FortiNAC - FortiWLC Wireless Controller Integration

Version 8.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

November 8, 2019
FortiNAC 8.x FortiWLC Wireless Controller Integration
49-800-000000-20191108

TABLE OF 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.

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

Component	Requirement
Device Firmware	Version 5.1.47 or higher
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.

Individual SSID Configuration

FortiNAC supports individual SSID configuration and management for the FortiWLC wireless controller only when the SSIDs are configured for 802.1x. SSIDs configured for MAC Authentication cannot be identified in a RADIUS request and therefore are not modeled and managed independently from the device. SSIDs configured for MAC Authentication are managed based on the configuration stored for the controller in the FortiNAC Model Configuration. Refer to the Wireless Integration Overview document available in the Fortinet online Resource Center or in your online help.

FortiWLC Internal Captive Portal (ICP)

On an unsecured SSID (not 802.1x) the ICP feature on FortiWLC controllers provides a faster transition between one FortiNAC host state and another because it allows the wireless host to keep the production IP Address assigned when the host connected to the network. Users connecting to an SSID configured for ICP are always initially considered unauthenticated and have restricted network access based upon a set of default firewall rules that block all access to the network except for DHCP and DNS. See FortiWLC documentation for more information on their internal captive portal feature.

Network access control is accomplished on the FortiWLC controller through the application of this set of default of Firewall Rules to redirect hosts to an internal web page on the device. Hosts are given access only to DHCP and DNS to obtain an IP Address and all HTTP traffic is redirected to an internal web page. The web page, which consists of a customized page that must be uploaded to the controller, forces a refresh and directs the host browser to the FortiNAC captive portal or isolation interface. If the host is in a state to be allowed on the production network, FortiNAC commands the FortiWLC device to change the state of the wireless client within the controller to authenticated. For authenticated users, the default set of Firewall Rules are removed so the host can access the production network. For these users, a different set of Rules can optionally be defined and applied to provide other network restrictions based on an administrator's preference. Any such rules apply to all users connecting to the unsecured SSID however. Rules cannot be customized by user or host.

If a host needs to be isolated later, FortiNAC commands the FortiWLC device to reset the host to the unauthenticated state, and the restrictive Firewall Rules are reapplied.

This configuration can be used in place of the MAC Authentication configuration. For an SSID using 802.1x authentication, VLAN transition is still accomplished by forcing the host to request a new IP address in the new VLAN.

To use the ICP feature on the controller you must:

- Use a Layer 3 configuration on FortiNAC. Hosts will placed into the production network immediately, and remain there, but based on the host's state within FortiNAC, it will need to access the FortiNAC captive portal views on a different isolation network.
- You may need to add routes on any core network routers to allow machines on the wireless production network to access the FortiNAC isolation interface.

Additional Notes for ICP

- If ICP is enabled, FortiNAC attempts to manage all hosts connecting on all SSIDs that use WebAuth within their Security Profile.
- Browser caching may cause pages to redirect to the isolation page or timeout based on the level of access allowed by the firewall rules in effect. It may be necessary for the user to restart the browser.
- FortiNAC role based access is not available when using ICP. All users connected to the SSID that are not isolated have the same access to the network based on how it is configured for that SSID.
- There is no capability to automatically configure a supplicant or change the SSID to which the user is connecting. Users stay on the open SSID until they choose to connect elsewhere.
- If a user disconnects voluntarily from the wireless network, and subsequently reconnects, his machine may immediately be placed back on the network in his previous authenticated state subject to the value of the "L3 User Session Timeout" value configured for the captive portal on the controller. Other controller-based timeouts also apply including the "CaptivePortalSessionTimeout" and the "CaptivePortalActivityTimeout".

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.

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.

Overview

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.

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

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.

When integrating the FortiWLC device with FortiNAC you can use three authentication methods, 802.1x, MAC Authentication and Internal Captive Portal. If you are configuring multiple SSIDs on the FortiWLC controller you can use a different method for each SSID, subject to the limitations above for SSID management. This document provides general configuration instructions for each one. The SNMP and CLI Prompt configuration sections below are required for any FortiWLC FortiNAC integration.

SNMP

SNMP must be enabled and configured on the FortiWLC controller to allow FortiNAC to discover and manage the device. Both SNMPv1 or SNMPv3 are supported. If not using SNMPv3, enable both SNMPv1 and SNMPV2C in the controller. Enable SNMP by adding the FortiNAC appliance IP address as a client.

Note: SNMP is not started by default on the WLC.

Use the following command in the WLC to enable SNMP:

```
SNMP start
```

Use the following command in the WLC to verify SNMP is running:

`SNMP Status`

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.

FortiWLC Device Configuration - 802.1x

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

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.

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 configure the following:

- VLAN name
- VLAN ID
- The DHCP Pass-Through option should be set to On.

AP's Configured for Bridged Mode: Ensure VLANs configured on the AP are also created in the controller. Otherwise, those VLANs cannot be used when provisioning network access. FortiNAC needs visibility to all VLANs that it may be configured to assign. A centralized network is not required for each VLAN, but the VLAN must exist on the controller.

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 preconfigured to use port 1812 for authentication. Set the MAC Address delimiter to colon (:).
- **(No longer required as of FortiNAC version 8.5.2)**: You must also define the FortiNAC Server or FortiNAC Control Server as the RADIUS Accounting 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 1813 for accounting.
- In the RADIUS Server Configuration, set the **Called-Station-ID Type** to **MacAddress:SSID**.
- If setting up FortiNAC as the RADIUS server for a device in a Fortinet High Availability environment, the actual IP address of the primary control server must be used, 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.

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.

MAC Filtering

For MAC Filtering configure the following:

- FortiWLC Versions prior to 5.3: Make sure the ACL Environment State is set to Deny List Enabled
- FortiWLC Versions 5.3 and above: Enable RADIUS Change of Authorization (CoA)

For FortiWLC Versions 6.0 and Above

- MAC filtering feature is only necessary when implementing MAC Authentication, but must not be used for ESS Profiles configured for 802.1X.

For FortiWLC Versions Prior to 6.0

- MAC Filtering must be configured with 802.1X. If you are configuring only 802.1X SSIDs then the RADIUS profile Name field should be left at the default of "No RADIUS". If you are configuring any MAC 6 FortiNAC FortiWLC Wireless IntegrationAuth SSIDs, then select the RADIUS profile created above that designates your FortiNAC Server as the RADIUS server.

Authentication - Security Profile

On the FortiWLC controller the authentication method is configured as a Security Profile along with an encryption type, and other related parameters. These profiles are later associated with an SSID. It is possible to have multiple SSIDs supported simultaneously, some using one method and others using another.

When configuring a wireless device with multiple SSIDs that will be managed by FortiNAC, FortiNAC only allows a single VLAN mapping for each isolation state per device. For example, if the Remediation VLAN is VLAN 10 on one SSID it has to be VLAN 10 on all SSIDs, and if Dead End is VLAN 25 it has to be VLAN 25 for all SSIDs.

If you choose to use 802.1x Authentication you must create a separate Security Profile for that authentication type. Configure the profile as follows:

- In the **L2 Modes allowed** section select **WPA** or **WPA2**.
- Set Primary RADIUS server to the RADIUS profile created above that designates your FortiNAC Server as the RADIUS server.
- In the **Captive Portal** section select **Disabled**.
- Set the **802.1x Network Initiation** to **On**.
- Set **Mac Filtering** to **On**.

ESS Profile/SSID

SSID characterizes a wireless network on the FortiWLC controller. You can create one or more SSIDs on the controller and you may choose to have FortiNAC manage any number of them. Each SSID is represented by an ESS Profile. For each SSID you wish to have FortiNAC manage, create an ESS Profile aa follows:

- Create an **ESS Profile Name**.
- Create a **SSID Name**.
- Set the **Enable/Disable** field to **Enable**.
- Select the 802.1x **Security Profile** from the list.
- Set the **Tunnel Interface** type to **RADIUS VLAN Only**.
- Set **the IP Prefix Validation** field to **Off**. When enabled, it conflicts with configurations that require a radius change of VLANs via radius.

FortiWLC Device Configuration - MAC Authentication

This section provides instructions for configuring the FortiWLC controller with an SSID that uses MAC Authentication. Other methods of controlling which hosts are allowed on the network, such as 802.1x or Internal Captive Portal, can also be configured and are discussed in this document.

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

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.

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 configure the following:

- VLAN name
- VLAN ID
- The DHCP Pass-Through option should be set to On.

AP's Configured for Bridged Mode: Ensure VLANs configured on the AP are also created in the controller. Otherwise, those VLANs cannot be used when provisioning network access. FortiNAC needs visibility to all VLANs that it may be configured to assign. A centralized network is not required for each VLAN, but the VLAN must exist on the controller.

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 preconfigured to use port 1812 for authentication. Set the MAC Address delimiter to colon (:).

If setting up FortiNAC as the RADIUS server for a device in a Fortinet High Availability environment, the actual IP address of the primary control server must be used, 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.

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.

MAC Filtering

For MAC Filtering configure the following:

- FortiWLC Versions prior to 8.0: Make sure the ACL Environment State is set to Deny List Enabled
- FortiWLC Versions 8.0 and above: Enable RADIUS Change of Authorization (CoA)
- For MAC Auth SSIDs, select the RADIUS profile created above that designates your FortiNAC Server as the RADIUS server.

Authentication - Security Profile

On the FortiWLC controller the authentication method is configured as a Security Profile along with an encryption type, and other related parameters. These profiles are later associated with an SSID. It is possible to have multiple SSIDs supported simultaneously, some using one method and others using another.

When configuring a wireless device with multiple SSIDs that will be managed by FortiNAC, FortiNAC only allows a single VLAN mapping for each isolation state per device. For example, if the Remediation VLAN is VLAN 10 on one SSID it has to be VLAN 10 on all SSIDs, and if Dead End is VLAN 25 it has to be VLAN 25 for all SSIDs.

If you choose to use MAC Authentication you must create a Security Profile specifically for this authentication type. Note that with MAC Authentication the RADIUS server configured under the MAC Filter is always used. You cannot specify a different RADIUS server. Configure the profile as follows:

- In the L2 Modes allowed section select an encryption mode.
- In the Captive Portal section select Disabled.
- Set Mac Filtering to On.

ESS Profile/SSID

SSID characterizes a wireless network on the FortiWLC controller. You can create one or more SSIDs on the controller and you may choose to have FortiNAC manage any number of them. Each SSID is represented by an ESS Profile. For each SSID you wish to have FortiNAC manage, create an ESS Profile aa follows:

- Create an **ESS Profile Name**.
- Create a **SSID Name**.
- Set the **Enable/Disable** field to **Enable**.
- Select the MAC Authentication **Security Profile** from the list.
- Set the **Tunnel Interface** type to **RADIUS VLAN Only**.
- Set the **IP Prefix Validation** field to **Off**. When enabled, it conflicts with configurations that require a radius change of VLANs via radius.

SSID Location

FortiWLC controllers running firmware version 6.0 or higher can provide SSID Location information along with a MAC Authentication RADIUS request. This information allows FortiNAC to model the MAC Auth SSIDs. When SSIDs are modeled, FortiNAC can leverage User/Host Profiles that are based on the SSID location to assign policies. To send SSID Location to FortiNAC in a RADIUS request configure the following:

Under **Configuration > Security-RADIUS** set the **Called-Station-ID Type** option to **MAC MacAddress:SSID**

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.

Be sure to configure the IP address of the FortiNAC Server or Control Server as a client in the FortiWLC SNMP setup. If SNMP is not setup correctly, FortiNAC will not be able to communicate with the controller.

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.

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.
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-

Field	Definition
	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.  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	
Manage Captive Portal	If enabled, FortiNAC uses Firewall Rules to treat authenticated and unauthenticated users differently. See the ICP description in this document for more information. If the Captive Portal setting on any Security Profile for any SSID is set to WebAuth indicating that the SSID is being managed by Internal Captive Portal (ICP) on the Meru Controller and this check box is enabled, all SSIDs set to WebAuth will be managed by FortiNAC.
Read VLANs	Populates the Access Value fields with configured VLANs read from the controller.
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	
	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:

Field	Definition
Access Enforcement	**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.

Setup the Model Configuration

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.

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. In the Protocol section select either Telnet or SSHv2 if it is available on your device model.
5. Click Apply.
6. 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.

7. Enter the RADIUS Secret. This must match the value entered on the device itself and the value entered on the RADIUS settings window.
8. To use the ICP feature, enable the Manage Captive Portal check box
9. . Click Read VLANS to retrieve the Current Device Interface settings. This creates the interface models.
10. Select a setting in Access Enforcement for each host state.
11. In the Access Value column enter a VLAN ID for each host state that you wish to enforce.

Access Enforcement applies only to SSIDs configured for 802.1x or MAC authentication. SSIDs configured to use ICP or set to WebAuth will ignore Access Enforcement settings.

12. In the Preferred Container field, select the Container in which the Wireless Access Points should be placed as they are discovered.
13. 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.

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. It is recommended that you add the wireless device to the L3 Polling group, which does IP to MAC polling. You can set polling intervals on an individual device by going to the Device Properties window for that device.

Add FortiWLC Controller to L3 Polling Group

If you are using the ICP feature, the FortiWLC controller must be added to the L3 Polling Group with a higher priority than other devices. Modify the controller's group membership and priority as follows:

1. Select **Network Devices > Inventory**.
2. Locate the FortiWLC Controller in the list of devices and select it.
3. In the Views column select the **Group Membership** icon.
4. When the Group Membership dialog is displayed, click on the **L3 (IP->MAC)** group to mark it with a check mark and click **OK**.
5. On the Device Properties window click the **Polling** tab.
6. Scroll down to **L3 Polling** and set the priority to something higher than all other devices, such as High.
7. Click **Save**.

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 definitions, it is recommended that you read VLANs for that device again.

1. Select **Network Devices > Inventory**.
2. Expand the **Container** that stores the device.
3. Select the device and right-click. From the menu select **Network Access/VLANS**.
4. Click **Read VLANs**. This resynchronizes the FortiNAC software and the device configuration.

Administrator Permission Level

Make sure that the Administrator has a high enough permission level to allow the user to modify the device configuration. If the permission level is set too low the user cannot modify data. The level required can vary depending on the parameter being modified.

Required permission levels for each function are included in the FortiWLC Help files. Refer to the Help on the device for more detailed information.

FortiWLC 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.

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

Configuring MAC Authentication

The following is the section of the running configuration for the FortiWLC controller that specifies the configuration for MAC authentication. The relevant settings are in bold.

To summarize, the SSID FortiWLC uses the security profile called MacAuth with **allowed L2 modes** set to **clear**, and with **macfiltering** enabled. The Mac Filter configuration has access-list **deny** enabled which the FortiNAC appliance needs for dissociate purposes, and the access-list radius-server profile is qa245-MacAuth.

This radius profile points to 192.168.5.245:1812 as the RADIUS server:port.

```
essid MERU
security-profile MacAuth
tunnel-type radius-only
vlan name ""
gre name ""
virtual-cell-type per-station-bssid
countermeasure
dataplane tunneled
ssid MERU
ap-discovery join-ess
ap-discovery join-virtual-ap
publish-essid
beacon dtim-period 1
beacon period 100
supported-tx-rates 802.11b 1
supported-tx-rates 802.11b 2
supported-tx-rates 802.11b 5.5
supported-tx-rates 802.11b 11
supported-tx-rates 802.11a 6
supported-tx-rates 802.11a 9
supported-tx-rates 802.11a 12
supported-tx-rates 802.11a 18
supported-tx-rates 802.11a 24
supported-tx-rates 802.11a 36
supported-tx-rates 802.11a 48
```

```
supported-tx-rates 802.11a 54
supported-tx-rates 802.11an 6
supported-tx-rates 802.11an 9
supported-tx-rates 802.11an 12
supported-tx-rates 802.11an 18
supported-tx-rates 802.11an 24
supported-tx-rates 802.11an 36
supported-tx-rates 802.11an 48
supported-tx-rates 802.11an 54
supported-tx-rates 802.11an-mcs 0
supported-tx-rates 802.11an-mcs 1
supported-tx-rates 802.11an-mcs 2
supported-tx-rates 802.11an-mcs 3
supported-tx-rates 802.11an-mcs 4
supported-tx-rates 802.11an-mcs 5
supported-tx-rates 802.11an-mcs 6
supported-tx-rates 802.11an-mcs 7
supported-tx-rates 802.11an-mcs 8
supported-tx-rates 802.11an-mcs 9
supported-tx-rates 802.11an-mcs 10
supported-tx-rates 802.11an-mcs 11
supported-tx-rates 802.11an-mcs 12
supported-tx-rates 802.11an-mcs 13
supported-tx-rates 802.11an-mcs 14
supported-tx-rates 802.11an-mcs 15
supported-tx-rates 802.11g 6
supported-tx-rates 802.11g 9
supported-tx-rates 802.11g 12
supported-tx-rates 802.11g 18
supported-tx-rates 802.11g 24
supported-tx-rates 802.11g 36
supported-tx-rates 802.11g 48
supported-tx-rates 802.11g 54
supported-tx-rates 802.11bg 1
supported-tx-rates 802.11bg 2
supported-tx-rates 802.11bg 5.5
supported-tx-rates 802.11bg 11
supported-tx-rates 802.11bg 6
supported-tx-rates 802.11bg 9
supported-tx-rates 802.11bg 12
supported-tx-rates 802.11bg 18
supported-tx-rates 802.11bg 24
supported-tx-rates 802.11bg 36
supported-tx-rates 802.11bg 48
supported-tx-rates 802.11bg 54
supported-tx-rates 802.11bgn 1
supported-tx-rates 802.11bgn 2
supported-tx-rates 802.11bgn 5.5
supported-tx-rates 802.11bgn 11
supported-tx-rates 802.11bgn 6
```

```
supported-tx-rates 802.11bgn 9
supported-tx-rates 802.11bgn 12
supported-tx-rates 802.11bgn 18
supported-tx-rates 802.11bgn 24
supported-tx-rates 802.11bgn 36
supported-tx-rates 802.11bgn 48
supported-tx-rates 802.11bgn 54
supported-tx-rates 802.11bgn-mcs 0
supported-tx-rates 802.11bgn-mcs 1
supported-tx-rates 802.11bgn-mcs 2
supported-tx-rates 802.11bgn-mcs 3
supported-tx-rates 802.11bgn-mcs 4
supported-tx-rates 802.11bgn-mcs 5
supported-tx-rates 802.11bgn-mcs 6
supported-tx-rates 802.11bgn-mcs 7
supported-tx-rates 802.11bgn-mcs 8
supported-tx-rates 802 .11bgn-mcs 9
supported-tx-rates 802 .11bgn-mcs 10
supported-tx-rates 802 .11bgn-mcs 11
supported-tx-rates 802 .11bgn-mcs 12
supported-tx-rates 802 .11bgn-mcs 13
supported-tx-rates 802 .11bgn-mcs 14
supported-tx-rates 802 .11bgn-mcs 15
base-tx-rates 802.11b 11
base-tx-rates 802.11a 6
base-tx-rates 802.11a 12
base-tx-rates 802.11a 24
base-tx-rates 802.11an 6
base-tx-rates 802.11an 12
base-tx-rates 802.11an 24
base-tx-rates 802.11g 6
base-tx-rates 802.11g 9
base-tx-rates 802.11g 12
base-tx-rates 802.11g 18
base-tx-rates 802.11g 24
base-tx-rates 802.11g 36
base-tx-rates 802.11g 48
base-tx-rates 802.11g 54
base-tx-rates 802.11bg 11
base-tx-rates 802.11bg n 11
accounting interim-interval 3600
accounting primary-radius ""
accounting secondary-radius ""
no multicast-enable
no silent-client-enable
no wmm-support
ess-ap 1 1
calls-per-bss 0
exit
exit
```

```
security-profile MacAuth
key-rotation disabled
allowed-l2-modes clear
captive-portal disabled
captive-portal-passthru 0.0.0.0 0.0.0.0
psk key ""
firewall-capability none
firewall-filter-id ""
security-logging off
static-wep key ""
static-wep key-index 1
macfiltering
rekey period 0
group-rekey interval 0
radius-server primary ""
radius-server secondary ""
auth-supplicant-timeout 30
auth-server-timeout 30
auth-max-request 4
pae-max-reauth 4
pae-txperiod 30
no kddi
no captive-portal
no shared-authentication
no rekey period
no 8021x-network-initiation
no fast-handoff
no reauth
exit
access-list state deny
access-list radius-server primary qa245-MacAuth
radius-profile qa245-MacAuth
description ""
ip-address 192.168.5.245
key abc123
port 1812
mac-delimiter colon
password-type shared-secret
exit
```

Configuring 802.1X

The following is the section of the running configuration for the FortiWLC controller that specifies the configuration for 802.1x. The relevant settings are in bold.

This shows an 802.1X-enabled SSID, MERU-1X.

```
essid MERU-1X
security-profile 802-1X
```

```
tunnel-type radius-only
vlan name ""
gre name ""
virtual-cell-type per-station-bssid
countermeasure
dataplane tunneled
ssid MERU-1X
ap-discovery join-ess
ap-discovery join-virtual-ap
publish-essid
beacon dtim-period 1
beacon period 100
supported-tx-rates 802.11b 1
supported-tx-rates 802.11b 2
supported-tx-rates 802.11b 5.5
supported-tx-rates 802.11b 11
supported-tx-rates 802.11a 6
supported-tx-rates 802.11a 9
supported-tx-rates 802.11a 12
supported-tx-rates 802.11a 18
supported-tx-rates 802.11a 24
supported-tx-rates 802.11a 36
supported-tx-rates 802.11a 48
supported-tx-rates 802.11a 54
supported-tx-rates 802.11an 6
supported-tx-rates 802.11an 9
supported-tx-rates 802.11an 12
supported-tx-rates 802.11an 18
supported-tx-rates 802.11an 24
supported-tx-rates 802.11an 36
supported-tx-rates 802.11an 48
supported-tx-rates 802.11an 54
supported-tx-rates 802.11an-mcs 0
supported-tx-rates 802.11an-mcs 1
supported-tx-rates 802.11an-mcs 2
supported-tx-rates 802.11an-mcs 3
supported-tx-rates 802.11an-mcs 4
supported-tx-rates 802.11an-mcs 5
supported-tx-rates 802.11an-mcs 6
supported-tx-rates 802.11an-mcs 7
supported-tx-rates 802.11an-mcs 8
supported-tx-rates 802.11an-mcs 9
supported-tx-rates 802.11an-mcs 10
supported-tx-rates 802.11an-mcs 11
supported-tx-rates 802.11an-mcs 12
supported-tx-rates 802.11an-mcs 13
supported-tx-rates 802.11an-mcs 14
supported-tx-rates 802.11an-mcs 15
supported-tx-rates 802.11g 6
supported-tx-rates 802.11g 9
```

```
supported-tx-rates 802.11g 12
supported-tx-rates 802.11g 18
supported-tx-rates 802.11g 24
supported-tx-rates 802.11g 36
supported-tx-rates 802.11g 48
supported-tx-rates 802.11g 54
supported-tx-rates 802.11bg 1
supported-tx-rates 802.11bg 2
supported-tx-rates 802.11bg 5.5
supported-tx-rates 802.11bg 11
supported-tx-rates 802.11bg 6
supported-tx-rates 802.11bg 9
supported-tx-rates 802.11bg 12
supported-tx-rates 802.11bg 18
supported-tx-rates 802.11bg 24
supported-tx-rates 802.11bg 36
supported-tx-rates 802.11bg 48
supported-tx-rates 802.11bg 54
supported-tx-rates 802.11bgn 1
supported-tx-rates 802.11bgn 2
supported-tx-rates 802.11bgn 5.5
supported-tx-rates 802.11bgn 11
supported-tx-rates 802.11bgn 6
supported-tx-rates 802.11bgn 9
supported-tx-rates 802.11bgn 12
supported-tx-rates 802.11bgn 18
supported-tx-rates 802.11bgn 24
supported-tx-rates 802.11bgn 36
supported-tx-rates 802.11bgn 48
supported-tx-rates 802.11bgn 54
supported-tx-rates 802.11bgn-mcs 0
supported-tx-rates 802.11bgn-mcs 1
supported-tx-rates 802.11bgn-mcs 2
supported-tx-rates 802.11bgn-mcs 3
supported-tx-rates 802.11bgn-mcs 4
supported-tx-rates 802.11bgn-mcs 5
supported-tx-rates 802.11bgn-mcs 6
supported-tx-rates 802.11bgn-mcs 7
supported-tx-rates 802.11bgn-mcs 8
supported-tx-rates 802 .11bgn-mcs 9
supported-tx-rates 802 .11bgn-mcs 10
supported-tx-rates 802 .11bgn-mcs 11
supported-tx-rates 802 .11bgn-mcs 12
supported-tx-rates 802 .11bgn-mcs 13
supported-tx-rates 802 .11bgn-mcs 14
supported-tx-rates 802 .11bgn-mcs 15
base-tx-rates 802.11b 11
base-tx-rates 802.11a 6
base-tx-rates 802.11a 12
base-tx-rates 802.11a 24
```

```
base-tx-rates 802.11an 6
base-tx-rates 802.11an 12
base-tx-rates 802.11an 24
base-tx-rates 802.11g 6
base-tx-rates 802.11g 9
base-tx-rates 802.11g 12
base-tx-rates 802.11g 18
base-tx-rates 802.11g 24
base-tx-rates 802.11g 36
base-tx-rates 802.11g 48
base-tx-rates 802.11g 54
base-tx-rates 802.11bg 11
base-tx-rates 802.11bg n 11
accounting interim-interval 3600
accounting primary-radius ""
accounting secondary-radius ""
no multicast-enable
no silent-client-enable
no wmm-support
ess-ap 1 1
calls-per-bss 0
exit
exit
security-profile 802-1X
key-rotation disabled
allowed-l2-modes wpa
captive-portal disabled
captive-portal-passthru 0.0.0.0 0.0.0.0
encryption-modes tkip
psk key ""
firewall-capability none
firewall-filter-id ""
security-logging off
static-wep key ""
static-wep key-index 1
reauth
macfiltering
rekey period 0
group-rekey interval 0
8021x-network-initiation
radius-server primary qa245
radius-server secondary ""
auth-supplicant-timeout 30
auth-server-timeout 30
auth-max-request 4
pae-max-reauth 4
pae-txperiod 30
no kddi
no captive-portal
no shared-authentication
```

```
no rekey period
no fast-handoff
exit
radius-profile qa245
description ""
ip-address 192.168.5.245
key abc123
port 1812
mac-delimiter colon
password-type shared-secret
exit
```

Configuring Internal Captive Portal (ICP)

The following is the section of the running configuration for the FortiWLC controller that specifies the configuration for ICP. The relevant settings are in bold. For the purposes of our example configuration, VLAN 59 (172.16.59.0/24) is the production network and VLAN 46 (172.16.46.0/24) is the isolation network.

VLAN Definitions

```
vlan productionVlan tag 59
ip dhcp-server 0.0.0.0
ip address 172.16.59.10 255.255.255.0
ip default-gateway 172.16.59.1
ip dhcp-passthrough
tag 59
owner controller
vlan-version 0
interface FastEthernet controller 1
no ip dhcp-override
exit
vlan isolationVlan tag 46
ip dhcp-server 0.0.0.0
ip address 172.16.46.10 255.255.255.0
ip default-gateway 172.16.46.1
ip dhcp-passthrough
tag 46
owner controller
vlan-version 0
interface FastEthernet controller 1
no ip dhcp-override
exit
```

Firewall rules:

For unauthenticated users:

```
qosrule 3000 netprotocol 0 qosprotocol none
firewall-filter-id unauthUser
firewall-filter-id-match on
dstip 172.16.46.2
dstip-match on
dstmask 255.255.255.0
dstport 0
srcip 0.0.0.0
srcmask 0.0.0.0
srcport
action forward
droppolicy tail
priority 0
avgpacketrate 0
tokenbucketrate 0
dscp disabled
qosrulelogging off
qosrule-logging-frequency 60
packet-min-length 0
packet-max-length 0
no trafficcontrol
exit
qosrule 3010 netprotocol 0 qosprotocol none
firewall-filter-id unauthUser
firewall-filter-id-match on
dstip 0.0.0.0
dstmask 0.0.0.0
dstport 0
srcip 172.16.46.2
srcip-match on
srcmask 255.255.255.0
srcport 0
action forward
droppolicy tail
priority 0
avgpacketrate 0
tokenbucketrate 0
dscp disabled
qosrulelogging off
qosrule-logging-frequency 60
packet-min-length 0
packet-max-length 0
no trafficcontrol
exit
```

For authenticated users:

There are no required firewall rules for this. Whatever the admin wants to use to restrict access for their registered users.

Security Profile:

```
security-profile IntCP
security-version 0
key-rotation disabled
allowed-l2-modes clear
captive-portal webauth
captive-portal-auth-method internal
psk key ""
firewall-capability configured
passthrough-firewall-filter-id unauthUser
firewall-filter-id authUser
security-logging off
owner controller
static-wep key ""
static-wep key-index 1
rekey period 0
group-rekey interval 0
radius-server primary ""
radius-server secondary ""
auth-supplicant-timeout 30
auth-server-timeout 30
auth-max-request 4
pae-max-reauth 4
pae-txperiod 30
no kddi
no shared-authentication
no rekey period
no 8021x-network-initiation
no fast-handoff
no pmk-caching
no reauth
no macfiltering
exit
```

ESS Profile:

```
essid Guest
enable
security-profile IntCP
ess-version 0
tunnel-type configured-vlan-only
vlan name productionVlan
gre name ""
multicast-to-unicast-conversion
virtual-port
countermeasure
ap-vlan-tag 0
band-steering-mode disable
band-steering-timeout 5
dataplane tunneled
ssid MC1500-Guest
owner controller
ap-discovery join-ess
ap-discovery join-virtual-ap
publish-essid
publish-essid-vport disabled
beacon dtim-period 1
beacon period 100
supported-tx-rates 802.11b 1
supported-tx-rates 802.11b 2
supported-tx-rates 802.11b 5.5
supported-tx-rates 802.11b 11
supported-tx-rates 802.11a 6
supported-tx-rates 802.11a 9
supported-tx-rates 802.11a 12
supported-tx-rates 802.11a 18
supported-tx-rates 802.11a 24
supported-tx-rates 802.11a 36
supported-tx-rates 802.11a 48
supported-tx-rates 802.11a 54
supported-tx-rates 802.11an 6
supported-tx-rates 802.11an 9
supported-tx-rates 802.11an 12
supported-tx-rates 802.11an 18
supported-tx-rates 802.11an 24
supported-tx-rates 802.11an 36
supported-tx-rates 802.11an 48
supported-tx-rates 802.11an 54
supported-tx-rates 802.11an-mcs 0
supported-tx-rates 802.11an-mcs 1
supported-tx-rates 802.11an-mcs 2
supported-tx-rates 802.11an-mcs 3
supported-tx-rates 802.11an-mcs 4
supported-tx-rates 802.11an-mcs 5
```

```
supported-tx-rates 802.11an-mcs 6
supported-tx-rates 802.11an-mcs 7
supported-tx-rates 802.11an-mcs 8
supported-tx-rates 802.11an-mcs 9
supported-tx-rates 802.11an-mcs 10
supported-tx-rates 802.11an-mcs 11
supported-tx-rates 802.11an-mcs 12
supported-tx-rates 802.11an-mcs 13
supported-tx-rates 802.11an-mcs 14
supported-tx-rates 802.11an-mcs 15
supported-tx-rates 802.11an-mcs 16
supported-tx-rates 802.11an-mcs 17
supported-tx-rates 802.11an-mcs 18
supported-tx-rates 802.11an-mcs 19
supported-tx-rates 802.11an-mcs 20
supported-tx-rates 802.11an-mcs 21
supported-tx-rates 802.11an-mcs 22
supported-tx-rates 802.11an-mcs 23
supported-tx-rates 802.11g 6
supported-tx-rates 802.11g 9
supported-tx-rates 802.11g 12
supported-tx-rates 802.11g 18
supported-tx-rates 802.11g 24
supported-tx-rates 802.11g 36
supported-tx-rates 802.11g 48
supported-tx-rates 802.11g 54
supported-tx-rates 802.11bg 1
supported-tx-rates 802.11bg 2
supported-tx-rates 802.11bg 5.5
supported-tx-rates 802.11bg 11
supported-tx-rates 802.11bg 6
supported-tx-rates 802.11bg 9
supported-tx-rates 802.11bg 12
supported-tx-rates 802.11bg 18
supported-tx-rates 802.11bg 24
supported-tx-rates 802.11bg 36
supported-tx-rates 802.11bg 48
supported-tx-rates 802.11bg 54
supported-tx-rates 802.11bgn 1
supported-tx-rates 802.11bgn 2
supported-tx-rates 802.11bgn 5.5
supported-tx-rates 802.11bgn 11
supported-tx-rates 802.11bgn 6
supported-tx-rates 802.11bgn 9
supported-tx-rates 802.11bgn 12
supported-tx-rates 802.11bgn 18
supported-tx-rates 802.11bgn 24
supported-tx-rates 802.11bgn 36
supported-tx-rates 802.11bgn 48
supported-tx-rates 802.11bgn 54
```

```
supported-tx-rates 802.11bgn-mcs 0
supported-tx-rates 802.11bgn-mcs 1
supported-tx-rates 802.11bgn-mcs 2
supported-tx-rates 802.11bgn-mcs 3
supported-tx-rates 802.11bgn-mcs 4
supported-tx-rates 802.11bgn-mcs 5
supported-tx-rates 802.11bgn-mcs 6
supported-tx-rates 802.11bgn-mcs 7
supported-tx-rates 802.11bgn-mcs 8
supported-tx-rates 802 .11bgn-mcs 9
supported-tx-rates 802 .11bgn-mcs 10
supported-tx-rates 802 .11bgn-mcs 11
supported-tx-rates 802 .11bgn-mcs 12
supported-tx-rates 802 .11bgn-mcs 13
supported-tx-rates 802 .11bgn-mcs 14
supported-tx-rates 802 .11bgn-mcs 15
supported-tx-rates 802.11bgn-mcs 16
supported-tx-rates 802.11bgn-mcs 17
supported-tx-rates 802.11bgn-mcs 18
supported-tx-rates 802.11bgn-mcs 19
supported-tx-rates 802.11bgn-mcs 20
supported-tx-rates 802.11bgn-mcs 21
supported-tx-rates 802.11bgn-mcs 22
supported-tx-rates 802.11bgn-mcs 23
base-tx-rates 802.11b 11
base-tx-rates 802.11a 6
base-tx-rates 802.11a 12
base-tx-rates 802.11a 24
base-tx-rates 802.11an 6
base-tx-rates 802.11an 12
base-tx-rates 802.11an 24
base-tx-rates 802.11g 6
base-tx-rates 802.11g 9
base-tx-rates 802.11g 12
base-tx-rates 802.11g 18
base-tx-rates 802.11g 24
base-tx-rates 802.11g 36
base-tx-rates 802.11g 48
base-tx-rates 802.11g 54
base-tx-rates 802.11bg 11
base-tx-rates 802.11bg n 11
accounting interim-interval 3600
accounting primary-radius ""
accounting secondary-radius ""
overflow-from ""
no multicast-enable
no silent-client-enable
no multiple-ip-per-station
no expedited-forward-override
no wmm-support
```

```
no apsd-support
no multicast-mac-transparency
no ap-vlan-priority
ess-ap 3 1
calls-per-bss 0
exit
ess-ap 1 1
calls-per-bss 0
exit
ess-ap 1 2
calls-per-bss 0
exit
exit
```

SNMP

```
snmp-server community public 192.168.5.242 rw
```