Introduction

Managing Meraki with Security Cloud Control Firewall Management

Meraki MX is an enterprise security and software-defined wide-area-network (SD-WAN) next-generation firewall appliance designed for distributed deployments. It is managed remotely by the Meraki dashboard and now you can manage layer 3 network rules on Meraki MX devices using Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator). See Meraki Next-Gen Firewall Technologies and Meraki product documentation for more information. After you onboard a Meraki device to Security Cloud Control, Security Cloud Control communicates with the Meraki dashboard to manage that device. Security Cloud Control does not communicate with the MX directly. Security Cloud Control securely transfers configuration requests to the Meraki dashboard which then applies the new configuration to the device. See How Does Security Cloud Control Communicate With Meraki, on page 2 for more information.

Security Cloud Control helps you optimize your Meraki environment by identifying problems with objects and policies and generating possible fixes or alternative options. This applies to policies that are associated to both devices and templates. Use Security Cloud Control to:

- Simultaneously manage policies on one or more Meraki devices
- Monitor and manage Meraki policies or templates alongside your FTD and ASA devices in an all-encompassing environment.
- Use a Meraki template to manage multiple networks.
- Customize access rules with objects that are compatible across other supported platforms, such as FTD and ASA devices.

Onboard Meraki MX Devices

Prior to onboarding a device to Security Cloud Control, you **must** create an account with the Meraki dashboard and onboard your device or template to the dashboard. If your organization does not have an account in the Meraki dashboard, you will be unable to generate an API token and your device will not communicate to Security Cloud Control.

You can onboard either a Meraki MX device or a Meraki template to Security Cloud Control.

Handle Meraki MX login credentials and permissions through the Security Cloud Control console. Without the correct credentials or permissions, Security Cloud Control cannot communicate with the Meraki device. See Updating Meraki MX Credentials and Generate and Retrieve Meraki API Key for more information.

Meraki Layer 3 Rules and Security Cloud Control

At this time, Security Cloud Control supports layer 3 firewall rules only. Layer 3 rules enforce policy at the network layer of the OSI model. See Using Layer 3 Firewall Rules for more information.

The Meraki environment allows you to create Layer 3 outbound rules in the Meraki dashboard. Security Cloud Control reads in the layer 3 rules you have defined in the Meraki dashboard when you onboard a device into Security Cloud Control. You can then manage these rules just as you would manage FTD or ASA rules in Security Cloud Control. See Manage Meraki Access Control Policy for more information.

Objects

Fine-tune your new access control policy with objects. The Meraki dashboard uses protocols and groups of IP addresses or IP address ranges; in contrast, Security Cloud Control uses a variety of objects to manage rules. To understand how Security Cloud Control transfers Meraki protocols into objects, see Objects Associated with Meraki Devices for more information. The following objects can be created in Security Cloud Control and translated into IP groups in the Meraki dashboard:

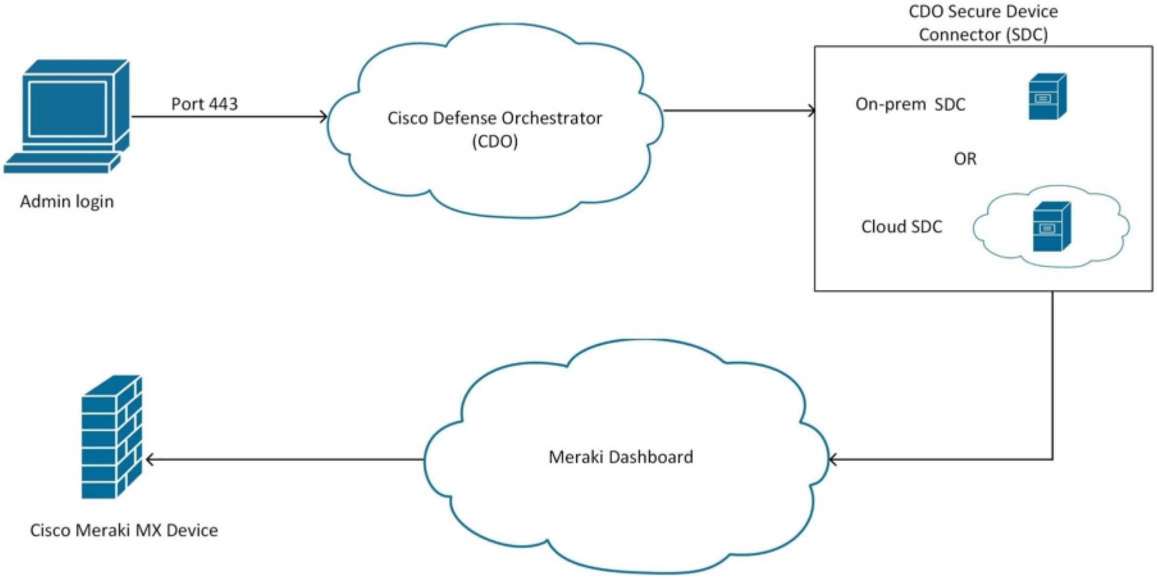
- Network objects or object groups
- Network service (port) objects

The Meraki environment allows you to create Layer 3 outbound rules in the Meraki dashboard. Security Cloud Control reads in the layer 3 rules you have defined in the Meraki dashboard when you onboard a device into Security Cloud Control. You can then manage these rules just as you would manage FTD or ASA rules in Security Cloud Control. See Manage Meraki Access Control Policy for more information.

How Does Security Cloud Control Communicate With Meraki

Deploy From Security Cloud Control to your Meraki Device

Security Cloud Control does not deploy configuration changes directly to a Meraki MX device; deployment is a multi-step process. See the diagram below:



Configuration changes that you make in Security Cloud Control for a Meraki MX device are staged in Security Cloud Control until you decide to deploy them. When you deploy the configuration changes, Security Cloud Control forwards them to the Meraki Dashboard, which implements them on the Meraki MX device. Security Cloud Control manages firewall policies while Meraki dashboard manages the network the policies are applied to. Both operations affect how traffic flows through the Meraki MX device and how it is processed.

Some customers with older tenants may connect the Meraki MX device to Security Cloud Control through an SDC. If you are one of those customers, you can continue to use this method or you can remove the SDC by re-onboarding your Meraki MX or updating the connection credentials. You do not need an SDC to connect Security Cloud Control to Meraki MX.

One difference between Security Cloud Control and the Meraki dashboard is the use of objects. For rules that are created on the Meraki dashboard, Security Cloud Control takes Meraki IP address groups or IP address ranges and turns them into objects that can be attached or associated to rules and the device policy. When you deploy objects that are created in Security Cloud Control to Meraki appliances, the Meraki dashboard translates those objects back into IP address groups or ranges. Objects in Security Cloud Control are unique and versatile since they are compatible with other device platforms; if you have other devices onboarded in Security Cloud Control, you may be able to create a single object for all your devices. See Objects Associated with Meraki Devices for more information.

Related Information:

- Onboard Meraki MX to Security Cloud Control
- Meraki Access Control Policy

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**, **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.