



FortiNAC

Aruba and Alcatel

Wireless Controllers Integration

Version 8.x

Date: December 4, 2020

Rev: H

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET KNOWLEDGE BASE

<http://kb.fortinet.com>

FORTINET BLOG

<http://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<http://support.fortinet.com>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

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>



Contents

Overview.....	4
Requirements.....	4
Other Devices.....	5
Considerations	5
Integration.....	6
Configure Aruba Device.....	6
Aruba Controller Redundancy Options	6
Aruba Wireless Network Options	8
Authentication Servers	13
Authentication.....	14
RAP Wired PortIntegration	14
Virtual AP	15
SNMP	15
Default CLI Prompt Requirements	15
Configure FortiNAC	16
RADIUS Server (Required for 802.1x Authentication)	16
Model the Device.....	16
Device Model Configuration.....	17
Discover AccessPoints	21
Device Groups	21
Port Groups	21
Prevent SSID Removal After Failed Read.....	21
Troubleshooting.....	22
SNMP.....	22
Resynchronize VLANs or Roles.....	22
Aruba Logon Lifetime Parameter	22
Appendix.....	23
Aruba Sample Configuration.....	23

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](#) reference manual in the Fortinet Document Library.

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

Component	Requirement
Aruba Firmware	Minimum: ArubaOS 3.1.x.x or higher Note: AOS 3.2.x.x is not supported. Preferred: ArubaOS 8.5.0.5 or higher – see Limitations 2
FortiNAC Software	Minimum: Version 8.0 or higher Preferred: Verison 8.6.2 or higher – see Limitations 3 Note: In many cases previous versions of FortiNAC can be used, however, instructions are written based on the version noted here.

Limitations:

1. Bridge Mode does not support RFC3576/CoA. FortiNAC must disconnect clients via CLI commands. Refer to the following link:
https://www.arubanetworks.com/techdocs/ArubaOS_85_Web_Help/Content/arubaos-solutions/behavior-defaults/unde-mode-supp.htm?Highlight=bridge%20mode
2. ArubaOS 8.5.0.5 fixes a known issue where SSH sessions could hang. This can affect Aruba integrations with FortiNAC that are not using RFC 3576 for disconnection and Change of Authorization (CoA). Refer to ArubaOS 8.5.0.5 Release Notes for details.
3. FortiNAC version 8.6.1 required for ArubaOS 8.5
4. FortiNAC versions 8.6.1 and 8.6.2 include several Aruba integration fixes. For details, see [8.6.2 Release Notes in the Fortinet Document Library](#).

Note: Aruba Instant AP devices cannot be configured for use with FortiNAC using this set of integration instructions. See [FortiNAC Aruba Instant AP Integration](#) reference manual in the Fortinet Document Library for instructions.

Other Devices

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

- Alcatel Wireless Controllers

Considerations

Before configuring your Aruba Wireless Controller, you should be aware of the following:

- **Aruba Software License Dependencies**
 - For all ArubaOS releases the PEF license is required to support Roles on the Aruba controller. Without the PEF license, only VLANs can be configured on the controller.
- **SSID Operation Mode and Authentication**
 - It is recommended that Aruba OS version 3.1.1 and above is running on mobility controllers integrating with FortiNAC software.
 - In environments that lack 802.1x infrastructure, enable MAC authentication. Set the security for an SSID using MAC authentication to Open System. This relies upon RADIUS transactions to provide dynamic role assignment to connecting hosts.

VLAN Pools

Aruba allows for the creation of VLAN pools on the controller. VLAN pools may be used with FortiNAC with the following configuration requirements:

- VLAN pools must be encapsulated within an Aruba role definition. FortiNAC assigns sessions to roles and is agnostic to the VLANs within the pool.
- Within the FortiNAC model configuration view for the Aruba controller, the Operational Mode must be set to "L2 Roles with VLANs". For additional details, refer to "FortiNAC Software Device Model Configuration".
- If VLAN pools are to be used for FortiNAC Isolation network states (Registration, Remediation, etc), FortiNAC must be configured for Layer 3 Network Type (isolation network traffic is routed to FortiNAC).
- VLAN pools within Aruba roles have been validated on Aruba version 6.4.4.9, although earlier versions of Aruba firmware may also support them.

Integration

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.

Configure Aruba Device

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.

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.

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.

The configuration of your Aruba controller will vary depending on the configuration of your network and how you choose to control network access.

Aruba Controller Redundancy Options

Active/Active Configuration

Note: For information on how to model a device that supports hot standby with virtual IP assignment, refer to the "Wireless Integration Requirements" section of the [Wireless Integration Overview](#) document.

Both master and local controllers are active on the network, supporting wireless traffic. In this environment, FortiNAC needs to be aware of both controllers because both are active in authenticating users and managing wireless sessions. In order for proper communication with both controllers to occur (providing security for all wireless sessions), both controllers must be modeled.

See [Model the Device](#) for instructions on modeling each controller.

Active/Passive Configuration

Only the master controller is active on the network processing wireless traffic. The passive controller operates in a standby mode ready to take over should the master fail.

In this environment, a virtual IP address is used. The virtual IP is owned by the actively running controller. Should the master fail, the local standby controller takes ownership of the virtual IP, along with all the wireless sessions being managed.

Although the controller is accessed using the virtual IP for session and other device queries, controllers with this configuration continue to source RADIUS authentication requests using their physical interface IP address.

FortiNAC will accept the request from the source but uses the NAS-IP RADIUS attribute in the packet to look up the actual controller model for FortiNAC configuration values.

Aruba Configuration Requirements for Active/Passive Configuration

Configure NAS-IP RADIUS attribute with the virtual IP. For specific details on how to configure this setting, consult Aruba documentation.

Model Controllers in FortiNAC for Active/Passive Configuration

- Create one model using the **virtual IP**. See [Model the Device](#) for instructions. Since only one controller is active at once, FortiNAC only needs to know about the virtual IP.
- Create a pingable model for each of the controllers. FortiNAC needs to recognize the source IP address of the RADIUS request in order to trust it, therefore, a pingable model must exist for each controller's physical IP address.
 1. Click **Network Devices > Topology**.
 2. Expand the desired Container icon.
 3. Right-click the desired container (such as Wireless Controllers), and select "Add Pingable Device."
 4. Populate the Name, the (physical) IP address of the controller, and Physical Address.
 5. Set Device Type to **Wireless Access Point**.
 6. Click **OK**.

Note: Although the controller is accessed using the virtual IP for session and other device queries, controllers with this configuration continue to source RADIUS authentication requests using their physical interface IPs rather than the virtual IP. Since FortiNAC needs to recognize the source IP of an authentication request in order to trust it, a pingable model must exist for each of the physical IPs, and the authentication packet must identify the virtual IP in the NAS-IP RADIUS attribute. This way, FortiNAC will accept the request from the source but use the NAS-IP attribute to look up the actual controller model for the FortiNAC configuration values.

Aruba Wireless Network Options

Before setting up the Aruba controller to integrate with FortiNAC, review the scenarios listed below to determine the configuration that best suits your environment. These include:

- Use of VLANs Only
- Use of [Aruba Roles mapped to multiple VLANs](#)
- Use of [Aruba Roles all mapped to a single VLAN](#)
- Use the [Aruba Controller as an in-line device](#)
- Use of [Aruba Server Derivation Rules](#) to determine Aruba Roles on the controller

VLANs Only

In this scenario VLANs are used to control network access. The PEF license is not required. No Aruba roles are configured. This is a very basic configuration.

On the Aruba controller, 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).

If you choose to control network access using only VLANs, in the FortiNAC model configuration of the controller, you would select the **L2 VLANs only** option. See [Device Model Configuration](#) for details.

In this configuration, when a host connects to the network the controller sends a RADIUS authentication request to FortiNAC. FortiNAC sends a RADIUS response that contains the VLAN assignment. This forces the host to automatically disassociate or disconnect for each state/VLAN change causing a delay while a new IP address is issued.

Table 1: VLANs Only Sample Configuration

	Aruba Role	Network VLAN	DHCP Server	Redirect Method	Transition Method
Registration		10	FortiNAC	DNS Wildcard	Blacklist
Authentication		20	FortiNAC	DNS Wildcard	Blacklist
Quarantine		30	FortiNAC	DNS Wildcard	Blacklist
Dead-End		40	FortiNAC	DNS Wildcard	Blacklist
Staff		100	Customer	N/A	Blacklist
Admin		200	Customer	N/A	Blacklist
Guests		300	Customer	N/A	Blacklist

Roles With VLANs

In this scenario, roles are configured on the controller and each role is associated with a VLAN or VLAN pool (see [VLAN Pools under Considerations](#)).

Each role can have its own VLAN or some roles can share VLANs. The key differentiating factor with this configuration is that at least one role is associated with a VLAN that is different than all of the other roles. When VLANs are used as the control mechanism for access to the network, the host is forced to renew its IP address when the host is moved from one VLAN to another, such as from Isolation to Production. As with VLAN only mode, this mode employs session blacklisting to disassociate sessions during state transitions to facilitate the acquisition of a new IP address.

On the Aruba controller, create Roles that correspond to the host states you wish to enforce. These include default (production) and isolation states including: registration, quarantine, authentication, and dead-end (disabled). Associate each role with a VLAN.

If you choose to control network access using Roles with VLANs, in the FortiNAC model configuration of the controller, you would select the **L2 Roles with VLANs** option. See [Device Model Configuration](#) for details.

In this configuration, when a host connects to the network the controller sends a RADIUS authentication request to FortiNAC. FortiNAC sends a RADIUS response that contains the Role assignment.

Table 2: Roles With VLANs Sample Configuration

	Aruba Role	Network VLAN	DHCP Server	Redirect Method	Transition Method
Registration	Reg	10	FortiNAC	DNS Wildcard	Blacklist
Authentication	Auth	10	FortiNAC	DNS Wildcard	Blacklist
Quarantine	Quar	40	FortiNAC	DNS Wildcard	Blacklist
Dead-End	DE	40	FortiNAC	DNS Wildcard	Blacklist
Staff	Staff	200	Customer	N/A	Blacklist
Admin	Admin	200	Customer	N/A	Blacklist
Guests	Guest	300	Customer	N/A	Blacklist

All Roles Share the Same VLAN

In this scenario Firewall Policies or ACLs associated with Roles are used to control network access. Unlike the previous modes, the host retains the same IP address throughout the session.

When hosts are placed into a Role configured for an isolation state (i.e..Registration, Quarantine, etc.) the controller must force user web access to the FortiNAC Captive Portal. When using VLANs, this is accomplished through DNS redirection where wireless hosts in an isolation state are provided a FortiNAC interface as their DNS server address within their DHCP assignment.

When all roles share a single VLAN, it is still possible to provide connecting hosts with a FortiNAC interface address as one of the DNS servers returned from DHCP. However, it is not the best solution because many handheld devices support only two DNS addresses. When sharing a single VLAN, a better method of redirecting web access to FortiNAC's captive portal is to use Aruba's DST-NAT feature.

DST-Nat can be configured in either of two ways. If you need to allow hosts to access other sites for remediation purposes, such as AV/AS updates, you must redirect DNS Traffic to FortiNAC. Do this by using DST-Nat to redirect all DNS traffic to the FortiNAC isolation interface. If your hosts would never need to be redirected to any destination other than FortiNAC, use DST-Nat to redirect only HTTP traffic to FortiNAC.

Configuration

- Create a Role for each host state you wish to enforce. These include default (production) and isolation states including: registration, quarantine, authentication, and dead-end (disabled).
- Configure a production IP Interface/VLAN. For this interface enable Inter- VLAN Routing and assign a static IP address and mask. Associate each role with the same VLAN.
- Create Firewall Policies or ACLs that control access to the network and associate policies with the appropriate role.
- If you choose to control network access by associating all Roles with the same VLAN, in the FortiNAC model configuration of the controller, you would select the **L2 Roles only**. See [Device Model Configuration](#) for details.

Table 3: Roles With A Single VLAN Sample Configuration

	Aruba Role	Network VLAN	Redirect Method	Transition Method
Registration	Reg	10	DST-Nat	Direct Role Change
Authentication	Auth	10	DST-Nat	Direct Role Change
Quarantine	Quar	10	DST-Nat	Direct Role Change
Dead-End	DE	10	DST-Nat	Direct Role Change
Staff	Staff	10	DST-Nat	Direct Role Change
Admin	Admin	10	DST-Nat	Direct Role Change
Guests	Guest	200	DST-Nat	Direct Role Change

Wired Hosts

With the controller configured with all roles in the same VLAN, you can manage hosts that connect to the controller via a wired port. These hosts authenticate through RADIUS and are managed using the same process as a wireless host. However, the VLAN assigned to the port must be the same VLAN associated with the host role.

Controller As An In-line Device

Aruba controllers can be configured to pass through traffic from another device that is connected directly to the controller, such as a VPN concentrator. In this configuration, there is no RADIUS setup required. FortiNAC sees only a list of sessions and IP addresses but does not see the MAC addresses of connecting hosts. The IP addresses used must be configured on the connecting device (e.g. the VPN), then Aruba rules control that series of IP addresses.

Each physical port on the controller can be trusted or untrusted. If the port is trusted, the traffic just passes through. If the port is untrusted, firewall rules are applied based on the role applied to the session. A default role can be set.

Initially, FortiNAC has no mechanism to set the role because it does not have any user data. VPN web pages in Fortinet's Captive portal are used to force the user to download the agent and run it on the host. The agent returns the MAC address to FortiNAC. This allows FortiNAC to identify the host machine, determine its state and whether the host should be isolated or not.

If you choose to use the controller as an in-line device, you cannot use it for any other network traffic. In the FortiNAC model configuration of the controller, you would select the **L3 Roles only**. See [Device Model Configuration](#) for details.

Using Server Derivation Rules On Aruba Controllers

In some cases, you may want to determine the role of a connecting host based on the SSID on which they connect or some other criteria. The controller provides a powerful facility called Server Derivation Rules that has the ability to use several criteria to determine and assign roles for connecting hosts. To use this controller feature you must be familiar with the use of Server Derivation Rules.

To allow the controller to assign a role to a connecting host, FortiNAC properties files must be modified. These modifications enable the use of a different RADIUS attribute than the attribute normally used to transmit the host Role. The attribute sent must be modified since the default attribute returned by FortiNAC takes precedence over all other values. A common attribute replacement is the standard RADIUS Filter-ID attribute.

To send a role using the Filter-ID attribute, the following property file must be modified:
`/bsc/campusMgr/master_loader/properties_plugin/radiusDevice.properties`

Important: This property file is overwritten and changes are lost each time FortiNAC is upgraded. Therefore, make a backup copy of the file or be sure to change the properties file again after upgrade.

Contact Support for assistance.

Procedure

1. Login to the FortiNAC CLI as root.
2. Navigate to the `/bsc/campusMgr/master_loader/properties_plugin` directory.
3. Use an editor such as `vi` to open `radiusDevice.properties`.
4. Comment out the following lines:

```
// VSA definitions
com.bsc.plugin.packets.RadiusPacket.ARUBA.vendorCode=14823
com.bsc.plugin.packets.RadiusPacket.14823.vlan.vsa.role=1
com.bsc.plugin.packets.RadiusPacket.14823.vsaType.1.name
=ArubaUserRole
com.bsc.plugin.packets.RadiusPacket.14823.vsaType.1.dataType
=String
com.bsc.plugin.packets.RadiusPacket.14823.vlan.vsa.vlan=2
com.bsc.plugin.packets.RadiusPacket.14823.vsaType.2.name
=ArubaUserVlan
com.bsc.plugin.packets.RadiusPacket.14823.vsaType.2. dataType=Integer
```

5. Uncomment the following lines:

```
//com.bsc.plugin.packets.RadiusPacket.ARUBA.vendorCode=1
//com.bsc.plugin.packets.RadiusPacket.ARUBA.rfc.val.role=11
//com.bsc.plugin.packets.RadiusPacket.ARUBA.rfc.dataType.11.
role=String
//com.bsc.plugin.packets.RadiusPacket.ARUBA.rfc.val.vlan=11
//com.bsc.plugin.packets.RadiusPacket.ARUBA.rfc.dataType
.11.vlan=String
```

Note: Wrapping or line breaks displayed above are caused by the limited size of the page. Lines in the properties file do not break in the middle of the line. Do not introduce any line breaks as you are editing the file.

6. Save the changes to the file.

7. Restart FortiNAC using the following command:

```
restartCampusMgr
```

If you choose to use Server Derivation Rules, in the FortiNAC model configuration of the controller, you must determine which Operational Mode to select. If all Roles share the same VLAN in your Aruba controller configuration, select the **L2 Roles only**. If one or more Roles have different VLANs, select **L2 Roles with VLANs**. See [Device Model Configuration](#) for details.

Authentication Servers

Define FortiNAC as Authentication Server

On the Aruba controller define the FortiNAC Server or Control Server as the RADIUS authentication and accounting server for the Server Group you choose for SSIDs secured by FortiNAC.

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.

- Use the management (eth0) 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 and port 1813 for accounting.
- Enter the RADIUS secret for this server.
- Add the RADIUS Server to a Server Group.

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.

Configure Client Disconnect Method

- **Tunnel Mode:** Recommended to configure **RFC 3576** for disconnection and Change of Authorization (CoA).
 - Add FortiNAC's eth0 IP address of the primary control server to the RFC 3576 server list on the Aruba controller under **AAA Profiles**.
 - Ensure the RADIUS secret for this server (must be identical to the secret configured above) under the **Auth Servers** section. **Note:** If the secret is incorrect, the CoA process will fail and the client will not disconnect.
- **Bridge Mode:** Aruba does not support CoA in Bridge Mode. FortiNAC must disconnect clients using CLI commands.
 - Ensure the Aruba controller's device model configuration has SSH account specified with write permissions.
 - Refer to the following link for information on Aruba unsupported mode features:

https://www.arubanetworks.com/techdocs/ArubaOS_85_Web_Help/Content/arubaos-solutions/behavior-defaults/unde-mode-supp.htm?Highlight=bridge%20mode

Authentication

Two forms of authentication are supported by FortiNAC: MAC Authentication and 802.1x. On the Aruba Wireless Controller, the authentication method is configured within an AAA Profile. Once you have configured one of the authentication methods below, associate that method with an AAA Profile.

- For MAC Authentication, create a MAC Authentication Profile and associate it with the Server Group you created in the previous section.
- For 802.1x Authentication, create an 802.1x Profile. You must also configure the necessary EAP types and encryption settings. Associate the profile with the Server Group created in the previous section.
- For RADIUS Accounting, associate the profile with the Server Group created in the previous section.
- For the RFC 3576 server, select the RFC server described in the previous section.

RAP Wired Port Integration

Fortinet supports management of end-stations connected to the wired ports on certain Aruba APs (e.g., RAP-3WNP). End-stations are managed much the same as wireless stations. The ports must be configured to send RADIUS authentication to FortiNAC (MAC-Authentication or 802.1x).

To find these configurations on compatible Aruba controllers, do the following:

1. Go to **Configurations > AP Configuration**, and then select an AP group.
2. Expand the **AP** section to display the list of ethernet interfaces for the APs.
3. Expand an interface to display its configuration.

4. Select the appropriate profiles for port management.
5. Use the same AAA profile you configured for wireless communication with FortiNAC.

If configured correctly, you will receive a RADIUS authentication request when a station connects to the corresponding wired port on the AP(s).

Virtual AP

In the Aruba Wireless Controller, a Virtual AP contains the WLAN configuration. Create a Virtual AP, associate the AAA Profile that should be used for authentication and add an SSID Profile.

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.

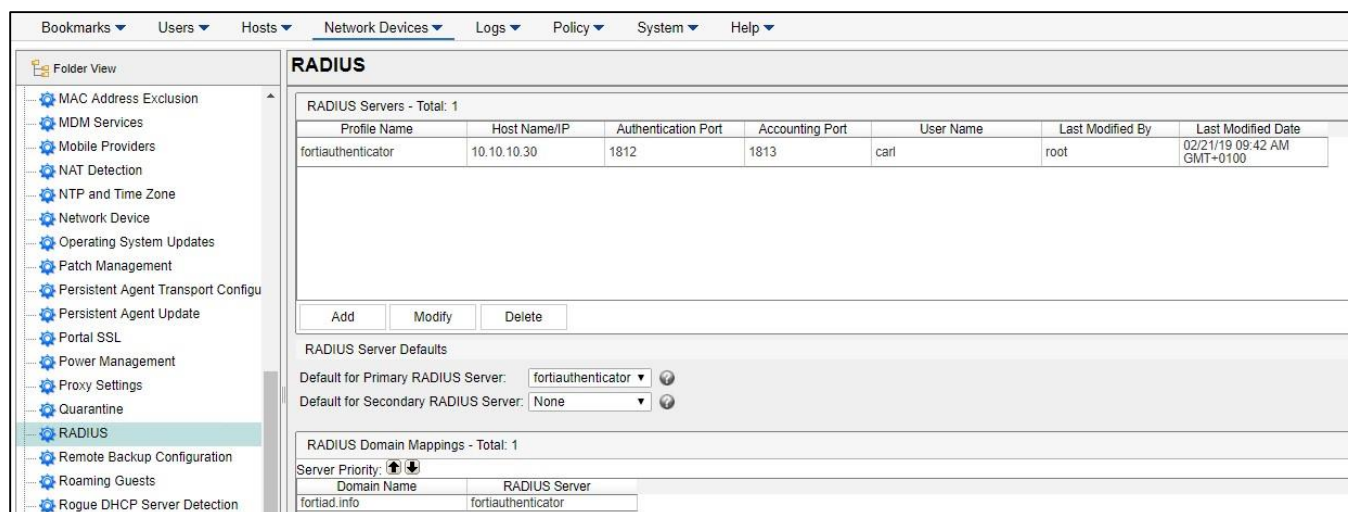
Configure FortiNAC

Note: Once connected to the network, APs will appear as rogue hosts in FortiNAC until they are identified by the controller as managed devices. As APs are identified, either as a result of device profiling or of AP discovery from a wireless device, the rogues will automatically be removed.

RADIUS Server (Required for 802.1x Authentication)

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. For instructions, see section [Configure RADIUS Settings](#) of the Administration Guide in the Fortinet Document Library.

Important: The RADIUS Secret used must be exactly the same on the RADIUS server.



The screenshot shows the FortiNAC administration console with the RADIUS configuration page. The left sidebar contains a folder view with various settings categories. The main content area is titled 'RADIUS' and displays the following information:

- RADIUS Servers - Total: 1**
- Table with columns: Profile Name, Host Name/IP, Authentication Port, Accounting Port, User Name, Last Modified By, Last Modified Date.
- Buttons: Add, Modify, Delete.
- RADIUS Server Defaults**
- Default for Primary RADIUS Server: fortiauthenticator
- Default for Secondary RADIUS Server: None
- RADIUS Domain Mappings - Total: 1**
- Server Priority: (up/down arrows)
- Table with columns: Domain Name, RADIUS Server.

Note: FortiNAC does not proxy RADIUS requests when using MAC authentication.

Model the Device

1. Navigate to **Network Device > Topology**
2. Discover or add all devices to be managed. See section [Add or modify a device](#) or [Discovery](#) of the **Administration Guide** in the Fortinet Document Library for instructions.

SNMP Settings: SNMP v1 or v3 credentials

Note: If a “?” appears as the icon, then support needs to be added for that device. See KB article [Options for Devices Unable to Be Modeled in Topology](#) for instructions.

3. Click the **Polling** tab in the right panel of the model.
4. Set **L2 (Hosts) Polling** to 10 minutes. And click **Save**.

Device Model Configuration

To manage a device, the FortiNAC software must have a model of the device in its database.

1. After modeling the device in the Topology View, right-click on the model and click **Model Configuration**.
2. Select the **Operational Mode** for this device. See the field definitions in the following table for information on the options in this field.
3. Fill in the fields as appropriate:
 - **User Name** used for CLI access
 - **Password** used for CLI access
 - **Protocol** used for CLI access
 - **Primary RADIUS Server (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.
 - **Secondary RADIUS Server (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.
 - **RADIUS Secret**: Required for both MAC and 802.1x authentication. Must match the value entered on the device itself and the value entered on the RADIUS settings window.
4. To enable **RFC 3576 (5176)** support, select the **Enable rfc5176 support** checkbox. Setting this value enables the use of both RADIUS Disconnect and RADIUS Change Of Authorization (CoA) requests depending on the Aruba model being used (“L2 Roles with VLANs” and “L2 Roles Only” respectively).
5. In the **Network Access** section, click the **Read VLANs** or **Read Roles** button. This populates the drop-down lists for the different connection states, such as Registration. Data in the drop-down lists represents the roles or VLANs created on the device.
6. Select a setting in **Access Enforcement** for each host state.
7. In the **Access Value** column select a Role or VLAN for each host state desired to enforce.
8. In the **Preferred Container** field, select the Container in Topology which the Wireless Access Points should be placed as they are discovered.
9. Click **Apply**.

Table 4: Aruba Model Configuration Field Definitions

Field	Definition
Device Operational Mode	
Operational Mode	<p>The Aruba controller can be configured in one of several ways to manage hosts connecting through it. These are represented in the Operational Modes selection of the Model Configuration.</p> <p>L2 Roles with VLANs — Represents an Aruba configuration that uses Roles on the controller to manage connecting users. Each Role is assigned to a VLAN or VLAN pool (see VLAN Pools under Considerations). When configured in this fashion, users who are moved between different Roles by FortiNAC are assumed to be placed into different networks, thus requiring them to obtain a new IP address for each Role. To ensure that hosts who are moved between Roles by FortiNAC correctly obtain a new IP address, it is necessary to temporarily sever their network connection. This process ensures a successful transition into the new network, however it also adds to the time required for the user to be functional in the new Role.</p> <p>L2 Roles only — Represents an Aruba configuration that utilizes Roles on the controller to manage connecting users where all the affected Roles belong to the same VLAN. When configured in this way, users who are moved between different Roles by FortiNAC are assumed to always belong to the same network and maintain their IP address throughout their entire connection. Because users never change networks, it is not necessary to disconnect them from the network during the Role transition, which allows for a smoother Role transition experience.</p> <p>L2 VLANs only — Represents an Aruba configuration that utilizes VLANs on the controller rather than Roles to manage connecting users. When configured this way, Roles either do not exist or are not used. This operates similarly to L2 Roles with VLANs in that changes between states represent a change of network and therefore an IP address re-assignment. Therefore, disconnecting the host from the network is necessary here for the same reasons as given above.</p> <p>L3 Roles only — Represents an Aruba controller that is being dedicated for use as an in-line point of access control device. This can be used in situations where downstream devices (either local or remote access) are not visible and manageable by FortiNAC. Hosts in this case are managed at the controller which is their point of access to the secured network. Controllers configured in this way must be dedicated to this mode and cannot be used for other wired or wireless traffic.</p>
General	
User Name	A valid user name used by FortiNAC to log onto the device via SSH for automated configuration purposes.
Password	A password for the given user name.
Enable Password	<p>An enable password for the device to allow privileged access.</p> <p>Note: The enable password is required for FortiNAC to successfully read roles from the device.</p>
RADIUS	

Field	Definition
Primary Server	Used only for 802.1x authentication. 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. See RADIUS Settings in the Help system for information on configuring your RADIUS Servers.
Secondary Server	Used only for 802.1 authentication. 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.
RADIUS Secret	Used for both 802.1x and Mac authentication. The Secret used for RADIUS authentication. Click the Modify button to change the RADIUS secret. 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	
Note: The Operational Mode selected above determines whether these fields represent Roles or VLANs.	
Read Roles From Device	Retrieves roles that currently exist on the device being configured. These roles are the names of the User Profiles created when you configured VLANs/Profiles on the device. Each VLAN is associated with a User Profile, represented on this window as a Role.
Default	The Default Role or VLAN value to be used for a connecting host when the host is not in an isolation state and the Role or VLAN is not determined by another method, such as a user, host or device role. Typically, if a Role or VLAN is specified as the Default, it is the Role VLAN used for "normal" or "production" network access. If you have selected the L2 Roles only operational mode, you must specify a Default Role. This indicates the role to which a known registered host should be assigned. For the L2 Roles with VLANs or VLANs only modes, the default may be left blank. This will cause FortiNAC to generate a RADIUS reply without contributing a Role or VLAN value. This is used in situations where either a terminating RADIUS server may use its own rules to contribute a value to the response, or where you want the controller to make the decision, such as when using Server Derivation Rules to calculate a Role for a session.
Registration	The registration VLAN or Role for this device. Isolates unregistered hosts from the production network during host registration.
Authentication	The authentication VLAN or Role for this device. Isolates registered hosts from the Production network during user authentication. Optional.
Dead End	The dead end VLAN or Role for this device. Isolates disabled hosts by providing limited network connectivity.

Field	Definition
Quarantine	The quarantine VLAN or Role 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	<p>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:</p> <p>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.</p> <p>Note: Endpoints that have been denied access may continuously request access which can unnecessarily consume system resources.</p> <p>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.</p> <p>Enforce — Indicates that the host will be placed in the VLAN/Role specified in the Access Value column for this state.</p>
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	<p>Aruba controllers centralize management for lightweight Access Points attached throughout a network. These lightweight APs are not directly manageable by FortiNAC. However, they are discovered from modeled controllers and models are created for them in the FortiNAC device topology. This is done for several reasons. First, since APs are attached to network switches throughout the network, they often show up as rogue hosts when the switches are polled for hosts, until they are known. To ensure that the switch ports do not end up being switched to an isolation network under these conditions, it is important to recognize that it is a legitimate network device that is connected. Therefore, APs that are read from the controller are automatically created as devices in the Topology View. Additionally, APs can be used to create Role mappings within FortiNAC to be used in the Role determination logic. This allows you to configure FortiNAC to assign hosts that connect to different APs to different roles based on those APs.</p> <p>Since device models are created by the system for the APs, this Container name indicates where in the Topology View the devices will be created. Enter the name of the Container in which these Wireless Access Points should be stored.</p> <p>Containers are created in the Topology View to group devices.</p>

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 Overview](#) in the Fortinet Document Library.

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.

Port Groups

When modeling mobility controller devices within FortiNAC, it is recommended that you remove all the ports where the device and its managed APs will be connected from the "Forced Registration", "Forced Remediation", and "Forced Authentication" groups. Connecting controller-managed unregistered APs to those ports will result in rogue clients being created in the database that will later be converted to device models after reading the list of managed Access Points from the controller. If those ports are left in any of the previously mentioned port groups, the APs will end up in the isolation VLAN associated with the policy and will not have connectivity to their controller. If the controller cannot communicate with an AP, the AP will not be discovered and created. Once a model exists for the AP, the ports can be placed into any of the forced isolation groups to subsequently protect those ports.

Prevent SSID Removal After Failed Read

If FNAC fails to read the SSIDs of an AP or controller, the existing SSIDs already associated with the device model are deleted (consequently removing SSID configuration and group membership). To prevent this from occurring, run the following command in the CLI (Note: This attribute is not set by default). Contact Support for assistance.

```
device -ip <devip> -setAttr -name PreserveSSIDs -value true
```

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 or Roles

If you have modified the device configuration by adding or removing VLAN or Role definitions, it is recommended that you read the 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 **Model Configuration**.
4. Click **Read VLANs** or **Read Roles**. This resynchronizes the FortiNAC software and the device configuration.

Aruba Logon Lifetime Parameter

Aruba wireless controllers have a preset `logon_lifetime` parameter that controls the amount of time the user remains authenticated on the controller after the client stops communicating, such as when the user disconnects from the network. The default setting for this parameter is 5 minutes.

The Logon Lifetime parameter is configurable. Results in FortiNAC will vary depending on the length of time set. You may want to change this setting depending on how you are using FortiNAC. For example, if you are doing testing you may want to set this to 0 minutes but for everyday use you may want to leave the default setting of 5 minutes.

If the time is set to the default of 5 minutes and a user disconnects and reconnects to the network in less than five minutes, the controller allows that user to go back on the network without re-authenticating. FortiNAC will not be aware that this has occurred and will not show the disconnect and subsequent reconnect. If the host has been manually deleted or aged out of the database for testing purposes, the host displays as an unmanaged rogue in FortiNAC. FortiNAC is not aware of that the host has reconnected because no authentication request was received.

If the time is set to 0 minutes, when users disconnect and reconnect to the network or stop communicating, they may need to re-authenticate. The need to re-authenticate frequently may cause a poor user experience. Additional authentication requests will be sent to FortiNAC resulting in more traffic. On a large network with many controllers additional traffic could cause a degradation of service.

Appendix

Aruba 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.

This configuration applies to Alcatel Wireless devices as well.

Sample Configuration Using Firewall Rules

```
version 3.4
enable secret
"d85e6b8d016f7aad463fe61d0140b832ee59fed7d1f6dbed18"
prompt ArubaMaster
login session timeout 60
hostname "ArubaMaster"
clock summer-time EDT recurring 2 sunday march 02:00 first
sunday november 02:00 -4
clock timezone EST -5
location "IT Lab"
mms config 0
controller config 1201
crypto-local pki ServerCert arubacontroller2009
arubacontrollerkey2009a.pem
ip access-list eth validuser
permit any
!
net service svc-snmp-trap udp 162
net service "Accounting-4610 to 4625" tcp 4610 4625
net service svc-smb-tcp tcp 445
net service svc-ike udp 500
net service svc-l2tp udp 1701
net service svc-syslog udp 514
net service svc-dhcp udp 67 68 alg dhcp
net service svc-https tcp 443
net service svc-pptp tcp 1723
```

```
netSERVICE svc-Pharos-LPD tcp 515
netSERVICE svc-telnet tcp 23
netSERVICE svc-sccp tcp 2000 alg sccp
netSERVICE Accounting-Dept-2000 tcp 2000 2001
netSERVICE svc-tftp udp 69 alg tftp
netSERVICE svc-sip-tcp tcp 5060
netSERVICE svc-kerberos udp 88
netSERVICE svc-pop3 tcp 110
netSERVICE svc-adp udp 8200
netSERVICE svc-cfgm-tcp tcp 8211
netSERVICE svc-noe udp 32512 alg noe
netSERVICE svc-http-proxy3 tcp 8888
netSERVICE Accounting-Dept tcp 1030 1031
netSERVICE "LabAdmin 40000s" tcp 40000 40200
netSERVICE svc-msrpc-tcp tcp 135 139
netSERVICE svc-rtsp tcp 554 alg rtsp
netSERVICE svc-dns udp 53 alg dns
netSERVICE svc-vocera udp 5002 alg vocera
netSERVICE svc-h323-tcp tcp 1720
netSERVICE svc-h323-udp udp 1718 1719
netSERVICE svc-http tcp 80
netSERVICE svc-nterm tcp 1026 1028
netSERVICE svc-sip-udp udp 5060
netSERVICE svc-http-proxy2 tcp 8080
netSERVICE svc-Pharos-Notify tcp 28201 28207
netSERVICE svc-papi udp 8211
netSERVICE svc-noe-oxo udp 5000 alg noe
netSERVICE svc-ftp tcp 21 alg ftp
netSERVICE svc-natt udp 4500
netSERVICE svc-Pharos-SignUp tcp 2351 2355
netSERVICE svc-svp 119 alg svp
netSERVICE svc-gre 47
netSERVICE svc-smtp tcp 25
netSERVICE LabAdmin tcp 1111
netSERVICE "Dept - 4625" tcp 4625
```



```
netSERVICE svc-smb-udp udp 445
netSERVICE svc-sips tcp 5061 alg sips
netSERVICE svc-esp 50
netSERVICE svc-bootp udp 67 69
netSERVICE svc-snmp udp 161
netSERVICE svc-v6-dhcp udp 546 547
netSERVICE svc-icmp 1
netSERVICE svc-ntp udp 123
netSERVICE svc-msrpc-udp udp 135 139
netSERVICE svc-ssh tcp 22
netSERVICE Accounting-Dept-4600 tcp 4600 4601
netSERVICE svc-http-proxy1 tcp 3128
netSERVICE svc-v6-icmp 58
netdestination cm-dns
host 192.20.130.100
host 192.20.190.100
!
netdestination PrivateNet
network 192.0.0.0 255.0.0.0
network 192.168.0.0 255.255.0.0
network 172.16.0.0 255.240.0.0
!
netdestination ProtectedServers
host 192.3.0.6
host 192.3.0.7
host 192.3.1.28
!
ip access-list session control
user any udp 68 deny
any any svc-icmp permit
any any svc-dns permit
any any svc-papi permit
any any svc-cfgm-tcp permit
any any svc-adp permit
any any svc-tftp permit
```

```
any any svc-dhcp permit
any any svc-natt permit
!
ip access-list session ChemLab
any any LabAdmin permit
any any "LabAdmin 40000s" permit
any any udp 1111 permit
!
ip access-list session validuser
any any any permit
!
ip access-list session vocera-acl
any any svc-vocera permit queue high
!
ip access-list session icmp-acl
any any svc-icmp permit
!
ip access-list session Secure
any alias ProtectedServers any deny log
any any any permit
!
ip access-list session captiveportal
user alias mswitch svc-https dst-nat 8081
user any svc-http dst-nat 8080
user any svc-https dst-nat 8081
user any svc-http-proxy1 dst-nat 8088
user any svc-http-proxy2 dst-nat 8088
user any svc-http-proxy3 dst-nat 8088
!
ip access-list session allowall
any any any permit
!
ip access-list session SecureExecutive
any alias ProtectedServers any deny log
any any any permit
```

```
!  
ip access-list session cm-dns-block  
any alias cm-dns svc-dns deny  
any any svc-dns permit  
!  
ip access-list session https-acl  
any any svc-https permit  
!  
ip access-list session sip-acl  
any any svc-sip-udp permit queue high  
any any svc-sip-tcp permit queue high  
!  
ip access-list session cm-dns-allow  
any alias cm-dns svc-dns permit  
any any svc-dns deny  
!  
ip access-list session dns-acl  
any any svc-dns permit  
!  
ip access-list session tftp-acl  
any any svc-tftp permit  
!  
ip access-list session skinny-acl  
any any svc-sccp permit queue high  
!  
ip access-list session srcnat  
user any any src-nat  
!  
ip access-list session vpnlogon  
user any svc-ike permit  
user any svc-esp permit  
any any svc-l2tp permit  
any any svc-pptp permit  
any any svc-gre permit  
!
```

```
ip access-list session logon-control
user any udp 68 deny
any any svc-icmp permit
any any svc-dns permit
any any svc-dhcp permit
any any svc-natt permit
!
ip access-list session cplogout
user alias mswitch svc-https dst-nat 8081
!
ip access-list session guest
!
ip access-list session http-acl
any any svc-http permit
!
ip access-list session dhcp-acl
any any svc-dhcp permit
!
ip access-list session BlockRogueDHCP
user any udp 68 deny
!
ip access-list session noe-acl
any any svc-noe permit queue high
!
ip access-list session svp-acl
any any svc-svp permit queue high
user host 224.0.1.116 any permit
!
ip access-list session ap-acl
any any svc-gre permit
any any svc-syslog permit
any user svc-snmp permit
user any svc-snmp-trap permit
user any svc-ntp permit
!
```

```

ip access-list session TechAccounting
any any svc-telnet permit
any any Lirary-Dept permit
any any Accounting-Dept-2000 permit
any any svc-snmp-trap permit
any any "Accounting-4610 to 4625" permit
!
ip access-list session TechPrint
any host 192.3.1.192 svc-http permit
any any svc-Pharos-SignUp permit log
any any svc-Pharos-Notify permit log
any any svc-Pharos-LPD permit log
!
ip access-list session BASS
any host 192.3.1.11 svc-http-proxy2 permit
!
ip access-list session h323-acl
any any svc-h323-tcp permit queue high
any any svc-h323-udp permit queue high
!
ip access-list session TechGuest
any any svc-dns permit
any any svc-dhcp permit
any alias PrivateNet any deny log
any any any permit
!
ipv6 access-list session v6-icmp-acl
any any svc-v6-icmp permit
!
ipv6 access-list session v6-https-acl
any any svc-https permit
!
ipv6 access-list session v6-control
user any udp 68 deny
any any svc-v6-icmp permit

```

```
any any svc-v6-dhcp permit
any any svc-dns permit
any any svc-tftp permit
!
ipv6 access-list session v6-dhcp-acl
any any svc-v6-dhcp permit
!
ipv6 access-list session v6-dns-acl
any any svc-dns permit
!
ipv6 access-list session v6-allowall
any any any permit
!
ipv6 access-list session v6-http-acl
any any svc-http permit
!
ipv6 access-list session v6-tftp-acl
any any svc-tftp permit
!
ipv6 access-list session v6-logon-control
user any udp 68 deny
any any svc-v6-icmp permit
any any svc-v6-dhcp permit
any any svc-dns permit
!
vpn-dialer default-dialer
ike authentication PRE-SHARE
195cc8274528de580a34ac6b7686dcd474a13c386373fb99
!
user-role ap-role
session-acl control
session-acl ap-acl
!
user-role DeadEnd
session-acl BlockRogueDHCP
```

```
!  
user-role Secure  
session-acl BlockRogueDHCP  
session-acl cm-dns-block  
session-acl Secure  
!  
user-role Registration  
session-acl BlockRogueDHCP  
session-acl cm-dns-allow  
session-acl allowall  
!  
user-role trusted-ap  
session-acl allowall  
!  
user-role default-vpn-role  
session-acl allowall  
ipv6 session-acl v6-allowall  
!  
user-role Quarantine  
session-acl BlockRogueDHCP  
session-acl cm-dns-allow  
session-acl allowall  
!  
user-role SecureExecutive  
session-acl BlockRogueDHCP  
session-acl cm-dns-block  
session-acl SecureExecutive  
!  
user-role voice  
session-acl sip-acl  
session-acl noe-acl  
session-acl svp-acl  
session-acl vocera-acl  
session-acl skinny-acl  
session-acl h323-acl
```

```
session-acl dhcp-acl
session-acl tftp-acl
session-acl dns-acl
session-acl icmp-acl
!
user-role guest-logon
captive-portal "default"
session-acl logon-control
session-acl captiveportal
!
user-role guest
session-acl http-acl
session-acl https-acl
session-acl dhcp-acl
session-acl icmp-acl
session-acl dns-acl
ipv6 session-acl v6-http-acl
ipv6 session-acl v6-https-acl
ipv6 session-acl v6-dhcp-acl
ipv6 session-acl v6-icmp-acl
ipv6 session-acl v6-dns-acl
!
user-role stateful-dot1x
!
user-role authenticated
session-acl allowall
ipv6 session-acl v6-allowall
!
user-role stateful
session-acl control
!
user-role TechGuest_CM
session-acl BlockRogueDHCP
session-acl cm-dns-block
session-acl TechPrint
```



```
session-acl ChemLab
session-acl TechGuest
!
user-role SecureAdmin
session-acl BlockRogueDHCP
session-acl cm-dns-block
session-acl allowall
!
user-role logon
session-acl logon-control
session-acl captiveportal
session-acl vpnlogon
ipv6 session-acl v6-logon-control
!
user-role TechGuest
session-acl BlockRogueDHCP
session-acl cm-dns-block
session-acl TechPrint
session-acl ChemLab
session-acl TechGuest
!
ip radius source-interface loopback
!
aaa timers dead-time 2
no spanning-tree
interface mgmt
dhcp
!
interface loopback
ip address 192.70.192.13
!
dialer group evdo_us
init-string ATQ0V1E0
dial-string ATDT#777
!
```

```
dialer group gsm_us
init-string AT+CGDCONT=1,"IP","ISP.CINGULAR"
dial-string ATD*99#
!
dialer group vivo_br
init-string AT+CGDCONT=1,"IP","zap.vivo.com.br"
dial-string ATD*99#
!
vlan 192
vlan 221
vlan 222
vlan 223
vlan 224
vlan 225
vlan 226
vlan 227
vlan 228
vlan 231
vlan 232
vlan 233
vlan 234
vlan 235
vlan 236
vlan 237
vlan 238
vlan 333
vlan 444
vlan 911
vlan 999
vlan-name anslem pool
vlan anslem 221-228
interface gigabitethernet 0/0
description "GE0/0"
trusted
trusted vlan 1-4094
```

```
switchport mode trunk
no spanning-tree
!
interface gigabitethernet 0/1
description "GE0/1"
trusted
trusted vlan 1-4094
!
interface gigabitethernet 0/2
description "GE0/2"
trusted
trusted vlan 1-4094
!
interface gigabitethernet 0/3
description "GE0/3"
trusted
trusted vlan 1-4094
!
interface gigabitethernet 0/4
description "GE0/4"
trusted
trusted vlan 1-4094
!
interface gigabitethernet 0/5
description "GE0/5"
trusted
trusted vlan 1-4094
!
interface gigabitethernet 0/6
description "GE0/6"
trusted
trusted vlan 1-4094
!
interface gigabitethernet 0/7
description "GE0/7"
```

```
trusted
trusted vlan 1-4094
!
interface gigabitethernet 0/8
description "GE0/8"
trusted
trusted vlan 1-4094
!
interface gigabitethernet 0/9
description "GE0/9"
trusted
trusted vlan 1-4094
!
interface gigabitethernet 0/10
trusted
trusted vlan 1-4094
!
interface gigabitethernet 0/11
trusted
trusted vlan 1-4094
!
interface vlan 1
!
interface vlan 192
ip address 192.70.192.12 255.255.252.0
!
interface vlan 221
ip address 192.20.221.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 222
ip address 192.20.222.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 223
```

```
ip address 192.20.223.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 224
ip address 192.20.224.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 225
ip address 192.20.225.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 226
ip address 192.20.226.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 227
ip address 192.20.227.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 228
ip address 192.20.228.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 231
ip address 192.20.231.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 232
ip address 192.20.232.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 233
ip address 192.20.233.2 255.255.255.0
ip helper-address 192.3.1.37
!
```

```
interface vlan 234
ip address 192.20.234.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 235
ip address 192.20.235.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 236
ip address 192.20.236.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 237
ip address 192.20.237.2 255.255.255.0
ip helper-address 192.3.1.37
!
interface vlan 238
ip address 192.20.238.2 255.255.255.0
ip helper-address 192.3.1.37
!
vrrp 165
priority 110
authentication aruba
ip address 192.70.192.16
description "MasterPrimary"
vlan 192
preempt
no shutdown
!
vrrp 166
authentication aruba
ip address 192.70.192.17
description "LocalPrimary"
vlan 192
preempt
```

```
!  
ip default-gateway 192.70.192.1  
ap mesh-recovery-profile cluster Recovery-gV-3AZLbc-bbo+5  
wpa-hexkey  
07b466a81428afd382a1c22dc0fd6fdf8bae046f19f89d7ef511537c4082  
0727a12e  
042962fcff6a348830b9618171d2ffb2bf5fa7f40813f687876a12ad07d5  
a52f83d5  
d4bfd8e9c83f0854e00d450d  
  
wms  
general poll-interval 60000  
general poll-retries 3  
general ap-ageout-interval 30  
general sta-ageout-interval 30  
general learn-ap disable  
general persistent-known-interfering enable  
general propagate-wired-macs enable  
general stat-update enable  
general collect-stats disable  
!  
crypto isakmp policy 20  
encryption aes256  
!  
crypto isakmp key  
"aac98ba6f2bb9a92a0c8b4023e6d23065fcd47a8dc508a54" address  
0.0.0.0 netmask 0.0.0.0  
crypto ipsec transform-set default-aes esp-aes256 esp-sha-  
hmac  
crypto dynamic-map default-dynamicmap 10000  
set transform-set default-transform default-aes  
!  
localip 0.0.0.0 ipsec  
f595067b48ac1e12ae7840bd5f2ba84c2a497571632b510d  
localip 192.70.192.15 ipsec  
577e1271980e8a1d0715645a16751fe85026eb0674619a83  
ip local pool "RAP-pool" 192.90.1.3 192.90.1.254  
vpdn group l2tp  
!
```

```
ip dhcp default-pool private
!
syslocation "IT Lab"
snmp-server community Fortinet
vpdn group pptp
!
mux-address 0.0.0.0
adp discovery enable
adp igmp-join enable
adp igmp-vlan 0
voip prioritization disable
voip rtcp-inactivity disable
voip sip-midcall-req-timeout disable
ssh mgmt-auth username/password
mgmt-user admin root
07ea2ecd010712fb4c1470a58dcbfdc5c4cf335b506ce875b6
ntp server 192.3.1.37
no database synchronize
database synchronize rf-plan-data
ip mobile domain default
!
ip igmp
!
no firewall attack-rate cp 1024
!
firewall cp
!
firewall cp
packet-capture-defaults tcp disable udp disable sysmsg
disable other disable
!
ip domain lookup
!
country US
aaa authentication mac "CMmacAuth"
```



```

delimiter colon
!
aaa authentication mac "default"
!
aaa authentication dot1x "Tech_802.1x"
termination enable
termination eap-type eap-peap
termination inner-eap-type eap-mschapv2
server-cert "arubacontroller2009"
!
aaa authentication dot1x "default"
!
aaa authentication-server radius "Tech_IAS"
host 192.3.1.37
key f865d7ba8915205eb12773b41b502a7cd3798492ee759176
!
aaa authentication-server radius "CAMPUSMANAGER"
host 192.3.1.105
key 8dea4674f0e0ce9928fdda605609020d5d0104f9126c83ac
!
aaa server-group "Tech_Server_Group"
auth-server Tech_IAS
set role condition Filter-Id equals "ExecutiveDL" set-value
Secure
set role condition Filter-Id equals "StaffDL" set-value
Secure
set role condition Filter-Id equals "WirelessAdminDL" set-
value SecureAdmin
!
aaa server-group "CMServerGroup"
auth-server CAMPUSMANAGER
!
aaa server-group "default"
auth-server Internal
set role condition role value-of
!

```

```
aaa profile "Tech_Guest_AAA"
initial-role "TechGuest"
mac-default-role "TechGuest"
!
aaa profile "Tech_Guest_CM_AAA"
initial-role "Quarantine"
authentication-mac "CMmacAuth"
mac-default-role "TechGuest_CM"
mac-server-group "CMServerGroup"
!
aaa profile "Tech_Secure_AAA"
authentication-dot1x "Tech_802.1x"
dot1x-default-role "SecureExecutive"
dot1x-server-group "Tech_Server_Group"
!
aaa profile "default"
!
aaa authentication captive-portal "default"
!
aaa authentication wispr "default"
!
aaa authentication vpn
server-group "internal"
!
aaa authentication mgmt
!
aaa authentication stateful-ntlm "default"
!
aaa authentication stateful-dot1x
!
aaa authentication wired
!
web-server
switch-cert "arubacontroller2009"
!
```

```
papi-security
!
guest-access-email
!
aaa password-policy mgmt
!
ap system-profile "default"
!
ap system-profile "LocalFirst"
lms-ip 192.70.192.17
!
ap system-profile "MasterFirst"
lms-ip 192.70.192.16
!
ap system-profile "RemoteAP"
lms-ip 66.155.211.15
!
ap regulatory-domain-profile "default"
country-code US
valid-11g-channel 1
valid-11g-channel 6
valid-11g-channel 11
valid-11a-channel 36
valid-11a-channel 40
valid-11a-channel 44
valid-11a-channel 48
valid-11a-channel 149
valid-11a-channel 153
valid-11a-channel 157
valid-11a-channel 161
valid-11a-channel 165
valid-11g-40mhz-channel-pair 1+
valid-11g-40mhz-channel-pair 5-
valid-11g-40mhz-channel-pair 7+
valid-11g-40mhz-channel-pair 11-
```

```
valid-11a-40mhz-channel-pair 36+
valid-11a-40mhz-channel-pair 40-
valid-11a-40mhz-channel-pair 44+
valid-11a-40mhz-channel-pair 48-
valid-11a-40mhz-channel-pair 149+
valid-11a-40mhz-channel-pair 153-
valid-11a-40mhz-channel-pair 157+
valid-11a-40mhz-channel-pair 161-
!
ap wired-ap-profile "default"
!
ap enet-link-profile "default"
!
ap mesh-ht-ssid-profile "default"
!
ap mesh-cluster-profile "TechMeshCluster1"
cluster "TechCluster1"
opmode wpa2-psk-aes
wpa-passphrase
cc4940f33598e1dded9ef2be7faaa0b3d01c7ba9c1852589
!
ap mesh-cluster-profile "TechMeshCluster2"
cluster "TechCluster2"
opmode wpa2-psk-aes
wpa-passphrase
ca4f03111febbcd97ca5e2df49bed22147d26f6d0a6f32f3
!
ap mesh-cluster-profile "default"
!
ap mesh-radio-profile "TechMeshRadio"
!
ap mesh-radio-profile "AcctMeshRadio"
!
ap mesh-radio-profile "default"
!
ap mesh-radio-profile "HodginsMeshRadio"
```

```

!
ap mesh-radio-profile "GordonMeshRadio"
!
ids general-profile "default"
!
ids unauthorized-device-profile "default"
!
ids profile "default"
!
rf arm-profile "default"
!
rf arm-profile "no_arm_enable_MeSh"
assignment disable
!
rf optimization-profile "default"
!
rf event-thresholds-profile "default"
!
rf dot11a-radio-profile "TechMeshRadio_MeSh"
no radio-enable
channel 165
tx-power 127
arm-profile "no_arm_enable_MeSh"
!
rf dot11a-radio-profile "AcctMeshRadio_MeSh"
no radio-enable
channel 40
tx-power 127
arm-profile "no_arm_enable_MeSh"
!
rf dot11a-radio-profile "default"
!
rf dot11a-radio-profile "default_MeSh"
no radio-enable
tx-power 127

```

```
arm-profile "no_arm_enable_MeSh"  
!  
rf dot11a-radio-profile "HodginsMeshRadio_MeSh"  
no radio-enable  
channel 36  
tx-power 127  
arm-profile "no_arm_enable_MeSh"  
!  
rf dot11a-radio-profile "mode_am"  
mode am-mode  
!  
rf dot11a-radio-profile "GordonMeshRadio_MeSh"  
no radio-enable  
channel 44  
tx-power 127  
arm-profile "no_arm_enable_MeSh"  
!  
rf dot11g-radio-profile "TechMeshRadio_MeSh"  
no radio-enable  
tx-power 127  
arm-profile "no_arm_enable_MeSh"  
!  
rf dot11g-radio-profile "AcctMeshRadio_MeSh"  
no radio-enable  
tx-power 127  
arm-profile "no_arm_enable_MeSh"  
!  
rf dot11g-radio-profile "default"  
no high-throughput-enable  
!  
rf dot11g-radio-profile "default_MeSh"  
no radio-enable  
tx-power 127  
arm-profile "no_arm_enable_MeSh"  
!
```

```
rf dot11g-radio-profile "HodginsMeshRadio_MeSh"  
no radio-enable  
tx-power 127  
arm-profile "no_arm_enable_MeSh"  
!  
rf dot11g-radio-profile "mode_am"  
mode am-mode  
!  
rf dot11g-radio-profile "GordonMeshRadio_MeSh"  
no radio-enable  
tx-power 127  
arm-profile "no_arm_enable_MeSh"  
!  
wlan dot11k-profile "default"  
!  
wlan voip-cac-profile "default"  
!  
wlan ht-ssid-profile "default"  
!  
wlan edca-parameters-profile station "default"  
!  
wlan edca-parameters-profile ap "default"  
!  
wlan ssid-profile "Tech_Guest_SSID"  
ssid "TechWZONE"  
mcast-rate-opt  
!  
wlan ssid-profile "Tech_Secure_SSID"  
ssid "TechWZONESecure"  
opmode wpa-tkip wpa2-aes  
mcast-rate-opt  
!  
wlan ssid-profile "default"  
!  
wlan ssid-profile "TEST-SSID"
```

```
    essid "TEST"
    !
    wlan virtual-ap "Tech_Guest_CM_VAP"
    aaa-profile "Tech_Guest_CM_AAA"
    ssid-profile "Tech_Guest_SSID"
    vlan 221-228
    multi-association
    vlan-mobility
    broadcast-filter arp
    band-steering
    !
    wlan virtual-ap "Tech_Guest_VAP"
    aaa-profile "Tech_Guest_AAA"
    ssid-profile "Tech_Guest_SSID"
    vlan 222-228
    multi-association
    vlan-mobility
    broadcast-filter arp
    band-steering
    !
    wlan virtual-ap "Tech_Guest_VAP_Mixed"
    aaa-profile "Tech_Guest_AAA"
    ssid-profile "Tech_Guest_SSID"
    vlan 444
    multi-association
    vlan-mobility
    broadcast-filter arp
    band-steering
    !
    wlan virtual-ap "Tech_Secure_VAP"
    aaa-profile "Tech_Secure_AAA"
    ssid-profile "Tech_Secure_SSID"
    vlan 231-238
    multi-association
    vlan-mobility
```



```

broadcast-filter arp
band-steering
!
wlan virtual-ap "default"
!
wlan traffic-management-profile "bandwidth_use"
shaping-policy fair-access
!
ap-group "Blue"
virtual-ap "Tech_Guest_CM_VAP"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "Area51"
virtual-ap "Tech_Secure_VAP"
virtual-ap "Tech_Guest_CM_VAP"
mesh-cluster-profile "TechMeshCluster1" priority 1
mesh-cluster-profile "TechMeshCluster2" priority 2
!
ap-group "Area_MeSh"
virtual-ap "Tech_Secure_VAP"
virtual-ap "Tech_Guest_CM_VAP"
dot11a-radio-profile "default_MeSh"
mesh-cluster-profile "TechMeshCluster1" priority 1
mesh-cluster-profile "TechMeshCluster2" priority 2
!
ap-group "Jones"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "LocalFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "Office-1st"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "LocalFirst"

```

```

!
ap-group "Kitchen"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "LocalFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "Smith"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "LocalFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "Acct"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "LocalFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "Acct Mesh"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "MasterFirst"
mesh-radio-profile "AcctMeshRadio"
mesh-cluster-profile "TechMeshCluster1" priority 1
mesh-cluster-profile "TechMeshCluster2" priority 2
!
ap-group "Acct Mesh_MeSh"
virtual-ap "Tech_Guest_CM_VAP"
dot11a-radio-profile "AcctMeshRadio_MeSh"
ap-system-profile "MasterFirst"
mesh-radio-profile "AcctMeshRadio"
mesh-cluster-profile "TechMeshCluster1" priority 1
mesh-cluster-profile "TechMeshCluster2" priority 2
!
ap-group "Elkins"

```

```

virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "LocalFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "default"
virtual-ap "default"
dot11a-radio-profile "mode_am"
dot11g-radio-profile "mode_am"
ap-system-profile "MasterFirst"
!
ap-group "Butterfly"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "MasterFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "Hodges"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "MasterFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "Hodgins Mesh"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "MasterFirst"
mesh-radio-profile "HodginsMeshRadio"
mesh-cluster-profile "TechMeshCluster1" priority 1
mesh-cluster-profile "TechMeshCluster2" priority 2
!
ap-group "Hodgins Mesh_MeSh"
virtual-ap "Tech_Guest_CM_VAP"
dot11a-radio-profile "HodginsMeshRadio_MeSh"
dot11g-radio-profile "mode_am"
ap-system-profile "MasterFirst"

```

```

mesh-radio-profile "HodginsMeshRadio"
mesh-cluster-profile "TechMeshCluster1" priority 1
mesh-cluster-profile "TechMeshCluster2" priority 2
!
ap-group "Francois"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "MasterFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "Accounting"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "MasterFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "NHTI"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "LocalFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "Open > Local-1st"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "LocalFirst"
!
ap-group "Open > Master-1st"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "MasterFirst"
!
ap-group "Open+Secure>Local-1st"
virtual-ap "Tech_Guest_CM_VAP"
virtual-ap "Tech_Secure_VAP"
ap-system-profile "LocalFirst"
!

```

```

ap-group "Fish"
virtual-ap "Tech_Secure_VAP"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "LocalFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "RemoteAP"
virtual-ap "Tech_Guest_VAP"
virtual-ap "Tech_Secure_VAP"
ap-system-profile "RemoteAP"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
!
ap-group "RemoteAPLocal"
virtual-ap "Tech_Guest_VAP"
virtual-ap "Tech_Secure_VAP"
ap-system-profile "LocalFirst"
!
ap-group "Engineering"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "LocalFirst"
!
ap-group "QA_Lab"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "MasterFirst"
!
ap-group "Gordon Mesh"
virtual-ap "Tech_Guest_CM_VAP"
ap-system-profile "MasterFirst"
dot11a-traffic-mgmt-profile "bandwidth_use"
dot11g-traffic-mgmt-profile "bandwidth_use"
mesh-radio-profile "GordonMeshRadio"
mesh-cluster-profile "TechMeshCluster1" priority 1
mesh-cluster-profile "TechMeshCluster2" priority 2

```

```
!  
ap-group "Gordon Mesh_MeSh"  
virtual-ap "Tech_Guest_CM_VAP"  
dot11a-radio-profile "GordonMeshRadio_MeSh"  
ap-system-profile "MasterFirst"  
dot11a-traffic-mgmt-profile "bandwidth_use"  
dot11g-traffic-mgmt-profile "bandwidth_use"  
mesh-radio-profile "GordonMeshRadio"  
mesh-cluster-profile "TechMeshCluster1" priority 1  
mesh-cluster-profile "TechMeshCluster2" priority 2  
!  
ap-name "Monitor"  
dot11a-radio-profile "mode_am"  
dot11g-radio-profile "mode_am"  
!  
logging level debugging network subcat all  
logging level debugging network subcat dhcp  
logging level debugging security  
logging level debugging security subcat all  
logging level debugging system subcat all  
logging level debugging user subcat all  
logging level debugging wireless subcat all  
logging level debugging user-debug 00:19:d2:6d:26:15  
snmp-server enable trap  
snmp-server host 192.3.1.3 version 1 Fortinet udp-port 162  
process monitor log  
end
```



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.