Meraki MX/Z Security and SD-WAN Licensing

Overview

The Meraki MX security appliance is a multi-functional security & SD-WAN enterprise appliance with a wide set of capabilities to address multiple use cases for organizations of all sizes, in all industries.

Given the range of use cases that can be solved, there are three license options for the MX security appliance that provides customers the flexibility to select the license most appropriate for their intended use.

Enterprise	Advanced Security	Secure SD-WAN Plus
"All I require is Auto VPN and a firewall"	*"I connect directly to the Internet so need a UTM too"*	*"My business is reliant on SaaS/IaaS/DC served apps"*
• Essential SD-WAN • Secure connectivity & basic security	• All enterprise features • Fully featured unified threat management	• All advanced security features • Advanced analytics with machine learning powered by Meraki Insight • Smart SaaS QoE • Internet intelligence from ThousandEyes • Internet outages from ThousandEyes

The licensing structure for MX security appliances is the same as that of any other Meraki device – 1:1 ratio of devices to licenses. Pair your chosen MX appliance(s) with the relevant license for your use case:

- Enterprise license

OR

- Advanced security license

OR

- Secure SD-WAN Plus license (Org-Wide and Per Device)

If you wish to use subscription licensing, please refer to the MX and Z subscription articles for all the details. At this time, subscription and co-termination licenses can not be mixed in the same dashboard organization.

A subscription order can be created with a mix of essentials and advantage licenses. You may have one or more subscription in the same org and

each network must be bound to one subscription to consume licenses from that subscription.

The vMX only supports Essentials and does not support the Advantage tier. Essentials tier will support all the Advanced Security features noted here.

Features by License Option

The following feature breakdown is from the latest stable release. For the latest firmware release and its features, please refer the features directory documentation.

For API support, please refer to the API documentation.

Feature	Enterprise	Advanced Security	Secure SD-WAN Plus
Centralized management	✓	✓	✓
Zero-touch firmware updates (including security patches)	✓	✓	✓
True zero-touch provisioning	✓	✓	✓
24x7 enterprise support	✓	✓	✓
Open APIs	✓	✓	✓
Automatic WAN failover	✓	✓	✓
Uplink Load Balancing/Failover conditions	✓	✓	✓
Sub-second dynamic path selection	✓	✓	✓
3G / 4G cellular failover	✓	✓	✓
High Availability	✓	✓	✓
Essential SD-WAN	✓	✓	✓
SD-WAN Over Cellular	✓	✓	✓

Feature	Enterprise	Advanced Security	Secure SD-WAN Plus
Sub-second Site-to-Site VPN failover	✓	✓	✓
Site-to-site VPN (Auto VPN and 3rd party peering)	✓	✓	✓
IPv6 Support	✓	✓	✓
MPLS to VPN Failover	✓	✓	✓
SD-WAN Steering and Policies	✓	✓	✓
Traffic shaping/prioritization	✓	✓	✓
Client VPN	✓	✓	✓
Policy-Based Routing	✓	✓	✓
VLAN to VLAN routing	✓	✓	✓
Source-Based Routing	✓	✓	✓
Local Breakout (IP and Port based)	✓	✓	✓
Advanced Routing	✓	✓	✓
Client connectivity alerts	✓	✓	✓
Security Appliance alerts	✓	✓	✓
Splash pages	✓	✓	✓
Mult-WAN (2 Active + 1 Backup)	✓	✓	✓
Wireless and/or Cellular functionality	✓	✓	✓

Feature	Enterprise	Advanced Security	Secure SD-WAN Plus
Cloud Integrations	✓	✓	✓
Group Policies	✓	✓	✓
Configuration templates	✓	✓	✓
Stateful firewall	✓	✓	✓
Next-gen Traffic Analytics Engine - Network-Based Application Recognition (NBAR) Integration	✓	✓	✓
Layer 7 (Application) Enforcement powered by NBAR	✓	✓	✓
Enhanced Live Firewall Logging and Troubleshooting	✓	✓	✓
Traffic Shaping Enforcement powered by NBAR	✓	✓	✓
Catalyst + Meraki SD-WAN Interconnect (eBGP over IPsec)	✓	✓	✓
IPsec SSE tunnel monitoring, redundancy, and DIA	✓	✓	✓
Cisco XDR Integration**		✓	✓
SD-AVC Integration - Smart Application Updates Delivered via the Cloud	✓	✓	✓
DH15 and DH21 support in IPsec	✓	✓	✓
Geography based firewall rules		✓	✓
Trusted Traffic Exclusions powered by NBAR		✓	✓
Intrusion Detection and Prevention System (IDS/IPS)		✓	✓

Feature	Enterprise	Advanced Security	Secure SD-WAN Plus
Content Filtering powered by Talos Intelligence		✓	✓
YouTube Content Restriction		✓	✓
Web Search Filtering		✓	✓
Cisco Advanced Malware Protection (AMP)		✓	✓
Umbrella DNS Integration**		✓	✓
Cisco Secure Malware Analytics Integration (formerly know as Threat Grid)**		✓	✓
ThousandEyes Agent Integration**		✓	✓
Adaptive Policy (SGT Transport)		✓	✓
Adaptive Policy (SGT Assignment)			✓
Internet Outages			✓
ThousandEyes Support with Meraki Dashboard**			✓
SD-Internet Steering and Policies			✓
Web App Health			✓
WAN Health			✓
VoIP Health			✓
Smart breakout			✓

**Requires a separate license

For licenses and their respective features available in mainland China, please refer to the following article for the details.

https://documentation.meraki.com/zGeneral_Administration/Licensing/Cisco_Meraki_Licensing_Guidelines_and_Limitations/CH

Teleworker Gateway License Breakdown

The Meraki Teleworker Gateway is a type of a security appliance intended for use in small remote offices and homes of remote workers. Allowing them to securely connect back to their head offices while also offering the same security as our MX security appliance Platform.

Refer to Meraki Licensing FAQs for more information.

With the introduction of the Z4/C, we are also introducing two new types of licenses for the Teleworker series.

These licenses are not be supported by the Z1 and Z3 teleworker gateways

Z-Enterprise

- Essential SD-WAN Features
- Secure connectivity & basic security
- Advanced Security Features
- Advanced Analytics

Teleworker Features by License Options

Feature	Z-Enterprise
Centralized management	✓
Zero-touch firmware updates	✓
True zero-touch provisioning	✓
24x7 enterprise support	✓
Open APIs	✓
Automatic WAN failover	✓

Feature	Z-Enterprise
Sub-second site-to-site VPN failover	✓
Sub-second dynamic path selection	✓
Cellular failover	✓
Stateful firewall	✓
VLAN to VLAN routing	✓
Advanced Routing	✓
Traffic shaping/prioritization	✓
Site-to-site VPN	✓
Client VPN	✓
Splash pages	✓
Configuration templates	✓
Group Policies	✓
Client connectivity alerts	✓
Source-Based Routing	✓
Local Breakout (IP based)	✓
Umbrella DNS Integration**	
Geography based firewall rules	
Content filtering	

Feature	Z-Enterprise
YouTube Content Restriction	
Web Search Filtering	
Cisco Advanced Malware Protection (AMP)	
Threat Grid Integration**	
WAN Health Analytics (MI)	
VoIP Health Analytics (MI)	
Smart breakout	

Z4 Licenses are as follows:

- Z-Enterprise: LIC-Z4-ENT-[X]Y
- Secure Teleworker: LIC-Z4-SEC-[X]Y

X= Number of Years

Virtual MX (vMX) License Breakdown

Meraki vMX is a virtual security and SD-WAN appliance that creates a fast, secure, and persistent connection between networks across different physical and virtual mediums, different cloud hyperscalers, and different public cloud regions.

Any vMX running firmware 19.1 and above supports two licensing options in Co-Termination licensing model.

Enterprise	
• Essential SD-WAN Features • Secure connectivity	• All enterprise features • Advanced Security Features

The vMX Enterprise and vMX Advanced Security have a similar feature set as the MX.

vMX Features by License Options

Feature	Enterprise
Centralized management	✓
Zero-touch firmware updates (including security patches)	✓
True zero-touch provisioning	✓
24x7 enterprise support	✓
Open APIs	✓
High Availability (Act- Act model, via eBGP to Cloud routers)	✓
Sub-second Site-to-Site VPN failover	✓
Site-to-site VPN (Auto VPN and 3rd party peering)	✓
IPv6 Support	✓
Client VPN	✓
Policy-Based Routing	✓
VLAN to VLAN routing	✓
Source-Based Routing	✓
Local Breakout (IP and Port based)	✓
Advanced Routing	✓
Client connectivity alerts	✓

Feature	Enterprise
Security Appliance alerts	✓
Splash pages	✓
Cloud Integrations	✓
Group Policies	✓
Configuration templates	✓
Stateful firewall	✓
Next-gen Traffic Analytics Engine - Network-Based Application Recognition (NBAR) Integration	✓
Layer 7 (Application) Enforcement powered by NBAR	✓
Enhanced Live Firewall Logging and Troubleshooting	✓
Traffic Shaping Enforcement powered by NBAR	✓
Intrusion Detection and Prevention System (IDS/IPS)	
Content Filtering powered by Talos Intelligence	
YouTube Content Restriction	
Web Search Filtering	

* Advanced Security supported on MX19.1+ for the vMX

vMX Licenses are as follows:

- vMX-Enterprise: LIC-VMX-S/M/L-ENT-[X]Y
- vMX-Advanced-Security: LIC-VMX-S/M/L-SEC-[X]Y

X= Number of Years

Per Device SD-WAN+ License

For Enterprise Agreement Customers, please reach out to your Meraki seller if you are interested in adding Per Device SD-WAN+ Licensing to your Meraki EA Dashboard. Please note the following key points about this licensing:

- Legacy Enterprise Agreement Dashboard customers will be able to utilize Per Device SD-WAN+ (Per Dev SDW+) as they would in an a-la-carte co-term dashboard.
- EA terms including True Forward and Value Shift will apply to per-device SDW as well.

This new license type will bring SDW+ license on a per-network basis for organizations on the Coterm Licensing model with Advanced Security Licensing. Customers can now purchase the appropriate license type and assign them to the respective network to get all SD-WAN features on a per-network basis. The terms available are 1, 3 and 5 years only. Please see the table below to have the MX platforms mapped to their respective SKUs.

Once the licenses are claimed under *Organization→ License info*, you will need to go to *Insight→ Configure→ Licensing* to assign the licenses to the respective compatible networks.

1. You can assign the licenses using the *'Add licenses to network'* or remove licenses using the '*Remove Licenses from network*'
2. You can assign a higher license-tiered SKU to a lower licensed-tiered network. Example: You can assign LIC-MX-SDW-M-1YR to a MX64

No extra term will be added or subtracted when you add a higher-licensed tier to lower-tiered devices.

If Per Dev SDW+ is added to an already licensed MI network, this will replace the license and the MI license will be added back to the MI license pool

3. Assigning the Per Dev SDW+ SKU to a network will give that network access to all of the below SD-WAN features

Enterprise licensed customers cannot be in a mixed license environment.

Advance Security License is required to support a mixed license environment on the Coterm Licensing model. Please refer to the FAQ section below for mode details.

Per Device SD-WAN+ License is a per network license used to upgrade a network from Advance Security to SD-WAN+.

MX Platform	SKU
MX64/W, MX65/W	LIC-MX-SDW-XS-1Y
MX64/W, MX65/W	LIC-MX-SDW-XS-3Y
MX64/W, MX65/W	LIC-MX-SDW-XS-5Y
MX67/C/W, MX68C/W	LIC-MX-SDW-S-1Y
MX67/C/W, MX68C/W	LIC-MX-SDW-S-3Y
MX67/C/W, MX68C/W	LIC-MX-SDW-S-5Y

MX Platform	SKU
MX75, MX84, MX85	LIC-MX-SDW-M-1Y
MX75, MX84, MX85	LIC-MX-SDW-M-3Y
MX75, MX84, MX85	LIC-MX-SDW-M-5Y
MX95, MX100, MX105	LIC-MX-SDW-L-1Y
MX95, MX100, MX105	LIC-MX-SDW-L-3Y
MX95, MX100, MX105	LIC-MX-SDW-L-5Y
MX250, MX450	LIC-MX-SDW-XL-1Y
MX250, MX450	LIC-MX-SDW-XL-3Y
MX250, MX450	LIC-MX-SDW-XL-5Y

Refer to Meraki Licensing FAQ's for more information.