Management Center onboarded to Security Cloud Control, this toggle button needs to be enabled manually. After you enable this option, Security Cloud Control discovers objects from your on-premises Firewall Management Center. You can then share and manage these objects, and use them to set consistent object definitions across other platforms managed by Security Cloud Control.

In Security Cloud Control, when you add overrides to objects that are discovered from an on-premises Firewall Management Center and push the changes back, these objects can now be overridden, even if overrides were not allowed previously. The **Allow Overrides** check box in the **View Network Object** window is selected automatically when an override is added from Security Cloud Control.

> **Note**
>
> If you want to assign already-existing objects in Security Cloud Control to your on-premises Firewall Management Center, choose the on-premises Firewall Management Center and click **Assign Objects** from the **Actions** pane.

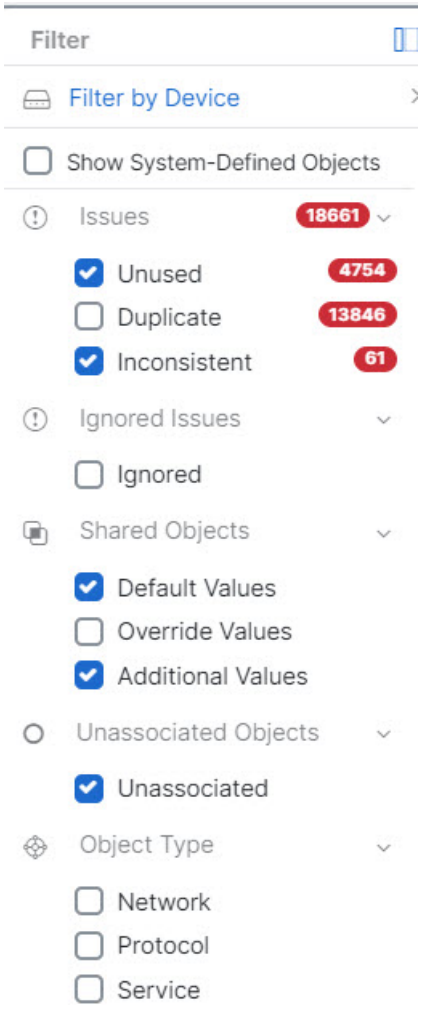
Object filters

Learn how to filter objects in Security Cloud Control by device, issue, shared state, association state, object type, system-defined status, and search value to find targeted object results.

Use filters on the **Objects** page to find objects by device, issue, shared state, association state, object type, or search value. You can also include or exclude system-defined objects.

The object type filter lets you filter by object types such as network object, network group, URL object, URL group, service object, and service group. The shared objects filter lets you filter objects that have default values, override values, or additional values.

You can combine device and object filters to create focused search strategies. For example, you can search for objects that match this logic: **Issues** is **Unused** OR **Inconsistent**, AND **Shared Objects** has **Default Values** OR **Additional Values**, AND **Unassociated Objects** is selected.



To filter, click in the left-hand pane of the Objects tab:

- **Filter by Device**: Shows objects found on selected devices.
- **Show System-Defined Objects**: Includes predefined system objects in search and filter results. System objects cannot be edited or deleted. Some devices come with predefined objects for common services. These system objects are convenient because they are already made for you and you can use them in your rules and policies. There can be many system objects in the objects table. System objects cannot be edited or deleted.

- **Issues**: Shows unused, duplicate, or inconsistent objects. If you select more than one issue, objects in any selected issue category are included.
- **Ignored Issues**: Shows objects whose issues were ignored by an administrator.
- **Shared Objects**: Shows shared objects. You can filter by default values, override values, additional values, or a combination.
- **Unassociated Objects**: Shows objects that are not associated with any rule or policy.
- **Object Type**: Shows selected object types, such as network objects, network groups, URL objects, URL groups, service objects, and service groups.

Within a main filter, subfilters can further narrow the results by object type, such as Network, Service, or Protocol. Filters across categories combine with an AND relationship. Multiple selections within a category can combine with an OR relationship.

For example, a filter set can search for objects that match this logic: objects on selected devices AND inconsistent objects AND network objects or service objects AND object names that contain **group**.

Enable AgenticOps insights

Enable AgenticOps Insights to start onboarding your organization and unlock AI-driven insights, recommendations, and planning tools for your firewall environment. After onboarding, AgenticOps begins analyzing data to help improve performance, security, and operational efficiency.

To take advantage of AgenticOps' benefits, you must enable AgenticOps insights. You must have **Super Admin** or **Admin** user roles to enable **AgenticOps Insights** in your tenant.

Procedure

1. In the left pane, click **Insights & Reports** > **Settings**.
2. Select **Confirm AgenticOps activation**, and click **Get Started**.
3. Review the available AgenticOps features for each detected Firewall Management Center. The page displays the supported AgenticOps features, software version, and the number of managed devices for each Firewall Management Center. Click **Setup AgenticOps**.
4. Click **Confirm Onboard**.

   The onboarding process begins, and it takes a few minutes to fetch the data that is required to provide the insights. When completed, the **AgenticOps** > **summary** page is displayed.

9 Policy Analyzer and Optimizer

Topics:

- About Policy Analyzer and Optimizer
- Common Policy Analyzer and Optimizer concepts
- Prerequisites to use Policy Analyzer and Optimizer
- Enable Policy Analyzer and Optimizer for Security Cloud Control-managed On-Premises Firewall Management Center
- Policy Analyzer and Optimizer licensing requirements
- Open Policy Analyzer and Optimizer and select a data source
- Search and filter policies in Policy Analyzer and Optimizer
- Access control policy analysis and optimization
- Network Address Translation policy analysis
- Troubleshooting Policy Analyzer and Optimizer
- Frequently Asked Questions About Policy Analyzer and Optimizer

Security Cloud Control provides the Policy Analyzer and Optimizer, which is an intelligent cloud service that can analyze security policies, detect anomalies, and provide recommendations on remediations that can be performed to optimize the policies.

Security Cloud Control provides the Policy Analyzer and Optimizer, which is an intelligent cloud service that can analyze security policies, detect anomalies, and provide recommendations on remediations that can be performed to optimize the policies.

About Policy Analyzer and Optimizer

Learn how Policy Analyzer and Optimizer in Security Cloud Control Firewall Management analyzes access control and NAT policies, identifies rule anomalies, reports optimization opportunities, and supports remediation where available.

AgenticOps for firewalls provides operational insights and tools that help improve firewall management, policy hygiene, and deployment readiness. One such capability is Policy Analyzer and Optimizer, which uses an algorithmic approach to evaluate firewall policy rules and identify anomalies such as duplicate, shadowed, redundant, or otherwise optimizable rules. For more information, refer to AgenticOpsInsights to know more about the various other functionalities that AgenticOps provides.

Secure Firewall Threat Defense devices with extensive policies may have numerous duplicate or shadowed rules. Such large policies with unoptimized rulesets can lead to excessive consumption of device memory, delayed loading of rules, and long search duration, resulting in inefficient security policy enforcement, reduced network speeds, and extended deployment durations.

Policy Analyzer and Optimizer is an intelligent Security Cloud Control Firewall Management service that analyzes firewall policies, detects rule anomalies, and helps you understand where a policy can be optimized. Policy Analyzer and Optimizer supports access control policies policies for Cloud-Delivered Firewall Management Center and supported Security Cloud Control-managed On-Premises Firewall Management Center data sources.

In addition, Policy Analyzer and Optimizer can do the following:

- View policy health and optimization opportunities for the selected management center data source.
- Analyze policies on demand or rely on scheduled analysis that runs every 24 hours.
- Download analysis reports as PDFs after analysis completes.
- Use Access Control Policy Analyzer and Optimizer remediation workflows where supported.
- Stage and apply remediation for an entire anomaly category, selected observations, or individual rules within supported observations.
- Use Network Address Translation Policy Analyzer and Optimizer findings and AgenticOps insights to investigate NAT policies that contain optimizable rules.

Supported policy types

Security Cloud Control Firewall Management performs anomaly analysis on the following policy types:

Table 3: Supported policy types for Policy Analyzer and Optimizer

Policy type	Use this section when	Current scope
Access control policy	You want to analyze access control policies, review access control findings, and apply supported remediations.	Analysis, remediation, reporting, remediation history, and policy insights.
Network address translation policy	You want to analyze NAT policies for shadowed and redundant NAT rules.	Analysis and reporting for fully shadowed and fully redundant NAT rules. NAT remediation is not available in this release.

Common Policy Analyzer and Optimizer concepts

Find details about common Policy Analyzer and Optimizer concepts. Policy Analyzer and Optimizer uses these shared concepts across access control policy analysis and NAT policy analysis.

Policy Analyzer and Optimizer uses these shared concepts across access control policy analysis and NAT policy analysis.

Table 4: Common Policy Analyzer and Optimizer concepts

Concept	Common behavior	Policy-type difference
Data source	A Cloud-Delivered Firewall Management Center or an On-Premises Firewall Management Center selected in Policy Analyzer and Optimizer.	The Access Control tab can be used for supported On-Premises Firewall Management Center data sources. The Network Address Translation tab is available only when Network Address Translation Policy Analyzer and Optimizer is enabled through AgenticOps for the selected data source.
Sync	Fetches current policy inventory and metadata, including newly created, deleted, or modified policies.	Sync does not, by itself, create a new analysis summary. If the policy changed after the last analysis, run analysis again or wait for scheduled analysis.
Analysis	Evaluates selected policies and produces policy health information, observations, and report data.	Access control Policy Analyzer and Optimizer evaluates access control rule and object findings. Network Address Translation Policy Analyzer and Optimizer evaluates NAT rule shadowing and redundancy.
Reporting	Provides a downloadable analysis report after analysis completes.	Access control Policy Analyzer and Optimizer also provides remediation reports after supported remediation is applied.

Concept	Common behavior	Policy-type difference
Remediation	A workflow that stages selected changes and applies them only when you select Apply Remediation.	Available for access control policies. Network Address Translation Policy Analyzer and Optimizer does not provide an Apply Remediation workflow. You can stage remediation for an entire anomaly category, selected observations within a category, or individual rules within an expanded observation. You can also select individual rules within an expanded observation. Using the suggested remediations, you can disable or delete selected Duplicate Rules and Expired Rules, remove selected fully overlapped objects from rules, and merge selected Mergeable Rules.

Prerequisites to use Policy Analyzer and Optimizer

Before you use Policy Analyzer and Optimizer, verify the prerequisites that apply to your policy type and data source.

Before you use Policy Analyzer and Optimizer, verify the prerequisites that apply to your policy type and data source.

- The On-Premises Firewall Management Center must be integrated with Security Cloud Control.

> **Note**
>
> In the On-Premises Firewall Management Center, navigate to **Integration > Cisco Security Cloud** and check the **Enable Policy Analysis & Optimization** checkbox after integrating with the Cisco Security Cloud.

Prerequisites to use Policy Analyzer and Optimizer for access control policy

- Access control policy analysis is supported on the On-Premises Firewall Management Center operating on Version 7.2 or later. The Cisco-recommended Version is 7.6 or later, because these versions support cross-launch to Policy Analyzer and Optimizer directly from On-Premises Firewall Management Center.
- Access control policy to be analyzed must be associated with a Firewall Threat Defense device that is managed by an On-Premises Firewall Management Center integrated with Security Cloud Control.

Prerequisites to use Policy Analyzer and Optimizer for Network Address Translation

- NAT policy analysis is supported on the On-Premises Firewall Management Center operating on Version 7.6 or later.
- Network Address Translation Policy Analyzer and Optimizer availability also depends on AgenticOps being enabled for the selected tenant and data source. For more information, refer to Enable AgenticOps Insights.

- Enable AgenticOps for the Cloud-Delivered Firewall Management Center or On-Premises Firewall Management Center data source that you want to analyze. Choose **Insights & Reports** > **Settings** > **Policy Analyzer and Optimizer** > **Data Sources** and enable AgenticOps for the management center you want.

> **Note**
>
> If an On-Premises Firewall Management Center is running a version earlier than 7.6, access control Policy Analyzer and Optimizer may still be available for analyzing access control policy, but Network Address Translation Policy Analyzer and Optimizer is not available for that data source.

Enable Policy Analyzer and Optimizer for Security Cloud Control-managed On-Premises Firewall Management Center

Onboard your On-Premises Firewall Management Center to Security Cloud Control, navigate to Administration > Integrations > Firewall Management Center, select the On-Premises Firewall Management Center, and choose Policy Analyzer and Optimizer under System in the right pane.

Onboard your On-Premises Firewall Management Center to Security Cloud Control, navigate to **Administration** > **Integrations** > **Firewall Management Center**, select the On-Premises Firewall Management Center, and choose **Policy Analyzer and Optimizer** under **System** in the right pane. See Onboard an On-Premises Firewall Management Center for more information.

If you have an On-Premises Firewall Management Center Version 7.6 and want to use Policy Analyzer and Optimizer, follow the steps below:

Procedure

1. In your On-Premises Firewall Management Center, navigate **Integration** > **Security Cloud Control**.
2. If you have not integrated your On-Premises Firewall Management Center with Cisco Security Cloud, click **Enable Security Cloud Control** and follow the steps. To authorize the cloud integration, you must choose an existing Security Cloud Control tenant or provision a new one, to which your on-premises Firewall Management Center will get onboarded, after the cloud integration is successful.
3. After integrating your On-Premises Firewall Management Center with Security Cloud Control, check the **Enable Policy Analyzer and Optimizer** checkbox and click **Save**.

Policy Analyzer and Optimizer licensing requirements

Policy Analyzer and Optimizer requires no additional licensing.

Policy Analyzer and Optimizer requires no additional licensing. It comes as part of the Security Cloud Control Firewall Management base subscription.

Open Policy Analyzer and Optimizer and select a data source

You can open Policy Analyzer and Optimizer from Security Cloud Control Firewall Management or cross-launch from supported On-Premises Firewall Management Center policy pages.

You can open Policy Analyzer and Optimizer from Security Cloud Control Firewall Management or cross-launch from supported On-Premises Firewall Management Center policy pages.

Follow these steps to open Policy Analyzer and Optimizer and select a data source:

Procedure

1. In the Security Cloud Control Firewall Management left pane, choose **Administration** > **Integrations** > **Firewall Management Center**.
2. Select **Cloud-Delivered FMC** or an On-Premises Firewall Management Center.
3. Click Policy Analyzer and Optimizer under **System**.

   Note

   Alternatively, choose **Insights & Reports** > **Policy Analyzer and Optimizer**.

4. Use the data source selector at the top of the Policy Analyzer and Optimizer page to choose the Cloud-Delivered Firewall Management Center or On-Premises Firewall Management Center whose policies you want to review.
5. Choose the **Access Control** tab depending on the policy type that you want to analyze.

   Note

   If the selected data source is not enabled for AgenticOps, the **Network address translation** tab shows a message indicating that the NAT Policy Analyzer and Optimizer require AgenticOps for the selected data source. However, you can still utilize the access control Policy Analyzer and Optimizer if the access control prerequisites are met.

Sync and analysis behavior

Policy Analyzer and Optimizer displays policy metadata, including analysis status, last modified time, and last analyzed time. Last modified reflects changes made to the policy in the management center that manages it. Last analyzed reflects the analysis run that produced the current Policy Analyzer and Optimizer summary.

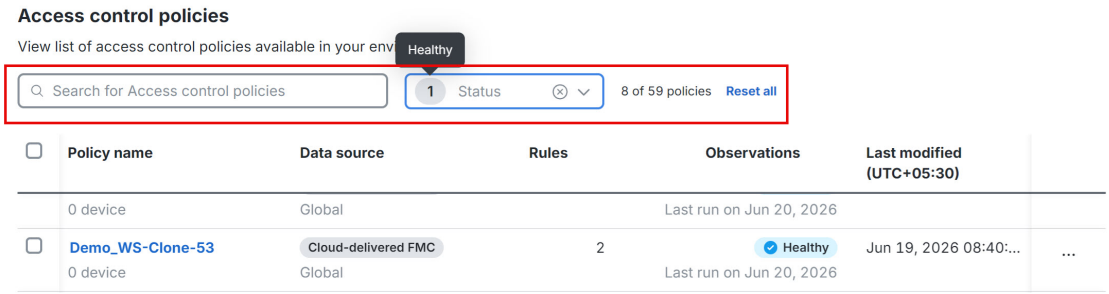
Use **Sync with FMC** to fetch the latest access control and NAT policy inventories and modified timestamps from the management center. Each Policy Analyzer and Optimizer tab shows the sync success or failure status for the policy type on that tab. If a policy was modified after the last analysis, the displayed analysis can be out of date until you run analysis again or a scheduled analysis runs.

Search and filter policies in Policy Analyzer and Optimizer

Use the Search for access control policies field and the Status field to narrow the access control policy list.

Use the **Search for access control policies** field and the **Status** field to narrow the access control policy list.

Search helps you find a policy by name. Status filtering helps you find policies by analysis state, such a **Healthy**, **Error**, **In progress**, **Analysis pending**, **Optimizable**, or **Analysis out of date**.



- **Search for access control policies**: Finds access control policies that match the policy name you enter.
- **Status**: Filters access control policies by their current analysis state.

Access control policy analysis and optimization

Learn how to analyze access control policies in Policy Analyzer and Optimizer, review findings, and apply supported remediations for access control rules and objects.

Use the **Access Control** tab when you want to analyze access control policies, review access control policy findings, and apply the remediations that Policy Analyzer and Optimizer supports for access control rules and objects.

After provisioning a Cloud-Delivered Firewall Management Center or onboarding an On-Premises Firewall Management Center to your Security Cloud Control Firewall Management tenant and creating policies, you can start analyzing them using the Policy Analyzer and Optimizer.

For more information, refer to Onboard an On-Premises Firewall Management Center and Enable Cloud-Delivered Firewall Management Center on Your Security Cloud Control.

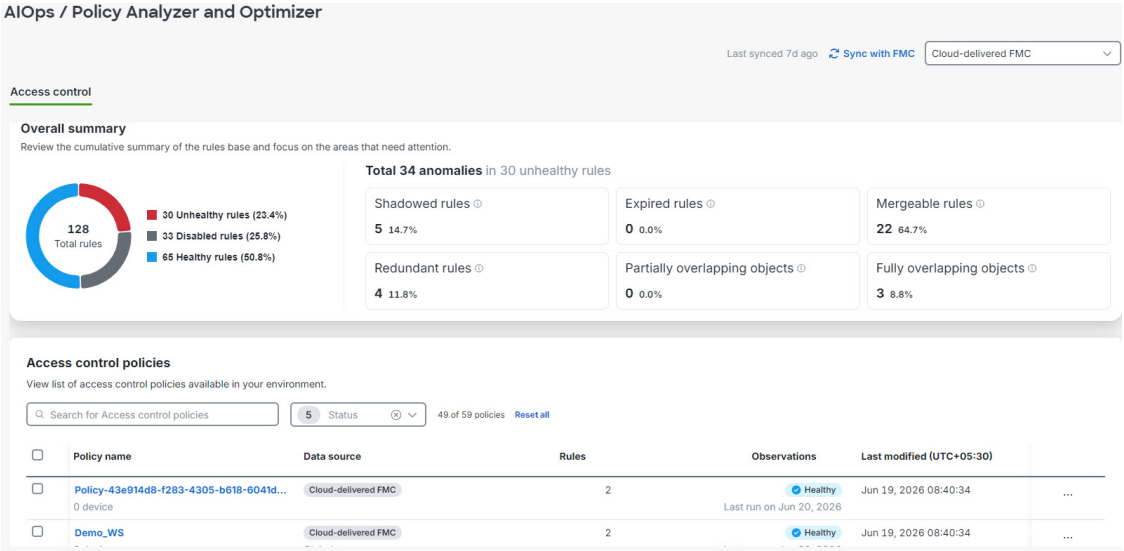
Analyze access control policies

Use this procedure to assess an access control policy before making changes, review policy health, or re-run analysis after policy updates. If a policy has not been analyzed, you can start a new analysis. If the analysis is out of date, you can re-analyze the policy to refresh the results.

> **Note**
>
> When you create a new policy, it might take a while for the Policy Analyzer and Optimizer to fetch the policy details and show up on the **Policy Analyzer and Optimizer**. Click the refresh ( ) button on the top-right corner to manually refresh the page to see new policies.

Procedure

1. Choose **Insights & Reports** > **Policy Analyzer and Optimizer**.



2. In the right pane, select **Cloud-delivered FMC** or an On-Premises Firewall Management Center from the drop-down list as the data source whose policies you wish to analyze.
3. In the **Access Control** area, select the policy you want to analyze or review.

> **Note**
>
> - For an unanalyzed policy, click on **Analyze Policies**.
> - If the policy status indicates **Analysis out of date**, click on **Re-analyze Policy** under **Analysis Actions** on the right.

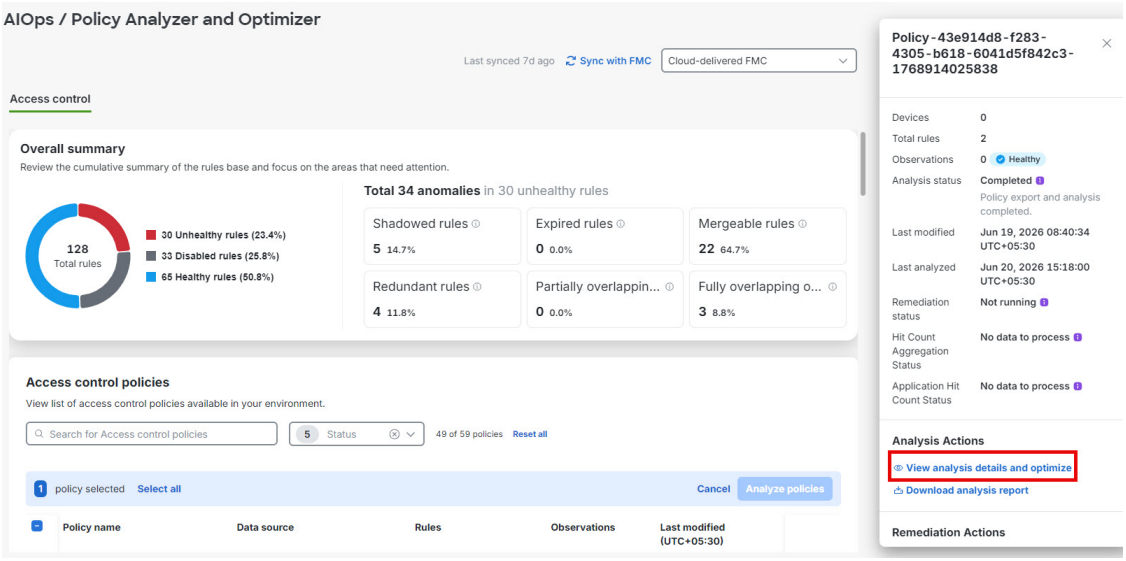
The **Overall summary** section displays the total number of rules categorized by their health status: healthy, disabled, or unhealthy, for the selected management center (Cloud-Delivered Firewall Management Center or On-Premises Firewall Management Center).

The dashboard also highlights specific anomalies within your unhealthy rules. You can review the count and percentage for the categories: Shadowed rules, Expired rules, Mergeable rules, Redundant rules, Partially overlapping rules, Fully overlapping objects.

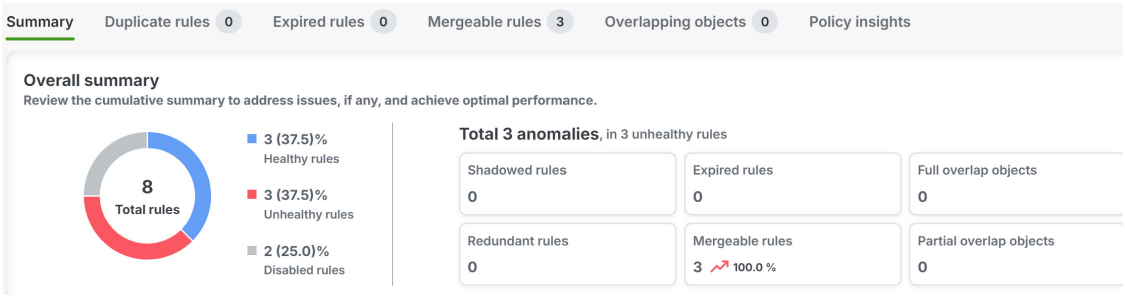
Access control policy analysis summary

When analysis completes, select an access control policy to review the right-pane summary and click **View analysis details and optimize**.

Alternatively, you can click the ellipse button associated with a policy and select **View details** to see the right-pane summary.



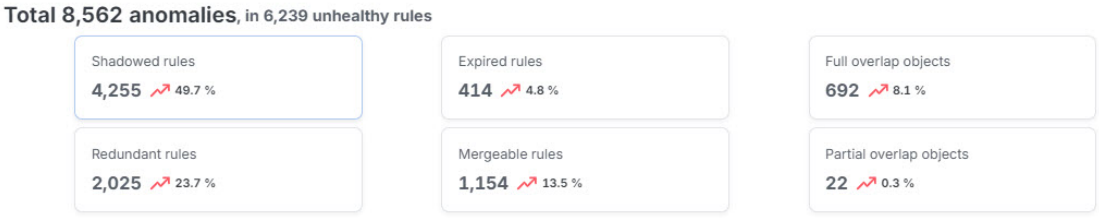
Overall summary–provides insights on how many rules are healthy, disabled, expired, and contain anomalies, using a pie chart for the selected access control policy. You can also hover over the part of the pie to view the percentage of rules.



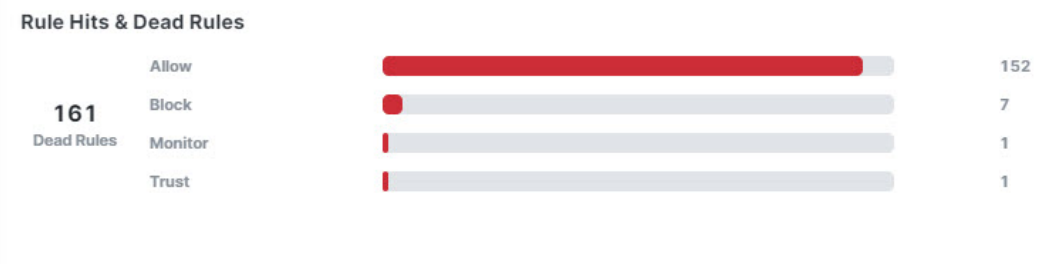
Rule usage history–shows how recently rules were used, with time periods.



Rules with Anomalies–provides insights on how many rules have anomalies.



Hits rules & dead rules–provides insights on hitcount of expired rules, for rule types including allow, block, monitor, and trust.

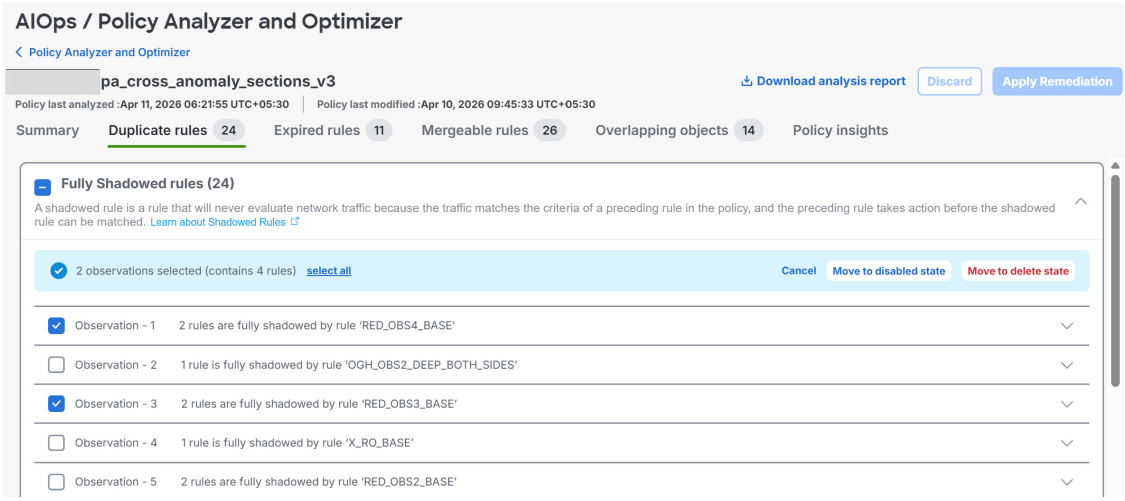


In remediation tabs such as **Duplicate rules**, **Expired rules**, **Mergeable rules**, **Overlapping objects**, and **Policy insights** you can select the check box next to a category to stage all observations in that category, or expand the category and select specific observations or rules. Available actions depend on the anomaly type.

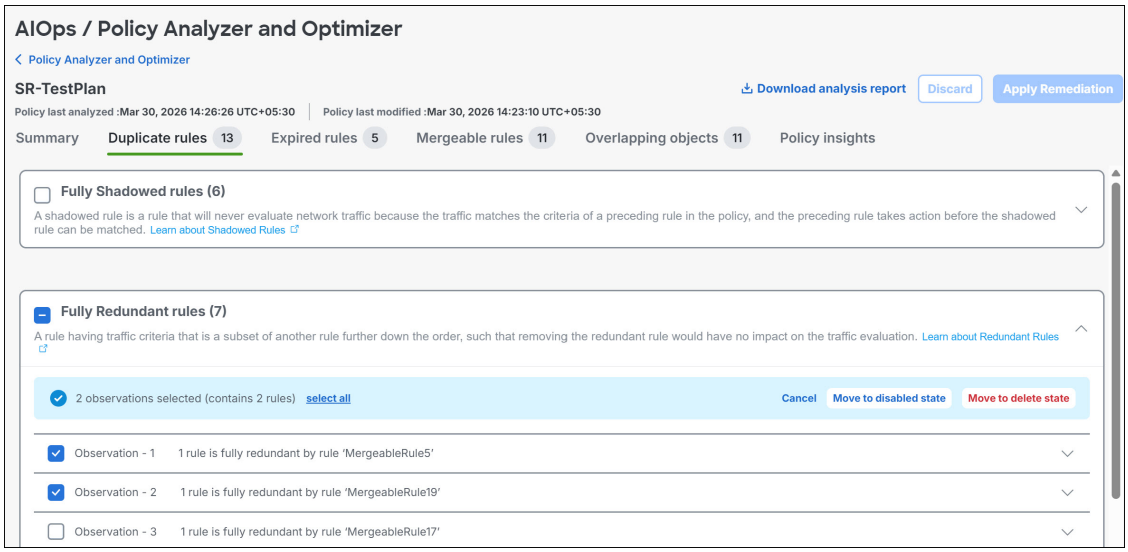
Analyze duplicate rules in access control policy

The **Duplicate Rules** tab lists shadowed and redundant rules with anomalies:

- A **Fully Shadowed rules** is one that will never evaluate network traffic because another rule that precedes it over shadows this rule.



- A **Fully Redundant rules** is one that is just a part of another larger rule, such that removing this redundant rule does not have an impact on the network traffic, because the traffic evaluation that this rule must perform is already performed by another rule.



You can remediate all duplicate-rule observations in a category, selected fully shadowed or fully redundant observations, or individual rules within an expanded observation. For selected duplicate rules, choose **Move to disabled state** or **Move to delete state**. Disable rules first when you want to measure the impact before deleting them.

> **Note**
>
> Expand each observation to review the affected rules before you stage a remediation. Each rule in the list is displayed with a set of attributes; click the settings button on the top right to select which rule attributes you want to display along with the rule.

When duplicate-rule remediation removes shadowed or redundant rules and retains a base rule, Policy Analyzer and Optimizer adds a standardized comment to the retained rule. The comment identifies the retained rule and the removed rules, which helps you audit the cleanup.

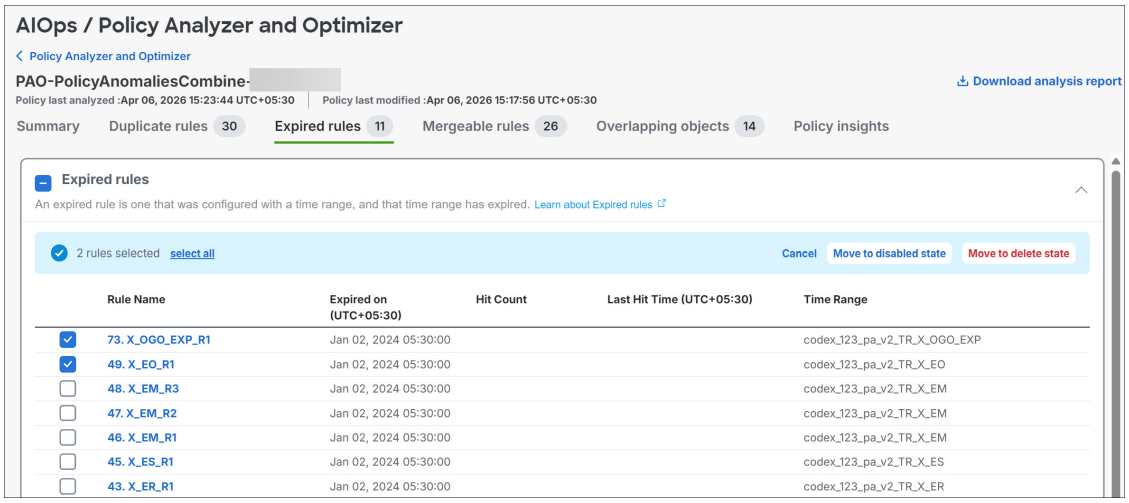
After you stage the selected duplicate-rule remediations, you can still **Undo** them before clicking **Apply Remediation**. It is recommended that you disable rules first to measure the impact and delete them later, because deleting them permanently removes them.

You can enable the disabled rules any time by navigating to the Cloud-Delivered Firewall Management Center or the On-Premises Firewall Management Center on which the rules are present.

Analyze expired rules in access control policy

The **Expired Rules** tab lists rules that were configured with a time range and the time range has expired. You can also see rule information such as the date on which the rule expired, hit count, last hit time, and the time range.

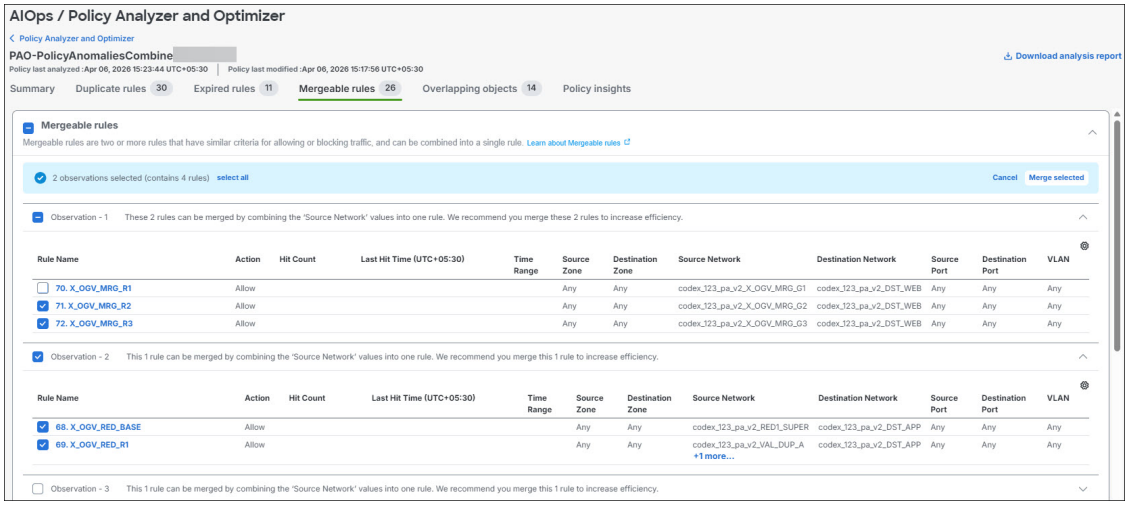
You can remediate all expired-rule observations in the category, selected expired-rule observations, or selected expired rules. For selected expired rules, choose **Move to disabled state** or **Move to delete state**. Only selected rules are changed when you apply remediation.



Analyze mergeable rules in access control policy

The **Mergeable Rules** tab lists the rules that have similar allow and block settings and can be merged into a single rule.

Review the mergeable-rule observations and stage remediation for the entire category, selected observations, or individual rules within an expanded observation. Click **Merge Selected** to merge only the staged items. Unselected mergeable-rule observations remain unchanged until you stage and apply remediation for them.



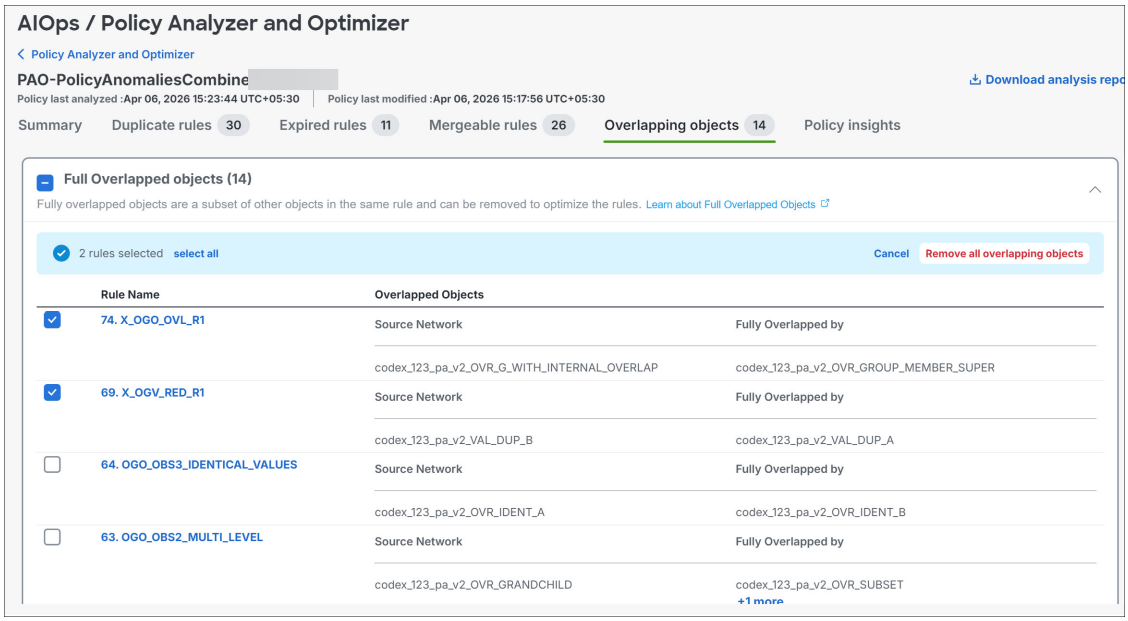
Note

When you select individual rules to merge, select only consecutive rules. The first selected rule in the sequence is updated with the merged rule criteria, and the remaining selected rules are removed. You can start the merge from any rule in a consecutive set. The first rule in the observation does not need to be selected.

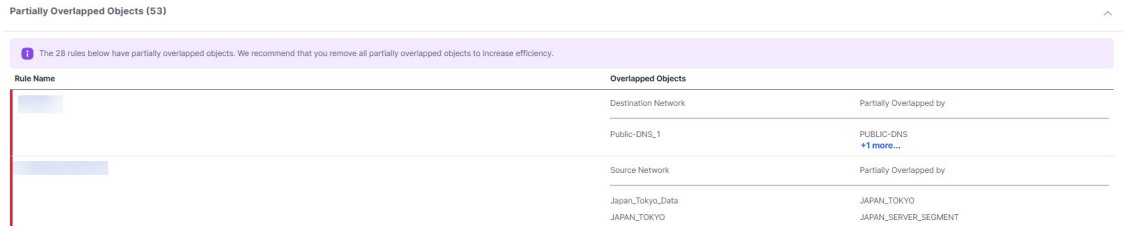
Analyze overlapping objects in access control policy

The **Overlapping Objects** tab lists objects that are either fully overlapping (the IP addresses or port numbers are either the same or a complete subset) or partially overlapping (some subset of IP addresses are repeated, but not all).

For example, if a rule contains an object for 192.168.1.1 and another for 192.168.1.0/24, the 192.168.1.1 object is fully overlapped by the other object and is not needed in the rule. For fully overlapped objects, you can remediate all fully overlapped observations in the category, selected observations, or selected rules. Click **Remove All Fully Overlapped Objects from Rules** to remove fully overlapped objects only from the staged items. For partial overlaps, evaluate each occurrence and edit the objects directly.



For partial overlaps, you need to evaluate each occurrence, determine if any changes can be made, and implement those changes directly by editing the objects.

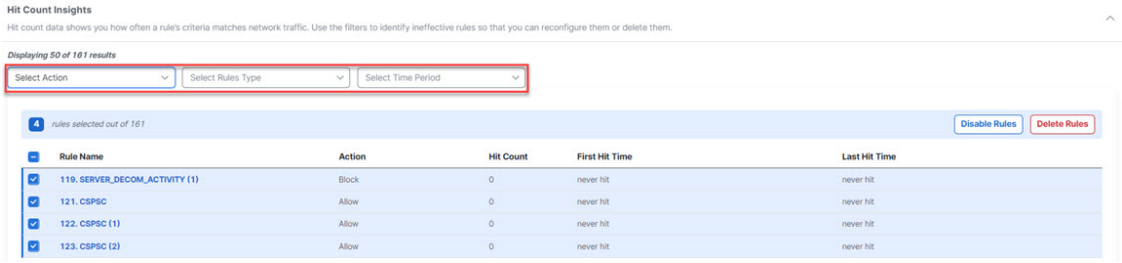


Analyze policy insights in access control policy

The **Policy Insights** tab has a **Hit Count** section that initially lists any rules that have never been triggered (**Never Hit Rules**). The hit count information is from all devices that are assigned to the policy. You can change criteria and see other hit count information, for example, **Not Hit Rules** for the past six months, or **Hit Rules** over a selected time period. You can filter the rules using the actions set in the rules, hit information, and time period:

- **Never Hit Rules**–Rules that have never been hit from the time they were created.
- **Hit Rules**–Rules that have been hit in the selected time period.
- **Not Hit Rules**–Rules that have not been hit in the selected time period.

Select the rules that you want to disable or delete, and select **Disable Rules** or **Delete Rules**. These changes are staged until you select **Apply Remediation**. First, disable the rules when you want to measure their impact before deleting them.



Access control policy remediation

Policy Analyzer and Optimizer stages remediation changes before it updates the policy. You can stage remediation for an entire anomaly category, selected observations, or individual rules within an expanded observation. Before you apply remediation, unselected observations and rules remain unchanged and available for later selection in the same analysis report.

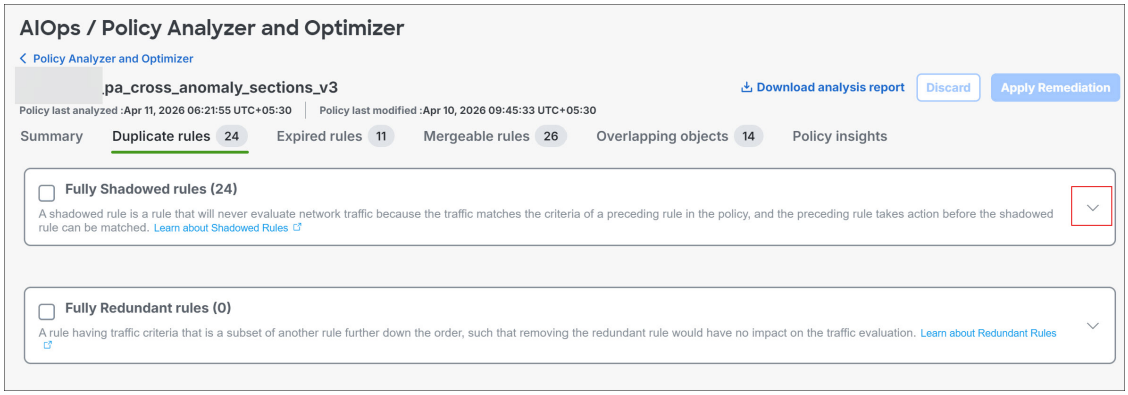
Review staged changes before you select **Apply Remediation**. After you apply remediation, you cannot apply more changes from the same analysis report. To remediate remaining anomalies, run policy analysis again on the updated policy and use the new report.

Before you begin

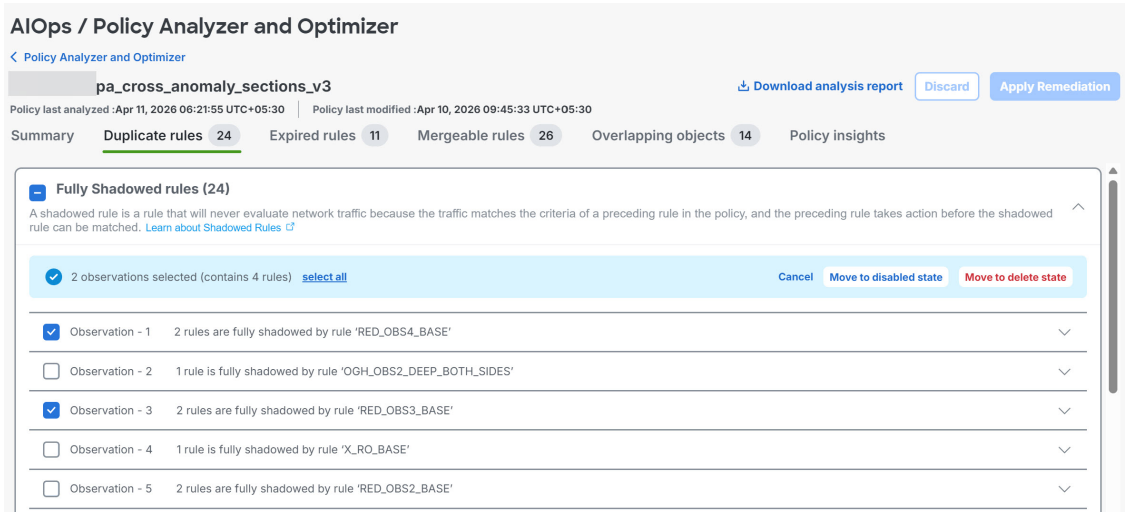
- Back up all policies before you apply remediation.
- Ensure that at least one remediation is staged. If no remediation is staged, **Apply Remediation** is disabled.
- Verify the **Policy Last Modified** and **Policy Last Analyzed** timestamps, and review the number of rules that are staged for remediation.

Procedure

1. In the **Policy Analyzer and Optimizer** page, select the policy to see details about the analysis on the right pane and click **View analysis details & optimize**.
2. Click the remediation tab that contains the anomalies that you want to fix.
3. Expand a remediation category. Select the check box for the category to stage all observations, or select the check boxes for specific observations or rules to stage only those items. Repeat this step in other remediation tabs, as needed.



4. Select the remediation action that applies to the staged items, such as **Move to disabled state**, **Move to delete state**, **Merge Selected**, **Remove All Fully Overlapped Objects from Rules**, **Disable Rules**, or **Delete Rules**.



5. Review the staged remediation. If you need to change the staged remediation before applying it, use the available undo or discard action.
6. Click **Apply Remediation**.
7. Read the confirmation message, which summarizes the remediations that will be applied. Confirm that the selected policy and staged remediation are correct.
8. Click **Apply**.

> **Note**
>
> For an On-Premises Firewall Management Center in which the Change Management Workflow is enabled, when policy remediations are applied, an internal workflow ticket is created and the changes are staged. The changes take effect only when the ticket is submitted or approved. See Change Management in *Cisco Secure Firewall Management Center Administration Guide* for more information.

After remediation is complete, the selected rules are updated. Policy Analyzer and Optimizer automatically analyzes the updated policy and generates a refreshed summary that shows any remaining issues. Verify the intended changes in the corresponding access control policy.

Download access control analysis report

The access control analysis report is a PDF summary of completed remediations for a selected policy. It includes only the remediation categories that apply to the changes you selected and applied. Each section lists the rule name, remediation action, and related comments. For example, if no duplicate rules were remediated, the report excludes the duplicate-rule remediation section.

The report includes only the remediation sections and rule details for remediations that you selected and applied. Unselected anomalies are not included in the report.

1. In the Policy Analyzer and Optimizer page, click **Access control**.
2. Select an access control policy, and in the right pane, click **Download analysis report**.

The report can include these sections:

- Remediation Summary
- Hit Count Remediation
- Expired Rules Remediation
- Duplicate Rules Remediation
- Mergeable Rules Remediation

Note

To determine whether a policy is remediated by the Policy Analyzer and Optimizer, navigate to **Policies** > **Access Policies** and edit a policy to view the rules in the **Policy Editor**. When a policy is remediated, a comment is added to the rules that are optimized.

You can also filter all the optimized rules using "updated by Policy Analyzer and Optimizer" to view all the remediated rules.

During duplicate rule remediation, the retained rule is updated with a comment specifying which rule was preserved and which were removed.

Network Address Translation policy analysis

Learn how to analyze NAT policies in Policy Analyzer and Optimizer, identify shadowed or redundant rules, review conflict ownership, and download NAT analysis reports.

Use the **Network Address Translation** (NAT) tab when you want to analyze NAT policies and find rules that are shadowed or redundant. NAT Policy Analyzer and Optimizer helps you identify rules that are not contributing to effective NAT behavior, understand which rule owns the conflict, and download a NAT analysis report for review.

NAT Policy Analyzer and Optimizer requirements

- NAT Policy Analyzer and Optimizer is available only when AIOps is enabled for the tenant and for the selected data source.
- For On-Premises Firewall Management Center, NAT Policy Analyzer and Optimizer requires Version 7.6 or later.
- If NAT Policy Analyzer and Optimizer is disabled in AIOps settings, NAT Policy Analyzer and Optimizer operations are blocked for all data sources.
- When AIOps is enabled for a data source, Policy Analyzer and Optimizer initiates the initial NAT synchronization and analysis for onboarded data sources.
- NAT Policy Analyzer and Optimizer performs analysis at the management center level, not on a per-device basis.

Note

Disabled NAT rules are excluded from being analyzed by the Policy Analyzer and Optimizer.

Analyze NAT policies

Network Address Translation (NAT) Policy Analyzer and Optimizer analyzes Cloud-Delivered Firewall Management Center and On-Premises Firewall Management Center NAT policies and categorizes NAT findings into shadowed rules and redundant rules.

NAT Policy Analyzer and Optimizer reports these NAT finding types.

Table 5:

NAT finding	Meaning	How to interpret it
Shadowed NAT rule	A rule that will never evaluate network traffic because another rule that precedes it over shadows this rule.	Review the shadowing rule and the shadowed rules together. A rule is marked shadowed only when the overlap is complete for the compared dimensions.
Redundant NAT rule	A rule can be removed without changing the final NAT behavior because another rule can handle the traffic with the same effective NAT action.	Policy Analyzer and Optimizer checks the translated action for redundancy. Matching traffic criteria alone is not enough when translated source, destination, service, or PAT behavior differs.

NAT rule sections and comparison behavior

NAT Policy Analyzer and Optimizer follows the high-level NAT evaluation model used by Cisco Secure Firewall NAT policies. NAT rules are evaluated in section order: Manual NAT before Auto NAT, Auto NAT, and Manual NAT after Auto NAT.

The NAT section determines the rule comparisons that can be reported by NAT Policy Analyzer and Optimizer.

NAT section	What it contains	NAT Policy Analyzer and Optimizer comparison behavior
Manual NAT before Auto NAT	Manual or twice NAT rules evaluated before Auto NAT.	Rules in this section can be compared with rules in the same section, Auto NAT, and Manual NAT after Auto NAT.
Auto NAT	Object NAT rules whose device order is determined internally.	Auto NAT rules can participate in comparisons with Manual NAT before or after sections. NAT Policy Analyzer and Optimizer does not report shadowed or redundant rules within the same Auto NAT section.
Manual NAT after Auto NAT	Manual or twice NAT rules evaluated after Auto NAT.	Rules in this section can be compared with rules in the same section and with rules from earlier comparable sections.

Supported NAT address families for Policy Analyzer and Optimizer

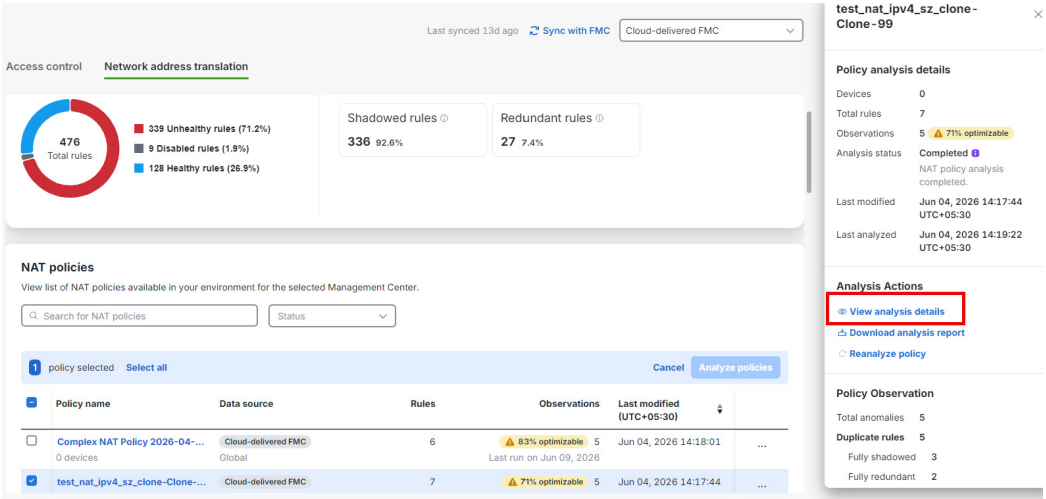
NAT Policy Analyzer and Optimizer supports these address-family flows.

Flow	Traffic family	Notes
NAT44	IPv4 to IPv4	Supported for standard IPv4 NAT and PAT behavior.
NAT66	IPv6 to IPv6	Supported for IPv6 NAT behavior.

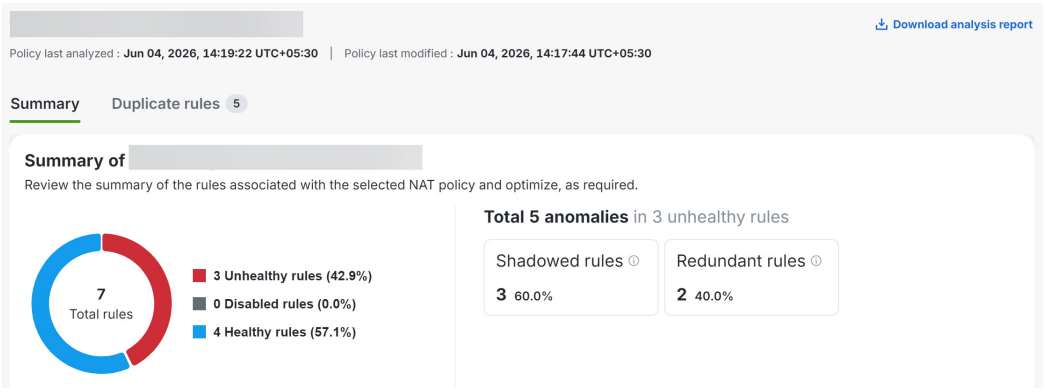
Flow	Traffic family	Notes
NAT64	IPv6 to IPv4	Supported when cross-family behavior is explicitly configured.
NAT46	IPv4 to IPv6	Supported when cross-family behavior is explicitly configured.

NAT policy analysis summary

When analysis completes, select a NAT policy to review the right-pane summary and click **View analysis details**.



The policy-specific page displaying the anomaly details is shown.



- **Overall summary**–provides insights on how many rules are unhealthy, disabled, healthy, using a pie chart for the selected NAT policy. You can also hover over the part of the pie to view the percentage of rules.
- **Total anomalies**–shows the number of rule anomalies detected in the selected NAT policy. Also indicates how many unhealthy rules contain those anomalies.

Download NAT analysis report

The NAT analysis report is available after NAT policy analysis is complete and can be downloaded as a PDF. The PDF report includes policy metadata, analysis timestamps, summary charts, counts for healthy, disabled, shadowed, and redundant rules, and tabular observation details.

1. In the Policy Analyzer and Optimizer page, click **Network address translation**.

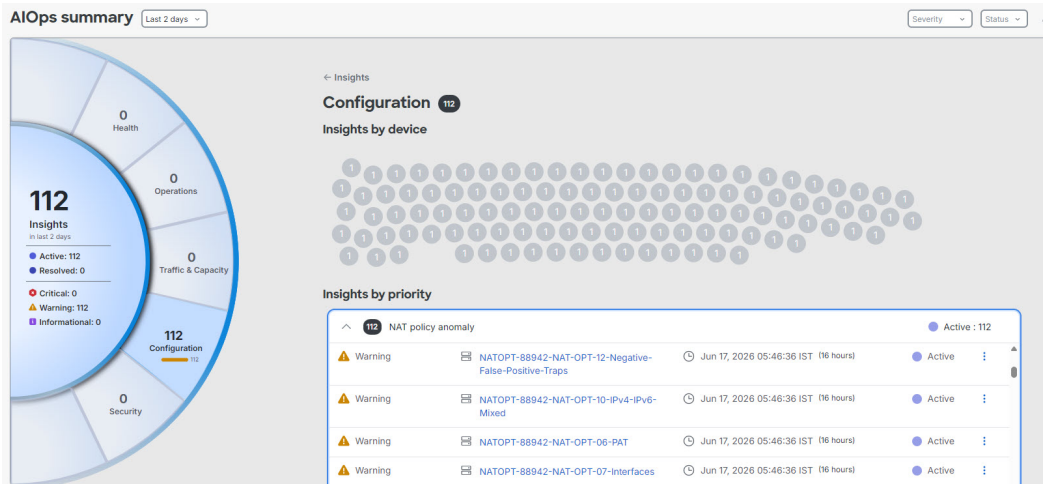
2. Select a NAT policy, and in the right pane, click **Download analysis report**.

The detailed rule information can include NAT section, rule type, direction, source and destination interface objects, original source, original destination, original service, translated source, translated destination, and translated service. Use these details to evaluate whether changes are needed in the management center. NAT Policy Analyzer and Optimizer does not apply NAT remediations in this release.

NAT Policy Analyzer and Optimizer and AgenticOps insights

When NAT Policy Analyzer and Optimizer analysis detects NAT policy anomalies, AgenticOpscan raise a NAT policy anomaly insight. From AIOps Insights, you can review NAT anomaly counts by data source, open the affected data source or policy, and navigate back to the NAT Policy Analyzer and Optimizer analysis details.

Navigation: **Insights & Reports** > **Summary**.



If you dismiss a NAT anomaly insight, it is dismissed for the current insight occurrence. A later scheduled analysis can raise the insight again if NAT anomalies are detected again.

Troubleshooting Policy Analyzer and Optimizer

Learn how to troubleshoot Policy Analyzer and Optimizer when policies do not analyze or appear.

Read the following sections to troubleshoot any issues with the Policy Analyzer and Optimizer:

Policy Analyzer and Optimizer Does Not Analyze Policies

If you notice that Policy Analyzer and Optimizer is not analyzing policies despite clicking **Analyze Policy**, try the following:

Procedure

1. Navigate **Administration** > **Integrations** > **Firewall Management Center**.
2. Select the On-Premises Firewall Management Center or **Cloud-Delivered FMC** for which the policy analysis is not happening and choose **Workflows** under **Actions** on the right pane.
3. If you see that the latest workflow's **Current State** shows up as **Error**, expand the workflow and scroll to the last action whose **END STATE** is **ERROR**.
4. Click **Error Message** under the **RESULT** column to see a detailed error message or click **Stack Trace** to see the series of exceptions that occurred, which caused the error.

5. Resolve the error or contact Cisco TAC for assistance.

Policy Analyzer and Optimizer Does Not Fetch Policies

If policies on your On-Premises Firewall Management Center are not displayed on the Policy Analyzer and Optimizer page on Security Cloud Control, do the following:

Procedure

1. On the On-Premises Firewall Management Center, navigate **Integration** > **Cisco Security Cloud**.
2. Ensure that the **Enable Policy Analyzer and Optimizer** checkbox is checked.
3. Optional: In the left navigation pane of your Security Cloud Control tenant, navigate **Administration** > **Integrations** > **Firewall Management Center**, and ensure that the On-Premises Firewall Management Center is active and reachable.

Frequently Asked Questions About Policy Analyzer and Optimizer

Find answers to common questions about Policy Analyzer and Optimizer, including AI Assistant support, analysis scheduling, reporting, licensing, remediation limits, rule handling, and failed remediation recovery.

Can Cisco AI Assistant analyze and remediate policies instead of manually doing it using Policy Analyzer and Optimizer?

The Cisco AI Assistant collaborates with Policy Analyzer and Optimizer to scrutinize policies with anomalies and notify users. However, the AI Assistant cannot automatically analyze and remediate policies.

Can Policy Analyzer and Optimizer detect new changes to an already-analyzed policy and run analysis again on the same policy?

No, the Policy Analyzer and Optimizer can analyze policies only when manually triggered or at a 24-hour scheduled policy analysis run.

For a shared policy, does the Policy Analyzer and Optimizer provide individual device-based reports?

No. The Policy Analyzer and Optimizer provides reports only based on the access policy analysis data.

I am an On-Premises Firewall Management Center user. Should I purchase the Security Cloud Control base license to use the Policy Analyzer and Optimizer?

No. The Policy Analyzer and Optimizer comes as part of an existing or a newly created Security Cloud Control tenant during the Cisco Security Cloud integration.

I provisioned a Security Cloud Control tenant when I integrated my On-Premises Firewall Management Center with the Cisco Security Cloud. What other features, except Policy Analyzer and Optimizer, can I leverage in Security Cloud Control?

You can only leverage Policy Analyzer and Optimizer capabilities of this Security Cloud Control tenant. To use other features of Security Cloud Control, you need to purchase the Security Cloud Control base license and other device-specific licenses.

For an On-Premises Firewall Management Center on which the change management workflow is enabled and there are policies with pending changes to be approved, can the Policy Analyzer and Optimizer still apply remediations those policies?

No. The remediation will be hindered with an error saying the policies are locked for use.

Is there a maximum number of rules that Policy Analyzer and Optimizer can analyze in a policy?

There are no such limits. The Policy Analyzer and Optimizer can analyze any number of policies and rules. However, when the policies have more number of rules, the analysis takes a long time too.

What is the difference between disable rules and delete rules? Which is the better option?

Deleting a rule removes the rule completely from the device memory. However, disabling a rule keeps it in the device memory as a backup and does not get deployed to the device.

If a policy remediation fails when it is partially done, are the changes automatically revoked by Policy Analyzer and Optimizer?

No. In such a case, you get a failure notification and a remediation report. You can read the report to know which rules were impacted by the half-done remediation, manually revoke the changes, and start the remediation all over again.

10 Manage device configuration

Topics:

- Read, discard, and deploy configuration changes
- Synchronizing configurations between Security Cloud Control and device

Learn how Security Cloud Control reads, compares, discards, accepts, and deploys device configuration changes to keep managed device configurations synchronized and resolve pending or conflicting changes.

To manage a device, Security Cloud Control stores a copy of the device configuration in its local database. When Security Cloud Control reads a configuration from a managed device, it copies and saves the configuration.

Security Cloud Control also reads and saves a copy of a device configuration when the device is onboarded. Each of these actions serves a specific purpose.

- **Discard Changes**: This action is available when a device configuration status is "Not Synced." In the **Not Synced** state, there are changes to the device configuration pending on Security Cloud Control. This option allows you to undo all pending changes. The pending changes are deleted and Security Cloud Control overwrites its copy of the configuration with the copy of the configuration stored on the device.
- **Check for Changes**: This action is available if the device configuration status is "Synced." Click **Check for Changes** to instruct Security Cloud Control to compare its copy of the device configuration with the copy stored on the device. If a difference is detected, Security Cloud Control immediately overwrites its copy of the device configuration with the copy stored on the device.
- **Review Conflict** and **Accept Without Review**: If you have enabled Conflict Detection on a device, Security Cloud Control checks for configuration changes made on the device every 10 minutes. If the copy of the configuration stored on the device has changed, Security Cloud Control notifies you by displaying the "Conflict Detected" configuration status.
  - **Review Conflict**: Click **Review Conflict** to review changes made directly on a device and accept or reject them.
  - **Accept Without Review**: This action overwrites the copy of the device configuration on Security Cloud Control with the latest copy of the configuration stored on the device. Security Cloud Control does not prompt you to confirm the differences in the two copies of the configuration before taking the overwriting action.

Read All: This is a bulk operation. You can select any number of devices in any state and click **Read All** to overwrite all the device configurations stored on Security Cloud Control with the configurations stored on the devices.

- **Deploy Changes**: When you make changes to a device configuration, Security Cloud Control saves your changes to its copy of the configuration. These changes remain **Pending** in Security Cloud Control until you deploy them to the device. If there are pending changes that have not been deployed, the device is in the **Not Synced** configuration state.

  Pending configuration changes do not affect network traffic. They take effect only after Security Cloud Control deploys them to the device.

  When Security Cloud Control deploys changes to a device configuration, only the elements that were changed are overwritten. The entire device

configuration file is not overwritten. You can deploy changes to one device or multiple devices simultaneously.

- **Discard All**: This option appears after you click **Preview and Deploy...**. When you click **Preview and Deploy...**, Security Cloud Control displays a preview of the pending changes in Security Cloud Control. You can delete all pending changes from Security Cloud Control without deploying them to the selected devices by clicking **Discard All**. Unlike "Discard Changes," deleting the pending changes completes the operation.

Read, discard, and deploy configuration changes

Learn about reading, discarding, and deploying configuration changes in Security Cloud Control Firewall Management.

Read All Device Configurations

If a configuration change is made to a device outside of Security Cloud Control, the device configuration stored on Security Cloud Control and the device's local copy of its configuration are no longer the same. You many want to overwrite Security Cloud Control's copy of the device's configuration with the configuration stored on the device to make the configurations the same again. You can perform this task on many devices simultaneously using the **Read All** link.

For more information about how Security Cloud Control manages the two copies of the device configuration, refer to Reading, Discarding, Checking for, and Deploying Configuration Changes.

Here are three configuration statuses where clicking **Read All** will overwrite Security Cloud Control's copy of the device's configuration with the device's copy of the configuration.

- **Conflict Detected**: If conflict detection is enabled, Security Cloud Control polls the devices it manages every 10 minutes for changes made to their configurations. If Security Cloud Control finds that the configuration on the device has changed, Security Cloud Control displays a "Conflict detected" configuration status for the device.
- **Synced**: If the device is in a synced state, and you click **Read All**, Security Cloud Control immediately checks the devices to determine if there have been any changes made to its configurations directly. After clicking **Read All**, Security Cloud Control confirms your intent to overwrite its copy of the device's configuration and then Security Cloud Control performs the overwrite.
- **Not Synced**: If the device is in the **Not Synced** state, and you click **Read All**, Security Cloud Control warns you that there are pending changes made to the device's configuration using Security Cloud Control and that proceeding with the **Read All** operation will delete those changes and then overwrite Security Cloud Control's copy of the configuration with the configuration on the device.

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. (Optional) Create a change request label to identify the results of this bulk action easily in the change log.
5. Select the devices whose configurations you want to save in Security Cloud Control.

   Security Cloud Control only provides command buttons for actions that can be applied to all the selected devices.

   Security Cloud Control warns you if there are configuration changes staged on Security Cloud Control for any of the devices you selected and asks if you want to continue with the bulk reading configurations action.
6. Click **Read All** to continue.
7. Look at the notifications tab for the progress of the **Read All** configurations operation.
8. If you created and activated a change request label, remember to clear it so that you don't inadvertently associate other configuration changes with this event.

Preview and deploy configuration changes for all devices

Learn how to review and deploy pending configuration changes to managed devices in Security Cloud Control, track deployment progress, and verify results in jobs or event logs.

Security Cloud Control informs you when you have made a configuration change to a device in your organization, but you have not deployed that change, by displaying an orange dot on the deploy icon . Each device affected by these changes displays a status of "Not Synced" in the **Security Devices** page. Click **Deploy** to review which devices have pending changes and deploy the changes to those devices.

This deployment method is available for all supported devices.

You can use this deployment method for a single configuration change. Alternatively, you can wait and deploy multiple changes at once.

Procedure

1. In the menu bar of Security Cloud Control click the **Deploy** button .
2. Select the devices with changes you want to deploy. If a device displays a yellow caution triangle, you cannot deploy changes to that device. Hover your pointer over the yellow caution triangle to see the reason.
3. (Optional) If you want to see more information about a pending change, click the **View Detailed Change log** link to open the change log associated with that change. Click the **Deploy** icon to return to the **Devices with Pending Changes** page.
4. Click **Deploy Now** to deploy the changes immediately to the devices that you selected. You will see the progress in the Active jobs indicator in the Jobs tray.
5. (Optional) After the deployment has finished, click **Jobs** in the Security Cloud Control navigation bar. The results of the deployment appear in a recent "Deploy Changes" job.
6. If you created a change request label and have no more configuration changes to associate with it, clear the label.

Bulk Deploy Device Configurations

If you have made changes to multiple devices, for instance by editing a shared object, you can apply those change to all of the affected devices at once:

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select all of the devices for which you have made configuration changes on Security Cloud Control. These devices should show "Not Synced" status.
5. Deploy the changes using one of these methods:
   - Click the button at the top-right of the screen to view the **Devices with Pending Changes** window. This gives you a chance to review the pending changes on the devices you selected before you deploy them. Click **Deploy Now** to deploy the changes.

> **Note**
>
> If you see a yellow warning triangle next to a device on the **Devices with Pending Changes** screen, you cannot deploy a change to that device. Hover your mouse over the warning triangle for information about why changes cannot be deployed to that device.

- Click **Deploy All** on the details pane. Review any warnings and click **OK**. The bulk deployment starts immediately without a review of the changes.

6. (Optional) Click the Jobs icon  in the navigation bar to view the results of the bulk deploy.

Preview and deploy On-Premises Firewall Management Center configurations

Use this procedure to deploy configuration changes made in Security Cloud Control to your on-premises Firewall Management Center, ensuring the updates are pushed and synchronized efficiently. Manually deploy these changes to your managed Firewall Threat Defense devices.

If you have made configuration changes to an object, such as changing a value or adding an override to an object, you can deploy all those changes at once to your on-premises Firewall Management Center.

> **Note**
>
> This task deploys configuration changes only to on-premises Firewall Management Center. To deploy these changes to your Firewall Threat Defense devices, you must deploy these changes manually from your on-premises Firewall Management Center. For more information, see Configuration Deployment in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Procedure

1. Choose **Administration** > **Integrations** > **Firewall Management Center**
2. Click the **FMC** tab.
3. Select the on-premises Firewall Management Center where you want to preview and deploy changes.

> **Note**
>
> Security Cloud Control identifies when your on-premises Firewall Management Center is out of sync and displays the status as **Not Synced**.

4. Click **Preview and Deploy** on the details pane.
5. Review any warnings. To deploy immediately, click **Deploy Now**. If you do not want to proceed, click **Discard All**.

6. Alternatively, click the download button  at the top-right corner of the screen to open the **Devices with Pending Changes** window. Select the devices, review the pending changes on the selected devices, and then deploy them.
7. Click **Deploy Now** to deploy the changes.

About Scheduled Automatic Deployments

Using Security Cloud Control, you can make configuration changes to one or more of the devices it manages and then schedule the changes to be deployed to those devices at a time that is convenient for you.

You can only schedule deployments if you Enable scheduled automatic deployments on page 134 in the **Tenant Settings** tab of the Settings page. Once this option is enabled, you can create, edit, or delete scheduled deployments. A scheduled deployment deploys all the staged changes saved on Security Cloud Control at the date and time set. You can also view and delete scheduled deployments from the Jobs page.

If there were changes made directly to the device that have not been read to Security Cloud Control, the scheduled deployment will be skipped until that conflict is resolved. The Jobs page will list any instance where a scheduled deployment fails. If **Enable the Option to Schedule Automatic Deployments** is turned off, all scheduled deployments are deleted.

> **Caution**
>
> If you schedule a new deployment for multiple devices, and some of those devices already have deployments scheduled, the new scheduled deployment overwrites the existing scheduled deployments.

> **Note**
>
> When you create a scheduled deployment, the schedule is created in your local time, not in the time zone of the device. Scheduled deployments *do not* automatically adjust for daylight savings time.

Enable scheduled automatic deployments

Enable the option to schedule automatic deployments to conveniently plan single or recurring updates for your devices. Use this task to automate deployment workflows and ensure updates occur at optimal times.

Enabling the option to schedule automatic deployments allows you to schedule future deployments at a date and time when it is convenient. Once you enable this option, you can schedule a single automatic deployment or set up recurring automatic deployments.

Changes you make on Security Cloud Control for a device are not automatically deployed to the device if it has pending changes . If a device is not in the **Synced** state, such as **Conflict Detected** or **Not Synced**, scheduled deployments are not executed. The jobs page lists any instance where a scheduled deployment fails.

If you turn off **Enable the Option to Schedule Automatic Deployments**, all scheduled deployments are deleted.

Important

If you use Security Cloud Control to create more than one scheduled deployment for a device, the new deployment overwrites the existing deployment. If you create more than one scheduled deployment for a device using the API, you **must** delete the existing deployment before scheduling the new deployment.

Follow these steps to enable scheduled automatic deployments:

Procedure

1. Choose **Administration** > **General Settings**.
2. Turn on the **Enable the option to schedule automatic deployments** toggle button to enable it.

Schedule an Automatic Deployment

The deployment schedule can be a single event or a recurring event. You may find recurring automatic deployments a convenient way to line up recurring deployments with your maintenance window. Follow this procedure to schedule a one-time or a recurring deployment for a single device.

Important

This procedure applies only to ASAs and FDM-managed devices.

To schedule deployments for Secure Firewall Threat Defense devices managed by on-premises Firewall Management Center or Cloud-Delivered Firewall Management Center, see Scheduling.

Note

If you schedule a deployment for a device that has an existing deployment scheduled, the new scheduled deployment overwrites the existing deployment.

Procedure

1. From the Security Cloud Control home page, choose **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select one ore more devices.
5. In the Device Details pane, locate the Scheduled Deployments tab and click **Schedule**.
6. Select when the deployment should occur.
   - For a one-time deployment, click the **Once on** option to select a date and time from the calendar.
   - For a recurring deployment, click the **Every** option. You can choose either a daily or once a week deployment. Select the **Day** and **Time** the deployment should occur.
7. Click **Save**.

Edit a Scheduled Deployment

Follow this procedure to edit a scheduled deployment:

Procedure

1. From the Security Cloud Control home page, choose **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select one or more devices.
5. In the **Device Details** pane, locate the Scheduled Deployments tab and click **Edit** .



6. Edit the recurrence, date, or time of a scheduled deployment.
7. Click **Save**.

Delete a Scheduled Deployment

Follow this procedure to delete a scheduled deployment:

> **Note**
>
> If you schedule a deployment for multiple devices, and then change or delete the schedule for some of the devices, the original scheduled deployment for the remaining devices will be preserved.

Procedure

1. Click the **Devices** tab.
2. Click the appropriate device type tab.
3. Select one or more devices.
4. In the **Device Details** pane, locate the **Scheduled Deployments** tab and click **Delete** .

- Reading, Discarding, Checking for, and Deploying Configuration Changes
- Read All Device Configurations on page 131
- Preview and deploy configuration changes for all devices on page 131

Check for Configuration Changes

Check for Changes to determine if the device's configuration has been changed directly on the device and it is no longer the same as the copy of the configuration stored on Security Cloud Control. You will see the this option when the device is in the "Synced" state.

To check changes:

Procedure

1. From the Security Cloud Control home page, choose **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select the device, whose configuration you suspect may have been changed directly on the device.
5. Click **Check for Changes** in the Synced pane on the right.
6. The behavior that follows is slightly different depending on the device:

   - For device if there has been a change to the device's configuration, you will receive the message:

     ```
     Reading the policy from the device. If there are active deployments on the
     device, reading will start after they are finished.
     ```

     - Click **OK** to continue. The configuration on the device will overwrite the stored configuration on Security Cloud Control.
     - Click **Cancel** to cancel the action.

   - For device:

   a. Compare the two configurations presented to you. Click **Continue**. The configuration labeled **Last Known Device Configuration** is the configuration stored on Security Cloud Control. The configuration labeled **Found on Device** is the configuration saved on the ASA.

   b. Select either:

      1. **Reject** the out-of-band changes to keep the "Last Known Device Configuration."
      2. **Accept** the out-of-band changes to overwrite the device's configuration stored in Security Cloud Control with the configuration found on the device.

   c. Click **Continue**.

Discard Configuration Changes

Click **Discard Changes** when you want to "undo" all the *undeployed* configuration changes you made to a device's configuration using Security Cloud Control. When you click **Discard Changes**, Security Cloud Control *completely overwrites* its local copy of a device's configuration with the configuration stored on the device.

When you click **Discard Changes**, your device's configuration status is in a **Not Synced** state. After you discard your changes, the copy of the configuration on Security Cloud Control will be the same as the copy of the configuration on the device and the configuration status in Security Cloud Control will return to Synced.

To discard, or "undo," all of your undeployed configuration changes for a device:

Procedure

1. From the Security Cloud Control home page, choose **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select the device you have been making configuration changes to.
5. Click **Discard Changes** in the **Not Synced** pane on the right.

- For FDM-managed devices-Security Cloud Control warns you that "Pending changes on Security Cloud Control will be discarded and the Security Cloud Control configuration for this device will be replaced with the configuration currently running on the device." Click **Continue** to discard your changes.
- For Meraki devices-Security Cloud Control deletes the change immediately.
- For AWS devices-Security Cloud Control displays what you are about to delete. Click **Accept** or **Cancel**.

Discard On-Premises Firewall Management Center configuration changes

Learn how to discard all configuration changes made in Security Cloud Control for an on-premises Firewall Management Center, ensuring the configuration matches the version stored on the managed device.

To undo all configuration changes you made in Security Cloud Control, such as changes to objects shared between your Security Cloud Control and on-premises Firewall Management Center, follow this procedure. When you perform this task, Security Cloud Control *completely overwrites* its local configuration copy with the configuration stored on the device.

Procedure

1. Choose **Administration** > **Integrations** > **Firewall Management Center**.
2. Click the **FMC** tab.
3. Select the on-premises Firewall Management Center for which you want to discard changes.
4. Click **Discard Changes** in the **Not Synced** pane.

   When you click **Discard Changes**, your on-premises Firewall Management Center configuration status changes to **Not Synced**. After you discard your changes, the configuration copy stored in Security Cloud Control matches the configuration on on-premises Firewall Management Center. The status in Security Cloud Control then returns to **Synced**.

Out-of-Band Changes on Devices

Out-of-band changes refer to changes made directly on the device without using Security Cloud Control. These changes may be made using the device's command-line interface over an SSH connection or by using a local manager like the Adaptive Security Device Manager (ASDM) for the ASA, the FDM for the FDM-managed device, or for an On-Premises Firewall Management Center on the On-Premises Firewall Management Center user interface. An out-of-band change causes a conflict between the device's configuration stored on Security Cloud Control and the configuration stored on the device itself.

Detecting Out-of-Band Changes on Devices

If Conflict Detection is enabled for an ASA, or an FDM-managed device, a Cisco IOS device, or an On-Premises Firewall Management Center, Security Cloud Control checks the device every 10 minutes searching for any new changes made directly to the device's configuration outside of Security Cloud Control.

If Security Cloud Control finds that there are changes to the device's configuration that are not stored on Security Cloud Control, it changes the **Configuration Status** of that device to the "Conflict Detected" state.

When Security Cloud Control detects a conflict, one of two conditions is likely:

- There have been configuration changes made to the device directly that have not been saved to Security Cloud Control's database.
- In the case of an FDM-managed device, there may be "pending" configuration changes on the FDM-managed device that have not been deployed.

- In the case of an On-Premises Firewall Management Center, there may be changes made, for instance, to objects outside Security Cloud Control, which are pending to be synchronized with Security Cloud Control or changes made in Security Cloud Control which are pending to be deployed to the On-Premises Firewall Management Center.

Synchronizing configurations between Security Cloud Control and device

Learn how to synchronize configurations between Security Cloud Control and device.

About configuration conflicts

In the **Security Devices** page, you may see devices or services have the status "Synced," "Not Synced," or "Conflict Detected." To know the status of an On-Premises Firewall Management Center that you manage using Security Cloud Control, navigate **Administration** > **Integrations** > **Firewall Management Center**.

- When a device is **Synced**, the configuration on Security Cloud Control) and the configuration stored locally on the device are the same.
- When a device is **Not Synced**, the configuration stored in Security Cloud Control was changed and it is now different that the configuration stored locally on the device. Deploying your changes from Security Cloud Control to the device changes the configuration on the device to match Security Cloud Control's version.
- Changes made to devices outside of Security Cloud Control are called **out-of-band changes**. When out-of-band changes are made, you'll see the device state change to "Conflict Detected," if conflict detection is enabled for the device. Accepting the out-of-band changes, changes the configuration on Security Cloud Control to match the configuration on the device.

Conflict Detection

When conflict detection is enabled, Security Cloud Control polls the device for the default interval to to determine if a change has been made to the device's configuration outside of Security Cloud Control. If Security Cloud Control detects that a change was made, it changes the configuration status for the device to **Conflict Detected**. Changes made to a device outside of Security Cloud Control are called "out-of-band" changes.

In the case of an On-Premises Firewall Management Center that is managed by Security Cloud Control, if there are changes that are staged and the device is in **Not Synced** state, Security Cloud Control stops polling the device to check for changes. When there are changes made outside Security Cloud Control which are pending to be synchronized with Security Cloud Control and changes made in Security Cloud Control which are pending to be deployed to the on-premises Firewall Management Center, Security Cloud Control declares the on-premises Firewall Management Center to be in the **Conflict Detected** state.

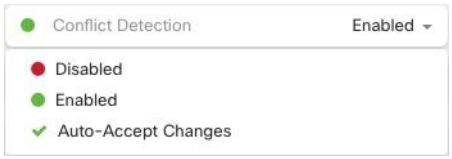
Once this option is enabled, you can configure how often conflicts or OOB changes are detected per device. See Schedule polling for device changes on page 143 for more information.

Enable Conflict Detection

Enabling conflict detection alerts you to instances where changes have been made to a device outside of Security Cloud Control.

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab.
3. Select the appropriate device type tab.
4. Select the device or devices for which you want to enable conflict detection.
5. In the **Conflict Detection** box at the right of the device table, select **Enabled** from the list.



Enable conflict detection for an On-Premises Firewall Management Center

This section helps you enable conflict detection for an on-premises Firewall Management Center that you manage using Security Cloud Control.

Enabling conflict detection for an on-premises Firewall Management Center keeps you informed when there are changes made outside Security Cloud Control that are pending synchronization with Security Cloud Control, and when there are changes made in Security Cloud Control that are pending deployment to on-premises Firewall Management Center.

Procedure

1. Choose **Administration** > **Integrations** > **Firewall Management Center**.
2. From the list, select the on-premises Firewall Management Center for which you want to enable conflict detection.
3. In the **Conflict Detection** box on the right pane, select **Enabled** from the list.

> **Note**
>
> Unlike other devices managed by Security Cloud Control, for an on-premises Firewall Management Center, you can either enable or disable conflict detection; you cannot opt to auto-accept changes.

Automatically Accept Out-of-Band Changes from your Device

You can configure Security Cloud Control to automatically accept any change made directly to a managed device by enabling auto-accept changes. Changes made directly to a device without using Security Cloud Control are referred to as out-of-band changes. An out-of-band change creates a *conflict* between the device's configuration stored on Security Cloud Control and the configuration stored on the device itself.

The auto-accept changes feature is an enhancement to conflict detection. If you have auto-accept changes enabled on your device, Security Cloud Control checks for changes every 10 minutes to determine if there have been any out-of-band changes made to the device's configuration. If there have been configuration changes, Security Cloud Control automatically updates its local version of the device's configuration without prompting you.

Security Cloud Control will ***not*** automatically accept a configuration change if there are configuration changes made on Security Cloud Control that have not yet been deployed to the device. Follow the prompts on the screen to determine your next action.

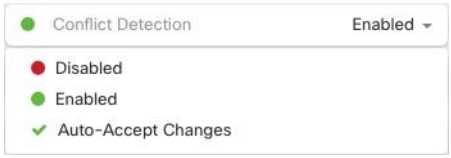
To use auto-accept changes, you first enable the tenant to display the auto-accept option in the Conflict Detection menu on the **Security Devices** page; then, you enable auto-accept changes for individual devices. For on-premises Firewall Management Center, you can do this from the **Services** page by navigating **Administration** > **Integrations** > **Firewall Management Center** and selecting the FMC.

If you want Security Cloud Control to detect out-of-band changes but give you the option to accept or reject them manually, enable Conflict Detection on page 139 instead.

Configure Auto-Accept Changes

Procedure

1. Log in to Security Cloud Control using an account with Admin or Super Admin privileges.
2. Choose **Administration** > **General Settings**.
3. In the **Tenant Settings** area, click the toggle to **Enable the option to auto-accept device changes**. This enables the Auto-Accept Changes menu option to appear in the Conflict Detection menu on the **Security Devices** page.
4. In the left pane, click **Security Devices** and select the device for which you want to automatically accept out-of-band changes.
5. In the **Conflict Detection** menu, select **Auto-Accept Changes** in the drop-down menu.



Disabling Auto-Accept Changes for All Devices on the Tenant

Procedure

1. Log-in to Security Cloud Control using an account with Admin or Super Admin privileges.
2. Choose **Administration** > **General Settings**.
3. In the **Tenant Settings** area, disable the "**Enable the option to auto-accept device changes**" by sliding the toggle to the left so it shows a grey X. This disables Auto-Accept Changes option in the Conflict Detection menu and disables the feature for every device on your tenant.

> **Note**
>
> Disabling "Auto-Accept" will require you to review each device conflict before you can accept it into Security Cloud Control. This includes devices previously configured to auto-accept changes.

Resolve configuration conflicts

This section explains how to resolve configuration conflicts that occur on the device.

Resolve the Not Synced Status

Use the following procedure to resolve a device with a "Not Synced" Configuration Status:

Procedure

1. Choose **Security Devices**.

> **Note**
>
> For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.
4. Select the device reported as Not Synced.
5. In the **Not synced** panel to the right, select either of the following:
   - **Preview and Deploy...** -If you want to push the configuration change from Security Cloud Control to the device, preview and deploy the changes you made now, or wait and deploy multiple changes at once.
   - **Discard Changes** -If you do **not** want to push the configuration change from Security Cloud Control to the device, or you want to "undo" the configuration changes you started making on Security Cloud Control. This option overwrites the configuration stored in Security Cloud Control with the running configuration stored on the device.

Resolve the conflict detected status

Security Cloud Control allows you to enable or disable conflict detection on each live device. If Conflict Detection on page 139 is enabled and there was a change made to the device's configuration without using Security Cloud Control, the device's configuration status will show **Conflict Detected**.

To resolve a **Conflict Detected** status, follow this procedure:

Procedure

---

1. Choose **Security Devices**.

> **Note**
>
> For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

2. Click the **Devices** tab to locate your device.
3. Click the appropriate device type tab.
4. Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.
5. In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.
   - The panel labeled "Last Known Device Configuration" is the device configuration stored on Security Cloud Control.
   - The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.
6. Resolve the conflict by selecting one of the following:
   - **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on** Security Cloud Control with the device's running configuration.

> **Note**
>
> As Security Cloud Control does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.

- **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on Security Cloud Control.

> **Note**
>
> All configuration changes, rejected or accepted, are recorded in the change log.

Schedule polling for device changes

Optimize Security Cloud Control by customizing schedule polling for device changes. When conflict detection or auto-accept is enabled, define specific polling intervals per device. This overrides the tenant default, ensuring precise monitoring of device configuration changes across your network for efficient, automated device management and synchronization.

If you enable Conflict Detection on page 139 or **Enable the option to auto-accept device changes** from the **Settings** page, Security Cloud Control polls the device at the default interval to check for configuration changes made outside Security Cloud Control. You can set how often Security Cloud Control polls for changes for each device. This customization can be applied to multiple devices.

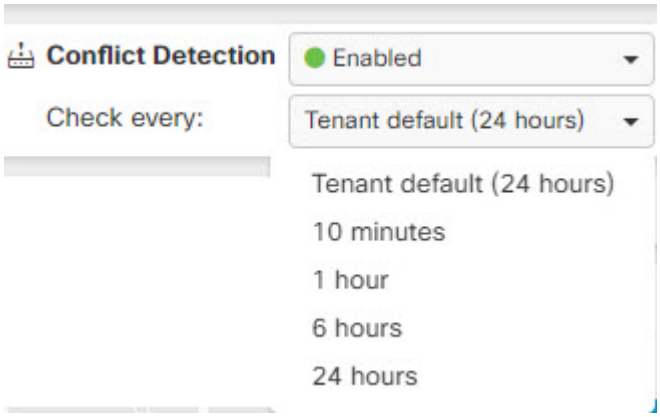
If you do not configure a selection for a device, the interval is automatically configured for "tenant default".

> **Note**
>
> If you set a custom interval per device on the **Security Devices** page, it overrides the polling interval selected as the Default Conflict Detection Interval on the **General Settings** page.

After you enable **Conflict Detection** from the **Security Devices** page or **Enable the option to auto-accept device changes** from the **Settings** page, you can schedule how often Security Cloud Control polls your devices with this procedure.

Procedure

1. Choose **Security Devices**.
2. Click the **Devices** tab to locate your device.
3. Click the appropriate device type tab.
4. Select the devices where you want to enable conflict detection.
5. Next to **Conflict Detection**, click the drop-down menu for **Check every** and select the polling interval you want.


Conflict Detection
Enabled
Check every:
Tenant default (24 hours)
Tenant default (24 hours)
10 minutes
1 hour
6 hours
24 hours

11 Monitor and report change logs, workflows, and jobs

Topics:

- Change logs in Security Cloud Control
- View change log differences
- Change request management
- Export the change log
- Jobs monitoring in Security Cloud Control
- Monitor workflows in Security Cloud Control

Describes how to monitor and report change logs, workflows, and jobs to track configuration changes, bulk device operations, and device communication processes for understanding network security posture.

Security Cloud Control effectively monitors configuration change logs, bulk device operations, and the process that runs when communicating with devices. This helps you understand how your network's existing policies influence its security posture.

Change logs in Security Cloud Control

Explains how to use change logs in Security Cloud Control to review configuration changes, track who made them and when, identify conflict entries, compare differences, and export log data for troubleshooting or reporting.

A change log is a configuration tracking feature that

- captures configuration changes made in Security Cloud Control, providing a single view that includes changes in all the supported devices and services
- provides a side-by-side comparison of changes made to device configuration
- records onboarding and removal of devices, and
- detects policy change conflicts occurring outside Security Cloud Control.

Change log management capabilities

Change logs provide these capabilities for configuration management and troubleshooting:

- Provides labels for all change log entries
- Provides answers about who, what, and when during an incident investigation or troubleshooting
- Enables downloading of the complete change log, or only a portion of it, as a CSV file

> **Note**
>
> Changes made in Cloud-Delivered Firewall Management Center are not reflected in the change log.

Change log capacity: Security Cloud Control retains the change log information for one year and deletes data older than a year.

There is a difference between the change log information stored in Security Cloud Control's database and what you see in an exported change log. See Export the change log on page 154 for more information.

Change log entries: A change log entry reflects the changes to a single device configuration, an action performed on a device, or the change made to a device outside Security Cloud Control:

- For change log entries that contain configuration changes, you can view details about the change by clicking anywhere in the corresponding row.
- For out-of-band changes made outside Security Cloud Control and are detected as conflicts, the **System User** is reported as the **Last User**.
- Security Cloud Control closes a change log entry after a device's configuration on Security Cloud Control is synced with the configuration on the device, or when a device is removed from Security Cloud Control. Configurations are considered to be in sync after they read the configuration from the device to Security Cloud Control or after deploying the configuration from Security Cloud Control to the device.
- Security Cloud Control creates a new change log entry immediately after completing an existing entry, irrespective of whether the change was a success or failure. Additional configuration changes are added to the new change log entry that opens.
- Events are displayed for read, deploy, and delete actions for a device. These actions close a device's change log.

- A change log is closed after Security Cloud Control is in sync with the configuration on the device (either by reading or deploying), or when Security Cloud Control no longer manages the device.
- If a change is made to the device outside of Security Cloud Control, a *Conflict detected* entry is included in the change log.

Pending and completed change log entries: Change logs have a status of either Pending or Completed. As you make changes to a device's configuration using Security Cloud Control, these changes are recorded in a Pending change log entry. Activities that complete a Pending change log:

- Reading a configuration from a device to Security Cloud Control
- Deploying changes from Security Cloud Control to a device
- Deleting a device from Security Cloud Control
- Running a CLI command that updates the running configuration file

Search and filter change log entries: You can search and filter change log entries. Use the search field to find events. Use the filter ( ) to find the entries that meet the criteria you specify. You can also combine the two tasks by filtering the change log and adding a keyword to the search field to find an entry within the filtered results.

View change log differences

Configure a side-by-side comparison view to examine added, modified, deleted, and message entries for device configuration changes in the change log.

View change log differences to analyze configuration changes made to devices by examining before and after states of the running configuration file.

Change log differences provide a detailed comparison between the original and modified configuration files, helping you understand what changes were made to device configurations. The side-by-side view highlights additions, modifications, and deletions in the running configuration.

Procedure

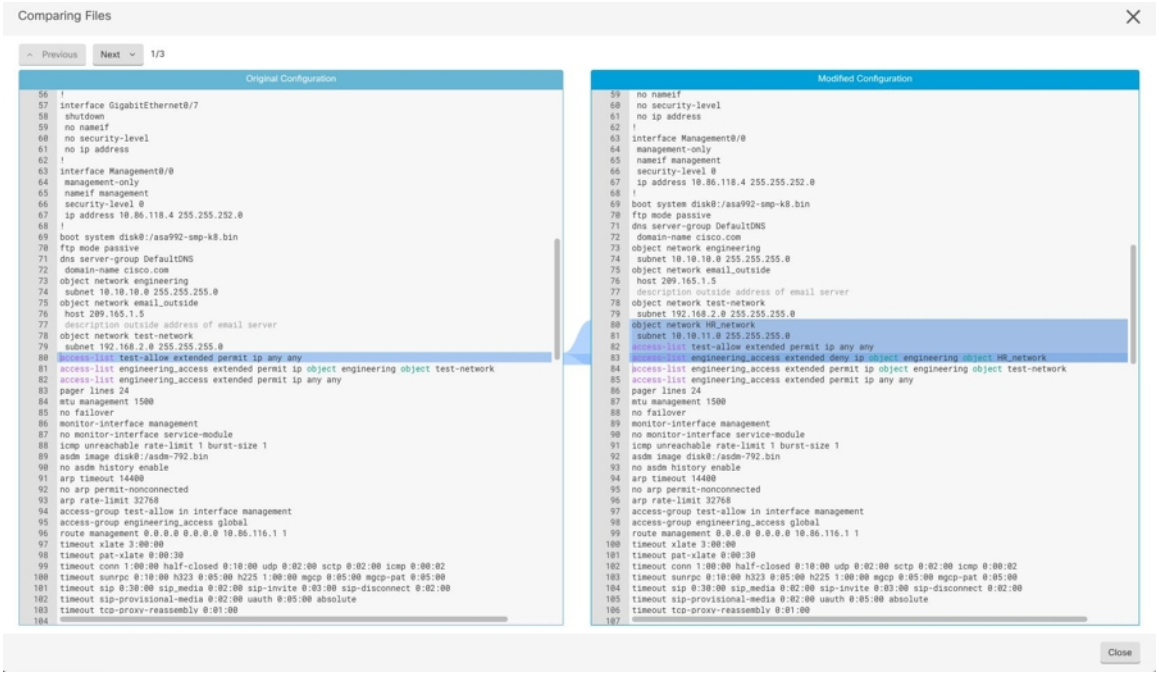
1. Click **Diff** in the change log.

   A side-by-side comparison of the changes in the running configuration file of the device opens.

   The **Original Configuration** column shows the running configuration file before a change was written to the ASA device. The **Modified Configuration** column shows the running configuration file after the change was written.

2. Follow the lines across from the left to the right column to see the changes.

   In the comparison view, you can see additions such as the *HR_network* object and the access rule preventing addresses in the *engineering* network to reach addresses in the *HR_network* network. The **Original Configuration** column highlights rows that provide reference points for understanding the changes in the **Modified Configuration** column.



3. Click **Previous** and **Next** to move through the changes in the file.

You can view and analyze the configuration differences between the original and modified device configurations, understanding exactly what changes were made during the configuration update process.

Change request management

Explains how change request management enables linking business justifications to change log events through third-party ticketing systems.

Change request management is a functionality that

- enables the linking of a **Change Request** and its business justification to a **Change Log** event
- opens the **Change Request** in a third-party ticketing system, and
- allows creation of a **Change Request** in Security Cloud Control and associates it with change log events.

Change request management usage

Use **Change Request Management** to create a **Change Request** in Security Cloud Control and associate it with change log events. You can search for this change request by **Name** within the change log.

> **Note**
>
> In Security Cloud Control, **Change Request Tracking** and **Change Request Management** refer to the same functionality.

Enable change request management

Configure change request tracking to monitor and manage configuration changes across your organization.

Enable change request tracking to provide visibility and control over configuration changes made by all users in your organization.

Enabling change request tracking affects all users of your organization.

Procedure

1. Choose **Administration** > **General Settings**.
2. Enable the **Change Request Tracking** toggle button.



When enabled, the **Change Request** menu appears at the bottom-left corner and the **Change Request** drop-down list is available in the **Change Log** page.

Change request tracking is now enabled for your organization. The Change Request menu is available at the bottom-left corner, and the Change Request drop-down list appears in the Change Log page.

Create a change request

Configure a change request to track and manage device configuration changes in your organization.

Create a change request to organize and track configuration changes that will be made to devices in your network, ensuring proper documentation and oversight of modifications.

Change requests provide a structured way to group related configuration changes and maintain an audit trail of modifications. Once created, all subsequent changes will be associated with the active change request until it is cleared or disabled.

Procedure

1. In Security Cloud Control, click the **Create Change Request** (**+**) icon in the **Change Request** menu at the bottom-left corner.
2. Enter a **Name** and **Description**.

   Ensure that the **Name** corresponds to a **Change Request** name that your organization intends to use, and that the **Description** describes the purpose of the change.

> **Note**
>
> You cannot modify the name of a **Change Request** after you create it.

3. Click **Save**.

> **Note**
>
> When a **Change Request** is saved, Security Cloud Control associates all the new changes with the corresponding **Change Request** name. This association continues until you either disable change requests or clear the change request details from the menu.

The change request is created and becomes the active change request. All subsequent configuration changes will be associated with this change request until you disable change request management or clear the change request details.

Associate a change request with a change log event

Configure the association between a change request and a change log event to track configuration changes.

Associate change requests with change log events to maintain an audit trail and track the reasons for configuration changes.

Use this procedure when you need to link a change request to a specific change log event to document the authorization and rationale for configuration changes.

Procedure

1. In the left pane, click **Events & Logs** > **Logs** > **Change Log**.
2. Expand the change log to view the events you want to associate with a **Change Request**.
3. Click the drop-down list adjacent to the corresponding change log entry.

> **Note**
>
> The latest change requests are displayed at the top of the change request list.

4. Select a change request and click **Select**.

The change request is now associated with the change log event, creating a traceable link between the authorization and the configuration change.

Search for change log events with change requests

Configure search parameters to find change log events that are associated with specific change requests in the system.

This task helps you locate specific change log events by searching for associated change request names, allowing you to track changes and their corresponding documentation.

Use this procedure when you need to find change log events that are linked to particular change requests for auditing, tracking, or analysis purposes.

Procedure

1. In the left pane, click **Events & Logs** > **Logs** > **Change Log**.
2. In the change log search field, enter the name of a change request to find the associated change log events.

   Security Cloud Control highlights the change log events that are exact matches.

The system displays change log events that match your search criteria, with exact matches highlighted for easy identification.

Search for a change request

Configure a search to locate change requests by name or keywords in the change request system.

Enable users to quickly locate existing change requests by searching through names and descriptions using partial matches.

Use this search functionality when you need to find specific change requests among multiple entries in the system.

Procedure

1. In Security Cloud Control, click the **Create Change Request** (**+**) icon in the **Change Request** menu at the bottom-left corner.
2. Enter the name of the **Change Request** or a relevant keyword in the search field. As you enter a value, the results that partially match your input, appear in both the **Name** and **Description** fields.

The system displays change requests that match your search criteria in both the name and description fields, allowing you to locate the desired change request quickly.

Filter change requests

Configure filters to search and view specific change requests in the Change Log table.

Filter change requests to quickly locate and review specific configuration changes or events in your security environment.

Use the filter functionality in the Change Log to narrow down the list of change requests based on specific criteria. This helps you efficiently review and manage configuration changes across your devices.

Procedure

1. In the left pane, click **Events & Logs** > **Logs** > **Change Log**.
2. Click the filter icon to view all the options.
3. In the search field, enter the name of a **Change Request**.

   As you enter a value, the results that partially match your entry appear.
4. Select a change request by checking the corresponding check box.

The matches appear in the **Change Log** table. Security Cloud Control highlights the change log events that are exact matches.

The Change Log table displays only the filtered change requests that match your search criteria, with exact matches highlighted for easy identification.

Clear the change request toolbar

Configure the change request toolbar to avoid automatic association of change log events with an existing change request.

Clear the change request toolbar to prevent change log events from being automatically associated with an existing change request.

When you need to avoid automatic association of change log events with an existing change request, clear the information in the change request toolbar.

Procedure

---

1. Click the **Create Change Request** (**+**) icon in the **Change Request** menu at the bottom-left corner.
2. Click **Clear**.

   The **Change Request** menu now displays **None**.

The change request toolbar is cleared and displays **None**, ensuring that change log events will not be automatically associated with any existing change request.

Clear a change request associated with a change log event

Configure the disassociation of change requests from change log events to remove unwanted connections between these items.

This task allows you to remove the association between a change request and a change log event when the connection is no longer needed or was created in error.

Use this procedure when you need to disassociate change requests from change log events in the Change Log interface. This helps maintain accurate tracking and organization of changes.

Procedure

---

1. In the left pane, click **Events & Logs** > **Logs** > **Change Log**.
2. Expand the **Change Log** to view the events that you want to disassociate from **Change Requests**.
3. Click the drop-down list adjacent to the corresponding change log entry.
4. Click **Clear**.

The change request is successfully disassociated from the selected change log event, and the connection between them is removed.

Delete a change request

Configure the deletion of a change request to remove it from the change request list while preserving it in the change log.

Delete a change request to remove it from the active change request list when it is no longer needed.

Deleting a **Change Request** removes it from the change request list, but not from the **Change Log**.

Procedure

1. Click the **Create Change Request** (**+**) icon in the **Change Request** menu at the bottom-left corner.
2. Select the change request and click the bin icon to delete it.
3. Click the check mark to confirm.

The change request is removed from the change request list but remains available in the change log for historical reference.

Disable change request management

Configure your account to disable Change Request Management or Change Request Tracking features.

This task disables Change Request Management functionality for your account when it is no longer needed or desired.

Disabling **Change Request Management** or **Change Request Tracking** affects all users of your account.

Procedure

1. Choose **Administration** > **General Settings**.
2. Disable the **Change Request Tracking** toggle button.

Change Request Management and Change Request Tracking features are disabled for all users in your account.

Manage change requests and associate change log events

Configure change request management to track changes made to firewall devices and associate them with external tickets or change requests.

This task helps you track changes made to firewall devices and associate them with change requests to resolve tickets maintained in external systems. You can create change requests, associate change log events with them, and search for events related to specific change requests.

These use cases assume that you have enabled Change Request Management. You can use change request management in various scenarios to maintain audit trails and associate firewall changes with external ticketing systems.

Procedure

1. Track changes made to the firewall device to resolve a ticket maintained in an external system.

   This use case describes a scenario where you want to make changes to a firewall device to resolve a ticket maintained in an external system and want to associate the change log events resulting from these firewall changes to a change request.

   a. Create a change request on page 149.

   b. Use the ticket name or number from the external system as the name of the change request and add the justification for the change and other relevant information in the **Description** field.

   c. Ensure that the new change request is visible in the change request toolbar.

   d. Make the changes to the firewall device.

e. In the navigation pane, click **Change Log** and find the change log events that are associated with your new change request.

f. Clear the change request toolbar on page 152 to avoid automatic association of change log events with an existing change request.

2. Manually update individual change log events after changes are made to the firewall device.

   This use case describes a scenario where you have made changes to a firewall device to resolve a ticket that is maintained in an external system, but forgot to use the Change Request Management feature to associate change requests with the change log events. You want to update the change log events with the ticket number.

   a. Create a change request on page 149. Use the ticket name or number from the external system as the name of the change request. Use the **Description** field to add the justification for the change and other relevant information.

   b. In the navigation pane, click **Change Log** and search for the change log events that are associated with the changes.

   c. Associate a change request with a change log event on page 150.

   d. Clear the change request toolbar on page 152 to avoid automatic association of change log events with an existing change request.

3. Search for change log events associated with a change request.

   This use case describes a scenario where, you want to find out what change log events were recorded in the change log because of the work done to resolve a ticket maintained in an external system.

   a. In the navigation pane, click **Change Log.**

   b. Search for change log events that are associated with change requests using one of these methods:

      - In the **Change Log** search field, enter the exact name of the change request to find change log events associated with that change request. Security Cloud Control highlights change log events that are exact matches.
      - Filter change requests on page 151 to find the change log events.

   c. View each change log to find the highlighted change log events showing the associated change request.

You have successfully managed change requests and associated change log events with external tickets. The change log now contains trackable events linked to your change requests, providing an audit trail for firewall modifications.

Export the change log

Configure the export of all or selected change log data to a CSV file so you can filter, sort, and retain change records for reporting or analysis.

Export change log data to a comma-separated value (.CSV) file to enable filtering, sorting, and analysis of change records outside of the system.

You can export all or a subset of the Security Cloud Control change log to a comma-separated value (.CSV) file so that you can filter and sort the information, as required.

To export the change log to a .CSV file, follow this procedure:

Procedure

1. In the left pane, click **Events & Logs** > **Logs** > **Change Log**.
2. Find the changes you want to export by doing one of the following tasks:
   - Use the filter ( ) and the search field to find what you want to export. For example, filter by device to see only the changes for your selected device or devices.
   - Clear all the filters and search criteria in the change log. This allows you to export the entire change log.

   Note

   Security Cloud Control retains 1 year of change log data. It is recommended to filter the change log contents and download the results to a .CSV file rather than downloading the entire change log history for a year.

3. Click the export icon at the top right corner of the page.
4. Save the .CSV file to your local file system, with a descriptive name.

The change log data is exported to a CSV file on your local system, allowing you to perform additional filtering, sorting, and analysis as needed.

Differences between change log capacity in Security Cloud Control and size of an exported change log

Explains the differences between the change log information that Security Cloud Control stores in its database and the information included in an exported change log.

Change log capacity differences are data storage variations that

- distinguish between the complete change log information stored in Security Cloud Control's database and the subset of information included in exported files
- result from different storage requirements for database operations versus export functionality, and
- affect file sizes when users export change log data.

Change log storage structure

For every change log, Security Cloud Control stores two copies of the device's configuration–the *starting* configuration and either the *ending* configuration in the case of a closed change log or the *current* configuration in the case of an open change log. This allows Security Cloud Control to display configuration differences side by side. In addition, Security Cloud Control tracks and stores every step (*change event*) with the username that made the change, the time the change was made, and other details.

However, when you export the change log, the export does not include the two complete copies of the configuration. It only includes the *change events*, which makes the export file much smaller than the change log that Security Cloud Control stores.

Security Cloud Control stores change log information for a year. This includes two copies of the configuration.

Jobs monitoring in Security Cloud Control

Explains how to monitor bulk operations in Security Cloud Control, review job progress and device-level results, search or filter jobs by action, user, or status, and reinitiate or cancel bulk actions.

Jobs monitoring in Security Cloud Control is a management interface that

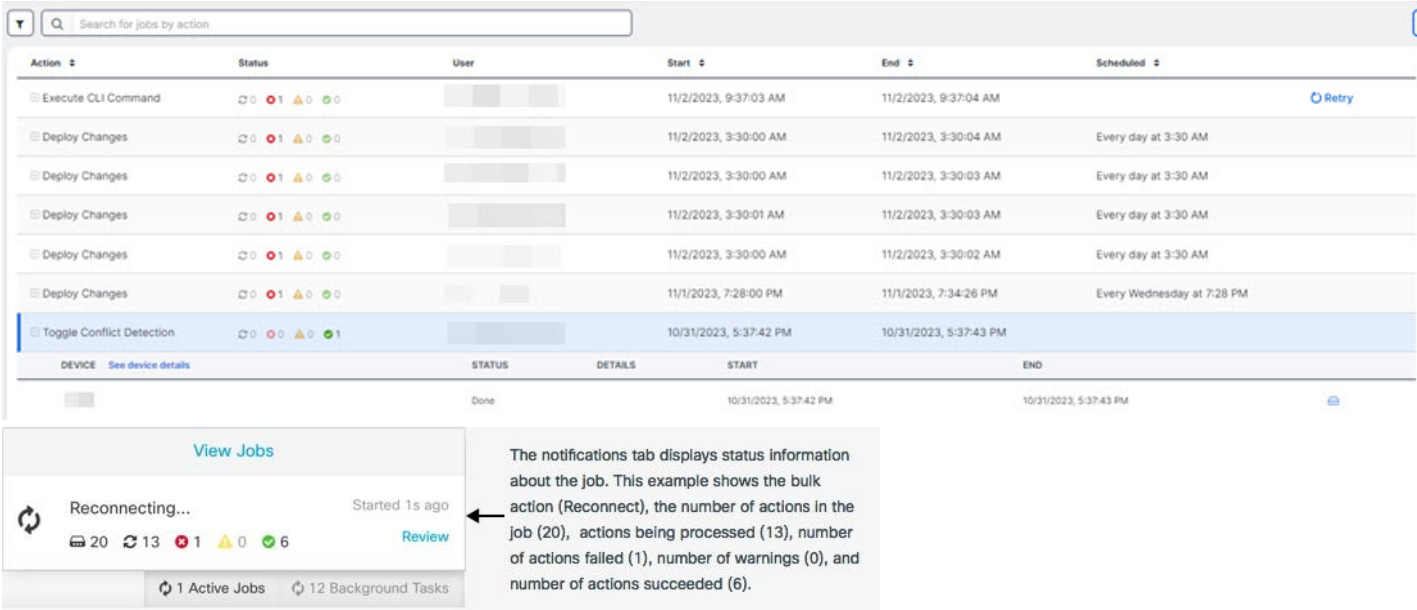
- provides an overview of the progress of bulk operations, such as reconnecting multiple devices, reading configurations from multiple devices, or upgrading multiple devices simultaneously
- uses color-coded rows along with the status of individual actions, indicating if they have succeeded or failed, and
- displays results for each of the devices affected by the bulk operation when a row is expanded.

Job access methods

You can reach the **Jobs** page in two different ways:

- In the **Notifications** tab, when there is a new Job notification, click the **Review** link. You will be redirected to the **Jobs** page and see the specific job represented by the notification.
- In the left pane, click **Events & Logs** > **Events heading** > **Jobs**. This table shows a complete list of the bulk actions performed in Security Cloud Control.

One row in the table represents a single bulk operation. This one bulk operation may have been, for example, an attempt to reconnect 20 devices. Expanding a row in the **Jobs** page displays the results for each of the devices affected by the bulk operation.



When you're on the **Jobs** page, you can filter and search by different actions, the users who performed them, and the action status.

Reinitiate a bulk action

Configure a bulk action retry to address failed actions in a previously executed bulk operation.

This task allows you to retry failed actions within a bulk operation without re-running the entire job.

After reviewing the **Jobs** page, if you find that one or more actions in a bulk action have failed, you can retry the bulk action after making the necessary corrections. Note that Security Cloud Control will re-run the job only for the failed actions.

Procedure

1. In the **Jobs** page, select the row that indicates a failed action.
2. Click the **Retry** (↻) icon.

The system retries only the failed actions from the original bulk operation, and the job status updates accordingly.

Cancel a bulk action

Configure the cancellation of bulk actions that are currently in progress on multiple devices.

Cancel bulk actions that are currently in progress when you need to stop ongoing operations on multiple devices that may be taking longer than expected or are no longer needed.

You can cancel the bulk actions that are currently in progress on multiple devices. For example, if you have tried to reconnect four managed devices, and three of them have successfully reconnected, but the fourth device is still neither connected nor disconnected, you can cancel the bulk action.

Procedure

1. From the Security Cloud Control Home page, click **Firewall**.
2. In the left pane, click **Events & Logs** > **Events heading** > **Jobs**.
3. Identify the running bulk action and click the **Cancel** link on the right side.

> **Note**
>
> If any part of the bulk action is successful, it cannot be undone. Any ongoing action will be cancelled.

The bulk action is cancelled, stopping any ongoing operations while preserving any successfully completed portions of the action.

Monitor workflows in Security Cloud Control

Explains how to monitor Security Cloud Control workflows, troubleshoot failed device or connector tasks, export workflow details for TAC analysis, and copy stack traces for unresolved errors.

Workflow monitoring is a Security Cloud Control capability that

- tracks every process that Security Cloud Control runs when communicating with devices, Secure Device Connector (SDC), or Secure Event Connector (SEC), and when applying ruleset changes to devices,
- creates an entry in the workflow table for every step and displays its outcome, and
- contains information pertaining only to the action performed by Security Cloud Control and not the device it is interacting with.

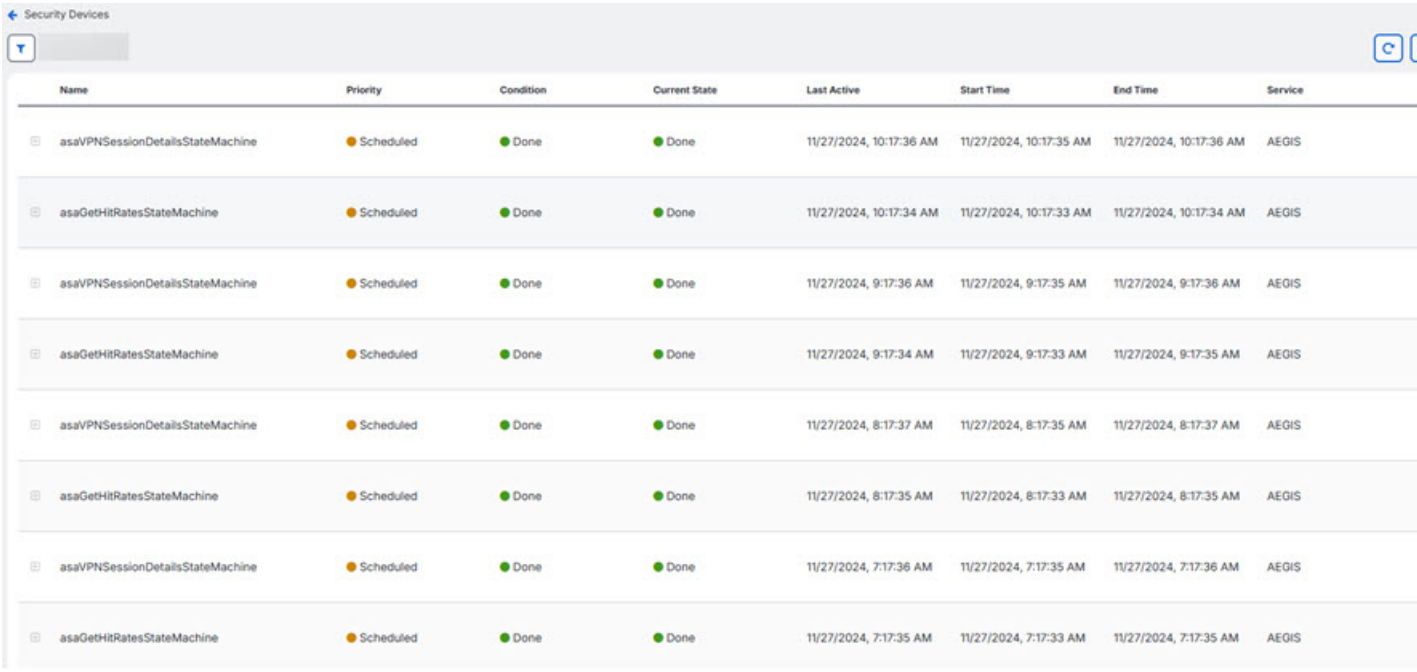
Workflow error reporting and troubleshooting

Security Cloud Control reports an error when it fails to perform a task on a device. Navigate to the **Workflows** page to see the step where the error occurred, for more details.

This page also helps you determine and troubleshoot errors or share information with TAC, when required.

To navigate to the **Workflows** page, in the left pane, click **Security Devices** and, click the **Devices** tab. Click the appropriate device type tab to locate the device and select the device you want. Under the **Devices and Actions** in the right pane, click **Workflows**.

Figure 6: Workflows page with entries in the workflow table



Export device workflows:

- You can download the complete workflow information to a JSON file and provide it when the TAC team asks for further analysis. To export the workflow information, select the corresponding device and, navigate to its **Workflows** page and click the export ( ) icon appearing at the top-right corner.

Copy stack trace:

- If you have an error you cannot resolve and you approach TAC, they may ask you for a copy of the stack trace. To collect the stack trace for the error, click the **Stack Trace** link and click **Copy Stacktrace** to copy the stacks appearing on the screen, to a clipboard.

12 Integrating Security Cloud Control with Cisco Security Cloud Sign On

Topics:

- Merge Your Security Cloud Control and Cisco XDR Tenant Accounts

Merge Your Security Cloud Control and Cisco XDR Tenant Accounts

Learn how to merge your Learn how to merge your Security Cloud Control tenant with SecureX, or Cisco XDR accounts so devices can register, share events, and use connected Cisco security features.

If your Secure Firewall Threat Defense or On-Premises Firewall Management Center is used with Security Cloud Control or Cisco Security Analytics and Logging (SaaS) and Cisco XDR, you must link your Security Cloud Control tenant account with the Cisco XDR tenant account associated with the device.

Be mindful of when you initiate this process. This merging process may take an extended amount of time.

See Merge Accounts for instructions.

Note

If you have accounts on more than one regional cloud, you must merge accounts separately for each regional cloud.

13 Terraform

Topics:

- About Terraform

Learn how to automate the setup and management of your Security Cloud Control organization using Terraform providers and modules.

This chapter explains how to set up and manage Security Cloud Control.

About Terraform

Learn how to use Security Cloud Control Terraform providers and modules to manage users, onboard firewall devices, deploy Secure Device and Event Connectors, and maintain repeatable, version-controlled infrastructure configurations.

Security Cloud Control customers can use the Security Cloud Control Terraform provider and Security Cloud Control Terraform modules to rapidly set up their tenants using code that is repeatable and version-controlled. The Security Cloud Control Terraform provider allows users to do the following:

- **Manage** users
- **Onboard** Secure Firewall Threat Defense devices on Cloud-Delivered Firewall Management Centers, Cisco Secure ASA devices, and iOS devices
- **Onboard** secure device connectors on vSphere and AWS
- **Onboard** secure event connectors on AWS

For more information, refer to the following pages:

- Security Cloud Control Terraform Provider page
- Security Cloud Control SDC on vSphere module page
- Security Cloud Control SDC on AWS module page
- Security Cloud Control SEC on AWS module page
- Work through the Devnet learning lab
- Automating Security Infrastructure Management Using the Security Cloud Control Terraform Provider - Learning Lab
- Security Cloud Control automation examples on GitHub

Support

The Security Cloud Control Terraform provider and modules are published as Open Source Software under the Apache 2.0 license. Please file issues on GitHub in the repositories below if you require support:

Module	Repository
Security Cloud Control Terraform Provider	https://github.com/ciscodevnet/terraform-provider-Security Cloud Control
Security Cloud Control SDC Module (vSphere)	https://github.com/CiscoDevNet/terraform-vsphere-Security Cloud Control-sdc
Security Cloud Control SDC Module (AWS)	https://github.com/CiscoDevNet/terraform-aws-Security Cloud Control-sdc
Security Cloud Control SEC Module (AWS)	https://github.com/CiscoDevNet/terraform-aws-Security Cloud Control-sec

Contribution to repositories

The Security Cloud Control team welcomes contributions to the repositories above. Please create pull pequests on these GitHub repositories if you wish to contribute to improving the provider and modules.

Related topics

- Deploy an SDC to vSphere Using Terraform
- Deploy an SDC to AWS VPC Using Terraform
- Deploy an SEC to AWS VPC Using Terraform

14 Troubleshooting

Topics:

- Troubleshoot a Secure Device Connector
- Troubleshoot Security Cloud Control
- Device connectivity states

This chapter details how to troubleshoot errors that may occur when working with various components in Security Cloud Control Firewall Management.

Troubleshoot a Secure Device Connector

Learn how to troubleshoot Secure Device Connector issues, including unreachable SDCs, inactive status, IP address changes, device connectivity problems, system time errors, version issues, and AWS certificate or connection errors.

Use these topics to troubleshoot an on-premises Secure Device Connector (SDC).

If none of these scenarios match yours, open a case with Cisco Technical Assistance Center.

SDC is Unreachable

An SDC is in the state "Unreachable" if it has failed to respond to two heartbeat requests from Security Cloud Control in a row. If your SDC is unreachable, your tenant will not be able to communicate with any of the devices you have onboarded.

Security Cloud Control indicates that an SDC is unreachable in these ways:

- You see the message, “Some Secure Device Connectors (SDC) are unreachable. You will not be able to communicate with devices associated with these SDCs.” on the Security Cloud Control home page.
- The SDC's status in the Services page is "Unreachable."

Frist, attempt to reconnect the SDC to your tenant to resolve this issue:

1. Check that the SDC virtual machine is running and can reach a Security Cloud Control IP address in your region.

   See Allow inbound access for direct cloud connectivity on page 44.

2. Attempt to reconnect Security Cloud Control and the SDC by requesting a heartbeat manually. If the SDC responds to a heartbeat request, it will return to "Active" status. To request a heartbeat manually:

   a. In the left pane, choose **Administration** > **Integrations** > **Secure Connectors**.

   b. Click the SDC that is unreachable.

   c. In the Actions pane, click **Request Heartbeat**.

   d. Click **Reconnect**.

3. If the SDC does not return to the Active status after manually attempting to reconnect it to your tenant, follow the instructions in SDC Status not Active on Security Cloud Control After Deployment on page 166.

   .

SDC Status not Active on Security Cloud Control After Deployment

If Security Cloud Control does not indicate that your SDC is active in about 10 minutes after deployment, connect to the SDC VM using SSH using the `Security Cloud Control` user and password you created when you deployed the SDC.

Procedure

1. In Security Cloud Control, click on the SDC that isn't showing as active, and click **Request Heartbeat**.
2. Ensure that the container is running using the command:

   ```
   docker ps
   ```

3. View the SDC logs and check for errors using the command:

   ```
   sdc show logs
   ```

4. Restart the container using the command:

```
sdc restart
```

Changed IP Address of the SDC is not Reflected in Security Cloud Control

To view the updated IP address of an SDC, request a heartbeat using the steps provided earlier, and then refresh your browser.

Request a Heartbeat

In Security Cloud Control, click on the SDC that isn't showing as active, and, in the sidebar, click **Request Heartbeat**.

1. Make sure the container is running using the command: `docker ps`
2. View the SDC logs and check for errors using the command `sdc show logs`
3. Restart the container using the command `sdc restart`

Troubleshoot Device Connectivity with the SDC

Use this tool to test connectivity from Security Cloud Control, through the Secure Device Connector (SDC) to your device. You may want to test this connectivity if your device fails to onboard or if you want to determine, before on-boarding, if Security Cloud Control can reach your device.

Procedure

1. In the left pane, click **Administration** > **Integrations** > **Firewall Management Center**, and click the **Secure Connectors** tab.
2. Select the SDC.
3. In the **Troubleshooting** pane on the right, click **Device Connectivity**.
4. Enter a valid IP address or FQDN and port number of the device you are attempting to troubleshoot, or attempting to connect to, and click **Go**. Security Cloud Control performs the following verifications:
   a) **DNS Resolution** - If you provide a FQDN instead of an IP address, this verifies the SDC can resolve the domain name and acquires the IP address.
   b) **Connection Test** - Verifies the device is reachable.
   c) **TLS Support** - Detects the TLS versions and ciphers that both the device and the SDC support.
      - **Unsupported Cipher** - If there are no TLS version that are supported by both the device and the SDC, Security Cloud Control also tests for TLS versions and ciphers that are supported by the device, but not the SDC.

   d) SSL Certificate - The troubleshoot provides certificate information.
5. If you continue to have issues onboarding or connecting to the device, contact Security Cloud Control support.

Intermittent or No Connectivity with SDC

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies only to an on-premise SDC and if you are still using CentOS.

Symptom: Intermittent or no connectivity with SDC.

Diagnosis: This problem may occur if the disk space is almost full (above 80%).

Perform the following steps to check the disk space usage.

1. Open the console for your Secure Device Connector (SDC) VM.
2. Log in with the username **cdo**.
3. Enter the password created during the initial login.
4. First, check the amount of free disk space by typing `df -h` to confirm that there is no free disk space available.

   You can confirm that the disk space was consumed by the Docker. The normal disk usage is expected to be under 2 Gigabytes.
5. To see the disk usage of the **Docker** folder,

   execute `sudo du -h /var/lib/docker | sort -h`.

   You can see the disk space usage of the **Docker** folder.

Procedure

If the disk space usage of the Docker folder is almost full, define the following in the docker config file:

- Max-size: To force a log rotation once the current file reaches the maximum size.
- Max-file: To delete excess rotated log files when the maximum limit it reached.

Perform the following:

1. Execute `sudo vi /etc/docker/daemon.json`.
2. Insert the following lines to the file.

```
{
"log-driver": "json-file",
"log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. Press **ESC** and then type `:wq!` to write the changes and close the file.

   > **Note**
   >
   > You can execute `sudo cat /etc/docker/daemon.json` to verify the changes made to the file.

4. Execute `sudo systemctl restart docker` to restart the docker file.

   It will take a few minutes for the changes to take effect. You can execute `sudo du -h /var/lib/docker | sort -h` to see the updated disk usage of the docker folder.
5. Execute `df -h` to verify that the free disk size has increased.
6. Before your SDC status can change from Unreachable to Active, you must go to the **Secure Connectors** tab which you can navigate to from **Administration** > **Integrations** > **Firewall Management Center** and click **Request Reconnect** from the Actions menu.

Container Privilege Escalation Vulnerability Affecting Secure Device Connector: cisco-sa-20190215-runc

The Cisco Product Security Incident Response Team (PSIRT) published the security advisory **cisco-sa-20190215-runc** which describes a high-severity vulnerability in Docker. Read the entire PSIRT team advisory for a full explanation of the vulnerability.

This vulnerability impacts all Security Cloud Control customers:

- Customers using Security Cloud Control's cloud-deployed Secure Device Connector (SDC) do not need to do anything as the remediation steps have already been performed by the Security Cloud Control Operations Team.
- Customers using an SDC deployed on-premise need to upgrade their SDC host to use the latest Docker version. They can do so by using the following instructions:
  - Updating a Security Cloud Control-Standard SDC Host on page 169
  - Updating a Custom SDC Host on page 170
  - Bug Tracking on page 170

Updating a Security Cloud Control-Standard SDC Host

- The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

  For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

  This procedure applies if you are still using CentOS.
- Use these instructions if you deployed an SDC using the Security Cloud Control image.

Procedure

1. Connect to your SDC host using SSH or the hypervisor console.
2. Check the version of your Docker service by running this command:

```
docker version
```

3. If you are running one of the latest virtual machines (VMs) you should see output like this:

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

   It's possible you may see an older version here.

4. Run the following commands to update Docker and restart the service:

```
> sudo yum update docker-ce
> sudo service docker restart
```

> **Note**
>
> There will be a brief connectivity outage between Security Cloud Control and your devices while the docker service restarts.

5. Run the docker version command again. You should see this output:

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

6. You are done. You have now upgraded to the latest, and patched, version of Docker.

Updating a Custom SDC Host

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies if you are still using CentOS.

- If you have created your own SDC host you will need to follow the instructions to update based on how you installed Docker. If you used CentOS, yum and Docker-ce (the community edition) the preceding procedure will work.
- If you have installed Docker-ee (the enterprise edtion) or used an alternate method to install Docker, the fixed versions of Docker may be different. You can check the Docker page to determine the correct versions to install: Docker Security Update and Container Security Best Practices.

Bug Tracking

Cisco is continuing to evaluate this vulnerability and will update the advisory as additional information becomes available. After the advisory is marked Final, you can refer to the associated Cisco bug for further details:

CSCvo33929-CVE-2019-5736: runc container breakout

Invalid System Time

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies if you are still using CentOS.

- Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control must migrate your existing SDC to the new communication method by February 1, 2024.

  Note

  If your SDC is not migrated by February 1, 2024, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

- Security Cloud Control's operations team attempted to migrate your SDC but was unsuccessful because your SDC system time was 15 minutes ahead or behind the AWS system time.

Follow the steps below to correct the system time issue. Once this problem is resolved, you can proceed with the migration.

Procedure

1. Login to your SDC VM throught the VM terminal or by making an SSH connection.
2. At the prompt, enter `sudo sdc-onboard setup` and authenticate.
3. You are now going to respond to the SDC setup questions as if you are were setting up the SDC for the first time. Re-enter all the same passwords and network information as you had before, except take special note of the NTP server address:
   a) Reset the root and Security Cloud Control user passwords with the same passowrds you used to setup the SDC.
   b) When prompted, enter **y** to re-configure the network.
   c) Enter the value for IP address/CIDR as you had before.
   d) Enter the value for the network gateway as you had before.
   e) Enter the value for the DNS Server as you had before.
   f) When prompted for the NTP server, be sure to provide a valid NTP server address, such as `time.aws.com`.
   g) Review the values you provided and enter **y** if they are correct.
4. Validate that your time server is reachable and synchronized with your SDC by entering `date` at the prompt. The UTC date and time are displayed and you can compare it to your SDC time.

   Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the Security Cloud Control operations team can complete your SDC migration to the new communication method.

SDC version is lower than 202311****

The Secure Device Connector (SDC) has been installed on CentOS 7 virtual machines up to now. However, as CentOS has reached its end-of-life and is no longer supported by Firewall in Security Cloud Control, we recommend migrating all SDCs from CentOS 7 to an Ubuntu virtual machine.

For more information, see Migrate an On-Premises Secure Device Connector and Secure Event Connector from a CentOS 7 Virtual Machine to an Ubuntu Virtual Machine.

This procedure applies if you are still using CentOS.

- Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control must migrate your existing SDC to the new communication method by February 1, 2024.

> **Note**
>
> If your SDC is not migrated by February 1, 2024, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

- Security Cloud Control's operations team attempted to migrate your SDC but was unsuccessful because your tenant is running a version lower than 202311****.
- The current version of your SDC is listed on the Secure Connectors page by navigating from the Security Cloud Control navigation menu, **Administration** > **Integrations** > **Secure Connectors**. After selecting your SDC, its version number is found in the **Details** pane on the right of the screen.

Please follow the steps below to upgrade the SDC version. Once this problem is resolved, Security Cloud Control operations will run the migration process again.

Procedure

1. Log in to the SDC VM and authenticate.
2. At the prompt, enter `sudo su - sdc` and authenticate.
3. At the prompt, enter `crontab -r`.

   If you receive the message `no crontab for sdc` you can ignore it and move to the next step.
4. At the prompt, enter `./toolkit/toolkit.sh upgrade`. Security Cloud Control will determine if you need an upgrade and upgrade the toolkit. Ensure that no errors were reported in the console.
5. Verify the new version of the SDC:
   a) Log in to Security Cloud Control.
   b) Navigate to the Secure Connectors page by navigating from the Security Cloud Control menu bar, **Tools & Services** > **Secure Connectors**.
   c) Select your SDC and click **Request Heartbeat** in the **Actions** pane.
   d) Validate that the SDC version is 202311**** or later.

   Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the Security Cloud Control operations team can run the migration process again.

Certificate or Connection errors with AWS servers

Security Cloud Control is adapting a new way of communicating with the Secure Device Connector (SDC). To facilitate this, Security Cloud Control must migrate your existing SDC to the new communication method by February 1, 2024.

Note

If your SDC is not migrated by February 1, 2024, Security Cloud Control will no longer be able to communicate with your devices through the SDC.

Security Cloud Control's operations team attempted to migrate your SDC but was unsuccessful because they experienced a connection issue.

Please follow the steps below to correct the connection issue. Once this problem is resolved, we will be able to proceed with the migration.

Procedure

1. Create firewall rules that allow outbound proxy connections, on port 443, to the domains in your region:
   - Production tenants in the Australia region:
     - cognito-identity.ap-southeast-2.amazonaws.com
     - cognito-idp.ap-southeast-2.amazonaws.com
     - sns.ap-southeast-2.amazonaws.com
     - sqs.ap-southeast-2.amazonaws.com
   - Production tenants in the India region:
     - cognito-identity.ap-south-1.amazonaws.com
     - cognito-idp.ap-south-1.amazonaws.com
     - sns.ap-south-1.amazonaws.com
     - sqs.ap-south-1.amazonaws.com
   - Production tenants in the US region:
     - cognito-identity.us-west-2.amazonaws.com
     - cognito-idp.us-west-2.amazonaws.com
     - sns.us-west-2.amazonaws.com
     - sqs.us-west-2.amazonaws.com
   - Production tenants in the EU region:
     - cognito-identity.eu-central-1.amazonaws.com
     - cognito-idp.eu-central-1.amazonaws.com
     - sns.eu-central-1.amazonaws.com
     - sqs.eu-central-1.amazonaws.com
   - Production tenants in the APJ region:
     - cognito-identity.ap-northeast-1.amazonaws.com
     - cognito-idp.ap-northeast-1.amazonaws.com

- sqs.ap-northeast-1.amazonaws.com
- sns.ap-northeast-1.amazonaws.com

2. You can determine the full list of IP addresses you need to add to your firewall's "allow list" by using one of the commands below.

> **Note**
>
> The commands below are for users that have **jq** installed. The IP addresses will be displayed in a single list.

- Production tenants in the US region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[]
 | select( (.service == "AMAZON" ) and .region == "us-west-2") | .ip_prefix'
```

- Production tenants in the EU region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[]
 | select( (.service == "AMAZON" ) and .region == "eu-central-1") |
.ip_prefix'
```

- Production tenants in the APJ region:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[]
 | select( (.service == "AMAZON" ) and .region == "ap-northeast-1") |
.ip_prefix'
```

> **Note**
>
> If you don't have **jq** installed, you can use this shortened version of the command:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json
```

Contact the Cisco Technical Assistance Center (TAC) once you have completed these steps, or in case you encounter any errors. Once you have successfully completed these steps, the Security Cloud Control operations team can complete your SDC migration to the new communication method.

Troubleshoot Security Cloud Control

Learn how to troubleshoot Security Cloud Control issues, including login failures, access and certificate problems, and object-related errors.

Troubleshooting login failures

If you can't log in or you can't reach Security Cloud Control Firewall Management, try one of these troubleshooting tips.

Login Fails Because You are Inadvertently Logging in to the Wrong Security Cloud Control Region

Make sure you are logging in to the appropriate Security Cloud Control region. After you log in to https://sign-on.security.cisco.com, you will be given a choice of what region to access.

Troubleshooting Login Failures after Migration

Login to Security Cloud Control Fails Because of Incorrect Username or Password

If you try to log in to Security Cloud Control and you *know* you are using the correct username and password and your login is failing, or you try the "forgot password" option and cannot recover a viable password, you may have tried to log in without creating a new Cisco Security Cloud Sign On account. You need to sign up for a new Cisco Security Cloud Sign On Account.

Login to the Cisco Security Cloud Sign On Dashboard Succeeds but You Can't Launch Security Cloud Control

You may have created a Cisco Security Cloud Sign On account with a different username than your Security Cloud Control tenant. Contact the Cisco Technical Assistance Center (TAC) to standardize your user information between Security Cloud Control and Cisco Secure Sign-On.

Login Fails Using a Saved Bookmark

You may be attempting to log in using an old bookmark you saved in your browser. The bookmark could be pointing to https://cdo.onelogin.com.

Log in to https://sign-on.security.cisco.com.

- If you have created your new secure sign-on account, click the Security Cloud Control tile on the dashboard that corresponds to the region in which your tenant was created:
  - Security Cloud Control APJ
  - Security Cloud Control Australia
  - Security Cloud Control EU
  - Security Cloud Control India
  - Security Cloud Control US
- Update your bookmark to point to https://sign-on.security.cisco.com.

Troubleshooting Access and Certificates

Resolve New Fingerprint Detected State

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Select the device in the **New Fingerprint Detected** state.
5. Click **Review Fingerprint** in the New Fingerprint Detected pane.
6. When prompted to review and accept the fingerprint:
   a. Click **Download Fingerprint** and review it.
   b. If you are satisfied with the fingerprint, click **Accept**. If you are not, click **Cancel**.

7. After you resolve the new fingerprint issue, the connectivity state of the device may show **Online** and the Configuration Status may show "Not Synced" or "Conflict Detected." Review Resolve Configuration Conflicts to review and resolve configuration differences between Security Cloud Control and the device.

Troubleshooting network problems using Security and Analytics Logging events

Troubleshoot network problems using security and analytics logging events by reviewing symptoms, configuration details, likely causes, and corrective actions for managed devices.

Here is a basic framework you can use to troubleshoot network problems using the Events Viewer.

This scenario assumes that your network operations team has had a report that a user can't access a resource on the network. Based on the user reporting the issue and their location, the network operations team has a reasonable idea of which firewall controls their access to resources.

> **Note**
>
> This scenario also assumes that an FDM-managed device is the firewall managing the network traffic. Security Analytics and Logging does not collect logging information from other device types.

Procedure

---

1. In the left pane, click **Events & Logs** > **Events** > **Event Logging**.
2. Click the **Historical** tab.
3. Start filtering events by **Time Range**. By default, the Historical tab shows the last hour of events. If that is the correct time range, enter the current date and time as the **End** time. If that is not the correct time range, enter a start and end time encompassing the time of the reported issue.
4. Enter the IP address of the firewall that you suspect is controlling the user's access in the **Sensor ID** field. If it could be more than one firewall, filter events using **attribute:value** pairs in the search bar. Make two entries and combine them with an OR statement. For example: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.
5. Enter the user's IP address in the **Source IP** field in the Events filter bar.
6. If the user can't access a resource, try entering that resource's IP address in the **Destination IP** field.
7. Expand the events in the results and look at their details. Here are some details to look at:
   - **AC_RuleAction** - The action taken (Allow, Trust, Block) when the rule was triggered.
   - **FirewallPolicy** - The policy in which the rule that triggered the event resides.
   - **FirewallRule** - The name of the rule that triggered the event. If the value is Default Action then it was the default action of the policy that triggered the event and not one of the rules in the policy.
   - **UserName** - The user associated with the initiator IP address. The Initiator IP address is the same as the Source IP address.
8. If the rule action is preventing access, look at the FirewallRule and FirewallPolicy fields to identify the rule in the policy that is blocking access.

Troubleshooting SSL Decryption Issues

Handling Web Sites Where Decrypt Re-sign Works for a Browser but not an App (SSL or Certificate Authority Pinning)

Some apps for smart phones and other devices use a technique called SSL (or Certificate Authority) pinning. The SSL pinning technique embeds the hash of the original server certificate inside the app itself. As a result, when the app receives the resigned certificate from the Firepower Threat Defense device, the hash validation fails and the connection is aborted.

The primary symptom is that users cannot connect to the web site using the site's app, but they can connect using the web browser, even when using the browser on the same device where the app fails. For example, users cannot use the Facebook iOS or Android app, but they can point Safari or Chrome at https://www.facebook.com and make a successful connection.

Because SSL pinning is specifically used to avoid man-in-the-middle attacks, there is no workaround. You must choose between the following options:

More Details

If a site works in a browser but not in an app on the same device, you are almost certainly looking at an instance of SSL pinning. However, if you want to delve deeper, you can use connection events to identify SSL pinning in addition to the browser test.

There are two ways an app might deal with hash validation failures:

- Group 1 apps, such as Facebook, send an SSL ALERT Message as soon as it receives the SH, CERT, SHD message from the server. The Alert is usually an "Unknown CA (48)" alert indicating SSL Pinning. A TCP Reset is sent following the Alert message. You should see the following symptoms in the event details:
  - `SSL Flow Flags include ALERT_SEEN.`
  - `SSL Flow Flags do not include APP_DATA_C2S or APP_DATA_S2C.`
  - `SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE.`
- Group 2 apps, such as Dropbox, do not send any alerts. Instead they wait until the handshake is done and then send a TCP Reset. You should see the following symptoms in the event:
  - `SSL Flow Flags do not include ALERT_SEEN, APP_DATA_C2S, or APP_DATA_S2C.`
  - `SSL Flow Messages typically are: CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED.`

Troubleshooting Login Failures after Migration

Login to Security Cloud Control Fails Because of Incorrect Username or Password

If you try to log in to Security Cloud Control and you *know* you are using the correct username and password and your login is failing, or you try the "forgot password" option and cannot recover a viable password, you may have tried to log in without creating a new Cisco Security Cloud Sign On account. You need to sign up for a new Cisco Security Cloud Sign On Account.

Login to the Cisco Security Cloud Sign On Dashboard Succeeds but You Can't Launch Security Cloud Control

You may have created a Cisco Security Cloud Sign On account with a different username than your Security Cloud Control tenant. Contact the Cisco Technical Assistance Center (TAC) to standardize your user information between Security Cloud Control and Cisco Secure Sign-On.

Login Fails Using a Saved Bookmark

You may be attempting to log in using an old bookmark you saved in your browser. The bookmark could be pointing to https://cdo.onelogin.com.

Log in to https://sign-on.security.cisco.com.

- If you have created your new secure sign-on account, click the Security Cloud Control tile on the dashboard that corresponds to the region in which your tenant was created:
  - Security Cloud Control APJ
  - Security Cloud Control Australia
  - Security Cloud Control EU
  - Security Cloud Control India
  - Security Cloud Control US
- Update your bookmark to point to https://sign-on.security.cisco.com.

Device connectivity states

Learn how to interpret device connectivity states in Security Cloud Control and troubleshoot issues such as offline devices, insufficient licenses, invalid credentials, onboarding errors, new certificates, and unregistered devices.

You can view the connectivity states of the devices onboarded in your Security Cloud Control tenant. This topic helps you understand the various connectivity states. On the **Security Devices** page, the **Connectivity** column displays the device connectivity states.

When the device connectivity state is 'Online' it means that the device is powered on and connected to Security Cloud Control. The other states described in the table below usually occur when the device is running into problems for various reasons. The table provides the method to recover from such problems. It may be that there is more than one problem causing the connection failure. When you attempt to reconnect, Security Cloud Control will prompt you to fix all of these problems first before performing the reconnect.

Device Connectivity State	Possible Reasons	Resolution
Online	Device is powered on and connected to Security Cloud Control.	NA
Offline	Device is powered down or lost network connectivity.	Check whether the device is offline.
Insufficient licenses	Device doesn't have sufficient licenses.	Troubleshoot Insufficient Licenses on page 179
Invalid credentials	Username and password combination used by Security Cloud Control to connect to the device is incorrect.	Troubleshoot Invalid Credentials on page 179
Onboarding	Device onboarding is initiated but is not complete.	Check you device's connectivity and ensure you complete the device registration.

Device Connectivity State	Possible Reasons	Resolution
Unknown	Device onboarding failed and Security Cloud Control cannot fetch the connectivity state of the device.	On the **Security Devices** page, select the device and choose **Check for Changes** from the right pane, to attempt fetching the latest configuration from the device.
New Certificate Detected	Certificate on the device has changed. If the device uses a self-signed certificate, then this could have happened due to the device being power cycled.	Troubleshoot New Certificate Issues on page 180
Onboarding Error	Security Cloud Control may have lost connectivity with the device when onboarding it.	Troubleshoot Onboarding Error on page 188

Troubleshoot Insufficient Licenses

If the device connectivity status shows "Insufficient License", do the following:

- Wait for some time until the device attains the license. Typically it takes some time for Cisco Smart Software Manager to apply a new license to the device.
- If the device status doesn't change, refresh the Security Cloud Control portal by signing out from Security Cloud Control and signing back to resolve any network communication glitch between license server and device.
- If the portal refresh doesn't change the device status, perform the following:

Procedure

1. Generate a new token from Cisco Smart Software Manager and copy it. You can watch the Generate Smart Licensing video for more information.
2. In the left pane, click **Security Devices**.
3. Click the **Devices** tab.
4. Click the appropriate device type tab and select the device with the **Insufficient License** state.
5. In the **Device Details** pane, click **Manage Licenses** appearing in **Insufficient Licenses**. The **Manage Licenses** window appears.
6. In the **Activate** field, paste the new token and click **Register Device**.

   Once the token is applied successfully to the device, its connectivity state turns to **Online**.

Troubleshoot Invalid Credentials

Perform the following to resolve device disconnection due to invalid credentials:

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.

3. Click the appropriate device type tab and select the device with the **Invalid Credentials** state.
4. In the **Device Details** pane, click **Reconnect** appearing in **Invalid Credentials**. Security Cloud Control attempts to reconnect with your device.
5. When prompted enter the new username and password for the device.
6. Click **Continue**.
7. After the device is online and ready to use, click **Close**.
8. It is likely that because Security Cloud Control attempted to use the wrong credentials to connect to the device, the username and password combination Security Cloud Control should use to connect to the device was changed directly on the device. You may now see that the device is "Online" but the configuration state is "Conflict Detected." Use Resolve Configuration Conflicts to review and resolve configuration differences between Security Cloud Control and the device.

Troubleshoot New Certificate Issues

Security Cloud Control's Use of Certificates

Security Cloud Control checks the validity of certificates when connecting to devices. Specifically, Security Cloud Control requires that:

1. The device uses a TLS version equal to or greater than 1.0.
2. The certificate presented by the device is not expired, and its issuance date is in the past (i.e. it is already valid, not scheduled to become valid at a later date).
3. The certificate must be a SHA-256 certificate. SHA-1 certificates will not be accepted.
4. One of these conditions is true:
   - The device uses a self-signed certificate, and it is the same as the most recent one trusted by an authorized user.
   - The device uses a certificate signed by a trusted Certificate Authority (CA), and provides a certificate chain linking the presented leaf certificate to the relevant CA.

These are the ways Security Cloud Control uses certificates differently than browsers:

- In the case of self-signed certificates, Security Cloud Control overrides the domain name check, instead checking that the certificate exactly matches the one trusted by an authorized user during device onboarding or reconnection.
- Security Cloud Control does not yet support internal CAs. There is currently no way to check a certificate signed by an internal CA.

  It is possible to disable certificate checking for ASA devices on a per-device basis. When an ASA's certificate cannot be trusted by Security Cloud Control, you will have the option of disabling certificate checking for that device. If you have attempted to disable certificate checking for the device and you are still unable to onboard it, it is likely that the IP address and port you specified for the device is incorrect or unreachable. There is no way to disable certificate checking globally, or to disable certificate checking for a device with a supported certificate. There is no way to disable certificate checking for non-ASA devices.

  When you disable certificate checking for a device, Security Cloud Control will still use TLS to connect to the device, but it will not validate the certificate used to establish the connection. This means that a passive man-in-the-middle attacker will not be able to eavesdrop on the connection, but an active man-in-the-middle could intercept the connection by supplying Security Cloud Control with an invalid certificate.

Identifying Certificate Issues

There are several reasons that Security Cloud Control may not be able to onboard a device. When the UI shows a message that "Security Cloud Control cannot connect to the device using the certificate presented," there is a problem with the

certificate. When the UI does not show this message, the problem is more likely related to connectivity problems (the device is unreachable) or other network errors.

To determine why Security Cloud Control rejects a given certificate, you can use the openssl command-line tool on the SDC host or another host that can reach the relevant device. Use the following command to create a file showing the certificates presented by the device:

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

This command will start an interactive session, so you will need to use Ctrl-c to exit after a couple of seconds.

You should now have a file containing output like the following:

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN =
*.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
```

```
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB

    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

The first thing to note in this output is the last line, where you see the **Verify return code**. If there is a certificate issue, the return code will be non-zero and there will be a description of the error.

Expand this list of certificate error code to see common errors and how to remediate them

0 X509_V_OK The operation was successful.

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT The issuer certificate of an untrusted certificate could not be found.

3 X509_V_ERR_UNABLE_TO_GET_CRL The CRL of a certificate could not be found.

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value. This is only meaningful for RSA keys.

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE The CRL signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value. Unused.

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY The public key in the certificate SubjectPublicKeyInfo could not be read.

7 X509_V_ERR_CERT_SIGNATURE_FAILURE The signature of the certificate is invalid.

8 X509_V_ERR_CRL_SIGNATURE_FAILURE The signature of the certificate is invalid.

9 X509_V_ERR_CERT_NOT_YET_VALID The certificate is not yet valid: the notBefore date is after the current time. See Verify return code: 9 (certificate is not yet valid) below for more information.

10 X509_V_ERR_CERT_HAS_EXPIRED The certificate has expired; that is, the notAfter date is before the current time. See Verify return code: 10 (certificate has expired) below for more information.

11 X509_V_ERR_CRL_NOT_YET_VALID The CRL is not yet valid.

12 X509_V_ERR_CRL_HAS_EXPIRED The CRL has expired.

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD The certificate notBefore field contains an invalid time.

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD The certificate notAfter field contains an invalid time.

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD The CRL lastUpdate field contains an invalid time.

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD The CRL nextUpdate field contains an invalid time.

17 X509_V_ERR_OUT_OF_MEM An error occurred trying to allocate memory. This should never happen.

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT The passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates.

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN The certificate chain could be built up using the untrusted certificates but the root could not be found locally.

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY The issuer certificate of a locally looked up certificate could not be found. This normally means the list of trusted certificates is not complete.

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE No signatures could be verified because the chain contains only one certificate and it is not self-signed. See "Verify return code: 21 (unable to verify the first certificate)" below for more information. Verify return code: 21 (unable to verify the first certificate) below for more information.

22 X509_V_ERR_CERT_CHAIN_TOO_LONG The certificate chain length is greater than the supplied maximum depth. Unused.

23 X509_V_ERR_CERT_REVOKED The certificate has been revoked.

24 X509_V_ERR_INVALID_CA A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.

25 X509_V_ERR_PATH_LENGTH_EXCEEDED The basicConstraints pathlength parameter has been exceeded.

26 X509_V_ERR_INVALID_PURPOSE The supplied certificate cannot be used for the specified purpose.

27 X509_V_ERR_CERT_UNTRUSTED The root CA is not marked as trusted for the specified purpose.

28 X509_V_ERR_CERT_REJECTED The root CA is marked to reject the specified purpose.

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH The current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate. Only displayed when the -issuer_checks option is set.

30 X509_V_ERR_AKID_SKID_MISMATCH The current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate. Only displayed when the -issuer_checks option is set.

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH The current candidate issuer certificate was rejected because its issuer name and serial number were present and did not match the authority key identifier of the current certificate. Only displayed when the -issuer_checks option is set.

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN The current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing.

50 X509_V_ERR_APPLICATION_VERIFICATION An application specific error. Unused.

New Certificate Detected

If you upgrade a device that has a self-signed certificate and a new certificate is generated after the upgrade process, Security Cloud Control may generate a "New Certificate Detected" message as both a **Configuration Status** and **Connectivity** status. You must manually confirm and resolve this issue before you can continue managing it from Security Cloud Control. Once the certificate is synchronized and the device is in a healthy state, you can manage the device.

> **Note**
>
> When you bulk reconnect more than one managed device to Security Cloud Control at the same time, Security Cloud Control automatically reviews and accepts the new certificates on the devices and continues to reconnect with them.

Use the following procedure to resolve a new certificate:

1. In the left pane, click **Security Devices**.
2. Use the filter to display devices with a **New Certificate Detected** connectivity or configuration status and select the desired device.
3. In the action pane, click **Review Certificate**. Security Cloud Control allows you to download the certificate for review and accept the new certificate.
4. In the Device Sync window, click **Accept** or in the Reconnecting to Device window, click **Continue**.

   Security Cloud Control automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the page to see the device once it's synced.

Certificate Error Codes

Verify return code: 0 (ok) but Security Cloud Control returns certificate error

Once Security Cloud Control has the certificate, it attempts to connect to the URL of the device by making a GET call to "https://<device_ip>:<port>". If this does not work, Security Cloud Control will display a certificate error. If you find that the certificate is valid (openssl returns 0 ok) the problem may be that a different service is listening on the port you're trying to connect to. You can use the command:

```
 curl -k -u <username>:<password>
https://<device_id>:<device_port>/admin/exec/show%20version
```

to determine whether you are definitely talking to an ASA and check if HTTPS server running on the correct port on the ASA:

```
 # show asp table socket
Protocol         Socket         State         Local Address             Foreign
 Address
SSL              00019b98         LISTEN        192.168.1.5:443
0.0.0.0:*
SSL              00029e18         LISTEN        192.168.2.5:443
0.0.0.0:*
TCP              00032208         LISTEN        192.168.1.5:22
0.0.0.0:*
```

Verify return code: 9 (certificate is not yet valid)

This error means that the issuance date of the certificate provided is in the future, so clients will not treat it as valid. This can be caused by a poorly-constructed certificate, or in the case of a self-signed certificate it can be cause by the device time being wrong when it generated the certificate.

You should see a line in the error including the notBefore date of the certificate:

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
```

```
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

From this error, you can determine when the certificate will become valid.

Remediation

The notBefore date of the certificate needs to be in the past. You can reissue the certificate with an earlier notBefore date. This issue can also arise when the time is not set correctly either on the client or issuing device.

Verify return code: 10 (certificate has expired)

This error means that at least one of the certificates provided has expired. You should see a line in the error including the notBefore date of the certificate:

```
 error 10 at 0 depth lookup:certificate has expired
```

The expiration date is located in the certificate body.

Remediation

If the certificate is truly expired, the only remediation is to get another certificate. If the certificate's expiration is still in the future, but openssl claims that it is expired, check the time and date on your computer. For instance, if a certificate is set to expire in the year 2020, but the date on your computer is in 2021, your computer will treat that certificate as expired.

Verify return code: 21 (unable to verify the first certificate)

This error indicates that there is a problem with the certificate chain, and openssl cannot verify that the certificate presented by the device should be trusted. Let's look at the certificate chain from the example above to see how certificate chains should work:

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

The certificate chain is a list of certificates presented by the server, beginning with the server's own certificate and then including increasingly higher-level intermediate certificates linking the server's certificate with a Certificate Authority's top-level certificate. Each certificate lists its Subject (the line starting with 's:' and its Issuer (the line starting with 'i').

The Subject is the entity identified by the certificate. It includes the Organization name and sometimes the Common Name of the entity for which the certificate was issued.

The Issuer is the entity that issued the certificate. It also includes an Organization field and sometimes a Common Name.

If a server had a certificate issued directly by a trusted Certificate Authority, it would not need to include any other certificates in its certificate chain. It would present one certificate that looked like:

```
--- Certificate chain 0
s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com i:/C=US/O=Trusted
 Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

Given this certificate, openssl would verify that the ExampleCo certificate for ***.example.com** was correctly signed by the Trusted Authority certificate, which would be present in openssl's built-in trust store. After that verification, openssl would successfully connect to the device.

However, most servers do not have certificates signed directly by a trusted CA. Instead, as in the first example, the server's certificate is signed by one or more intermediates, and the highest-level intermediate has a certificate signed by the trusted CA. OpenSSL does not trust these intermediate CAs by default, and can only verify them if it is given a complete certificate chain ending in a trusted CA.

It is critically important that servers whose certificates are signed by intermediate authorities supply ALL the certificates linking them to a trusted CA, including all of the intermediate certificates. If they don't supply this entire chain, the output from openssl will look something like this:

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
 Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
```

```
 Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

This output shows that the server only provided one certificate, and the provided certificate was signed by an intermediate authority, not a trusted root. The output also shows the characteristic verification errors.

Remediation

This problem is caused by a misconfigured certificate presented by the device. The only way to fix this so that Security Cloud Control or any other program can securely connect to the device is to load the correct certificate chain onto the device, so that it will present a complete certificate chain to connecting clients.

To include the intermediate CA to the trustpoint follow one of the links below (depending on your case - if CSR was generated on the ASA or not):

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

New Certificate Detected

If you upgrade a device that has a self-signed certificate and a new certificate is generated after the upgrade process, Security Cloud Control may generate a "New Certificate Detected" message as both a **Configuration Status** and **Connectivity** status. You must manually confirm and resolve this issue before you can continue managing it from Security Cloud Control. Once the certificate is synchronized and the device is in a healthy state, you can manage the device.

Note

When you bulk reconnect devices more than one managed device to Security Cloud Control at the same time, Security Cloud Control automatically reviews and accepts the new certificates on the devices and continues to reconnect with them.

Use the following procedure to resolve a new certificate:

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab.
3. Click the appropriate device type tab.
4. Use the filter to display devices with a **New Certificate Detected** connectivity or configuration status and select the desired device.
5. In the action pane, click **Review Certificate**. Security Cloud Control allows you to download the certificate for review and accept the new certificate.
6. In the Device Sync window, click **Accept** or in the Reconnecting to Device window, click **Continue**.

Security Cloud Control automatically synchronizes the device with the new self-signed certificate. You may have to manually refresh the page to see the device once it's synced.

Troubleshoot Onboarding Error

The device onboarding error can occur for various reasons.

You can take the following actions:

Procedure

1. In the left pane, click **Security Devices**.
2. Click the appropriate device type tab and select the device running into this error. In some cases, you will see the error description on the right. Take the necessary actions mentioned in the description.

   Or

3. Remove the device instance from Security Cloud Control and try onboarding the device again.

Resolve the conflict detected status

Security Cloud Control allows you to enable or disable conflict detection on each live device. If Conflict Detection on page 139 is enabled and there was a change made to the device's configuration without using Security Cloud Control, the device's configuration status will show **Conflict Detected**.

To resolve a **Conflict Detected** status, follow this procedure:

Procedure

1. Choose **Security Devices**.

   > **Note**
   >
   > For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

2. Click the **Devices** tab to locate your device.
3. Click the appropriate device type tab.
4. Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.
5. In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.
   - The panel labeled "Last Known Device Configuration" is the device configuration stored on Security Cloud Control.
   - The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.
6. Resolve the conflict by selecting one of the following:
   - **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on** Security Cloud Control with the device's running configuration.

     > **Note**
     >
     > As Security Cloud Control does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.

   - **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on Security Cloud Control.

   > **Note**
   >
   > All configuration changes, rejected or accepted, are recorded in the change log.

Resolve the Not Synced Status

Use the following procedure to resolve a device with a "Not Synced" Configuration Status:

Procedure

1. Choose **Security Devices**.

> **Note**
>
> For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

2. Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
3. Click the appropriate device type tab.
4. Select the device reported as Not Synced.
5. In the **Not synced** panel to the right, select either of the following:
   - **Preview and Deploy...** -If you want to push the configuration change from Security Cloud Control to the device, preview and deploy the changes you made now, or wait and deploy multiple changes at once.
   - **Discard Changes** -If you do **not** want to push the configuration change from Security Cloud Control to the device, or you want to "undo" the configuration changes you started making on Security Cloud Control. This option overwrites the configuration stored in Security Cloud Control with the running configuration stored on the device.

15 FAQ and support

Topics:

- Security Cloud Control
- FAQ about onboarding devices to Security Cloud Control
- Device types
- Security
- Troubleshooting
- How do I transfer a Firewall Threat Defense device to a new or existing Security Cloud Control organization?
- Terminologies and definitions used in Zero-Touch Provisioning
- Policy optimization
- Connectivity
- About Data Interfaces
- How Security Cloud Control processes personal information
- Contact Security Cloud Control support

This chapter contains the following sections:

Security Cloud Control

Learn how Security Cloud Control helps administrators create, monitor, and maintain consistent security policies across supported devices from a single cloud-based interface.

What is Security Cloud Control?

Security Cloud Control (formerly Cisco Defense Orchestrator) is a cloud-based multi-device manager that allows network administrators to create and maintain consistent security policies across various security devices.

You can use Security Cloud Control to manage these devices:

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Threat Defense
- Cisco Umbrella
- Meraki
- Cisco IOS devices
- Amazon Web Services (AWS) instances
- Devices administered using an SSH connection

Security Cloud Control administrators can monitor and maintain all these device types through a single interface.

FAQ about onboarding devices to Security Cloud Control

Learn about onboarding FAQs for supported device types in Security Cloud Control, including Secure Firewall ASA, Firewall Threat Defense, on-premises Firewall Management Center, Meraki, SSH, and IOS devices.

FAQs About Onboarding Secure Firewall ASA to Security Cloud Control

How do I onboard an ASA using credentials?

You can onboard ASAs one at a time or in a bulk operation. device at a time. When onboarding an ASA that is part of a high-availability pair, use Onboard an ASA Device to onboard only the primary device of the pair. The method of onboarding a security context or admin context is the same for onboarding any other ASA.

How do I onboard more than one ASA at a time?

You can create a list of ASAs using a CSV file, and Security Cloud Control will onboard all the ASAs in the list. See Onboard ASAs in Bulk for instructions on how to bulk onboard ASAs.

What do I do after onboarding my ASAs?

See Managing ASA with Security Cloud Control to get started.

FAQs About Onboarding Secure Firewall Threat Defense to Cloud-Delivered Firewall Management Center

How do I onboard Secure Firewall Threat Defense?

You can onboard an FTD device using a CLI registration key, through zero-touch provisioning, or with a serial number.

What do I do after onboarding my Secure Firewall Threat Defense?

Once the device is sychronized, navigate to **Administration** > **Integrations** > **Firewall Management Center** and select an action from the Actions, Management, or Settings pane to begin configuring your threat defense device in Cloud-Delivered Firewall Management Center. See Cloud-delivered Firewall Management Center Application Page to get started.

How do I troubleshoot my Secure Firewall Threat Defense?

See Troubleshoot Onboarding Secure Firewall Threat Defense.

FAQs About on-premises Firewall Management Center

This concept explains how you can onboard an on-premises Firewall Management Center to Security Cloud Control, but device management changes must still be made directly in the on-premises Firewall Management Center UI.

How do I onboard an on-premises Firewall Management Center?

You can onboard an on-premises Firewall Management Center to Security Cloud Control. Onboarding an on-premises Firewall Management Center also onboards all the devices registered to on-premises Firewall Management Center. Security Cloud Control does not support creating or modifying objects or policies associated with on-premises Firewall Management Center or the devices registered to on-premises Firewall Management Center. You must make these changes in the on-premises Firewall Management Center UI. For more information, see Onboard an On-Prem Management Center.

FAQs About Onboarding Meraki Devices to Security Cloud Control

How do I onboard a Meraki device?

MX devices can be managed by both Security Cloud Control and the Meraki dashboard. Security Cloud Control deploys configuration changes to the Meraki dashboard, which in turn deploys the configuration securely to the device. See Onboard Meraki MX Devices to get started.

FAQs About Onboarding SSH Devices to Security Cloud Control

How do I onboard an SSH device?

You can use the username and password of a highly privileged user stored on the SSH device to onboard the device with a Secure Device Connector (SDC). See Onboard an SSH Device to get started.

How do I delete a device?

You can delete a device from the **Security Devices** page.

FAQs About Onboarding IOS Devices to Security Cloud Control

How do I onboard a Cisco IOS device?

You can onboard a live Cisco device running Cisco IOS (Internetwork Operating System) with a Secure Device Connector (SDC). See Onboard a Cisco IOS Device to get started.

How do I delete a device?

You can delete a device from the **Security Devices** page.

Device types

Learn about frequently asked questions for device types in Security Cloud Control, including sync and conflict states, deployment behavior, scale limits, and support for ISR, ASR, and SMA devices.

What is an Adaptive Security Appliance (ASA)?

The Cisco ASA provides advanced stateful firewall and VPN concentrator functionality in one device as well as integrated services with add-on modules. The ASA includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), clustering (combining multiple firewalls into a single firewall), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, IPsec VPN, SSL VPN, and clientless SSL VPN support, and many more features. ASAs can be installed on virtual machines or supported hardware.

What is an ASA Model?

An ASA model is a copy of the running configuration file of an ASA device that you have onboarded to Security Cloud Control. You can use an ASA model to analyze the configuration of an ASA device without onboarding the device itself.

When is a device Synced?

When the configuration on Security Cloud Control and the configuration stored locally on the device are the same.

When is a device Not Synced?

When the configuration stored in Security Cloud Control was changed and it is now different that the configuration stored locally on the device.

When is a device in a Conflict Detected state?

When the configuration on the device was changed outside of Security Cloud Control (out-of-band), and is now different than the configuration stored on Security Cloud Control.

What is an out-of-band change?

When a change is made to the device outside of Security Cloud Control. The change is made directly on the device using CLI command or by using the on-device manager such as ASDM or FDM. An out-of-band change causes Security Cloud Control to report a "Conflict Detected" state for the device.

What does it mean to deploy a change to a device?

After you onboard a device to Security Cloud Control, Security Cloud Control maintains a copy of its configuration. When you make a change on Security Cloud Control, Security Cloud Control makes a change to its copy of the device's configuration. When you "deploy" that change back to a device, Security Cloud Control copies the changes you made to the device's copy of its configuration. See these topics:

- Preview and deploy configuration changes for all devices on page 131

What ASA commands are currently supported?

All commands. Click the **Command Line Interface** link under Device Actions to use the ASA CLI.

Are there any scale limitations for device management?

Security Cloud Control's cloud architecture allows it to scale to thousands of devices.

Does Security Cloud Control manage Cisco Integrated Services Routers and Aggregation Services Routers?

Security Cloud Control allows you to create a model device for ISRs and ASRs and import its configuration. You can then create templates based on the imported configurations and export the configuration as a standardized configuration that can be deployed to new or existing ISR and ASR devices for consistent security.

Can Security Cloud Control manage SMA?

No, Security Cloud Control does not currently manage SMA.

Security

Learn about security FAQs, including data protection, multi-factor authentication, OTP login errors, Secure Device Connector usage, private device connectivity, and VPN tunnel status checks.

I received the error "Could not validate your OTP" when logging into Security Cloud Control for the first time

Check that your desktop or mobile device clock is synchronized with a world time server. Clocks being out of sync by less or more than a minute can cause incorrect OTPs to be generated.

Is my device connected directly to Security Cloud Control cloud platform?

Yes. The secured connection is performed using the Security Cloud Control SDC which is used as a proxy between the device and Security Cloud Control platform. Security Cloud Control architecture, designed with security first in mind, enables having complete separation between data traversing back and forth to the device.

Does the SDC require any additional cost or license?

No.

How can I check the tunnel status? State options

Security Cloud Control performs the tunnel connectivity checks automatically every hour, however ad-hoc VPN tunnel connectivity checks can be performed by choosing a tunnel and requesting to check connectivity. Results may take several seconds to process.

Can I search a tunnel based on the device name as well as its IP address of one of its peers?

Yes. Search and pivot to a specific VPN tunnel details by using available filters and search capabilities on both name and the peers IP addresses.

Troubleshooting

Learn about troubleshooting FAQs for Security Cloud Control, including deployment warnings, out-of-band configuration differences, conflict resolution, and certificate rejection issues.

While performing complete deploy of device configuration from Security Cloud Control to managed device, I get a warning "Cannot deploy changes to device". What can I do to solve that?

If an error occurrs when you deploy a full configuration (changes performed beyond Security Cloud Control supported commands) to the device, click "Check for changes" to pull the latest available configuration from device. This may solve the problem and you will be able to continue making changes on Security Cloud Control and deploy them. In case the issue persist, please contact Cisco TAC from the **Contact Support** page.

While resolving out-of-band issue (changes performed outside of Security Cloud Control; directly to a device), comparing the configuration present in Security Cloud Control that of the device, Security Cloud Control presents additional metadata that were not added or modified by me. Why?

As Security Cloud Control expands its functionality, additional information will be collected from the device's configuration to enrich and maintain all required data for better policy and device management analysis. These are not changes that occurred on managed device but already existing information. Resolving the conflict detected state can be easily solved by checking for changes from the device and reviewing the changes occurred.

How do I transfer a Firewall Threat Defense device to a new or existing Security Cloud Control organization?

Learn about FAQs for transferring a Firewall Threat Defense device to a new or existing Security Cloud Control organization, including downloading pending changes, removing the device from the source organization, and onboarding it with a CLI registration key.

To transfer a Firewall Threat Defense device to a new or existing Security Cloud Control organization, follow these steps:

1. Ensure that all pending changes are downloaded to the Firewall Threat Defense device so that the latest changes are available on it.
2. Remove the Firewall Threat Defense device from the source Security Cloud Control organization.
3. (optional) Create a new Security Cloud Control organization in the desired region by using Security Cloud Control Provisioning Portal and enable Cloud-delivered Firewall Management Center on it. Skip this step if the target Security Cloud Control organization already exists.
4. Onboard the Firewall Threat Defense device to the new Security Cloud Control organization using the CLI registration key method.

Terminologies and definitions used in Zero-Touch Provisioning

Learn about FAQs for zero-touch provisioning terminology in Security Cloud Control, including claimed and parked devices, initial provisioning, and how FTD devices are onboarded through the Cisco Cloud.

- **Claimed** - Used in the context of serial number onboarding in Security Cloud Control. A device is "claimed" if its serial number has been onboarded to a Security Cloud Control tenant.
- **Parked** - Used in the context of serial number onboarding in Security Cloud Control. A device is "parked" if it has connected to the Cisco Cloud, and a Security Cloud Control tenant has not claimed its serial number.
- **Initial provisioning** - Used in the context of the initial FTD setup. During this phase, the device accepts EULA, creates a new password, configures management IP address, sets FQDN, sets DNS servers, and chooses to manage the device locally with FDM.
- **Zero-Touch Provisioning** - It is the process of shipping an FTD from the factory to a customer site (typically a branch office), an employee at the site connects the FTD to their network, and the device contacts the Cisco Cloud. At that point, the device is onboarded to Security Cloud Control tenant if its serial number has already been "claimed," or the FTD is "parked" in the Cisco cloud until a Security Cloud Control tenant claims it.

Policy optimization

Learn about FAQs for policy optimization in Security Cloud Control, including how to identify fully shadowed access rules within the same access group using Network Policy Management.

How can I identify a case when two or more access lists (within the same access group) are shadowing each other?

Security Cloud Control Network Policy Management (NPM) is able to identify and alert the user if within a rule set, a rule higher in order, is shadowing a different rule. User can either navigate between all network policies or filter to identify all shadow issues.

> **Note**
>
> Security Cloud Control supports only fully shadowed rules.

Connectivity

Learn about Security Cloud Control connectivity FAQs, including how to handle SDC IP address changes, update device IP addresses, reconnect managed devices, and meet ASA networking requirements.

The Secure Device Connector changed IP address, but this was not reflected within Security Cloud Control. What can I do to reflect the change?

In order to obtain and update the new Secure Device Connector (SDC) within Security Cloud Control, you will need to restart the container using the following commands:

```
 Stop Docker deamon>#service docker stop
Change IP address
Start Docker deamon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$
./cdo/toolkit/toolkit.sh restartSDC <tenant-name>
```

What happens if the IP address used by Security Cloud Control to manage my devices (FTD or ASA) changes?

If the IP address of the device changes for any reason, whether it is a change in the static IP address or a change in the IP address due to DHCP, you can change the IP address that Security Cloud Control uses to connect to the device (see Changing a device's IP address in Security Cloud Control Firewall Management on page 84) and then reconnect the device (see Bulk reconnect devices to Security Cloud Control Firewall Management on page 88). When reconnecting the device you will be asked to enter the new IP address of the device as well as re-enter the authentication credentials.

What networking is required to connect my ASA to Security Cloud Control?

- ASDM image present and enabled for ASA.
- Public interface access to 52.25.109.29, 52.34.234.2, 52.36.70.147
- ASA's HTTPS port must be set to 443 or to a value of 1024 or higher. For example, it cannot be set to port 636.
- If the ASA under management is also configured to accept AnyConnect VPN Client connections, the ASA HTTPS port must be changed to a value of 1024 or higher.

About Data Interfaces

Learn about data interface, including using management or data interfaces for FTD communication, remote management from outside interfaces, high availability support, and key data interface limitations.

You can use either the dedicated management interface or a regular data interface for communication with the device. Security Cloud Control access on a data interface is useful if you want to manage the FTD remotely from the outside

interface, or you do not have a separate management network. Security Cloud Control supports high availability on the FTD managed remotely from the data interface.

FTD management access from a data interface has the following limitations:

- You can only enable manager access on one physical, data interface. You cannot use a subinterface or EtherChannel.
- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the FTD and the WAN modem.
- The interface must be in the global VRF only.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using Security Cloud Control. Because the management interface gateway will be changed to be the data interfaces, you also cannot SSH to the management interface from a remote network unless you add a static route for the management interface using the **configure network static-routes** command.

How Security Cloud Control processes personal information

Learn about FAQs for how Security Cloud Control processes personal information, including where to find Cisco's Privacy Data Sheet for details on handling personally identifiable information.

To learn how Security Cloud Control processes your personal identifiable information, see the Security Cloud Control Privacy Data Sheet.

Contact Security Cloud Control support

Learn how to contact Security Cloud Control support, export workflow details, open a Cisco TAC support ticket, and check the Security Cloud Control service status page.

This chapter covers the following sections:

Export The Workflow

We strongly recommend exporting the workflow of a device that is experience issues prior to opening a support ticket. This additional information can help the support team expeditiously identify and correct any troubleshooting efforts.

Use the following procedure to export the workflow:

Procedure

1. In the left pane, click **Security Devices**.
2. Click the **Devices** tab to locate your device.
3. Click the appropriate device type tab and select the device you need to troubleshoot.

   Use the **filter** or **search bar** to locate the device you need to troubleshoot. Select the device so it is highlighted.
4. In the **Device Actions** pane, select **Workflows**.
5. Click the **Export** button located at the top right of the page, above the table of events. The file automatically saves locally as a **.json** file. Attach this to any emails or tickets you open with TAC.

Open a Support Ticket with TAC

A customer using a 30-day trial or a licensed Security Cloud Control account can open a support ticket with Cisco's Technical Assistance Center (TAC).

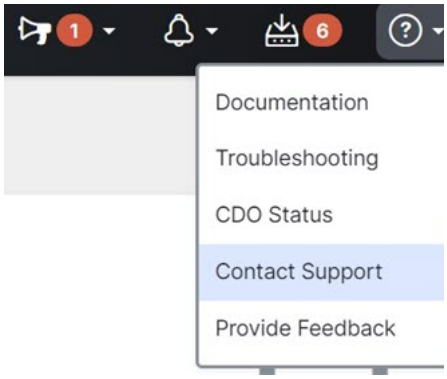
- How Security Cloud Control Customers Open a Support Ticket with TAC.
- How Security Cloud Control Trial Customers Open a Support Ticket with TAC.

How Security Cloud Control Customers Open a Support Ticket with TAC

This section explains how a customer using a licensed Security Cloud Control tenant can open a support ticket with Cisco's Technical Assistance Center (TAC).

Procedure

1. Log in to Security Cloud Control.
2. Next to your tenant name, click the help button and select **Contact Support**.



3. Click **Support Case Manager**.
4. Click the blue **Open New Case** button.
5. Click **Open Case**.
6. Select **Products and Services** and then click **Open Case**.
7. Choose a **Request Type**.
8. Expand **Find Product by Service Agreement** row.
9. Fill in all the fields. Many of the fields are obvious. This is some additional information:
   - **Product Name (PID)** - If you no longer have this number, see the Security Cloud Control Data Sheet.
   - **Product Description** - This is the description of the PID.
   - **Site Name** - Enter your site name. If you are a Cisco Partner opening a case for one of your customers, enter the customer's name.
   - **Service Contract** - Enter your service contract number.
     - **Important**: In order for your case to be associated with your Cisco.com account, you need to associate your contract number to your Cisco.com profile. Use this procedure to associate your contract number to your Cisco.com profile.
       a. Open to Cisco Profile Manager.
       b. Click the **Access Management** tab.
       c. Click **Add Access**.

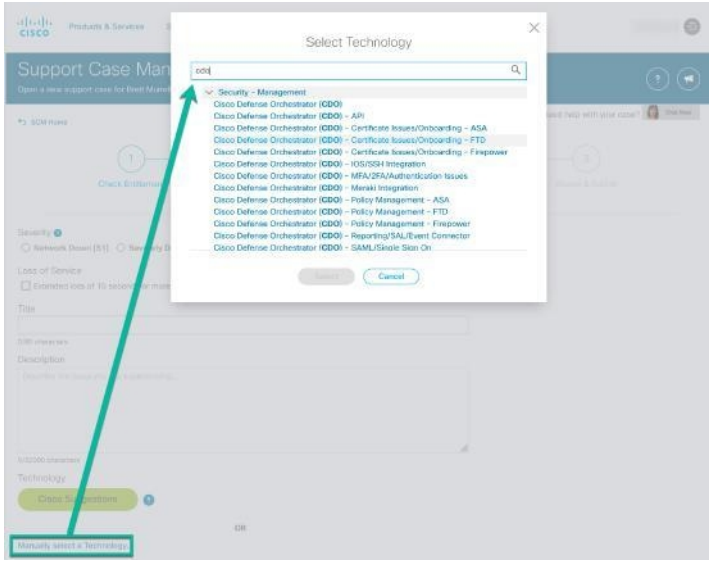
d. Choose **TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com** and click **Go**.

e. Enter service contracts number(s) in the space provided and click **Submit**. You will receive notification via email that the service contract associations have been completed. Service contract association can take up to 6 hours to complete.

Important

Important: If you are not able to access any of the links below, please contact your authorized Cisco partner or re-seller, your Cisco account representative, or the individual in your company who manages Cisco service agreement information.

10. Click **Next.**
11. In the **Describe Problem** screen, scroll down to **Manually select a Technology**, click it, and type **Security Cloud Control** in the search field.
12. Select the category that best matches your request, and click **Select**.



13. Complete the remainder of the service request and click **Submit**.

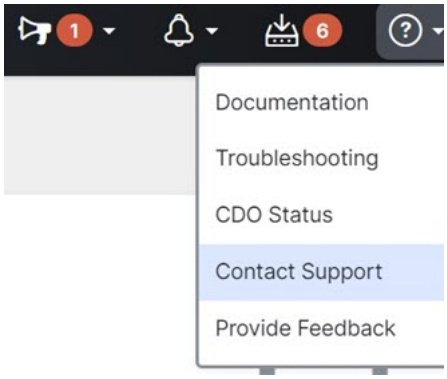
How Security Cloud Control Trial Customers Open a Support Ticket with TAC

This section explains how a customer using a free trial of a Security Cloud Control tenant can open a support ticket with Cisco's Technical Assistance Center (TAC).

Procedure

---

1. Log in to Security Cloud Control.
2. Next to your tenant and account name, click the help button and select **Contact Support**.



3. In the **Enter Issue or request below** field, specify the issue that you are facing or your request and click **Submit**.

   Your request, along with the technical information, will be sent to the support team, and a technical support engineer will respond to your query.

Security Cloud Control Service Status Page

Security Cloud Control maintains a customer-facing service status page that shows you if the Security Cloud Control service is up and any service interruptions it may have had. You can view up-time information with daily, weekly, or monthly graphs.

You can reach the Security Cloud Control status page by clicking **Security Cloud Control Status** in the help menu on any page in Security Cloud Control.

On the status page, you can click the **Subscribe to Updates** to receive a notification if the Security Cloud Control service goes down.