



Managing Meraki with Cisco Defense Orchestrator

- [Managing Meraki with Cisco Defense Orchestrator](#), on page i

Managing Meraki with Cisco Defense Orchestrator

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 Cisco Defense Orchestrator (CDO). See [Meraki Next-Gen Firewall Technologies](#) and [Meraki product](#) documentation for more information. After you onboard a Meraki device to CDO, CDO communicates with the Meraki dashboard to manage that device. CDO does not communicate with the MX directly. CDO securely transfers configuration requests to the Meraki dashboard which then applies the new configuration to the device. See [How Does CDO Communicate With Meraki](#) for more information.

CDO 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 CDO 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 CDO, 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 CDO.

You can onboard either a [Meraki MX device](#) or a [Meraki template](#) to CDO.

Handle Meraki MX login credentials and permissions through the CDO console. Without the correct credentials or permissions, CDO 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 CDO

At this time, CDO 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. CDO reads in the layer 3 rules you have defined in the Meraki dashboard when you onboard a device into CDO. You can then manage these rules just as you would manage FTD or ASA rules in CDO. 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, CDO uses a variety of objects to manage rules. To understand how CDO transfers Meraki protocols into objects, see [Objects Associated with Meraki Devices](#) for more information. The following objects can be created in CDO 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. CDO reads in the layer 3 rules you have defined in the Meraki dashboard when you onboard a device into CDO. You can then manage these rules just as you would manage FTD or ASA rules in CDO. See [Manage Meraki Access Control Policy](#) for more information.