



FortiNAC

Trapeze

3 Com Wireless LAN Mobility System

Nortel WLAN Security Switch 2300

Series

Juniper Wireless Controllers

Integration

Version 8.x

Date: 8/30/2018

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-training/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>



Thursday, August 30, 2018

Contents

Overview	1
Requirements	1
Other Devices	1
Configuration	2
Trapeze Device Configuration	2
RADIUS Server	2
VLANs	3
SSIDs	3
Authentication	4
SNMP	4
Default CLI Prompt Requirements	4
FortiNAC Software Configuration	5
FortiNAC Software Device Model Configuration	5
Discover Access Points	8
VLAN Pooling	9
Device Groups	9
Troubleshooting	9
SNMP	9
Resynchronize VLANs	9
Trapeze Sample Configuration	10

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 Trapeze wireless controller with your Administrative software, you must meet the requirements listed in this table.

Component	Requirement
Device Firmware	Version 7.0 or higher. Also compatible with Version 6 but configuration may vary slightly.
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.

Other Devices

The wireless devices listed below are configured using the same instructions as the Trapeze device.

- 3 Com Wireless LAN Mobility System
- Nortel WLAN Security Switch 2300 Series
- Juniper Wireless Controllers

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.

Trapeze 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 Trapeze controller. Make sure the following items are configured.

Note: FortiNAC supports controllers in standalone or cluster mode. Configure each controller or SSID to be managed by FortiNAC as specified in this document.

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.

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). Create each VLAN with a name and a tag. It is the VLAN name that FortiNAC uses for dynamic assignment. For each VLAN enable the DHCP option that allows an IP to be automatically obtained and the Interface option.

Note: VLAN names should not exceed 15 characters. This wireless device allows VLAN names that are longer than 15 characters, but FortiNAC does not.

It is sometimes desirable to have the controller determine the appropriate production VLAN for healthy hosts. For example, when the production VLAN is dependent on a specific location, such as, building 1 uses VLAN 1 and building 2 uses VLAN 2. In this type of deployment, the default VLAN assignment for the device within FortiNAC can be left blank. To allow this behavior on the controller, make sure its SSID definition contains the instructions to fall through to the last-resort assignment. Use the following Trapeze CLI command:

```
set service-profile <ssid profile name> auth-fallthru last-resort
```

SSIDs

SSIDs characterize a wireless network on the Trapeze controller. You can create one or more SSIDs on the controller and you may choose to have FortiNAC manage any number of them. For each SSID you wish to have FortiNAC manage, the following configuration values must be set.

- Each SSID must have a unique profile name.
- Make sure the **Beacon** option is enabled.
- Set the **VLAN** option to **None**.
- Configure the settings for authentication for each SSID individually. Both MAC-Authentication and 802.1x are supported. If using 802.1x select the appropriate WPA/WEK settings.

Authentication

Two forms of authentication are supported by FortiNAC: MAC Authentication and 802.1x. On the Trapeze controller the authentication method is configured with each SSID, along with an encryption type, and other related parameters. It is possible to have multiple SSIDs supported simultaneously, some using one method and others using another. When configured in this way FortiNAC only allows a single VLAN mapping for each isolation state per device.

MAC Authentication

If you choose to use MAC Authentication, the FortiNAC Server or Control Server should be configured as the RADIUS server on your device. Use the primary interface IP address of the FortiNAC Server.

802.1x Authentication

802.1x is configured in much the same way, however, you must also configure the necessary EAP types and encryption settings for the SSIDs. See the section on 802.1x in the Wireless Integration Overview.

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.

Table 1: Trapeze 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.
Enable Password	The enable password for this 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.
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.

Field	Definition
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 a 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.
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	

Field	Definition
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. Enter the **Enable Password** used for CLI access on this device.

Note: Depending on how your device is configured, you may only need to enter User Name and Enable Password or User Name and Password. Typically you do not need to enter all three.

5. 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.
6. Enter the **RADIUS Secret**. This must match the value entered on the device itself and the value entered on the RADIUS settings window.
7. In the **Protocol** section select either Telnet or SSHv2 if it is available on your device model.
8. In the Network Access section, click **Read VLANs** to retrieve the Current Device Interface settings. This creates the interface models.
9. Select a setting in **Access Enforcement** for each host state.
10. In the **Access Value** column select a **Role** or a **VLAN** for each host state that you wish to enforce.
11. In the **Preferred Container** field, select the **Container** in which the Wireless Access Points should be placed as they are discovered.
12. 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.

VLAN Pooling

If you are using VLAN Pooling on the device, there is no option in the Model Configuration to assign a VLAN Pool to a particular Host State. Therefore, you must use a Network Access Policy and Network Access Configuration. Enter the name of the VLAN Pool in the Access Value/VLAN field on the Network Access Configuration. This allows you to assign a VLAN Pool based on the name of the pool for hosts that need access to the production network. This mechanism cannot be used for hosts that are in Isolation. For Isolation settings you must use a specific VLAN and set that on the Model Configuration. Refer to Network Access Policies in the Help system for instructions on setting up a policy and configuration.

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.

Trapeze Sample Configuration

This section contains a sample running configuration for this wireless device and the attributes you should consider when configuring it to communicate with the FortiNAC appliance. You can configure the device through its UI or the CLI.

Note: This information is provided only for the purposes of illustration. There is no guarantee that this configuration will work in your environment.

```
# Configuration nvgen'd at 2009-10-09 15:25:55
# Image 7.0.12.2.0
# Model MXR-2
# Last change occurred at 2009-10-09 15:25:47
set ip route default 192.168.5.1 1
set log console disable severity debug
set log session enable severity debug
set system name MXR-2-330BAC
set system ip-address 192.168.5.155
set auto-config enable
set system countrycode US
set timezone EST -5 0
set summertime EST-S start first sun apr 02 00 end last sun
oct 02 00
set service-profile trapeze-Mac ssid-name trapeze-Mac
set service-profile trapeze-Mac ssid-type clear
set service-profile trapeze-Mac cipher-tkip enable
set service-profile trapeze-Mac auth-dot1x disable
set radius server qa205 address 192.168.5.205 timeout 5
retransmit 3 deadtime 0 encrypted-key 08204e4d584b56
set server group webview-default members qa205
set enablepass password 5223ada243105fa35e66a61324d6ec746b44
set authentication console ** local
set authentication mac ssid trapeze-Mac * webview-default
set authentication dot1x ssid trapeze ** peap-mschapv2 local
set user admin password encrypted 020417585a545c
set user admin attr vlan-name default
set user admin attr service-type 6
set radio-profile default service-profile trapeze-Mac
```

```
set radio-profile webqs-rp
set ap 1 port 2 model MP-372
set ap 1 force-image-download enable
set ap 1 radio 1 mode enable
set ap 1 radio 2 mode enable
set ip telnet server enable
set ip snmp server enable
set port poe 2 enable
set snmp protocol v2c enable
set vlan 1 port 1
set vlan 35 name production
set vlan 35 port 1 tag 35
set vlan 85 name registration
set vlan 85 port 1 tag 85
set vlan 86 name authentication
set vlan 86 port 1 tag 86
set vlan 87 name isolation
set vlan 87 port 1 tag 87
set interface 1 ip 192.168.5.155 255.255.255.0
set interface 1 ip dhcp-server disable start 192.168.100.2
stop 192.168.100.254
set interface 35 ip dhcp-client enable
set interface 85 ip dhcp-client enable
set interface 86 ip dhcp-client enable
set interface 87 ip dhcp-client enable
set snmp community name public access read-write
```