FortiNAC

Cisco Meraki Integration
MR Access Points

Version: 8.3, 8.5, 8.6, 8.7. 8.8

Date: November 4, 2021

Rev: I

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

Contents

Overview

The information in this document provides guidance for configuring the Meraki device to be managed by FortiNAC. This document details the items that must be configured.

Note: We attempt to provide as much information as possible about the integration of this device with your FortiNAC software. However, your hardware vendor may have made modifications to the device's firmware that invalidate portions of this document. If you are having problems configuring the device, contact the vendor for additional support.

How it Works

The integration of Cisco Meraki Devices (MR, MS and MX) and FortiNAC is designed around RADIUS authentication and disconnection. As devices connect to the wireless Meraki network, they are assigned their network posture through Meraki Group Policies. Meraki Group Policies can be created to use VLANs or firewall rules or both (based on how the administrator wishes to isolate their hosts on their network). When FortiNAC needs to change a host's network posture, it disconnects the client using RADIUS (RFC 5176) over port 1700. This causes a new authentication in which a new Group Policy is assigned.

Considerations

- FortiNAC is unable to read live sessions from Meraki APs. Therefore, when FortiNAC starts up, it will not see any non-managed sessions that may have started or stopped while FortiNAC was not running. FortiNAC will learn of new session status as it learns of them through live messages. The L2 polling function is not applicable.
- Syslog messages are not generated for connections terminated when SSID's are disabled in the Meraki. Associated adapter records will continue to show as "online" in FortiNAC and concurrent licenses will not be released.

MR Access Point Integration

Configure Access Point

Note: It is recommended that Meraki APs are configured with a static IP address.

1. Configure SSIDs
   a. Navigate to **Wireless > Access Control**
   b. Configure the SSIDs to be managed by FortiNAC. The values in the table below are required when integrating with FortiNAC. Configure all other settings as appropriate. Refer to vendor documentation for additional information.

Association Requirements	MAC-based access control (no encryption) WPA2-Enterprise with my RADIUS server
Splash page	Setting depends upon the FortiNAC RADIUS Mode used. For details see Local RADIUS Server in the Administration Guide. Proxy Mode: Select **None** Local Mode (FortiNAC version 8.8.0 and greater) • 802.1x Authentication: Select **None** • MAC Authentication: Select **Cisco Identity Services Engine (ISE) Authenticator** Includes the Service-Type Call-Check attribute required by the Local RADIUS Server to process MAC Authentication Access Requests.
RADIUS Servers	Host: FortiNAC Server/Control Server eth0 IP Address Port: 1812 High Availability (HA) Environments: Add both Primary and Secondary Servers. Do not use Shared IP Address.
RADIUS Testing	Disabled
RADIUS CoA support	Enabled
RADIUS attribute specifying group policy name	Filter-Id

Client IP assignment	Bridge mode: Make clients part of the LAN
RADIUS override	RADIUS response can override VLAN tag

2. Configure a Group Policy for each VLAN.
    a. Navigate to **Network-Wide > Group Policies**
    b. To add a group policy, click **Add a group**
    c. For **VLAN**, select **Tag VLAN** from drop-down and specify the VLAN ID
    d. Save Changes

3. Configure Meraki to send Syslog messages to FortiNAC. Syslog messages notify FortiNAC of wireless clients disconnecting.
    a. Navigate to **Network-wide > General**
    b. Under the **Logging** section click **Add a syslog server**
    c. Configure using the table below

Server IP	FortiNAC Server/Control Server eth0 IP Address
Port	514
Roles	• Wireless event log • Flows (may be necessary if FortiNAC does not obtain the IP address of wireless sessions efficiently from other L3 devices)

High Availability (HA) Environments: Add both Primary and Secondary Servers as syslog servers. Do not use Shared IP Address.

4. Configure SNMP access to allow for FortiNAC device discovery. Under the **SNMP** section, allow either v1/v2 or v3 access.

Note:

- RADIUS accounting is not utilized for Meraki APs
- Syslog messages are not generated for connections terminated when SSID's are disabled in the Meraki. Associated adapter records will continue to show as "online" in FortiNAC and concurrent licenses will not be released.
- Other options can be set as desired, though any settings that may interfere with the features stated above might have an impact on the integration

Configure FortiNAC

1. In the FortiNAC Administration UI, navigate to **Network Devices > Topology.**
2. Discover or add the Meraki APs using the SNMP values previously configured on the Meraki APs. For instructions, see section **Add or modify a device** of the **Administration Guide** in the Fortinet Document Library.
3. Under the **RADIUS** section, configure the secret
4. Under the **Additional Access Values** section, add all the Group Policy names that were configured on the Meraki AP for all SSIDs controlled by FortiNAC. This is required since Group Policies cannot be read directly from the Meraki APs.
5. Click **Save**.
6. In the left panel, right click on the model and select **Resync Interfaces.** The groups should now populate under the **Ports** tab.
7. Under **Model Configuration**, configure the following
    - RADIUS secret (must be identical to the secret configured in the AP and RADIUS Server).
    - RADIUS server definitions if FortiNAC is managing any 802.1x SSIDs.
    - Network Access:
        - Set the Access Enforcement for each host state appropriately.
        - For the corresponding Access Value, enter the applicable Group Policy name.
8. Click **Save**.

Troubleshooting

Related KB Articles

Refer to the applicable KB article(s):
Troubleshooting SNMP Communication Issues
Troubleshooting Poll Failures
Online wireless hosts displaying offline status
Rogue Wireless Clients Cannot Connect to SSID
Troubleshooting RADIUS clients not connecting
Troubleshooting Wireless Clients Moved to the Wrong VLAN

Debugging

FortiNAC Commands

For instructions on enabling debugs and gathering logs see related KB article FD50687.

Send a RADIUS Disconnect:
```
SendCoA -ip <devip> -mac <clientmac> -dis
```

RADIUS activity (prints to /bsc/logs/output.master):
```
CampusMgrDebug -name RadiusManager true
```

L2 related activity (prints to /bsc/logs/output.master):
```
CampusMgrDebug -name BridgeManager true
```

Vendor specific debug (prints to /bsc/logs/output.master):
```
CampusMgrDebug -name Meraki true
```

Disable debugging feature
```
CampusManagerDebug -name <value> false
```

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

Appendix

Supplemental Documentation

Configure Clients for 802.1X and Meraki Authentication
The following article outlines the necessary steps to associate a Windows or MacOSX client to an SSID using 802.1X with Meraki-hosted RADIUS:
https://documentation.meraki.com/MR/Encryption_and_Authentication/Configuring_Clients_for_802.1X_and_Meraki_Authentication