FortiNAC

Ruckus Smart Zone Wireless Controller Device Integration

Version: 9.x

Date: March 24, 2022

Rev: K

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET KNOWLEDGE BASE

https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase

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 Ruckus Smart Zone device to be managed by FortiNAC. This document details the items that must be configured.

Note: As much information as possible about the integration of this device with FortiNAC is provided. However, the hardware vendor may have made modifications to the device's firmware that invalidate portions of this document. If having problems configuring the device, contact the vendor for additional support.

What it Does

Enables FortiNAC to manage wireless clients connecting to Smart Zone wireless controllers.

How it Works

To manage wireless hosts with FortiNAC, FortiNAC acts as the RADIUS server to authenticate users for the Smart Zone. FortiNAC responds to the RADIUS authentication requests with an accept or reject message. When accepting users, FortiNAC can include information that identifies the network the connecting host can access.

Network access is based upon the host's current FortiNAC state and the Network Access Policy that applies to the host/user at the time network access is required. Configuration of host network access varies depending on the device and can include: VLAN IDs and names or proprietary network identifiers.

Requirements

To integrate the Ruckus Smart Zone wireless controller with your Administrative software, you must meet the requirements listed below.

Device Firmware	Minimum Supported FortiNAC Software
Version 3.2.0 to 3.4	Version 7.3.2 or higher
Version 3.5 - 5.1	Version 8.2 or higher
Version 5.2, 6.0 or higher	Version 9.1.6, 9.2.3 or higher

API Support
Port 8443 (7443 port had been deprecated)

- Supported FortiNAC Engine Version: 8.7.1 and greater
- Supported Ruckus SZ version: 5.0 and greater

Ruckus Smart Zone Integration

Configure Ruckus

Note the following:

- **Configure the device first.** To integrate your device with your FortiNAC software, there are configuration requirements on both the device and FortiNAC. It is recommended to configure the device first.

- **Avoid certain characters.** 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.

- **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.

- **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 Ruckus controller. Make sure the following items are Configured:

- RADIUS AAA Server
- VLANs
- WLANs
- Authentication
- SNMP

RADIUS (AAA) Server

Define the FortiNAC Server or FortiNAC Control Server as the RADIUS (AAA) 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

Ruckus Smart Zone controllers use VLANs to affect the network access for different sessions. FortiNAC creates interfaces for all the VLANs supported on a device. It obtains those VLANs from each device it manages. The Ruckus controller does not require the configuration of a comprehensive list of supported VLANs, but it does allow for VLANs to be configured as part of a WLAN definition. Therefore, in order to create a list of supported VLANs on the controller that FortiNAC may access, you must create WLANs on the controller to define each VLAN you plan to use. These VLAN IDs can then be read by FortiNAC when the wireless controller is modeled in the database.

WLANs created exclusively as a placeholder for VLANs should be disabled. Only enable those that you choose to make accessible to connecting users. When a user connects to one of the enabled WLANs, FortiNAC assigns the appropriate VLAN to the session overriding any default value defined.

Create VLANs/WLANs 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 WLANs that are created only as placeholders for VLANs, most of the WLAN configuration options are not important. The only WLAN parameters that must be configured for these are the name and the default Access VLAN ID. It is recommended that you also hide the SSID.

WLANs

WLANs characterize a wireless network on the Ruckus Smart Zone wireless controller. You can create one or more WLANs on the controller and you may choose to have FortiNAC manage any number of them. For example, you may have one WLAN for staff and another for Guests.

Within your controller configuration you will have two types of WLANs configured. The first type is simply used to define the list of VLAN IDs for FortiNAC and they are disabled as described in the previous section. The second type is fully configured and enabled to allow hosts to connect to the network. For those WLANs that are enabled and used for host connections, the following configuration values must be set.

- Assign each WLAN a name.
  Important: If location based policies may be used, the WLAN Name and SSID name must match exactly. For details, see Appendix A.
- Select either **MAC Address** or **802.1x EAP** for the Authentication Options Method. (**Note:** For MAC Authentication, use the format "aa:bb:cc:dd:ee:ff".)
- Configure your encryption method.
- Configure your authentication server (RADIUS Server).
- Enable RADIUS accounting and specify the FortiNAC Server as the accounting server.
- Select the **Enable AAA VLAN Override** option.
- Provide an Access **VLAN ID** (typically this would be your production VLAN).
- Set the **Called Station ID** to "AP MAC" format under the RADIUS Option. This option enables FortiNAC to associate the wireless client and the AP to which it connects.

Authentication

Two forms of authentication are supported by FortiNAC: MAC Authentication and 802.1x. On the Ruckus Smart Zone controller the authentication method is configured with each WLAN, along with an encryption type, and other related parameters. It is possible to have multiple WLANs supported simultaneously, some using one method and others using another. When configured in this way Network Sentry only allows a single VLAN mapping for each isolation state per device. Further, for each controller, it also only supports a single production VLAN mapping per host / FortiNAC role, regardless of the WLAN to which they connect.

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 WLANs. See the section on 802.1x in the Wireless Integration Overview.

SNMP

On the **Configure::System** page inside Network Management, you must enable the SNMP Agent setting to allow FortiNAC to discover and manage the device.
FortiNAC requires a SNMPv3 user.

Configure FortiNAC

Discover Device

Add the Ruckus Controller(s) to Inventory individually or in bulk, providing SNMP and CLI/API credentials.

Click on the link below for instructions.
Add or modify a device - Instructions to add an individual device
Discovery - Instructions to add devices in bulk by defining a range of IP addresses.

Data entered is stored in the FortiNAC database and is used to allow interaction with the device. Passwords are encrypted.

Troubleshooting
Troubleshooting SNMP Communication Issues
Unable to add device to Topology due to CLI credentials
Options for Devices Unable to Be Modeled in Topology ("?" appears as the icon)

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

RADIUS (802.1x)

If using 802.1x authentication, make sure one of the following is configured:

3rd Party RADIUS server: FortiNAC acts as a proxy for 802.1x requests. 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.

Local RADIUS Server: FortiNAC's Local RADIUS Server processes RADIUS MAC and 802.1x EAP authentication without the need to proxy to an external RADIUS server. If not already enabled, configure and enable Local RADIUS Services. Refer to the Local RADIUS Server reference manual for instructions.

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.

1. Click **Network > Inventory**.
2. Expand the Container icon.
3. Right-click on the device, and then click **Model Configuration**.
4. Configure using the table below.

Ruckus Smart Zone Model Configuration Field Definitions

General

User Name	The user name used to authenticate to the REST API (web GUI).
Password	The password required to authenticate to the REST API (web GUI).

Protocol Type – 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.
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.

5. Click **Read VLANs** to retrieve the Current Device Interface settings. This creates the interface models.

Note: If the model doesn't include the SSID tab, FortiNAC may not using the correct API version to communicate with the device. For instructions, see Configure REST API Version for Communication in the Appendix.

6. Complete configuration using the table below, then click **Apply**.

Network Access – Host State

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

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.

Troubleshooting

Related KB Articles

Troubleshooting SNMP Communication Issues
Troubleshooting Poll Failures
Rogue Wireless Clients Cannot Connect to SSID
Troubleshooting RADIUS clients not connecting
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)	`nacdebug -name RadiusManager true`	/bsc/logs/output.master
FortiNAC Server (Local RADIUS)*	`nacdebug -name RadiusAccess true`	/bsc/logs/output.master
RADIUS Service (Local RADIUS)	`radiusd -X -l /var/log/radius/radius.log` Stop logging: Ctrl-C	/var/log/radius/radius.log
L2 related activity	`nacdebug -name BridgeManager true`	/bsc/logs/output.master
Vendor specific debugging	`nacdebug -name Ruckus true`	/bsc/logs/output.master
SSH/Telnet CLI activity	`nacdebug -name TelnetServer true`	/bsc/logs/output.master
SNMP activity	`nacdebug -name SnmpV1 true`	/bsc/logs/output.master
Disable debug	`nacdebug -name <debug name> false`	N/A

Note: If not using VLANs, will always return policy value “NativePolicy” in RADIUS response. Otherwise, a VLAN value is returned.

*Enables logging for a given MAC Address:

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

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
```

Appendix

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. For instructions see Resync interfaces in the Administration guide.

Using Location Based Policies

When using location based policies created with a location group containing SSID models, the SSID name must exactly match the name of the WLAN to which it belongs.

Example:
Policy uses User/Host Profile with the following criteria:
Where (Location): (Port group containing WLAN)

The SmartZone transmits the SSID name in the RADIUS packet (not the WLAN name). If the WLAN Name does not match the SSID name exactly, any location based policies will fail to match correctly for clients connecting to that particular SSID.

Under WLAN Config in Ruckus admin UI, ensure the WLAN Name matches the SSID name exactly. As of this writing, it was found under the General Options section.

Correct:
WLAN Name: testguest
SSID: testguest

Incorrect:
WLAN Name: TestGuest
SSID: testguest

Configure REST API Version for Communication

The API version used by SmartZone can change depending upon the version of SmartZone. To ensure FortiNAC uses the proper API version to communicate, do the following:

1. Login to the Control Server CLI as root and run the following command:

```
Device -ip <ruckusip> -setAttr -name RuckusAPIVersion -value <API value>
```

API version examples (based on SZ version 5.1):
"v6_0", "v6_1", "v7_0", "v8_0"

Example:

```
Device -ip 192.168.10.15 -setAttr -name RuckusAPIVersion -value "v6_0"
```

2. Re-evaluate the controller interfaces. Right-click on the controller's device model in Inventory and select **Resync Interfaces**.

Note: API values can change. Refer to the public API reference guide of the applicable SZ version: http://docs.ruckuswireless.com/smartzone/

See also API Version Recommendations.

To remove the API version:

```
Device -ip <ruckusip> -delAttr -name RuckusAPIVersion
```

API Version Recommendations

The following are based on customer feedback.

Device Firmware	API version
Version 5.2 Compatible API versions listed here: http://docs.ruckuswireless.com/smartzone/5.2.0/vsze-public-api-reference-guide-520.html	v8_2
Version 6.1.0 Compatible API versions listed here: http://docs.ruckuswireless.com/smartzone/6.1.0/vsze-public-api-reference-guide-610.html	v9_0

SNMP Strings

The following strings are read for Access Point information:

```
private final String ruckusSZWLANAPMacAddrPrefix = "1.3.6.1.4.1.25053.1.4.2.1.1.2.2.1.1";
private final String ruckusSZWLANAPName = "1.3.6.1.4.1.25053.1.4.2.1.1.2.2.1.5";
private final String ruckusSZWLANAPModelPrefix = "1.3.6.1.4.1.25053.1.4.2.1.1.2.2.1.8";
private final String ruckusSZWLANAPSerialNumber = "1.3.6.1.4.1.25053.1.4.2.1.1.2.2.1.9";
private final String ruckusSZWLANAPIPAddr = "1.3.6.1.4.1.25053.1.4.2.1.1.2.2.1.10";
```

If above return an error, the following are read:

```
private final String ruckusSZWLANAPMacAddrPrefixAlt = "1.3.6.1.4.1.25053.1.3.2.1.1.2.2.1.1";
private final String ruckusSZWLANAPNameAlt = "1.3.6.1.4.1.25053.1.3.2.1.1.2.2.1.5";
private final String ruckusSZWLANAPModelPrefixAlt = "1.3.6.1.4.1.25053.1.3.2.1.1.2.2.1.8";
private final String ruckusSZWLANAPSerialNumberAlt = "1.3.6.1.4.1.25053.1.3.2.1.1.2.2.1.9";
private final String ruckusSZWLANAPIPAddrAlt = "1.3.6.1.4.1.25053.1.3.2.1.1.2.2.1.10";
```