Introduction

- An Introduction to Security Cloud Control, on page 1
- Managing On-Premises Firewall Management Center with Security Cloud Control, on page 2
- The Security Cloud Control Dashboard, on page 5

An Introduction to Security Cloud Control

Security Cloud Control (formerly Cisco Defense Orchestrator) is a cloud-based multi-device manager that facilitates management of security policies in highly distributed environments to achieve consistent policy implementation.

Security Cloud Control helps you optimize your security policies by identifying inconsistencies with them and by giving you tools to fix them. Security Cloud Control gives you ways to share objects and policies, as well as make configuration templates, to promote policy consistency across devices.

Because Security Cloud Control coexists with local device managers such as the Adaptive Security Device Manager (ASDM), it keeps track of configuration changes made by Security Cloud Control and by other managers, and then reconcile the differences between managers.

Security Cloud Control has an intuitive user interface that allows you to 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 also provides a guided "Day 0" experience helping you quickly onboard threat defense devices to your on-premises or cloud-delivered Firewall Management Center. It also presents you with other key features you may benefit from and helps you enable and configure them.

Onboard Devices

Before you onboard a device, make sure that you have successfully completed the installation wizard and licensed the device. Then use Security Cloud Control's onboarding wizard to onboard your device. Security Cloud Control can easily manage large deployments.

See Onboard Devices and Services.

Note Once you have onboarded devices to a Security Cloud Control tenant, you cannot migrate the devices from one Security Cloud Control tenant to another. If you want to move your devices to a new tenant, you need to re-onboard the devices to the new tenant.

For a complete list of devices that Security Cloud Control supports and manages, see Supported Devices, Software, and Hardware.

Cisco Online Privacy Statement

Cisco Systems, Inc. and its subsidiaries (collectively "Cisco") are committed to protecting your privacy and providing you with a positive experience on our websites and while using our products and services ("Solutions"). Please read Cisco Online Privacy Statement carefully to get a clear understanding of how we collect, use, share, and protect your personal information.

Managing On-Premises Firewall Management Center with Security Cloud Control

About On-Premises Firewall Management Center

On-Premises Management Center support is limited to onboarding, viewing its managed devices, viewing, managing network objects and cross-launching to On-Premises Management Center UI to manage associated devices and objects. Additional features will be supported soon. For functionality that may not be supported by Security Cloud Control at this time, you must use the On-Premises Management Center console. See the Cisco Secure Firewall Management Center Configuration Guide of the version your system is running, to know more about the features provided by On-Premises Management Center.

The On-Premises Management Center is a centralized management console with graphical user interface that you can use to perform administrative, management, analysis, and reporting tasks. It is a management console that is comparable, but not identical, to ASDM and FDM.

For a list of On-Premises 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. An On-Premises Management Center can manage older devices, usually a few major versions back. For example, devices running version 6.6.0 can manage a Version 6.4.0 device. If an On-Premises 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 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 the On-Premises Management Center, and the On-Premises Management Center then uses its designated client to channel the requests to its managed devices. Because the device does not allow multiple logins with the same login credentials, we recommend creating a new user on the On-Premises Management Center specifically for Security Cloud Control communication that has 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** permission. Without an admin login, Security Cloud Control will not be able to successfully use REST API commands to modify or create policy, rules, or objects.

Onboard or Remove an On-Premises Management Center

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

Once an On-Premises Management Center is onboarded, select the On-Premises 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 lets you enter the public IP address or the FQDN and the port number of your management center. Clicking **Continue** cross-launches to the selected On-Premises Management Center web UI in a new tab using the IP address you entered. You can also add external links manually in the **Add External Links** option under **External Links** on the right pane.

Removing an On-Premises Management Center from your Security Cloud Control tenant also removes the devices registered to that On-Premises Management Center. See Remove an FMC from Security Cloud Control for more information. If an On-Premises Management Center experiences an "Invalid Credentials" status after onboarding, you can **reconnect** the appliance. See Troubleshoot Invalid Credentials for more information.

Note Devices running Firepower 6.6 do not support the **reconnect** feature. If you have to reconnect the appliance, we recommend removing the On-Premises Management Center and re-onboarding the appliance.

On-Premises Management Center High Availability Pairs

Security Cloud Control does not support high availability (HA) functionality for On-Premises Management Center appliances. If a pair of On-Premises Management Center appliances are configured for HA, the pair is listed as individual appliances in the **Services** page.

Devices Managed by an On-Premises Management Center

Once you onboard an On-Premises Management Center to Security Cloud Control, all of the devices registered to that On-Premises Management Center are also read into Security Cloud Control. From the **Security Devices** page, you can see device information such as name, IP address, type of device, software version, and the state. Note that your On-Premises 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, type of device, and status. Clicking the devices icon on the **Services** page, which displays the number of devices your FMC manages, takes you to the **Security Devices** page, with the device filter applied, so all the devices managed by the On-Premises Management Center you selected are displayed.

You can perform actions using relevant options in the **Device Actions**, **Monitoring**, **Device Management**, and **Policies** panels on the right pane in the **Security Devices**. If you select a device that is currently managed by an FMC and click these options, Security Cloud Control automatically launches the On-Premises 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 here you can opt to view all the devices managed by the onboarded On-Premises Management Center, as well as the other supported device types. In addition, you can expand or collapse devices in a cluster and select them indivdually or as a group to perform actions.

Device Health Status

Security Cloud Control displays the health status of threat defense devices in 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 Management Center user interface.

Note Security Cloud Control keeps automatically updating the device health status every 10 minutes; however, you can do this manually by selecting the device and clicking **Check for Changes**.

Manage Security Policies in Security Cloud Control

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. You can use Security Cloud Control to configure security policies on many different types of devices.

Objects

After you onboard an On-Premises Management Center to Security Cloud Control, you can choose to discover objects from the On-Premises Management Center and manage them in Security Cloud Control. You can do this by navigating to **Administration** > **Integrations** > **Firewall Management Center**, selecting the desired On-Premises Management Center, and clicking **Settings**. You can turn the **Discover & Manage Network Objects** toggle button on; when this option is enabled, Security Cloud Control automatically reads all the objects from the On-Premises Management Center-managed devices into Security Cloud Control. Once imported, the objects can be managed from Security Cloud Control. Note that you need to have the super admin or admin user role to be able to use the **Settings** button.

When making a configuration change to an object from Security Cloud Control, the change gets staged in Security Cloud Control and you can manually push the change to the On-Premises Management Center after reviewing it from **Pending Changes**. In addition, when you make a configuration change to an object from the On-Premises Management Center user interface, Security Cloud Control detects those changes as out-of-band changes that can be synchronized later. If you want your changes to be automatically synchronized with on-premises management center and not staged for review, turn the **Enable automatic sync of network objects** toggle on.

If you have existing objects in Security Cloud Control that you want to assign to your On-Premises Management Center, select the On-Premises Management Center from the **Services** page and choose **Assign Objects** on the right pane. Security Cloud Control displays all the existing objects and lets you select ones that you want to associate with the On-Premises Management Center that you selected. This heps promote consistency in network object definitions across platforms managed by Security Cloud Control. Note that you can use the **Assign Objects** button only if **Discover & Manage Network Objects** is enabled for the selected on-premises management center.

Note

- You cannot turn the **Discover & Manage Network Objects** toggle on if the on-premises management center that you have selected has one or more child domains or has the Chanage Management workflow enabled on it..
- You cannot turn the **Enable automatic sync of network objects** toggle on if the **Discover & Manage Network Objects** toggle is turned off.

On-Premises Management Center supports the following object types:

- Network Objects
- Network-Group Objects

Object Issues

Security Cloud Control identifies the duplicate, inconsistent, or ununsed objects. 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 when searching and filtering 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 of your devices and view them in one place in Security Cloud Control.

The events are stored in the Cisco cloud and viewable from the Event Logging page in Security Cloud Control where you can filter and review them to gain a clear understanding of what security rules are triggering 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.

The Security Cloud Control Dashboard

The Security Cloud Control 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 the widgets you want to view on the dashboard.
3. You can drag and drop the widgets to arrange them as you prefer.

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.