FortiNAC - IP Phone Integrations

Version F 7.x

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

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

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

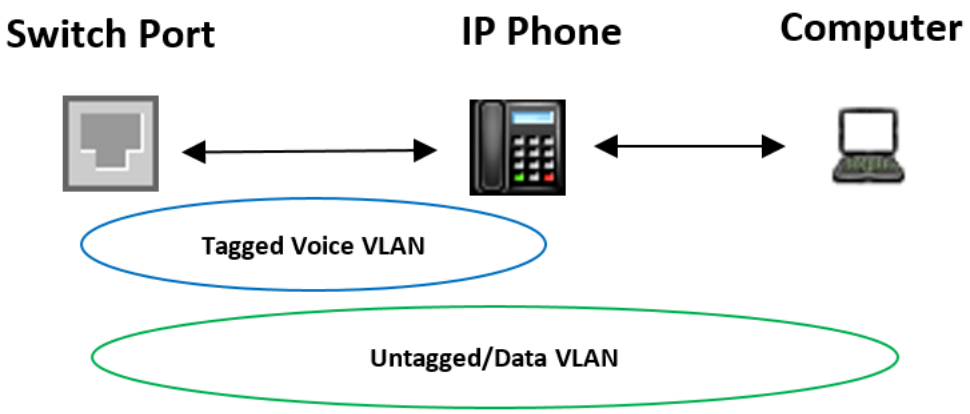
May 15, 2023
FortiNAC F 7.x IP Phone Integrations
49-922-769106-20211216

TABLE OF CONTENTS

IP Phones Using Tagged Voice VLANs

Overview

Important: This document is intended to be used in environments where IP Phones utilize a tagged Voice VLAN. This VLAN operates independently of the untagged VLAN that governs other traffic (data) on the connecting switch port. If the IP Phones to be integrated do not use tagged Voice VLANs, see section IP Phones Using Untagged VLANs for instructions.



What it Does

Provides visibility and control for endpoints connecting behind IP Phones on the network.

FortiNAC does not provide any special integration logic for different IP phone vendors. Typically, the network administrator deploys the organization's IP phone infrastructure independently of configuring the FortiNAC. Because FortiNAC's focus is on endpoints daisy-chained to the phone, the type of phone that is used is unimportant.

How it Works

- **IP phone MAC address is ignored when determining the appropriate untagged VLAN for a port**: The untagged VLAN on a given port (data VLAN) will not be switched based upon the presence of a device with the **IP Phone** device type. The untagged VLAN will only switch based upon a device connecting behind the phone.

  Example:

1. An unregistered/Rogue IP phone connects to a switch port and is isolated.
2. Device is registered using type **IP Phone**.
3. Although the device is now registered, the untagged VLAN will not change because the IP Phone device type is ignored.

- **Voice VLAN manipulation**: By default, FortiNAC does not provision voice VLANs when an IP phone connects. Additional configuration is required using one of the following methods:
  - FlexCLI: FortiNAC configures the port to support voice when an IP Phone is detected. The configuration is removed when the phone disconnects. FortiNAC has limited support for this by leveraging the FlexCLI feature to specify the switch-specific commands to manage this process. For a list of supported vendors, refer to the CLI Configuration section of the Administration Guide.
  - RADIUS: When IP Phone connects, FortiNAC includes the Voice VLAN value in the RADIUS response. Switch ports must be configured for RADIUS authentication.
- **IP Phone Connection information**: Cisco switches can send CDP notifications triggered by IP Phone traffic that is transmitted across untagged VLANs. Other switches have the ability to send MAC Notification messaging as well. FortiNAC has the ability to process this traffic and update connection information for endpoints already classified as IP Phones. The ability to process and update IP Phone connectivity information is applicable for the following use cases:
  - Device Profiling: Revalidate IP Phone on connect
  - Automated Voice VLAN Configuration

    Note: Function is disabled by default.
- **Connection information of hosts daisy-chained to the phone**: FortiNAC learns when endpoints come and go from the phone ports through either MAC Notification Traps or RADIUS authentication. FortiNAC cannot rely on linkUp/linkDown traps since the IP Phone keeps the link state up.

Note: RADIUS authentication may not provide real time information when an endpoint disconnects.

Host Connection Process Through Phone Port

1. PC connects to the port on the back of the phone.
2. FortiNAC learns of the connection:
   - If MAC Notification Traps are enabled, a trap is sent to FortiNAC.
   - If RADIUS is configured, an Access Request is sent to FortiNAC.
   - If neither MAC Notification Traps nor RADIUS are configured, then the presence of the host connection is not detected until the next L2 Poll. The host will connect immediately to the network or VLAN to which the port is currently set. If the polling interval is very long, a host may have to wait before being able to register or moving to the correct VLAN.
3. FortiNAC searches for the PC's MAC address in the database to determine whether or not it is registered.
4. If it is not registered, the PC is placed in the Registration VLAN but the phone remains in the Voice VLAN.
5. If it is registered, the PC is placed in the Production VLAN but the phone remains in the Voice VLAN.

Note: Once an IP Phone is connected to a port, FortiNAC does not bring down the interface to change VLANs. If there is an agent installed on the connected machine, the agent does a release/renew of the IP address (see **PA Optimization** under Device Properties in the Administration Guide). If there is no agent installed, the user must wait for the IP address lease to expire. Default lease times for FortiNAC isolation scopes are 60 seconds.

Requirements

- RADIUS or MAC Notification Traps for accurate and timely connection information regarding endpoints behind IP Phones.

  Note:
  - Some switches may not support MAC Notification Traps or RADIUS. In such cases, consider increasing the L2 Poll frequency for the switch model.

- When a registered IP Phone connects or moves to another wired port, the change is not detected until an L2 poll is performed on the switch. By default, MAC Notification Traps for IP Phones are ignored. This setting can be changed under Network > Settings > Network Device, however, enabling the processing of traps for IP Phones could potentially impact performance.

- Do not trunk Cisco ports that have IP Phones connected. Configure the access (untagged) VLAN and Voice VLAN for the port. FortiNAC does not manage trunked ports.

Steps

Step 1: Configure Switch(es) and Phones

1. Configure a tagged Voice VLAN on switches to which IP Phones will be connected.
2. Configure RADIUS or MAC Notification traps on the same set of switches. For trap configuration, see the Configuring Traps for MAC Notification reference manual in the Fortinet Document Library. If the switches do not support either function, the L2 Polling frequency can be increased under the Polling tab of the switch model in **Network > Inventory**.
3. Provision the phones with their proprietary configuration.

Step 2: Review Model Configuration for Connecting Switches

1. Ensure the switches to which IP Phones are connecting are modeled in Topology. If not yet modeled, see Add or modify a device in the Administration Guide.
2. Define Voice VLANs (if necessary):
   - The Voice VLAN is automatically detected for most switches. Therefore, if the Voice VLAN(s) field is present, it can be left blank.
   - (Cisco non-IOS switches only): Under Network > Inventory, modify the Model Configuration and enter a comma separated list of Voice VLANs in the Voice VLAN(s) field. This indicates to FortiNAC that devices on that VLAN should never be moved to any other VLAN.

Step 3: Automated Voice VLAN Configuration (optional)

FortiNAC can automatically configure the Voice VLAN using the following methods:

Method	Description
FlexCLI	FortiNAC configures the port to support voice when an IP Phone is detected. The configuration is removed when the phone disconnects. FortiNAC has limited support for this by leveraging the FlexCLI feature to specify the switch-specific commands to manage this process. See section in Appendix for instructions.
RADIUS	When IP Phone connects, FortiNAC includes the Voice VLAN value in the RADIUS response. Switch ports must be configured for RADIUS authentication. See section in Appendix for instructions.

Step 4: Create Host Group for IP Phones

Use a host group for configuring automatic removal of stale IP Phone records from the database. Otherwise, IP Phone records will remain in the database indefinitely.

1. In Administrative UI, select **System > Groups.**
2. From the Group view, click **Add**.
3. Enter a Group Name such as “IP Phones”.
4. Select Member Type **Host**.
5. Configure aging properties:
   - **Days Valid**: Calculates the Expiration Date for each host in the group (regardless of online status). If left blank, the record will not be removed based on this setting.
   - **Days Inactive**: The number of consecutive days a host is seen offline before removing from the database.
6. Enter a Group Description (optional).
7. Click **OK** to save the new group.

Step 5: Add IP Phones to the FortiNAC Database

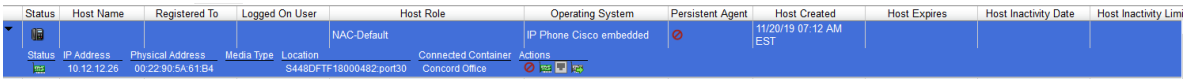
IP Phones can be added to the FortiNAC database using one of the methods in the table below. Regardless of the method used ensure the following:

- Device Type = IP Phone. This Device Type indicates to FortiNAC these devices should be ignored when determining the VLAN for the port.
- Register as a Device.

Method	Description
Device Profiling Rules	Automatically identify and classify IP Phones. See Add Phones Using Device Profiler.
Import using a .csv file	For details, see Import Hosts, Users Or Devices in the Administration Guide.
Manually register existing phones	Connect phones to the network then convert host records to IP Phones using the Register As Device tool. For details, see Register A Host As A Device in the Administration Guide.
Manually add phones before they connect	Add a new host record in the Host View, choose Register As A Device in the Add window, then select IP Phone as the device type. For details, see Add or Modify a Host in the Administration Guide.

Validate

1. Ensure the switch port is configured for enforcement. Right-click on the switch port in Port View and select **Group Membership** to verify.
2. Under **Users & Hosts > Hosts** verify IP Phone host record appears with Device Type IP Phone and shows an online connection status (green adapter record).



3. Check the phone has the proper IP address assigned and is working.
4. Connect an unknown computer behind the phone and attempt to access the network.
5. Verify the following:
   - Host shows online and connected to the switch port in Users & Hosts > Hosts.
   - Ports tab shows the following icon on the switch port:

     - The port's untagged (data) VLAN configuration is changed to the isolation VLAN.

       Note:
       - Once an IP Phone is connected to a port, FortiNAC does not bring down the interface to change VLANs.
       - If there is an agent installed on the connected machine, the agent does a release/renew of the IP address.

- If there is no agent installed, the user must wait for the IP address lease to expire. If not using agents on host machines, configuring shorter lease times for production DHCP scopes may be desired.

6. Once isolated, register the host.
7. Verify the following:
   - Host icon reflects properly in **Users & Hosts > Hosts**.
   - **Ports** tab shows the following icon on the switch port:

- The port's untagged (data) VLAN configuration is changed to the appropriate VLAN.

  Note: If there is no agent installed, the user must wait for the IP address lease to expire. Default lease times for FortiNAC isolation scopes are 60 seconds.

IP Phones Using Untagged Voice VLANs

Overview

This document provides the steps required to add IP Phones that use untagged VLANs to the FortiNAC database. FortiNAC does not provide any special integration logic for different IP phone vendors. Typically, the network administrator deploys the organization's IP phone infrastructure independently of configuring the FortiNAC.

Important: This document is intended to be used in environments where IP Phones do not utilize a tagged Voice VLAN.

What it Does

- Because an untagged voice VLAN is defined for the IP Phone, it is possible for FortiNAC to assign VLANs based on the IP Phone connectivity.
- Provide visibility and control for IP Phone connections on the network as well as endpoints connecting behind IP Phones. **Note**: There are caveats regarding control. See considerations below.

Considerations

The following applies to switches configured for port based VLAN switching:

- The port will be temporarily disabled during any port VLAN switching.
- If a computer is plugged in behind the phone, both devices should be configured to communicate over the same untagged VLAN.
- If a computer is plugged in that requires FortiNAC to isolate (e.g. Rogue, At-Risk or not authenticated), the VLAN will be switched. This will cause the IP phone to lose communication.

Steps

Step 1: Configure Switch(es) and Phones

1. Configure an untagged VLAN on switches to which IP Phones will be connected. If a computer will be plugged in behind the IP Phone, both devices should be configured to communicate over the same untagged VLAN.
2. Configure RADIUS or MAC Notification traps on the same set of switches. For trap configuration, see the Configuring Traps for MAC Notification reference manual in the Fortinet Document Library. If the switches do not support either function, the L2 Polling frequency can be increased under the **Polling** tab of the switch model in **Network > Inventory.**
3. Provision the phones with their proprietary configuration.

Step 2: Determine Device Type

As long as the device is identified as an IP phone (i.e. the device was registered using “IP Phone” device type), FortiNAC does not consider its presence when calculating the VLAN for the port. If FortiNAC needs to be able to switch VLANs based on the IP Phone’s presence, a different device type must be used.

Select a Different Device Type (optional)

1. Navigate to **Network > Settings > Identification > Device Types**.
2. Review the existing device types and determine which one will be used to identify the IP Phone (other than “IP Phone”). The **In Use** button allows you to see whether a device type is currently being used in the system.

   A new device type can be created to identify the IP Phones. This is helpful to ensure no other devices use the device type. In addition, Network Access Policies can then be configured based on matching the new device type in order to assign the voice VLAN.

   Create a new device type:

   a. Click **Add**.

   b. Either

      To select from a list of custom icons, click Select from Archive, choose an icon from the list. Search for “phone” to view options from the archive for alternative phone icons. Then click **OK**.

      Or

      Add a custom icon by selecting the **Upload Icon**.

   c. Enter a name for the device type icon, and click **OK**.

Step 3: Create Host Group for IP Phones

Use a host group for configuring automatic removal of stale IP Phone records from the database. If a host group is not used, the global age settings in Users & Hosts > Settings > Aging will apply as long as an alternate device type is used. Global age settings do not apply to the standard IP Phone device type.

1. In Administrative UI, select **System > Groups.**
2. From the Group view, click **Add**.
3. Enter a Group Name such as “IP Phones”.
4. Select Member Type **Host**.
5. Configure aging properties:
   - **Days Valid**: Calculates the Expiration Date for each host in the group (regardless of online status). If left blank, the record will not be removed based on this setting.
   - **Days Inactive**: The number of consecutive days a host is seen offline before removing from the database. It is recommended to set this value.
6. Enter a Group Description (optional).
7. Click **OK** to save the new group.
8. Proceed with desired method to add phones to the database.

Step 4: Add IP Phones to the FortiNAC Database

IP Phones can be added to the FortiNAC database using one of the methods in the table below.

Method	Description
Device Profiling Rules	Automatically identify and classify IP Phones. See Add Phones Using Device Profiler.
Import using a .csv file	For details, see Import Hosts, Users Or Devices in the Administration Guide.
Manually register existing phones	Connect phones to the network then convert host records to IP Phones using the Register As Device tool. For details, see Register A Host As A Device in the Administration Guide.
Manually add phones before they connect	Add a new host record in the Host View, choose Register As A Devicein the Add window, then select IP Phone as the device type. For details, see Add or Modify a Host in the Administration Guide.

Validate

1. Ensure the switch port is configured for enforcement. Right-click on the switch port in Port View and select **Group Membership** to verify.
2. Under **Users & Hosts > Hosts** verify IP Phone host record appears with the intended device type and shows an online connection status (green adapter record).
3. Check the phone has the proper IP address assigned and is working.
4. If a computer is connected behind the phone, verify the following:

- Host shows online and connected to the switch port in **Users & Hosts > Hosts.**
- Ports tab shows one of the following icons on the switch port:

Using Standard IP Phone Device Type

Using Alternate IP Phone Device Type

Troubleshooting

Related KB Articles

Confirming MAC Notification traps via Administration UI

Troubleshooting VLANs not changing on a wired switch

Appendix

Add Phones with Voice VLANs Using Device Profiler

Configure Device Profiling Rule(s)

1. Select Users & Hosts > Device Profiling Rules.
2. Click the Add button or select a rule and click Modify.
3. Under the General tab, fill in fields as necessary. For information on each field, see section Adding a rule in the Administration Guide.

   Required Settings:
   - Type = IP Phone
   - Register as = Device in Host View
4. Click Add to Group and select the new IP Phone group created previously.
5. On the Methods tab, one or more methods for identification can be selected. For details on method selection and rule ranking, see Device Profiler Configuration.

Resulting Workflow

1. Rogue IP phone connects.
2. Device Profiler detects the IP phone.
3. The phone is evaluated. If a rule matches, one of the following occurs:
   - Registration = automatic: Phone is registered and searchable in **Users & Hosts > Hosts.** Phone is listed under **Users &Hosts > Profiled Devices.**
   - Registration = manual: phone is a rogue record and searchable in **Users & Hosts > Hosts.** Phone is listed under **Users & Hosts > Profiled Devices** from where the device can be registered manually.
4. IP Phone Host group: Once registered, the host becomes a member of the new host group, which then applies to the host record any values set in Days Valid or Days Inactive.
5. Aging: After the defined age time has passed, the IP phone is deleted from the database.
6. If the phone reconnects, it is re-profiled and any configured group aging properties are re-applied.

Proceed to Validate.

Automated Voice VLAN Configuration Using FlexCLI

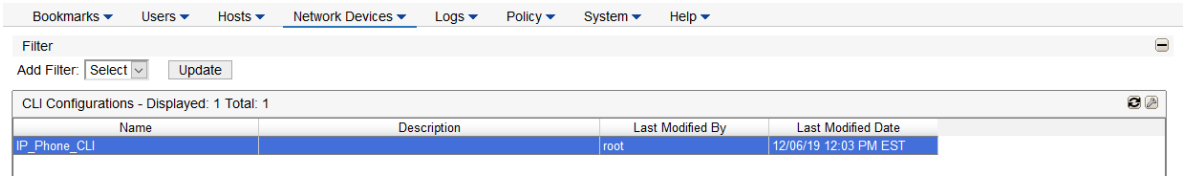
Configure FortiNAC to assign Voice VLAN via RADIUS as IP Phones connect. For a list of supported vendors, refer to the CLI Configuration section of the Administration Guide.

Cisco CLI example:

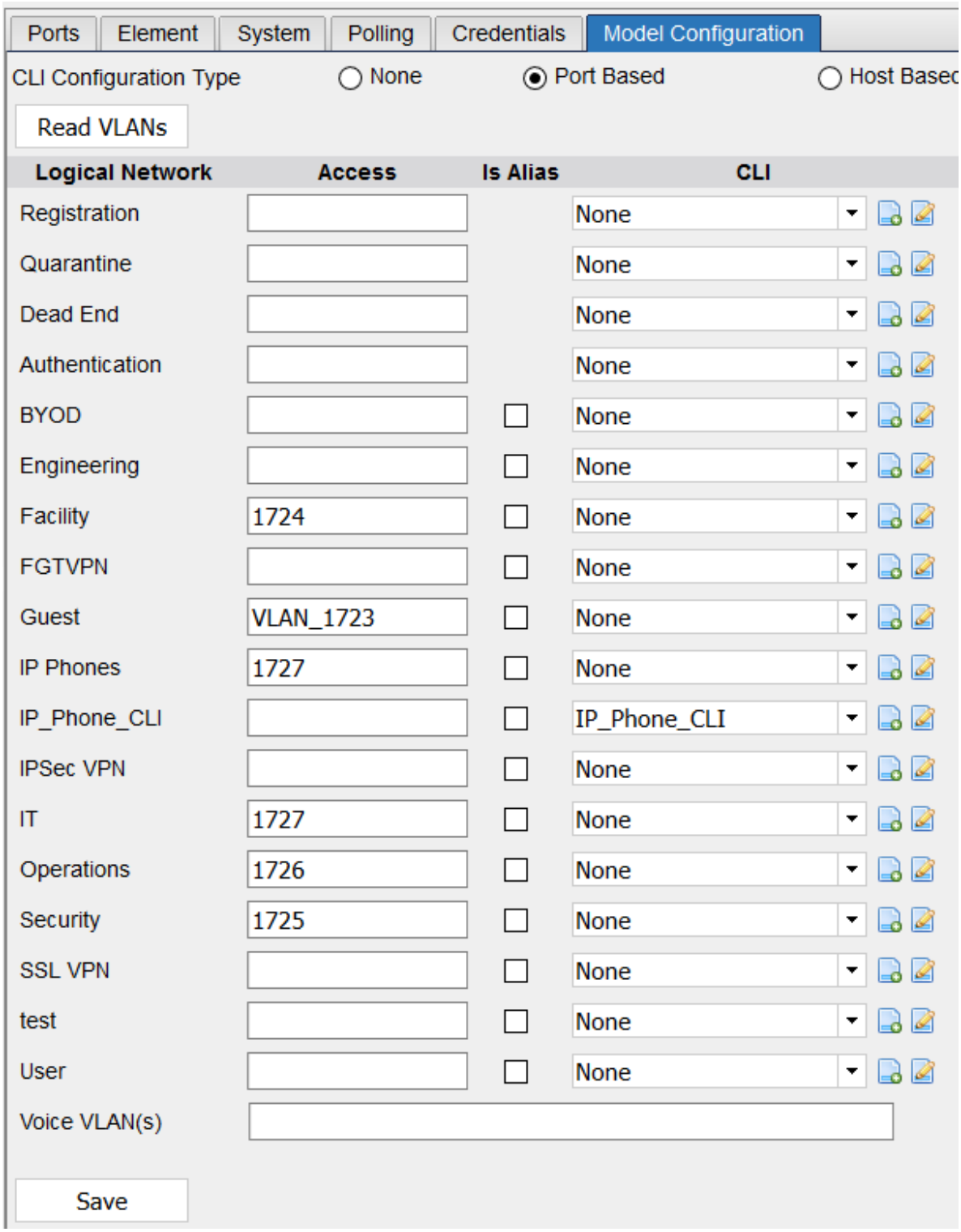
```
interface FastEthernet2/0/10

switchport access vlan 10
```

```
switchport mode access
switchport voice vlan 99
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
snmp trap mac-notification change added
snmp trap mac-notification change removed
auto qos voip cisco-phone
spanning-tree portfast
service-policy input AutoQoS-Police-CiscoPhone
!
```

1. Navigate to **Network > CLI Configuration** and add the CLI configuration to set the voice VLAN. See section CLI Configuration/Add or modify a configuration of the Administration Guide for more details.



2. Navigate to Network > Inventory and modify the switch's Model Configuration and define the CLI configuration created in the previous step. See section Assigning access values and CLI configurations of the Administration Guide for more details.



3. Create a Network Access Policy to apply the CLI configuration when the phone connects.

   User/Host Profile Requirement

   Who/What by Attribute: Host [Device Type: IP Phone]

   Or

Who/What by Group: <Group created for phones in previous step>

Configuration Requirement

Logical Network: <Logical Network associated with the CLI Configuration>

See section Add or modify a policy of the Administration Guide for more details.

4. Once ready to start the automated provisioning, add to the **Role-Based Access** port group the ports desired to make the CLI change when an IP Phone connects. This can be done via the Groups or the Ports view. **Important**: Test with one port to ensure proper behavior before adding all ports to this group.
5. For real-time Voice VLAN provisioning as phones connect, proceed to Enable IP Phone MAC Notification Trap Processing.

Automated Voice VLAN Configuration Using RADIUS

This configuration is required when the device model is set for Proxy RADIUS mode. It is not required for Local RADIUS mode. For details on modes see Model configuration in the Administration Guide.

Configure FortiNAC to assign Voice VLAN via RADIUS as IP Phones connect.

- When set to true, FNAC responds with VLAN value via RADIUS.
- When set to false (default), FNAC responds with access accept with no vlan (NativePolicy).

Contact Support for assistance.

1. Login to FortiNAC CLI as root.
2. Modify /bsc/campusMgr/master_loader/.masterPropertyFile and add the following lines:

```
FILE_NAME=./properties_plugin/bridgeManager.properties
{
com.bsc.plugin.bridge.BridgeManager.provisionIPPhones=true
}
```

3. Save file.
4. Restart FortiNAC processes for the change to take affect:
   shutdownNAC
   <wait 30 seconds>
   startupNAC
5. For real-time Voice VLAN provisioning as phones connect, proceed to **Enable IP Phone MAC Notification Trap Processing**.

Enable IP Phone MAC Notification Trap Processing

The ability to process and update IP Phone connectivity information is applicable for the following use cases:

- Device Profiling: Revalidate IP Phone on connect

- Automated Voice Provisioning via CLI

Note: This function should only be enabled when necessary. It has been observed some IP Phones may initiate frequent Notification Traps. FortiNAC must process each trap, and this behavior can cause unnecessary work.

To enable FortiNAC to process the traffic, navigate to Network > Settings > Network device and de-select the checkbox next to Ignore MAC Notification Traps for IP Phones.

Proceed to Create Host Group for IP Phones.

Cisco Switch RADIUS Configuration

This configuration is to prevent a Cisco IP Phone from disconnecting when a VLAN is changed for the computer connected behind the phone. Otherwise, it is possible for the IP Phone to be forced to re-authenticate at the same time as the computer.

Requires RADIUS authentication via Local RADIUS Server.

Behavior:

1. FortiNAC sends a CoA message to disconnect the computer.
2. Computer disconnects from the port and re-authenticates while the IP phone remains authenticated.

Cisco Switch Port Configuration

It is recommended to use multi-domain.

Example:

```
interface TenGigabitEthernet1/3
switchport mode access
switchport voice vlan 1130
authentication host-mode multi-domain
authentication port-control auto
authentication periodic
authentication timer reauthenticate 180
mab
dot1x pae authenticator
dot1x timeout quiet-period 3
dot1x timeout server-timeout 10
dot1x timeout tx-period 5
dot1x timeout supp-timeout 6
spanning-tree portfast edge
spanning-tree bpduguard enable
end
```

FortiNAC Configuration:

1. Configure and enable Local RADIUS Services. Refer to the Local RADIUS Server reference manual for instructions.
2. Create a Logical Network for the Voice VLAN. For instructions see Configure Logical Networks.
3. Create Network Access Policies to provision VLANs. For instructions see Network access policies in the Administration Guide.

   Dynamically Provision Voice VLAN for IP Phones (optional)

- **User/Host Profile** – Match criteria unique to the IP Phones. The simplest matching criteria to use is Device Type = IP Phone. Other criteria can be used as desired.
- **Network Access Configuration** to assign the data VLAN's logical network.

4. Select the Cisco switch Device Model under **Network > Inventory** and click the **Model Configuration** tab.
5. Click **Enable RADIUS authentication** for this device and click Local.
6. Configure the appropriate VLAN ID and RADIUS Attribute Group for each Logical Network as they apply.

Data VLAN

- Access Value = Data VLAN ID
- RADIUS Attribute Group: RFC_Vlan
  Note: Use Default can be used if the Default Attribute Group = RFC_Vlan

Tagged Voice VLAN

- Access Value = <Voice VLAN ID >
- Create a custom RADIUS Attribute Group
  a. Click the Add icon next to Logical Network for the Voice VLAN.
  b. Enter the RADIUS Attribute Group name "Cisco IP Phone".
  c. Add the attribute:
  Attribute: Cisco-AVPair
  Response value: device-traffic-class=voice
  d. Click OK to save.
  Hint: Use the Name filter to locate the various attributes in the Available Attributes list.