ı|ıı|ıı Meraki
CISCO

MX450 Installation Guide

This document describes how to install and set up the MX450 security appliance. Additional reference documents are available online at: www.meraki.com/library/products.

MX450 Overview

The Meraki MX450 is an enterprise security appliance designed for distributed networks that require remote administration. It is ideal for network administrators who demand both ease of deployment and a state-of-the-art feature set. The MX450 appliance provides the following new features:

- Two dedicated uplink SFP+10GbE ports
- Support for eight configurable GbE(RJ45), eight GbE SFP and eight 10GbE SFP+ connections
- USB port, to support approved 3G/4G cards for failover to cellular networks
- 128GB (SSD) cache storage
- Dedicated management port
- Front-panel rack mounts

Package Contents

In addition to the MX450, the following are provided:

2 CAT6 Ethernet Cables

Rack Mounting Kit

MX450 Front Panel

## Ports and Status Indicators

The MX450 uses LEDs to inform the user of the device's status. When the device powers on, all the Internet LEDs flash twice. Additional functions are described below, from left to right.

Item	Function	LED Status	Meaning
1	Power	Solid orange	Power is applied
		Rainbow colors	Unit is attempting to contact the Cloud
		Flashing white	Operation is in progress
		Solid white	Fully operational
2	USB connectivity	Off	During boot or USB link
		Solid orange	Initial link
		Flashing orange	Internet connectivity not complete
		Green	USB connection detected
3	HA status	Off	No HA available
		Orange	Initial link
		Flashing orange	High availability not complete
		Green	HA available
Reset button	Insert a paper clip if a reset is required. A brief, momentary press: To delete a downloaded configuration and reboot. Press and hold for more than 10 seconds: To force the unit into a full factory reset.		

MX450 Back Panel
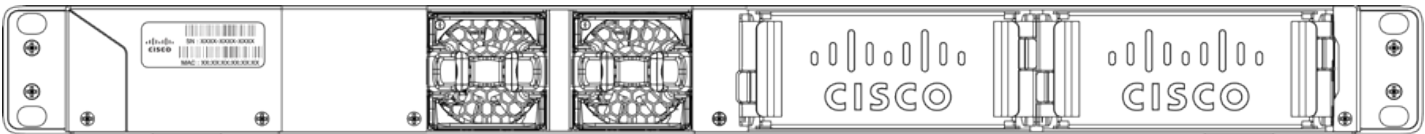
Please note that the serial number is located on the product label at the back panel of the MX450-HW.

Mounting Hardware

The mounting hardware includes four sets of standard slot-head rack screws and nuts. The additional screws and nuts are different screw standards meant to accommodate the most common rack mounts. When installing the appliance, make sure that there is sufficient space between the rear of the rack and other obstacles to ensure adequate airflow. Ventilation is from side to side not from front to back. This MX security appliance requires a minimum of 10mm clearance between the venting holes and any obstruction.

Safety Guidelines

Warning: The system must be disconnected from all sources of power and the power cord removed from the power supply module(s) before accessing, installing, or removing system components.

Caution: The Optical Transceiver product should use UL listed, and Rated Laser Class I, 3.3Vdc.

Connecting to WAN

All Meraki MX devices must have an IP address. This section describes how to configure your local area network before you deploy it. A local management web service, running on the appliance, is accessed through a browser running on a client PC. This web service is used for configuring and monitoring basic ISP/WAN connectivity.

Setting up a Static IP Address

> ⊘ To ensure that the client PC is redirected to the local web service in the following step, you must disable all other network services (ex: wi-fi) on your client machine.

Do the following to configure basic connectivity and other networking parameters:

1. Using a client machine such as a laptop, connect to the **management** port of the MX.
2. Using a browser on the client machine, access the appliance's built-in web service by browsing to http://setup.meraki.com. (You do not have to be connected to the Internet to reach this address)
3. Click **Uplink configuration** under the **Local status** tab. The default credentials use the device serial number as the username, with a blank password field.
4. Choose **Static** for the **IP Assignment option**.
5. Enter the IP address, subnet mask, default gateway IP and DNS server information.

Setting up a DHCP IP Address

By default all MX devices are configured to DHCP from upstream WAN / ISP servers. Simply plug the MX's WAN / Internet port to your upstream circuit and wait a few minutes for the unit to negotiate a DHCP address.

> ⓘ When the WAN connection is fully enabled, Internet LED will turn green.

Additional Settings

> ⓘ Please note that all these settings below are accessible only via the local management console.

Setting VLANs

If your WAN uplink is on a trunk port, choose **VLAN tagging > Use VLAN tagging** and enter the appropriate value for **VLAN ID** for your network.

Setting PPPoE

PPPoE authentication may be required if you are connecting MX device to a DSL circuit. You need to know your authentication option and credentials (supplied by your ISP) in order to complete these steps.

- Choose **Connection Type > PPPoE.**
- Select your **Authentication** option.
- If you select **Use authentication**, enter appropriate values for **Username** and **Password**.

Web Proxy Settings

These settings take effect if the MX device has to fall back to using HTTP to contact the Cloud Controller. By default, web proxy is disabled. To enable web proxy, do the following:

- Choose **Web proxy > Yes**.
- Enter values as appropriate for **Hostname or IP** and **Port**.
- If you require authentication, choose **Authentication > Use authentication**, and enter appropriate values for **Username** and **Password**.

> ⓘ To apply all configuration settings to the appliance, be sure to click **Save Settings** at the bottom of the page.

Configuring Physical link settings

To configure physical link settings on the Ethernet ports, click **Local status > Ethernet configuration**. You can enable half duplex, full duplex, and autonegotiation, as well as set 10 or 100-Mbps data rates.

Warranty

MX Warranty coverage periods are as follows:

Product	Warranty Period	Warranty Information
MX450	Lifetime	Full lifetime hardware warranty with next-day advanced replacement included.
MX450 Accessories	1 Year	The following are considered accessories: SFP Modules, all mounting kits and stands, interface modules, additional power cords

Additional warranty information can be found on the Return Policy and Requesting an RMA page of the Cisco Meraki website.

If your Cisco Meraki device fails and the problem cannot be resolved by troubleshooting, contact support to address the issue. Once support determines that the device is in a failed state, they can process an RMA and send out a replacement device free of charge. In most circumstances, the RMA will include a pre-paid shipping label so the faulty equipment can be returned.

ⓘ In order to initiate a hardware replacement for non-functioning hardware that is under warranty, you must have access to the original packaging the hardware was shipped in. The original hardware packaging includes device serial number and order information, and may be required for return shipping.