

# Configure Secure Access with Meraki MX for High Availability and Health Monitoring

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

### [Configure the VPN on Secure Access](#)

[Secure Access VPN Configuration](#)

### [Configure the VPN on Meraki MX](#)

[Site-to-site VPN](#)

[VPN Settings](#)

[Non-Meraki VPN Peers](#)

[Configure Primary Tunnel](#)

[Configure Secondary Tunnel](#)

[Configure Traffic Steering \(Tunnel Traffic Bypass\)](#)

### [Verify](#)

### [Troubleshoot](#)

[Verify HealthChecks](#)

### [Related Information](#)

---

## Introduction

This document describes how to configure Cisco Secure Access with Meraki MX for High Availability using health checks.

## Prerequisites

- [Review IPsec Tunnel Requirements with Secure Access](#)
- Understand Secure Access Components
- [Understand Health Check Functionality in Meraki MX](#)

## Requirements

- Meraki MX must be running firmware version 19.1.6 or later
- When using Private Access, only one tunnel is supported due to a Meraki limitation that prevents changing the health check IP, making NAT required for additional SPA (Secure Private Access) tunnels. This does not apply when using SIA (Secure Internet Access).
- Clearly define which internal subnets or resources are routed through the tunnel to Secure Access.

## Components Used

- Cisco Secure Access
- Meraki MX Security Appliance (firmware version 19.1.6 or later)
- Meraki Dashboard
- Secure Access Dashboard

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information



Cisco Secure Access is a cloud-native security platform that enables secure access to both private applications (via Private Access) and internet destinations (via Internet Access). When integrated with Meraki MX, it allows organizations to establish secure IPsec tunnels between branch sites and the cloud, ensuring encrypted traffic flow and centralized security enforcement.

This integration uses static routing IPsec tunnels. Meraki MX establishes primary and secondary IPsec tunnels to Cisco Secure Access, and leverages its built in uplink health checks to perform automatic failover

between tunnels. This provides a resilient and high-availability configuration for branch connectivity.

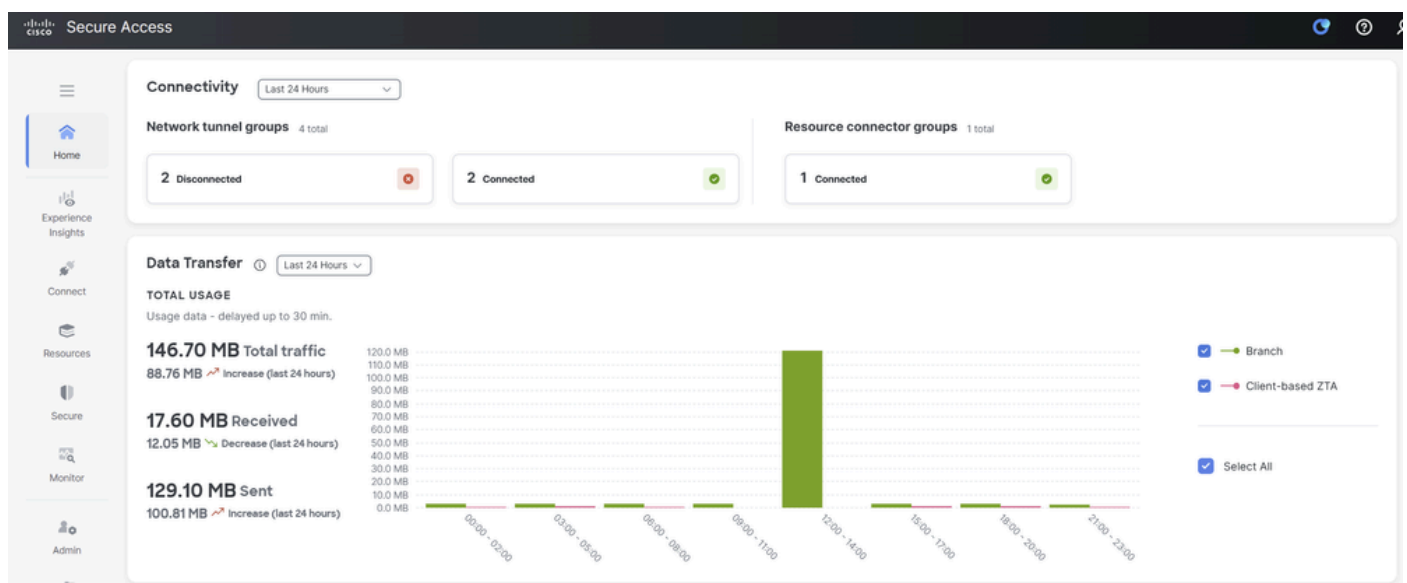
Key elements of this deployment include:

- Meraki MX acting as a non-Meraki VPN peer to Cisco Secure Access.
- Primary and secondary tunnels configured statically, with health checks determining availability.
- Private Access supports secure access to internal applications through SPA (Secure Private Access), while Internet Access allows traffic to reach internet-based resources with policy enforcement in the cloud.
- Due to Meraki limitations in health check IP flexibility, only one tunnel group is supported in Private Access mode. If multiple Meraki MX devices need to connect to Secure Access for Private Access, you must either use [BGP](#) for dynamic routing, or configure static tunnels, understanding that only one Network Tunnel Group can support health checks and high availability. Additional tunnels operate without health monitoring or redundancy.

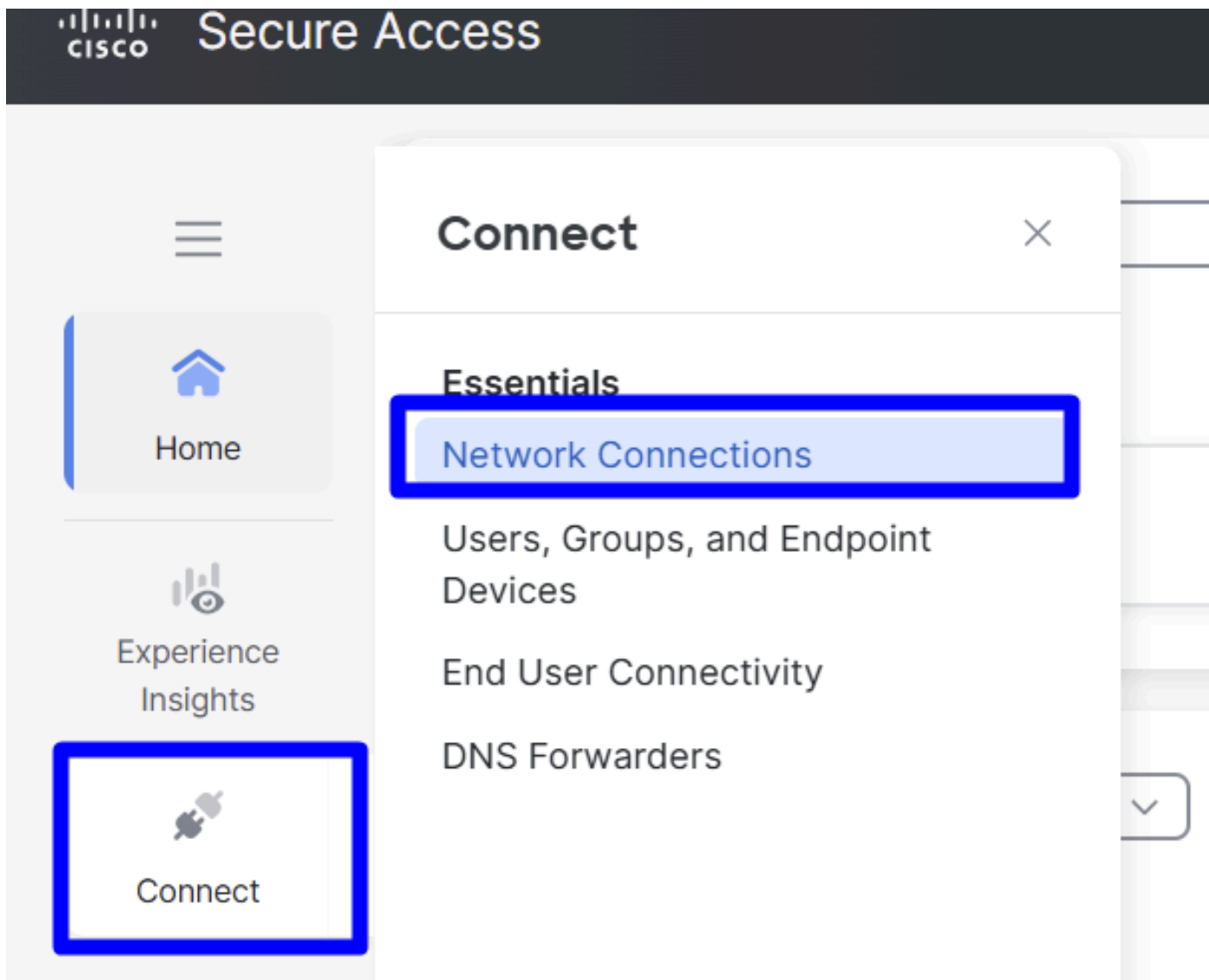
## Configure

### Configure the VPN on Secure Access

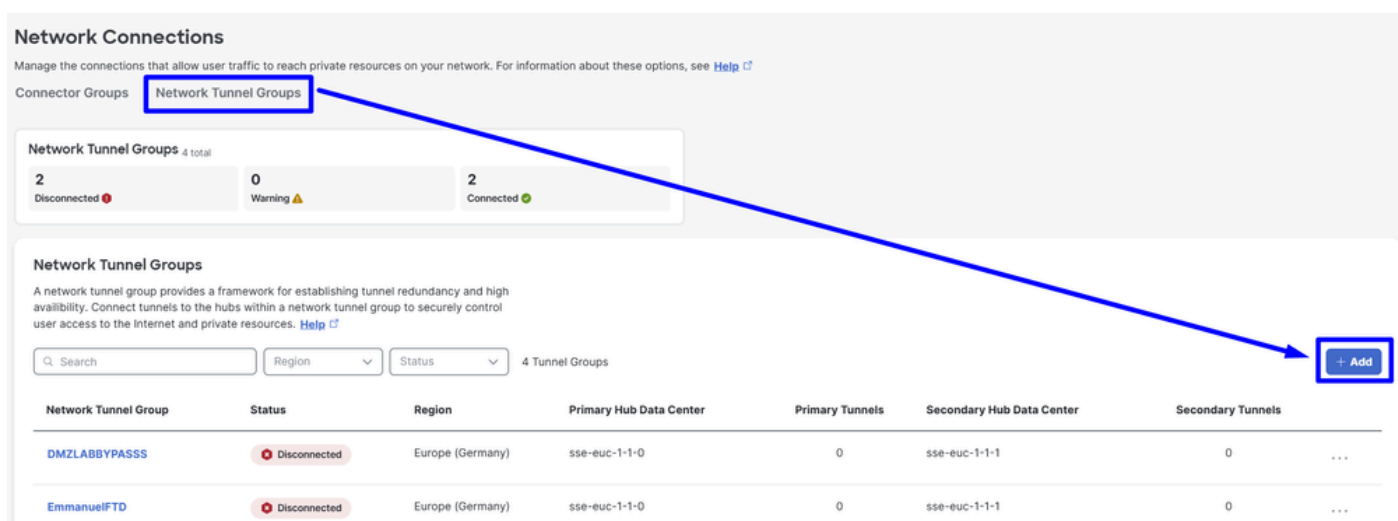
Navigate to the admin panel of [Secure Access](#).



- Click on Connect > Network Connections



- Under Network Tunnel Groups click on + Add



- Configure Tunnel Group Name, Region and Device Type
- Click Next

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

### General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

**Tunnel Group Name**

**Region**

**Device Type**

[<](#)
[Cancel](#)
[Next](#)

- Configure the Tunnel ID Format and Passphrase
- ClickNext

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

### Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

**Tunnel ID**

 @<org><hub>.sse.cisco.com
 

**Passphrase**

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

**Confirm Passphrase**

[<](#)
[Cancel](#)
[Back](#)
[Next](#)

- Configure the IP address ranges or hosts that you have configured on your network and want to pass the traffic through Secure Access and and make sure to include the Meraki monitoring probe IP 192.0.2.3/32 to allow return traffic from Secure Access back to the Meraki MX.
- ClickSave

- General Settings
- Tunnel ID and Passphrase
- Routing
- 4 Data for Tunnel Setup

## Routing options and network overlaps

Configure routing options for this tunnel group.

### Network subnet overlap

☐ Enable NAT / Outbound only

Select if the IP address space of the subnet behind this tunnel group overlaps with other IP address spaces in your network. When selected, private applications behind these tunnels are not accessible.

### Routing option

☒ Static routing

Use this option to manually add IP address ranges for this tunnel group.

#### IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

128.66.0.0/16, 192.0.2.0/24

Add

192.0.2.3/32

192.168.50.0/24

☐ Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

Advanced Settings

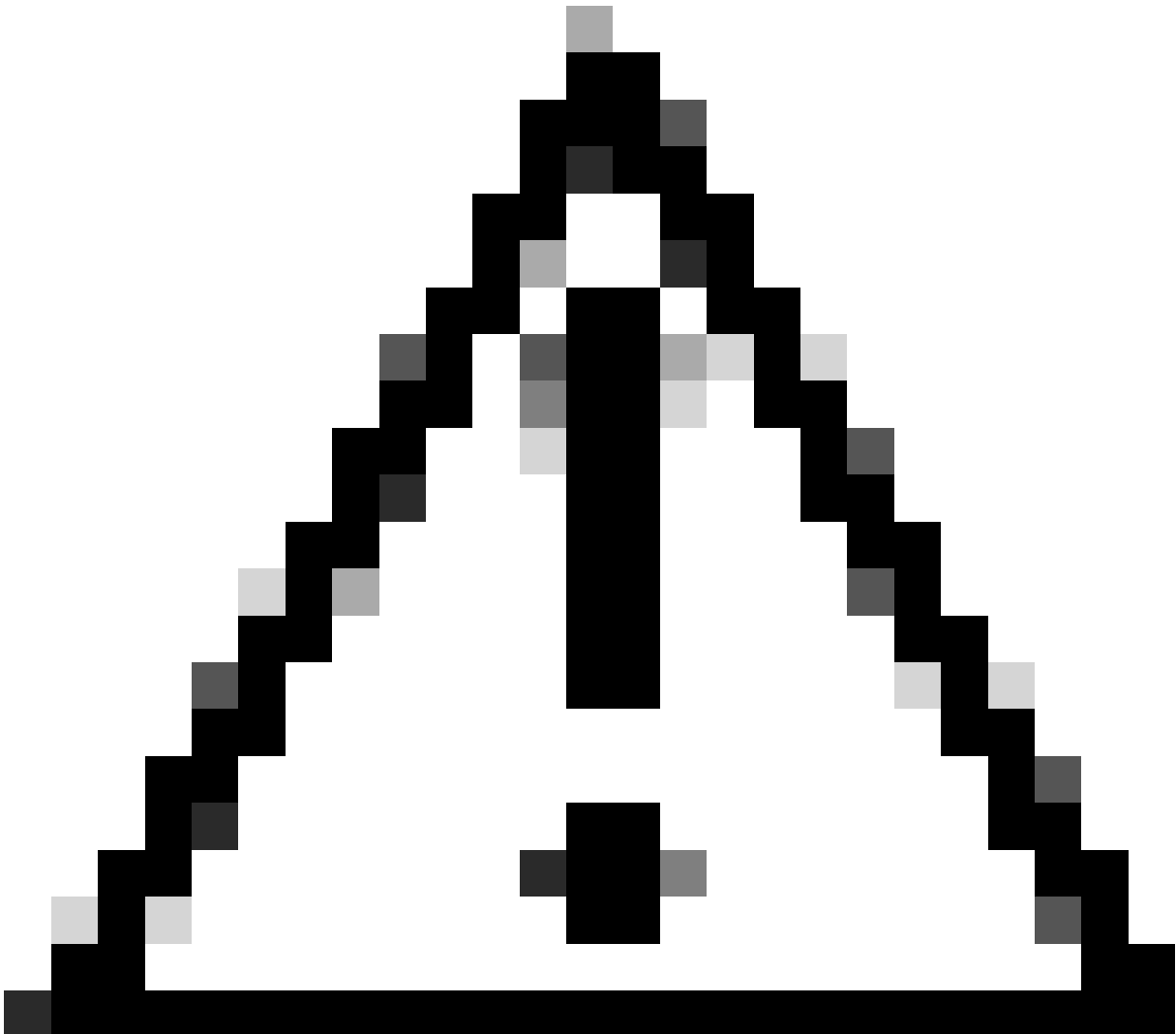


Cancel

Back

Save

Meraki MX Probe IP



**Caution:** Be sure to add the monitoring probe IP (192.0.2.3/32); otherwise, you can experience traffic issues on the Meraki device that route the traffic to Internet, VPN Pools and CGNAT Range 100.64.0.0/10 used by ZTNA.

- After you click on **Save** the information about the tunnel gets displayed, please save that information for the next step, **Configure the tunnel on Meraki MX**.

## Secure Access VPN Configuration

Copy the configuration of the tunnels in a notepad, Use this information to complete the configuration in Meraki Non-Meraki VPN Peers.

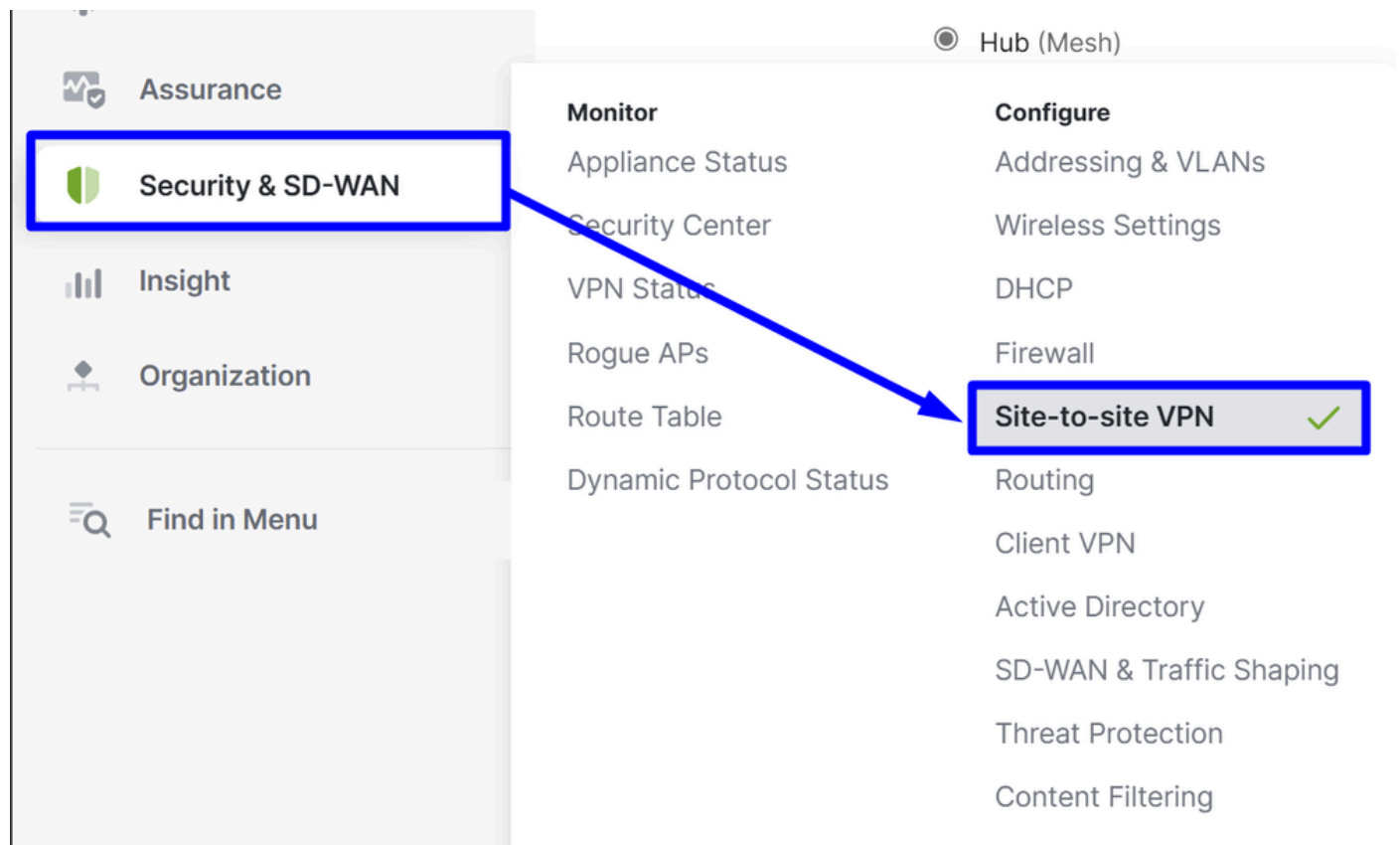
**Data for Tunnel Setup**  
Review and save the following information for use when setting up your network tunnel devices.

Primary Tunnel ID:	MerakiShadow@
Primary Data Center IP Address:	18.156.145.74
Secondary Tunnel ID:	MerakiShadow@
Secondary Data Center IP Address:	3.120.45.23

[Download CSV](#) [Done](#)

## Configure the VPN on Meraki MX

Navigate to your Meraki MX and click on **Security & SD-WAN** > Site-to-site VPN



## Site-to-site VPN

Choose Hub.

### Site-to-site VPN

Type 

☐ Off

Do not participate in site-to-site VPN.

☒ Hub (Mesh)

Establish VPN tunnels with all hubs and dependent spokes.

☐ Spoke






Establish VPN tunnels with selected hubs.

## VPN Settings

Choose the networks that you selected to send traffic to Secure Access:

### VPN settings

Local networks

Name	VPN mode	Subnet	Uplink
Default	Disabled ▾	 192.168.0.0/24	Any
SSE-MERAKI	Enabled ▾	 192.168.50.0/24	Any
LAB NETWORK	Disabled ▾	 192.168.10.0/24	
LAB NETWORK-30	Disabled ▾	 192.168.30.0/24	
FMC	Disabled ▾	 100.64.0.0/10	

Choose in NAT Traversal Automatic



NAT traversal

☒ Automatic

Connections to remote peers are arranged by the Meraki cloud.

☐ Manual: Port forwarding

Remote peers contact the WAN appliance using a public IP and port that you specify.

Use this if your WAN appliance is behind another NAT and "Automatic" traversal does not work.

## Non-Meraki VPN Peers

You need to configure the health checks that Meraki uses to route traffic to Secure Access:

Click on **Configure Health Checks**

- Click on **+Add health Check**

Health check

Endpoint

Cancel

Done



Health check name  
can't be blank.

- Health Check:** Configure a name for the test
- Endpoint:** Use the one recommended by Secure Access <http://service.sig.umbrella.com>



**Note:** This domain responds only when accessed via a site-to-site tunnel with Secure Access or Umbrella: access attempts from outside these tunnels fail.

---

Then click **Done** two times to finalize.

## Configure health checks

Configure your health checks to use for tunnel health. Health check will use this IP for probing when the MX is in passthrough mode. Only one health check per tunnel can be used.

[+ Add health check](#)

Health check	Endpoint	
<input type="text" value="SSE"/>	<input type="text" value="http://service.sig.umbrella.com"/>	<a href="#">Cancel</a> <a href="#">Done</a>

Rows per page  [<](#) [1](#) [>](#)

[Cancel](#) [Done](#)

Now your health checks are configured and you are ready to configure the Peer:

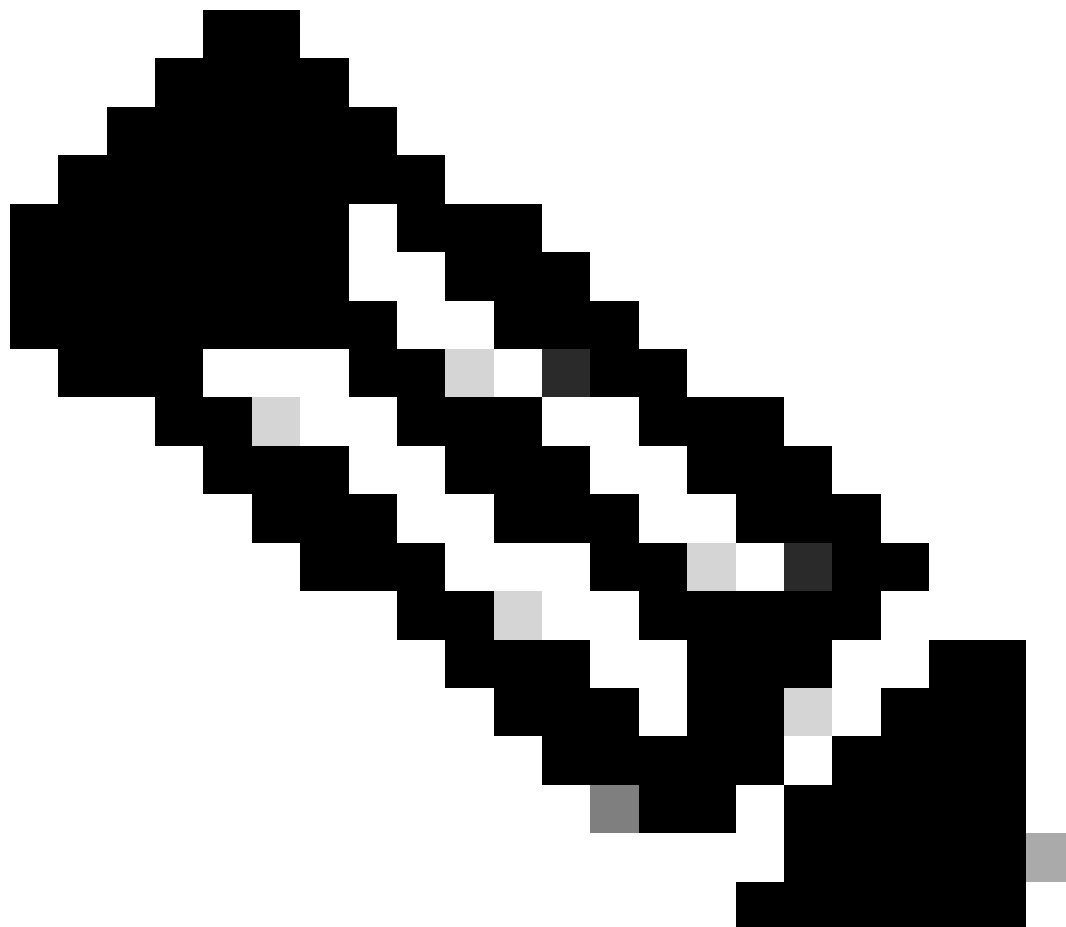
## Configure Primary Tunnel

- Click on [+ Add a peer](#)

<b>Name</b> <input type="text" value="SSE-MERAKI Primary"/>	<b>Remote ID</b> ⓘ <input type="text" value="Optional"/>	<b>Availability</b> ⓘ <input type="text" value="All networks"/>
<b>IKE version</b> <input type="text" value="IKEv2"/> <small>IKEv2 is required to support backup tunnels and failover features</small>	<b>Shared secret</b> <input type="text" value="....."/> <a href="#">Show</a>	<b>Tunnel monitoring</b>
<b>Peers</b> ^	<b>Routing</b> <input checked="" type="radio"/> Static <input type="radio"/> Dynamic (BGP) <small>Static routing is required to support backup tunnels and failover features</small>	<b>Health check</b> <input type="text" value="SSE"/>
<b>Public IP or Hostname</b> <input type="text" value="18.156.145.74"/>	<b>Private subnets</b> ⓘ <input type="text" value="0.0.0.0/0"/>	<b>Failover directly to internet</b> ⓘ <input checked="" type="checkbox"/> Enable failover
<b>Local ID</b> <input type="text" value="Merakishadow@...cit"/>		<b>IPsec policy</b> ^
		<b>Preset</b> <input type="text" value="Umbrella"/>

- Add VPN Peer**
  - Name:** Configure a name for the VPN to Secure Access
  - IKE version:** Choose IKEv2
- Peers**
  - Public IP or Hostname:** Configure the **Primary Datacenter IP** given by Secure Access in the step [Secure Access VPN Configurations](#)
  - Local ID:** Configure the **Primary Tunnel ID** given by Secure Access in the step [Secure Access VPN Configurations](#)
  - Remote ID:** N/A
  - Shared secret:** Configure the **Passphrase** given by Secure Access in the step [Secure Access VPN Configurations](#)
  - Routing:** Choose Static

- **Private subnets:** If you plan to configure both Internet Access and Private Access, use **0.0.0.0/0** as the destination. If you are configuring only Private Access for that VPN tunnel, specify the **Remote Access VPN IP Pool** and the CGNAT range **100.64.0.0/10** as destination networks
  - **Availability:** If you have only one Meraki device, you can select **All Networks**. If you have multiple devices, make sure to select only the specific Meraki network where you are configuring the tunnel.
  - **Tunnel Monitoring**
    - **Health check:** Use the previously configured health check to monitor tunnel availability
    - **Failover directly to internet:** If you enable this option, and both Tunnel 1 and Tunnel 2 fail their health checks, traffic is redirected to the WAN interface to prevent loss of internet access.
- 



**Health Check Functionality:** If Tunnel 1 is being monitored and its health check fails, traffic automatically fails over to Tunnel 2. If Tunnel 2 also fails, and the **Failover directly to Internet** option is enabled, traffic is routed through the WAN interface of the Meraki device.

---

- **IPsec policy**
  - Preset: Choose **Umbrella**

Then click **Save**.

# Configure Secondary Tunnel

To configure the secondary tunnel, click on the options menu of the primary tunnel:

- Click on the three dots

#	Name	IKE version	IPsec policies	Public IP or Hostname	Local ID	Remote ID	IPsec subnets	Health check	Preshared secret	Availability/Network		
> 1	SSE-MERAKI Primary	Primary	IKEv2	Umbrella	18.156.145.74	merakijairo@8195126-646082001-sse.cisco.com	—	0.0.0.0/0	SSE	*****	All networks	...

1-1 of 1 Rows per page 10 < 1 >

- Click on + Add Secondary peer

## Primary



Edit primary peer



Move to



Delete primary peer

---

## Secondary



Add secondary peer

- Click on `Inherit` primary peer configurations

# Add Secondary VPN Peer



**Inherit primary peer configurations**



**Name**

SSE Secondary

IKE version

**IKEv2**

---

Then you notice some fields are filled in automatically. Review them, make any necessary changes, and complete the rest manually:

## Peers



Public IP or Hostname

Local ID

Remote ID ⓘ

Shared secret

 [Show](#)

Routing

Static

Private subnets ⓘ

0.0.0.0/0

## Tunnel monitoring

Health check

 ⓘ ▾

- **Peers**

- **Public IP or Hostname:** Configure the **Secondary Datacenter IP** given by Secure Access in the step [Secure Access VPN Configurations](#)
- **Local ID:** Configure the **Secondary Tunnel ID** given by Secure Access in the step [Secure Access VPN Configurations](#)
- **Remote ID:** N/A
- **Shared secret:** Configure the **Passphrase** given by Secure Access in the step [Secure Access VPN Configurations](#)

- **Tunnel Monitoring**

- **Health check:** Use the previously configured health check to monitor tunnel availability

Then after that you can click **Save**, and the next alert appears:

The settings you requested require confirmation. Please review the following list.

- The VLAN subnets 192.168.0.0/24 and 192.168.50.0/24 overlap with remote VPN subnets on non-Meraki peers SSE-MERAKI Primary (0.0.0.0/0) and SSE-MERAKI Primary Secondary (0.0.0.0/0). IP traffic will be routed to the smallest subnet that contains the IP address.
- In the non-Meraki VPN peers configuration, potential overlaps might occur between the subnets on SSE-MERAKI Primary (0.0.0.0/0), SSE-MERAKI Primary Secondary (0.0.0.0/0), and SSE (1.1.1.1/32). Please note that in this case, IP traffic will be routed to the most specific subnet.
- In the non-Meraki VPN peers configuration, potential conflicts might occur between the subnets on SSE-MERAKI Primary (0.0.0.0/0) and SSE-MERAKI Primary Secondary (0.0.0.0/0). Before confirming your changes, please review the network tags under the Availability column for each of these non-Meraki VPN peers and ensure that there are no Security Appliances within your Organization that are tagged across different non-Meraki VPN peers with conflicting subnets. Please note that in the event that a single Security Appliance is configured with the same private subnets for more than one non-Meraki VPN peer, the routing behavior of your IP traffic will be undefined.
- To learn more, please refer to the Peer Availability section of the Site-to-site VPN Settings knowledge base article (accessible through the non-Meraki VPN peers tooltip).

[Confirm Changes](#)

[Cancel](#)

Do not worry and click **Confirm Changes**.

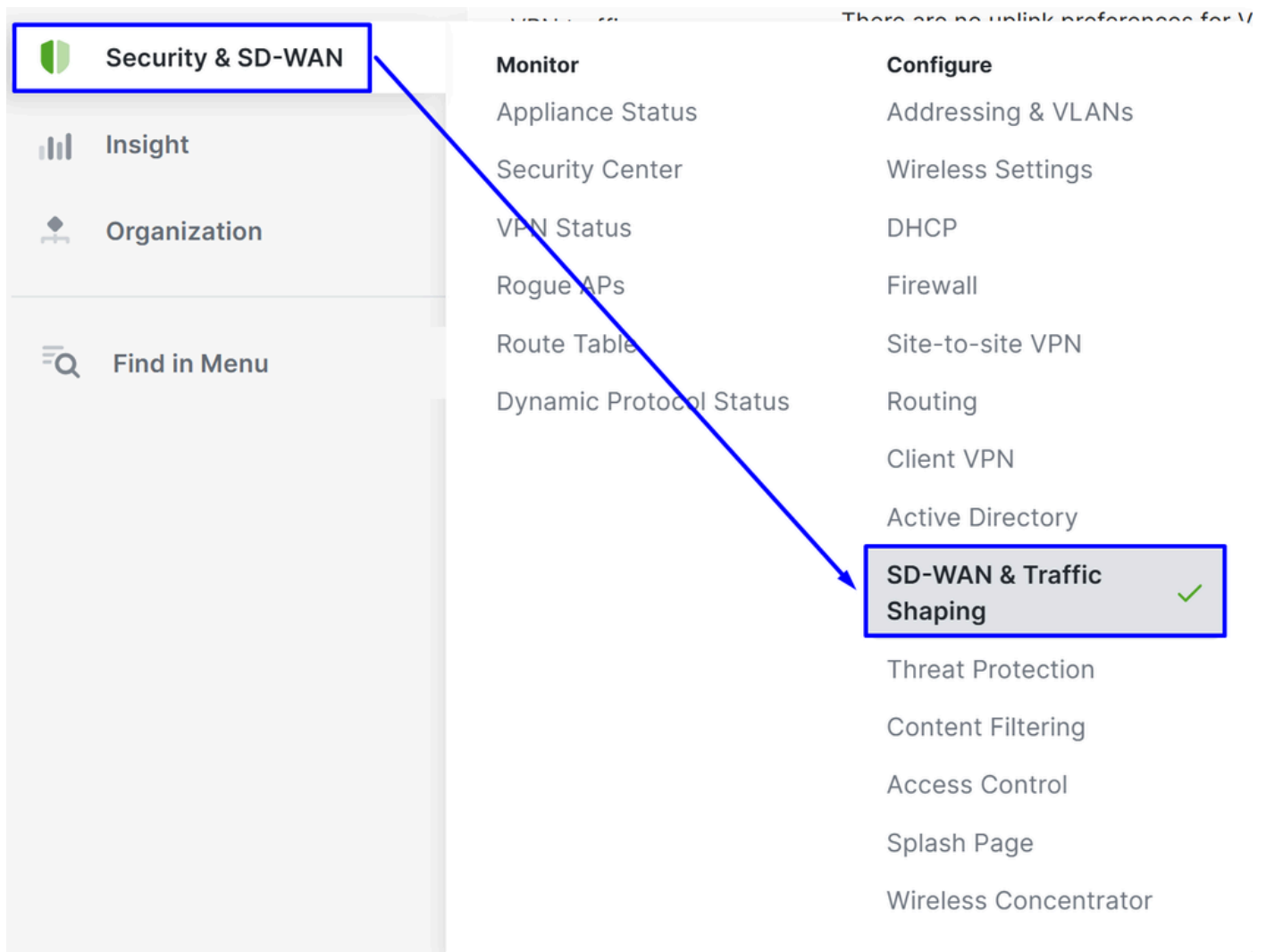
## Configure Traffic Steering (Tunnel Traffic Bypass)

This feature allows you to bypass specific traffic from the tunnel by defining domains or IP addresses in the



## SD-WAN Bypass configuration:

- Navigate to **Security & SD-WAN** > SD-WAN & Traffic Shaping



- Scroll down to the **Local Internet Breakout** section and click on **Add+**

## Local internet breakout

### VPN exclusion rules

Add +

Then create the bypass based on **Custom Expressions** Or **Major Applications**:

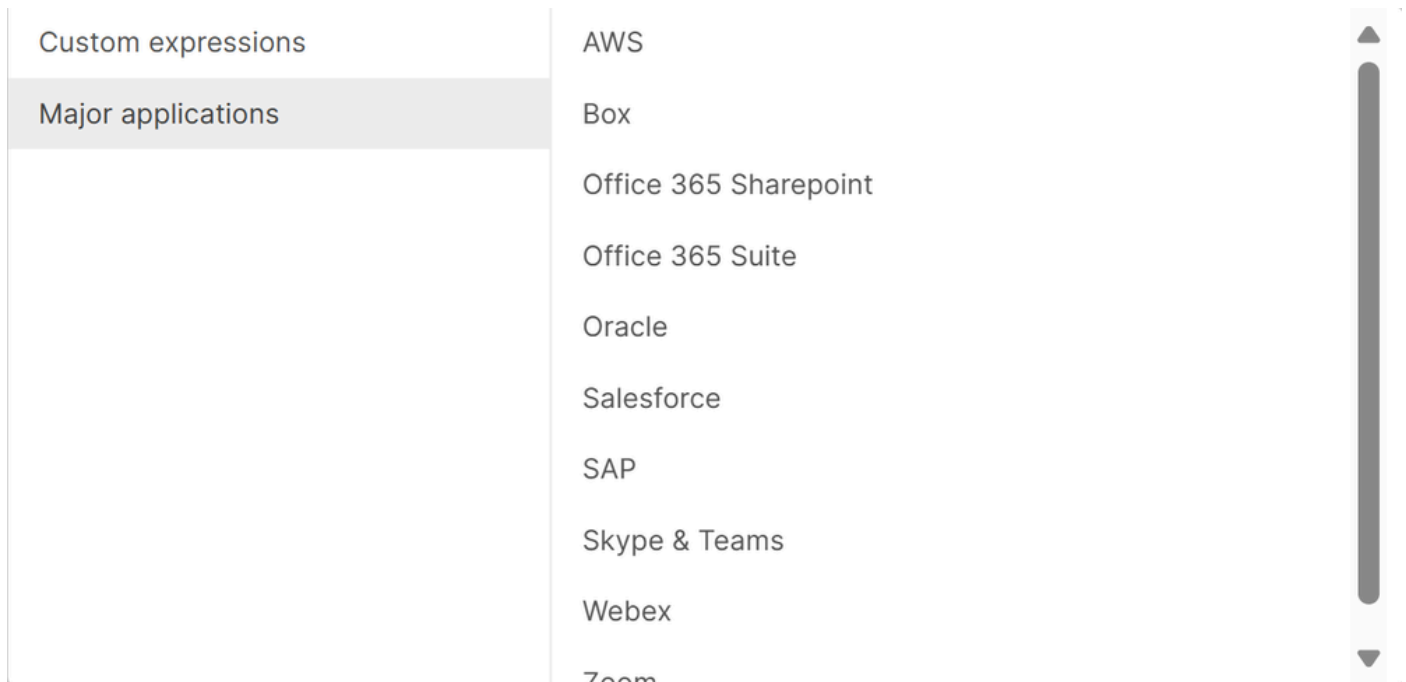
## Custom Expressions - Protocol

Custom expressions	<b>Custom expressions</b>
Major applications	Protocol <div>TCP</div>
	Destination ⓘ <div>8.8.8.8</div>
	Dst port ⓘ <div>443</div>
	<div>Add expression</div>

## Custom Expressions - DNS

Custom expressions	<b>Custom expressions</b>
Major applications	Protocol <div>DNS</div>
	Destination ⓘ <div>facebook.com</div>
	Dst port ⓘ <div>443</div>
	<div>Add expression</div>

## Major Applications

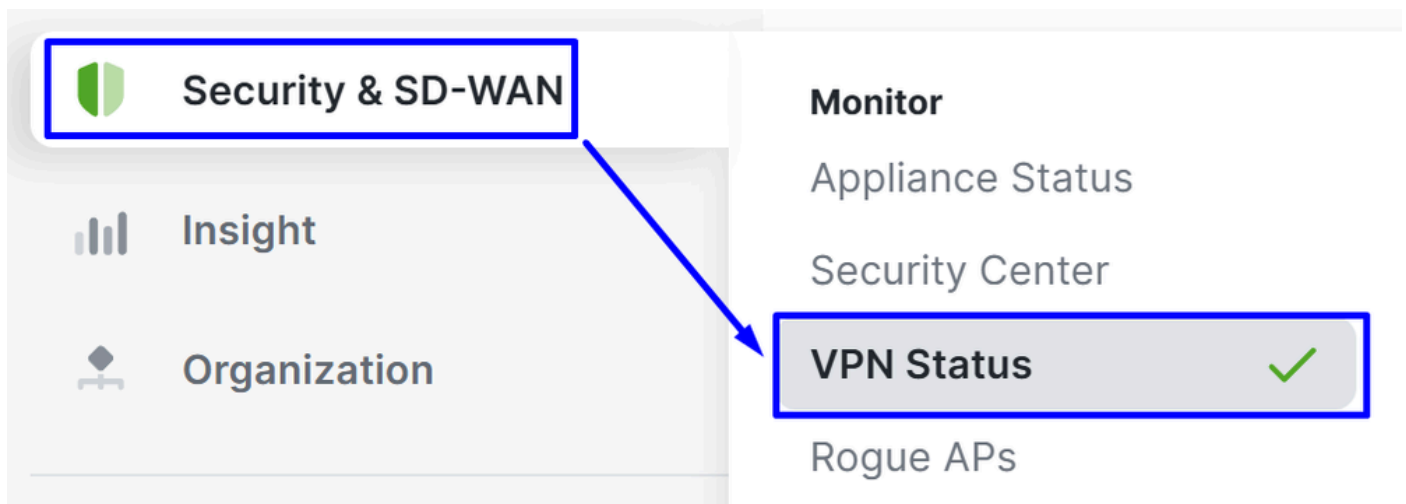


For more information, please visit: [Configuring VPN Exclusion Rules \(IP/Port/DNS/APP\)](#)

## Verify

To check if the tunnels are up, please verify the status in:

- Click on Security & SD-WAN > **VPN Status** on the Meraki Dashboard.



- Click on Non-Meraki peers:

Status ▲	Name	Public IP	Subnets	+
●	SSE-MERAKI Primary	18.156.145.74	0.0.0.0/0	
●	SSE-MERAKI Primary Secondary	3.120.45.23	0.0.0.0/0	
2 total				

If both the Primary and Secondary VPN statuses are shown in green, it means the tunnels are up and active.

## Meraki VPN Status Codes

Status Indicator	Color	Meaning
 Primary/Secondary Up	Green	Phase 1 and phase 2 are up
 Partial Connectivity	Amber	Phase 1 is up but phase 2 is down
 Tunnel Down	Red	Phase 1 and phase 2 are both down

## Troubleshoot

### Verify HealthChecks

To verify if Meraki health checks for the VPN are working properly, Navigate to:

- Click on **Assurance** > Event Log

## Event log

Client:

Any

Before:

04/18/2025

06:15

(PDT)

Event type include:

All

Event type ignore:

None

Search

[Reset filters](#)

Under **Event Type Include**, choose Non-Meraki VPN Healthcheck

# Event log

Client:

Any

Before:

04/18/2025

06:15

(PDT)

Event type include:

All

Event type ignore:

None

Search

[Reset filters](#)



Client:

Any

Before:

04/18/2025

06:15

(PDT)

Event type include:

Non-Meraki VPN Healthcheck x

Event type ignore:

None

Search

[Reset filters](#)

When the primary tunnel to Cisco Secure Access is active, packets arriving through the secondary tunnel are dropped to maintain a consistent routing path.

The secondary tunnel remains in standby and is only used if a failure occurs on the primary tunnel, either from the Meraki side or within Secure Access, as determined by the health check mechanism.

## Event log

Client:

Any

Before:

04/18/2025

06:15

(PDT)

Event type include:

Non-Meraki VPN Healthcheck x

Event type ignore:

None

Search

[Reset filters](#)

Download as

[« newer](#) [older »](#)

Time (PDT) ▾	Client	Category	Event type	Details
Apr 15 22:16:30	Non-Meraki VPN	Non-Meraki VPN	Non-Meraki VPN Healthcheck	group: 1, peer: 711568741124546470, peer_name: SSE-MERAKI Primary Secondary, status: down
Apr 15 22:16:22	Non-Meraki VPN	Non-Meraki VPN	Non-Meraki VPN Healthcheck	group: 1, peer: 711568741124546440, peer_name: SSE-MERAKI Primary, status: up
2 total				

- The Primary tunnel health check shows status: up, meaning it is currently passing and actively forwarding traffic.
- The Secondary tunnel health check shows status: down, not because the tunnel is unavailable, but because the primary is healthy and actively in use. This behavior is expected, as traffic is only permitted to pass through Tunnel 1, causing the secondary tunnel's health check to fail.

## Related Information

- [Cisco Technical Support & Downloads](#)
- [Cisco Secure Access Help Center](#)
- [Cisco Secure Access Meraki BGP Configuration Guide](#)