FortiNAC - Network Device Modeling

Version 7.2 F

July 17, 2023
FortiNAC 7.2 F Network Device Modeling
00-400-000000-20181031

TABLE OF CONTENTS

Overview

This document provides the steps necessary for establishing network visibility by modeling the network infrastructure in the FortiNAC Administration UI. It is intended to be used in conjunction with the Deployment Guide in the Fortinet Document Library.

What it Does

The network infrastructure is "discovered" and added to FortiNAC's database. Network devices are identified as either L2 (e.g. switches) or L3 (e.g. routers). Once added, FortiNAC can gather connectivity information from these network devices to provide real-time inventory of what's connected to the network and where.

How it Works

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

- RADIUS communication
- L2 Polling (reads the device's MAC address table)
- L3 Polling (reads the device's ARP cache)

Requirements

FortiNAC

- FortiNAC-OS appliances (FNC-CAX-xx): allowaccess snmp option must be configured in CLI. See FortiNAC-OS CLI reference manual for details.
- Enable SSH Keyboard-interactive (KBD) for device models requiring KBD for CLI access. Examples include (but may not be limited to) Arista switches. For details see KB 244979.

Network Devices

Must be configured with the following:

- SNMP credentials
  - Devices FortiNAC will control: Read/write privileges*
  - L3 devices from which FortiNAC will obtain ARP information but not control: Read privileges
  - Related KB articles:

    Configure and validate Cisco SNMPv3
- CLI or REST API credentials

- Devices FortiNAC will control: Read/write privileges (Cisco must be level 15 local user account)*
- L3 devices from which FortiNAC will obtain ARP information but not control: Read access (level 7)

Able to respond to PING requests from FortiNAC eth0 IP address.* For device modeling, only read privileges are required.

Avoid certain characters. When configuring the device itself, use only letters, numbers and hyphens (-) in names for items within the device configuration, in SNMP and CLI credentials. Other characters may prevent FortiNAC from reading the device configuration. For example, in many cases the # sign is interpreted by FortiNAC as a prompt. Cisco restricts the use of @ and #.

For more details regarding requirements, see the **Requirements Task List** in the Deployment Guide.

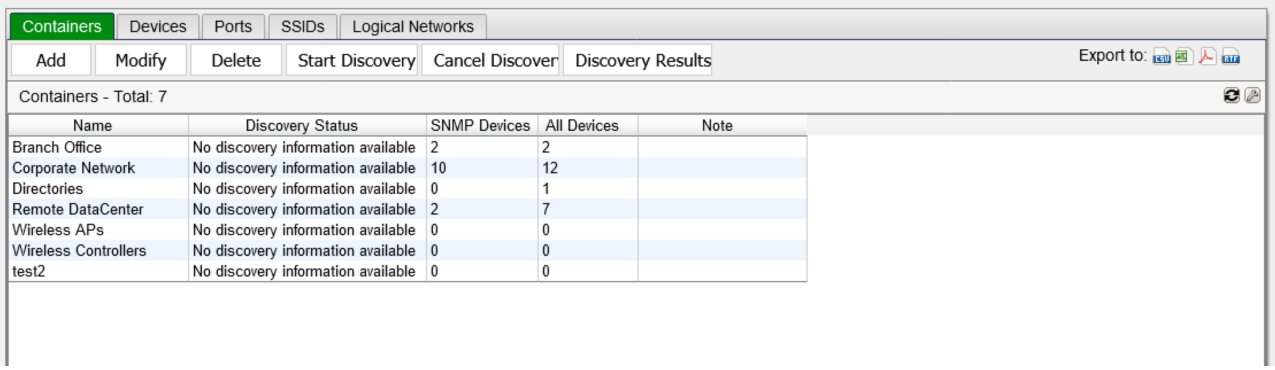
Procedure Overview

1. **Create Containers: Create logical grouping of network devices.**
2. **Add Infrastructure Devices: Add the network infrastructure devices to Inventory.**
3. **Configure Layer 3 Sources: Configure FortiNAC to collect endpoint IP address information regarding connected endpoints on the network.**
4. **Validate: Review the values populated for the ports (Label, Connection State, VLAN, etc) and verify they are accurate.**
5. **Review Uplinks: Review ports FortiNAC has identified as Threshold Uplinks.**
6. **Modify System Defined Uplink Count: Set the threshold value FortiNAC uses to convert a port to a Threshold Uplink.**
7. **Configure Additional Maintenance Tasks (for Wireless Devices Only)**

Step 1: Create Containers

Create Containers for logical grouping of network devices.

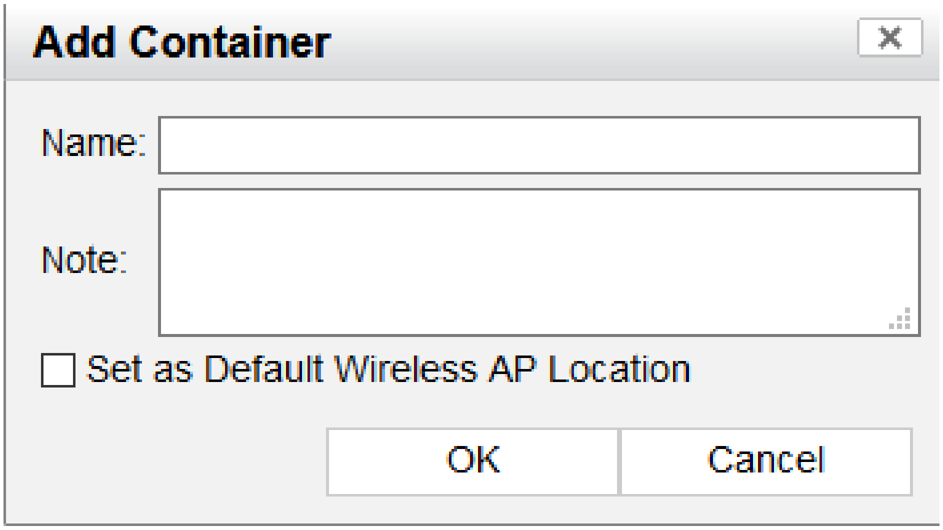
1. Navigate to **Network > Inventory.**



Containers - Total: 7

Name	Discovery Status	SNMP Devices	All Devices	Note
Branch Office	No discovery information available	2	2	
Corporate Network	No discovery information available	10	12	
Directories	No discovery information available	0	1	
Remote DataCenter	No discovery information available	2	7	
Wireless APs	No discovery information available	0	0	
Wireless Controllers	No discovery information available	0	0	
test2	No discovery information available	0	0	

2. Under the **Containers** tab, click **Add**.


Add Container

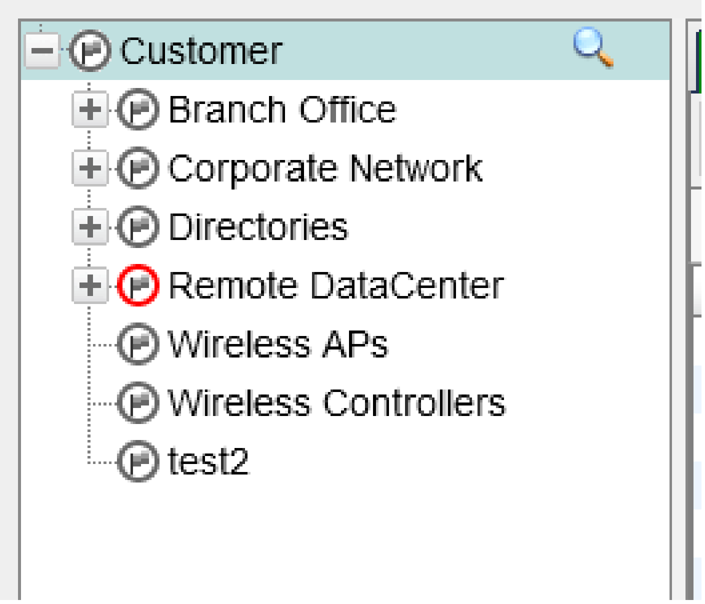
Name:

Note:

☐ Set as Default Wireless AP Location

3. Specify container name and any desired notes. Example: Houston, Bldg 8, Fl 2
4. Click **OK**.
5. Containers appear in the left panel. Once devices are added, they will appear in the tree under the appropriate

container



- Customer
  - Branch Office
  - Corporate Network
  - Directories
  - Remote DataCenter
  - Wireless APs
  - Wireless Controllers
  - test2

Note: At this time, containers cannot be nested.

For more information on this view, see section Inventory in the Administration Guide.

Step 2: Add Infrastructure Devices

Add the network infrastructure devices to Inventory. This includes:

- Switches
- Routers
- Wireless controllers
- Autonomous Access Points

Important: When adding wireless infrastructure, do not add AP's managed by controllers. They will be automatically discovered later on.

Vendor Specific

See **Appendix** for the following:

Replacing Classic Aerohive with AerohiveNG

Aruba/Alcatel Controller (Redundancy Configurations)

Aruba IAP

Cisco Meraki MS Switch

Cisco Meraki MX Router

Mist Access Points

General Instructions (All Other Vendors)

Add devices to Inventory individually or in bulk, providing SNMP and CLI/API credentials.

Click on the link below for instructions.

Add or modify a device - Instructions to add an individual device

Discovery - Instructions to add devices in bulk by defining a range of IP addresses.

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

Troubleshooting

Troubleshooting SNMP Communication Issues

Unable to model device in GUI ("?" appears as the icon)

Duplicate switch names and duplicate port names when adding a switch

Dell switches using directory for CLI access fail credential validation

Step 3: Configure Layer 3 Sources

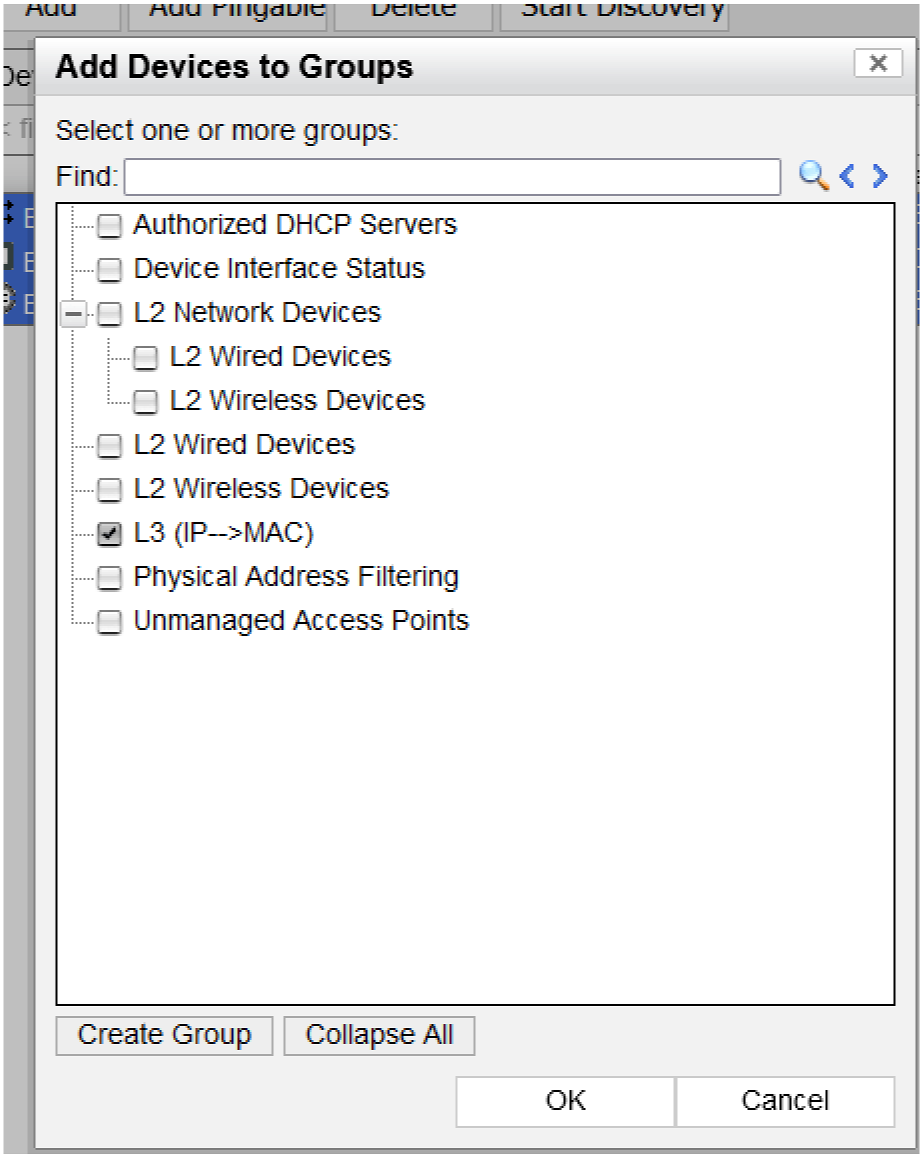
Configure FortiNAC to collect IP address information for connected endpoints on the network. For more details, L3 polling in the Administration Guide.

Add Devices to L3 (IP-> MAC) Group

This group should contain all devices that are a source of ARP information. This includes routers, L3 switches, wireless controllers and autonomous AP’s.

1. Navigate to **Network > Inventory**.
2. Click the desired container.
3. Click the **Devices** tab.
4. To add members to the group, multi-select the L3 devices listed in the **Devices** panel.
5. Right-click and select **Add Devices to Groups**.

6. Select **L3 (IPàMAC)** and click **OK**.



Select one or more groups:

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

L3 polling is automatically enabled for those devices with the following settings:

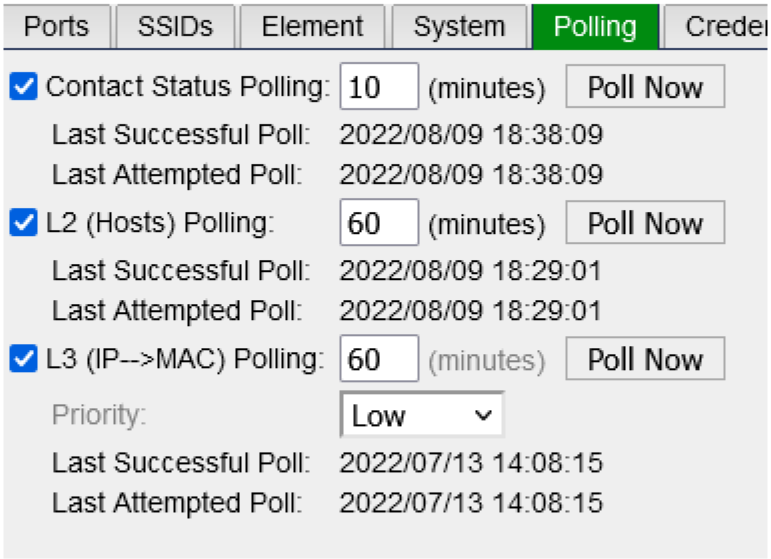
- L3 Polling = Enabled, 30 min
- L3 Priority = Low

Configure L3 Polling Settings

Devices are polled in batches based on priority to retrieve host IP addresses. It is recommended that high traffic routers and switches be given a higher priority.

Individual Device

1. In **Inventory**, select the device and click the **Polling** tab.
2. Set the desired interval (minutes) and Priority (Low, Medium or High).
3. Click **Save**.



☑ Contact Status Polling: 10 (minutes)

Last Successful Poll: 2022/08/09 18:38:09

Last Attempted Poll: 2022/08/09 18:38:09

☑ L2 (Hosts) Polling: 60 (minutes)

Last Successful Poll: 2022/08/09 18:29:01

Last Attempted Poll: 2022/08/09 18:29:01

☑ L3 (IP-->MAC) Polling: 60 (minutes)

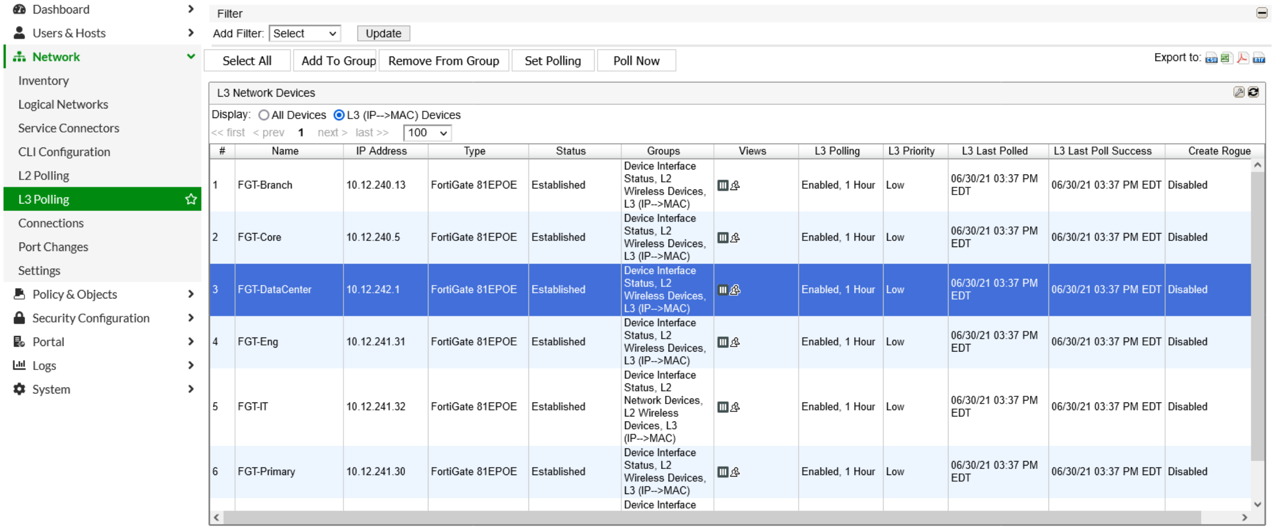
Priority: Low

Last Successful Poll: 2022/07/13 14:08:15

Last Attempted Poll: 2022/07/13 14:08:15

Multiple Devices

1. Navigate to **Network > L3 Polling**.
2. Select one or more devices from the list. To select all devices, click **Select All**.
3. Click **Set Polling**.
4. Select the **Enable Polling** check box to enable polling for the selected device.
5. Select a time interval to control how often polling should occur. The interval can be set in Hours or Minutes.
6. Click **OK**.



Display: ○ All Devices ● L3 (IP-->MAC) Devices

#	Name	IP Address	Type	Status	Groups	Views	L3 Polling	L3 Priority	L3 Last Polled	L3 Last Poll Success	Create Rogue
1	FGT-Branch	10.12.240.13	FortiGate 81EPOE	Established	Device Interface Status, L2 Wireless Devices, L3 (IP-->MAC)		Enabled, 1 Hour	Low	06/30/21 03:37 PM EDT	06/30/21 03:37 PM EDT	Disabled
2	FGT-Core	10.12.240.5	FortiGate 81EPOE	Established	Device Interface Status, L2 Wireless Devices, L3 (IP-->MAC)		Enabled, 1 Hour	Low	06/30/21 03:37 PM EDT	06/30/21 03:37 PM EDT	Disabled
3	FGT-DataCenter	10.12.242.1	FortiGate 81EPOE	Established	Device Interface Status, L2 Wireless Devices, L3 (IP-->MAC)		Enabled, 1 Hour	Low	06/30/21 03:37 PM EDT	06/30/21 03:37 PM EDT	Disabled
4	FGT-Eng	10.12.241.31	FortiGate 81EPOE	Established	Device Interface Status, L2 Wireless Devices, L3 (IP-->MAC)		Enabled, 1 Hour	Low	06/30/21 03:37 PM EDT	06/30/21 03:37 PM EDT	Disabled
5	FGT-IT	10.12.241.32	FortiGate 81EPOE	Established	Device Interface Status, L2 Network Devices, L2 Wireless Devices, L3 (IP-->MAC)		Enabled, 1 Hour	Low	06/30/21 03:37 PM EDT	06/30/21 03:37 PM EDT	Disabled
6	FGT-Primary	10.12.241.30	FortiGate 81EPOE	Established	Device Interface Status, L2 Wireless Devices, L3 (IP-->MAC)		Enabled, 1 Hour	Low	06/30/21 03:37 PM EDT	06/30/21 03:37 PM EDT	Disabled
					Device Interface						

For more information on the options in this view, see L3 Polling in the Administration Guide.

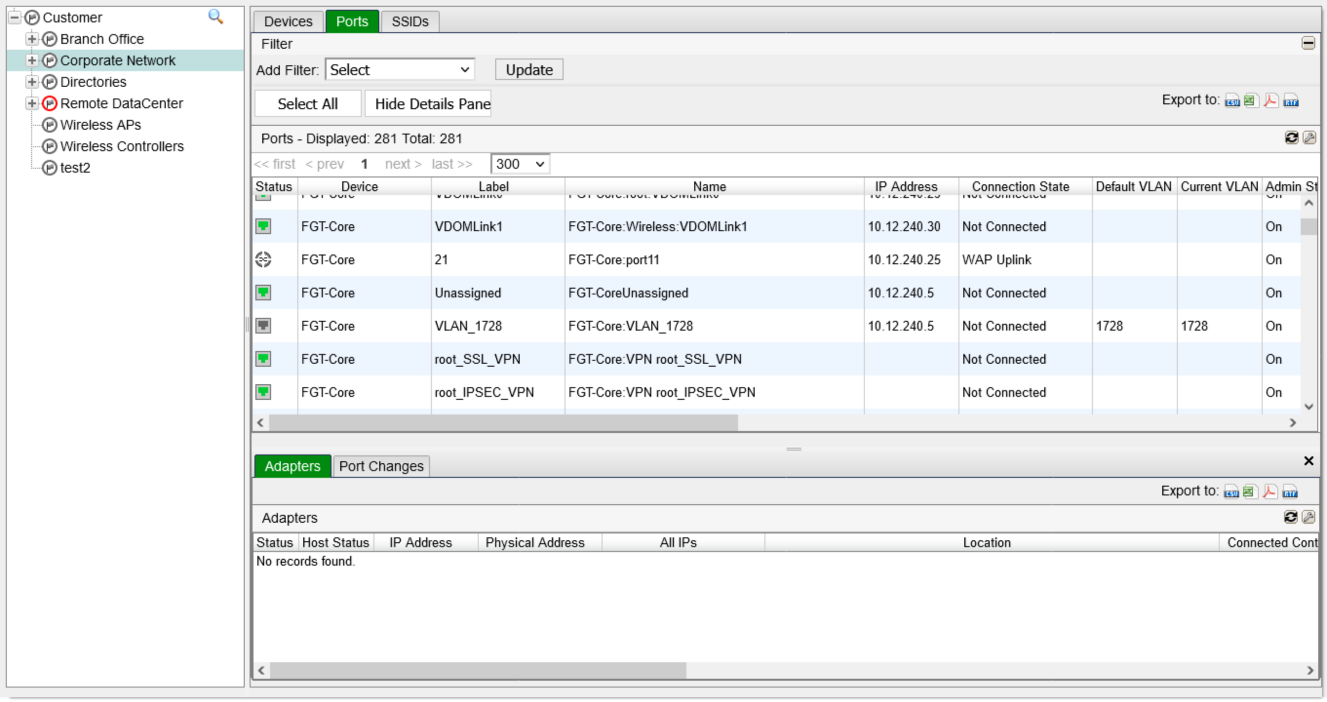
Step 4: Validate

Review Port Level Information

Review the values populated for the ports (Label, Connection State, VLAN, etc) and verify they are accurate.

Note: Current VLAN values may not be accurate for switches authenticating using RADIUS (such as Meraki). 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.

1. Navigate to **Network > Inventory.**
2. Select the container in the left panel and click the **Ports Tab**.
3. Click **Update** to display the ports.
4. If the **Adapter** tab is not already visible, click the **Show Details Panel** button.
5. Verify connection information for connected hosts 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.



- Customer
  - Branch Office
  - Corporate Network
  - Directories
  - Remote DataCenter
  - Wireless APs
  - Wireless Controllers
  - test2

Devices | Ports | SSIDs

Filter

Add Filter: Select | Update

Select All | Hide Details Pane | Export to:

Ports - Displayed: 281 Total: 281

<< first < prev 1 next > last >> 300

Status	Device	Label	Name	IP Address	Connection State	Default VLAN	Current VLAN	Admin St
🟩	FGT-Core	VDOMLink1	FGT-Core:Wireless:VDOMLink1	10.12.240.30	Not Connected			On
⊕	FGT-Core	21	FGT-Core:port11	10.12.240.25	WAP Uplink			On
🟩	FGT-Core	Unassigned	FGT-CoreUnassigned	10.12.240.5	Not Connected			On
■	FGT-Core	VLAN_1728	FGT-Core:VLAN_1728	10.12.240.5	Not Connected	1728	1728	On
🟩	FGT-Core	root_SSL_VPN	FGT-Core:VPN root_SSL_VPN		Not Connected			On
🟩	FGT-Core	root_IPSEC_VPN	FGT-Core:VPN root_IPSEC_VPN		Not Connected			On

Adapters | Port Changes

Export to:

Adapters

Status	Host Status	IP Address	Physical Address	All IPs	Location	Connected Cont

No records found.

Replacing a Modeled Device

When adding a switch or router that will use the same IP address as the original device, the original model in Topology must be deleted from the database and a new model added. This ensures all internal mappings and files associated to that model are correct for the new device. Otherwise, unexpected behavior can occur such as…

- Unable to read VLANS
- L2/L3 Poll failures
- Credential validation failure
- Switching VLANs on the wrong ports

Note: Deleting the model from FortiNAC removes all manual switch device and port groupings done on the switch model.

For instructions, see section Replace a device using the same IP address of the Administration Guide.

Troubleshooting

Step 5: Review Uplinks

When devices are discovered in Inventory, switch ports are given a specific connection status depending upon the connected device(s). An uplink connection status indicates the port should not be controlled by FortiNAC. A common example is a switch port connecting to another switch. These ports will not be manipulated in any way, nor will they display endpoint connection information.

There are different types of uplinks. Each uplink type is triggered by different criteria. For a complete list of uplink types and how they are detected, see section Port uplink types of the Administration Guide.

The System Defined Uplink Count is the threshold value FortiNAC uses to convert a port to a Threshold Uplink. Identify ports in the network where FortiNAC has determined that the number of MAC addresses on the port exceeds the System Defined Uplink Count (default value = 20). Review these ports and verify whether or not these are legitimate uplinks.

Navigate to **Network > Inventory.**

1. Filter on the Connection Status “Threshold Uplinks” under the **Ports** tab. This can be done at the top level or container level.
2. Click **Update** to apply filter.
3. Review the resulting port list and note the ports where uplinks are not expected. Multi-select the unknown ports, right-click and select **Modify Properties**.
4. Click **Note**.
5. Enter “Threshold” and click **OK**.

Switches with a mix of servers and access ports: Mark server ports as user defined uplinks *if* ports are physically secure and there is no interest in visibility of those servers.

For instructions see section Port properties of the Administration Guide.

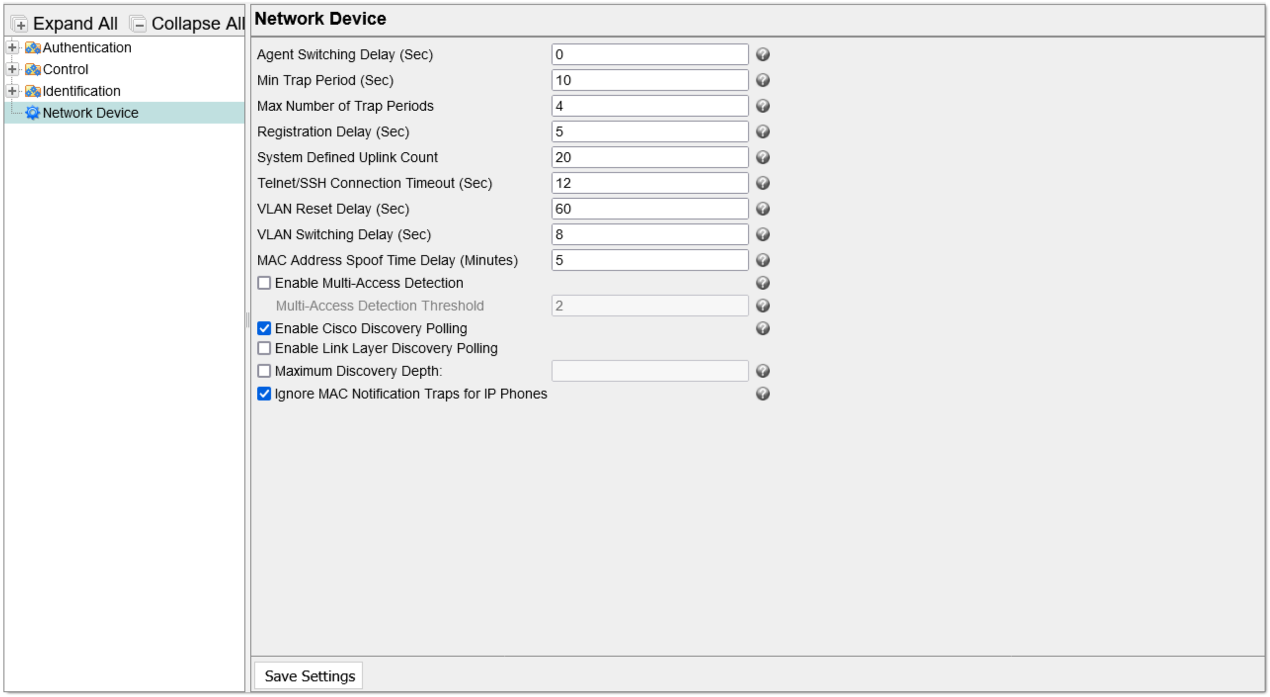
Related KB Articles

Cisco WLC Port Channel not classified as Learned Uplink

Step 6: Modify System Defined Uplink Count

Once the infrastructure has been discovered, change the System Defined Uplink Count from its default of 20 to 2000. This helps avoid ports changing to uplinks due to connecting computers generating an unusually high number of MAC addresses.

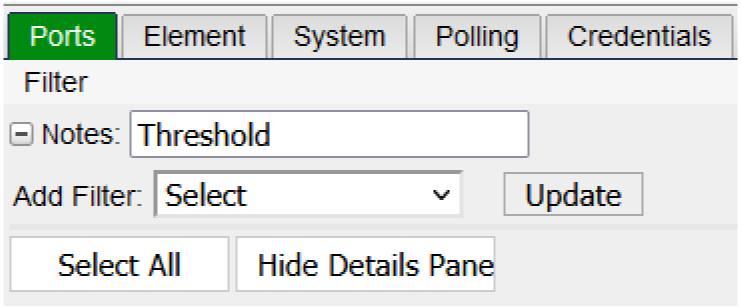
1. Log into the Administration UI.
2. Navigate to **Network > Settings > Network Device.**
3. Change **System Defined Uplink Count** to 2000.
4. Click **Save Settings** at the bottom of the view.



Network Device

Agent Switching Delay (Sec)	0
Min Trap Period (Sec)	10
Max Number of Trap Periods	4
Registration Delay (Sec)	5
System Defined Uplink Count	20
Telnet/SSH Connection Timeout (Sec)	12
VLAN Reset Delay (Sec)	60
VLAN Switching Delay (Sec)	8
MAC Address Spoof Time Delay (Minutes)	5
☐ Enable Multi-Access Detection	
Multi-Access Detection Threshold	2
☑ Enable Cisco Discovery Polling	
☐ Enable Link Layer Discovery Polling	
☐ Maximum Discovery Depth:	
☑ Ignore MAC Notification Traps for IP Phones	

5. Clear ports of the “Threshold Uplink” Connection Status.
   a. Navigate to **Network > Inventory.**
   b. Filter on **Notes: Threshold** under the **Ports** tab. This can be done at the top level or container level.



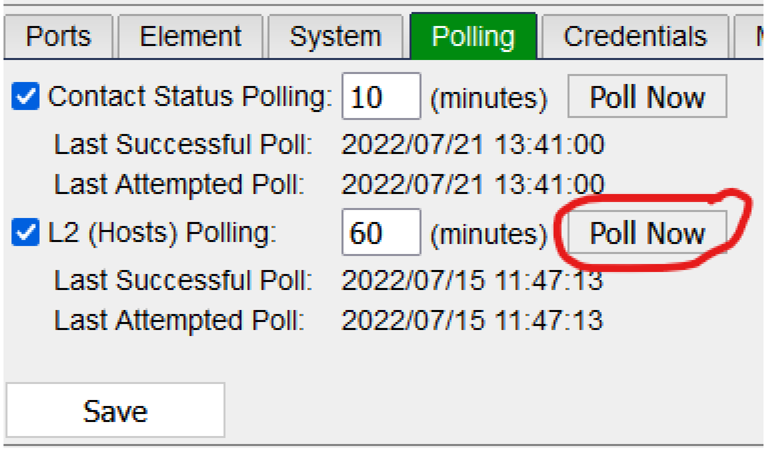
Notes: Threshold

Add Filter: Select

   c. Click **Update** to apply filter.
   d. Multi-select the ports, right-click and select **Modify Properties**.

   e. Click **Uplink Mode**.
   f. Click **Clear** then **OK**.

6. Under **Polling** tab of the applicable switch, click **Poll Now** to re-evaluate the ports.



☑ Contact Status Polling: 10 (minutes)
Last Successful Poll: 2022/07/21 13:41:00
Last Attempted Poll: 2022/07/21 13:41:00

☑ L2 (Hosts) Polling: 60 (minutes)
Last Successful Poll: 2022/07/15 11:47:13
Last Attempted Poll: 2022/07/15 11:47:13

7. Once L2 poll has completed, click **Update** under the **Ports** tab. The Connection State will update depending upon the connected device.
8. Delete the Notes filter and change filter to **Connection Status: Threshold Uplink**.
9. Click **OK**.
10. Ports detected with devices other than the discovered infrastructure or Wireless Access Points will remain. The administrator can now investigate why these ports are being detected with a number of MAC addresses exceeding the System Defined Uplink Count (now set to 2000).
11. Manually set ports that should be an uplink to “Always Uplink.” This is a way to keep track of which uplinks have been verified. If any ports display “Threshold Uplink” as a Connection State in the future, it will indicate a new connection and should be verified.

Step 7: Configure Additional Maintenance Tasks (for Wireless Devices Only)

Prevent SSID Removal After Failed Read of Wireless Device

If FortiNAC fails to read the SSIDs of an AP or controller, the existing SSIDs already associated with the device model are deleted (consequently removing SSID configuration and group membership).

To prevent this from occurring, run the following command in the CLI (**Note**: This attribute is not set by default). Contact Support for assistance.

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

Update FortiNAC After Controller or AP Changes

For proper functionality, FortiNAC should be updated when any of the following components are changed or added to the controller:

- APs
- SSIDs
- VLANs
- AP's IP Address

If this is not done, FortiNAC will not be able to be configured to use these components in the Device Model.

Manual Update

1. Navigate to **Network > Inventory**.
2. Expand the **Container** that stores the device.
3. Select the device and right-click.
4. Click **Resync Interfaces**. This resynchronizes the FortiNAC software and the device configuration.

Automated Update

The Scheduler task **Resynchronize Device**, which is associated to a group of controllers, will do the same thing as Resync Interfaces. It is suggested this Scheduler task be created and run daily.

1. Navigate to **System > Scheduler**.
2. From the Scheduler view, click **Add**.
3. The **Enabled** check box is selected by default. Uncheck it if you want this task to be disabled.
4. Enter a Name for the task and an optional description.
5. In the **Action Type** field, select **System**.

6. From the list of system actions, select **Resynchronize Device**.
7. From the **Group** dropdown list, select the group on which the action will be performed. The list contains only the group types specific to that Action. The WLCs are automatically part of the **L2 Wireless Devices** group. If desired, a new device group could be created.
8. From the **Schedule Type** drop down list, select either Fixed Day or Repetitive and set the day and time that the task is to be performed. It is suggested to run the task daily.

For more information, see section Scheduler of the **Administration Guide** in the Fortinet Document Library.

Appendix

Replacing Classic Aerohive APs with AerohiveNG

This procedure is necessary due to differences in how interface mapping is done between the classic and NG models. If the NGs will be using the same IP addresses as the classic APs, do the following:

1. Delete the existing classic AP models in **Network > Inventory**.
2. Proceed to add the NGs to Inventory. Click on the link below for instructions.

   Add or modify a device - Instructions to add an individual device

   Discovery - Instructions to add devices in bulk by defining a range of IP addresses.

Return to Add Infrastructure Devices.

Aruba/Alcatel Controller Redundancy Configurations

Active/Active

1. Model both controllers since both are active in authenticating users and managing wireless sessions. Click on the link below for instructions.

   Add or modify a device - Instructions to add an individual device

   Discovery - Instructions to add devices in bulk by defining a range of IP addresses.
2. Enable the PreserveSSIDs attribute. If FortiNAC fails to read the SSIDs of an AP or controller, the existing SSIDs already associated with the device model are deleted (consequently removing SSID configuration and group membership). To prevent this from occurring, login to the FortiNAC CLI as root and run the following command:

   ```
   device -ip <Aruba ip address> -setAttr -name PreserveSSIDs -value true
   ```

   Note: This attribute is not set by default. Contact Support for assistance.

Return to Add Infrastructure Devices.

Active/Active – Mobility Master and VIPs per Controller

Each controller is active and has both a virtual and physical IP address. Should one of the controllers fail, one of the other controllers take ownership of the virtual IP, along with all the wireless sessions being managed.

RADIUS authentication requests are sourced from the physical interface IP address. Virtual IP is used for session and other device queries.

FortiNAC accepts the request from the controller’s individual IP address. The NAS-IP RADIUS attribute in the packet is used to look up the actual controller model for FortiNAC configuration values.

FortiNAC needs to recognize the source IP address of the RADIUS request in order to trust it, therefore, a pingable model must exist for each controller's physical IP address.

Controller Configuration Requirement

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

Model Controllers in FortiNAC

1. Model the **virtual IP**. Click on the link below for instructions.

   Add or modify a device - Instructions to add an individual device

   Discovery - Instructions to add devices in bulk by defining a range of IP addresses.
2. Create a pingable model for each of the controllers using the physical IP address. See Add or modify a pingable device for instructions. Configure the following:
   - Name
   - Physical IP address of the controller
   - Physical Address of the controller
   - Set Device Type to **Wireless Access Point.**
3. (Optional) create a pingable model for the Mobility Master to provide device contact status information only. **Important**: Do not model the Mobility Master, as duplicate information and unnecessary extra logging within FortiNAC can result. See Add or modify a pingable device for instructions.
4. Enable the PreserveSSIDs attribute. If FortiNAC fails to read the SSIDs of an AP or controller, the existing SSIDs already associated with the device model are deleted (consequently removing SSID configuration and group membership). To prevent this from occurring, login to the FortiNAC CLI as root and run the following command:

   ```
   device -ip <Aruba ip address> -setAttr -name PreserveSSIDs -value true
   ```

   Note: This attribute is not set by default. Contact Support for assistance.

Return to Add Infrastructure Devices.

Active/Passive

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

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

RADIUS authentication requests are sourced from the physical interface IP address. Virtual IP is used for session and other device queries.

FortiNAC accepts the request from the controller’s individual IP address. The NAS-IP RADIUS attribute in the packet is used to look up the actual controller model for FortiNAC configuration values.

FortiNAC needs to recognize the source IP address of the RADIUS request in order to trust it, therefore, a pingable model must exist for each controller's physical IP address.

Controller Configuration Requirement

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

Model Controllers in FortiNAC

1. Model the **virtual IP**. See Add or modify a device for instructions. Since only one controller is active at once, FortiNAC only needs to know about the virtual IP.
2. Create a pingable model for each of the controllers using the physical IP address. See Add or modify a pingable device for instructions. Configure the following:
   - Name
   - Physical IP address of the controller
   - Physical Address of the controller
   - Set Device Type to **Wireless Access Point.**
3. Enable the PreserveSSIDs attribute. If FortiNAC fails to read the SSIDs of an AP or controller, the existing SSIDs already associated with the device model are deleted (consequently removing SSID configuration and group membership). To prevent this from occurring, login to the FortiNAC CLI as root and run the following command:

   ```
   device -ip <Aruba ip address> -setAttr -name PreserveSSIDs -value true
   ```

   Note: This attribute is not set by default. Contact Support for assistance.

Return to Add Infrastructure Devices.

Aruba IAP

1. Add the master AP to Inventory using the Virtual IP address (VIP). See Add or modify a device for instructions.
2. Add all AP's (including the master physical IP) as pingable devices. This can be done individually or in bulk.

Individual

1. In the Inventory Tree, right click on the applicable container and select **Add Pingable Device**.
2. Populate the following information then click **OK**:
   - Name
   - IP Address (for the master, use the actual IP and not the VIP)
   - Physical Address
   - Select Device Type **Wireless Access Point**

In Bulk

This is done by creating a .csv file containing information about the APs and importing the information using the CLI device import tool.

1. Create the CSV file with a text editor, or by exporting the device information from an application that can generate the CSV file format. The file should be formatted as follows:

   <Container name>,<IP address of AP>,<Name of AP>,<MAC address of AP>,,,,

   Note:

   - There must be a Unix style carriage return at the end of each line in the file, including the final line in the CSV file. Any lines without carriage returns at the end will not be imported.
   - If a field is null, the field delimiter (comma) must still be included.

- The container specified will be the container in Inventory where the AP models will be placed. This can be in a separate container if desired. If the container is not yet created, it will be created upon import.

Example:

```
East Campus,192.168.10.82,IAP_1,04:03:04:05:03:02,,,,
East Campus,192.168.10.83,IAP_2,04:03:04:05:03:03,,,,
East Campus,192.168.10.84,IAP_4,04:03:04:05:03:04,,,,
```

2. Use a secure copy tool to copy the CSV file from your local PC to the FortiNAC appliance (e.g., use Winscp).
3. Back up the current FortiNAC database before proceeding. See section Backup or restore a database of the Administration Guide in the Fortinet Documentation Library for instructions.
4. From the FortiNAC appliance CLI, navigate to the following directory:

   cd /bsc/campusMgr/bin
5. Run the DeviceImport tool to import the AP data and create the APs as WAP devices:

   DeviceImport <absolutePathToImportFile> -type WAP

   Example:

```
> DeviceImport /root/IAPexport.csv -type WAP
 addDevice - start - ip = 192.168.10.82 contact = false
Adding Pingable to domain - East Campus
 DeviceImport::setDeviceType - importType - 4
 addDevice - start - ip = 192.168.10.83 contact = false
Adding Pingable to domain - East Campus
 DeviceImport::setDeviceType - importType - 4
 addDevice - start - ip = 192.168.10.84 contact = false
```

6. In the FortiNAC Administration UI, navigate to **Network > Inventory** and verify that the devices have been imported. If necessary, modify the device properties.
7. Right click on the VIP (master) model and click **Resync Interfaces**. This will associate the newly added APs with the master.

Once the WAPs are added, the switch ports connecting to the WAPs will display as WAP uplinks under the **Ports** tab of the switch model. For details see section Port uplink types of the Administration Guide.

Return to Add Infrastructure Devices.

Cisco Meraki MS Switch

Configure Switch

API Key

Obtain the API Key (this will be used in the FortiNAC Model Configuration). Once generated, the same API Key can be used in multiple devices. If the API key has not already been generated, do the following:

1. Navigate to **Organization > Settings**
2. Under **Dashboard API access,** select **Enable access to the Cisco Meraki Dashboard API**
3. Click Profile link

4. Under **API Access**, click **Create new API key**
5. Copy the generated key and save to a file

Serial Number

Obtain switch Serial number (this will be used in the FortiNAC Model Configuration).

1. Navigate to **Switch > Switches**
2. Select the switch
3. Copy the Serial Number and save to a file

SNMP

Configure SNMP access to allow for FortiNAC device discovery. Under the **Network-wide > General > SNMP** section, allow either v1/v2 or v3 access

Configure FortiNAC

1. Add switches to Inventory. For instructions see Add or modify a device (add an individual device) or Discovery (add devices in bulk) in the Administration Guide.

   Troubleshooting

   Troubleshooting SNMP Communication Issues

   Unable to add device to UI due to CLI credentials

   Unable to model device in GUI (“?” appears as the icon)
2. Select the newly added model.
3. Right click on the model and select **Model Configuration**.
4. Fill in the following fields as they apply and **Save**:
   - Serial Number
   - REST API Key

Return to Add Infrastructure Devices.

Cisco Meraki MX Router

Note: FortiNAC only collects IP to MAC information (L3 poll) from MX routers.

Configure Router

API Key

Obtain the API Key (this will be used in the FortiNAC Model Configuration). Once generated, the same API Key can be used in multiple devices. If the API key has not already been generated, do the following:

1. Navigate to **Organization > Settings**
2. Under **Dashboard API access,** select **Enable access to the Cisco Meraki Dashboard API**
3. Click **Profile** link
4. Under **API Access**, click **Create new API key**
5. Copy the generated key and save to a file

Serial Number

Obtain router Serial Number (this will be used in the FortiNAC Model Configuration).

1. Navigate to **Security Appliance > Appliance**
2. Copy the Serial Number and save to a file

SNMP

Configure SNMP access to allow for FortiNAC device discovery. Under the **Network-wide > General > SNMP** section, allow either v1/v2 or v3 access

Configure FortiNAC

1. Add the routers to Inventory. For instructions see Add or modify a device (add an individual device) or Discovery (add devices in bulk) in the Administration Guide.

   Troubleshooting

   Troubleshooting SNMP Communication Issues

   Unable to add device to UI due to CLI credentials

   Unable to model device in GUI (“?” appears as the icon)

   Note: The MX will not display ports. This is normal.
2. Select the newly added model and click the **Credentials** tab.
3. Fill in the following and **Save**:
   - Serial Number
   - REST API Key
4. Right click on the model and select **Group Membership.**
5. Select the box next to **L3 (IP-->MAC)** and click **OK**.
6. Click the **Polling** tab.
7. Select the box next to **L3 (IPàMAC) Polling** and set the interval to 30 minutes.
8. Click **Poll Now**. Verify the timestamps for **Last Successful Poll** and **Last Attempted Poll** update to the current time.

Return to Add Infrastructure Devices.

Mist Access Points

Configure Access Points

1. Record the Mist Site ID. This will be used when adding the device to FortiNAC.

   The Site ID can be retrieved from the Monitor page, or other https://manage.mist.com pages. Site ID is in the form of " xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "

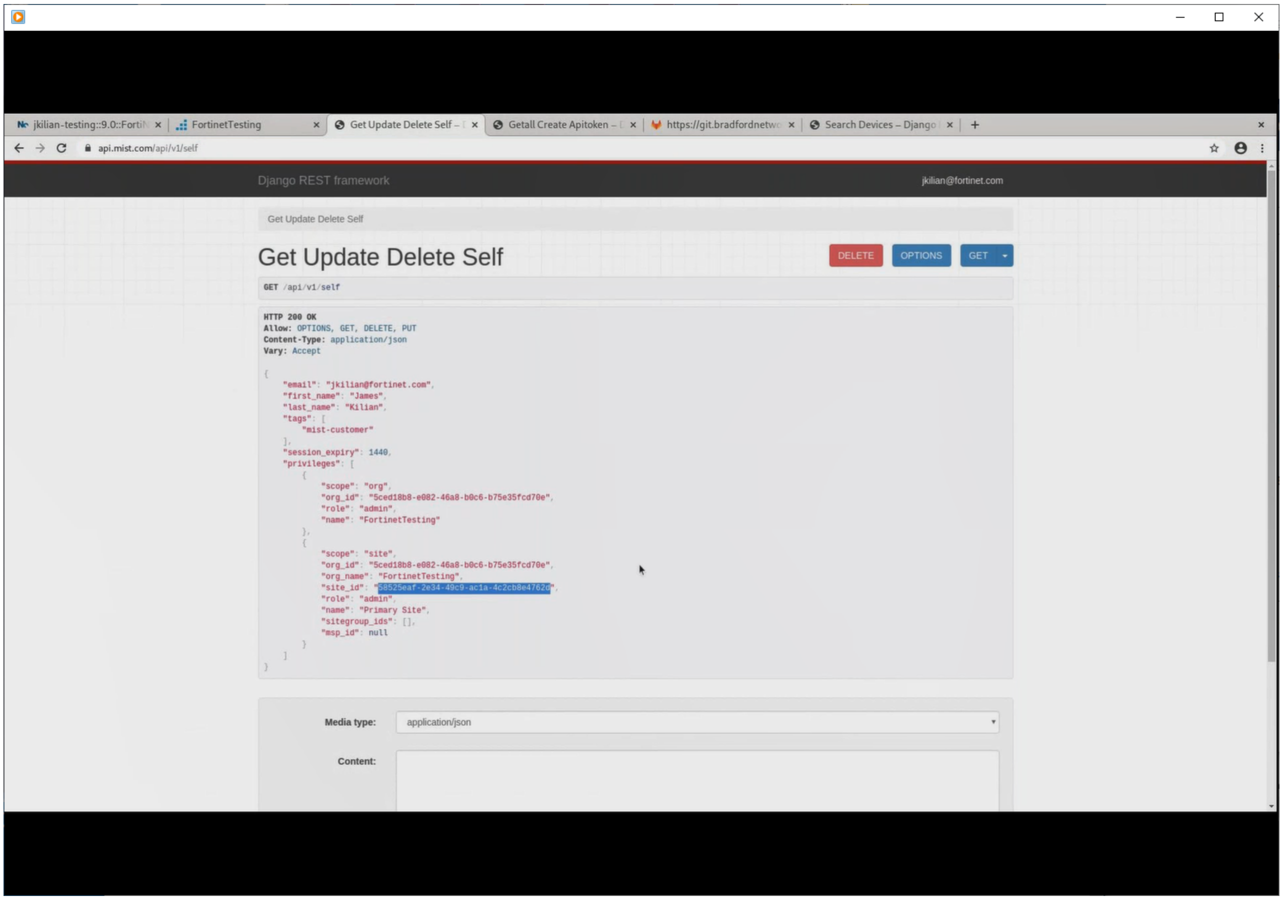
   Example:

   https://manage.mist.com/admin/?org_id=ORG_ID#!dashboard/insights/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

   Alternatively, use Mist API. Navigate to the following URL

   https://api.mist.com/api/v1/self

Record the value for “site_id”:



Get Update Delete Self

```
GET /api/v1/self
```

```
HTTP 200 OK
Allow: OPTIONS, GET, DELETE, PUT
Content-Type: application/json
Vary: Accept

{
    "email": "jkilian@fortinet.com",
    "first_name": "James",
    "last_name": "Kilian",
    "tags": [
        "mist-customer"
    ],
    "session_expiry": 1440,
    "privileges": [
        {
            "scope": "org",
            "org_id": "5ced18b8-e082-46a8-b0c6-b75e35fcd70e",
            "role": "admin",
            "name": "FortinetTesting"
        },
        {
            "scope": "site",
            "org_id": "5ced18b8-e082-46a8-b0c6-b75e35fcd70e",
            "org_name": "FortinetTesting",
            "site_id": "58525eaf-2e34-49c9-ac1a-4c2cb8e4762d",
            "role": "admin",
            "name": "Primary Site",
            "sitegroup_ids": [],
            "msp_id": null
        }
    ]
}
```

Media type: application/json

Content:

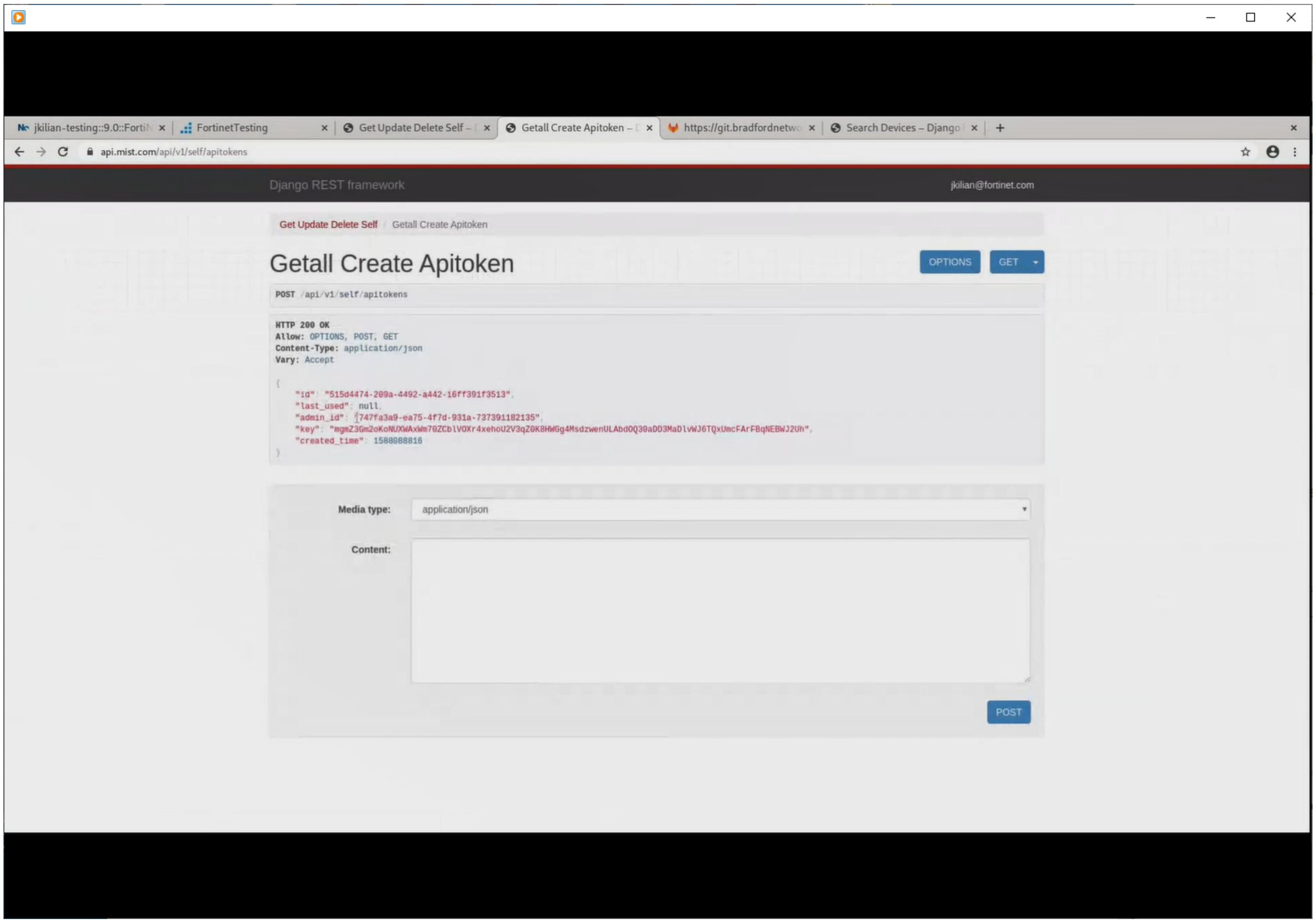
2. Generate API key.

a. Using Mist API go to https://api.mist.com/api/v1/self/apitokens

b. Click **POST** to generate key.

c. Refresh page.

d. Once key is displayed, copy and paste to a text file immediately. **Note:** Key is only viewable once.



Getall Create Apitoken

```
POST /api/v1/self/apitokens
```

```
HTTP 200 OK
Allow: OPTIONS, POST, GET
Content-Type: application/json
Vary: Accept

{
    "id": "515d4474-209a-4492-a442-16ff391f3513",
    "last_used": null,
    "admin_id": "747fa3a9-ea75-4f7d-931a-737391182135",
    "key": "mgmZ3Gm2oKoNUXWAxWm70ZCblVOXr4xehoU2V3qZ0K8HWGg4MsdzwenULAbdOQ30aDD3MaDlvWJ6TQxUmcFArFBqNEBWJ2Uh",
    "created_time": 1588088816
}
```

Media type: application/json

Content:

Configure FortiNAC

1. Login to the FortiNAC CLI as root.
2. Run the API tool to add the Mist device to the FortiNAC database. Use the API key and site ID recorded in previous section.

   CloudAPITool -domain api.mist.com -action discovery -port 443 -apikey "<API_KEY>" -site <SITE_ID> -container <container>

   Note:

   - If container is specified but does not exist, it will be created.
   - If no container is specified, the AP's will be added to a container named "MistWirelessAPs".

Model is now populated under **Network > Inventory**.Return to Add Infrastructure Devices.

Replacing a Modeled Device

When adding a switch or router that will use the same IP address as the original device, the original model in Topology must be deleted from the database and a new model added. This ensures all internal mappings and files associated to that model are correct for the new device. Otherwise, unexpected behavior can occur such as…

- Unable to read VLANS
- L2/L3 Poll failures
- Credential validation failure
- Switching VLANs on the wrong ports

Note: Deleting the model from FortiNAC removes all manual switch device and port groupings done on the switch model.

For instructions, see section Replace a device using the same IP address of the Administration Guide.

Modifying Switch Components in a Stack

When adding, replacing, or removing switches from a stack, FortiNAC must re-learn the interface mappings to ensure they are correct with the new stack configuration. Otherwise, unexpected behavior can occur (such a VLANs switching on the wrong ports).

The following procedure allows FortiNAC to re-learn the new interface structure before taking action on any enforced ports. **Note**: If the indexing has changed and FortiNAC needs to remodel the interfaces, FortiNAC will delete and recreate new port models to represent the re-indexed switch interfaces. This will affect manual port grouping done for the interface models.

1. Click on the device in **Inventory**.
2. Click on the **Element** tab.
3. De-Select **VLAN Switching Enabled.** This prevents FortiNAC from manipulating VLAN configurations on the switch.
4. Click **SAVE**.
5. Make the changes to the stack.
6. Right-click on the model in the tree and select **Re-Sync Interfaces** (this may take a few moments depending upon the size of the stack).
7. Verify the port view and group membership is accurate based upon the new configuration.
8. Perform L2 poll to ensure the latest MAC address information for the switch. Click the polling tab and next to L2 (Hosts) Polling and click **Poll Now**.
9. Once polling completes and port view looks accurate, re-select **VLAN Switching Enabled**.

Click **SAVE**.