



# FortiNAC - FortiSwitch FortiLink Integration Guide

Version F 7.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](mailto:techdoc@fortinet.com)

April 15, 2024

FortiNAC F 7.x FortiSwitch FortiLink Integration Guide

49-922-769106-20211216

---

# TABLE OF CONTENTS

<b>Change log</b>	<b>5</b>
<b>Overview</b>	<b>6</b>
What it Does	6
How it Works	6
Requirements	10
Limitations	12
Considerations	12
<b>Base Lab Topology and Device Addresses</b>	<b>14</b>
<b>FortiGate Configuration</b>	<b>16</b>
1. Enable FortiLink on FortiGate	16
2. Configure Port Connecting to FortiSwitch	16
3. Configure Port Connecting to Network Management Interface of FortiNAC	17
4. Configure Port Connecting to Network Interface of FortiNAC	17
5. Configure SNMP Settings	18
6. System Administrator Account	19
7. REST API Administrator Account	19
8. REST API	19
9. VLANs	21
10. Configure Firewall Policy to Allow Traffic	21
11. MAC Retention Period (FortiOS 6.2.1 and above)	21
12. Configure Syslogs	22
13. Configure L2 MAC Traps	23
14. Configure RADIUS	25
Firewall Policy	25
Service Definition	25
Server and User Group	26
Security Policy for 802.1x	28
Apply Policy to FortiSwitch Ports	30
<b>FortiSwitch Configuration</b>	<b>32</b>
Management Interface	32
1. SNMP Traps (Optional) (FortiOS 6.2.1 and above)	33
2. SNMP Traps (Optional) (FortiOS 6.2.0 and below)	34
3. RADIUS (Enable CoA)	35
FortiNAC Version F 7.2.x	36
FortiNAC Version F7.4 +	36
<b>FortiNAC Configuration</b>	<b>37</b>
1. Create Logical Network	37
2. Create Network Access Policy	37
3. Integrate FortiNAC with FortiGate	39
4. Enable L3 Polling (Optional)	41
5. Enable L2 Polling (Optional)	43

---

6. Device Model Configuration .....	45
7. Configure RADIUS .....	46
8. Review Enforcement Checklist .....	46
9. Configure Port of FortiSwitch .....	47
<b>Validate Enforcement .....</b>	<b>48</b>
<b>Troubleshooting .....</b>	<b>49</b>
Related KB Articles .....	49
Debugging .....	49
FortiGate Commands .....	49
FortiSwitch Commands .....	50
FortiNAC Commands .....	51
Other Tools .....	52
<b>Appendix .....</b>	<b>53</b>
Syslog Messages for MAC Address Notification .....	53
API Calls Made to FortiGate During Poll .....	53

## Change log

Date	Change Description
31-Jan-2024	995826
20-Feb-2024	1001753
3-May-2024	1009378
28-May-2024	959138
31-May-2024	1037529
20-Jun-2024	1044155
19-Jul-2024	1033728
19-Jul-2024	1042949
9-Aug-2024	1064051
14-Aug-2024	1058383
6-Sep-2024	1070636
6-Sep-2024	1057198
9-Sep-2024	1047999
10-Sep-2024	1046578
25-Sep-2024	1080087
2-Oct-2024	1026224
16-Oct-2024	1071995
5-Nov-2024	1089988
5-Nov-2024	1074607
20-Dec-2024	1109088
28-Jan-2025	1071992
29-Jan-2025	1119269
24-Feb-2025	1046585
19-Mar-2025	1133483
31-Mar-2025	1140998
9-May-2025	1143823
	1154818
	This guide was generated in F 7.2.

# Overview

This document will guide Fortinet FortiNAC customers on how to integrate FortiNAC with Fortinet FortiSwitch and FortiGate.

The following sections will walk-through configuring FortiSwitch devices for management by FortiNAC through FortiLink Mode, as well as the required configurations on FortiGate. The order of topics in the Device Configuration section does not indicate the sequence for configuration tasks, as it may be subject to change due to device or FortiNAC software updates. Familiarizing oneself with basic FortiNAC wired management features is recommended by referring to the available FortiNAC documentation.

**Tip:** For hyperlinks referencing other documentation, right-click the link and select **Open in New Tab**.

For all other connections to be managed by FortiNAC, do not use this document. Refer to one of the following in the Document Library:

- Clients connecting to a FortiAP: [FortiAP Integration Guide](#)
- Clients connecting through FortiGate VPN tunnel: [FortiGate VPN Device Integration](#)
- Ethernet access ports on the FortiGate (directly connected endpoints or unmanaged switches where endpoints connect): [FortiGate Endpoint Management Integration Guide](#)
- Wireless via built-in access point on a FortiWiFi unit: [FortiGate Endpoint Management Integration Guide](#)

## What it Does

FortiNAC provides network visibility (where endpoints connect) and manages VLAN assignment at the point of connection for the endpoint. This is accomplished by sending the appropriate configuration commands to the device.

## How it Works

### Visibility

FortiNAC learns where endpoints are connected on the network using the following methods:

- SNMP traps sent by the switch (See table below for details)
- Syslog MAC Add/Remove/Delete messages (See table below for details)
- RADIUS communication
- L2 Polling (MAC address table read)
- L3 Polling (Arp Cache read)

### Endpoint Connectivity Notification Methods

Method	Description	Advantages	Disadvantages
<b>SNMP Link Traps</b>	<p>Link Traps originate from the FortiSwitch and are routed through the FortiGate.</p> <p>When a link trap is received, FortiNAC performs a L2 poll of the FortiGate to update the database with the new connection information.</p>	<ul style="list-style-type: none"> <li>• Configuration simplicity: FortiSwitch has link traps enabled by default on all ports</li> <li>• Link state traps are standard. Additional support is not required</li> </ul>	<ul style="list-style-type: none"> <li>• FortiNAC is not notified of indirect connections (computers behind IP Phones, hubs or unmanaged access points). Will not learn of change until the next L2 poll</li> <li>• Much higher L2 polling activity. Can cause significantly more work for FortiNAC in large environments where there is frequent movement of directly connected wired endpoints</li> <li>• Increased SSH activity to network devices where FortiNAC uses the CLI to retrieve MAC table information</li> </ul>
<b>Syslog Messages</b>	<p>FortiGate sends MAC Add, Delete, and Move messages.</p> <p>When a syslog message is received, FortiNAC updates the database with the new connection information (MAC address and location). FortiNAC does not process syslog messages for connecting Access Points.</p>	<ul style="list-style-type: none"> <li>• More efficient than Link traps: L2 poll not required</li> <li>• FortiNAC is notified of indirect connections (computers behind IP Phones, hubs or unmanaged access points)</li> <li>• Simple configuration on FortiGate</li> </ul>	<ul style="list-style-type: none"> <li>• Not real time</li> <li>• Syslog sends on all interfaces including uplinks</li> </ul>

Method	Description	Advantages	Disadvantages
<b>SNMP MAC Notification (L2 MAC) Traps</b>	FortiSwitch sends MAC Add, Delete, and Move SNMP traps. When a trap is received, FortiNAC updates the database with the new connection information (MAC address and location).	<ul style="list-style-type: none"> <li>• More efficient than Link traps: L2 poll not required</li> <li>• FortiNAC is notified of indirect connections (computers behind IP Phones, hubs or unmanaged access points)</li> <li>• More real time than Syslog</li> </ul>	<ul style="list-style-type: none"> <li>• Must configure all switches and access ports for MAC traps. FortiSwitch does not have a simple means to enable MAC traps on ports in bulk</li> <li>• Requires support for processing MAC Notification traps. A table of supported traps is included under SNMP trap support in the Administration Guide</li> </ul>
<b>RADIUS</b> (Configuration outside the scope of this document)	RADIUS requests sent to FortiNAC for endpoints connecting to downstream devices that are themselves connected to the FortiSwitch such as hubs or IP Phones (as well as directly connecting to the switch). It is possible to assign unique VLANs to each endpoint connecting to a single port, allowing for greater flexibility and security.	<ul style="list-style-type: none"> <li>• More efficient than Link traps: L2 poll not required</li> <li>• FortiNAC is notified of indirect connections (computers behind IP Phones, hubs or unmanaged access points)</li> <li>• More real-time than Syslog</li> <li>• More security options (MAC auth vs 802.1x)</li> <li>• Switch configuration doesn't change (FortiManager may try to override otherwise)</li> </ul>	<ul style="list-style-type: none"> <li>• FortiNAC becomes a single point of failure</li> <li>• More configuration intensive: <ul style="list-style-type: none"> <li>• RADIUS proxy or Local RADIUS</li> <li>• RADIUS configured on network infrastructure</li> <li>• FortSwitches must have a unique and routable IP address</li> </ul> </li> </ul>

### Control

FortiNAC provisions a device's network access by managing VLAN assignments based upon the switch's model configuration or an applicable network access policy and the state of the device. The VLAN configuration is modified using the appropriate method based upon the switch vendor and model.

FortiSwitches in FortiLink mode are managed by the FortiGate. Clients are managed by FortiNAC on FortiSwitch devices by assigning them to VLANs appropriate to their state in the FortiNAC system.

FortiGates/FortiSwitches managed by FortiManager: When FortiNAC makes any changes to the FortiGate or FortiSwitch, the Fortigate/FortiSwitch updates FortiManager. This keeps FortiManager in sync.

### Device Support Methods



Endpoint Connectivity Notification	Detecting Managed FortiSwitches	Reading MAC Address Tables (L2 Poll)	Reading IP Tables (L3 Poll)	Reading VLANs	Switching VLANs	De-auth
SNMP MAC Notification Traps** Syslog MAC Add/Move/Delete SNMP Link Traps	REST API*	SSH (TCP 22) REST API	SSH (TCP 22) REST API	REST API	REST API RADIUS	RADIUS Disconnect*

\* When the API call to detect managed switches no longer reports the device as managed by the return data from the FortiGate, it will be removed from FortiNAC. For a list of API calls, see [API Calls Made to FortiGate During Poll](#).

\*\*Requires specific FortiNAC software and FortiOS firmware versions.

### Enforcement Groups

Enforcement groups are used to specify which ports and switches FortiNAC should dynamically provision network access. Each enforcement group controls a different function. The enforcement groups used are dependent upon the network access requirements. See [Enforcement Groups](#) for details.

## Requirements

### FortiNAC

Feature/Function Support	Requirement
<b>FOS 6.x/7.0/7.1/7.2/7.3</b>	All F7.x FortiNAC versions
<b>FOS 7.4</b>	FortiNAC version F7.2.4 +
<b>Syslog Support</b>	FortiNAC version F7.2.6 +
<b>All other configurations</b>	FortiNAC version F7.2.4 +
<b>SNMP MAC Notification Traps</b>	FortiNAC version F7.2.1 +

### FortiGate

Feature/Function Support	Requirement
<b>General</b>	FOS 6.0.5 +
<b>Recommended</b>	FOS 6.2: 6.2.8 +
<b>Using post-login banner</b>	FOS 7.0 +
<b>SNMP MAC Notification Traps</b>	FOS 7.2 +  Important: SNMP parameters must be configured in FortiGate. See <a href="#">Considerations</a> for details.
<b>Syslog Messages</b>	FOS 6.2.1 +
<b>FortiNAC managing multiple FortiGates</b>	<ul style="list-style-type: none"> <li>FortiSwitch IP addresses must be routable</li> <li>FortiSwitch IP addresses must be unique</li> </ul>
<b>TLSv1-3 Support</b>	TLSv1-3 is supported
<b>Administrator account</b>	<ul style="list-style-type: none"> <li>Visibility only: System read access to all VDOMs</li> <li>Control: System read/write access to all VDOMs</li> </ul>
<b>FortiNAC manages RADIUS connections for FortiSwitches in Link Mode and FortiAPs through the same FortiGate</b>	The same RADIUS server settings cannot be used. RADIUS is sourced differently for the two devices and require unique RADIUS server configurations
<b>VDOMs</b>	<ul style="list-style-type: none"> <li>Multiple VDOM/Split-Task VDOMs are supported</li> </ul>

- FortiNAC currently supports one VLAN instance per FortiLink port per VDOM

#### FortiSwitch

Feature/Function Support	Requirement
<b>SNMP Traps or RADIUS</b>	<ul style="list-style-type: none"><li>• FortiSwitch IP addresses must be routable</li><li>• FortiSwitch IP addresses must be unique</li></ul>
<b>SNMP MAC Notification Traps</b>	FOS 7.2 +

## Limitations

- Prior to FortiOS version 6.2, MAC Address entries could remain in the FortiGate session table for long periods of time after the device disconnected. As of version 6.2, FortiGate offers the option to age entries immediately from the session table once the FortiSwitch removes the corresponding entry from its own table.
- Syslog messaging for FortiSwitches in Link Mode may not be sent to the appliance consistently when Multiple VDOM/Split-Task VDOMs are configured. To be addressed in FortiOS 6.4.6 and 7.0.0 (ID 0700842).
- Some FortiOS versions may allow illegal characters in the switch name. This will prevent Rest API communication from working. See KB article [353964](#).

## Considerations



**Important:** SNMP parameters must be configured in FortiGate. As of 6.2.1, SNMP parameters configured in the FortiSwitch are overwritten upon reboot of the FortiGate, including blank SNMP configurations. This results in erasing the SNMP configuration on the FortiSwitch.

- FortiGate can only support one FSSO agent sending tags for a specific endpoint IP address. If there are multiple agents, the FortiGate entries will be overwritten when other FSSO agents send information for the same endpoint IP. Therefore, the following should be done prior to integration:
  - Identify any other FSSO agents that provide logon information for the same endpoints FortiNAC would be managing through the FortiGate. For additional information, see section **Agent-based FSSO** in the FortiOS 6.0.0 Handbook:  
<https://docs2.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso>
  - For those agents, logon events must be blocked. See related KB article **Excluding IP addresses from FSSO logon events**:  
<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Excluding-IP-addresses-from-FSSO-logon-events/ta-p/196270>
  - Develop a plan to make the appropriate modifications to existing firewall policies to accommodate FortiNAC as the FSSO agent for the managed endpoint IP address scope.
- Groups for location matching: The FortiSwitch interfaces must be part of a port group. Device groups that specify the FortiSwitch will not match. This is due to the fact that the FortiGate is considered the parent device.
- FortiGate High Availability (HA): A number of deployment scenarios exist for FortiGate HA.
  - FortiNAC supports FortiGate HA configurations using a Virtual/Shared IP (VIP). The VIP is used to model the Fortigate in FortiNAC's Inventory.
  - FortiNAC currently does not support FortiGate HA configurations using a standalone IP (where Fortigate-A and FortiGate-B are modeled separately).

For details on FortiGate HA reference

<https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/666376/high-availability>

<https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/900885/ha-active-passive-cluster-setup>

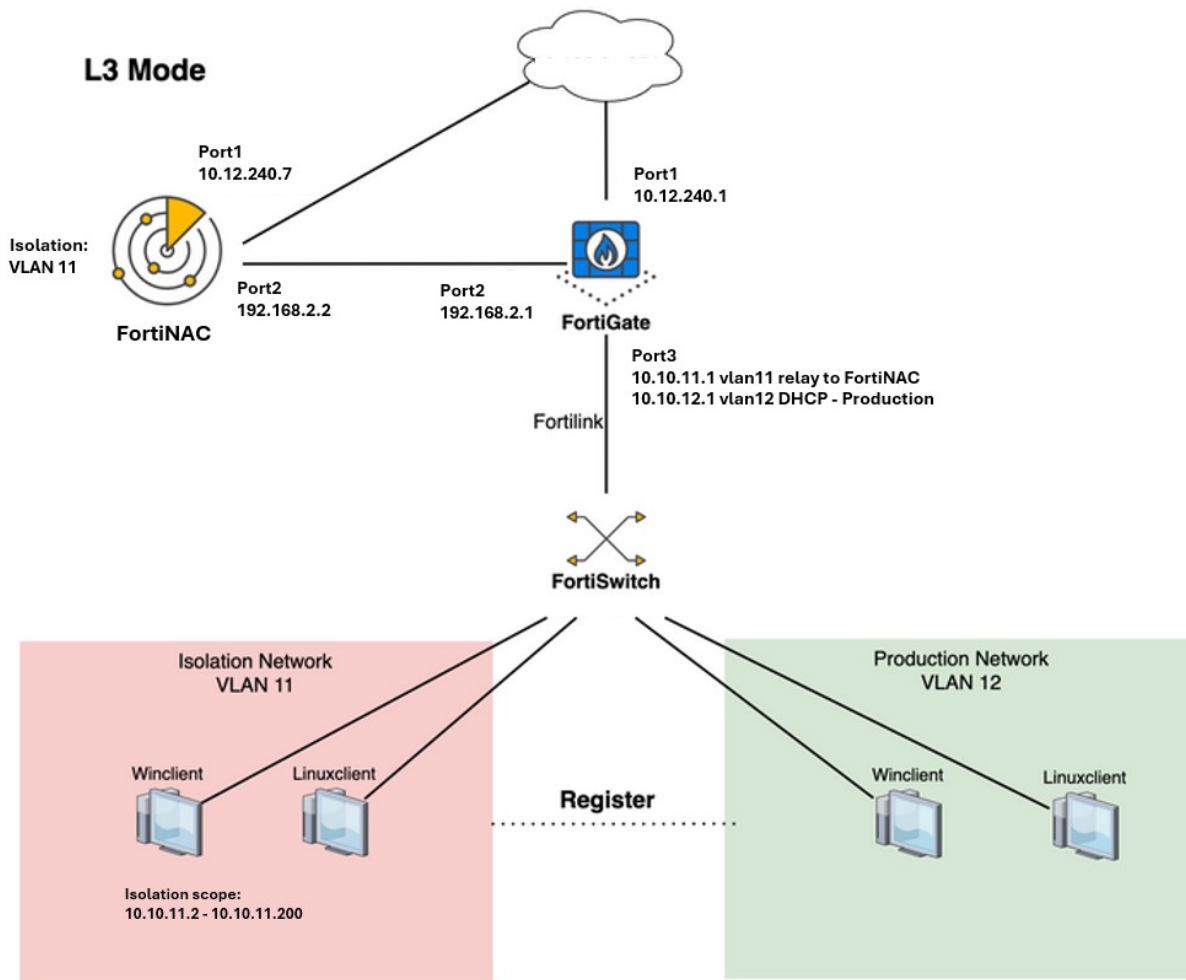
<https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/357558/ha-active-active-cluster-setup>

- FortiNAC versions F7.2.5 and lower: When a FortiGate High Availability (HA) failover occurs, FortiNAC can no longer connect via SSH and credential validation fails. This is because the SSH fingerprint has changed for the modeled device.

Workaround:

- a. Navigate to **Network > Inventory** and select the FortiGate's Device Model.
- b. Click the **Clear Known Hosts** button under the Credentials tab.
- c. Click **Validate Credentials** to confirm FortiNAC can SSH to the FortiGate.

# Base Lab Topology and Device Addresses



In this example of a base lab topology:

- Devices connecting to the network are authenticated and authorized by FortiNAC based on predefined policies and compliance checks.
- FortiNAC communicates with FortiGate to enforce network access control policies and provide visibility into the network traffic.
- The FortiGate manages the network traffic and security policies.
- The FortiSwitch is connected to FortiGate via FortiLink, allowing for centralized management and control of switch ports and network traffic.

This example topology provides a basic framework for network access control and security enforcement. FortiNAC serves as the central point for device authentication and access control. FortiGate manages network security policies, and FortiSwitch provides network connectivity.

**Note:** this example topology is for illustrative purposes only and your actual configurations may vary based on the specific requirements and constraints of your network environment. The following chapters will use this

example topology as a reference point for more detailed configurations and integrations with FortiNAC, FortiGate and FortiSwitches.

# FortiGate Configuration

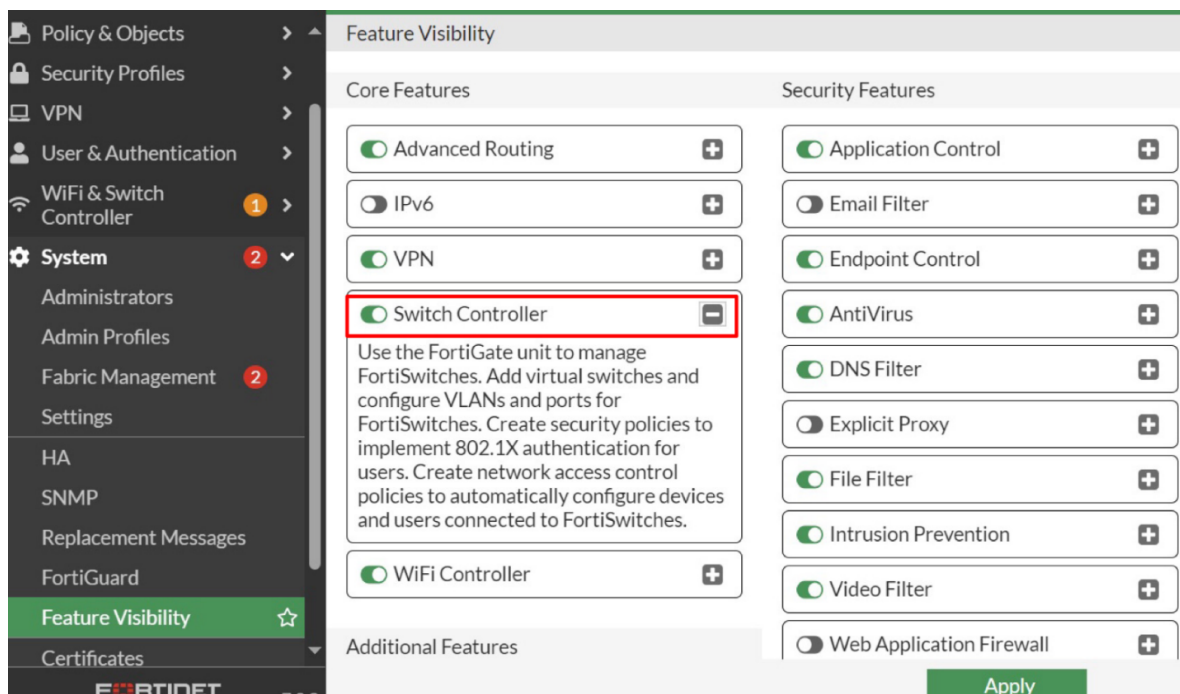
In FortiLink mode, FortiGate acts as a controller for FortiSwitches to enable centralized management and configuration of the FortiSwitches through FortiGate's interface.

This integration streamlines network management tasks, enhances security by enforcing consistent policies across both the FortiGate firewall and the FortiSwitches. Also, it enables features such as VLAN (Virtual Local Area Network) segmentation, traffic shaping, and monitoring.

By deploying FortiGate and FortiSwitches in FortiLink mode, organizations can simplify network operations, improve visibility and control and enhance overall network security posture.

## 1. Enable FortiLink on FortiGate

1. Login to the FortiGate web interface.
2. Go to **System > Feature Visibility**.
3. Enable **"Switch Controller"**.



## 2. Configure Port Connecting to FortiSwitch

1. In the FortiGate web interface, go to **Network > Interfaces**.
2. Edit the interface connected to the FortiSwitch.



3. Make sure the interface type is set to “**FortiLink**”.

The screenshot shows the FortiGate web interface with the 'Edit Interface' configuration page for an interface named 'fortilink'. The left sidebar shows the 'Network' menu with 'Interfaces' selected. The main configuration area shows the following settings:

- Name: fortilink
- Alias: (empty)
- Type: FortiLink (802.3ad Aggregate) (highlighted with a red box)
- VRF ID: 0
- Interface members: port3 (with a plus sign to add more)
- Addressing mode: Manual (selected), DHCP, Auto-managed by IPAM, Dedicated to FortiSwitch
- IP/Netmask: 10.255.1.1/255.255.255.0
- Connected devices: 1 FortiSwitch(es)
- Automatically authorize devices: ☒
- FortiLink split interface: ☒
- IoT scanning: ☐
- DHCP Server: ☐

At the bottom right, there are 'OK' and 'Cancel' buttons.

### 3. Configure Port Connecting to Network Management Interface of FortiNAC

1. In the FortiGate web interface, go to **Network > Interfaces**.
2. Edit the interface used to communicate with FortiNAC (management port eth0/port1) to allow the required protocols.
3. Under Administrative Access, enable the following protocols:
  - HTTPS
  - PING
  - SNMP
  - SSH
  - RADIUS Accounting (required if configuring RADIUS authentication)
  - Security Fabric Connection

The remaining protocols are not required by FortiNAC.
4. Click **OK** to save any modifications.

### 4. Configure Port Connecting to Network Interface of FortiNAC

1. In the FortiGate web interface, go to **Network > Interfaces**.
2. Edit the interface connected to the network interface of FortiNAC (eth1/port2) that provides client authentication path.
3. Under Administrative Access, enable the following protocols:

PING

The remaining protocols are not required by FortiNAC.

4. Click **OK** to save any modifications.

## 5. Configure SNMP Settings

1. In the FortiGate web interface, go to **System > SNMP**.
2. Enable **SNMP Agent** to enable the SNMP service on the FortiGate.
3. Under the appropriate SNMP Protocol (v1/v2c or v3), click **Create New** to create a new Community to use with FortiNAC or verify the following are already configured in an existing Community.

SNMP community strings act as passwords for SNMP access.

### SNMP Settings (v1/v2c)

<b>Community Name</b>	Community Name
<b>Enabled</b>	Selected
<b>Hosts</b>	<b>IP Address:</b> <eth0/port1 IP address of FortiNAC Control Server> <b>Host Type:</b> Accept queries and send traps
<b>Queries</b>	V1 or v2 enabled <b>Port:</b> 161
<b>Traps</b>	V1 or v2 enabled <b>Port:</b> 162
<b>SNMP Events</b>	<b>Single FortiGate:</b> <all disabled> <b>FortiGate in High Availability Mode</b> Enable the following: <ul style="list-style-type: none"> <li>• HA cluster status change</li> <li>• HA cluster member up</li> <li>• HA cluster member down</li> </ul>

### SNMP Settings (v3)

<b>User Name</b>	User Name
<b>Enabled</b>	Selected
<b>Security Level</b>	Authentication (No Private) <ul style="list-style-type: none"> <li>• <b>Authentication Algorithm:</b> SHA1 or MD5</li> <li>• <b>Password</b></li> </ul> Authentication (Private) <ul style="list-style-type: none"> <li>• <b>Authentication Algorithm:</b> SHA1 or MD5</li> <li>• <b>Password</b></li> <li>• <b>Encryption Algorithm:</b> DES or AES256</li> </ul>

<b>Hosts</b>	<b>IP Address:</b> <eth0/port1 IP address of FortiNAC Control Server> <b>Host Type:</b> Accept Queries Only
<b>Queries</b>	Enabled <b>Port:</b> 161
<b>Traps</b>	Enabled <b>Port:</b> 162
<b>SNMP Events</b>	<all disabled>

## 6. System Administrator Account

A System Administrator account is used for SSH and REST API access on the FortiGate.

To create or view user accounts, navigate to **System > Administrators** in the FortiGate UI.

## 7. REST API Administrator Account

A FortiGate REST API Administrator key can be used in addition to the System Administrator Account. The API key allows FortiNAC to bypass the need to authenticate every time it connects, improving performance.

1. Navigate to **System > Administrators**
2. Click **Create New > REST API Admin**.
3. Configure the settings as needed.
4. Click **OK**. The New API key window opens.
5. Copy the key to the clipboard and click **Close**.
6. Click **OK**.
7. Save the key for use in the FortiNAC configuration section.
8. Ensure the FortiGate is configured to allow API access using the API key. In the FortiGate CLI enter the following:

```
config system global
set rest-api-key-url-query enable
end
```

## 8. REST API

REST API is required for communication with FortiNAC and must be configured. Verify the appropriate port is configured:

1. In the FortiGate UI, navigate to **System > Settings**.
2. Under **Administration Settings**, modify the **HTTPS port** as necessary (another service may already use 443).
3. Click **Apply** to save any modifications.

## 9. VLANs

1. In the FortiGate UI, navigate to **WiFi & Switch Controller > FortiSwitch VLANs**.
2. Ensure VLANs are configured and working on the FortiSwitch for all FortiNAC states desired to be enforced (Registration, Remediation, etc).
3. Enable Device Detection for each applicable VLAN interface on the FortiGate. This enables FortiGate to see connected devices on the FortiSwitch for that VLAN.
  - a. Select the VLAN interface, right-click and select **Edit**.
  - b. Enable **Device Detection** and click **OK**.

## 10. Configure Firewall Policy to Allow Traffic

Set up Policies on the FortiGate to control traffic passing from the FortiSwitch to the FortiNAC.

1. In the FortiGate web interface, go to **Policy & Objects > Firewall Policy**.
2. Configure Firewall policies to do the following.
  - Allow traffic from Production VLAN 12 to Port1 of the FortiNAC
  - Allow RADIUS (if configured) and SNMP traffic from the FortiSwitch to Port1 of the FortiNAC via the FortiGate
  - Allow traffic from Isolation VLAN 11 to Port2 of the FortiNAC
  - Block outbound DNS from Isolation VLAN 11 except to Port2 of the FortiNAC. This prevents isolated devices from resolving DNS from any other server

Note: Firewall Policy configuration is outside the scope of this document.

## 11. MAC Retention Period (FortiOS 6.2.1 and above)

FortiNAC determines the device's connection status through L2 polls, SNMP traps and syslog messaging from the FortiGate. Configure the mac-aging-interval and mac-retention-period options in the FortiGate CLI in order to receive timely notifications when endpoints disconnect from the network.

**mac-retention-period:** Time in hours after which an inactive MAC address is removed from FortiGate client database. Default value is 24 hours. (Value range: 0 to 168, 0 = aged out based on mac-aging-interval). It is recommended to set this value to 0 so the client database updates when the corresponding entry in the FortiSwitch is removed.

Reference

<https://docs.fortinet.com/document/fortigate/7.0.5/cli-reference/242620/config-switch-controller-global>

<https://docs.fortinet.com/document/fortigate/6.4.8/cli-reference/228620/config-switch-controller-global>

Type the following commands:

```
config switch-controller global
```

```
set mac-retention-period 0
```

```
end
```

Once an inactive MAC address is aged out of the FortiSwitch, the FortiGate removes the corresponding client entry. If syslog messages are configured, the FortiGate sends a "MAC Delete" message to FortiNAC and the connection information is updated. Otherwise, upon the next L2 Poll of the FortiGate, FortiNAC updates the connection information.

For more details, see section "Dynamic MAC address learning" under "FortiSwitch port features" of the "Managed Switch (FortiOS 6.2)" Admin Guide found in the Fortinet Document Library:

<https://docs.fortinet.com/product/fortiswitch/6.2>

Click on the appropriate link below to continue FortiGate configuration (only one of the following should be configured):

[Configure Syslogs](#)

[Configure L2 MAC Traps](#)

[Configure Radius](#)

## 12. Configure Syslogs

### Syslog (Optional) (FortiOS 6.2.1 and above)

In the FortiGate CLI, configure syslog to send MAC Add, Delete, and Move messages to FortiNAC. "MAC Learned" and "MAC Removed" events are logged in FortiNAC as these messages are processed.



If L2 MAC traps or RADIUS will be used, skip this section.

#### Note:

- For best performance, configure syslog filter to only send relevant syslog messages.
- Multiple syslog servers (up to 4) can be created on a FortiGate with their own individual filters. In High Availability FortiNAC environments, configure 2 (Primary server and Secondary server).
- Use the default syslog format. Other formats (CEF, CSV, rfc5424) are not supported.

```
config log syslogd setting
set status enable
set server "<FortiNAC eth0 IP address> "
set source-ip <Device IP address modeled in FortiNAC>
set format default
end
config log syslogd filter
set forward-traffic disable
set local-traffic disable
set multicast-traffic disable
```

```
set sniffer-traffic disable
set ztna-traffic disable
set anomaly disable
set voip disable
config free-style
edit 1
set category event
set filter "(logid 0115032615 0115032616 0115032617)"
set filter-type include
end
end
config log syslogd2 setting
set status enable
set server "<FortiNAC Secondary Server eth0 IP address>"
set source-ip <Device IP address modeled in FortiNAC>
set format default
end
config log syslogd2 filter
set forward-traffic disable
set local-traffic disable
set multicast-traffic disable
set sniffer-traffic disable
set ztna-traffic disable
set anomaly disable
set voip disable
config free-style
edit 1
set category event
set filter "(logid 0115032615 0115032616 0115032617)"
set filter-type include
end
end
```

## 13. Configure L2 MAC Traps



If Syslog or RADIUS is or will be configured, skip this section.

---

Configure L2 MAC traps to be sent to FortiNAC's primary IP address when clients connect or disconnect. Traps are configured per switch port.

Type the following commands in the FortiGate CLI:

1. Create custom script to enable either SNMP v2 or SNMP v3 L2 MAC traps.

**Option 1: SNMPv2**

```
config switch-controller custom-command
edit "<name>"
set command "config system snmp sysinfo %0a set status enable %0a end %0a config
system snmp community %0a edit <id> %0a set events l2mac %0a end"
next
end
```

Parameter	Description	Type	Size
id	Community ID.	integer	Minimum value: 0 Maximum value: 4294967295

### Option 2: SNMPv3



Username must match name configured in step 7 (Configure SNMP Settings)

```
config switch-controller custom-command
edit "<name>"
set command "config system snmp sysinfo %0a set status enable %0a end %0a config
system snmp user %0a edit <snmp-username> %0a set security-level no-auth-no-
priv %0a set events l2mac %0a set notify-hosts <fortinac-address-or-range>
%0a next %0a end"
next
end
```

### 2. Create custom script to configure access ports to send L2 MAC traps (each port must be listed).

FOS v7.2/7.4:

```
config switch-controller custom-command
edit "<name>"
set command "config switch interface %0a edit <port> %0a set log-mac-event enable
%0a next %0a edit <port> %0a set log-mac-event enable %0a end %0a"
next
end
```

FOS v7.6:

```
config switch-controller custom-command
edit "<name>"
set command "config ports %0a edit <port> %0a set log-mac-event enable %0a next
%0a edit <port> %0a set log-mac-event enable %0a end %0a"
next
end
```

### 3. Apply the Custom Scripts to the FSW

```
config switch-controller managed-switch
edit <switch name or serial number>
config custom-command
edit 1
set command-name "<custom command name from step 2>"
next
edit 2
set command-name "<custom command name from step 1>"
next
end
end
```

### Example: Enable L2 MAC trap (SNMPv3) on switch FLR200 ports 2 & 3

```
config switch-controller custom-command
edit "SNMPv3_Event"
set command "config system snmp user %0a edit SNMPuname %0a set events l2mac %0a end"
next
```



```
end
config switch-controller custom-command
edit "108e-f_mac_notification"
set command " config system snmp sysinfo %0a set status enable %0a end %0a config
    switch interface %0a edit port2 %0a set log-mac-event enable %0a next %0a edit
    port3 %0a set log-mac-event enable %0a end %0a"
next
end

config switch-controller managed-switch
edit FLR200
config custom-command
edit 1
set command-name "108e-f_mac_notification"
next
edit 2
set command-name "SNMPv3_Event"
next
end
end
To confirm the configuration applied, log in to FortiSwitch CLI and type
config system snmp sysinfo
show
end
config system snmp community
show
end
config switch interface
show
end
```

See related KB article: [L2 to MAC events/traps are not generated on FortiSwitch](#)

## 14. Configure RADIUS

**Note:** If Syslog or L2 MAC Traps are configured, skip this step.

### Firewall Policy

1. In the FortiGate UI, navigate to **Policy & Objects > Firewall Policy**.
2. Ensure a firewall policy exists to disable NAT for RADIUS traffic.

### Service Definition

In the FortiGate UI, ensure the RADIUS Service Definition is allowing the proper ports.

1. Navigate to **Policy & Objects > Services**.
2. Under **Authentication** edit **RADIUS**.
3. Review the ports and edit as required based upon the ports to be used by FortiNAC (see table below).

<b>Authentication port</b>	Specify the port used by FortiNAC to receive RADIUS authentication requests. Default: UDP 1812 Port values modifiable in the FortiNAC UI under <a href="#">Local RADIUS</a> and <a href="#">Proxy</a> settings.
<b>Accounting port</b>	Specify the port used by FortiNAC to receive RADIUS accounting requests. Default: UDP 1813 Accounting Port value is modifiable in the FortiNAC UI under <a href="#">Proxy</a> setting.
<b>CoA port</b>	UDP 3799

## Server and User Group

In the FortiGate, designate FortiNAC as the RADIUS server and create a user group.

Multiple VDOM/Split-Task VDOMs: RADIUS settings must be configured for each VDOM sending RADIUS requests to FortiNAC.

### Reference:

<https://docs.fortinet.com/document/fortigate/7.2.9/administration-guide/759080/configuring-a-radius-server>

<https://docs.fortinet.com/document/fortigate/7.2.9/administration-guide/29900/user-groups>

### UI Method

1. Navigate to **User & Authentication > RADIUS Servers**.
2. Create a new RADIUS server. Configure using the table below.
3. Click **OK**.

#### RADIUS Server Settings (config user radius)

<b>Name</b>	Name representing RADIUS server (FortiNAC)
<b>user radius</b>	
<b>Authentication Method</b>	Default (802.1x authentication) Specify Authentication Method (PAP) (Required for MAC-Authentication only)
<b>NAS IP/Call Station ID</b>	Leave blank
<b>server</b>	FortiNAC Server/Control server eth0/port1 interface IP Address <b>High Availability:</b> IP address of primary control server (Do not use Shared IP address)

<b>secret</b>	<b>Important:</b> This value must match the secret values configured on FortiNAC and any optional terminating RADIUS server used to support 802.1x.
<b>secondary-server</b>	<b>High Availability:</b> IP address of secondary control server (Do not use Shared IP address)
<b>secondary-secret</b>	<b>Important:</b> This value must match the secret values configured on FortiNAC and any optional terminating RADIUS server used to support 802.1x.
<b>radius-coa</b>	Enable (Disabled by default)
<b>acct-interim-interval</b>	86400

#### Accounting Server Settings (config accounting-server)

<b>status</b>	Enable (Disabled by default)
<b>server</b>	FortiNAC Server/Control server eth0/port1 interface IP Address <b>High Availability:</b> IP address of primary control server (Do not use Shared IP address)
<b>secret</b>	<b>Important:</b> This value must match the secret values configured on FortiNAC and any optional terminating RADIUS server used to support 802.1x.

4. Navigate to **User & Authentication > User groups**.
5. Create a new user group. Configure using the table below.
6. Click **OK**.

#### User Group Settings (config user group)

<b>user group name</b>	Name of the group which the Radius server will be a member
<b>member</b>	User name of Radius server

#### CLI Method

Reference:

<https://docs.fortinet.com/document/fortigate/7.2.9/cli-reference/164332072/config-user-radius>

<https://docs.fortinet.com/document/fortigate/7.2.9/cli-reference/328136827/config-user-group>

```
config user radius
edit "<name>"
set server "<FortiNAC eth0/port1 IP address>"
set secret <secret>
set acct-interim-interval 86400
set radius-coa enable
config accounting-server
edit <number>
set status enable
set server "<FortiNAC eth0/port1 IP address>"
```

```
set secret <secret>
next
end
config user group
edit "<user group name>"
set member "<name>"
next
end
```

Example:

Radius server name = FortiNAC-Radius

Eth0/port1 IP address = 10.12.240.7

Group Name = FNAC-Radius-Grp

```
config user radius
edit "FortiNAC-Radius"
set server "10.12.240.7"
set secret ENC ldddd
set acct-interim-interval 86400
set radius-coa enable
config accounting-server
edit 1
set status enable
set server "10.12.240.7"
set secret ENC ldddd
next
end
config user group
edit "FNAC-Radius-Grp"
set member "FortiNAC-Radius"
next
end
```

## Security Policy for 802.1x

In the FortiGate UI, create a security policy with the new user group.

<https://docs.fortinet.com/document/fortiswitch/7.2.9/fortilink-guide/756049/fortiswitch-security-policies#Define>

### UI Method

1. Navigate to **WiFi & Switch Controller > FortiSwitch Security Policies**
2. Use the default 802-1X-policy-default, or create a new security policy.

3. Configure using the table below.
4. Click **OK**.

**Security Policy Settings (config switch-controller security-policy 802-1X)**

Name	Policy Name
<b>security mode</b>	802.1X-mac-based
<b>user-group</b>	RADIUS server group created previously
<b>mac-auth-bypass</b>	Enable (optional) (Sends 802.1x authentication request to client. If no response, uses MAC authentication)
<b>auth-fail-vlan</b> <b>auth-fail-vlan-id</b>	Enable (Recommended). VLAN to assign if clients fail RADIUS authentication to FortiNAC.
<b>eap-passthru</b>	Enable

**CLI Method**

```
config switch-controller security-policy 802-1X
edit "<policy name>"
set security-mode 802.1X-mac-based
set user-group "<user group name>"
set mac-auth-bypass enable
set open-auth disable
set eap-passthru enable
set guest-vlan disable
set auth-fail-vlan enable
set auth-fail-vlan-id {string}
set framevid-apply enable
set radius-timeout-overwrite disable
next
end
```

**Example:**

```
config switch-controller security-policy 802-1X
edit "802-1X-policy-default"
set security-mode 802.1X-mac-based
set user-group "FNAC-Radius-Grp"
set mac-auth-bypass enable
```

```
set open-auth disable
set eap-passthru enable
set guest-vlan disable
set auth-fail-vlan enable
set auth-fail-vlan-id Guest
set framevid-apply enable
set radius-timeout-overwrite disable
next
end
```

## Apply Policy to FortiSwitch Ports

Apply the 802.1x security policy to the desired edge ports of the managed FortiSwitch.

Reference:

<https://docs.fortinet.com/document/fortiswitch/7.2.9/fortilink-guide/756049/fortiswitch-security-policies#Apply>

### UI Method

1. Navigate to **WiFi & Switch Controller > FortiSwitch Ports**
2. Multi-select the desired ports and click on the pencil icon under the Security Policy column.  
**Note:** If the Security Policy column is not visible, right click on the column header, select Security policy and click **Apply**.
3. Select the security policy and click **Apply**.

### FortiGate CLI Method

```
config switch-controller managed-switch
edit <FortiSwitch serial number>
config ports
edit "<FortiSwitch edge port to be configured for RADIUS>"
set port-security-policy "<policy name> "
next
edit "<FortiSwitch edge port to be configured for RADIUS>"
set port-security-policy "<policy name> "
next
end
next
```

```
end
```

### Example:

```
config switch-controller managed-switch
edit S248EPTF1800XXXX
config ports
edit "port2"
set port-security-policy "802-1X-policy-default"
next
edit "port3"
set port-security-policy "802-1X-policy-default"
next
end
next
end
```

Allow all downstream FortiSwitch units in Link Mode to receive CoA and disconnect messages.

### CLI Method

#### Reference:

<https://docs.fortinet.com/document/fortiswitch/7.2.9/fortilink-guide/756049/fortiswitch-security-policies#RADIUS2>

```
config switch-controller security-policy local-access
edit default
append mgmt-allowaccess radius-acct
append internal-allowaccess radius-acct
end
```

# FortiSwitch Configuration

## Management Interface

In the FortiSwitch CLI, configure the management interface. Refer to the appropriate FortiSwitch CLI Reference Manual for options.

Reference:

<https://docs.fortinet.com/document/fortiswitch/7.0.4/fortiswitchos-cli-reference/511852/config-switch#config11>

Allow the following protocols:

PING

HTTPS

SSH

FortSwitches configured for RADIUS authentication must have a valid IP address (not 169.x.x.x). FortiNAC uses this address when disconnecting clients (RADIUS CoA).

1. Configure management interface name (if not already created). Type  
**config switch lldp settings**  
**show**
2. If not configured, type  
**set management-interface "internal"**  
**end**
3. Click on the appropriate link below to continue FortiSwitch configuration:  
[Radius \(Enable CoA\)](#)  
[SNMP Traps \(Optional\) \(FortiOS 6.2.1 and above\)](#)  
[SNMP Traps \(Optional\) \(FortiOS 6.2.0 and below\)](#)



## 1. SNMP Traps (Optional) (FortiOS 6.2.1 and above)

**Note:** If Syslog is already configured, do not configure SNMP traps and proceed to [Configure FortiNAC](#).

In the FortiSwitch CLI, set the system interface to allow SNMP via the FortiGate.

Reference:

<https://docs.fortinet.com/document/fortiswitch/7.0.4/fortiswitchos-cli-reference/500379/config-system#config16>

<https://docs.fortinet.com/document/fortiswitch/6.4.3/fortiswitchos-cli-reference/500379/config-system#config16>

Type the following commands

```
config system interface  
edit "internal"  
set mode dhcp  
set allowaccess ping https ssh snmp  
set type physical  
set snmp-index 30  
set defaultgw enable  
next  
end
```

Example:

```
FSW-Corp-Eng-01 (internal) # show  
config system interface  
    edit "internal"  
        set mode dhcp  
        set allowaccess ping https ssh snmp  
        set type physical  
        set snmp-index 30  
        set defaultgw enable  
    next  
end
```

Proceed to [Configure FortiNAC](#).

## 2. SNMP Traps (Optional) (FortiOS 6.2.0 and below)

**Note:** If Syslog is already configured, do not configure SNMP traps and proceed to [Configure FortiNAC](#).

In the FortiSwitch CLI, configure Link State traps to be sent to FortiNAC's primary IP address when clients connect or disconnect. Traps are configured per switch.

Reference:

[https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a2951442-519d-11e9-94bf-00505692583a/FortiSwitch-6.2.0-Managed\\_by\\_FortiOS\\_6.2.pdf](https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a2951442-519d-11e9-94bf-00505692583a/FortiSwitch-6.2.0-Managed_by_FortiOS_6.2.pdf)

Type the following commands

```
config system interface
edit "internal"
set mode dhcp
set allowaccess ping https http ssh snmp telnet
set type physical
set snmp-index 12
set defaultgw enable
next
end
config system snmp sysinfo
set status enable
end
config system snmp community
edit <number>
config hosts
edit <number>
set ip <FortiNAC eth0 IP/port1 address> <mask>
next
end
set name "<community string>"
set trap-v2c-status disable
next
end
```

**SNMPv1 Example**

The below is used in all the following configuration examples:

internal = Management interface name

10.12.240.7/24 = Primary NAC Server eth0 IP address

Community name = fortinet

```
config system interface
    edit "internal"
        set mode dhcp
        set allowaccess ping https ssh snmp
        set type physical
        set snmp-index 12
        set defaultgw enable
    next
end
config system snmp sysinfo
    set status enable
end
config system snmp community
    edit 1
        config hosts
            edit 1
                set ip 10.12.240.7 255.255.255.0
            next
        end
        set name "fortinet"
        set trap-v2c-status disable
    next
end
```

Proceed to [Configure FortiNAC](#).

### 3. RADIUS (Enable CoA)

**Note:** If RADIUS was not configured in FortiGate, skip this step.

## FortiNAC Version F 7.2.x

In the FortiSwitch CLI, enable the processing of RADIUS CoA and disconnect messages by including **radius-acct** as a permitted management access type and enabling CoA.

Reference:

<https://docs.fortinet.com/document/fortiswitch/7.6.1/fortilink-guide/756049/fortiswitch-security-policies#RADIUS2>

CLI Method:

```
config system interface
edit "<interface connected to the FortiGate>"
set allowaccess ping https ssh radius-acct
next
config user radius
edit "<RADIUS_server_name>"
set radius-coa enable
end
```

Example:

```
config system interface
edit "internal"
set allowaccess ping https ssh radius-acct
next
config user radius
edit "FortiNAC-Radius"
set radius-coa enable
end
```

Proceed to Configure FortiNAC.

## FortiNAC Version F7.4 +

RADIUS CoA will be configured for the FortiSwitch in the following section.

Proceed to Configure FortiNAC.

# FortiNAC Configuration

## 1. Create Logical Network

A logical Network defines network segments within your organization's network infrastructure. Logical Networks help organize devices and resources based on their function roles, security requirements, etc.

1. In the FortiNAC Web Interface, locate and click on **"Logical Network"** under **Network**.
2. Click on **"Create New"**.
3. Specify the name and description of the logical network.

The screenshot shows the FortiNAC web interface. The top navigation bar is green with the FortiNAC logo and a search icon. The left sidebar contains a menu with icons and labels: Dashboard, Users & Hosts, Network (highlighted with a green checkmark), Inventory, Logical Networks, RADIUS, Service Connectors, CLI Configuration, L2 Polling, L3 Polling, Network Events, Port Changes, Policy & Objects, Portal, Logs, and System. The main content area is titled 'Create Logical Network' and contains two input fields: 'Name' with the value 'Production' and 'Description' which is empty. At the bottom right, there are two buttons: 'OK' (green) and 'Cancel' (white).

## 2. Create Network Access Policy

Network Access Policy defines how devices are allowed or denied access to your network based on various criteria such as device type, user identity, compliance status, etc.

1. In the FortiNAC web interface, navigate to **Policy & Objects > Network Access** and select **Create New**.
2. Specify a name for this Network Access Policy and select the **create** button for **Configuration**.

FortiNAC

Dashboard > Create Network Access Policy

Users & Hosts > Name

Network > Notes

**Policy & Objects** > Configuration

User/Host Profiles

Portal Policy

Authentication

**Network Access** ☆

Endpoint Compliance

Supplicant EasyConnect

Passive Agent

Remediation Configuration

Roles

Network Device Roles

Portal >

Logs >

System >

Configuration

Enabled

User/Host Profile

Conditions

Name

Who/What Any

Where Any

When Always

Notes

Search

+ Create

Network Access Configuration (0)

Edit

3. Select the Logical Network created in '6.1.2 Create Logical Network' to create a **configuration**.

Create Network Access Configuration

Name production\_logical\_network

Logical Network Production

Note

Search

+ Create

Logical Networks (1)

Production

OK

Cancel

**FortiNAC**

Dashboard > Edit Network Access Policy

Users & Hosts > Name production-net-access-policy

Network > Notes

**Policy & Objects** ✓

User/Host Profiles Configuration production\_logical\_network

Portal Policy Enabled ☒

Authentication User/Host Profile Global Authentication Conversion

**Network Access** ☆

Endpoint Compliance Conditions

Supplicant EasyConnect Use Existing Clone

Passive Agent Name Global Authentication Conversion

Remediation Configuration Who/What ☒ Any

Roles Where ☒ Any

Network Device Roles When Always

Portal Notes Converted from Global Authentication Policy - Tue Feb 27 18:46:14 EST 2024

Logs

System

OK Cancel

### 3. Integrate FortiNAC with FortiGate

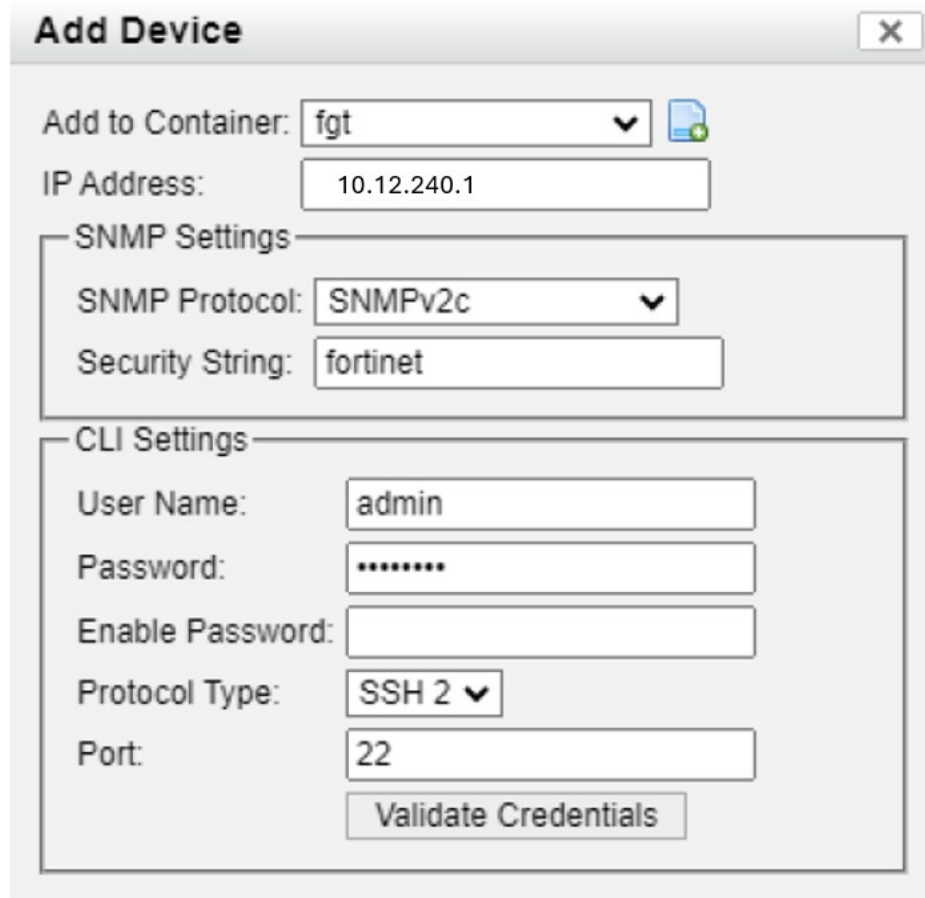
#### Add/Discover FortiGate to FortiNAC

1. In the FortiNAC Administration UI, navigate to **Network > Inventory**.
2. Discover or add the configured FortiGate. FortiNAC should automatically detect FortiSwitches connected to the FortiGate via FortiLink.

Include the following configurations:

SNMP Settings: SNMP v1 or v3 credentials created in “4.6 Configure SNMP Settings” from FortiGate configuration

CLI Settings: Administrator account credentials used



**Add Device**

Add to Container: fgt

IP Address: 10.12.240.1

**SNMP Settings**

SNMP Protocol: SNMPv2c

Security String: fortinet

**CLI Settings**

User Name: admin

Password: \*\*\*\*\*

Enable Password:

Protocol Type: SSH 2

Port: 22

Validate Credentials

Note: If CLI credentials are not included when adding the device, any managed FortiSwitches will not be discovered until the CLI credentials are added to the Model Configuration for API Access.

**Note the following:**

1. Models for Fortiswitch devices using self-assigned IP addresses will show contact status lost. These are internal IP addresses and are not reachable. Polling can be disabled under the **Polling** tab of the FortiSwitch model to avoid confusion
2. The ports will be listed under the **Ports** tab. If ports are not listed, ensure the CLI credentials are populated in the model. Once added, right click on the model and select **Resync Interfaces**.
3. If utilizing the FortiGate API key do the following:
  - a. Right-click on the FortiGate model in the tree and select **Model Configuration**.
  - b. Paste the key in the Fortigate API Token field.
  - c. Click **Apply**.

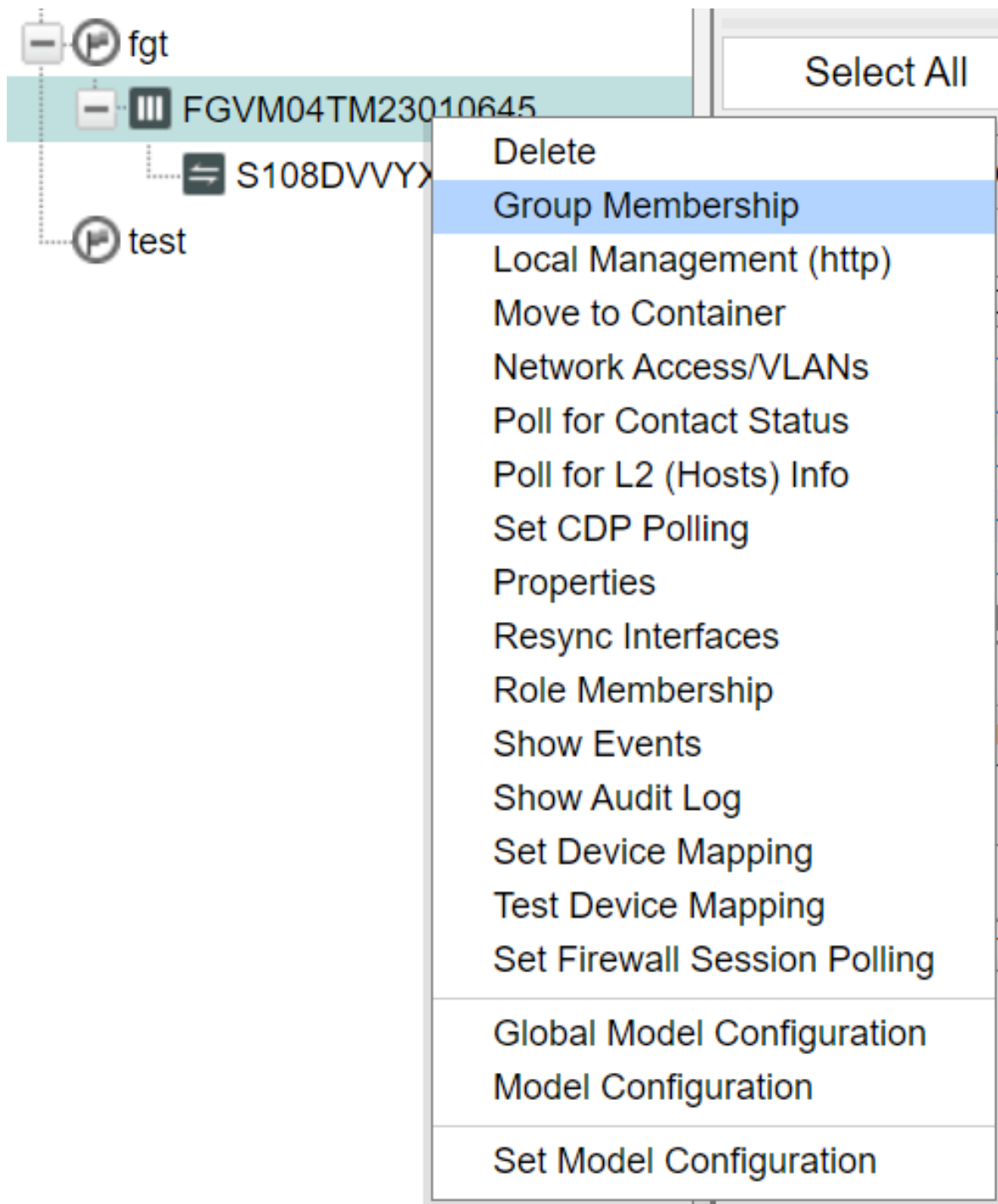
Instructions from the administration guide <http://docs.fortinet.com/document/fortinac-f/7.4.0/administration-guide/614635/add-or-modify-a-device>



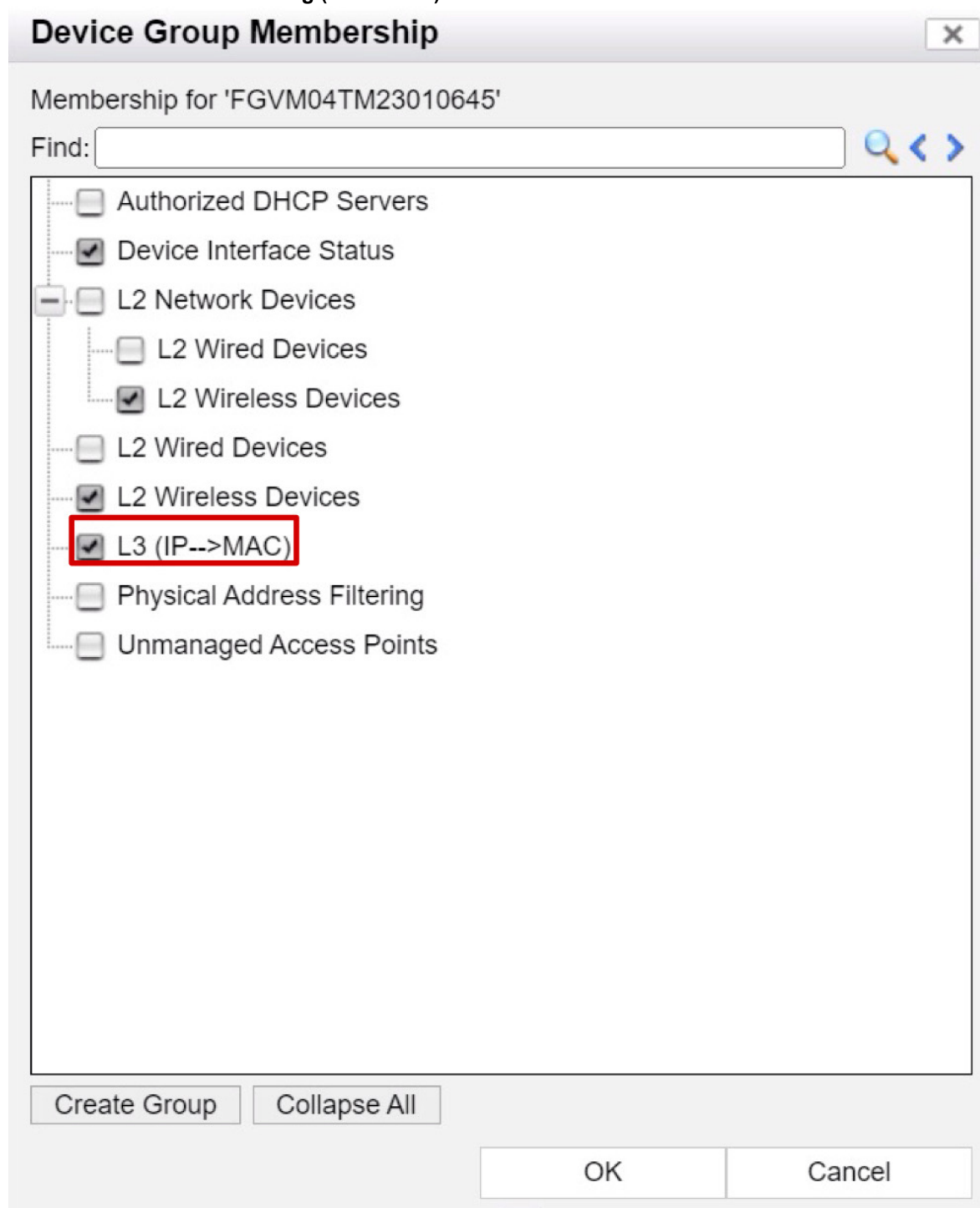
## 4. Enable L3 Polling (Optional)

When L3 Polling is enabled, FortiNAC collects additional information about network traffic at the IP layer, such as IP Addresses, subnets, and traffic flows. This information can enhance the visibility and analysis capabilities of FortiNAC, allowing for better monitoring of network activity and detection of anomalies.

1. Right click on the model in the left panel and select **Group Membership**.



2. Check the box next to **L3 Polling (IP --> MAC)** and click **OK**.



The image shows a 'Device Group Membership' dialog box for the group 'FGVM04TM23010645'. It features a search bar and a list of membership options. The 'L3 (IP-->MAC)' option is highlighted with a red box. At the bottom, there are buttons for 'Create Group', 'Collapse All', 'OK', and 'Cancel'.

**Device Group Membership**

Membership for 'FGVM04TM23010645'

Find:

- ☐ Authorized DHCP Servers
- ☒ Device Interface Status
- ☐ L2 Network Devices
  - ☐ L2 Wired Devices
  - ☒ L2 Wireless Devices
- ☐ L2 Wired Devices
- ☒ L2 Wireless Devices
- ☒ **L3 (IP-->MAC)**
- ☐ Physical Address Filtering
- ☐ Unmanaged Access Points

Create Group Collapse All

OK Cancel

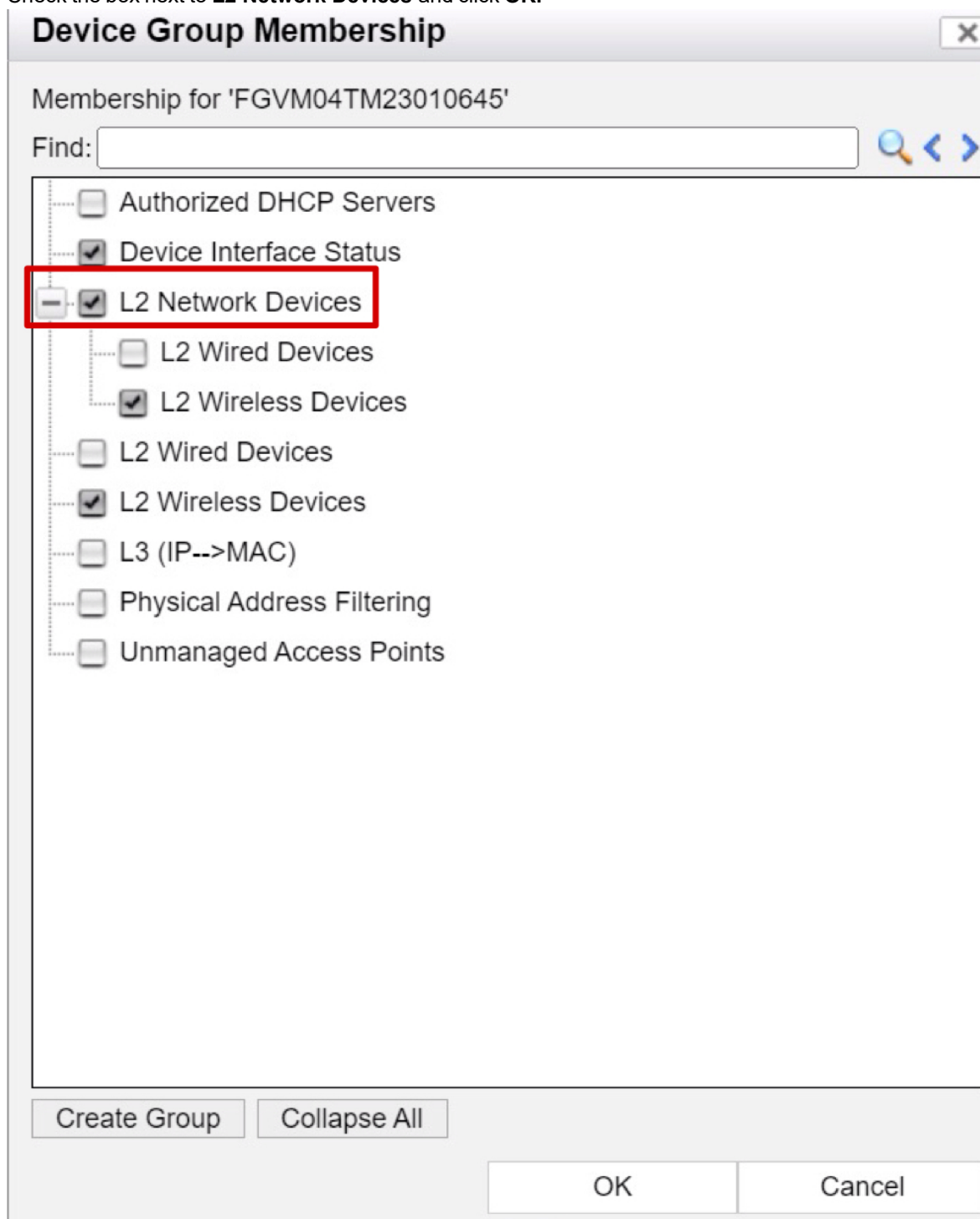
## 5. Enable L2 Polling (Optional)

Enabling L2 polling can enhance the integration between FortiGate and FortiSwitches, involving collecting data about the devices connected to network switches, including MAC addresses, VLAN information, and port status.

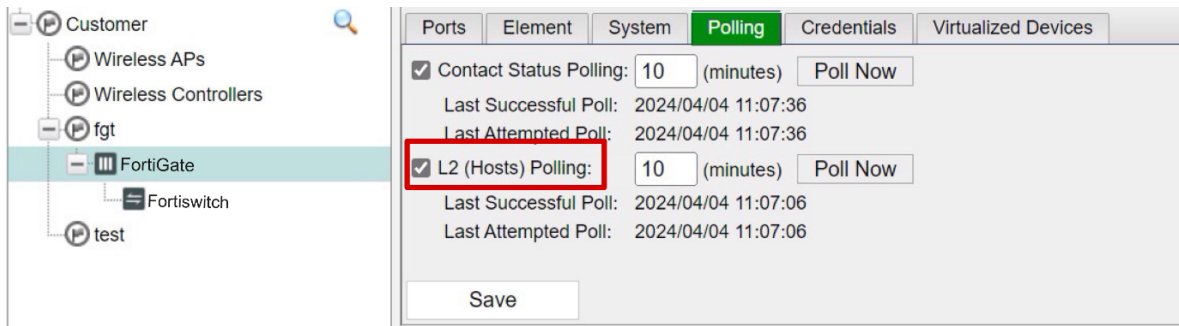
When FortiGate manages FortiSwitches through FortiLink, it primarily focuses on configuration management, security policies, and traffic control rather than detailed device monitoring at the MAC address level.

Therefore, L2 polling is optional for the basic integration between FortiGate and FortiSwitches.

1. Right click on the model in the left panel and select **Group Membership**.
2. Check the box next to **L2 Network Devices** and click **OK**.

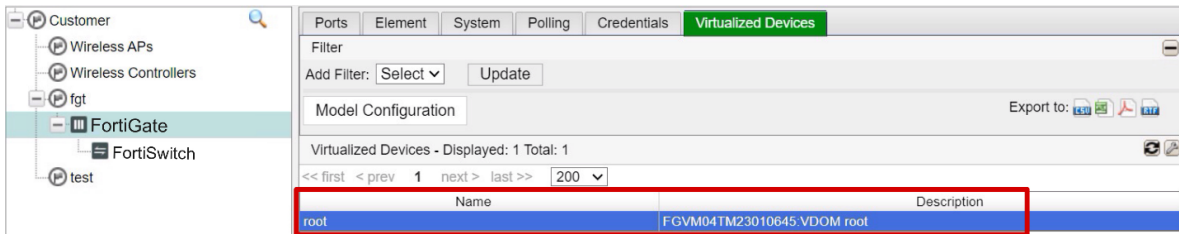


3. Click the **Polling** tab.
4. Check the box next to **L2 Hosts Polling**. If configuring Device Detection traps, set the **L2 (Hosts) Polling** value for 10 minutes.



## 6. Device Model Configuration

1. In the FortiNAC web interface, locate and click on the newly added/discovered FortiGate from the topology in **Network > Inventory**.
2. Select **Virtualized Devices** tab and double-click on **root** to go to Device Model Configuration



3. Under Logical Network Configuration, select the VLANs from the drill-down for each logical network as they apply:
  - a. Isolation VLANs (Registration, Quarantine, Dead End, Authentication)
  - b. Production VLANs

## c. Default VLAN (the “catch all” VLAN for registered endpoints)

## Edit Logical Network Configuration

Logical Network	?	Production
Network Access	?	Enforce
		VLAN Name <b>VLAN ID</b> Manual
		12
Additional RADIUS Attributes	?	None
Firewall Tags	?	+
Send Groups To Firewall	?	<input type="checkbox"/>
Firewall Groups	?	+

OK Cancel

## 7. Configure RADIUS

**Note:** If not using RADIUS, skip this section.

1. Configure the RADIUS server (local or proxy) and the appropriate access options. See the reference manual [Configure FortiNAC RADIUS Server for Device Integration](#)
2. Configure RADIUS Disconnect/CoA messages to enable FortiNAC to disconnect RADIUS clients. For instructions see [RFC5176 CoA/Disconnect Message Cookbook](#).

## 8. Review Enforcement Checklist

Before enabling enforcement, verify the following:

- The connected host or the host to be used for testing is in the expected host state (e.g. Rogue, Registered, etc).
- **Important:** Rogue MAC addresses detected on enforced ports will be isolated.
- Isolation VLANs are working. Test client in isolation VLAN is able to:
  - Obtain IP address via DHCP (if scopes are defined in ConfigWizard)
  - Access the Portal (if configured)

## 9. Configure Port of FortiSwitch

Enable enforcement on the test port by adding it to the appropriate enforcement group(s).

1. Expand the newly added/discovered FortiGate and select the FortiSwitch under it.
2. Under **Ports** tab, double click the port for usage to open the window for **Port Properties**.
3. Select **Group Membership** at the bottom and select the enforcement group(s) as required.

## Validate Enforcement

Connect a rogue host to the newly enforced port. Verify the following:

- Host is moved to the isolation VLAN
- Host is able to access the captive portal (if configured)
- Register the system and verify it moves to the appropriate VLAN
- Disable the system and verify it moves to the Dead End VLAN

For details on the above, refer to the Validate section of the [Enable Enforcement on Wired Network](#) reference manual.

If any of the below do not work as expected, refer to the Troubleshooting section of this document.



# Troubleshooting

## Related KB Articles

Refer to the applicable KB article(s):

[L2 to MAC events/traps are not generated on FortiSwitch](#)

[Troubleshooting SNMP Communication Issues](#)

[Troubleshooting Poll Failures](#)

[Wired hosts displaying incorrect status](#)

[Troubleshooting RADIUS clients not connecting](#)

[Troubleshooting VLANs Not Changing on a Wired Switch](#)

[Confirming Link State Traps via Administration UI](#)

[Link state SNMP traps not received by FortiSwitch](#)

[Confirming MAC Notification traps via Administration UI](#)

[Troubleshooting Link Mode FortiSwitch syslog for MAC notifications](#)

[No MAC notification syslog received from FortiSwitch in Link mode](#)

[IP address not updating after changing VLANs on a FortiSwitch using RADIUS](#)

[FortiNAC-F, FortiSwitch, FortiLink SNMPv3 MAC Notification Traps](#)

## Debugging

### FortiGate Commands

Function	Syntax
Enable debugging feature	<code>diagnose debug enable</code>
802.1X	<code>diagnose debug app eap_proxy 31 (EAP daemon)</code>
RADIUS Disconnect	<code>diag debug app radius-das 8</code>
Security Fabric Communication	<code>diagnose debug authd fsso list</code>
RADIUS sessions (Link Mode)	<code>diagnose switch-controller switch-info 802.1X</code>
Disable debugging feature	<code>diagnose debug disable</code>

RADIUS sessions (Link Mode) example response:

Client with MAC 00:0c:29:d4:4f:3c successfully authenticated using MAC-based 802.1x connecting to switch S248EPTF1800XXXX port 6, and was assigned VLAN 1.

**Managed Switch : S248EPTF1800XXXX**

**port6 : Mode: mac-based** (mac-by-pass disable)

Link: Link up

**Port State: authorized:** ( )

EAP pass-through mode : Enable

Native Vlan : 1

Allowed Vlan list: 1,4093

Untagged Vlan list: 1,4093

Guest VLAN :

Auth-Fail Vlan :

Switch sessions 1/240, Local port sessions:1/20

**Client MAC Type Vlan Dynamic-Vlan**

**00:0c:29:d4:4f:3c 802.1x 1 0**

**Sessions info:**

**00:0c:29:d4:4f:3c**

**Type=802.1x,MD5,state=AUTHENTICATED,etime=6,eap\_cnt=3 params:reAuth=3600**

## FortiSwitch Commands

RADIUS CoA activity:

diagnose user radius coa

Example response

25375.846 DAS: :radius\_das\_diag\_handler:

RADIUS DAS Server List:

FortiNAC-Radius:

Type: RADIUS\_8021X, IP: 10.12.240.7,

Last CoA/DM Client IP Addr : 10.12.240.7

Disc Reqs : 7

Disc ACKs : 5

```

Disc NAKs      : 2
CoA Reqs      : 0
CoA ACKs      : 0
CoA NAKs      : 0
1. DAS Server List

```

## FortiNAC Commands

Use the following KB article to gather the appropriate logs using the debugs below.

[Gather logs for debugging and troubleshooting](#)

**Note:** Debugs disable automatically upon restart of FortiNAC control and management processes.

Function	Syntax	Log File
FortiNAC Server (Proxy RADIUS)*	<code>nacdebug -name RadiusManager true</code>	<code>/bsc/logs/output.master</code>
FortiNAC Server (Local RADIUS)**	<code>nacdebug -name RadiusAccess true</code>	<code>/bsc/logs/output.master</code>
RADIUS Service (Local RADIUS)	<code>radiusd -X -l /var/log/radius/radius.log</code> Stop logging: Ctrl-C	<code>/var/log/radius/radius.log</code>
L2 related activity	<code>nacdebug -name BridgeManager true</code>	<code>/bsc/logs/output.master</code>
Syslog activity	<code>nacdebug -name SyslogServer true</code>	<code>/bsc/logs/output.master</code>
SSH/Telnet CLI activity	<code>nacdebug -name TelnetServer true</code>	<code>/bsc/logs/output.master</code>
SNMP activity	<code>nacdebug -name SnmpV1 true</code>	<code>/bsc/logs/output.master</code>
Standalone FortiSwitch specific	<code>nacdebug -name FortiSwitch true</code>	<code>/bsc/logs/output.master</code>

Function	Syntax	Log File
Managed (FortiLink) FortiSwitch	<code>nacdebug -name Fortinet true</code>	<code>/bsc/logs/output.master</code>
Disable debug	<code>nacdebug -name &lt;debug name&gt; false</code>	N/A

**\*Note:** FortiNAC will always return policy value “NativePolicy” in RADIUS Access Accept messages. Example:

```
yams.RadiusManager INFO :: ... :: RadiusPollThread0 RadiusServer accepting client
<client MAC address> for device <FortiSwitch or FortiGate IP address> and policy
```

**NativePolicy** ptime=0:0:13:13:13:17\*\*Logging for a given MAC Address:

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

Disable:

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

## Other Tools

**Send a RADIUS Disconnect:**

```
SendCoA -ip <devip> -mac <clientmac> -dis
```

Example:

```
SendCoA -ip 10.1.0.25 -mac 00:1B:77:11:CE:2F -dis
```

# Appendix

## Syslog Messages for MAC Address Notification

The FortiGate sends MAC Add, Delete, and Move syslog messages under the following conditions:

**Add/Discover** - Device generates traffic for the first time

**Delete** - MAC is removed from the address table. The time it takes for this to occur depends upon how the device is connected.

- Directly connected devices: MAC entry is removed immediately
- Devices behind an IP Phone, non-managed switch or hub: MAC entry must age out of the switch's MAC address table. This is based on the age time configured within the switch (typically minutes).

**Move** - device whose MAC is already learned on a port moves and connects to another port and generates traffic

## API Calls Made to FortiGate During Poll

### Layer 2 Poll

```
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 12:37:44:723 :: PollThread-
trap2 request WebTarget = https://10.12.240.13:443/api/v2/monitor/user/detected-
device?filter=is_online%3D%3Dtrue&global=1
```

```
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 12:37:44:830 :: PollThread-
trap2 request WebTarget =
https://10.12.240.13:443/api/v2/monitor/wifi/client/select?global=1
```

```
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 12:37:44:926 :: PollThread-
trap2 request WebTarget =
https://10.12.240.13:443/api/v2/monitor/vpn/ssl/select?vdom=%2A
```

```
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 12:37:46:995 :: PollThread-
trap2 request WebTarget =
https://10.12.240.13:443/api/v2/monitor/vpn/ipsec/select?vdom=%2A
```

FortiSwitches linked to the FortiGate

```
https://10.180.2.6:443/api/v2/monitor/switch-controller/managed-switch
```

## Layer 3 Poll

```
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 13:37:23:288 :: pool-5-thread-1  
request WebTarget = https://10.12.240.13:443/api/v2/cmdb/system/vdom
```

SSH to the device

modify each vdom returned by the previous command

issue a "get system arp" in each vdom and exit

```
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 13:37:23:677 :: pool-5-thread-1  
request WebTarget = https://10.12.240.13:443/api/v2/monitor/user/detected-  
device?filter=is\_online%3D%3Dtrue&global=1
```

```
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 13:37:23:787 :: pool-5-thread-1  
request WebTarget =  
https://10.12.240.13:443/api/v2/monitor/vpn/ipsec/select?vdom=%2A
```

```
yams.Fortigate.FortigateCommon INFO :: 2020-11-30 13:37:23:884 :: pool-5-thread-1  
request WebTarget =  
https://10.12.240.13:443/api/v2/monitor/vpn/ssl/select?vdom=%2A
```



Copyright© 2025 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.