FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com
http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM
http://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
Contents

Overview .................................................................................................................................................. 5
What it Does ........................................................................................................................................ 5
How it Works .......................................................................................................................................... 5
FortiLink Mode ..................................................................................................................................... 6
Standalone Mode .................................................................................................................................... 6
FortiSwitch FortiLink Integration ........................................................................................................... 7
Requirements .......................................................................................................................................... 7
Limitations ............................................................................................................................................... 7
Connection Notification Methods .......................................................................................................... 7
Configure FortiGate (Link Mode) .............................................................................................................. 9
  SNMP (System Level) ........................................................................................................................... 9
  Management Interface Configuration .................................................................................................... 10
  REST API ........................................................................................................................................... 10
VLANs .................................................................................................................................................. 10
  MAC Retention Period (FortiOS 6.2.1 and above) .............................................................................. 10
  Syslog (Optional) (FortiOS 6.2.1 and above) .................................................................................... 12
  Radius (Optional) .............................................................................................................................. 14
  SNMP Traps (Optional) ....................................................................................................................... 20
Configure FortiSwitch (Link Mode) .......................................................................................................... 24
  Management Interface ........................................................................................................................ 24
  RADIUS (Optional) ............................................................................................................................ 25
  SNMP Traps (Optional) (FortiOS 6.2.1 and above) ........................................................................... 26
  SNMP Traps (Optional) (FortiOS 6.0.0 and below) .......................................................................... 27
Configure FortiNAC (Link Mode) ........................................................................................................... 29
  Model the Device ............................................................................................................................... 29
  Device Model Configuration ............................................................................................................... 30
FortiSwitch Standalone Integration ........................................................................................................ 33
Requirements .......................................................................................................................................... 33
Connection Notification Methods ........................................................................................................... 33
RADIUS Authentication ......................................................................................................................... 33
  Management Interface IP Address .................................................................................................... 34
  SNMP ............................................................................................................................................... 35
  VLANs .............................................................................................................................................. 35
  RADIUS Authentication .................................................................................................................... 33
Overview

The information in this document provides guidance for configuring FortiSwitch devices 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 changes in device or FortiNAC software, the configuration order is subject to change. Therefore, this document simply details the items that must be configured to enable the management and control of users connecting to FortiSwitches. It is recommended to become familiar with basic FortiNAC wired management features by reading the available FortiNAC documentation.

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 Link State traps sent by the switch
- Syslog MAC Add/Remove/Delete messages (available for FortiLink Mode only)
- RADIUS communication
- L2 Polling (MAC address table read)
- L3 Polling (Arp Cache read)

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.

FortiNAC can manage the FortiSwitch in two different operational modes: Standalone and Link Mode.
FortiLink Mode

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

### Device Support Methods (FortiLink Mode)

<table>
<thead>
<tr>
<th>Endpoint Connectivity Notification</th>
<th>Reading MAC Address Tables (L2 Poll)</th>
<th>Reading IP Tables (L3 Poll)</th>
<th>Reading VLANs</th>
<th>Switching VLANs</th>
<th>De-auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Link Traps</td>
<td>REST API</td>
<td>REST API</td>
<td>REST API</td>
<td>REST API</td>
<td>RADIUS Disconnect*</td>
</tr>
<tr>
<td>Syslog MAC Add/Move/Delete</td>
<td>REST API</td>
<td>REST API</td>
<td>REST API</td>
<td>RADIUS</td>
<td></td>
</tr>
<tr>
<td>RADIUS (802.1x or MAC-auth)</td>
<td>REST API</td>
<td>REST API</td>
<td>REST API</td>
<td>RADIUS</td>
<td></td>
</tr>
</tbody>
</table>

Standalone Mode

FortiSwitches configured in standalone mode behave like typical network switches in FortiNAC. Management of endpoints connecting to the switches is accomplished using VLANs by placing assigning either ports or the endpoints themselves to VLANs according to their state within the FortiNAC system. As the state of an endpoint changes, its VLAN assignment is changed to reflect it.

FortiSwitch notifies FortiNAC of endpoint connectivity using either SNMP Traps or RADIUS. All other communication between FortiNAC and FortiSwitches occur using HTTPS (RESTful API). HTTPS access must be allowed on the FortiSwitch interface used to communicate to FortiNAC.

### Device Support Methods (Standalone Mode)

<table>
<thead>
<tr>
<th>Endpoint Connectivity Notification</th>
<th>Reading MAC Address Tables (L2 Poll)</th>
<th>Reading IP Tables (L3 Poll)</th>
<th>Reading VLANs</th>
<th>Switching VLANs</th>
<th>De-auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Link Traps</td>
<td>REST API</td>
<td>REST API</td>
<td>REST API</td>
<td>REST API</td>
<td>RADIUS Disconnect*</td>
</tr>
<tr>
<td>RADIUS (802.1x or MAC-auth)</td>
<td>REST API</td>
<td>REST API</td>
<td>REST API</td>
<td>RADIUS</td>
<td></td>
</tr>
</tbody>
</table>

*Some FortiSwitch models (such as the 1xxE) do not support RADIUS CoA and Disconnect. Refer to the list of supported features in the FortiSwitch Release Notes in the Fortinet Document Library for more details. FortiNAC must disconnect (de-auth) in order to change network access.

Click on the appropriate link below to begin configuration:

- FortiSwitch FortiLink Integration
- FortiSwitch Standalone Integration
FortiSwitch FortiLink Integration

Requirements

- FortiNAC Software Version
  - Minimum 8.3.2
  - Preferred 8.3.6 or higher – see Limitation 1 below
  - RADIUS support for FortiLink FSW's: 8.7.0 or higher
- FortiOS Version
  - Minimum 6.x
  - Preferred 6.2.x – see Limitation 2 below
- FortiGate
  - SNMP community or account
  - Account for SSH and REST API access
- FortiSwitch
  - SNMP community or account
  - Valid IP address (not 169.x.x.x) for switches configured for RADIUS authentication.

Limitations

1. FortiNAC versions 8.3.6 and above dynamically learn REST API port in use via SSH. FortiNAC versions below 8.3.6 uses port TCP 443 by default. To modify FortiNAC port, see Appendix.

2. 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.

Connection Notification Methods

- **Syslog Messages**: FortiGate sends MAC Add, Delete, and Move messages. When a syslog message is received, FortiNAC updates the database with the new connection information (MAC address and location). This functionality is similar to SNMP MAC Notification traps used by other switch vendors.
  - Requires FNAC version 8.6.2 or higher
  - Requires FortiOS 6.2.1 or higher

- **Radius Authentication**: 802.1x and MAC Authentication methods are supported. Sends RADIUS requests 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.
  - Requires FNAC 8.7.0 or higher.
  - FortiSwitches configured for RADIUS authentication must have a valid IP address (not 169.x.x.x). FNAC uses this address when disconnecting clients (RADIUS CoA).
802.1x RADIUS Server Requirement: The encryption method for user names and passwords passed between FortiNAC and the RADIUS server must be set to PAP. This affects the following accounts or user names and passwords created on the RADIUS server:

- The validation account created for communication with FortiNAC and entered in the RADIUS Server Profile configuration.
- Network users that access the network via the captive portal and are authenticated through RADIUS.
- Admin UI users authenticated through RADIUS.
- VPN Users authenticated through RADIUS.

Do not use asymmetric routing between the FortiGate and the FortiNAC server. RADIUS requests and responses between the FortiNAC server and the FortiGate must travel through the same interface on the FortiNAC server.

FortiNAC does not control the Guest and Auth-Fail VLANs. Endpoints placed in those VLANs may not be managed.

Link traps can be used in conjunction with RADIUS Authentication if desired.

**SNMP Link Traps:** This is the least efficient method of endpoint notification. Link Traps originate from the FortiSwitch and are routed through the FortiGate. When a link trap is received, FortiNAC performs a L2 poll of the FortiGate to update the database with the new connection information.

**Note:** SNMP Link Traps DO NOT notify FortiNAC of indirect connections. This includes both new connections and disconnects. Examples include connections behind IP Phone, hub or unmanaged access point.
Configure FortiGate (Link Mode)

**SNMP (System Level)**

SNMP is required for communication with FortiNAC and must be configured. SNMP versions 1, 2c and 3 are supported.

1. In the FortiGate UI, navigate to System > SNMP.
2. Enable SNMP Agent.
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.
4. Click OK to save any modifications.

### SNMP Settings (v1/v2c)

<table>
<thead>
<tr>
<th>Community Name</th>
<th>Community Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Selected</td>
</tr>
<tr>
<td>Hosts</td>
<td>IP Address: &lt;eth0 IP address of FortiNAC Control Server&gt;</td>
</tr>
<tr>
<td></td>
<td>Host Type: Accept Queries Only</td>
</tr>
<tr>
<td>Queries</td>
<td>V1 or v2 enabled</td>
</tr>
<tr>
<td></td>
<td>Port: 161</td>
</tr>
<tr>
<td>Traps</td>
<td>V1 or v2 enabled</td>
</tr>
<tr>
<td></td>
<td>Port: 162</td>
</tr>
<tr>
<td>SNMP Events</td>
<td>&lt;all disabled&gt;</td>
</tr>
</tbody>
</table>

### SNMP Settings (v3)

<table>
<thead>
<tr>
<th>User Name</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Selected</td>
</tr>
<tr>
<td>Security Level</td>
<td>Authentication (No Private)</td>
</tr>
<tr>
<td></td>
<td>Authentication Algorithm: SHA1 or MD5</td>
</tr>
<tr>
<td></td>
<td>Password</td>
</tr>
<tr>
<td></td>
<td>Authentication (Private)</td>
</tr>
<tr>
<td></td>
<td>Authentication Algorithm: SHA1 or MD5</td>
</tr>
<tr>
<td></td>
<td>Password</td>
</tr>
<tr>
<td></td>
<td>Encryption Algorithm: DES or AES256</td>
</tr>
<tr>
<td>Hosts</td>
<td>IP Address: &lt;eth0 IP address of FortiNAC Control Server&gt;</td>
</tr>
<tr>
<td></td>
<td>Host Type: Accept Queries Only</td>
</tr>
<tr>
<td>Queries</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>Port: 161</td>
</tr>
<tr>
<td>Traps</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>Port: 162</td>
</tr>
<tr>
<td>SNMP Events</td>
<td>&lt;all disabled&gt;</td>
</tr>
</tbody>
</table>
Management Interface Configuration

Configure the interface used to communicate with FortiNAC to allow the required protocols.

1. In the FortiGate UI, navigate to **Network > Interfaces**.
2. Double click the interface whose IP address will be used to communicate with FortiNAC.
3. Under **Administrative Access**, enable the following protocols:
   - HTTPS
   - HTTP
   - SNMP
   - SSH
   - RADIUS Accounting (required if configuring RADIUS authentication)
   - Security Fabric Connection

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

REST API

REST API is required for communication with FortiNAC and must be 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.

VLANs

In the FortiGate UI, ensure VLANs are configured and working on the FortiSwitch for all FortiNAC states desired to be enforced (Registration, Remediation, etc). This information can be accessed in the FortiGate UI under **WiFi & Switch Controller > FortiSwitch VLANs**.

MAC Retention Period (FortiOS 6.2.1 and above)

In the FortiGate CLI, set the mac-retention-period option to 0 in the global settings. When set to 0, the MAC is no longer retained beyond the mac-aging-interval.

Type the following commands:

```
config switch-controller global
set mac-retention-period 0
end
```

FortiNAC polls the FortiGate in order to determine the device’s connection status. Setting the mac-retention-period to 0 enables FortiNAC to provide more accurate connection information: FortiGate entries age immediately once the FortiSwitch removes the corresponding entry from its own table. 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 FGT configuration:
- Syslog (Optional) (FortiOS 6.2.1 and above)
- Radius (Optional)
- SNMP Traps (Optional)
**Syslog (Optional) (FortiOS 6.2.1 and above)**

Configure the FortiGate to send MAC Add, Delete, and Move syslog messages to FortiNAC. Messages trigger under the following conditions:

**Add** - 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

"MAC Learned" and "MAC Removed" events are logged in FortiNAC as these messages are processed.

1. In the FortiGate CLI configure syslog to send messages to FortiNAC. For best performance, setup a filter to only send the relevant syslog messages. Otherwise, the FortiGate sends FortiNAC all the syslog messages sent when “System activity event” logging is enabled.

```
config log syslogd setting
set status enable
set server "<FortiNAC eth0 IP address>"
set source-ip <Device IP address modeled in FortiNAC>
end
config log syslogd filter
set filter "logid(0100032615,0100032616,0100032617)"
end
```

Multiple syslog servers (up to 4) can be created on a FortiGate with their own individual filters. This is useful for High Availability environments:

```
config log syslogd2 setting
set status enable
set server "<FortiNAC Secondary Server eth0 IP address>"
end
config log syslogd2 filter
set filter "logid(0100032615,0100032616,0100032617)"
end
```
Example:
Primary FortiNAC server: 10.12.240.7
Secondary FortiNAC server: 10.12.240.8

config log syslogd setting
    set status enable
    set server "10.12.240.7"
end
config log syslogd filter
    set filter "logid(0100032615,0100032616,0100032617)"
end
config log syslogd setting
    set status enable
    set server "10.12.240.8"
end
config log syslogd filter
    set filter "logid(0100032615,0100032616,0100032617)"
end

2. Enable MAC event logging.
   config switch-controller global
   set mac-event-logging enable
   end

Proceed to Configure FortiSwitch.
**Radius (Optional)**

**Firewall policy for RADIUS traffic**

Create a firewall policy to allow the RADIUS authentication related traffic from the Fortilink interface to the outbound interface on the FortiGate.

**UI Method**

1. In the FortiGate UI, navigate to **Policy & Objects > IPv4 Policy**
2. Either add or modify an existing policy
3. Configure using the table below.

<table>
<thead>
<tr>
<th>Policy Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Policy Name</td>
</tr>
<tr>
<td><strong>Incoming Interface</strong></td>
</tr>
<tr>
<td>FortiLink interface(s) and Management interface used to communicate with FortiNAC</td>
</tr>
<tr>
<td><strong>Outgoing Interface</strong></td>
</tr>
<tr>
<td>FortiLink interface(s) and Management interface used to communicate with FortiNAC</td>
</tr>
<tr>
<td><strong>Source</strong></td>
</tr>
<tr>
<td>All</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>All</td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
</tr>
<tr>
<td>Always</td>
</tr>
<tr>
<td><strong>Service</strong></td>
</tr>
<tr>
<td>All</td>
</tr>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>Accept</td>
</tr>
<tr>
<td><strong>NAT</strong></td>
</tr>
<tr>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Enable this policy</strong></td>
</tr>
<tr>
<td>Selected</td>
</tr>
</tbody>
</table>
CLI Example

cfg firewall policy
def 5
    set name "Wired FSW Radius"
    set uuid 1dddd
    set srcintf "FortiLink" "Management"
    set dstintf "Management" "FortiLink"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set nat disable
next
de

RADIUS Server and User Group

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

<table>
<thead>
<tr>
<th>RADIUS Server Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Name representing RADIUS server (FortiNAC)</td>
</tr>
<tr>
<td><strong>Authentication Method</strong></td>
<td>Default (802.1x authentication) Specify Authentication Method (PAP) (Required for MAC-Authentication only)</td>
</tr>
<tr>
<td><strong>NAS IP/Call Station ID</strong></td>
<td>Leave blank</td>
</tr>
<tr>
<td><strong>Primary Server Address</strong></td>
<td>FortiNAC Server/Control server eth0 interface IP Address</td>
</tr>
<tr>
<td><strong>Primary Server Secret</strong></td>
<td>Important: This value must match the secret values configured on FNAC and any optional terminating RADIUS server used to support 802.1x.</td>
</tr>
<tr>
<td><strong>Secondary Server Name/IP</strong></td>
<td>High Availability: IP address of secondary control server (Do not use Shared IP address)</td>
</tr>
<tr>
<td><strong>Secondary Server Secret</strong></td>
<td>Important: This value must match the secret values configured on FNAC and any optional terminating RADIUS server used to support 802.1x.</td>
</tr>
<tr>
<td><strong>Change of Authorization (CoA)</strong></td>
<td>Enabled (Disabled by default) Note: This setting can only be enabled via CLI</td>
</tr>
<tr>
<td><strong>Accounting</strong></td>
<td>Enabled (Disabled by default) Note: This setting can only be configured via CLI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Group Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Name of the group which the Radius server will be a member</td>
</tr>
<tr>
<td><strong>Members</strong></td>
<td>User name of Radius server</td>
</tr>
</tbody>
</table>
config user radius
edit "<name>"
set server "<FNAC eth0 IP address>"
set secret <secret>
set acct-interim-interval 86400
set radius-coa enable
config accounting-server
edit <number>
set status enable
set server "<FNAC eth0 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 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 1ddddd
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 1ddddd
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.

**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**.

<table>
<thead>
<tr>
<th>Security Policy Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Security mode</strong></td>
</tr>
<tr>
<td><strong>User groups</strong></td>
</tr>
<tr>
<td><strong>MAC authentication bypass</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>EAP pass-through</strong></td>
</tr>
</tbody>
</table>

**CLI Method**

```bash
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 disable
set auth-fail-vlan disable
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 disable
  set framevid-apply enable
  set radius-timeout-overwrite disable
next
end

5. RADIUS Authentication is enabled on a per port basis. Apply the 802.1x security policy to the desired edge ports of the managed FortiSwitch.

UI Method
a. Navigate to WiFi & Switch Controller > FortiSwitch Ports
b. 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.
c. Select the security policy and click Apply.
CLI Method:
config switch-controller managed-switch
edit <FSW serial number>
config ports
edit "<FSW edge port to be configured for RADIUS>"
set port-security-policy "<policy name>"
next
edit "<FSW 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

Proceed to Configure FortiSwitch.
SNMP Traps (Optional)

Firewall Policy for SNMP Traps

In the FortiGate UI, configure a firewall policy to allow the SNMP Link traps to be forwarded to the FortiNAC from the Dedicated to FortiSwitch port.

Example

1. Navigate to Network > Interfaces and identify the port and associated interface with the FortiLink. In the below screen capture, port 11 is connected to a FortiSwitch via FortiLink.
2. Navigate to **Policy & Objects > IPv4 Policy**.

3. Create or modify an existing policy to allow traps to be sent from the FortiLink port to the FortiGate uplink.
   
   **Requirement:** NAT must be enabled so that traffic is sent to FortiNAC from the FortiGate IP address. This allows the traps to be recognized and processed.
Note: Some FortiOS versions may not show FortiLink ports as available options when creating the policy in FortiGate’s UI. In these cases, configure via the FortiGate CLI. For instructions on accessing the CLI via the FortiGate UI, see Appendix.

Type the following commands:

```bash
config firewall policy
edit <number>
set name "<policy name>"
set srcintf "<incoming interface name>"
set dstintf "<outgoing interface name>"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set fsso disable
set nat enable
next
end
```

Example:
```bash
edit 17
set name "FSW->LAN"
set uuid b6cf8c8e-660d-51e9-8cb9-4be8c95c7466
set srcintf "Link"
set dstintf "lan"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set fsso disable
set nat enable
next
```
**Configure Link Traps (FortiOS 6.2.1 and above)**

In the FortiGate CLI, configure the SNMP parameters for the link mode FortiSwitch. If High Availability, include Secondary Server information where indicated.

**Important:** 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.

In the FortiGate CLI, type the following commands:

```
config switch-controller snmp-sysinfo
set status enable
end
config switch-controller snmp-community
edit <number>
set name "<community name>"
config hosts
edit <number>
set ip <FortiNAC eth0 IP address> <FortiNAC eth0 mask>
next
edit <new number>
set ip <Secondary FortiNAC eth0 IP address> <Secondary FortiNAC eth0 mask>
end
set trap-v2c-status disable
next
end
```

Example:

FortiNAC ETH0 IP address: 10.12.240.7/24
FortiNAC (Secondary Server) ETH0 IP address: 10.12.240.8/24
Community name: fortinet

```
config switch-controller snmp-sysinfo
set status enable
end
config switch-controller snmp-community
edit 1
set name "fortinet"
config hosts
edit 1
set ip 10.12.240.7 255.255.255.0
next
edit 2
set ip 10.12.240.8 255.255.255.0
end
set trap-v2c-status disable
next
end
```
Configure FortiSwitch (Link Mode)

Management Interface

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

Allow the following protocols:
PING
HTTPS
SSH

FortiSwitches configured for RADIUS authentication must have a valid IP address (not 169.x.x.x). FNAC 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

Click on the appropriate link below to continue FSW configuration:
Radius (Optional)
SNMP Traps (Optional) (FortiOS 6.2.1 and above)
SNMP Traps (Optional) (FortiOS 6.2.0 and below)
**RADIUS (Optional)**

In the FortiSwitch CLI, enable the processing of RADIUS CoA and disconnect messages by including `radius-acct` as a permitted management access type. For FortiSwitch CLI access instructions, see Appendix.

CLI Method:
```
config system interface
edit "internal"
set allowaccess ping https ssh radius-acct
next
```

Example:
```
config system interface
  edit "internal"
    set allowaccess ping https ssh radius-acct
next
end
```

Proceed to [Configure FortiNAC](#).
**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. For FortiSwitch CLI access instructions, see Appendix.

```
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.
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. For FortiSwitch CLI access instructions, see Appendix.

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 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.
Configure FortiNAC (Link Mode)

Model the Device

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

1. In the Administration UI, Navigate to Network Device > Topology

2. Discover or add the FortiGate. For instructions, see Add/Modify a Device or Discover Devices in the Administration Guide in the Fortinet Documentation Library.

   SNMP Settings: SNMP v1 or v3 credentials
   
   CLI Settings: Credentials used for both SSH and API access.
   
   - FNAC establishes SSH session to determine the appropriate API port. If the FGT is using a port other than 22 for SSH, update the FGT model in FNAC with the correct port. See KB article for instructions:
     
     Modify Telnet and SSH port settings for device models
     https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD47479
   
   - Must allow access to the global domain and with the user-admin admin profile. This is to support access for multiple VDOMs. To create or view user accounts, navigate to System > Administrators in the FortiGate UI.

The FortiGate will display in Topology as a wireless device since it can act as a wireless controller. Any FortiSwitches managed by the FortiGate are automatically added. In the below example, the managed switch is S108EN4N17001579.

Note the following:

- If CLI credentials were not included when adding the device, any managed FortiSwitches will not be discovered until the CLI credentials are added to the Model Configuration. Once credentials are added, right click on the model and select Resync Interfaces.

- Although the switch is listed separately in Topology, all ports will be displayed in the FortiGate Ports tab. The FortiSwitch model will not display any ports.

- 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.
3. (FortiNAC versions 8.3.5 and below) Modify FortiNAC to use a different API port if necessary. FortiNAC uses 443 by default. For instructions, see Modify API Port in the Appendix.

Device Model Configuration

All FortiSwitch ports for all VDOMs are consolidated into a single list that appears under the "Ports" tab for the Fortigate model. The port names are constructed from the FortiSwitch serial number and the Port name (ie. S108EN4N17001579:port8).

All configuration of groups, VLANs and any other functionality is done using the FortiGate device model. The individual FortiSwitch models will show an empty listing under the “Ports” tab (Ports – Displayed:0 Total:0).

VLANs (FortiNAC version 8.5 and higher)

Logical Networks: Introduced in version 8.5. For more information, see section Logical Networks in the Administration Guide in the Fortinet Documentation Library.

1. With the FortiGate’s model selected in the left panel, click the Virtualized Devices tab in the right panel.
2. Click the desired VDOM, right click and select **Model Configuration**.

![Model Configuration Diagram]

3. Under **Network Access**, select the VLANs from the drill-down for each logical network as they apply:
   - Isolation VLANs (Registration, Quarantine, Dead End, Authentication)
   - Production VLANs
   - Default VLAN (the “catch all” VLAN for registered endpoints)

**Important:** The list of VLANs displayed in the drill-down contains all VLANs configured for all “Virtualized Devices” (VDOMs). Therefore, only select a VLAN that is appropriate to the selected VDOM and switch.

![Network Access Diagram]

4. Click **Submit Query**. Proceed to **Validate Visibility**
VLANs (FortiNAC versions below 8.5)

1. With the FortiGate’s model selected in the left panel, click the **Virtualized Devices** tab in the right panel.

2. Click the desired VDOM, right click and select **Model Configuration**.

3. Under Network Access, select the VLANs from the drill-down for as they apply:
   
   - Isolation VLANs (Registration, Quarantine, Dead End, Authentication)
   - Default VLAN (the “catch all” VLAN for registered endpoints)

   **Important:** The list of VLANs displayed contains all VLANs configured for all “Virtualized Devices” (VDOMs). Therefore, only select a VLAN that is appropriate to the selected VDOM.

   **Note:** Each port model in FortiNAC is initialized with a default VLAN value. This default is the untagged VLAN to which each port belongs when the Fortigate and FortiSwitch is discovered. Setting the "Default" VLAN in the VDOM model configuration view forces an overwrite of that per-port value to the new value. Therefore, in many cases, the Default VLAN should be left as "(None)" to initialize per-port defaults.

4. Click **Submit Query**.

Proceed to **Validate Visibility**
FortiSwitch Standalone Integration

Requirements

- FortiNAC Software Version 8.3.3 or higher
- FortiSwitch Firmware Version 6.0.0 build 0042 or higher
- SNMP community or account on each FortiSwitch
- Account for SSH and REST API access
- Enable SNMP traps on each FortiSwitch if RADIUS Authentication is not used

Connection Notification Methods

- **SNMP Link Traps:** Link Traps originate from the FortiSwitch. When a link trap is received, FortiNAC performs a L2 poll to update the database with the new connection information. SNMP Link Traps DO NOT notify FortiNAC of indirect connections. This includes both new connections and disconnects. Examples include connections behind IP Phone, hub or unmanaged access point.

- RADIUS Authentication

RADIUS Authentication

Sends notifications 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).

  - **MAC-based Authentication:** Endpoints are authenticated based on the MAC address. This requires no configuration on the endpoint.
  - **802.1x Authentication:** Endpoints are authenticated based on user information. This requires supplicant configuration on the endpoint.

Multi-Access: it is possible to assign unique VLANs to each endpoint connecting to a single port. Since each endpoint is managed independently, this configuration allows for greater flexibility and security.

Note the following:

  - FortiNAC does not control the Guest and Auth-Fail VLANs. Endpoints placed in those VLANs may not be managed.
  - Link traps can be used in conjunction with RADIUS Authentication if desired.

802.1x RADIUS Server Requirements

- The encryption method for user names and passwords passed between FortiNAC and the RADIUS server must be set to PAP on the FortiSwitch. This affects the validation account created for communication with FortiNAC and entered in the RADIUS Server Profile configuration.
**Network Requirements**

- Do not use asymmetric routing between the FortiSwitch and the FortiNAC server. RADIUS requests and responses between the FortiNAC server and the FortiSwitch must travel through the same interface on the FortiNAC server.

Configure FortiSwitch (Standalone Mode)

**Management Interface IP Address**

In the FortiSwitch CLI, configure the management interface IP address. For FortiSwitch CLI access instructions, see Appendix.

**Requirements**: Allow the following protocols: SNMP, ping, https, SSH, radius-acct

1. Configure management interface name (if not already created). Type

   ```
   config switch lldp settings
   show
   ```

2. If not configured, type

   ```
   set management-interface "<management interface name>"
   end
   ```

3. Configure management interface. Type

   ```
   config system interface
   edit "<management interface name>"
   set ip <management IP address> <mask>
   set allowaccess ping https http ssh snmp radius-acct
   set type physical
   set snmp-index <number>
   next
   end
   ```

**Management IP Example**

internal = Management interface name
10.12.240.13/24 = FortiSwitch management interface IP address

```plaintext
config system interface
dep "internal"
   set ip 10.12.240.13 255.255.255.0
   set allowaccess ping https http ssh snmp radius-acct
   set type physical
   set snmp-index 12
next
end
```
**SNMP**

1. In the FortiSwitch UI, navigate to **System > Config > SNMP**.
2. Enable SNMP agent with credentials that can be used to communicate with the FortiNAC primary Control Server eth0 IP address.

**VLANs**

In the FortiSwitch UI, navigate to **Switch > VLAN**. Ensure VLANs are configured and working for all FortiNAC states desired to be enforced (Registration, Remediation, etc).
**RADIUS (Optional)**

**Requirements:**
- RADIUS timeouts should be large enough to allow some transaction delays. Many devices use default timeout values under 10 seconds. It is recommended to use larger values for busy environments, though experimentation to find the optimal value may be needed.
- For 801.x environments, consider setting up the actual RADIUS server as a backup to be used in the event that none of the FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.

1. In the FortiSwitch UI, navigate to **System > Authentication > RADIUS**.
2. Add FortiNAC as the RADIUS server using the configurations in the table below.

<table>
<thead>
<tr>
<th><strong>RADIUS Settings</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Name of FortiNAC Server</td>
</tr>
<tr>
<td><strong>Authentication Scheme</strong></td>
<td>Specify Authentication Method (PAP) (Required for MAC-Authentication only)</td>
</tr>
<tr>
<td><strong>NAS IP/Call Station ID</strong></td>
<td>FortiSwitch management IP address</td>
</tr>
<tr>
<td><strong>Primary Server Address</strong></td>
<td>FortiNAC Server/Control server eth0 interface IP Address</td>
</tr>
<tr>
<td><strong>Primary Server Secret</strong></td>
<td><strong>Important:</strong> This value must match the secret values configured on FNAC and any optional terminating RADIUS server used to support 802.1x.</td>
</tr>
<tr>
<td><strong>Secondary Server Name/IP</strong></td>
<td><strong>High Availability:</strong> IP address of secondary control server (Do not use Shared IP address)</td>
</tr>
<tr>
<td><strong>Secondary Server Secret</strong></td>
<td><strong>Important:</strong> This value must match the secret values configured on FNAC and any optional terminating RADIUS server used to support 802.1x.</td>
</tr>
<tr>
<td><strong>Authentication port</strong></td>
<td>UDP 1812</td>
</tr>
</tbody>
</table>

3. Click **Update**.
4. Connect to the FortiSwitch CLI and enable Change of Authorization (CoA) and Accounting. Type the following commands

```
config user radius
edit "<name entered for RADIUS server in UI>"
set radius-coa enable
set acct-interim-interval 86400
config acct-server
edit 1
set status enable
set server "<FortiNAC Server/Control server eth0 interface IP Address>"
next
end
```

**RADIUS Example**

```
config user radius
edit "FNAC"
  set acct-interim-interval 86400
  config acct-server
    edit 1
    set status enable
    set server "10.12.240.7"
  set secret ENC
next
end
set auth-type pap
set nas-ip 10.12.240.13
set radius-coa enable
set secret ENC pm46fi...
set server "10.12.240.7"
next
end
```

Proceed to Configure FortiNAC.
**SNMP Traps (Optional)**

Enable SNMP traps on each FortiSwitch if RADIUS Authentication will not be used.

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.

Type the following commands

```plaintext
config system snmp community
edit <number>
config hosts
edit <number>
set interface ""<management interface name>""
set ip <eth0 IP address> <mask>
next
end
set trap-v2c-status disable
next
end
```

**SNMP Trap Example**

The below is used in all the following configuration examples:

10.12.240.7/24 = Primary NAC Server eth0 IP address  
Community name = fortinet

```plaintext
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](#).
Configure FortiNAC (Standalone mode)

Model RADIUS Server (Optional)

802.1x only: 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 more information, see section Configure RADIUS Server Profiles in the Administration Guide in the Fortinet Documentation Library.

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

Note: This configuration is not required for MAC-Authentication configurations.

Model the Device

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

1. Navigate to Network Device > Topology

2. Discover or add the FortiSwitch using the management IP address. For instructions, see Add/Modify a Device or Discover Devices in the Administration Guide in the Fortinet Documentation Library.

SNMP Settings: SNMP v1 or v3 credentials

CLI Settings: Credentials used for API access (must have an access profile of super_admin on the switch)
Device Model Configuration (Version 8.5 and Higher)

1. With the FortiSwitch model selected in the left panel, click the **Model Configuration** tab in the right panel.

2. Fill in the following fields as they apply. For more details, see **Model Configuration** in the Administration Guide in the Fortinet Documentation Library.

   - **Logical Networks**: Introduced in version 8.5. For more information, see section **Logical Networks** in the Administration Guide in the Fortinet Documentation Library.

   Under **Network Access**, select the VLANs from the drill-down for each logical network as they apply:
   - Isolation VLANs (Registration, Quarantine, Dead End, Authentication)
   - Production VLANs

   ![Model Configuration Screenshot]

   - **802.1x Radius Authentication**: Optional. Click **Enable RADIUS authentication for this device** to expose the below options.
     - Select the desired RADIUS servers FortiNAC will proxy the RADIUS requests.
     - Enter the RADIUS Secret. **Important**: The RADIUS Secret used must be exactly the same in the Model Configuration, the FortiSwitch and the RADIUS server.

3. Click **Save**.

   Proceed to **Validate Visibility**
Device Model Configuration (Versions below 8.5)

1. With the FortiSwitch model selected in the left panel, click the right click and select Model Configuration.

2. Fill in the following fields as they apply. For more details, see Model Configuration Parameters in the Administration Guide in the Fortinet Documentation Library.

- **Network Access**
  - VLAN ID for each state (Registration, Remediation, Authentication, Deadend)
  - VLAN ID Default (the “catch all” VLAN for registered endpoints).

  **Note:** Each port model in FortiNAC is initialized with a default VLAN value. This default is the untagged VLAN to which each port belongs when the FortiSwitch is discovered. Setting the "Default" VLAN model configuration view forces an overwrite of that per-port value to the new value. Therefore, in many cases, the Default VLAN should be left as "(None)" to initialize per-port defaults.

- **802.1x Radius Authentication** (Optional):
  - Under RADIUS, select the desired RADIUS servers FortiNAC will proxy the RADIUS requests.
  - Enter the RADIUS Secret. **Important:** The RADIUS Secret used must be exactly the same in the Model Configuration, the FortiGate and the RADIUS server.

3. Click Apply.

Proceed to Validate Visibility.
Validate Visibility

1. Poll the newly added devices to read the device's MAC address table (L2 Poll) and ARP cache (L3 Poll) if applicable.
   - **Standalone Mode:** Click the Polling tab in the right panel of the FortiSwitch model and click Poll Now next to L2 (Hosts) Polling.
   - **FortiLink Mode:** Click the Polling tab in the right panel of the FortiGate model.
     - Click Poll Now next to L2 (Hosts) Polling
     - Click Poll Now next to L3 (IP → MAC) Polling

2. Click on the Ports tab of the FortiSwitch (Standalone Mode) or FortiGate (FortiLink Mode).

3. Review the values populated for each port (Label, Connection State, etc) and verify they are accurate. FortiLink ports: Ports connecting back to FortiGate in FortiLink mode display a Connection State of Learned Uplink.

For details regarding this view, see Ports View in the Administration Guide in the Fortinet Documentation Library.

![Port Details](image)

Note: Current VLAN values may not be accurate for switches authenticating using RADIUS. At this time, the port view only allows for a single port-based VLAN to be displayed for the Current VLAN. This VLAN usually does not match the dynamic VLAN assigned to the clients that have authenticated using RADIUS.
4. If the Adapter tab is not already visible, click the Show Details Panel button at the bottom of the window.

5. Verify connection information for endpoints currently connected to those is accurate by clicking on one of the ports showing a connection. The adapter tab below should reflect the correct Adapter Status, Host Status, IP Address, Physical (MAC) Address, Location and Access Value. If connection information is not correct, see Inaccurate Port Connection Information in the Troubleshooting section.

Once visibility has been successfully validated, proceed to Configure Enforcement.
Configure Enforcement

Configure Network Access Policies
Create Network Access Policies to dynamically provision network access for registered endpoints when they connect to the network. Network Access Policies are very helpful when the port VLAN configuration can change depending upon the type of device connecting.

For details on configuration, see Network access policies section of the Administration Guide in the Fortinet Document Library.

Determine the Required Enforcement Groups
There are several enforcement groups available. Review the list below to decide which groups will be required.

Forced Authentication (Port Group): Ports that participate in forced authentication when unauthenticated users connect. If you have a port in this group, when an endpoint connects to this port and is unauthenticated, the port is put into isolation VLAN and the endpoint is forced to authenticate.

Forced Registration (Port Group): Ports that participate in forced registration when unregistered endpoints connect.

Add switch ports that participate in forced registration when an Unregistered Endpoint connects to the Forced Registration port group. Only ports that participate have their VLAN ID set to the Registration VLAN when an Unregistered Endpoint connects.

Forced Remediation (Port Group): Ports that participate in forced remediation VLAN switching when endpoints connect.

Add switch ports that participate in forced remediation when an endpoint is marked At-Risk. Only ports that participate have their VLAN ID set to the Quarantine VLAN when endpoints marked At-Risk connect.

Role-Based Access (Port Group): Ports that participate in role-based access and switch VLANs, based on the role of network endpoints, such as printers, when they connect. Example: A printer is set up with the role “Accounting”. When the printer connects to a port in this group, the printer is switched to the VLAN associated with the “Accounting” role.

Ports must be members of this group in order to use Network Access Policies to dynamically provision network access.
Physical Address Filtering (Device Group): Devices that participate in the enabling and disabling of endpoints.

Add switches that participate in endpoint disabling to this group. If an endpoint is connected to a switch that is not in the Physical Address Filtering group, and that endpoint is disabled through FortiNAC, the endpoint remains connected to the network and is displayed as in violation. Add the switch regardless of whether an endpoint is disabled through a Dead End VLAN, or through MAC address security.

Example Requirements
1.Endpoints must register through the Captive Portal prior to being granted access to the network.
2.Endpoints must be scanned for posture. If scan fails, device must remediate prior to accessing the network.
3.Network access for registered endpoints must be provisioned based on access policies.
4.Provide the ability to disable registered endpoints.

Determine Enforcement Groups
The following would needed based upon the requirements listed above:
Requirement #1: Forced Registration
Requirement #2: Forced Remediation
Requirement #3: Role-Based Access
Requirement #4: Physical Address Filtering

Organize Groups
Once it has been determined which enforcement groups will be required, decide how groups will be organized. Members can be added directly to the enforcement groups or new groups can be nested within the enforcement group(s). Group nesting is advantageous because enforcement can be removed quickly (if necessary) by simply removing the nested group from the enforcement group. Two examples of group nesting are described.

Group organization can be done in several ways and is up to the customer to determine what works best for them. It is recommended to remain consistent with whichever method is decided upon for group organization. See Add Groups in the Online Help or Administration guide for instructions.

Important: Since enabling enforcement can disrupt network communication, do not add members to groups until ready to enable enforcement.
**Group Nesting Examples**

“Master” and location based port groups: Create a “Master” enforcement group and add it to the appropriate system enforcement groups (e.g. Forced Registration, Forced Remediation and Role-Based Access). Adding switch or location based port groups to the Master enforcement group automatically enables enforcement on those ports within the switch groups.

- **Add/Remove enforcement per port:** Add/remove switch port from the switch port group
- **Add/Remove enforcement per switch or location:** Add/remove switch port group from the Master enforcement port group
- **Add/Remove enforcement for all locations:** Add/remove Master enforcement port group from the system enforcement groups

---

Location based port groups: Create location or switch specific port groups and add them directly to the system enforcement groups.

- **Add/Remove enforcement per port:** Add/remove switch port from the switch port group
- **Add/Remove enforcement per switch or location:** Add/remove switch port group from the system enforcement groups
- **Add/Remove enforcement for all locations:** Add/remove all switch port groups from the system enforcement groups

---

![Diagram](image)
**Review Enforcement Checklist**

Before enabling enforcement, verify the following:

- The Current and Default VLANS are correct on each switch. (Current and Default should match, or there will be a VLAN switch when ports are placed under enforcement, unless a network access policy overrides the default)
- All uplinks are marked as uplinks in Topology. See [Uplink Review](#) in the Appendix.
- Isolation VLANS are working.
- Each switch model configuration has the appropriate isolation VLAN for all desired enforcement states.
- Review ports to be placed under enforcement and note any remaining unregistered endpoints (Rogues).

**Important:** Unregistered endpoints detected on enforced ports will be isolated.

---

**Enable Enforcement**

To place switch ports under FortiNAC’s control, add the desired ports or switches to the appropriate group(s) under **System > Groups**.

**Important:** Since enabling enforcement can potentially disrupt network communication, it is recommended to enforce a small, low impact area first to ensure functionality.

Proceed to [Validate Enforcement](#).
Validator Enforcement

Connect an unregistered endpoint to one of the newly enforced ports. If any of the below do not work as expected, refer to the Troubleshooting section of this document.

**Forced Registration**

Verify the following:
- Connected port’s VLAN is configured for the appropriate VLAN for Registration
- Endpoint receives an IP Address from the scope configured for that isolation network
- Endpoint is able to access the Captive Portal

**Role-Based Access**

Register the system and verify the port’s VLAN is changed to the appropriate non-isolation VLAN.

**Forced Remediation**

Scan an endpoint that does not meet the requirements and verify the following:
- Endpoint is marked At-Risk and VLAN is switched to Quarantine
- Endpoint is able to download the appropriate program and rescan
- Once scan passes, endpoint is moved back to the appropriate non-isolation VLAN

**Physical Address Filtering**

1. In **Hosts > Host View**, right click host record and select **Disable Host(s)**.
2. Verify the VLAN is switched to Dead End.
3. Once verified, right click on the host record and select **Enable Host(s)**.
4. Verify the VLAN is switched back to the appropriate non-isolation VLAN.
Troubleshooting

Unable to Connect Using SNMP
Refer to KB article Troubleshooting SNMP Communication Issues.

Inaccurate Port Connection Information

L2 Polling
1. Click the Polling tab and verify L2 (Hosts) Polling completed. The timestamps for Last Successful Poll and Last Attempted Poll should be the same.

2. If Last Successful Poll is not current, click the Credentials tab and click the Validate Credentials button. If credentials fail, refer to the following KB articles:
   Troubleshooting SNMP Communication Issues
   Troubleshooting CLI credential failure

SNMP Traps
Host record does not appear online after connection.

1. Validate FortiNAC’s ability to process the traps. For instructions, refer KB article Confirming Link State Traps via Administrative UI.

2. If Link State trap events are not listed in NAC, verify the FortiSwitch is sending traps via the FortiSwitch CLI.
   diag sniffer packet any “udp and port 162”

   Output should show the FortiSwitch sending traps to FortiNAC IP address:
   9.298683 <FortiSwitch IP address>.162 -> <FortiNAC IP address>.162: udp 184

3. If the FortiSwitch is sending traps, verify if FortiNAC received the traps using tcpdump from the FortiNAC CLI.

   FortiLink Mode:
   tcpdump -nni any port 162 and host <FortiGate IP address>

   Standalone:
   tcpdump -nni any port 162 and host <FortiSwitch management IP address>
Example output from FortiSwitch in FortiLink mode:

- Source IP is the FortiGate (10.12.240.2)
- Switch serial number (108EN4N17001579)
- Switch internal IP address (169.254.2.2)
- Port number (port5)
- Link state (linkup)

Trap(167), .1.3.6.1.4.1.12356.106 169.254.2.2 linkUp 502198510
.1.3.6.1.2.1.2.1.2.1.2.5="port5", .1.3.6.1.2.1.2.1.1.5=5
.1.3.6.1.2.1.2.1.2.1.8.5=1
.1.3.6.1.4.1.12356.106.1.1.0="S108EN4N17001579"
.1.3.6.1.2.1.1.5.0="S108EN4N17001579"

4. If FortiNAC is not receiving the traps, verify the policy configuration in the FortiGate. In the FortiGate UI, navigate to Policy & Objects > IPv4 Policy.

5. If the FortiNAC is receiving the traps, verify the system is processing them using the debug tools in FortiNAC CLI for SNMP activity.

CampusMgrDebug -name SnmpV1 true

Example output

- Source IP is the FortiGate (10.12.240.2)
- Switch serial number (108EN4N17001579)
- Switch internal IP address (169.254.2.2)
- Port number (5)
- Link state (linkup = 0.3)
2:59:45.10,enterprise=1.3.6.1.4.1.12356.106,\texttt{genericTrap=3},specificTrap =0, VBS[1.3.6.1.2.1.2.2.1.2.5 = \texttt{port5}; 1.3.6.1.2.1.2.2.1.1.5 = 5; 1.3.6.1.2.1.2.2.1.7.5 = 1; 1.3.6.1.2.1.2.2.1.8.5 = 1; 1.3.6.1.4.1.12356.106.1.1.1.0 = \texttt{S108EN4N17001579}; 1.3.6.1.2.1.1.5.0 = \texttt{S108EN4N17001579}], messageProcessingModel=0, securityName=fortinet, processed=false, peerAddress=10.12.240.2/673, transportMapping=org.snmp4j.transport.DefaultUdpTransportMapping@54f74762, tmStateReference=null]
yams.SnmpV1 FINER :: 2019-09-30 13:02:16:848 :: receiveTrap() ip = \texttt{169.254.2.2} version = 1 securityName = fortinet

YamsEvent:

- Landscape = -1 FF:FF:FF:FF:FF:FF
- ID = -1
- State = Active
- Name = 0.3
  - element type = Unknown
  - element ID = -1
  - element name = null
- Date = 09/30/2019 13:02:16.848
- Message = null
- Number of Mib Elements = 9

NameValue:

- Name = Trap Def
  - Value = 0.3

NameValue:

- Name = Community
  - Value = fortinet

NameValue:

- Name = 1.3.6.1.2.1.2.2.1.2.5
  - Value = [B@20b9e3a8

NameValue:

- Name = 1.3.6.1.2.1.2.2.1.1.5
  - Value = 5

NameValue:

- Name = 1.3.6.1.2.1.2.2.1.7.5
  - Value = 1

NameValue:

- Name = 1.3.6.1.2.1.2.2.1.8.5
  - Value = 1

NameValue:

- Name = 1.3.6.1.4.1.12356.106.1.1.1.0
  - Value = [B@6432f7ac

NameValue:
Name = 1.3.6.1.2.1.1.5.0
Value = [B@1052303f
NameValue:
Name = AgentID
Value = 169.254.2.2

yams.SnmpV1 FINER :: 2019-09-30 13:02:16:848 :: receiveTrap() name = 0.3 ip = 169.254.2.2 dbid = 519 possibleEventTypes = 0.3

6. Once the trap is processed, FortiNAC executes L2 poll in order to read the address table and update the database.

yams.BridgeManager INFO :: 2019-09-30 13:02:27:689 ::
********** sup-fgt-hw 10.12.240.2 PollThread-poll10 172 **********
readForwardingDatabase 0.833 Seconds
old client count = 0
lost client count = 0
new client count = 0
Done update Clients 0.836 Seconds
Link Up interface count = 1
-3235441
Add Back to Queue = true
Link Up Retry Count = 1
Queue Size = 1
******************************************************************************

7. If SNMP packets are processing and L2 poll initiates but fails, refer to L2 Polling.

**VLAN Not Switching Correctly**

Refer to KB article Troubleshooting VLANs Not Changing on a Wired Switch.
Syslog Messages

Host record does not appear online after connection.

1. Validate FortiNAC’s ability to process the syslog messages. For instructions, refer KB article Confirming MAC Notification traps via Administration UI.

2. If events are not listed in NAC, verify if FortiNAC received the traps using tcpdump from the FortiNAC CLI.

tcpdump -nni any host <FortiGate IP address> and port 514 -vvv | grep Switch-Controller -B3

The logid’s in the filter represent the ID of the add, delete, move FGT syslog messages.

Example:
> tcpdump -nni any host 10.12.240.2 and port 514 -vvv | grep Switch-Controller -B3

tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
16:43:43.146088 IP (tos 0x0, ttl 64, id 12635, offset 0, flags [none], proto UDP (17), length 400)
    Facility local7 (23), Severity info (6)
    Msg: date=2019-05-14 time=16:43:42 devname="FG81EPTK18005296"
      devid="FG81EPTK18005296" logid="0100032617" type="event" subtype="system"
      level="information" vd="root" eventtime=1557866623120174894 logdesc="FortiSwitch MAC move" user="Switch-Controller" ui="cu_acd" msg="00:21:70:d1:92:77 moved from interface port5 to interface port6 in vlan 100 on Switch S108EN4N17001579"

16:44:43.745439 IP (tos 0x0, ttl 64, id 12794, offset 0, flags [none], proto UDP (17), length 382)
    Facility local7 (23), Severity info (6)
    Msg: date=2019-05-14 time=16:44:43 devname="FG81EPTK18005296"
      devid="FG81EPTK18005296" logid="0100032615" type="event" subtype="system"
      level="information" vd="root" eventtime=1557866683718722489 logdesc="FortiSwitch MAC add" user="Switch-Controller" ui="cu_acd" msg="00:8c:fa:44:15:46 discovered on interface port2 in vlan 99 on Switch S108EN4N17001579"

16:44:43.745485 IP (tos 0x0, ttl 64, id 12795, offset 0, flags [none], proto UDP (17), length 366)
    Facility local7 (23), Severity info (6)
    Msg: date=2019-05-14 time=16:44:43 devname="FG81EPTK18005296"
      devid="FG81EPTK18005296" logid="0100032616" type="event" subtype="system"
      level="information" vd="root" eventtime=1557866683718877671 logdesc="FortiSwitch MAC delete" user="Switch-Controller" ui="cu_acd" msg="00:8c:fa:44:15:46 deleted from vlan 100 on Switch S108EN4N17001579"
Debugging

FortiGate Commands

Enable debugging feature
diagnose debug enable

802.1X
diagnose debug app eap_proxy 31 (EAP deamon)

RADIUS Disconnect
diag debug app radius-das 8

Disable debugging feature
diagnose debug disable

Security Fabric Communication
diagnose debug authd fsso list

RADIUS sessions (Link Mode)
diagnose switch-controller switch-info 802.1X

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

<table>
<thead>
<tr>
<th>MAC</th>
<th>Type</th>
<th>Vlan</th>
<th>Dynamic-Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0c:29:d4:4f:3c</td>
<td>802.1x</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

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**

Send a RADIUS Disconnect:
SendCoA -ip <devip> -mac <clientmac> -dis

RADIUS activity:
CampusMgrDebug -name RadiusManager true

Example response (Note: will always return policy value “NativePolicy”)
Client MAC address = D0-67-E5-36-6F-D4
FortiGate IP = 10.12.240.2

yams.RadiusManager INFO :: 2019-04-03 08:29:12:998 ::
RadiusPollThread0 RadiusServer accepting client D0-67-E5-36-6F-D4 for

L2 related activity:
CampusMgrDebug -name BridgeManager true

Standalone FortiSwitch specific:
CampusMgrDebug -name FortiSwitch true

Managed (FortiLink) FortiSwitch and FortiGate wired port specific:
CampusMgrDebug -name Fortinet true

SNMP activity:
CampusMgrDebug -name SnmpV1 true
Enable debugging feature:
CampusMgrDebug -name <value> false

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

FortiSwitch FortiLink Mode CLI Access
The FortiSwitch CLI is accessed via SSH session from the managing FortiGate.

From FortiGate UI:
1. In the left pane, navigate to Wifi and Switch Controller > Managed FortiSwitch
2. In the right pane, right-click on the desired switch and select Connect to CLI

From FortiGate CLI:
exec ssh admin@169.254.1.2

FortiGate CLI Access
The FortiGate UI can be used to initiate SSH sessions: click on the “>_” icon in the upper right corner of the page.

FortiSwitch Standalone Mode CLI Access
The FortiSwitch UI can be used to initiate SSH sessions: click on the icon in the upper right corner of the page.
Modify API Port

**Note:** The below change is required for FortiNAC versions 8.3.5 and below. As of 8.3.6, FortiNAC dynamically learns the API port in use.

FortiNAC uses port 443 by default for REST API. To change the port FortiNAC uses for when communicating with the FortiGate, set the port to use through CLI:

```
Device -setAttr -ip <FortiGate IP> -name API_Port -value <Port value>
```

**Example:**
```
Device -setAttr -ip x.x.x.x -name API_Port -value 2222
```

```
************************* FWF60ETK18001734 *************************
Landscape = 207375981338 00:30:48:92:5B:1A
Pollable = true, Poll interval = 10 Minutes
Type = 1.3.6.1.4.1.12356.101.1.639
Group = 1.3.6.1.4.1.12356
MAC = null
Protocol = SnmpV1
Description =
IP = xxxx
State = Active
Status = Established
DBID = 8913
Attribute Count = 14
    Name = SnmpVersion value = 1 length = 1
    Name = CLI_CREDENTIALS value = CLICredentials
        User Name:[admin]
        Password:[***]
        Enable Password:[***]
        SessionType:[SSH2]
    Name = FirmwareVersion value = Fortigate36000 length = 14
    Name = SupportsVirtualization value = true length = 4
    Name = L2_ENABLED value = true length = 4
    Name = L2_POLL_DURATION value = 600 length = 3
    Name = L2_MIN_POLL_DURATION value = 300 length = 3
    Name = API_Port value = 2222 length = 3
    Name = 1.3.6.1.2.1.1.3.0 value = 58 days, 20:54:56.43 length = 20
    Name = userDefinedOID value = false length = 5
    Name = RestAPIVersion value = 0 length = 1
    Name = L2_LAST_POLL value = Mon Apr 01 08:23:24 EDT 2019 length = 28
    Name = L2_LAST_SUCCESSFUL_POLL value = Mon Apr 01 08:23:24 EDT 2019 length = 28
    Name = DEBUG value = ForwardingInterface length = 19
Community Strings: *****
```
Uplink Review

All devices connected to an uplink port are ignored. Therefore, it is important to verify the validity of any uplinks defined by FortiNAC based upon the number of MAC addresses learned off the port (Threshold uplink). For more information, see Port uplink types in the Administration Guide in the Fortinet Documentation Library.

Review the ports FortiNAC has listed as Threshold uplinks. If the port is legitimately an uplink, manually configure the port.

1. Filter on the Connection Status Threshold Uplink in Topology port view of the FortiSwitch (Standalone) or FortiGate (FortiLink Mode).

2. Manually set ports that should be uplinks to “Always Uplink.” This is a way to keep track of which uplinks have been verified.

Switches with a mix of servers and access ports: mark server ports as “Always Uplink” if ports are physically secure and there is no interest in visibility of those servers.

   a. Right click on the port and select Port Properties or multi-select ports and select Modify Port Properties.
   b. Click Always Uplink.

If any ports display “Threshold Uplink” as a Connection State in the future, it will indicate a new connection and should be verified.