FortiNAC

Configuration Wizard

Version: 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 9.1

Date: February 4, 2022

Rev: H

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

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

FORTINET KNOWLEDGE BASE
https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase

FORTINET BLOG
http://blog.fortinet.com

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

FORTINET COOKBOOK
http://cookbook.fortinet.com

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

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

Contents

Overview

This document provides the steps necessary for configuring the FortiNAC appliance(s). It is intended to be used in conjunction with the Deployment Guide in the Fortinet Document Library.

Terminology

Term	Definition
"Isolation" VLAN	Used for network segmentation of unknown and untrusted endpoints. Provides limited network access
FortiNAC Service Network Interface	Configured on the eth1 interface of the appliance. Serves DHCP, DNS and the Captive Portal to the "isolation" VLANs
FortiNAC Service Network VLAN	VLAN where the FortiNAC Service Network Interface resides in L3 Network Configurations. For more information, see FortiNAC Service Configuration (Network Type) in the Appendix

Requirements

- FortiNAC appliance has been staged and can be reached over the interface specified below
  - Virtual appliances and existing installations: eth0
  - New physical appliances: eth1 (see Appliance Installation Guide for details)
- License key(s)
- Appliance passwords
- Appliance Network Addressing
  - Hostname
  - IP address and Network Mask for Eth0 and Eth1
  - Default Gateway
  - Domain name
  - DNS server(s)
  - NTP server(s)
- At least one DHCP scope for "isolation" VLAN

See section **Requirements Task List** in the Appendix of the Deployment Guide for details regarding the above requirements.

Accessing Configuration Wizard

Configuration Wizard URL

Launch the Configuration Wizard by opening a browser and navigating to:

`https://<FortiNAC IP Address or hostname>:8443/configWizard`

Connecting to a Secondary Server in L2 High Availability

In a High Availability configuration, use the Secondary Server IP address when accessing the Secondary Server's Configuration Wizard. If redirected to the Primary Server Configuration Wizard, see Access Secondary Server Wizard Post L2 HA Configuration in the Appendix.

Procedure

Apply License Key

Note: It is not necessary to key the appliances in any specific order.

1. Launch the Configuration Wizard using the applicable URL below.

   Initial Physical Appliance Installations Only

   1. Connect PC to the eth1 interface of the physical appliance.
   2. Launch the Configuration Wizard by opening a browser and navigating to: `http://192.168.1.1:8080/configWizard`

   Configuration Wizard URL
   Open a browser and navigate to:

   `https://<FortiNAC IP Address or hostname>:8443/configWizard`

2. Enter the Configuration Wizard credentials.

   User Name = config

   Password = config

   The **License Key** window is displayed.

   Virtual: This field will be blank.

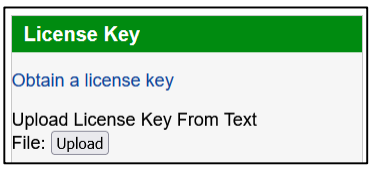
   Physical: This field will already be populated. All hardware appliances are shipped with an Appliance (Base) License Key.

3. Copy the key downloaded from FortiCare.

   Virtual Appliances: Click the **Upload** button and select the .lic file associated with the appliance's Serial Number. This must be done for every appliance.

   Physical Appliances:

   - Click the **Upload** button and select the .lic file associated with the managing server's Serial Number. This should be the Endpoint License key.
   - All other appliances: Proceed to step 4. **Important: Do not modify the key**.



4. Click **OK** at the bottom of the License Key window.
5. Click **OK** at the document screen.

Basic Network Configuration

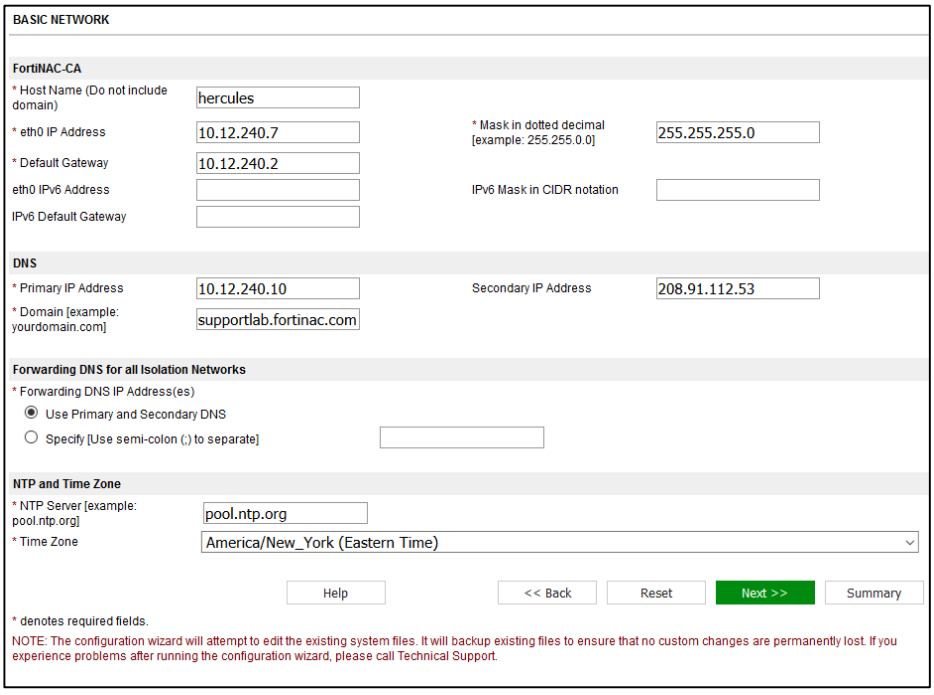
Note the following:

- The data displayed in the Configuration Wizard may not represent the current configuration of the appliance. When making edits in the Configuration Wizard, modifications are stored in a temporary file. This allows users to exit the Configuration Wizard before saving changes permanently.
- If the FortiNAC's hostname is not in DNS, or if the computer used to access the FortiNAC UI is not using the same DNS as the FortiNAC Server, make sure the following are defined in the computer's hosts file:
    - IP address
    - Host name
    - Fully-qualified domain name for eth0

Use the following buttons and links to navigate through the Configuration Wizard.

- **Steps pane**—This is the panel displayed on the left of each Configuration window. Each step is a link to its corresponding window. It is not required that you follow the configuration steps sequentially.
- **Help**—Opens a separate window to the FortiNAC section of the Fortinet Document Library.
- **Reset**—Click Reset to return field values to what they were when you opened the view. If you move to another window, you can no longer reset field values.
- **Summary**—Lists all configured settings. You can view a summary at any point in the configuration process and apply those settings.

The initial **Basic Network** screen displays the Product Descriptor and the type of system being configured.



1. Enter the values based on the definitions in **Basic Network Window Field Definitions** in the table below.

2. Click **Next** to go to the Passwords screen.

Basic Network Window Field Definitions

FortiNAC Product

Host Name	Name of the appliance you are configuring. Host names should contain only letters, numbers or hyphens (-). Uppercase letters are converted to lowercase automatically. **Note:** Do not use nac, isolation, registration, remediation, remotereg, remotescan, vpn, authentication, hub, or deadend. These names are reserved for system use.
eth0 IP Address	Management IP Address of the appliance you are configuring.
Default Gateway	Default Gateway IP address for the appliance you are configuring. A default gateway is the device that passes traffic from the local subnet to devices on other subnets.
Mask	Subnet mask for the appliance you are configuring. A subnet is a logical grouping of connected network devices; the mask defines the boundaries of the subnet.

DNS

Primary IP Address	IP address of the Primary DNS Server. This is used in the basic IP network configuration for the appliance.
Secondary IP Address	IP address of the Secondary DNS Server. This is used in the basic IP network configuration for the appliance.
Domain	Enter your domain name, such as megatech.com or megatech.edu.

Forwarding DNS for all "Isolation" Networks

Forwarding DNS IP Address(es)	The Forwarding DNS directs hosts to public update sites during registration and remediation as determined by the policy enforcement requirements. Select Use Primary and Secondary DNS to use your existing DNS servers or select Specify to enter a list of alternate DNS servers.

NTP and Time Zone

NTP Server	NTP and Time Zone settings keep the software date and time up-to-date. The NTP Server can be an IP Address or a name, such as pool.ntp.org.
Time Zone	Select the time zone for your server.

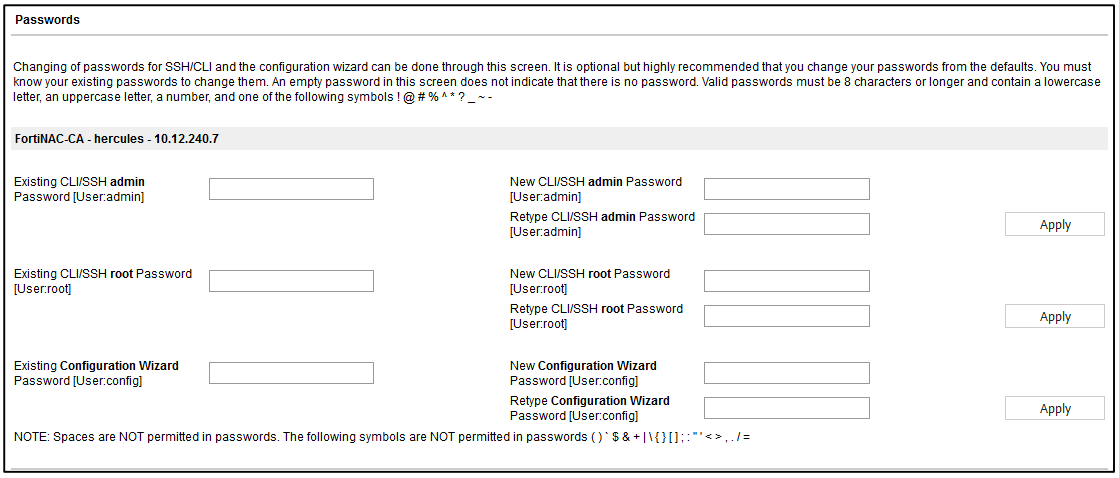
Configure Passwords

Password fields appear empty until a password is modified. Passwords can be modified again later by accessing the Change Passwords screen. See section Change Passwords After Configuration in the Appendix.

Configure passwords as required:

- **admin**—CLI/SSH password used to log into the appliance with limited permissions. For details see CLI Admin User Permissions in the Appendix.
- **root**—CLI/SSH password Customer Support uses to log into the appliance. It is required to change this password.
- **Configuration Wizard**—Password used to log into the Configuration Wizard. It is required to change this password.

Note: The Administration UI password is not configured within Configuration Wizard. The UI password will be configured in a later step.



Configuration Wizard - Password Setup

Procedure

1. Click in the **New Password** field and type the new password (8 to 64 characters).
2. Click in the **Retype Password** field and enter the new password again.
3. Click **Next**.

   Root and admin password changes take effect immediately. Changes to the Configuration Wizard password will not take effect until tomcat-admin has been restarted.

Configure Eth1 (FortiNAC Service Interface)

Configure FortiNAC's eth1 interface. The following components require configuration on FortiNAC:

- FortiNAC Service Interface(s): The interface(s) which FortiNAC uses to communicate with endpoints in the "isolation" VLANs.
- DHCP scope(s): Used by FortiNAC to deliver IP addressing to isolated endpoints. In some cases, FortiNAC also delivers IP addressing for known/trusted hosts.

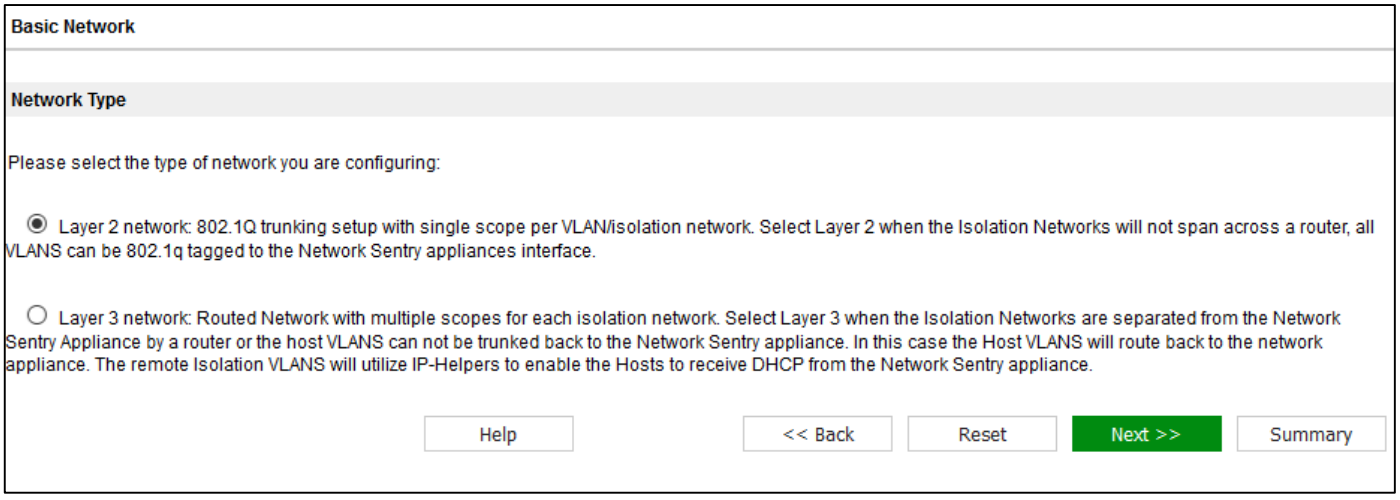
Select Network Type

1. Select one of the following options:
   - **Layer 2 network**: Traffic in the "isolation" VLANs are switched to the FortiNAC eth1 interface. 802.1Q tags are configured for the corresponding "isolation" VLANs, and eth1 IP addresses are within those networks. See screen capture below for additional information regarding this option.
   - **Layer 3 network**: Instead of trunking VLANs on eth1, eth1 is connected to a single VLAN on an untagged port. Network traffic is routed to the clients rather than the clients connecting to the same broadcast domain as the eth1 interface. See screen capture below for additional information regarding this option.

     For examples, see Appendix.

     High Availability: If appliances will be configured for High Availability, there are some design considerations. See High Availability Design Considerations in the Appendix.

2. Click **Next**.



Network Type

3. Proceed to the appropriate section:
   Layer 2 Network
   Layer 3 Network

Layer 2 Network

VLAN Types

VLANs are the basic networking construct used to limit network access. When you implement network access control, include at least one "isolation" VLAN. If there is the need to separate clients based on state, such as known vs. unknown or out-of-compliance, configure multiple VLANs. In the Configuration Wizard these additional VLANS are the Registration, Remediation, Dead End, VPN, Authentication, Isolation, and Access Point Management VLANs.

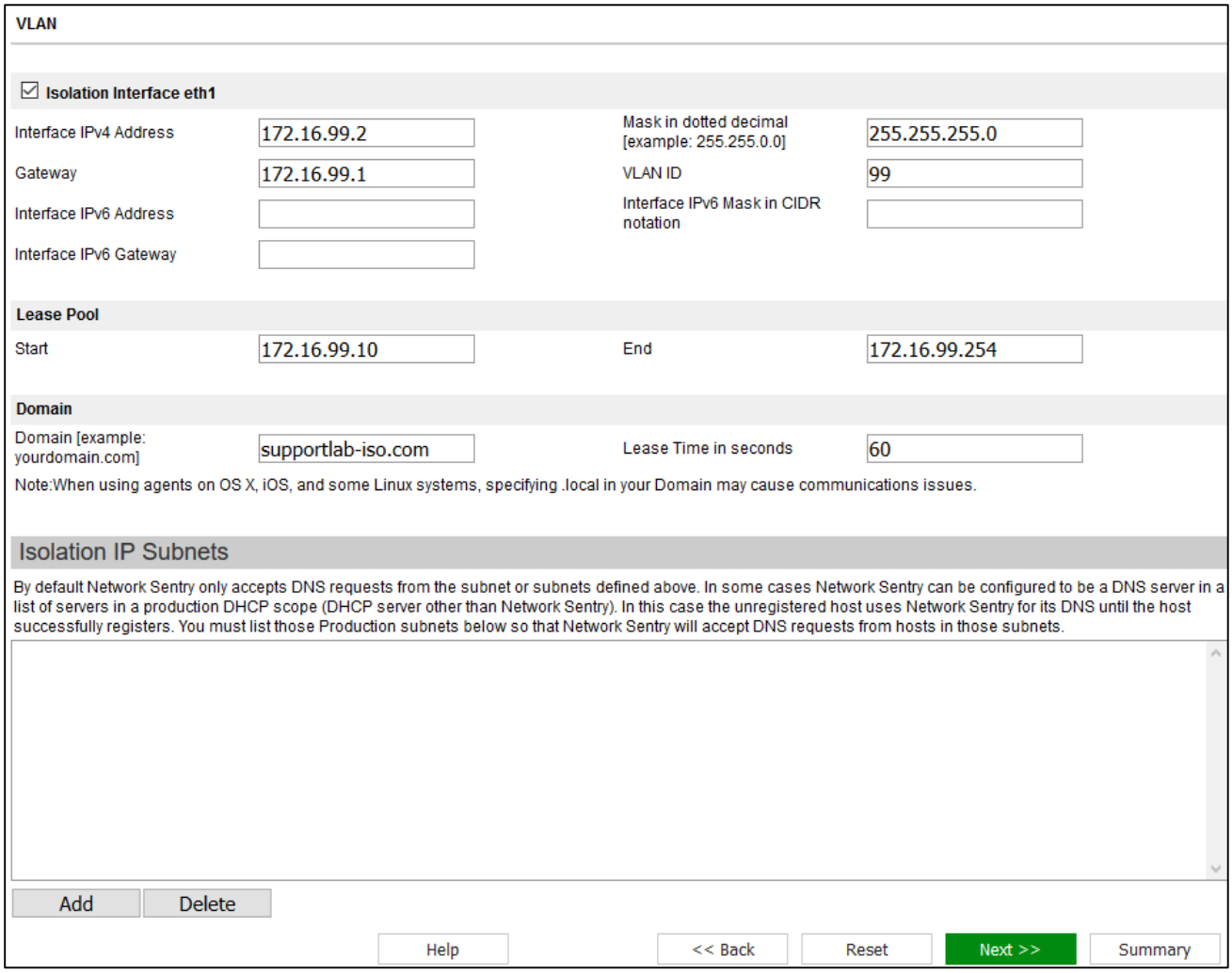
Layer 2 VLAN Types

VLAN Type	Definition
Layer 2 Isolation	Isolates all clients connecting to the network and redirects them to the appropriate isolation web pages. In the Isolation VLAN the state of the client, such as known vs. unknown or out-of-compliance, determines the access control information presented to the client via the web browser or persistent agent. If you use this VLAN type, the configuration of the other VLAN types is optional. You can use the Isolation VLAN with Registration, Remediation, Dead End, VPN, Authentication, or Access Point Management VLANs as another restrictive network.
Layer 2 Registration	Isolates unregistered clients from the production network during client registration.
Layer 2 Remediation	Isolates clients from the production network who pose a security risk because they failed a policy scan.
Layer 2 Dead End	Isolates disabled clients with limited or no network connectivity from the production network.
Layer 2 Virtual Private Network (VPN)	Used for clients who connect to the network through VPN services.
Layer 2 Authentication	Isolates registered clients from the Production network during user authentication.
Layer 2 Access Point Management	Used for clients that connect through devices managed by Access Point Management. Manage clients connected to hubs or simple access points by using DHCP as a means to control or restrict client access. See section Access point management of the Administration Guide in the Fortinet Document Library for additional configuration instructions.

Click on the applicable link below to configure the desired VLAN Type.
"Isolation" VLANs (Isolation, Registration, Remediation, Dead End, VPN, Authentication)
Access point Management VLANs

Configure "Isolation" VLANS

The configuration views for the Isolation, Registration, Remediation, Dead End, VPN, Authentication and VLAN types are similar. Sample of the Isolation view is shown below.



For each VLAN type to be configured:

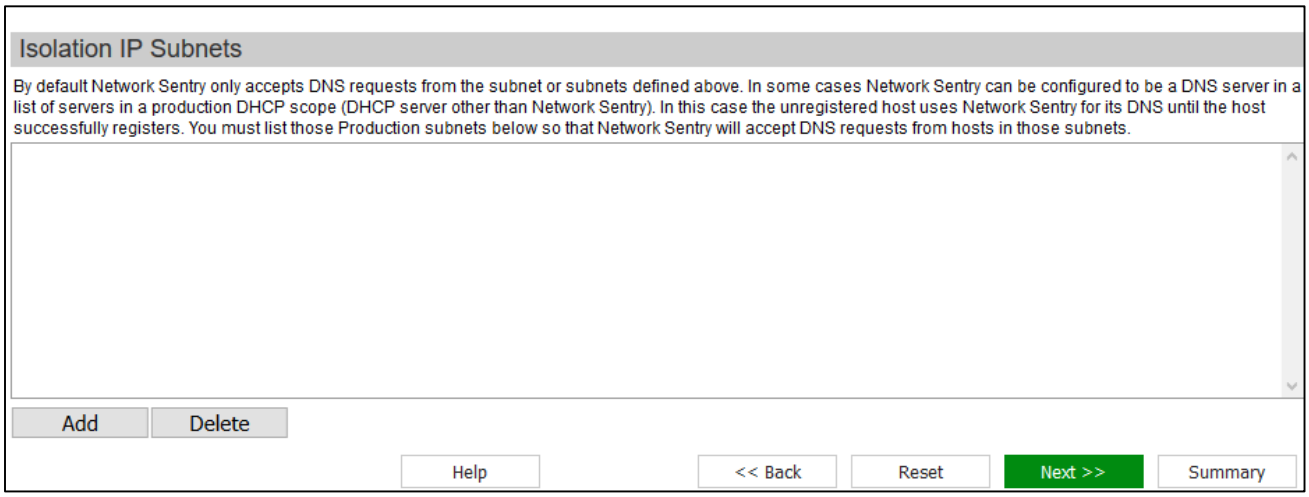
1. Click **Next** to proceed to the next configuration screen if not configuring the displayed VLAN type.
2. To configure the VLAN type displayed, select the **check box** next to the VLAN type, such as Isolation or Registration, and enter the required information. See the table below for field definitions.
3. Once all fields are populated as required, click **Next** to proceed to the next interface. If configuration is complete, click **Summary**.

VLAN Isolation Network Field Definitions

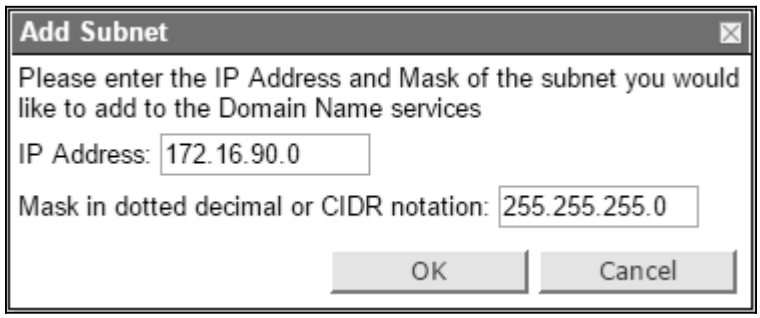
Interface IPv4 Address	IP4 address for the VLAN interface on eth1. Use a different IP for each VLAN you configure.
Mask	Subnet mask.
Gateway	Gateway for eth1 when clients connect through this VLAN.
VLAN ID	Number used to identify this VLAN throughout the system. This number is used within FortiNAC when modeling switch configurations and when setting up Network Access VLANS.
Interface IPv6 Address	IPv6 address for the VLAN interface on eth1. Use a different IP for each VLAN you configure.
Interface IPv6 Mask in CIDR notation	Subnet IPv6 mask for the VLAN interface in CIDR notation format (e.g., 64).
Interface IPv6 Gateway	IPv6 Gateway for the VLAN interface for eth1 when clients connect through this VLAN.
Lease Pool Start	Starting IP address that delineate the range of IP addresses available on this VLAN. **Azure VMs**: Leave this field blank. Scope will be configured in the on-premise DHCP server.
Lease Pool End	Ending IP address that delineate the range of IP addresses available on this VLAN. **Azure VMs**: Leave this field blank. Scope will be configured in the on-premise DHCP server.
Domain	Identifies the domain for this range of IP addresses. To help identify the VLAN, incorporate part of the name in the domain. **Note**: • Avoid using a domain already existing in the production network. Otherwise, DNS resolution may not work properly for any names using that production domain that are part of the Allowed Domains List. • If you use agents for OS X, iOS, and some Linux systems, using a .local suffix in Domain fields may cause communications issues. **Example:** Production domain is megatech.com For Isolation VLAN use **megatech-iso.com** For Registration VLAN use **megatech-reg.com**
Lease Time	Time in seconds that an IP address in this domain is available for use. When this time has elapsed the user is served a new IP address. The recommended lease time for Isolation, Registration, Remediation, Authentication, Dead End and VPN is 60 seconds.

Isolation IP Subnets (optional)
By default, FortiNAC only accepts DNS requests from the subnet or subnets defined by the DHCP scope(s). In some cases, it may be desired for FortiNAC to respond to DNS requests from other subnets used for restricted access where FortiNAC is not acting as the DHCP server. Some examples include:

- **Azure virtual appliances**: Specify the "isolation" VLAN address range(s) provided by the on-premise DHCP server.
- FlexCLI,
- Roles only Aruba/Xirrus integration
- FortiGate with directly connected endpoints (see FortiGate Endpoint Management Integration Guide)



To Add Subnets, click the **Add** button in the **Isolation DNS Subnets** section.

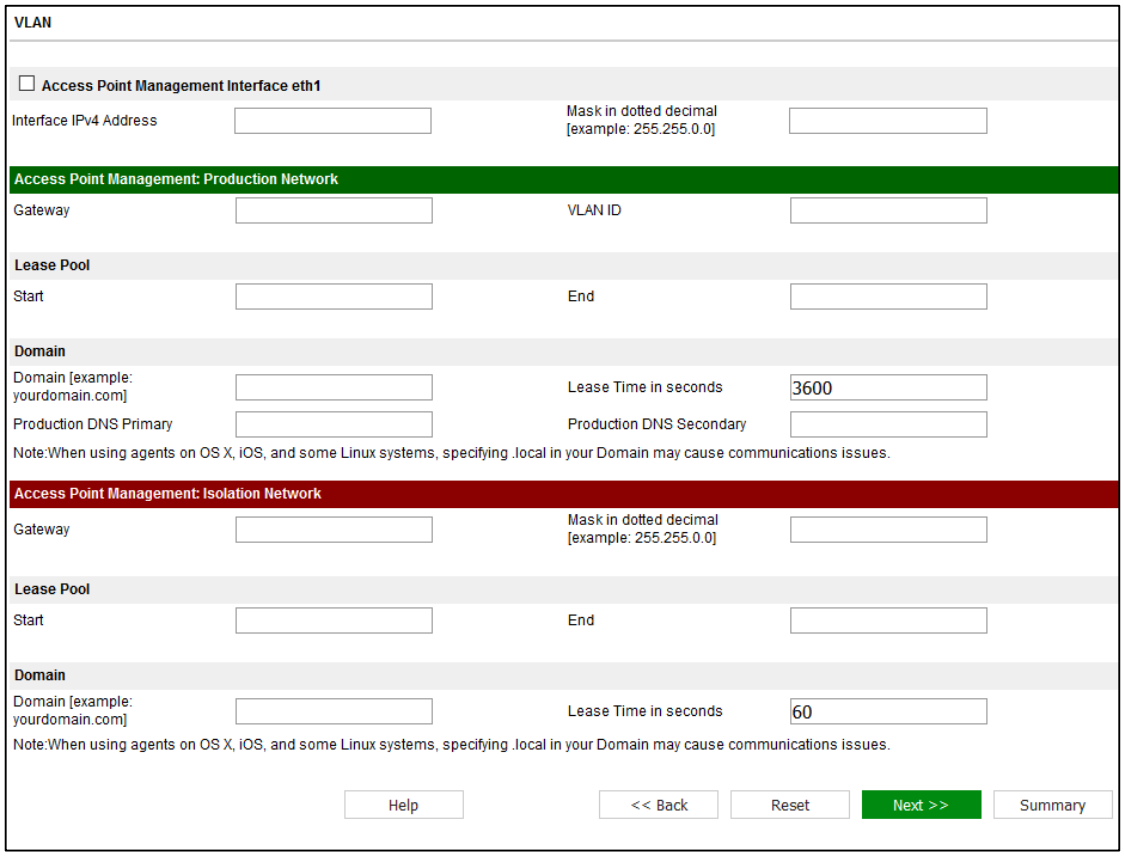


Define the network and mask for which FortiNAC will serve DNS then click **OK**.

Configure Access Point Management VLAN

Access point management provides the ability to manage hosts connected to hubs using DHCP as a means to control or restrict host access. Once configuration of FortiNAC is complete, see section **Access point management** of the **Administration Guide** in the Fortinet Document Library for additional configuration instructions.

The Access Point Management VLAN configuration view is slightly different in that it contains sections for both authorized and unauthorized clients. A sample of the Access Point Management view is shown below.



Layer 2 Access Point Management

Layer 2 Access Point Management Field Definitions

Interface IPv4 Address	IP address for the VLAN interface on eth1. This VLAN is used when more than one MAC address is detected on a single port. Typically occurs when network users connect to a hub or an unmanaged router.
Mask	Subnet mask.
Production Network Gateway	Gateway for eth1 when clients connect through this VLAN using the IP addresses defined for the Production Network.
Production Network VLAN ID	Number used to identify this VLAN throughout the system. This number is used by FortiNAC. Network users in this VLAN are divided into authenticated users and unauthenticated users: • Authenticated users can access the production network using a range of specified IP addresses. • Unauthenticated users are isolated from the production network based on a separate range of IP addresses. However, all users remain in the same VLAN.
Production Network Lease Pool Start	Starting IP address that delineate the range of IP addresses available on this VLAN.
Production Network Lease Pool End	Ending IP address that delineate the range of IP addresses available on this VLAN.
Production Network Domain	Identifies the domain for the range of IP addresses assigned to authenticated hosts. To help identify the VLAN, incorporate part of the name in the domain. **Note:** • Avoid using a domain already existing in the production network. Otherwise, DNS resolution may not work properly for any names using that production domain that are part of the Allowed Domains List. • If you use agents for OS X, iOS, and some Linux systems, using a .local suffix in Domain fields may cause communications issues. **Example:** Production domain is megatech.com Use **apm-prod.megatech.com**
Production Network Lease Time	Time in seconds that an IP address in this domain is available for use. When this time has elapsed the user is served a new IP address. The recommended lease time for Access Point Management/Production is 3600 seconds.
Production DNS Primary	IP address of the Primary DNS Server used in the production network.
Production DNS Secondary	IP address of the Secondary DNS Server used in the production network.
Isolation Network Gateway	Gateway for eth1 when clients connect through this VLAN using the IP addresses defined for the Isolation Network.
Isolation Network Lease Pool Start	Starting IP address that delineate the range of IP addresses available on this VLAN.
Isolation Network Lease Pool End	Ending IP address that delineate the range of IP addresses available on this VLAN.

Isolation Network Domain	Identifies the domain for the range of IP addresses assigned to unauthenticated hosts. To help identify the VLAN, incorporate part of the name in the domain. **Note:** • Avoid using a domain already existing in the production network. Otherwise, DNS resolution may not work properly for any names using that production domain that are part of the Allowed Domains List. • If you use agents for OS X, iOS, and some Linux systems, using a .local suffix in Domain fields may cause communications issues **Example:** Production domain is megatech.com Use **apm-iso.megatech.com**
Isolation Network Lease Time	Time in seconds that an IP address in this domain is available for use. When this time has elapsed the user is served a new IP address. The recommended lease time for Access Point Management/Isolation is 60.

Layer 2 Summary

1. Review the data on the Summary View to confirm the configured settings.

   Important: Confirm the check boxes for the required VLANs are selected. If they have not been selected, click the **Back** button to move through the configuration screens and select the check box(es) needed. Click **Next** to return to the Summary view.

2. Click **Apply**. The Configuration Wizard writes the data to the files on the appliances. This process may take several minutes to complete. When completed, the Results page appears. See Results: Layer 2/Layer3 Networks.

SUMMARY

Configuring: FortiNAC-CA

FortiNAC-CA			
Host Name	hercules		
eth0 IP Address	10.12.240.7	Mask in dotted decimal [example: 255.255.0.0]	255.255.255.0
Default Gateway	10.12.240.2		
eth0 IPv6 Address		IPv6 Mask in CIDR notation	
IPv6 Default Gateway			
DNS			
Primary IP Address	10.12.240.10	Secondary IP Address	208.91.112.53
Domain [example: yourdomain.com]	supportlab.fortinac.com		
Forwarding DNS for all Isolation Networks			
Use Primary and Secondary DNS			
NTP and Time Zone			
NTP Server [example: pool.ntp.org]	pool.ntp.org		
Time Zone	America/New_York		
☑ **Isolation**			
Interface IPv4 Address	172.16.99.2	Mask in dotted decimal [example: 255.255.0.0]	255.255.255.0
Gateway	172.16.99.1	VLAN ID	99
Interface IPv6 Address		IPv6 Mask in CIDR notation	
IPv6 Gateway			
Isolation Lease Pool			
Start	172.16.99.10	End	172.16.99.254
Isolation Domain			
Domain [example: yourdomain.com]	supportlab-iso.com	Lease Time in seconds	60
Isolation IP Subnets			
☐ **Registration**			
☐ **Remediation**			
☐ **Dead End**			
☐ **Virtual Private Network**			
☐ **Authentication**			
☐ **Access Point Management**			
Additional Routes			
None			

Help << Back Apply

Summary Of Layer 2 Network VLAN Configuration

Layer 3 Network

Traffic in the "isolation" VLANs are routed to the FortiNAC eth1 interface. IP Helpers are configured on the routers to forward DHCP traffic from the "isolation" VLANs to the FortiNAC eth1 interface.

Route Scopes

Multiple scopes are allowed for each isolation state (Registration, Remediation, Dead End, VPN, Authentication, Isolation, and Access Point Management). Within these scopes, multiple ranges in the lease pool are also permitted. In addition, you can add static routes. See **Layer 3 Network - Additional Routes**.

Note: When setting up Layer 3 Network Configurations in the Configuration Wizard, labels of DHCP Scopes should not begin with any of these strings: "REG_", "REM_", "AUTH_", "DE_", "ISOL_", "VPN_", or "HUB_". These are reserved.

Layer 3 Route Scopes

Route Scopes	Definition
Layer 3 Isolation	Isolates all clients connecting to the network and redirects them to the appropriate isolation web pages. In the Isolation route scope the state of the client, such as known vs. unknown or out-of-compliance, determines the access control information presented to the client via the web browser or persistent agent. If you use these scopes, configuring the other scopes (Registration, Remediation, Dead End, VPN, Authentication, or Access Point Management) is optional. You can use the Isolation scope with these scopes for other non-production network access.
Layer 3 Registration	Isolates unregistered clients from the production network during client registration.
Layer 3 Remediation	Isolates clients from the production network who pose a potential threat after a failed policy scan.
Layer 3 Dead End	Isolates disabled clients with limited or no network connectivity from the production network.
Layer 3 Virtual Private Network	Used for clients who connect to the network through VPN services.
Layer 3 Authentication	Isolates registered clients from the Production network during user authentication.
Layer 3 Access Point Management	Used for clients that connect through devices managed by Access Point Management. You can manage clients connected to hubs or simple access points by using DHCP as a means to control or restrict client access. Once you have completed your configuration and started FortiNAC, access Help for additional information about the Access Point Management Plugin.

Configure Route Scopes

The configuration views for the Isolation, Registration, Remediation, Dead End, VPN and Authentication scopes are similar. The Access Point Management scopes configuration view contains sections for both Production (authenticated) and Isolation (unauthenticated) clients. Sample Isolation and Access Point Management views are shown below.

For each set of route scopes being configured:

1. Click **Next** to proceed to the next configuration screen if you are not configuring the displayed type or select the type from the left-hand navigation pane.
2. To configure the route scopes displayed, select the **check box** next to the name, such as Isolation or Registration, and enter the required information. See the table below for definitions of the fields.
3. Click **Add** to add scopes or **Modify** to change existing scope information for this route.
4. Enter the Label, Gateway, and Mask.
5. In the **Lease Pools** section, click **Add** to add the lease pool information for the scope.

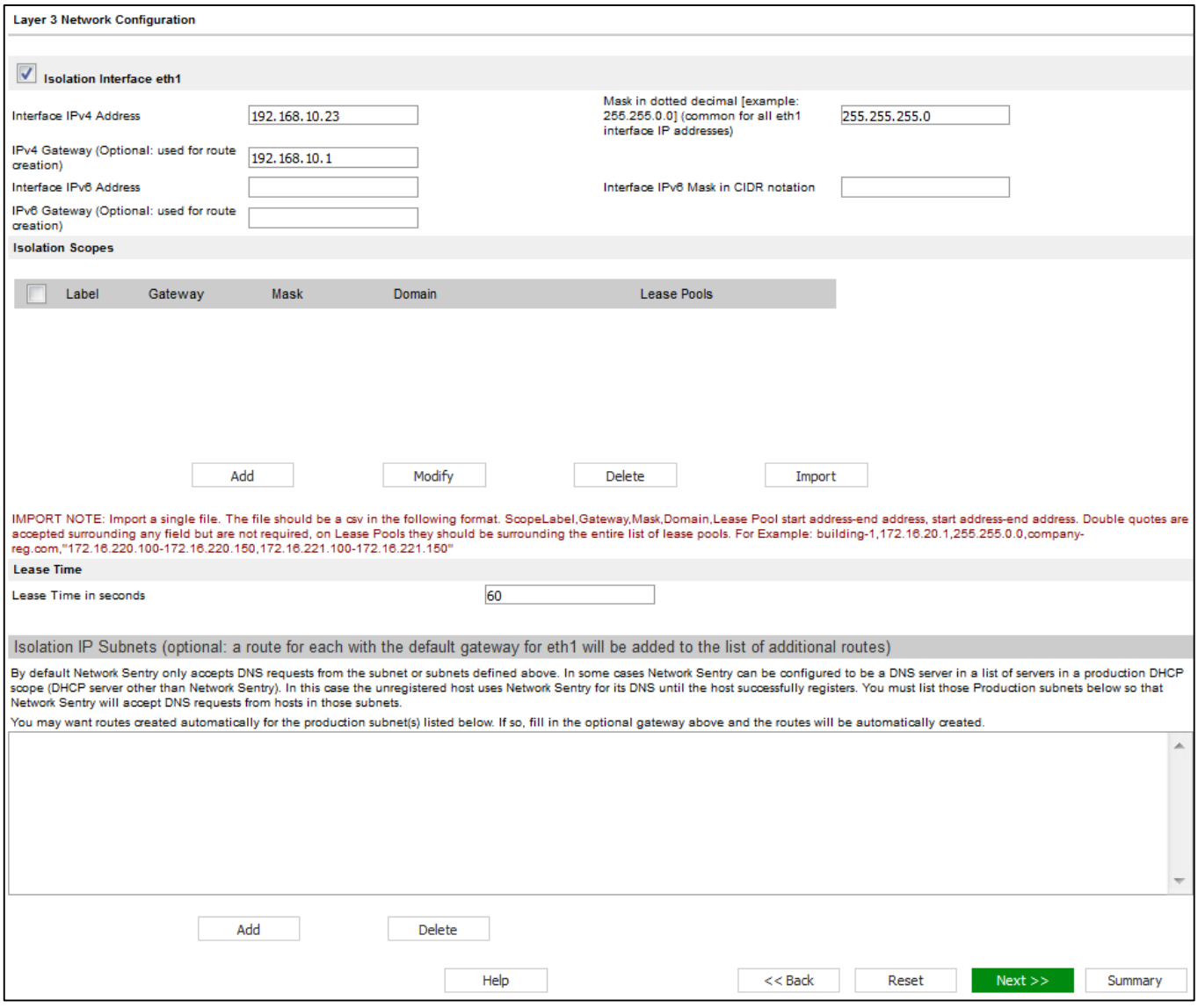
   Azure VMs: *Do not* add lease pools. They will be configured in the on-premise DHCP server.
6. Enter the IP Addresses for **Start** and **End** of the lease pool range, then click **Add**.
7. Repeat steps 3 through 6 to create additional scopes and lease pools.
8. In the Isolation IP Subnets section, enter the list of IP Addresses and corresponding Subnet Masks indicating IP addresses for which FortiNAC will serve DNS.
9. For the **Access Point Management** scopes, enter the Interface IP Address and Mask.
10. Enter the Access Point Management Scopes and Lease Pool information. Add or modify scopes and associated lease pools.
11. Enter the **Domain** information in both the **Production** and **Isolation** sections.
12. Click **Next** when finished.

Layer 3 Isolation Field Definitions

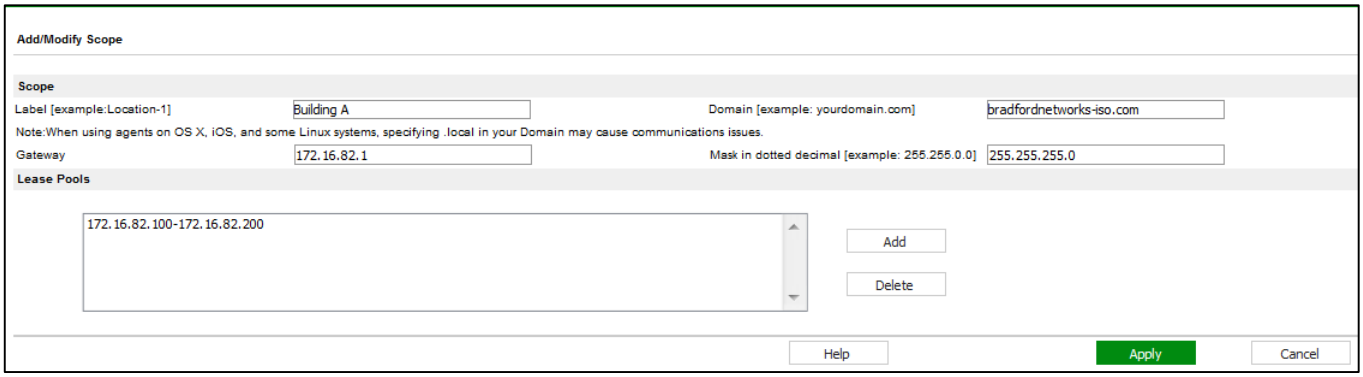
Field	Definition
Route Scope Interface eth1	
Interface IP Address	IP address for the Route Scope interface on eth1. Use a different IP for each route scope type you configure.
Mask	The subnet mask for the interface IP address. Note that the mask is shared between route scope types. If you modify the mask in one route scope, it changes in all others.

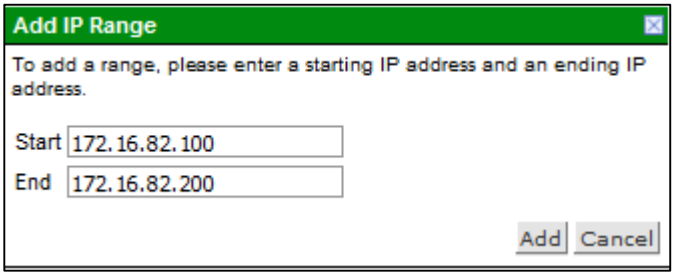
Field	Definition
Gateway	This field is optional and does not need to be configured if the appliance and all of the managed devices are on the same subnet. If the appliance and any managed devices are on different subnets, enter the IP address of the routing device. A gateway is the device that passes traffic from the local subnet to devices on other subnets. **Note:** Routes are automatically created for each Isolation Subnet to the Isolation Gateway. Routes traffic through eth1.
Isolation Scopes	
Label	User specified name for the scope. Can be associated with a location, such as Building-B, or a function within the organization, such as Accounting. Note: When setting up Layer 3 Network Configurations in the Configuration Wizard, labels of DHCP Scopes should not begin with any of these strings: "REG_", "REM_", "AUTH_", "DE_", "ISOL_", "VPN_", or "HUB_". These are reserved.
Gateway	Default gateway for the client lease pool you are adding. Do not use the default gateway for eth1.
Mask	Subnet mask for the default gateway.
Domain	Identifies the domain for this range of IP addresses. To help identify the network, incorporate part of the name in the domain. **Note:** • Avoid using a domain already existing in the production network. Otherwise, DNS resolution may not work properly for any names using that production domain that are part of the Allowed Domains List. • If you use agents for OS X, iOS, and some Linux systems, using a .local suffix in Domain fields may cause communications issues. **Example:** Production domain is megatech.com For Isolation VLAN use **megatech-iso.com** For Registration VLAN use **megatech-reg.com**
Lease Pools	Starting and ending IP addresses that delineate the range of IP addresses available on this route. You can use multiple ranges.
Lease Time	
Lease Time in seconds	Time in seconds that an IP address is available for use. When this time has elapsed the user is served a new IP address. The recommended lease time for Isolation, Registration, Remediation, Dead End, VPN and Authentication is 60 seconds.

Isolation IP Subnets	
Subnets	IP Subnets are optional and used in situations like Client control via FlexCLI or roles only Aruba/Xirrus integration. List of IP Addresses and corresponding Subnet Masks indicating IP addresses for which FortiNAC will serve DNS. Should only be used for hosts that are being isolated by FortiNAC. Can be any address on any subnet, as long as the same address is added to the filters as an isolation address when configuring the device.



Layer 3 Network Configuration - Isolation Scopes





Layer 3 Scopes - Add Lease Pool IP Range

Layer 3 Access Point Management Field Definitions

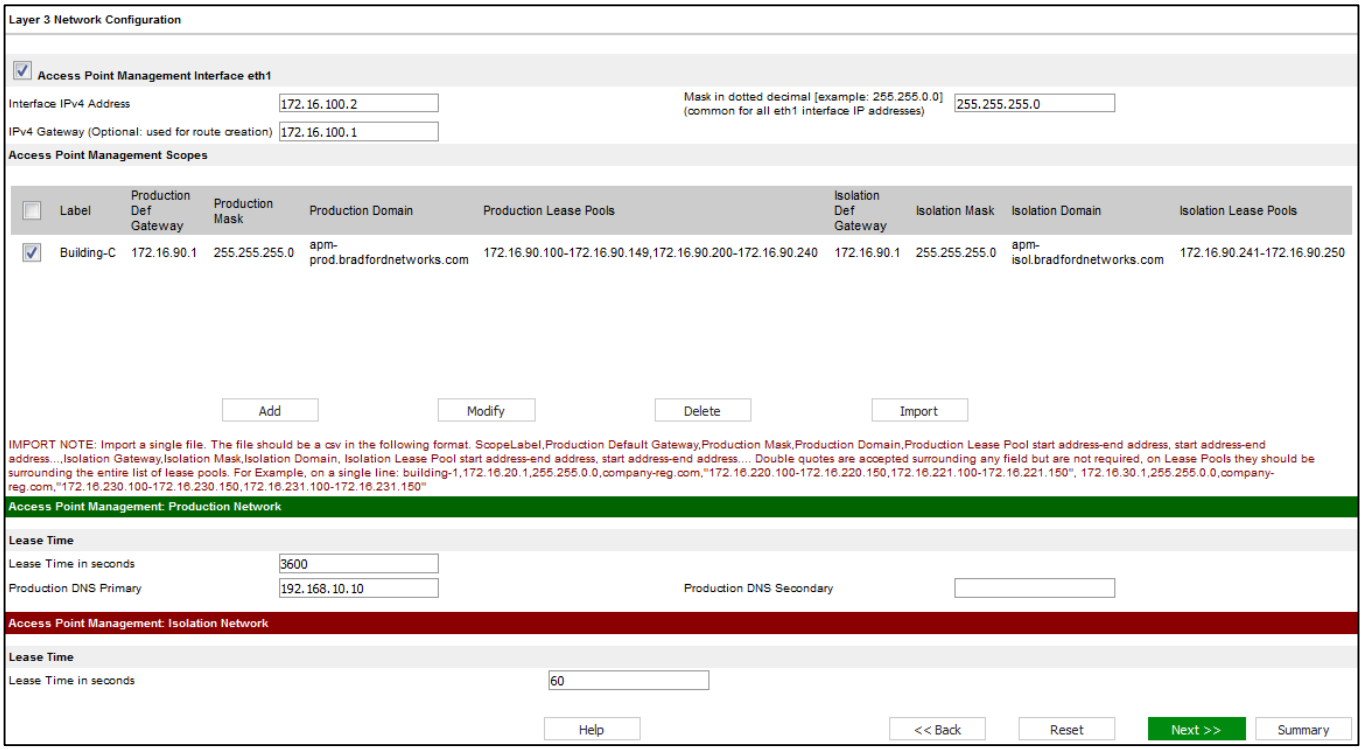
Field	Definition
Access Point Management Interface eth1	
Interface IP Address	IP address for the VLAN interface on eth1. This VLAN is used when more than one MAC address is detected on a single port. Typically occurs when network users connect to a hub or an unmanaged router.

Field	Definition
Mask	Subnet mask.
Access Point Management Scopes	
Label	User specified name for the scope. Can be associated with a location, such as Building-B, or a function within the organization, such as Accounting. **Note:** When setting up Layer 3 Network Configurations in the Configuration Wizard, labels of DHCP Scopes should not begin with any of these strings: "REG_", "REM_", "AUTH_", "DE_", "ISOL_", "VPN_", or "HUB_". These are reserved.
Production Def Gateway	Default gateway for the client lease pool you are adding. Do not use the default gateway for eth1.
Production Mask	Subnet mask for Production IP addresses.
Production Domain	Identifies the domain for the range of IP addresses assigned to authenticated hosts. To help identify the network, incorporate part of the name in the domain. **Note**: • Avoid using a domain already existing in the production network. Otherwise, DNS resolution may not work properly for any names using that production domain that are part of the Allowed Domains List. • If you use agents for OS X, iOS, and some Linux systems, using a .local suffix in Domain fields may cause communications issues. **Example**: Production domain is megatech.com Use **apm-prod.megatech.com**
Production Lease Pools	Starting and ending IP addresses that delineate the range of IP addresses available for authenticated users in this scope.
Isolation Def Gateway	Default gateway for eth1 when connecting through this scope using the IP addresses defined for the Isolation Network.
Isolation Mask	Subnet mask for Production IP addresses.

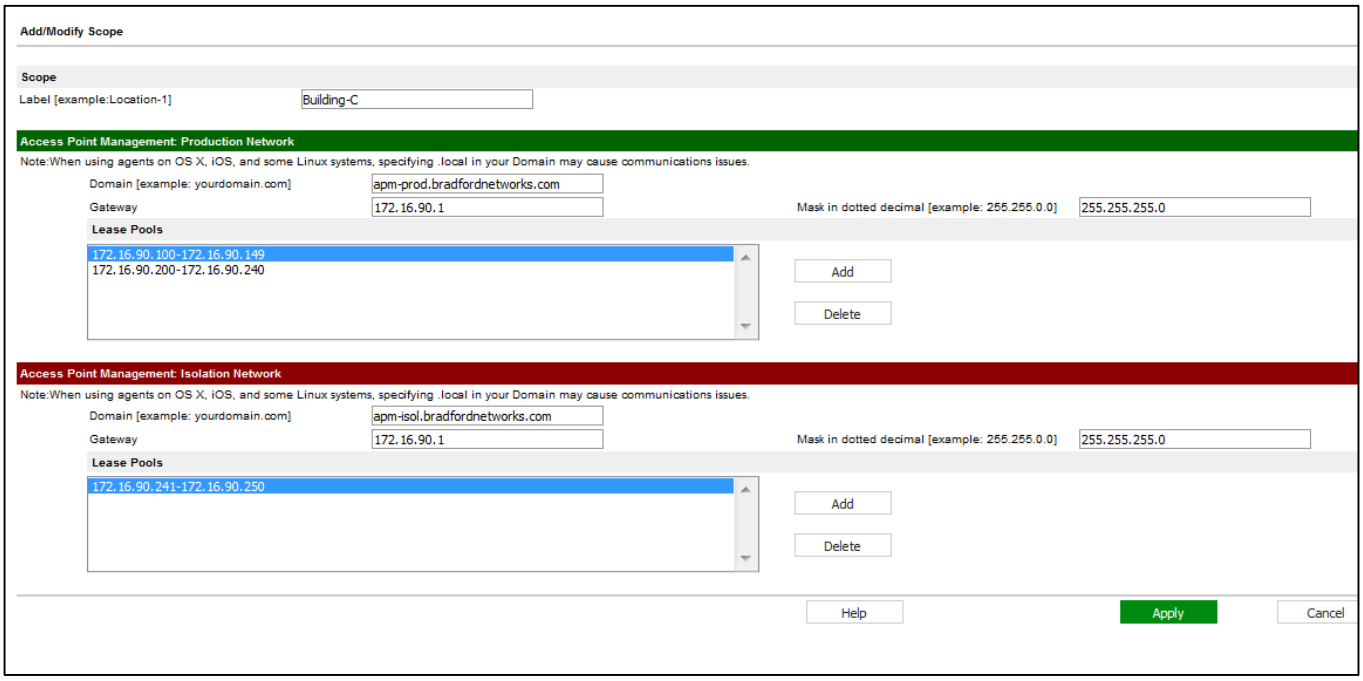
Isolation Domain	Identifies the domain for the range of IP addresses assigned to unauthenticated hosts. To help identify the network, incorporate part of the name in the domain. **Note:** • Avoid using a domain already existing in the production network. Otherwise, DNS resolution may not work properly for any names using that production domain that are part of the Allowed Domains List. • If you use agents for OS X, iOS, and some Linux systems, using a .local suffix in Domain fields may cause communications issues **Example:** Production domain is megatech.com Use **apm-iso.megatech.com**
Isolation Lease Pools	Starting and ending IP addresses that delineate the range of IP addresses available for unauthenticated users in this scope.

Access Point Management: Production Network Scopes

Field	Definition
Lease Time	Time in seconds that an IP address in this domain is available for use. When this time has elapsed the user is served a new IP address. The recommended lease time for Access Point Management/Production is 3600 seconds.
Production DNS Primary	IP address of the Primary DNS Server.
Production DNS Secondary	IP address of the Secondary DNS Server.
Access Point Management: Isolation Network Scopes	
Lease Time In Seconds	Time in seconds that an IP address in this domain is available for use. When this time has elapsed the user is served a new IP address. The recommended lease time for Access Point Management/Isolation is 60.



Layer 3 Access Point Management



Layer 3 Add Access Point Management Scopes

Importing DHCP Scopes

To import DHCP scopes from a csv file, use one of the following formats:

Single Route Format

```
ScopeLabel,Default Gateway,Mask,Domain,Lease Pool "start
address-end address,start address-end address"
```

Access Point Management Route Format

```
ScopeLabel,Production Default Gateway,Production
Mask,Production Domain,Production Lease Pool "start address-
end address,start address-end address",Isolation Default
Gateway,Isolation Mask,Isolation Domain,Isolation Lease Pool
"start address-end address, start address-end address"
```

Double quotes are accepted surrounding any field but are not required. On Lease Pools quotes should surround the entire list of lease pools.

ScopeLabel Field Requirements:

- Must be unique for each route scope imported. If it is not unique, the record with the first instance of the ScopeLabel field is duplicated for each subsequent instance of the identical ScopeLabel.
- Should not begin with any of these strings: "REG_", "REM_", "AUTH_", "DE_", "ISOL_", "VPN_", or "HUB_". These are reserved.
- Should not contain spaces

Single Route Scope Example

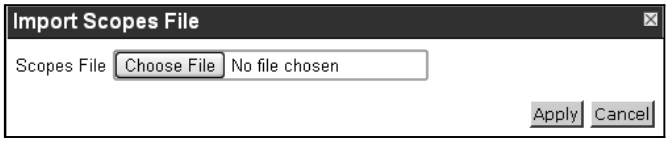
```
building-1,172.16.220.1,255.255.255.0,company-
reg.com,"172.16.220.100-172.16.220.150,172.16.220.200-
172.16.220.250"
```

Access Point Management Route Scope Example

```
building-1,172.16.220.1,255.255.255.0,company-apm-
prod.com,"172.16.220.100-172.16.220.150, 172.16.220.200-
172.16.220.250",172.16.220.1,255.255.255.0,company-apm-
isol.com,"172.16.220.151-172.16.220.175"
```

For each scope you are configuring:

1. Navigate to the scope window, for example, Isolation.
2. Click **Import**.
3. On the **Import Scopes File** window browse to the csv file and click **Apply**.



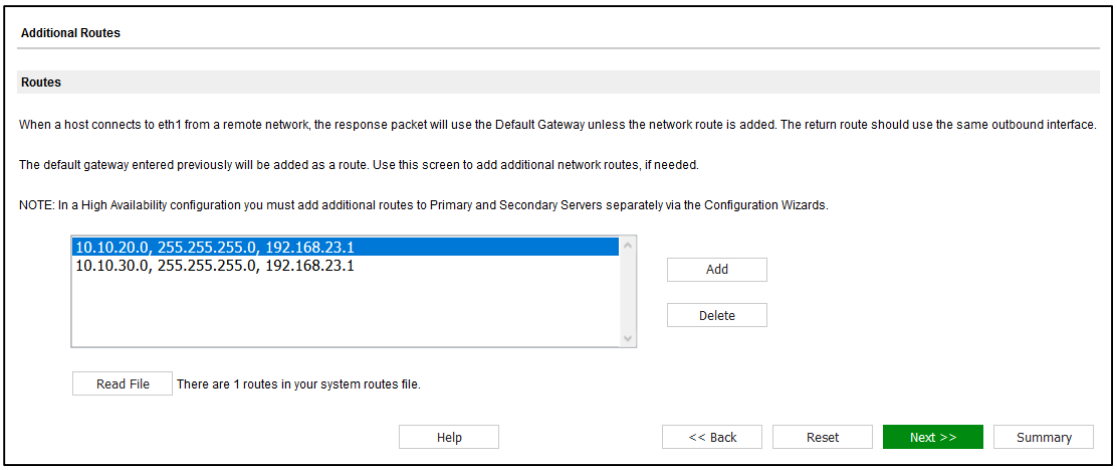
Layer 3 Routes - Import Route Scopes Window

Additional Routes

When a client connects on eth1 from a remote network, the return packet uses the eth0 Default Gateway unless a network route is added. It is recommended to configure the network so that outbound and inbound routing uses the same interface, such as eth1.

As isolation network DHCP scopes are configured, static routes are automatically created for those networks, specifying the gateway for the corresponding eth1 interface or sub-interface. The following example displays static routes automatically configured for DHCP scopes created under the Isolation eth1 interface with gateway 192.168.23.1

There may be routes in the system routes file that were not entered in the Configuration Wizard.



Additional Routes Window

Important:

- If the system routes file is imported, they overwrite any existing routes in the Additional Routes view.
- If routes are entered in the Additional Routes view and saved, these routes overwrite previous routes.
- If there are no routes in the Additional Routes view and you save, *all routes are erased* from the system routes file except for the Default Gateway.
- In a High Availability environment, additional routes must be added to both the Primary and Secondary servers.

To import system routes, click the **Read File** button on the Additional Routes window in the Configuration Wizard. The number of routes in the system routes file is listed next to the button.

For each route you are configuring:

1. On the **Additional Routes** screen click **Add**.
2. Enter the Network IP Address, Mask, and Gateway, then click **Add**.

Example:

When eth1 IP is 192.168.10.2 and the eth1 gateway is 192.168.10.1 for DHCP Lease Pool 192.168.110.100-192.168.110.200 add the following route:

Route Setup Field Example	Definition
Network 192.168.110.0	Identifies the network from which packets are coming.
Mask 255.255.255.0	Subnet mask for the network.
Gateway 192.168.10.1	Identifies the gateway for eth1. Do not use the gateway for the network.

3. Repeat step 2 to add additional routes.

Important: The routes you enter into the list on this view are written to the system routes file when you click Apply on the Summary view. If the list is blank, ALL routes in the system routes file with the exception of the Default Gateway are removed from the system routes file.

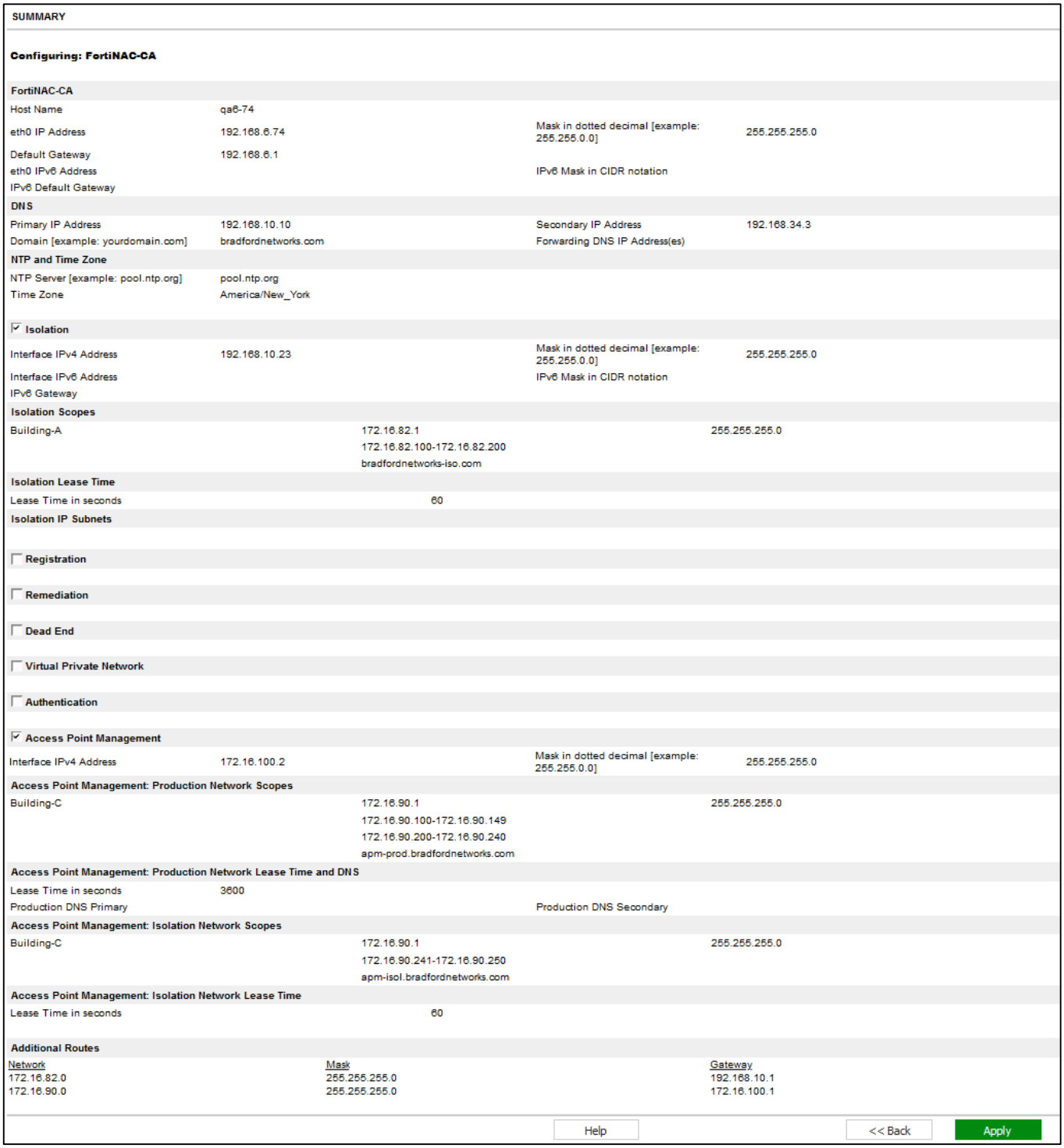
4. Click **Next**.

Layer 3 Summary

1. Review the data on the Summary View to confirm the configured settings.

   Important: Confirm the check boxes for the required networks are selected. If they have not been selected, click the **Back** button to move through the configuration screens and select the check box(es) needed. Click **Next** to return to the Summary view.

2. Click **Apply**. The Configuration Wizard writes the data to the files on the appliances. This process may take several minutes to complete. When completed, the Results page appears. See Results: Layer 2/Layer3 Networks.



SUMMARY

Configuring: FortiNAC-CA

FortiNAC-CA			
Host Name	qa6-74		
eth0 IP Address	192.168.6.74	Mask in dotted decimal [example: 255.255.0.0]	255.255.255.0
Default Gateway	192.168.6.1		
eth0 IPv6 Address		IPv6 Mask in CIDR notation	
IPv6 Default Gateway			
DNS			
Primary IP Address	192.168.10.10	Secondary IP Address	192.168.34.3
Domain [example: yourdomain.com]	bradfordnetworks.com	Forwarding DNS IP Address(es)	
NTP and Time Zone			
NTP Server [example: pool.ntp.org]	pool.ntp.org		
Time Zone	America/New_York		
☑ **Isolation**			
Interface IPv4 Address	192.168.10.23	Mask in dotted decimal [example: 255.255.0.0]	255.255.255.0
Interface IPv6 Address		IPv6 Mask in CIDR notation	
IPv6 Gateway			
Isolation Scopes			
Building-A	172.16.82.1 172.16.82.100-172.16.82.200 bradfordnetworks-iso.com		255.255.255.0
Isolation Lease Time			
Lease Time in seconds	60		
Isolation IP Subnets			
☐ **Registration**			
☐ **Remediation**			
☐ **Dead End**			
☐ **Virtual Private Network**			
☐ **Authentication**			
☑ **Access Point Management**			
Interface IPv4 Address	172.16.100.2	Mask in dotted decimal [example: 255.255.0.0]	255.255.255.0
Access Point Management: Production Network Scopes			
Building-C	172.16.90.1 172.16.90.100-172.16.90.149 172.16.90.200-172.16.90.240 apm-prod.bradfordnetworks.com		255.255.255.0
Access Point Management: Production Network Lease Time and DNS			
Lease Time in seconds	3600		
Production DNS Primary		Production DNS Secondary	
Access Point Management: Isolation Network Scopes			
Building-C	172.16.90.1 172.16.90.241-172.16.90.250 apm-isol.bradfordnetworks.com		255.255.255.0
Access Point Management: Isolation Network Lease Time			
Lease Time in seconds	60		

Additional Routes

Network	Mask	Gateway
172.16.82.0	255.255.255.0	192.168.10.1
172.16.90.0	255.255.255.0	172.16.100.1

Help << Back Apply

Summary

Results: Layer 2/Layer3 Networks

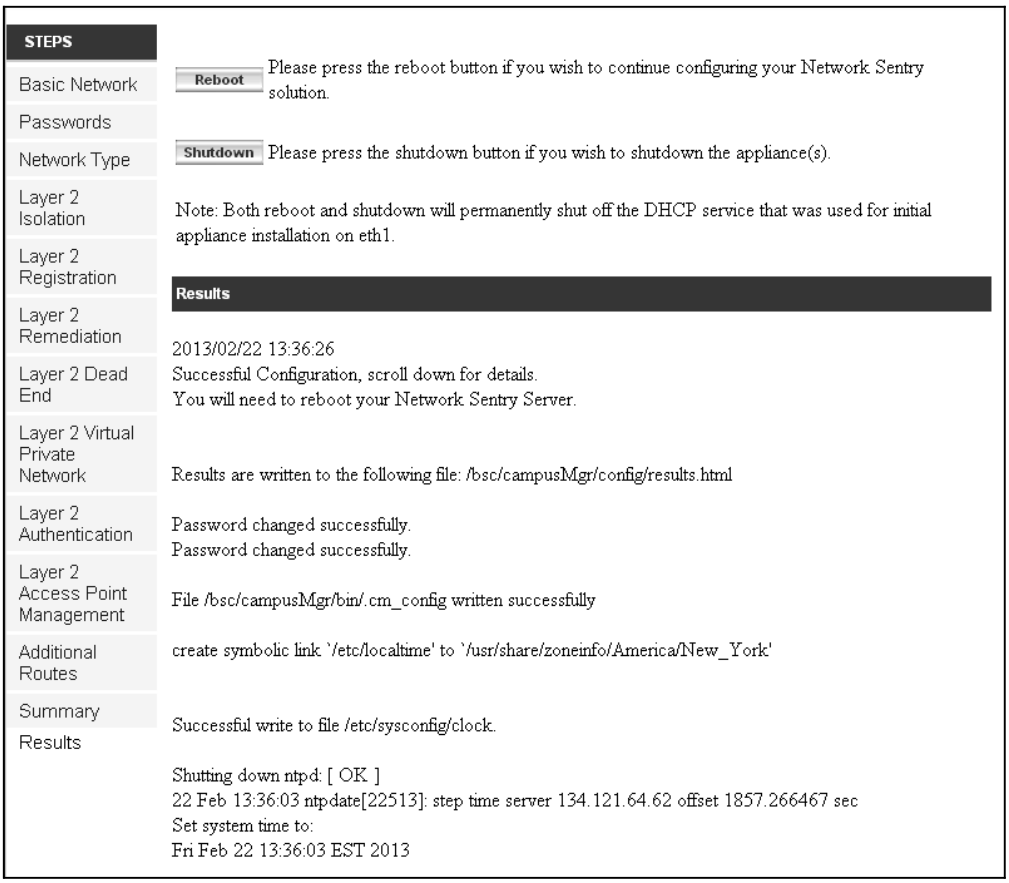
1. Review the Results. Errors are noted at the top of the Results page.
2. Scroll down through the results and note errors or warnings. Make changes and apply them until a successful configuration is written.
3. Click **Reboot** to continue with the installation and begin network modeling and policy creation.

   OR

   Click **Shutdown** to turn off the appliance.

   Physical Appliances: Once the reboot or shutdown is complete, disconnect from the eth1 interface. Configuration Wizard will no longer be accessible from this interface.

   Eth0 can now be connected to the network.



Results Window

Re-run the Configuration Wizard at a later time to continue with configuration of VLANs or adjust previous settings.

If assistance is needed contact FortiNAC Support.

Appliance configuration is now complete. Proceed to the FortiNAC Deployment Guide to continue deployment.

Appendix

CLI Admin User Permissions

View FortiNAC logs
tail -[fF] <filename>
more <filename>
less <filename>

Log Files:
/bsc/logs/output.mom
/bsc/logs/output.master
/bsc/logs/output.nessus
/bsc/logs/output.processManager
/bsc/logs/dhcpd.log
/bsc/logs/named.log
/bsc/logs/tomcat-portal/*
/bsc/logs/tomcat-admin/*

View System information
ifconfig
ip addr
cat /etc/hosts
sysinfo
sysinfo -v (requires sudo pw)

Other Functions
Start and stop services
Shutdown/halt/poweroff/reboot the appliance
View/set date/time
View/execute (sudo) any file in /bsc/campusMgr/bin
View/execute (sudo) any file in /bsc/campusMgr/bin/configWizard
View/execute any file in /bsc/campusMgrUpdates
Execute database backup (/bsc/campusMgr/master_loader/mysql/ydb_dated_backup)

Change Passwords After Configuration

Configuration files are overwritten whenever you run the Configuration Wizard. It is strongly recommended, therefore, that you do not make changes outside of the Configuration Wizard. Making all changes from within the Configuration Wizard prevents you from having custom configuration files that can be accidentally overwritten.

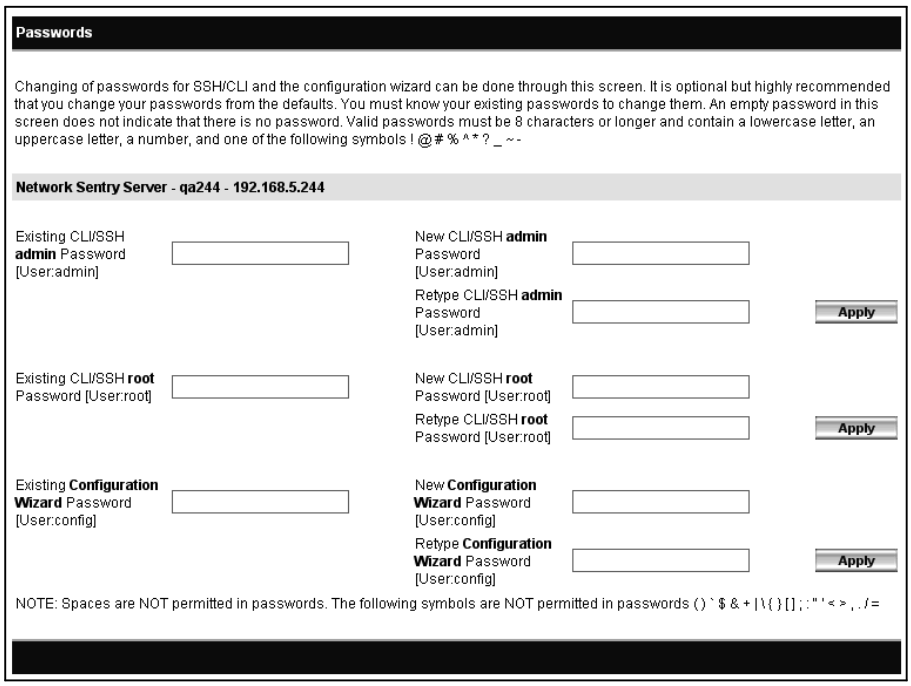
Running the Configuration Wizard to change passwords after the initial setup also causes all configuration files to be overwritten if you use the Next button to scroll through all of the pages. If no manual changes have been made, this does not cause a problem. However, it is recommended that you go directly to the Change Password window without running the entire Configuration Wizard, save the passwords and exit the wizard.

See **Configuration Wizard - Passwords** on page 18 for additional information on modifying your passwords.

To go directly to the Change Passwords window, type one of the following URLs:

`http://<Host Name>:8080/configWizard/PasswordChange.jsp`

`http://<IP  Address>:8080/configWizard/PasswordChange.jsp`



Change Passwords Window

To change passwords:

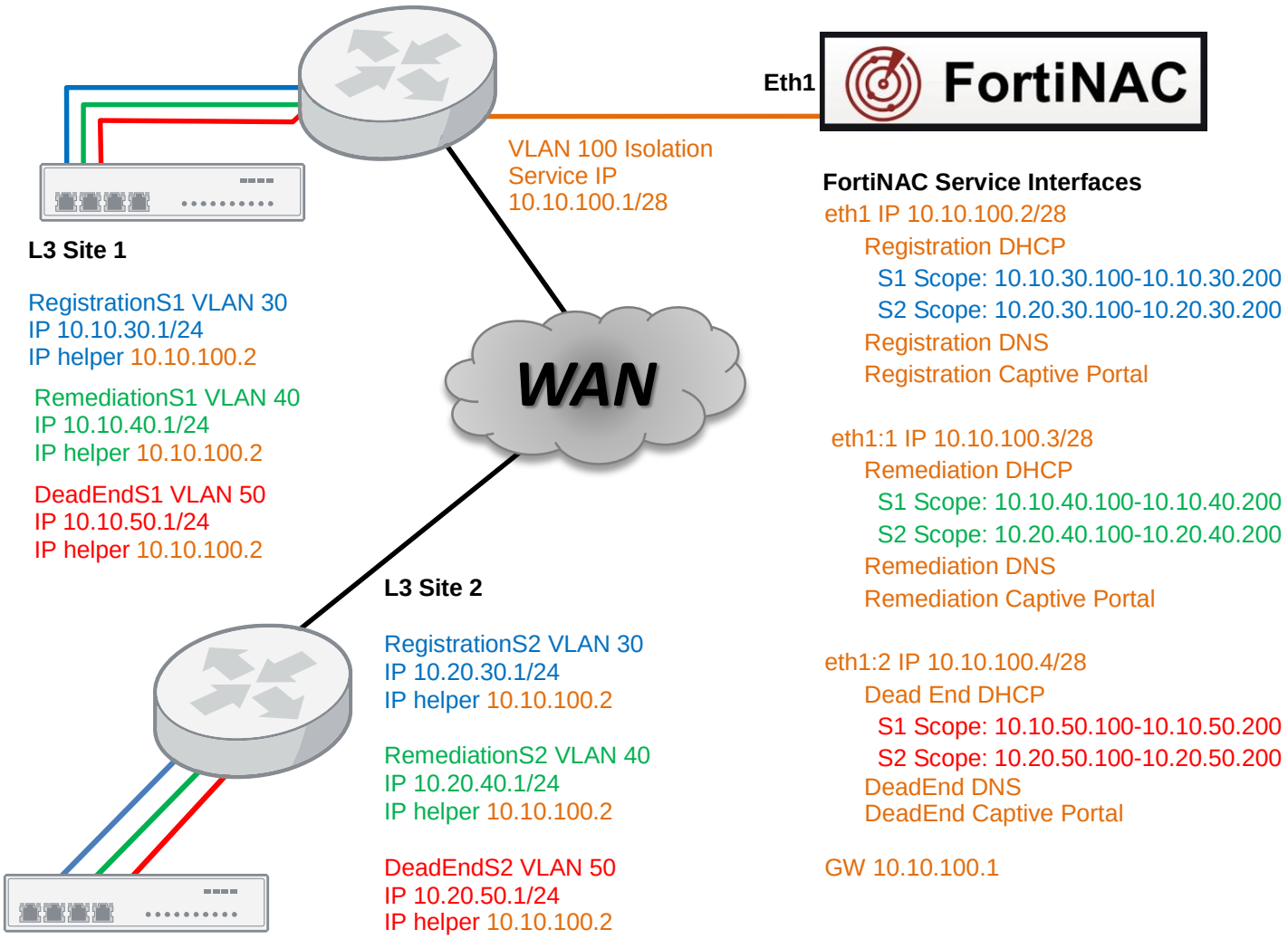
1. For each password that you modify, click in the **Existing Password** field and type the current password.
2. Click in the **New Password** field and type the new password (8 to 64 characters).
3. Click in the **Retype Password** field and enter the new password again.
4. Click **Apply**. Root and admin password changes take effect immediately. The Configuration Wizard password change will not take effect until tomcat-admin has been restarted.
5. You are asked if you would like to restart tomcat-admin. If you are working your way through the Configuration Wizard, do not restart at this time. The system will be restarted at the end of the process. If you are only changing passwords, you should click **OK** to restart.
6. Close the window or tab.

FortiNAC Service Configuration (Network Type)

The FortiNAC Service Interface (Eth1) can be configured for either a Layer 2 or Layer 3 implementation. This configuration is referred to as **Network Type** in the Configuration Wizard. See below for descriptions and logical diagrams for each implementation type. The most common Network Type used by customers is Layer 3.

Layer 3 Implementation

- The FortiNAC Service Interface is a standard interface
  - The interface exists on a single network
  - The interface is not within the same broadcast domain as a host assigned to an isolation network
  - The interface uses multiple IP addresses within the same subnet
  - DHCP relays must be configured on each isolation network pointing back to the isolation interface
  - The individual IP address is used by DNS



Layer 2 Implementation

- The FortiNAC Service Interface
  - 802.1q trunk
  - The interface accepts traffic tagged from any pf the isolation VLANs
  - Same broadcast domain as hosts
  - IP address for each isolation subnet

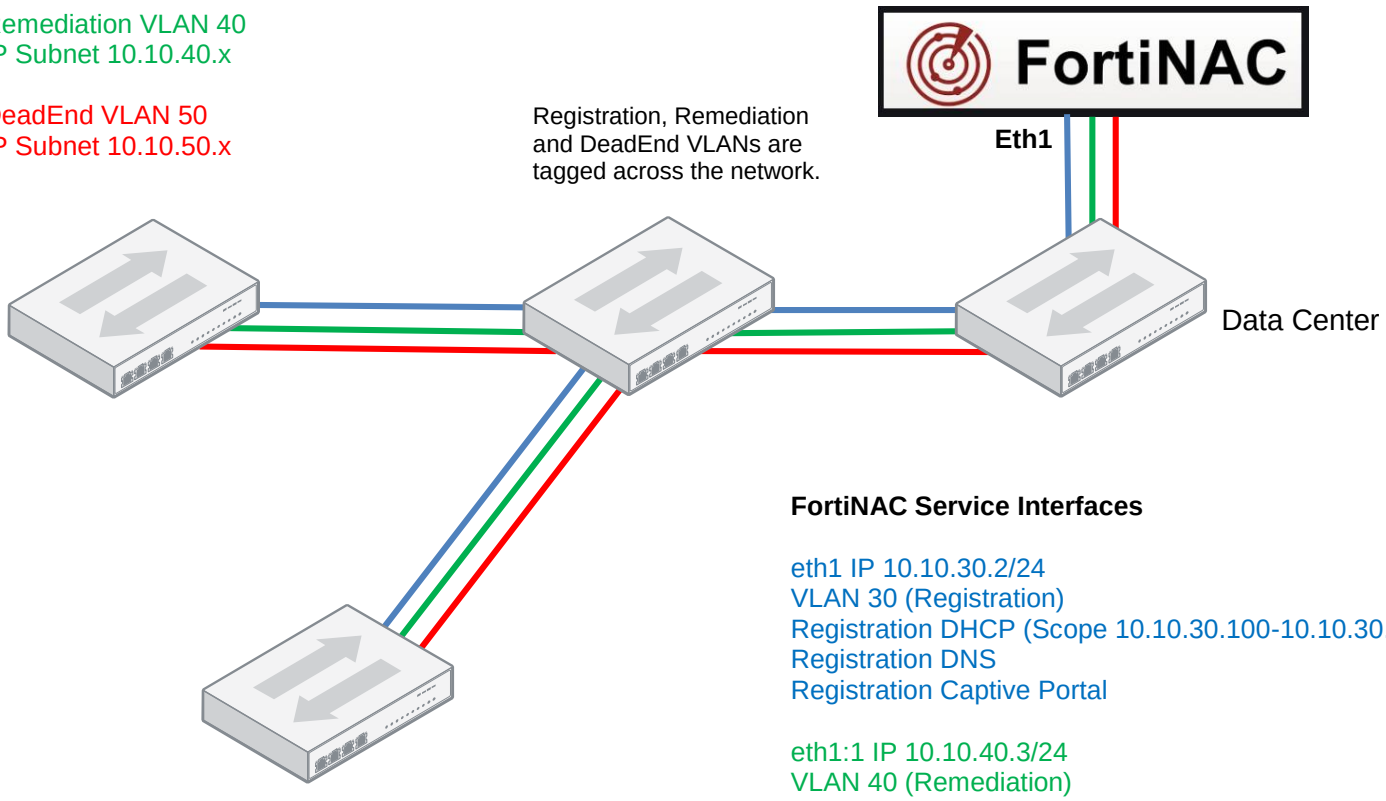
Building 1

Registration VLAN 30
IP Subnet 10.10.30.x

Remediation VLAN 40
IP Subnet 10.10.40.x

DeadEnd VLAN 50
IP Subnet 10.10.50.x

Registration, Remediation and DeadEnd VLANs are tagged across the network.



Building 2

Registration VLAN 30
IP Subnet 10.10.30.x

Remediation VLAN 40
IP Subnet 10.10.40.x

DeadEnd VLAN 50
IP Subnet 10.10.50.x

FortiNAC Service Interfaces

eth1 IP 10.10.30.2/24
VLAN 30 (Registration)
Registration DHCP (Scope 10.10.30.100-10.10.30.200)
Registration DNS
Registration Captive Portal

eth1:1 IP 10.10.40.3/24
VLAN 40 (Remediation)
Remediation DHCP (Scope 10.10.40.100-10.10.40.200)
Remediation DNS
Remediation Captive Portal

eth1:2 IP 10.10.50.4/24
VLAN 50 (DeadEnd)
DeadEnd DHCP (Scope 10.10.50.100-10.10.50.200)
DeadEnd DNS
DeadEnd Captive Portal

FortiNAC “Isolation” VLANs

In the switches to be controlled by FortiNAC, configure the appropriate “isolation” VLANs.

- Registration (Containment for Rogue hosts)
- Remediation (Quarantine: Containment for “At-Risk” hosts)
- Dead End (Containment for disabled hosts)

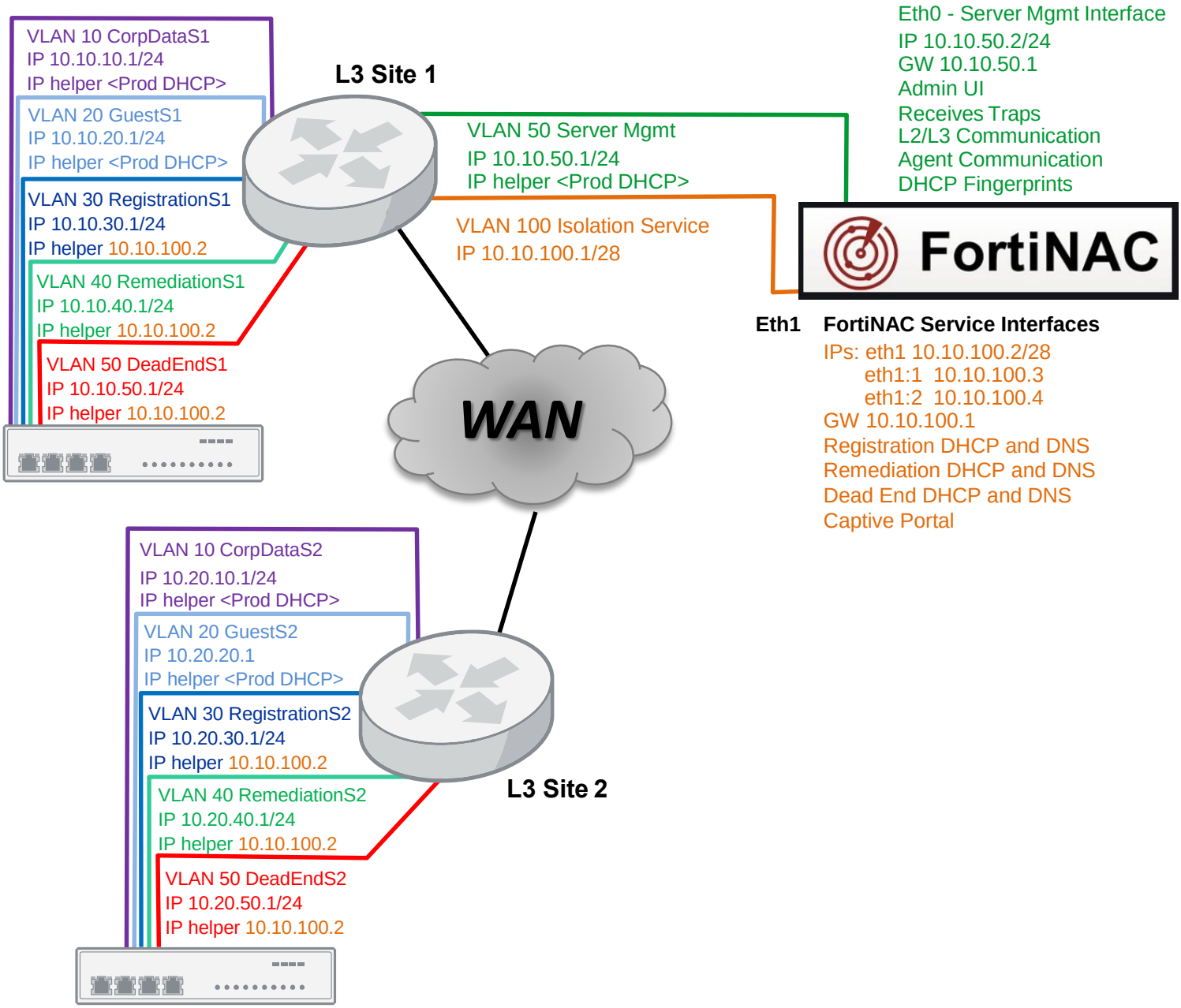
or alternatively

- Isolation (one “isolation” VLAN for all states)

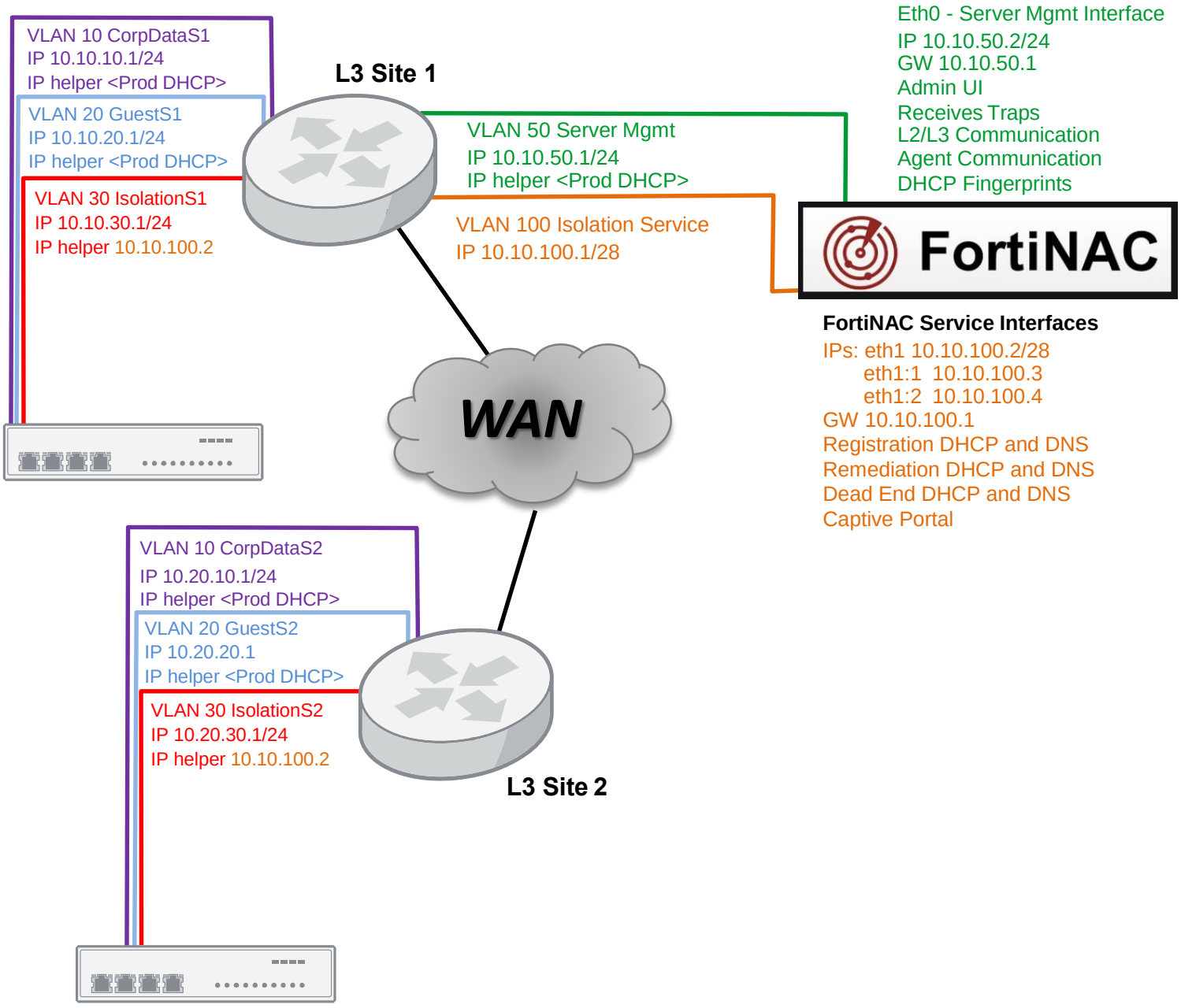
Layer 3 deployments require a VLAN per state per location that is separated by an L3 device.

See following pages for logical network diagram examples.

Multiple FortiNAC "Isolation" Network Configuration
Individual VLANs per State
(L3 Network Type)



Single FortiNAC "Isolation" Network Configuration
Shared VLAN for all States
(L3 Network Type)



High Availability Design Considerations

If appliances will be configured for High Availability, it is important to consider the following before configuring the FortiNAC Service Interface (eth1):

- **Primary and Secondary Servers reside on different networks** (e.g. Data Center and Disaster Recovery (DR) Data Center): Requires Layer 3 network type.
- **Primary and Secondary Servers reside on the same network:** There are no Configuration Wizard restrictions.

For more details regarding this feature, see High Availability in the Fortinet Document Library.

Click here to return to Eth1 configuration instructions.

Access Secondary Server Wizard Post L2 HA Configuration

In order to access Configuration Wizard on the Secondary Server, use the physical IP address/host name of the Secondary Server. In FNAC-CA appliances, the Secondary Server IP address or host name may not respond to HTTP/HTTPS requests by default in a L2 HA configuration with a shared IP address (VIP) configured.

If unable to reach the secondary via HTTP/HTTPS, review the Secondary Server's **/etc/hosts** file. Tomcat-Admin service binds to the address assigned to "nac", making it only accessible from that address. If the /etc/hosts file has the "nac" entry on the same line as the VIP:

```
192.168.8.25    oak.bradfordnetworks.com        oak cm nac
```

Then it will be necessary to modify the file in order to access the Secondary Server.

Note: When Control and Application servers are separate appliances, the "nac" hostname is assigned an IP address of "0.0.0.0" which makes it accessible from any address and any interface. This is not done for CA appliances so devices in the "isolation" network cannot access the Admin UI.

Modifying Hosts file for Secondary Server HTTP/HTTPS Access in L2 HA

1. In the CLI of the Secondary Server, edit **/etc/hosts**.
2. Locate the line containing the "nac" entry. This should be the line with the virtual IP address.
3. Remove "nac" from the line and save.

```
192.168.8.25    oak.bradfordnetworks.com        oak cm
```

4. Restart tomcat-admin service:
   service tomcat-admin restart
5. Connect on the Secondary Server via configWizard using actual eth0 IP.

Note: Once Configuration Wizard has been run, the /etc/hosts file will be restored automatically.