Introduction

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

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.

Managing SSH Devices with Security Cloud Control

Generic SSH devices include any other SSH-capable devices not running Cisco IOS, managed using a generic SSH interface. Devices such as Linux servers, Unix-based systems, or third-party network appliances accessible using SSH. Generic SSH refers to the use of the Secure Shell (SSH) protocol as a standard method to securely access and manage network devices remotely. These devices are accessible using SSH that can be onboarded and managed through Security Cloud Control by specifying the device's IP or FQDN, SSH port, and login credentials.

These are the features we support for those devices:

- Onboard a SSH Device. You can use the username and password of a highly privileged user stored on the SSH device to onboard the device.
- View a Device's Configuration File. You can view the device configuration file.
- Review policy and configuration changes from device. When you read the configuration file from the SSH device, it will be saved in Security Cloud Control's database.
- Out-of-band change detection. 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.
- Use the Security Cloud Control Command Line Interface Tool. You can issue all SSH device 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.
- Change Log. The change log captures all the commands you issue to the SSH device.

Security Cloud Control Firewall Management dashboard

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.