



vMX100 Setup Guide for Amazon AWS

Overview

This document is a walkthrough for setting up a virtual MX (vMX100) appliance in Amazon's AWS Cloud. After completing these steps outlined in this document, you will have a virtual MX appliance running in AWS that serves as an AutoVPN termination point to your physical MX devices.

Currently, vMX100 on AWS supports a one-armed concentrator configuration with split-tunnel VPN architecture. For more info on how to deploy a one-armed concentrator, please refer to [this](#) document.

Key Concepts

Before deploying a virtual MX, it is important to understand several key concepts.

Concentrator Mode

All MXs can be configured in either NAT or VPN concentrator mode. There are important considerations for both modes. For more detailed information on concentrator modes, [click here](#).

One-Armed Concentrator

In this mode, the MX is configured with a single Ethernet connection to the upstream network. All traffic will be sent and received on this interface. This is the only supported configuration for MX appliances serving as VPN termination points into AWS.

NAT Mode Concentrator

In this mode, the MX is configured with a single Ethernet connection to the upstream network and one Ethernet connection to the downstream network. VPN traffic is received and sent on the WAN interfaces connecting the MX to the upstream network and the decrypted, un-encapsulated traffic is sent and received on the LAN interface that connects the MX to the downstream network.



Note: This is not supported for virtual MX VPN concentrators operating within AWS.

VPN Topology

There are several options available for the structure of the VPN deployment.

Split Tunnel

In this configuration, branches will only send traffic across the VPN if it is destined for a specific subnet that is being advertised by another MX in the same Dashboard organization. The remaining traffic will be checked against other available routes, such as static LAN routes and third-party VPN routes, and if not matched will be NATed and sent out the branch MX unencrypted.

Full Tunnel

In full tunnel mode all traffic that the branch or remote office does not have another route to is sent to a VPN hub.



Note: This is not supported for virtual MX VPN concentrators operating within AWS.

AWS Terminology

This document will make reference to several key AWS-specific terms and concepts.

AWS

Amazon Web Services is a hosting platform that allows organizations to host infrastructures and services in the cloud.

VPC

A Virtual Private Cloud is a virtual and private network within Amazon's AWS infrastructure. A VPC has a block of associated IP addresses, which can be subdivided into multiple smaller subnets.

EC2

Elastic Compute Cloud is Amazon's virtual and cloud-based computing infrastructure. EC2 allows you to run virtual machines within your VPC. A virtual machine running on the EC2 platform is commonly referred to as an EC2 instance.

Additional Information

During the setup of your vMX100 instance, or over the course of working within AWS, you may encounter additional terminology which is not defined in this document. To find out more about these terms, and for additional details on the terms listed above, please see the [AWS glossary](#).

Meraki Dashboard Configuration

Begin by creating a new Security Appliance network in your organization. This [guide](#) will walk you through creating a new network in the Meraki Dashboard.

The Meraki Dashboard will require a vMX100 [license to be added](#) before you are able to continue. If you do not have access to a vMX100 license, please reach out to your Meraki Reseller or Sales Rep.

Once you have created the network and added the appropriate license you will be able to deploy a new vMX100 to your network by clicking on 'Add vMX':

My_Virtual_MX

There are no Meraki devices in this network. If you [add one](#) we can help you configure it. Alternatively, click on the button below to automatically add a vMX to your network:

Add vMX

After you add the new vMX100 to your network, navigate to **Security Appliance > Appliance status** and select "Generate AWS user-data" to generate the token for AWS user-data field.

● 0c:8d:db:5c:70:73
vMX100

Has never connected to the Meraki cloud

WAN Not connected

Hostname test-vmx-pttbpmqnr.dynamic-m.com

Serial number Q2AZ-EFGS-YNAB

Address

Notes

Firmware Up to date

Config Never fetched

Generate AWS user-data... ?

Remove appliance from network...

[View old version](#)

Authenticate AWS vMX to Meraki Cloud

To allow your vMX to be managed by the Meraki Cloud, generate a token for AWS user-data field using the "Generate authentication token..." button on the left

Copy the newly generated token and paste it into the User Data field of your EC2 instance.



The authentication token **must** be entered into the AWS instance within 1 hour of generating it. If it has been more than 1 hour then a new token must be generated.

AWS EC2 Authentication Token



Please copy/paste the following text verbatim into the "User Data" field of your AWS EC2 instance. Note that this one-time token expires in an hour and should be kept secret.



```
5cc29b577f423592920d58f130e6a066/316b3da23e9e7bf827e758a94b264b3218f
888833896e1519add686fd647b85c4dd9bfdf6bde8e9f2e15c8ed70a981eba8c88d22433
a00f8defbb5b48f632de5/ceea0624a5d3bb3746a8f7c47a8634154699466a1e1fc7d99d
15c6e28b525193
```

Next, follow the steps outlined in [this guide](#) to configure the vMX100 as a one-armed concentrator.


On the Site-to-Site VPN page, add each subnet in your VPC that should be accessible to remote Auto VPN peers to the list of "Local Network(s)." For more information on configuring Auto VPN, please refer to the [Site to Site VPN settings documentation](#).

AWS Setup

This section walks you through configuring the necessary requirements within AWS, and adding a vMX100 instance to your Virtual Private Cloud (VPC). For more details on setting up a VPC and other components, please refer to Amazon's AWS Documentation [here](#).

Accessing the AMI

To gain access to the AMI, navigate to [this link](#). A screenshot of the marketplace listing of vMX100 is included below:



Cisco Meraki vMX100

Sold by: [Cisco Systems, Inc.](#)

Cisco Meraki's virtual MX extends your physical MX deployment in minutes through the same Meraki dashboard. vMX100 can be used as your SD-WAN and Auto VPN node to easily connect your network with your AWS deployed services. Leveraging the power of the cloud, Cisco Meraki's virtual MX can configure, monitor, and maintain your VPN so you don't have to.

Customer Rating	★★★★★ (0 Customer Reviews)
Latest Version	1.0.0 (Other available versions)
Operating System	Linux/Unix, Other 3.18
Delivery Method	64-bit Amazon Machine Image (AMI) (Read more)
Support	See details below
AWS Services Required	Amazon EC2, Amazon EBS
Highlights	<ul style="list-style-type: none">3-click SD-WAN and Auto VPN with other Meraki MX appliancesCloud orchestrated SD-WAN and VPNQuick and easy to setup

Continue

You will have an opportunity to review your order before launching or being charged.

Pricing Information

Use the Region dropdown selector to see software and infrastructure pricing information for the chosen AWS region.

For Region

US East (N. Virginia)

Bring Your Own License (BYOL) Available for customers with current licenses purchased via other channels.

From the marketplace listing, hit **continue**.

Configuring the EC2 Image

After continuing, you will be prompted to configure the EC2 instance settings.

Begin by selecting **1-click launch**.

1-Click Launch Review, modify and launch	Manual Launch With EC2 Console, API or CLI
--	--

Leave the **version** as 1.0.0. It is the only selection available.

Version
1.0.0, released 04/25/2017

Select the **region** to launch the EC2 instance in. This should match the availability zone your VPC resides in.

Region
US West (Oregon)

Next, select the m4.large **EC2 instance** to deploy the vMX100 image on. The resources specifications of the instance type are listed upon selection.

▼ EC2 Instance Type

m4.large

Memory	8 GiB
CPU	6.5 EC2 Compute Units (2 Virtual cores with 3.25 Units each)
Storage	EBS storage only
Platform	64-bit
Network Performance	Moderate
API Name	m4.large



Running EC2 instances has an AWS infrastructure charge. Please be mindful of this when launching your instances. The charge can be found in the cost estimator table to the right of the instance type selection.

▼ Cost Estimator

Bring Your Own License (BYOL)

Available for customers with current licenses purchased via other channels.

plus

\$72.00 / month

EC2 Instance usage fees

Assumes 24 hour use over 30 days

AWS Infrastructure Charges

\$72.00 / month

Cost varies for storage fees

\$72.00 monthly EC2 instance fees for m4.large

[Varied EBS Storage and data transfer fees](#) 

As an example, this is the anticipated monthly AWS infrastructure charge for running the m4.large image. This estimate does **not** account for storage or data fees.

After selecting the instance type, select the **VPC** and **subnet** the instance will be a part of:

▼ VPC Settings

Select a VPC:

* vpc-90522bf4 (172.31.0.0/16)

Or [Create a VPC](#)

Select a subnet:

* subnet-c558d9b3 (172.31.32.0/20)

Or [Create a subnet](#)

** indicates a default vpc or subnet*

Next, select the **security group** for the EC2 instance. The default rule can be a good starting point for bringing the vMX100 online initially.

▼ Security Group

A security group acts as a firewall that controls the traffic allowed to reach one or more instances. Learn more about [Security Groups](#).

You can create a new security group based on seller-recommended settings or choose one of your existing groups.

default

! default VPC security group

Connection Method	Protocol	Port Range	Source (IP or Group)
	ALL	ALL	

! Rules with source of 0.0.0.0/0 allows all IP addresses to access your instance. We recommend limiting access to only known IP addresses.



The default security group provides fully open access to the EC2 instance. While this can be useful for connecting the vMX100 initially, it is recommended that security restrictions be put in place to restrict remote access after connecting the vMX100 to your Dashboard account.

Please see the Help -> Firewall Info page for information on connections that need to be allowed to provide Dashboard connectivity.

Finally, select the **key pair** to be used with the vMX100. This is a required step for EC2 instance setup, however, you will **not** be able to SSH into the vMX100.

▼ Key Pair

ⓘ To ensure that no other person has access to your software, the software installs on an EC2 instance with an EC2 key pair that you created. Choose an existing EC2 key pair in the list.


testing-stuff

If you do not already have a key pair created, follow the instructions provided by AWS on creating one:

▼ Key Pair

ⓘ Please create a new key pair.

Follow these steps to create a new key pair:

1. Visit the [Amazon EC2 Console](#) 
Ensure you are in the region that you wish to launch your software
2. Create a new key pair in the console
3. Return to this page and refresh the browser

After completing all of the launch configurations, click **launch with 1-click**.

Price for your Selections:

Bring Your Own License (BYOL)

Available for customers with current licenses purchased via other channels.

\$0.10 / hour

\$0.10 m4.large EC2 Instance usage fees +

\$0.00 hourly software fee

\$0.10 per GB-month of provisioned storage

EBS General Purpose (SSD) volumes

Launch with 1-click



You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#) and your use of AWS services is subject to the [AWS Customer Agreement](#).

Once this has been completed, it may be several minutes before the software subscription completes and the instance launches.

Provisioning the vMX100 for Connectivity to the Meraki Dashboard

Now that we have registered the software subscription for the vMX100 and created an EC2 instance, the vMX100 instance will need to be provisioned to communicate with the Meraki Dashboard.

The vMX100 will need to be given specific parameters before booting. In order to begin using these parameters, we must stop the instance, which starts automatically after creation. Begin by navigating to the EC2 instance console.


 Services ▾ Resource Groups ▾ 

EC2 Dashboard
Events
Tags
Reports
Limits


INSTANCES
Instances
Spot Requests

Launch Instance Connect Actions ▾

Filter by tags and attributes or search by keyword


<input type="checkbox"/>	Name ▾	Instance ID ▴	Instance Type ▾	Availability Zone ▾	Instance State ▾
<input type="checkbox"/>		i-0154b2445ce68c9f7	m4.large	ap-southeast-2b	 running

Select the vMX100 from the list of EC2 instances.

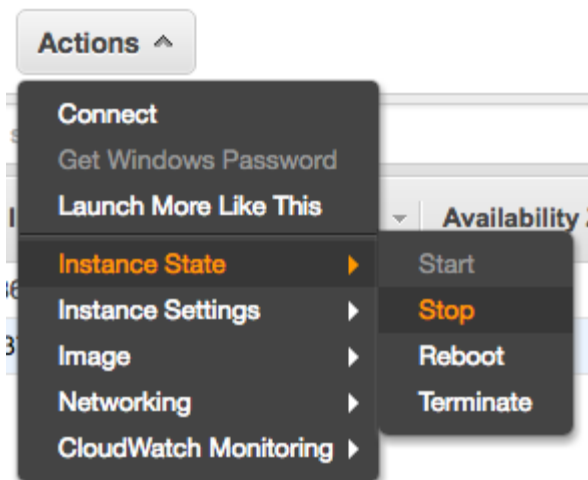


EC2 images are not given a name by default. If your EC2 instance has just been launched, an easy way to find it from the list is the *status checks* field. For new instances, it will be *initializing*.

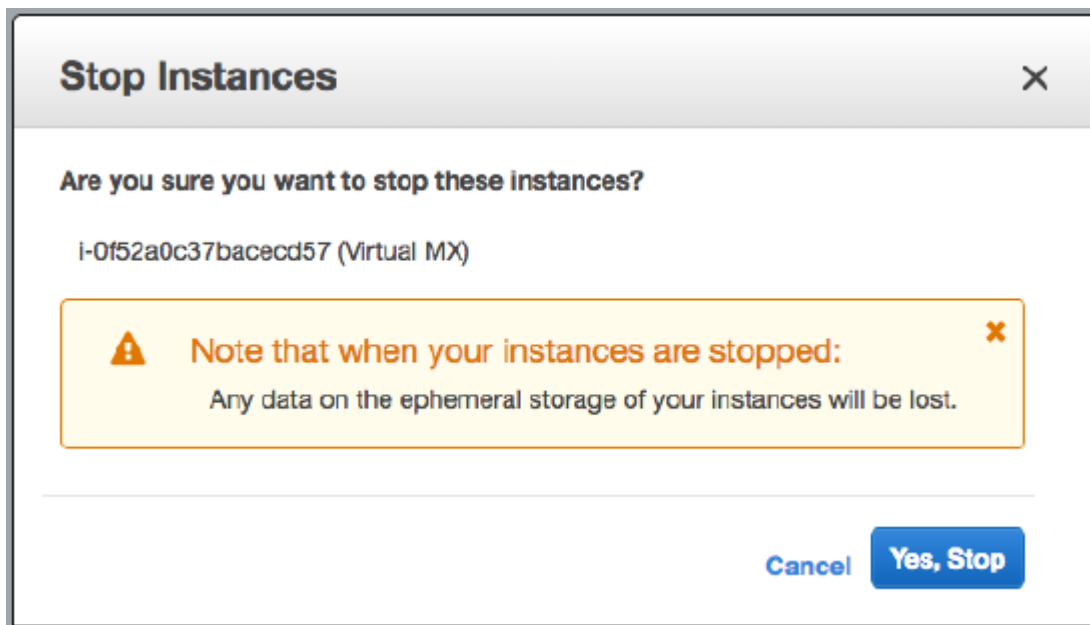
Status Checks ▾

 Initializing



With the instance selected, go to **Actions > Instance State** and select **stop**.



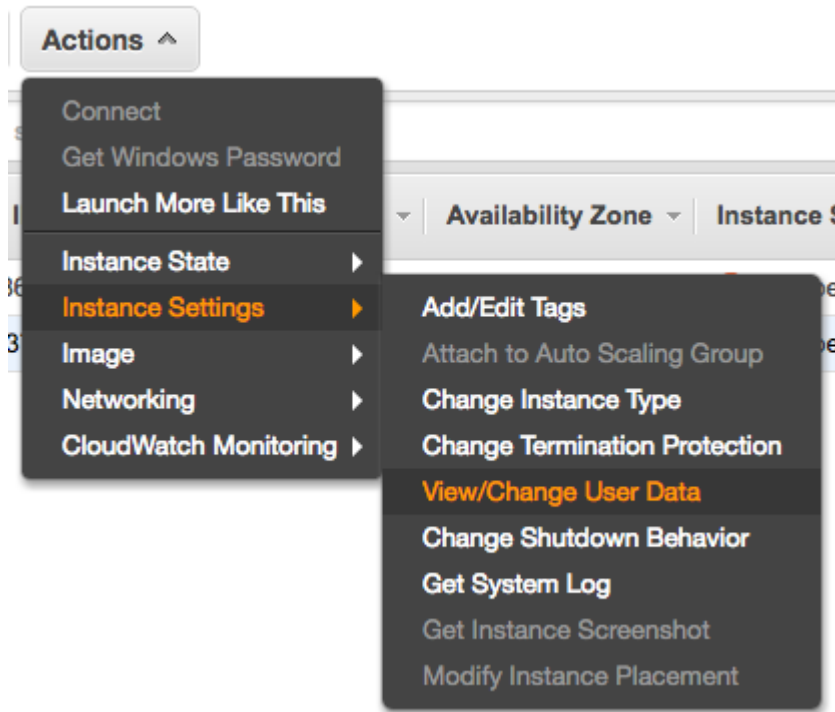
Select **yes, stop** from the following confirmation menu.



Wait until the instance state is **stopped**.

	i-0154b2445ce68c9f7	m4.large	ap-southeast-2b	 stopped
---	---------------------	----------	-----------------	---

After the instance is stopped, select the instance again and navigate to **Actions > Instance Settings** and select **view/change user data**.



In the user data text field, enter the token that was generated on the dashboard. The input type must be set as **plain text**. Then, hit **save**.

View/Change User Data



Instance ID: i-0673837627dc301b6

User Data:

```
57c500dfcf991dd7f7becadd2e90c892/c0bf5dc410179d5011d9eb1df8237dd07
af98b86afc8fbe33e186ee68994447b9d083bc2299cff9628ae9d389dd6e74dfe
656b8cdfaad4318e5ef0bd47ed625/4af6d64ad4aaaaa03d3139a386a07a06f5ab
6a4b878e46ba92788d49bdf46a74|
```

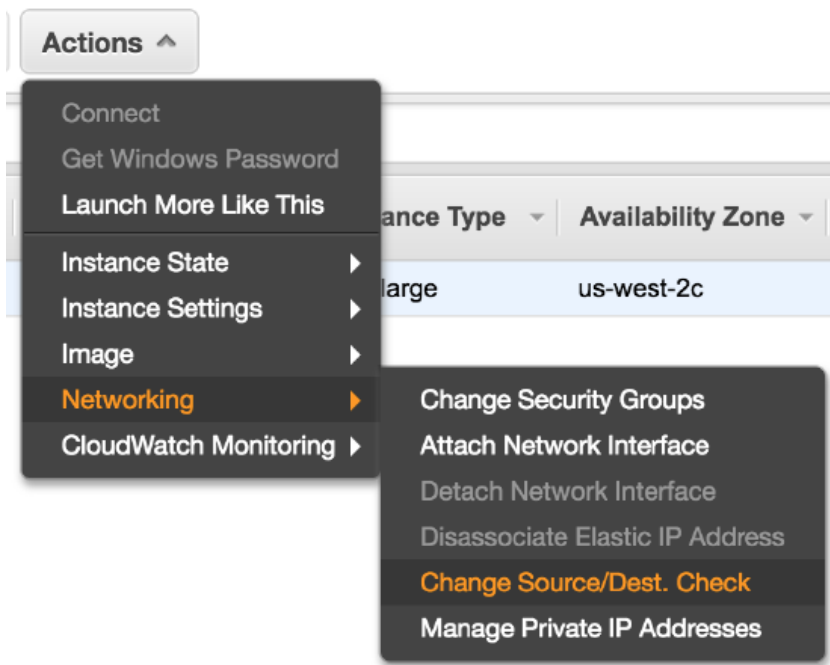
☒ Plain text ☐ Input is already base64 encoded

Cancel

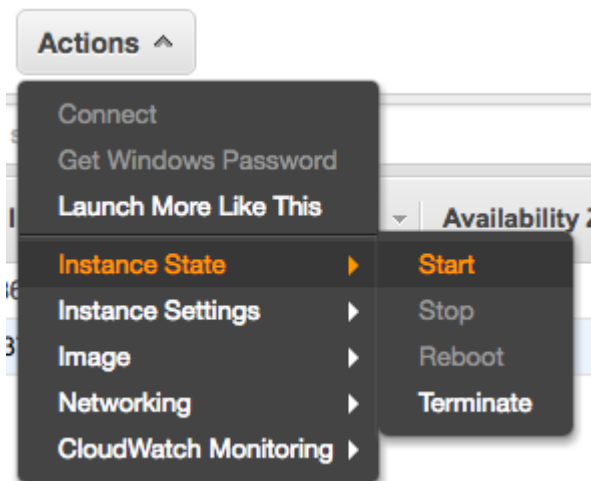
Save

Once the user data has been updated, you'll need to disable Source IP and Destination IP checking on the network interface attached to the Meraki vMX100 instance.

To do this, navigate to **Actions > Networking** and select **Change Source/Dest. Checking**. A dialog box will pop up - confirm the details and click on **Yes, Disable**.



After the **Source/Dest. Checking** has been disabled, select the instance, navigate to **Actions > Instance State** and select **start**. Hit **Yes, start** in the following confirmation menu.

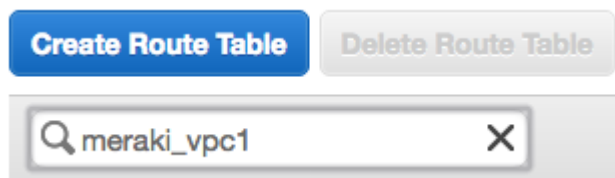


Additional VPC Configuration

The virtual MX appliance will allow for site-to-site VPN connectivity using AutoVPN between AWS and other remote MXs. In order to have proper bi-directional communication between remote subnets that are terminating into AWS via the vMX100 and hosts within AWS, the VPC routing table must be updated for the remote AutoVPN-connected subnets.

To do this, navigate to the "VPC" dashboard in AWS, and follow the steps below

1. Click on "Route Tables" on the left-hand side
2. Find the route table associated with the VPC or subnet the vMX100 is hosted in (you can quickly filter the list by typing in your VPC ID or name in the search box)



3. Click on the route table in the list to select it, then click on the "Routes" tab in the details pane below the list of routing tables
4. Click the "Edit" button
5. Click the "Add another route" button at the bottom of the route table
6. In the "Destination" column, add the routes available via AutoVPN
7. In the "Target" column, select the vMX100 instance or interface ID
8. Repeat steps 5-7 for each network available via AutoVPN and Client VPN if applicable. You may want to use a summary address. Below is an example of two networks available via AutoVPN.

Destination	Target	Status	Propagated	Remove
172.21.0.0/16	local	Active	No	
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="igw-9db909f9"/>	Active	No	✕
<input type="text" value="172.16.4.0/24"/>	<input type="text" value="eni-984668c6"/>	Active	No	✕
<input type="text" value="192.168.100.0/24"/>	<input type="text" value="eni-984668c6"/>	Active	No	✕

Troubleshooting

The virtual MX security appliance is fully managed through the Cisco Meraki Dashboard. This requires the vMX100 to establish bi-directional communication to the Meraki Cloud. If, after following the steps above, the vMX100 is inaccessible, please review the following:

1. The token is entered into the **user data** field.
2. The DNS server is reachable from the subnet that the vMX100 is in.
3. The vMX's security group allows outbound communication to the Meraki cloud.
 - If restrictive settings are in use, refer to the [Help > Firewall Info](#) page and [this](#) article for the connections that must be allowed for Dashboard communication
4. The VPC ACLs allows outbound communication to the Meraki cloud.
 - If restrictive settings are in use, refer to the [Help > Firewall Info](#) page and [this](#) article for the connections that must be allowed for Dashboard communication



Please note that Meraki Support does not troubleshoot AWS specific firewall rules and deployments.