



Configuration for Meraki MX Series 6300-CX

Configuration for Meraki MX Series



Meraki



Overview

The Accelerated 6300-CX LTE Router provides a reliable, high-speed cellular connection that is compatible with existing wireline infrastructure. While its 4G LTE speeds are capable of operating as a primary WAN uplink, the 6300-CX can also be configured as a backup. This network redundancy solution delivers the ultimate flexibility to minimize expenses when it comes time for upgrading equipment to the latest wireless standards.

Business continuity depends on the seamless integration of failover-connectivity solutions to prevent service interruptions. Now more than ever, contingency networks play a strategic role in sustaining business operations. Unplanned outages can cost companies significant time and money, frustrating employees and clients alike, which creates a negative perception that is difficult to overcome.

Cellular data (4G LTE) bypasses wireline Internet service providers (ISPs) to facilitate the best redundancy possible. Additionally, in some situations it may be a challenge to acquire access to wired circuits or an event may call for temporary online access. Accelerated Concepts extensively tests the 6300-CX LTE router to ensure its interoperability with a wide variety of security appliances, including equipment produced by Meraki, to best accommodate enterprise networks. Pairing the Accelerated 6300-CX with one of Meraki's MX-series devices offers comprehensive security and flexibility for small business, retail, government, remote sites, and branch offices.

Meraki's MX of Security Appliances are configured using a cloud-based dashboard designed to offer a dynamic management platform reachable via any web browser. From the dashboard, administrators have access to zero-touch provisioning, remote troubleshooting, and real-time reporting on all Meraki equipment within their network. Devices must maintain an active Internet connection to take advantage of cloud functionality, of course, which is why the MX line supports dual WAN interfaces with automated failover and load balancing. The Accelerated 6300-CX's embedded, carrier-certified cellular modem integrates effortlessly with all MX appliances as either the primary or backup uplink.

For additional information, please refer to Meraki's [MX-series user guides](#).

Interoperability Matrix

This section covers interoperability information of the hardware tested for this solution. It includes the firmware versions of both devices as well as the date of testing.

Date	Meraki Firmware	6300-CX Firmware
12/2016	N/A*	16.10.13

*At this time, Meraki does not publish firmware version numbers or specific change logs.

Caveats

The delivery of wireless services varies depending on the carrier and may lead to differences in the area of coverage, type of service (3G, 4G, LTE, etc.), available bandwidth, and IP address designation (Private or Public) among other factors. The interoperability test designed for this solution guide included LTE service, maximum coverage availability, and a public IP address assigned to each device.

Using the 6300-CX as a secondary connection assumes that a primary WAN Ethernet cable is plugged into the Internet-1 port on the Meraki device. Connect the 6300-CX's backup Ethernet cable to port labeled Internet 2 and proceed to the configuration described herein. (Compatible with all MX Security Appliances.)



Accelerated 6300-CX LTE Router Setup

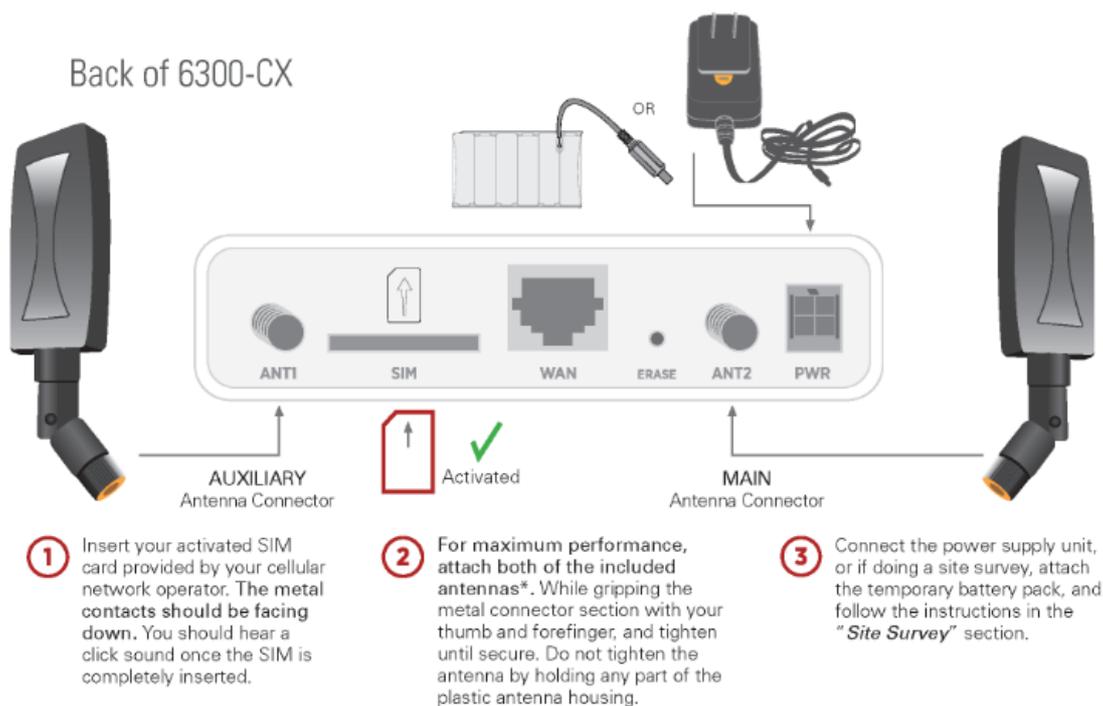
Initial Setup

Affix both antennas to the router and insert an activated SIM card before deploying the device. Be sure to select a location with optimal signal strength. For detailed instruction, refer to the tables that follow. Subsequent sections will outline site selection, powering options, and other device functionality.

Step-by-Step Guidance: Initial Setup

1. Insert the activated 2FF SIM card provided by your cellular network operator (putting the cut corner in first with metal contacts facing down). The card clicks into place when completely inserted.

2. Attach the two included antennas; both should be installed for optimal operation. Do this by gripping the metal connector section with your thumb and forefinger, tightening until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.
3. To determine the optimal location for the 6300-CX, please see the “Site Survey” section.
4. Refer to the section(s) for Remote or Direct Power Installations when ready to connect the 6300-CX to the permanent power supply unit.
5. The 6300-CX uses DHCP with IP passthrough by default, which satisfies the setup requirements for most environments. If required, please use Accelerated View™ or the 6300-CX local GUI to configure the 6300-CX for router mode.



* If a single antenna solution is required, it must be attached to the main antenna port labeled ‘ANT2’.

Site Survey

If you are unsure of the available cellular signal strength, or are choosing between several locations, please follow the instructions to identify the ideal installation site.

Step-by-Step Guidance: Site Survey

1. After following steps 1 and 2 in the “Initial Setup” section, connect the battery pack to temporarily power the Accelerated 6300-CX. The charge lasts two to four hours – it is not rechargeable and should be properly disposed of after use.
2. Move the 6300-CX to different locations within your site to determine the best compromise between signal strength and installation constraints. Since cellular signal strength may fluctuate, it is important to wait at each

location for 1 minute while observing the signal strength indicator on the front of the device. Minimum cellular signal strength for operation is 2 bars (3+ is preferred).

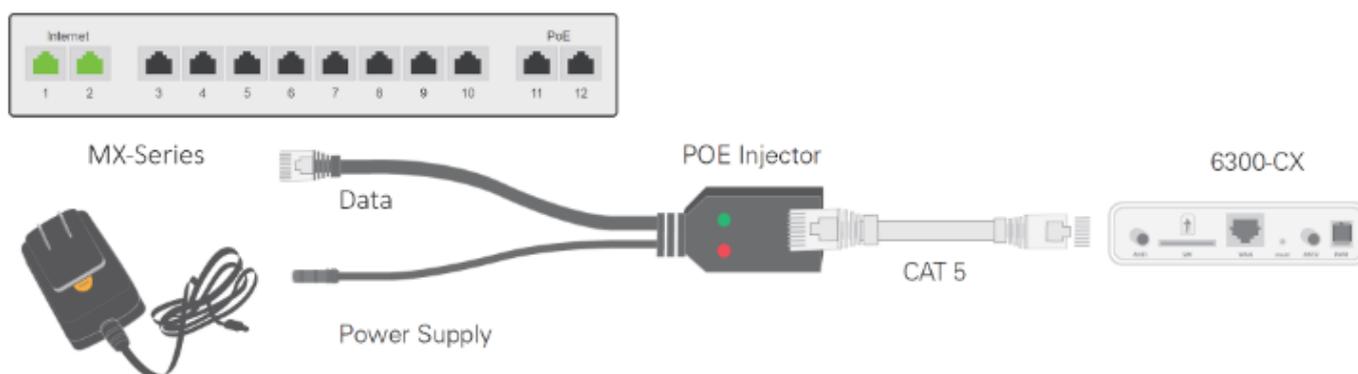
3. After determining the optimal location, remove the battery pack and connect the main power supply unit or Ethernet cable connected to the PoE injector (per the power option outlined below).

Remote Power Installation – Power Option #1

The included Power-over-Ethernet (PoE) injector allows the device to be positioned away from power outlets to simplify its installation needs. The adaptor consolidates the DC power and Ethernet connections so that both can be run to the 6300-CX via a single Ethernet cable. Distances of 300 ft have been tested on CAT6 and 250 ft on CAT5e. Note that cable conditions and the number of splices will impact actual distance.

Step-by-Step Guidance: Remote Power Installation

1. Plug the 6300-CX's power supply unit (PSU) into an AC power outlet.
2. Connect the end of the PSU into the DC input (4 pin connector) of the PoE injector.
3. Insert the male RJ45 connector of the PoE injector cable into the Meraki.
4. Connect an Ethernet cable from the RJ45 socket on the PoE injector cable to the Ethernet port of the 6300-CX. (See diagram.)

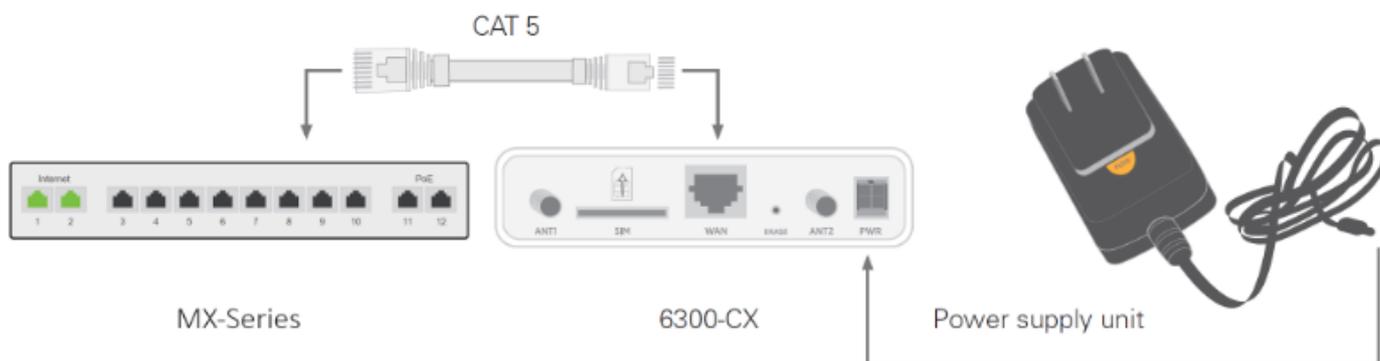


Direct Power Installation – Power Option #2

If you plan to collocate the 6300-CX with the MX device, you can directly power the 6300-CX without the PoE cable.

Step-by-Step Guidance: Direct Power Installation

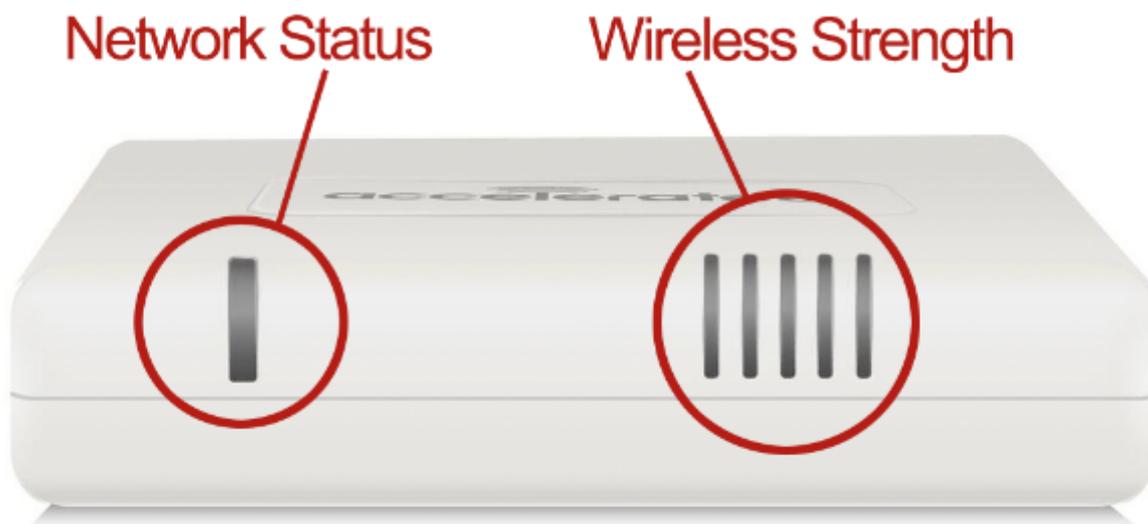
1. Use an Ethernet cable to connect the 6300-CX to the security appliance using port Internet 1 (to use the cellular network as the primary connection) or port Internet 2 (to configure a failover).
2. Plug the 6300-CX power supply unit (PSU) into an AC power outlet.
3. Connect the PSU into the 4-pin power connector of the 6300-CX. (See diagram.)



Understanding the 6300-CX LEDs

Once power has been established, your device will initialize and attempt to connect to the network. Device initialization may take 30-60 seconds. Indicator lights on the **Wireless Strength Indicator** show you the cellular network signal strength. The **Network Status Light** on the front left of the device displays connectivity information.

Please visit [accelerated.com](https://www.accelerated.com) for additional information and troubleshooting tips.



Network Status LED

	Solid Yellow Initializing or starting up.		Solid Green Connected to 2G or 3G and also has an Ethernet connection.
	Flashing Yellow In the process of connecting to the cellular network and to a device on its Ethernet port.		Flashing Blue Connected to 4G LTE and in the process of connecting to a device on its Ethernet port.
	Flashing White Has an Ethernet connection and is in the process of connecting to the cellular network.		Solid Blue Connected to 4G LTE and also has an Ethernet connection.
	Flashing Green Connected to 2G or 3G and is in the process of connecting to a device on its Ethernet port (or nothing is connected to the port).		Alternating Red/ Yellow Upgrading firmware. WARNING: DO NOT POWER OFF DURING FIRMWARE UPGRADE.

Wireless Strength LEDs

Signal Bars	Weighted dBm	Signal Strength %	Quality
	-113 to -99	0 - 23%	Bad
	-98 to -87	24 - 42%	Marginal
	-86 to -76	43 - 61%	OK
	-75 to -64	62 - 80%	Good
	-63 to -51	81 - 100%	Excellent

MX-Series Configuration with the Accelerated 6300-CX

Dual WAN Configuration

All Meraki MX Security Appliances support dual WAN connectivity right out of the box. To establish primary and secondary uplinks, connect an Ethernet cable from your modem to one of the interfaces labeled **Internet 1** or **Internet 2** on the back of the MX appliance. The secondary connection, WAN 2 unless otherwise specified, activates automatically to keep the device online should its primary WAN lose connectivity. While load balancing between the two uplinks is disabled by default, it and other traffic-related preferences can be configured to a variety of specifications via the **Traffic shaping** menu option found in the dashboard's **Security appliance** tab.

Access the Meraki dashboard at dashboard.meraki.com.

Please refer to the [MX Quick Start guide](#) for an in-depth walkthrough of how to manage your Meraki MX device.

Step-by-Step Guidance: Dual WAN Configuration

NOTE: Verify the device's MAC address, found on the bottom label of the MX series, to ensure the correct device is selected in the dashboard. (MACs, IPs, and Serial #s have been partially obscured in the screenshot above.)

1. From the **Security appliance** tab of the admin portal, select **Appliance status** (found under **Monitor**).
2. The **Live data** view shows which interfaces are currently in use by highlighting active ports green. When configured for primary and secondary internet connections, the device should indicate activity on its first two ports – Internet 1 and Internet 2.
3. Each connection's IP address is displayed next to its WAN designation along with its connection status.

Load Balancing and Automatic Failover

Traffic shaping

Uplink configuration

WAN 1	100 Mbps		details
WAN 2	20 Mbps		details

From the Meraki dashboard, MX Security Appliances can be configured for customized WAN utilization, or “traffic shaping,” which allows network administrators to model the flow of data according to the needs and specifications of their enterprise environment.

The **uplink configuration** sliders define the throughput for WAN 1 and WAN 2 to implement load distribution (or load balancing) across the two connections. When set to differing values, a ratio is established that defines flow control. For example, setting WAN 1 to 100 Mbps and WAN 2 to 20 Mbps creates a 5:1 ratio between the two for every five “flows” sent over WAN 1, a single flow will be sent over WAN 2.

Before the uplink configuration takes effect, load balancing must be initialized from the corresponding menu option found under **Global preferences**. Traffic will route according to the slider-defined proportion so long as the feature is enabled. When disabled, data transmission defaults to the primary uplink. Exceptions can be defined on a case-by-case basis with or without active load balancing via flow preferences and traffic-shaping rules.

Uplink selection

Global preferences

Primary uplink

WAN 1 ▼

Load balancing

Enabled

Traffic will be spread across both uplinks in the proportions specified above. Management traffic to the Meraki cloud will use the primary uplink.

Disabled

All Internet traffic will use the primary uplink unless overridden by an uplink preference or if the primary uplink fails.

Please refer to the [Meraki knowledge article](#) for an in-depth walkthrough of load balancing and flow preferences.

Step-by-Step Guidance: Load Balancing and Automatic Failover

NOTE: Clicking the details link allows for upload- and download-specific settings.

1. From the **Security appliance** tab of the admin portal, select **Traffic shaping** (found under **Configure**).
2. Use the **Uplink configuration** sliders to establish a proportional rate between WAN 1 and WAN 2.
3. These settings are not active until selecting **Enable** next to **Load balancing** under the **Global preferences** heading of the **Uplink selection** menu.
4. The **Primary uplink** pull-down establishes which WAN serves as the primary connection. The secondary WAN handles traffic only when load balancing is enabled (or if the primary WAN goes offline).
5. Define any exceptions by setting **Flow preferences** or **Traffic-shaping rules**, which allows for utilization of the secondary WAN on a case-by-case basis.