



## Introduction

---

- [Managing IOS Devices with Security Cloud Control, on page 1](#)
- [An Introduction to Security Cloud Control, on page 2](#)
- [The Security Cloud Control Dashboard, on page 2](#)

## Managing IOS Devices with Security Cloud Control

Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator) allows you to manage Cisco IOS devices. These are the features we support for those devices:

- [Onboard Integrations](#). You can use the username and password of a highly privileged user stored on the IOS device to onboard the device.
- [View a Device's Configuration File](#). You can view the device configuration file.
- [Read Changes from Firewalls](#). When you check for changes in the configuration file from the Cisco IOS device, it will be saved in Security Cloud Control's database.
- [Out-of-Band Changes on Devices](#). When you enable Conflict Detection, Security Cloud Control checks the device every 10 minutes for changes to the device's configuration. If there is a change, the device's status will change to Conflict Detected and you will be able to [resolve the conflict](#).
- [Security Cloud Control Command Line Interface](#). You can issue all IOS commands to the device through Security Cloud Control's command line interface.
- Individual CLI commands and groups of commands can be turned into editable and reusable "[macros](#)." You can use the system-defined macros provided by Security Cloud Control and create your own macros for tasks you perform often.
- [Detect and manage SSH fingerprint changes](#). If any credentials or properties of the device change, and that causes a change to the SSH fingerprint, Security Cloud Control detects that change and gives you a chance to review and accept the new fingerprint.
- [Manage Change Logs in Security Cloud Control](#). The change log captures all the commands you issue to the IOS device.

# 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.

# 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**, and **Online**.

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.

