

A decorative pattern of concentric hexagons in a light blue color, scattered across the top dark blue header area.

FortiNAC - Cisco Meraki Wired Integration

Version 9.4.x

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

February 15, 2024

FortiNAC 9.4.x Cisco Meraki Wired Integration

49-922-769106-20211216

TABLE OF CONTENTS

	4
Overview	5
What it Does	5
Meraki MS Switch	6
How it Works	6
Requirements	6
Considerations	7
Visibility	8
Configure MS Switch	8
Configure FortiNAC	8
Validate Visibility	9
Control	9
Configure MS Switch	9
Configure FortiNAC (Proxy RADIUS)	10
Configure FortiNAC (Local RADIUS)	11
Create Enforcement Groups	14
Review Enforcement Checklist	15
Enable Enforcement	15
Validate Control	16
Meraki MX Router	17
How it Works	17
Requirements	17
Visibility	17
Configure MX Router	18
Configure FortiNAC	18
Validate Visibility	19
Troubleshooting	20
Related KB Articles	20
Debugging	20
Log Message Examples	21
Other Tools	21
Appendix	22
HTTP Status Code 429	22
Meraki API Call Limits	22

Overview

This document provides guidance with the required configurations necessary for FortiNAC management with Cisco Meraki devices. For additional assistance in device configuration, refer to product documentation or contact vendor for additional support.

Most devices are modeled using the same procedure, however, there are some exceptions. Special instructions for those vendors are included in the following sections.

What it Does

Meraki MS Switch

FortiNAC provides network visibility (where endpoints connect) and manages network access for hosts connecting to the Meraki MS.

Meraki MX Router

FortiNAC provides IP address (L3) information regarding connecting endpoints by retrieving ARP information from the Meraki MX. **Note:** FortiNAC only collects ARP information and *does not* manage network access for connecting endpoints. This applies to all MX models.

Click on the desired link to proceed:

[Meraki MS Switch](#)

[Meraki MX Router](#)

Meraki MS Switch

How it Works

Registered host network access is provisioned through VLAN assignment based on FortiNAC Network Access Policies. Unregistered (rogue) host network access is provisioned based upon the Access Values configured within FortiNAC's device model for the Meraki MS. Meraki integration with FortiNAC is designed around RADIUS authentication and disconnection. This requires the creation of at least one Access Policy within the switch in order to define the RADIUS settings that will apply to connecting hosts. Access policies must then be applied to every port that FortiNAC is intended to manage.

When a host connects to the Meraki switch, a RADIUS Access Request is sent to FortiNAC. A RADIUS response is returned with the appropriate VLAN based upon the matching Network Access Policy or Model Configuration Access Value. When FortiNAC needs to change a host's network posture, it disconnects the client using RADIUS (RFC 5176) causing a new authentication in which a new VLAN is assigned.

Device Support Methods

	Endpoint Connectivity Notification	Reading MAC Address Tables (L2 Poll)	Reading IP Tables (L3 Poll)	Reading VLANs/Resync Interfaces	Switching VLANs	De-auth
MS Switch	RADIUS (802.1x or MAC-auth)	SNMP	REST API*	API*	RADIUS	RADIUS Disconnect (CoA)

* FortiNAC makes API requests to the cloud (<https://dashboard.meraki.com/>) and not to the switch directly. A tcpdump using the switch IP Address alone will not show these API requests.

Requirements

FortiNAC

- Supported Engine Version: 8.3 and greater
- Recommended Engine Version:
 - Meraki API v1 support: 9.2 and greater <https://community.meraki.com/t5/Developers-APIs/Dashboard-API-v0-End-of-Support-Sunset-and-Grace-Period/m-p/138696>
 - Stacked Meraki switch support: 9.4.5 and greater
- FortiNAC has internet access to <https://dashboard.meraki.com/>.

Meraki MS

- Supported Firmware Version: Meraki firmware that supports RADIUS CoA.
- SNMP community or account (Read/write access)
- Account for API access
 - Visibility only: System read access
 - Control: System read/write access

RADIUS Server (802.1x Proxy Mode Configurations)

- The encryption method for user names and passwords passed between FortiNAC and the RADIUS server must be set to PAP. This affects the following accounts or user names and passwords created on the RADIUS server:
 - The validation account created for communication with FortiNAC and entered in the RADIUS Server Profile configuration.
 - Network users that access the network via the captive portal and are authenticated through RADIUS.

Network

- Do not use asymmetric routing between your device and the FortiNAC server. RADIUS requests and responses between the FortiNAC server and the wireless device must travel through the same interface on the FortiNAC server.
- **Important:** FortiNAC's capacity for processing RADIUS requests is approximately 60 requests per second. Capacity is affected by the use of other features in the program such as the Persistent Agent or MAC Notification Traps. Any requests that are not immediately processed are placed in queue. After 5 seconds any unprocessed requests are discarded.

If FortiNAC is going to be installed in an environment where it is expected to receive more than 60 RADIUS requests per second, an additional FortiNAC appliance may be required to handle the load.

Considerations

- Dynamically assigning tagged Voice VLANs for IP Phones (optional): Specific Cisco-AVPair attribute is required to be returned by the RADIUS server. For details see **Multi-Domain** under **Host Modes** in the following article:
[https://documentation.meraki.com/MS/Access_Control/MS_Switch_Access_Policies_\(802.1X\)](https://documentation.meraki.com/MS/Access_Control/MS_Switch_Access_Policies_(802.1X))
 - MAB Authentication: Meraki Device Model must be set for Local Radius mode in order to provide the Cisco-AVPair attribute. Proxy mode is not supported.
 - 802.1x authentication:
 - Either Local RADIUS or Proxy mode is supported.
 - If Proxy mode, the backend RADIUS server must be configured to provide the Cisco-AVPair attribute.
- FortiNAC must L3 poll each Meraki switch if there is no Meraki MX router modeled. Otherwise, FortiNAC will have an incomplete listing of IP to MAC address information.

Visibility

Configure MS Switch

SNMP

Configure SNMP access to allow for FortiNAC device discovery.

Version 1/2c:

Under **Network-wide > General > Reporting** set SNMP access and SNMP user credentials.

Version 3

1. Under **Network-wide > General > Reporting** set SNMP access and SNMP user credentials.
2. Under **Organization > Settings** set version, authentication mode and privacy mode.

API Key

Obtain the API Key (this will be used in the FortiNAC Model Configuration). Once generated, the same API Key can be used in multiple devices. If the API key has not already been generated, do the following:

1. Navigate to **Organization > Settings**
2. Under **Dashboard API access**, select **Enable access to the Cisco Meraki Dashboard API**
3. Click **Profile** link
4. Under **API Access**, click **Generate new API key**
5. Copy the generated key and save to a file

Client Tracking

FortiNAC requires the "MAC Address" Client tracking option in order to collect L2/L3 data.

1. Navigate to **Security & SD-WAN > Configure > Addressing & VLANS**.
2. Under **Client tracking**, select **MAC Address (Default)**.

Configure FortiNAC

1. In the FortiNAC Administration UI, navigate to **Network > Inventory** and discover or add the Meraki switch. Use the SNMP values previously configured on the Meraki switch. For instructions see [Add or modify a device](#) or [Discovery](#) (for multiple devices) in the Administration Guide.

Note: If a "?" appears as the icon, then support needs to be added for that device. See KB article [198477](#) to add the device using an existing model.

2. Select the newly added model and click the **Credentials** tab.
3. Enter the following under **CLI Settings** and **Save**:

Username: <should display the Serial Number>

Password: REST API Key

4. If no MX router is being polled by FortiNAC, ensure each Switch has L3 polling enabled:
 - a. Right click on the model and select **Group Membership**.
 - b. Select the box next to **L3 (IP à MAC)** and click **OK**.
 - c. Click the **Polling** tab.
 - d. Select the box next to **L3 (IP à MAC)** Polling and set the interval to 30 minutes.
 - e. Click Poll Now. Verify the timestamps for Last Successful Poll and Last Attempted Poll update to the current time.

Validate Visibility

1. Click on the **Ports** tab of the switch.
2. Review the values populated for each port (Label, Connection State, etc) and verify they are accurate.
Note: Current VLAN values may not be accurate for switches authenticating using RADIUS (such as Meraki). At this time, the port view only allows for a single port-based VLAN to be displayed for the Current VLAN. This VLAN usually does not match the dynamic VLAN assigned to the clients that have authenticated using RADIUS.
3. If the **Adapter** tab is not already visible, click the **Show Details Panel** button at the bottom of the window.
4. Verify connection information for hosts currently connected is accurate by clicking on one of the ports showing a connection. The adapter tab below should reflect the correct Adapter Status, Host Status, IP Address, Physical (MAC) Address, Location and Access Value.

If unexpected results occur, see [Troubleshooting](#).

Control

Configure MS Switch

Enable full control of network connections to enforce compliance and provision network access.

Reference article

https://documentation.meraki.com/MS/Access_Control/Configuring_Microsoft_NPS_for_MAC-Based_RADIUS_-_MS_Switches

1. Navigate to **Switch > Configure > Access Policies**
2. Configure an Access Policy. The values in the table below are required when integrating with FortiNAC. Configure all other settings (Host Mode, Access Policy Type, etc) as appropriate.

Authentication Method	my RADIUS server
Host	FortiNAC eth0 IP Address

	High Availability (HA) Environments: Add both Primary and Secondary Servers. Do not use Shared IP Address.
Port	Proxy RADIUS Mode: 1812 Local RADIUS Mode: Value defined in Local RADIUS Server configuration in FortiNAC
Secret	Secret must match the secret entered in the FortiNAC device model
RADIUS Testing	Disabled
RADIUS CoA Support	RADIUS CoA enabled
RADIUS Accounting Servers	RADIUS Accounting enabled
Host	FortiNAC eth0 IP Address High Availability (HA) Environments: Add both Primary and Secondary Servers. Do not use Shared IP Address.
Port	1813
Secret	Secret must match the secret entered in the FortiNAC device model
Ensure "Increase access speed"	Unchecked

3. Assign ports to the Access Policy. **Important:** An Access Policy must be applied to every port that FortiNAC is intended to manage.
 - a. Navigate to **Switch > Monitor > Switch Ports**.
 - b. Select the port(s) to which the access policy will be applied and press the **Edit** button.
 - c. Convert the port type from trunk to **access**. **Note:** Access Policies can only apply to access ports.
4. From the **Access Policy** drop-down box, select the Access Policy and press the **Update ports** button.

Proceed to the applicable section:

[Configure FortiNAC \(Proxy RADIUS\)](#) - FortiNAC proxies 802.1x RADIUS requests to a 3rd party RADIUS server

[Configure FortiNAC Local RADIUS](#) - FortiNAC processes all RADIUS requests

Configure FortiNAC (Proxy RADIUS)

1. In the FortiNAC Administration UI, add a RADIUS server (such as FortiAuthenticator) to FortiNAC in order to proxy the 802.1x packets to the correct server.
See [Configure RADIUS Settings](#) in the Administration Guide for instructions.
Important: The RADIUS Secret used must be exactly the same on the RADIUS server.

RADIUS

RADIUS Servers - Total: 1

Profile Name	Host Name/IP	Authentication Port	Accounting Port	User Name	Last Modified By	Last Modified Date
fortiauthenticator	10.10.10.30	1812	1813	carl	root	02/21/19 09:42 AM GMT+0100

Add Modify Delete

RADIUS Server Defaults

Default for Primary RADIUS Server: fortiauthenticator

Default for Secondary RADIUS Server: None

RADIUS Domain Mappings - Total: 1

Domain Name	RADIUS Server
fortiad.info	fortiauthenticator

2. Create Network Access Policies to assign VLANs for connecting registered hosts. For instructions, see section [Network access policies](#) in the Administration Guide.
- Important:** All VLAN assignments for registered hosts require a Network Access Policy.
3. Navigate to **Network > Inventory**.
 4. Select the new Device Model and click the **Model Configuration** tab.
 5. Click **Enable RADIUS authentication for this device** and click **Proxy**.
 6. Configure the appropriate VLAN ID for each Logical Network as they apply (Registration, Quarantine, Dead End, Authentication, etc).
 7. Click **Save**.

Proceed to [Create Enforcement Groups](#).

Configure FortiNAC (Local RADIUS)

1. Configure and enable Local RADIUS Services. Refer to the [Local RADIUS Server](#) reference manual for instructions.
2. Create Network Access Policies to provision VLANs. For instructions see [Network access policies](#) in the Administration Guide.

Important: All VLAN assignments for registered hosts require a Network Access Policy.

Dynamically Provision Voice VLAN for IP Phones (optional)

- **User/Host Profile** – Match criteria unique to the IP Phones. The simplest matching criteria to use is **Device Type = IP Phone**. Other criteria can be used as desired. For details on registering IP Phones, refer to the [IP Phone Integration](#) reference manual in the Document Library.
- **Logical Network** for the Voice VLAN. For instructions see [Configure Logical Networks](#).

Logical Networks - Total: 9	
<< first < prev 1 next > last >> 250 ▾	
Name	Description
Engineering	
Corporate	
BYOD	
Guest	
Printer	
Camera	
UPS	
IP-Phones	
AlexsCLIDeviceNetworkF	

- **Network Access Configuration** to assign the data VLAN's logical network. For instructions see [Network Access Configurations](#).

3. Navigate to **Network > Inventory**.
4. Select the new Device Model and click the **Model Configuration** tab.
5. Click **Enable RADIUS authentication for this device** and click **Local**.
6. Configure the appropriate VLAN ID and RADIUS Attribute Group for each Logical Network as they apply (Registration, Quarantine, Dead End, Authentication, etc).

Isolation/Data VLANs

- **Access Value** = Data VLAN ID
- **RADIUS Attribute Group**: RFC_Vlan



Note: **Use Default** can be used if the **Default Attribute Group** = RFC_Vlan

☒ Enable RADIUS authentication for this device












RADIUS

Mode: ☒ Local ☐ Proxy

Server Configuration: DefaultConfig ▾

Default Attribute Group: RFC_Vlan ▾  


Shared Secret: *****

Logical Network	Access	Is Alias	Additional RADIUS Attribute Group
Registration	98		Use Default ▾ 
Quarantine	97		Use Default ▾ 
Dead End	96		Use Default ▾ 
Authentication			Use Default ▾ 
BYOD	1728	<input type="checkbox"/>	Use Default ▾ 
Camera		<input type="checkbox"/>	Use Default ▾ 
Corporate		<input type="checkbox"/>	Use Default ▾ 
Engineering	1722	<input type="checkbox"/>	Use Default ▾ 
Guest	1723	<input type="checkbox"/>	Use Default ▾ 
IP-Phones	1728	<input type="checkbox"/>	RFC_Vlan-phone ▾  

Tagged Voice VLAN (optional)

Configure the following for FortiNAC to dynamically assign the tagged Voice VLAN.

- **Access Value** = <Voice VLAN ID >
- Create a custom RADIUS Attribute Group

7. Click the Add icon  next to the IP Phone Logical Network.
8. Enter the RADIUS Attribute Group name (Example: Vlan-Phone).

Add the attributes values using the chart below. Click **OK** to save.

Hint: Use the **Name** filter to locate the various attributes in the Available Attributes list.

Attribute Name	Response Value
Tunnel-Medium-Type	IEEE-802
Tunnel-Type	VLAN
Tunnel-Private-Group-Id	%ACCESS_VALUE%
Cisco-AVPair	device-traffic-class=voice

Add RADIUS Attribute Group

Name:

Filter

☐ Name:

Available Attributes

<< first < prev 1 next > last >> 250

Name	Vendor
Cisco-Abort-Cause	Cisco
Cisco-Account-Info	Cisco
Cisco-Assign-IP-Pool	Cisco
Cisco-AVPair	Cisco
Cisco-Call-Filter	Cisco
Cisco-Call-Type	Cisco
Cisco-Command-Code	Cisco
Cisco-Control-Info	Cisco
Cisco-Data-Filter	Cisco
Cisco-Data-Rate	Cisco
Cisco-DHCP-Relay-GiAddr	Cisco
Cisco-DHCP-Subscriber-Id	Cisco

Selected Attributes

Name	Response Values
Tunnel-Medium-Type	IEEE-802
Tunnel-Type	VLAN
Tunnel-Private-Group-Id	%ACCESS_VALUE%
Cisco-AVPair	device-traffic-class=voice

IP-Phones 1700 ☐

Proceed to [Create Enforcement Groups](#).

Create Enforcement Groups

Step 1: Determine the Required Groups

In order for FortiNAC to manage ports, they must be members of the appropriate enforcement group. There are several enforcement groups available. Review the table below to decide which groups will be required.

Enforcement Groups

Group	Definition
Forced Authentication (Port Group)	Ports that participate in forced authentication when unauthenticated users connect. If you have a port in this group, when a host connects to this port and is unauthenticated, the port is put into isolation VLAN and the host is forced to authenticate.
Forced Registration (Port Group)	Ports that participate in forced registration when unregistered hosts connect. Add switch ports that participate in forced registration when an Unregistered Host connects to the Forced Registration port group. Only ports that participate have their VLAN ID set to the Registration VLAN when an Unregistered Host connects.
Forced Remediation (Port Group)	Ports that participate in forced remediation VLAN switching when hosts connect.
Role-Based Access (Port Group)	Required in order to apply Network Access Policies. If port is not a member of this group, FortiNAC will not switch VLAN based upon a matching Network Access Policy.
Physical Address Filtering (Device Group)	Devices that participate in the enabling and disabling of hosts. Add switches that participate in host disabling to this group. If a host is connected to a switch that is not in the Physical Address Filtering group, and that host is disabled through FortiNAC, the host remains connected to the network and is displayed as in violation. Add the switch regardless of whether a host is disabled through a Dead End VLAN, or through MAC address security.

Step 2: Configure Groups for Enforcement

Port Groups: Configure port groups to which ports will be added to enable enforcement. Port Group configuration can be done in several ways. One approach is to create a group that will be a member of all desired enforcement groups. This simplifies the enforcement process, as the administrator only needs to add the port to one port group as opposed to multiple in order to enable enforcement. It is recommended to remain consistent with whichever method is decided upon for group organization.

Device Groups (for use with Physical Address Filtering): Device Group configuration can be done in several ways. One approach is to create location-based device groups to be members of the Physical Address

Filtering Group. It is recommended to remain consistent with whichever method is decided upon for group organization.

Note: Device groups are suggested for organizational purposes. It is possible to add a switch directly to the Physical Address Filtering group if desired.

Example

Requirements for devices connecting to Switch 1A in the Corp IT Department:

- Devices will register prior to being granted access to the network.
- Devices will be scanned for posture. If scan fails, device must remediate prior to accessing the network.
- Once registered, network access will be provisioned based upon matching a certain Network Access Policy.
- Ability to disable registered hosts and isolate them from the rest of the network.

Procedure

1. Navigate to **System > Groups**.
2. Create port group named "Switch 1A Ports".
3. Right click on "Switch 1A Ports" and select **Group Member Of**.
4. Select the check boxes for the desired enforcement groups and click **OK**:
 - Forced Registration
 - Forced Remediation
 - Role-Based Access
5. Create device group named "Corp IT Switches".
6. Right click on "Corp IT Switches" and select **Group Member Of**.
7. Select the check box for Physical Address Filtering and click **OK**.
8. For more information, see [Groups View](#) in the Administration Guide.

Review Enforcement Checklist

Before enabling enforcement, verify the following:

- The Current and Default VLANS are correct on each switch. (Current and Default should match, or there will be a VLAN switch when ports go live, unless a network access policy overrides the default)
- All uplinks are marked as uplinks in Topology
- There are little or no rogue MAC addresses on the switch(es).
Important: Rogue MAC addresses detected on enforced ports will be isolated.
- Isolation VLANS are working.
- Each switch model configuration has the appropriate isolation VLAN for all desired enforcement states.

Enable Enforcement

Add the desired ports/switches to the appropriate enforcement group.

Important: Always test behavior on a small number of ports prior to enforcing the entire switch.

Example

Enable enforcement on Switch 1A ports 1-5

1. Navigate to **System > Groups**.
2. Right click on group "Switch 1A Ports" and select **Modify**.
3. In the left column, expand Switch 1A to reveal ports.
4. Select ports 1-5 and click ">" to move to the **Selected Members** column.
5. Click **OK**.
6. Right click on group "Corp IT Switches" and select **Modify**.
7. In the left column, select Switch 1A and click ">" to move to the **Selected Members** column.
8. Click **OK**.

For more information, see [Groups View](#) in the Administration Guide.

Validate Control

1. Connect a rogue host to one of the newly enforced ports.
2. Verify the following:
 - Host is moved to the Isolation VLAN
 - Host is able to access the captive portal (if configured)
 - Register the system and make sure it gets moved to the appropriate VLAN.
 - Host is moved to the Dead End VLAN when disabled in Host view.

If unexpected results occur, see [Troubleshooting](#).

Meraki MX Router

How it Works

FortiNAC collects ARP information by reading the MX's session table using the REST API. The API request sent by FortiNAC includes the Serial Number and key.

Device Support Methods

	Endpoint Connectivity Notification	Reading MAC Address Tables (L2 Poll)	Reading IP Tables (L3 Poll)	Switching VLANs	De-auth
MX Router	N/A	N/A	REST API*	N/A	N/A

* FortiNAC makes API requests to the cloud (<https://dashboard.meraki.com/>) and not to the MX directly.

Requirements

FortiNAC

- Supported Engine Version: 8.3 and greater
- FortiNAC has internet access to <https://dashboard.meraki.com/>.

Meraki MX

- Supported Firmware Version: Any

SNMP community or account (Read only)

Visibility

Note: FortiNAC only collects IP to MAC information (L3 poll) from MX routers.

Configure MX Router

API Key

Obtain the API Key (this will be used in the FortiNAC Model Configuration). Once generated, the same API Key can be used in multiple devices. If the API key has not already been generated, do the following:

1. Navigate to **Organization > Settings**
2. Under **Dashboard API access**, select **Enable access to the Cisco Meraki Dashboard API**
3. Click **Profile** link
4. Under **API Access**, click **Create new API key**
5. Copy the generated key and save to a file

Serial Number

Obtain router Serial Number (this will be used in the FortiNAC Model Configuration).

1. Navigate to **Security Appliance > Appliance**
2. Copy the Serial Number and save to a file

SNMP

Configure SNMP access to allow for FortiNAC device discovery. Under the **Network-wide > General > Reporting** section, allow either v1/v2 or v3 access

Client Tracking

FortiNAC requires the “MAC Address” Client tracking option in order to collect L2/L3 data.

1. Navigate to **Security & SD-WAN > Configure > Addressing & VLANS**.
2. Under **Client tracking**, select **MAC Address (Default)**.

Configure FortiNAC

Model the Device

In the FortiNAC Administration UI, navigate to **Network > Inventory** and discover or add the Meraki switch. Use the SNMP values previously configured on the Meraki switch. For instructions see [Add or modify a device](#) or [Discovery](#) (for multiple devices) in the Administration Guide.

Note:

- The MX will not display ports. This is normal.
- If a “?” appears as the icon, then support needs to be added for that device. See KB article [198477](#) to add the device using an existing model.

Device Model Configuration

1. Select the newly added model and click the **Credentials** tab.
2. Fill in the following and **Save**:
 - User Name: <Serial Number >
 - Password: <REST API Key>
3. Right click on the model and select **Group Membership**.
4. Select the box next to **L3 (IP-->MAC)** and click **OK**.
5. Click the **Polling** tab.
6. Select the box next to **L3 (IPàMAC) Polling** and set the interval to 30 minutes.
7. Click **Poll Now**. Verify the timestamps for **Last Successful Poll** and **Last Attempted Poll** update to the current time.

Validate Visibility

Verify FortiNAC is properly reading the ARP cache of the Meraki MX.

1. In the FortiNAC Administration UI, navigate to **Users & Hosts > Adapters**.
2. In the right hand search field, enter an IP address for which the MX should have ARP cache entry. Alternatively, a wildcard can be used to search for a subnet (example: 192.168.5.*). For other search and filter options, see [Filters](#) in the Administration Guide.
3. Review the IP address values for the adapter(s) and verify they are accurate.
If unexpected results occur, see [Troubleshooting](#).

Troubleshooting

Related KB Articles

Refer to the applicable KB article(s):

[Troubleshooting SNMP Communication Issues](#)

[Troubleshooting Poll Failures](#)

[Wired hosts displaying incorrect status](#)

[Troubleshooting RADIUS clients not connecting](#)

[Troubleshooting VLANs Not Changing on a Wired Switch.](#)

[Troubleshooting Wireless Clients Moved to the Wrong VLAN](#)

Debugging

Use the following KB article to gather the appropriate logs using the debugs below.

[Gather logs for debugging and troubleshooting](#)

Note: Debugs disable automatically upon restart of FortiNAC control and management processes.

Function	Syntax	Log File
FortiNAC Server (Proxy RADIUS)	<code>nacdebug -name RadiusManager true</code>	<code>/bsc/logs/output.master</code>
FortiNAC Server (Local RADIUS)*	<code>nacdebug -name RadiusAccess true</code>	<code>/bsc/logs/output.master</code>
RADIUS Service (Local RADIUS)	<code>radiusd -X -l /var/log/radius/radius.log Stop logging: Ctrl-C</code>	<code>/var/log/radius/radius.log</code>
L2 related activity	<code>nacdebug -name BridgeManager true</code>	<code>/bsc/logs/output.master</code>
Meraki MX specific		<code>/bsc/logs/output.master</code>

Function	Syntax	Log File
	<code>nacdebug -name Meraki true</code>	
Meraki MS specific	<code>nacdebug -name merakiSwitch true</code>	<code>/bsc/logs/output.master</code>
SNMP activity	<code>nacdebug -name SnmpV1 true</code>	<code>/bsc/logs/output.master</code>
Disable debug	<code>nacdebug -name <debug name> false</code>	N/A

*Logging for a given MAC Address:

```
nacdebug -logger 'yams.RadiusAccess.RadiusAccessEngine.00:11:22:33:44:55' -level
FINEST
```

Disable:

```
nacdebug -logger 'yams.RadiusAccess.RadiusAccessEngine.00:11:22:33:44:55'
```

Log Message Examples

RADIUS response (Debug: RadiusManager)

Client MAC address = D0-67-E5-36-6F-D4

Meraki MS IP = 10.12.240.2

VLAN = Staff

```
yams.RadiusManager INFO :: 2019-04-03 08:29:12:998 :: RadiusPollThread0
RadiusServer accepting client D0-67-E5-36-6F-D4 for device 10.12.240.2 and policy Staff
ptime=0:0:13:13:13:17
```

Other Tools

Send a RADIUS Disconnect:

```
SendCoA -ip <devip> -mac <clientmac> -dis
```

Example:

```
SendCoA -ip 10.1.0.25 -mac 00:1B:77:11:CE:2F -dis
```

Packet capture for Local RADIUS traffic:

```
tcpdump -nni any -v port 1645 or 1700 or 3799
```

Appendix

HTTP Status Code 429

HTTP status code 429 can be returned if the API call limit is exceeded. Reference article

<https://community.meraki.com/t5/Developers-APIs/Inquire-about-HTTP-status-code-429/m-p/111071>

Meraki API Call Limits

Meraki dashboard.meraki.com only allows 10 simultaneous connections for one organization.



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.