FortiNAC

HP MSM 7XX Wireless Controller

(HP Mobility)

Version: .x

Date: 8/29/2018

Rev: B

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

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM

http://www.fortinet.com/support-and-trainingt/training.html

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

FORTINET

Wednesday, August 29, 2018

Contents

Overview

The information in this document provides guidance for configuring the wireless device to be managed by FortiNAC. The order of the topics presented in the Device Configuration section of this document does not represent the order in which the configuration must be done. Due to firmware upgrades, the configuration order is subject to change. Therefore, this document simply details the items that must be configured. It is recommended that you also read the ***Wireless Integration Overview*** document available in the Fortinet online Resource Center or in your online help.

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.

Requirements

To integrate the HP MSM 7XX wireless controller with your Administrative software, you must meet the requirements listed in this table.

Component	Requirement
Device Firmware	MSM firmware version 5.4.0.0-01-8027
FortiNAC Software	Version: 8.1 or higher **Note:** In many cases previous versions of FortiNAC can be used, however, instructions are written based on the version noted here.

If you are running your HP MSM Controller in a Teaming environment, refer to Teaming on page 11 for additional information.

Configuration

To integrate your device with your FortiNAC software, there are configuration requirements on both the device and FortiNAC. It is recommended that you configure the device first.

Note: Use only letters, numbers and hyphens (-) when creating names for items in the device configuration. Other characters may prevent FortiNAC from reading the device configuration.

Network devices should have static IP addresses (or dynamic IP addresses that are reserved). Once a device that provides network services had been identified in FortiNAC there is no mechanism to automatically update the IP address for that device if there is a change. If the IP address on the device itself is changed, the device appears in FortiNAC to be offline or to have a communication error.

HP MSM Device Configuration

Before integrating a device with FortiNAC set the device up on your network and ensure that it is working correctly. Take into account the VLANs you will need for Production and Isolation. Confirm that hosts can connect to the device and access the network. When the device is running on your network, then begin the integration process with FortiNAC.

FortiNAC supports individual SSID configuration and management for this device. Refer to the ***Wireless Integration Overview*** document available in the Fortinet online Resource Center or in your online help for additional information.

Use a browser to log into the HP MSM controller. Make sure the following items are configured.

Note: When configuring security strings on network devices or names for items within the configuration, it is recommended that you use only letters, numbers and hyphens (-). Other characters may prevent FortiNAC from communicating with the device, such as #. Some device manufacturers prohibit the use of special characters.

RADIUS Server

Define the FortiNAC Server or FortiNAC Control Server as the RADIUS server for the devices you want to manage with FortiNAC. Use the management IP Address of your FortiNAC Server as the IP of the RADIUS Server. The FortiNAC software is pre-configured to use port 1812 for authentication.

If you are setting up FortiNAC as the RADIUS server for a device in a Fortinet High Availability environment, you must use the actual IP address of the primary control server, not the Shared IP address. Set up the secondary control server as a secondary RADIUS server using its actual IP address. Regardless of the environment, you may also want to set up your actual RADIUS server to be used in the event that none of your FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.

Important: The RADIUS Secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration.

Important: If you are operating in a Teaming environment, you must add the Team IP Address as the NAS ID for each RADIUS server. Failing to do so will cause FortiNAC to respond incorrectly to RADIUS requests from the team members. See Teaming on page 11 for additional information.

VLANs

Create the VLANs that correspond to the host states you wish to enforce. These connection states include default (production) and isolation states including: registration, quarantine, authentication, and dead-end (disabled). For each VLAN do the following:

- Create a **Network Profile** and assign it a **VLAN ID**
- Create the **VLAN** and associated it with a **Network Profile**.
- When creating the VLAN make sure to select **None** for the **Assign IP Address via** option.

VSC Profile (SSID)

A VSC Profile characterizes a wireless network on the HP MSM controller. You can create one or more VSC Profiles. VSC Profiles that do not have the FortiNAC server as their RADIUS server are not managed by FortiNAC. For those WLANs you wish to have FortiNAC manage, the following configuration values must be set.

- Assign an **SSID** name to the VSC Profile.
- Remove the check mark from the **Access Control** check box.
- Make sure the **Authentication** check box is checked.
- Make sure **Wireless Mobility** is unchecked.
- Make sure **Wireless Security Filters** is unchecked.
- Select an **Authentication** type and configure it as desired. For 802.1x configure **Wireless Protection** as desired.
- For the Authentication type, select **Remote** and specify the **RADIUS Server Profile** created earlier.

Authentication

Two forms of authentication are supported byFortiNAC: MAC Authentication and 802.1x. On the HP MSM controller the authentication method is configured with each VSC Profile along with other related parameters. It is possible to have multiple

VSC Profiles supported simultaneously, some using one method and others using another.

AP Groups

The wireless controller is designed to manage Wireless Access Points distributed across your network. On the controller you must create one or more groups of APs and associate a VSC Profile with each group. The VSC Profile controls the SSID that will be broadcast by the APs within the group. When your AP group or groups have been created and associated with a VSC Profile, make sure to synchronize the configuration.

Local Networks

To support mobility between Access Points, you must associate Network Profiles created earlier in this process with Access Points. You can associate Network Profiles with all APs, APs within a group or an individual AP.

SNMP

You must select an SNMP setting on the device to allow FortiNAC to discover and manage the device. Both SNMPv1 or SNMPv3 are supported. If you are not using SNMPv3, enable both SNMPv1 and SNMPv2C in the controller.

Default CLI Prompt Requirements

FortiNAC must be able to communicate effectively with the device in order to read the session table to determine which hosts are connected and to disassociate or disconnect a host when necessary. To accomplish these tasks FortiNAC uses the device's command line interface. FortiNAC expects to see prompts that end as follows:

Prompt Type	Characters Required
User Login	> Prompt must end with this character or FortiNAC will not be able to communicate with the device.
Enable	# Prompt must end with this character or FortiNAC will not be able to communicate with the device.

FortiNAC Software Configuration

For the FortiNAC software to recognize your device, you must add it to the Topology View either by prompting the FortiNAC software to discover the device or by adding it manually. Refer to the Help files contained within your FortiNAC software for instructions on Discovery or Adding a Device.

Regardless of how the device is added, the FortiNAC software must be able to communicate with it. To provide initial communication, you must indicate within the FortiNAC software whether to use SNMPv1 or SNMPv3 along with the appropriate SNMP access parameters.

FortiNAC Software Device Model Configuration

To manage a device, the FortiNAC software must have a model of the device in its database. First create or discover the device in the FortiNAC software. Once the device has been identified by FortiNAC, use the Model Configuration window to enter device information.

The Model Configuration window allows you to configure devices that are connected to your network so that they can be monitored or managed. Data entered in this window is stored in the FortiNAC database and is used to allow interaction with the device.

Important: If you are managing controllers in a Teaming environment, only model the Team IP Address. Modeling individual team members causes FortiNAC to improperly handle de-authentication requests for hosts connected to those controllers. See Teaming on page 11 for additional information.

Table 1: HP MSM Model Configuration Field Definitions

Field	Definition
General	
User Name	The user name used to log on to the device for configuration. This is for CLI access.
Password	The password required to configure the device. This is for CLI access.
Protocol Type	
Telnet **SSH2**	Use either Telnet or SSHv2 if it is available on your device.
RADIUS	
Primary Server	The RADIUS server used for authenticating users connecting to the network through this device. Select the Use Default option from the drop-down list to use the server indicated in parentheses. Used only for 802.1x authentication. See RADIUS Settings in the Help system for information on configuring your RADIUS Servers.

Field	Definition
Secondary Server	If the Primary RADIUS server fails to respond, this RADIUS server is used for authenticating users connecting to the network until the Primary RADIUS Server responds. Select the Use Default option from the drop-down list to use the server indicated in parentheses. Used only for 802.1 authentication.
RADIUS Secret	The Secret used for RADIUS authentication. Click the Modify button to change the RADIUS secret. Used for both 802.1x and Mac authentication. **Important:** The RADIUS Secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration.
Network Access - Host State	
Read VLANs From Device	Retrieves VLANs that currently exist on the device being configured.
Default	The Default VLAN value is stored in the database and is used when the VLAN is not determined by another method, such as user, host or device role. Typically, if a VLAN is specified as the Default, it is the VLAN used for "normal" or "production" network access.
Registration	The registration VLAN for this device. Isolates unregistered hosts from the production network during host registration.
Authentication	The authentication VLAN for this device. Isolates registered hosts from the Production network during user authentication. Optional.
Dead End	The dead end VLAN for this device. Isolates disabled hosts by providing limited or no network connectivity.
Quarantine	The quarantine VLAN for this device. Isolates hosts from the production network who pose a security risk because they failed a policy scan.
Network Access - Access Parameters	
Access Enforcement	This set of drop-down menus works in conjunction with the Host States listed above to determine treatment for hosts when no VLAN/Role value is supplied or when access control is being enforced. Options include: **Deny** — Host will be denied access to the network when the host is in this state. For example, if the host is not registered and Registration is set to Deny, the host connection will be rejected. Note: Endpoints that have been denied access may continuously request access which can unnecessarily consume system resources. **Bypass** — Host will be allowed access to the network when it the host is in this state. The host will be placed on the default VLAN/Role configured on the device for this port or SSID. For example, if Quarantine is set to Bypass, hosts that fail a scan and would normally be placed in Quarantine are placed in the default VLAN/Role on the device. **Enforce** — Indicates that the host will be placed in the VLAN/Role specified in the Access Value column for this state.

Field	Definition
Access Value	VLAN/Role where a host in this state should be placed when it connects to the network. If Enforce is selected in the Access Enforcement field you must enter a value in the Access Value field.
Wireless AP Parameters	
Preferred Container Name	If this device is connected to any Wireless Access Points, they are included in the Topology View. Enter the name of the Container in which these Wireless Access Points should be stored. Containers are created in the Topology View to group devices.

Setup The Model Configuration

Important: The RADIUS Secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration.

Note: Because you are using 802.1x authentication, make sure you have a RADIUS Server configured. Select Network Devices > RADIUS Settings. See Configuring RADIUS Server Profiles in the Help system for additional information on adding a RADIUS Server.

1. After you have discovered or added the device in the Topology View, navigate to the Model Configuration window. Right-click on the device, select the device name, and then click **Model Configuration**.
2. Enter the **User Name** used for CLI access on this device.
3. Enter the **Password** used for CLI access on this device.
4. If you are using MAC authentication, only the RADIUS Secret is required. If you are using 802.1x authentication, either the default RADIUS server or a pre-configured RADIUS server must be selected. RADIUS servers are configured on the RADIUS Settings window.
5. Enter the **RADIUS Secret**. This must match the value entered on the device itself and the value entered on the RADIUS settings window.
6. In the **Protocol** section select either Telnet or SSHv2 if it is available on your device model.
7. In the Network Access section, click **Read VLANs** to retrieve the Current Device Interface settings. This creates the interface models.
8. Select a setting in **Access Enforcement** for each host state.
9. In the **Access Value** column select a **Role** or a **VLAN** for each host state that you wish to enforce.
10. In the **Preferred Container** field, select the **Container** in which the Wireless Access Points should be placed as they are discovered.
11. Click **Apply**.

Discover Access Points

Access Points connected to the controller must be added to FortiNAC to allow FortiNAC to see and manage connected hosts. Refer to the Wireless Integration section of the FortiNAC online help or locate the PDF version of that document in the Fortinet online Resource Center.

Teaming

If you are running controllers in a Teaming environment and you are using FortiNAC to manage both your wireless and wired networks, there are some additional configuration considerations. If FortiNAC is managing the wired network a controller connected to a wired port will be treated like a host and could be placed in isolation. To prevent this from happening you add the controller to FortiNAC as a pingable device and set the port where the controller is connected to uplink.

Add Controller As A Pingable

1. Click **Network Devices> Topology**.
2. Select the **Container** icon.
3. Right-click a container and select **Add Pingable Device**.
4. Enter the **Device Name**, **IP Address**, and **Physical Address**. Physical address is required when you have identified a Rogue host as a device and wish to move it from the Host View to the Topology View. Typically physical address is read from the device.
5. Set the **Device Type** to Pingable.
6. The **Palo Alto User Agent** check box is specifically for integrating with a Palo Alto firewall device. Leave this check box blank.
7. Set **Deep Packet Device** type to pingable.
8. Click **OK**.

Set Port To Uplink

1. In FortiNAC select **Network Devices > Topology**.
2. Expand the Contaner where the device is located.
3. Select a device.
4. In the Port View in the right panel, right-click on the port where the controller is connected and select **Port Properties**. The Port Properties window displays.
5. Set the **Uplink Mode** for the port to **Always Uplink**.
6. Click **OK** to save.

Device Groups

To detect which hosts have disconnected from the wireless device, you must set up a frequent polling interval for your wireless devices. Devices are automatically added to the appropriate system group as they are added to the system. The default polling interval is 10 minutes. Devices are added automatically to the L2 Polling group, which polls for connected MAC addresses. You can set polling intervals on an individual device by going to the Device Properties window for that device.

Troubleshooting

If you are having problems communicating with the device, review the following:

SNMP

If the SNMP parameters set are not the same on both the device and the device configuration in your FortiNAC software, the two will not be able to communicate. You will not be able to discover or add the device.

Resynchronize VLANs

If you have modified the device configuration by adding or removing VLAN/Group definitions, it is recommended that you read Roles for that device again.

1. Select **Network Devices > Topology**.
2. Expand the **Container** that stores the device.
3. Select the device and right-click. From the menu select the device name, then select **Model Configuration**.
4. Click **Read Roles** or **Read VLANs**. This resynchronizes the FortiNAC software and the device configuration.

Teaming

If you are using your HP MSM controller in a teaming environment, there are additional considerations. In FortiNAC only the Virtual IP Address of the team is modeled under Model Configuration. On the MSM Team this Virtual IP Address represents the current Team Manager.

FortiNAC relies on RADIUS requests from a wireless device to determine that a host has connected and to take action on that host, such as placing it in a VLAN. Depending on the configuration of the Team Manager and the individual Team Members, FortiNAC receives RADIUS requests from one of two sources.

If the Team is configured to tunnel authentication through the controllers, RADIUS requests will contain a source IP address of the controller that sent the request, not the Virtual IP address of the team.

If the Team is configured for local drop-off, where the Access Points handle RADIUS, then the RADIUS request contains a source IP address of the AP that sent the request, not the Virtual IP address of the team.

FortiNAC needs the Virtual IP address of the team, and it is not sent as the source IP in the RADIUS request. Therefore, when FortiNAC receives a RADIUS request and the source IP does not match any devices modeled in FortiNAC, the NAS ID is checked. NAS ID will contain the Virtual IP address of the team. Using that IP address, FortiNAC can manage the host connection.

FortiNAC sends the RADIUS response to the source IP of the RADIUS request, so the response goes to the original device that issued the request, either the AP or the controller.

FortiNAC requires that the Virtual IP address of the Team Manager be used for the device that is modeled in the database in order to be able to disassociate a host. If team members were modeled, then FortiNAC would attempt to disassociate hosts from individual controllers which would fail.

To accommodate these RADIUS requirements the following must be configured:

HP MSM Controller Configuration

Set the NAS ID to be the Virtual IP address of the team.

- If RADIUS requests are sent from the controllers (tunneled), the NAS ID can be set in the RADIUS Profiles Configuration for the team.
- If RADIUS requests are set from the APs (local drop-off), the NAS ID can be set in the AP's RADIUS Profiles Configuration for the team.

FortiNAC Configuration

You must model the VIP of the Team Manager and create pingables for each of the controllers in the team.

Add Team Manager

Add the Team Manager as a device using the Virtual IP Address of the Team.

1. Click **Network Devices > Topology**.
2. Select the Domain icon.
3. Right-click a domain and select **Add Device**.
4. Enter the IP address of the device.
5. Select an SNMP protocol.
   - For SNMPv1 communication, enter the security string to use when communicating with the device.

   > **Note:** If the device has multiple security strings, enter only the Read/Write security string. This is the string that will ensure that FortiNAC has the ability to control the device.

   - For SNMPv3 communication enter the User Name, select the Authentication Protocol, and then enter the Authentication Password you used when you configured the device. For Snmpv3-AuthPriv, you must enter the Privacy Protocol and Privacy Password. These settings must match the corresponding settings on the device you are adding.
6. Click **Apply**.

Table 2: SNMPv3 Field Definitions

Field	Definition
User Name	User Name for access to the device. Recommended but not required.
Authentication Protocol	Available options are MD5 and SHA1.
Authentication Password	Enter the password you configured on the device.
Privacy Protocol	Available options are DES and AES. Used only for AuthPriv
Privacy Password	Enter the password you configured on the device. Used only for AuthPriv.

Add Controllers As Pingables

If you are running controllers in a Teaming environment and you are using FortiNAC to manage both your wireless and wired networks, there are some additional configuration considerations. If FortiNAC is managing the wired network, a controller connected to a wired port will be treated like a host and could be placed in isolation. To prevent this from happening you add the controller to FortiNAC as a pingable device and set the port where the controller is connected to uplink.

Add Pingable

1. Click **Network Devices > Topology**.
2. Select the **Domain** icon.
3. Right-click a domain and select **Add Pingable Device**.
4. Enter the **Device Name**, **IP Address**, and **Physical Address**. Physical address is required when you have identified a Rogue host as a device and wish to move it from the Host View to the Topology View. Typically physical address is read from the device.
5. Set the **Device Type** to Pingable.
6. The **Palo Alto User Agent** check box is specifically for integrating with a Palo Alto firewall device. Leave this check box blank.
7. Set **Deep Packet Device** type to pingable.
8. Click **Apply**.

Set Port To Uplink

1. In FortiNAC select **Network Devices > Topology**.
2. Expand the Domain where the device is located.
3. Select a device.
4. In the Device Summary view right-click on the port where the controller is connected and select **Port Properties**. The Port Properties window displays.
5. Click the **Port** tab in the Port Properties window.
6. Set the **Uplink Mode** for the port to **Always Uplink**.
7. Click **Apply** to save.