Upstream Firewall Rules for Cloud Connectivity

The Cisco Meraki Dashboard provides centralized management, optimization, and monitoring of Cisco Meraki devices. In order to manage a Cisco Meraki device through Dashboard, it must be able to communicate with the Cisco Meraki Cloud (Dashboard) over a secure tunnel. This tunnel is created between Cisco Meraki devices and Dashboard to pass management and reporting traffic in both directions.

Because the Dashboard is located on the public Internet, the tunnel is always initiated outbound from the managed device. Once a connection is established, the device maintains the connection by occasionally sending packets and receiving a response. When a firewall or gateway exists in the data path between the managed device and Dashboard, certain protocols and port numbers must be permitted outbound through the firewall for the secure tunnel to function.

Addresses & Ports to Allow

A complete list of destination IP addresses, ports, and their respective purposes can be found in Dashboard under Help > Firewall info:

Source IP	Destination IP	Ports	Protocol	Direction	Description	Devices using this rule
Your network(s)	64.62.142.12/32, 108.161.147.0/24, 199.231.78.0/24, 209.206.48.0/20	1024-65535, 7351	UDP	outbound	Meraki cloud communication, Meraki cloud telephony media	Access points, Cameras, MX Security Appliance, Phones, Switches
Your network(s)	52.208.175.132/32, 52.33.92.73/32, 52.39.236.233/32, 35.162.65.76/32, 35.161.241.24/32, 35.162.58.56/32, 209.206.48.0/20	443, 30001	TCP	outbound	Camera streaming proxy	Cameras
Your network(s)	Any	80, 443	TCP	bidirectional	Phone media, Backup Meraki cloud communication, Splash pages	Access points, Cameras, MX Security Appliance, Phones, Switches
Your network(s)	64.62.142.2/32, 108.161.147.0/24, 199.231.78.0/24, 209.206.48.0/20	7734, 7752	TCP	outbound	Backup configuration downloads, Throughput tests live tool, Backup firmware downloads	Access points, Cameras, MX Security Appliance, Phones, Switches
Your network(s)	Any	123	UDP	outbound	NTP time synchronization	Access points, Cameras, MX Security Appliance, Switches
Your network(s)	8.8.8.8/32	53	UDP	outbound	Uplink connection monitor	MX Security Appliance
Your network(s)	108.161.147.0/24, 199.231.78.0/24, 209.206.48.0/20	3478, 5020-5021, 7011	TCP / UDP	bidirectional	Telephony cloud communication, Meraki cloud telephony signaling	Phones
Your network(s)	8.8.8.8/32, 209.206.48.0/20		ICMP	outbound	Uplink connection monitor	MX Security Appliance

CSV Version

> "Source_IP","Destination_IP","Ports","Protocol","Direction","Description","Devices_using_this_rule"
> "Your network(s)","199.231.78.0/24, 108.161.147.0/24, 64.62.142.12/32, 209.206.48.0/20","7351","UDP","outbound","Meraki cloud communication","Access points, Cameras, MX Security Appliance, Phones, Switches"
> "Your network(s)","199.231.78.0/24, 64.156.192.245/32, 108.161.147.0/24, 209.206.48.0/20","9350","UDP","outbound","VPN registry","Access points, MX Security Appliance"
> "Your network(s)","64.62.142.2/32, 108.161.147.0/24, 199.231.78.0/24, 209.206.48.0/20","80, 443, 7734, 7752","TCP","outbound","Backup configuration downloads, Backup Meraki cloud communication, Throughput tests live tool, Backup firmware downloads, Splash pages","Access points, Cameras, MX Security Appliance, Phones, Switches"
> "Your network(s)","Any","123","UDP","outbound","NTP time synchronization","Access points, Cameras, MX Security Appliance, Switches"
> "Your network(s)","8.8.8.8/32","53","UDP","outbound","Uplink connection monitor","MX Security Appliance"
> "Your network(s)","8.8.8.8/32, 209.206.48.0/20","","ICMP","outbound","Uplink connection monitor","MX Security Appliance"

It's important to note that different organizations may communicate with different servers, so this list can vary between organizations.

Changes to Cisco Meraki Cloud (Dashboard) Addresses

There are some circumstances where the IP address or port used to communicate with Dashboard may change. If this type of change is required, administrators are notified in advance. Secure tunnel connectivity is also redundant and will continue to operate though a secondary connection.

Devices Using the 'backup Cloud connection'

While devices will primarily connect to Dashboard using UDP port 7351 for their tunnel, they will attempt to use HTTP/HTTPS if unable to connect over port 7351. When devices are operating like this, a message will be displayed on the device's status page indicating that the 'Connection to the Cisco Meraki Cloud is using the backup Cloud connection.' If this is observed, please ensure that port 7351 is being allowed outbound through the firewall or security appliance traffic from the Cisco Meraki devices will pass through.

If unable to configure the recommended firewall settings for the backup cloud connection due to security constraints, please note that Cisco Meraki devices will continue to operate normally, but some features of the Cisco Meraki Dashboard may be slower to respond. This includes, but is not limited to:

- Configuration updates
- Live tools
- Firmware upgrades

Unlike other features, Meraki Authentication is always sent over UDP 7351, and will not work over a backup connection

Note: While it is possible for Cisco Meraki devices to operate without the recommended firewall settings in place for the backup cloud connection, the

firewall settings for Meraki cloud communication are still **required** for the devices to function correctly.

Devices Using the 'Uplink connection monitor'

Cisco Meraki MX Security Appliances include features to use multiple redundant WAN links for Internet connectivity.

These features rely on connectivity tests using multiple protocols to various public Internet addresses.

We ask that Network Administrators allow these common protocols (HTTP, HTTPS, DNS and ICMP) to '**any**' Internet address to allow the connectivity tests to function correctly.

MX Connection Tests

The MX runs tests to determine uplink status:

DNS test

- Query the DNS servers (primary or secondary) configured on the Internet interface for the following hosts:
  - meraki.com
  - google.com
  - yahoo.com

Internet test

- Ping 8.8.8.8 every second.
- Uses a round-robin technique to send an HTTP GET to http://google.com, http://yahoo.com, or http://meraki.com. An HTTP response of any kind will result in a success.

ARP test

- ARP for the default gateway and its own IP (to detect a conflict).

Connection monitoring runs on the uplink once it is activated, meaning a carrier is detected and an IP address is assigned (static or dynamic).

The first test DNS query is sent, if a DNS response is received, DNS is marked as good for 300 seconds on that uplink. During this time, the MX continues running the DNS test every 150 seconds. Each successful DNS query test results in DNS being marked as good for another 300 seconds.

If a test DNS query times out at any point, the MX decreases the testing interval to 30 seconds. If the DNS test continues to fail for a time period exceeding 300 seconds which is last time the test was successful, DNS will be marked as failed on the uplink. Otherwise, a successful test will again mark the DNS as good for another 300 seconds. Once marked as good, the test is run every 150 seconds.

The MX begins performing the round robin Internet test, if each of the tests are successful, the Internet is marked as good for 300 seconds on that uplink. During this time, the MX continues running the Internet test every 150 seconds. Each successful Internet test results in the Internet as being marked good for another 300 seconds. If any test within the Internet test group fails, the MX decreases the testing interval to 20 seconds. If the tests continue to fail for a time period exceeding 300 seconds which is last time the test was successful, the Internet will be marked as failed on the uplink. Otherwise, a successful test will again mark the Internet as good for another 300 seconds. Once marked as good, the test is run every 150 seconds.

When both tests have been unsuccessful for a period of time that exceeds 300 seconds, the uplink will be failed over. Therefore it will take approximately 5 minutes for failover to occur in the event of a **soft failure** (link is still up, but provides no upstream access).

Upstream Firewall Rules for MX Content Filtering Categories

In instances where another firewall is positioned upstream from the MX, the following FQDN destinations need to be allowed in order for categorization information traffic to pass successfully to the MX, so it can use the proper category classifications. Keep in mind that the IP addresses these domains resolve to will be different regionally, so ensure you are allowing the correct, current IPs if using IP-based rules instead of FQDN rules on your upstream firewall.
Domain Names to Whitelist on Upstream Firewall

- **meraki.brightcloud.com** (resolves a CNAME to service.brightcloud.com)
- **service2.brightcloud.com**