FortiNAC - Configuration Wizard

Version F 7.6.0

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

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

August 26, 2024
FortiNAC F 7.6.0 Configuration Wizard
49-922-769106-20211216

TABLE OF CONTENTS

Overview

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

Note: The data displayed in the Config Wizard may not represent the current configuration of the appliance. When making edits in the Config Wizard, modifications are stored in a temporary file. This allows users to exit the Config Wizard before saving changes permanently.

Terminology

Term	Definition
“Isolation” VLAN	Used for network segmentation of unknown and untrusted endpoints. Provides limited network access
FortiNAC Service Network Interface ("Isolation" network interface)	Configured on the port2 interface of the appliance. Serves DHCP, DNS and the Captive Portal to the “isolation” VLANs **Important**: Configuring port1 and port2 in the same network is not recommended or supported.
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 Deployment Guide.

Requirements

- FortiNAC appliance has been staged and can be reached over the interface specified below
  - Virtual appliances and existing installations: port1
  - New physical appliances: port2 (see Appliance Installation Guide for details)
- License key(s)
- Appliance passwords
- Appliance Network Addressing
  - Hostname
  - IP address and Network Mask for Port1 and Port2
  - Default Gateway
  - Domain name
  - DNS server(s)
  - NTP server(s)
- At least one DHCP scope for “isolation” VLAN

See the Requirements Task List in the Deployment Guide for details regarding the above requirements.

Considerations

If appliances will be configured for High Availability, it is important to consider the following before configuring the FortiNAC Service Interface (port2):

- **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 Config Wizard restrictions.

For more details on this feature, refer to the following documents in the Fortinet Document Library:

High Availability

N + 1 Failover

Accessing the FortiNAC GUI for the first time

First time users of the FortiNAC device should get started by going to the FortiNAC deployment guide.

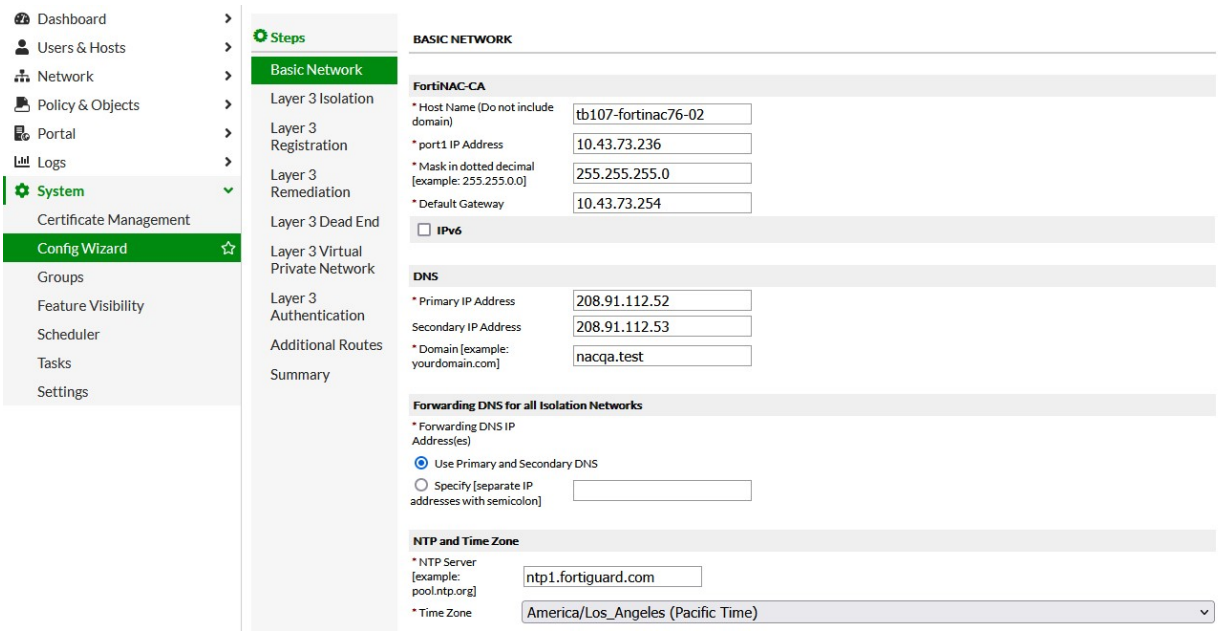
1. Use the DHCP address or (If Required) configIP
2. Browse to
   `https://<IP address of port1>:8443/`
3. Login using the Default FortiNAC Admin GUI Credentials
   User: root
   Password: YAMS
4. Read the End User License Agreement. Accept the terms and continue.
5. For your license key, click **import** .lic file, and select the .lic file previously downloaded. It is **not** recommended to copy and paste into the box.
   Click **Next**.
6. Enter a new User ID and Password to use when logging in to the Admin GUI. This user record is locally stored in the server's database. Click **Next**.
   For password requirement details, see Passwords.
   Note: The CLI account is not updated with a change until the Config Wizard is completed and a Config Wizard reboot is executed.
7. Select the installation method you would like to use.
   Note: We recommend that new users use the **Guided Installation.**
   Guided Installation will create a series of Tasks that will help walk through the set up of the product to gain visibility as quickly as possible. Click **Next.**
8. Select the customer requirements for the **Guided Installation**. This creates a widget checklist that shows you whether or not the task has been done.
   Click **OK**.
9. The Config Wizard view will display.

- To modify/update License Key after initial configuration, navigate to **System > Settings > System Management > License Management.**
- For instructions to change CLI passwords, see Passwords.

Navigating Config Wizard

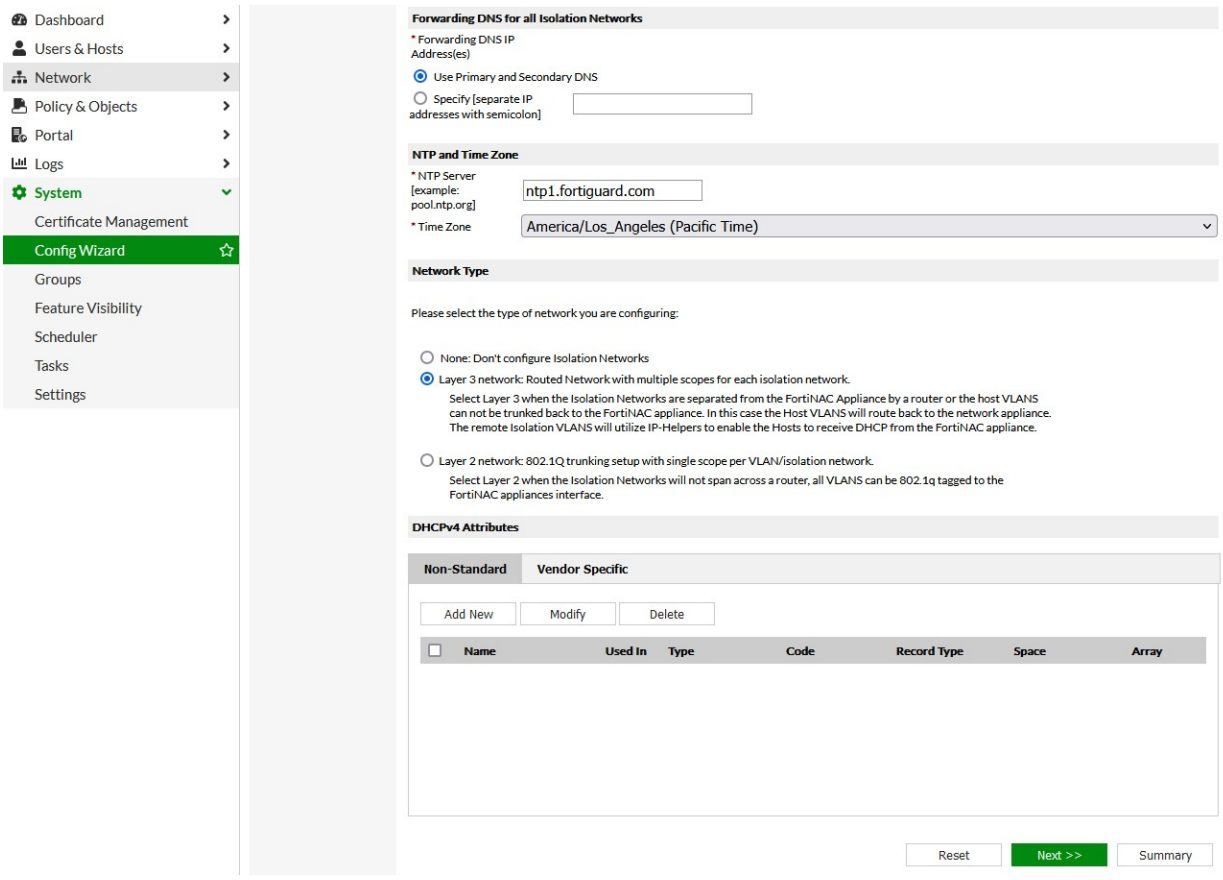
Use the following buttons and links to navigate through the Config Wizard.

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.



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.


Dashboard
Users & Hosts
Network
Policy & Objects
Portal
Logs
System
Certificate Management
Config Wizard
Groups
Feature Visibility
Scheduler
Tasks
Settings
Forwarding DNS for all Isolation Networks
* Forwarding DNS IP Address(es)
Use Primary and Secondary DNS
Specify [separate IP addresses with semicolon]
NTP and Time Zone
* NTP Server [example: pool.ntp.org]
ntp1.fortiguard.com
* Time Zone
America/Los_Angeles (Pacific Time)
Network Type
Please select the type of network you are configuring:
None: Don't configure Isolation Networks
Layer 3 network: Routed Network with multiple scopes for each isolation network.
Select Layer 3 when the Isolation Networks are separated from the FortiNAC Appliance by a router or the host VLANS can not be trunked back to the FortiNAC appliance. In this case the Host VLANS will route back to the network appliance. The remote Isolation VLANS will utilize IP-Helpers to enable the Hosts to receive DHCP from the FortiNAC appliance.
Layer 2 network: 802.1Q trunking setup with single scope per VLAN/isolation network.
Select Layer 2 when the Isolation Networks will not span across a router, all VLANS can be 802.1q tagged to the FortiNAC appliances interface.
DHCPv4 Attributes
Non-Standard
Vendor Specific
Add New
Modify
Delete
Name
Used In
Type
Code
Record Type
Space
Array
Reset
Next >>
Summary

Step 1: Basic Network Configuration

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

Enter the values based on the definitions in the table below.

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.
port1 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.

Step 2: Select Network Type

Configures FortiNAC's port2 interface (FortiNAC Service Interface) for network segmentation of untrusted hosts connecting to the network. For Layer 2 and Layer 3 examples, refer to the Deployment Guide.

Select one of the following options.

None	Do not configure Isolation Networks. When None is selected, captive portal service will be disabled.
Layer 3 network	Port2 is connected to a single VLAN on an untagged port. Network traffic is routed to the clients for each isolation network. The following components are configured: • FortiNAC Service Interface(s): The interface(s) which FortiNAC uses to communicate with endpoints in the "isolation" networks. • DHCP scope(s): Used by FortiNAC to deliver IP addressing to isolated endpoints. At least one scope must be configured.
Layer 2 network	Traffic in the "isolation" VLANs are switched to the FortiNAC port2 interface. 802.1Q tags are configured for the corresponding "isolation" VLANs, and port2 IP addresses are within those networks. The following components are configured: • FortiNAC Service Interface(s): The interface(s) which FortiNAC uses to communicate with endpoints in the "isolation" networks. • DHCP scope(s): Used by FortiNAC to deliver IP addressing to isolated endpoints. At least one scope must be configured.

Step 3: Define DHCPv4 Attributes

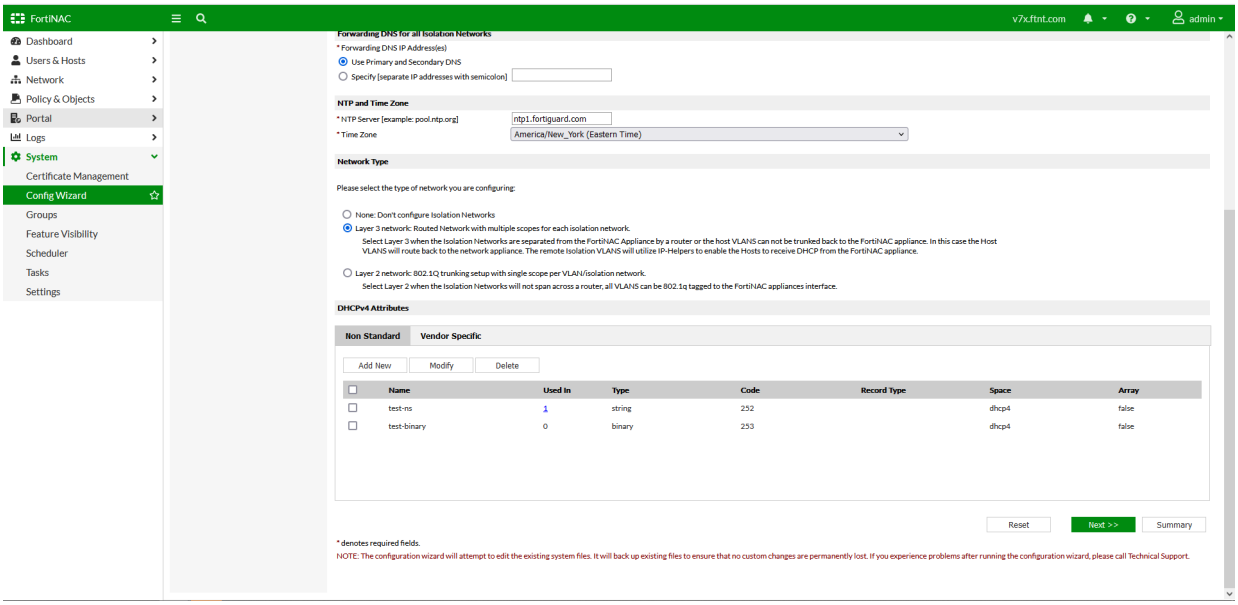
If the Network Type option “none” was selected in step 2, skip this step and proceed to **Step 4: Configure Network Type**.

Starting from FortiNAC 7.6, users can configure non-standard and vendor-specific DHCP options, as well as next-server and boot-file-name BOOTP fields in config wizard.

Before adding DHCP options in isolation networks, the user should define the non-standard or vendor-specific attributes they want to add in DHCP messages in isolation networks.

The non-standard or vendor-specific attributes definition in L2 network and in L3 network are separate; the attribute defined in L2 network will not be in L3 network, and vice versa.

If there are no non-standard or vendor-specific attributes to add, proceed to **Step 4: Configure Network Type.**



Define Standard Attribute

Here you can define standard attributes that will be included in DHCP messages to the hosts. Note that you will fill in the values of these attributes in isolation network configuration; here you only decide what Fields and attributes will be included.

You can also modify or delete standard attributes here, by selecting an attribute and clicking the "modify" or "delete" button. Please note that attributes in use cannot be deleted.

Available Standard Attributes

See following table for attribute type definitions. These are selectable via drill-down menu.

Attribute name	DHCP Option Value Type	Record Types (For “Record” Option Value Type)
time-offset	int32	
routers	ipv4-address	
time-servers	ipv4-address	
name-servers	ipv4-address	
domain-name-servers	ipv4-address	
log-servers	ipv4-address	
cookie-servers	ipv4-address	
lpr-servers	ipv4-address	
impress-servers	ipv4-address	
resource-location-servers	ipv4-address	
boot-size	uint16	
merit-dump	string	
domain-name	fqdn	
swap-server	ipv4-address	
root-path	string	
extensions-path	string	
ip-forwarding	boolean	
non-local-source-routing	boolean	
policy-filter	ipv4-address	
max-dgram-reassembly	uint16	
default-ip-ttl	uint8	
path-mtu-aging-timeout	uint32	
path-mtu-plateau-table	uint16	
interface-mtu	uint16	
all-subnets-local	boolean	

Attribute name	DHCP Option Value Type	Record Types (For “Record” Option Value Type)
broadcast-address	ipv4-address	
perform-mask-discovery	boolean	
mask-supplier	boolean	
router-discovery	boolean	
router-solicitation-address	ipv4-address	
static-routes	ipv4-address	
trailer-encapsulation	boolean	
arp-cache-timeout	uint32	
ieee802-3-encapsulation	boolean	
default-tcp-ttl	uint8	
tcp-keepalive-interval	uint32	
tcp-keepalive-garbage	boolean	
nis-domain	string	
nis-servers	ipv4-address	
ntp-servers	ipv4-address	
netbios-name-servers	ipv4-address	
netbios-dd-server	ipv4-address	
netbios-node-type	uint8	
netbios-scope	string	
font-servers	ipv4-address	
x-display-manager	ipv4-address	

Attribute name	DHCP Option Value Type	Record Types (For “Record” Option Value Type)
dhcp-option-overload	uint8	
dhcp-server-identifier	ipv4-address	
dhcp-message	string	
dhcp-max-message-size	uint16	
vendor-class-identifier	string	
nwip-domain-name	string	
nwip-suboptions	binary	
nisplus-domain-name	string	
nisplus-servers	ipv4-address	
tftp-server-name	string	
boot-file-name	string	
mobile-ip-home-agent	ipv4-address	
smtp-server	ipv4-address	
pop-server	ipv4-address	
nntp-server	ipv4-address	
www-server	ipv4-address	
finger-server	ipv4-address	
irc-server	ipv4-address	
streettalk-server	ipv4-address	
streettalk-directory-assistance-server	ipv4-address	
user-class	binary	
slp-directory-agent	record	boolean,ipv4-address

Attribute name	DHCP Option Value Type	Record Types (For “Record” Option Value Type)
slp-service-scope	record	boolean,string
nds-server	ipv4-address	
nds-tree-name	string	
nds-context	string	
bcms-controller-names	fqdn	
bcms-controller-address	ipv4-address	
client-system	uint16	
client-ndi	record	uint8,uint8,uint8
uuid-guid	record	uint8,binary
uap-servers	string	
geoconf-civic	binary	
pcode	string	
tcode	string	
v6-only-preferred	uint32	
netinfo-server-address	ipv4-address	
netinfo-server-tag	string	
v4-captive-portal	string	
auto-config	uint8	
name-service-search	uint16	
domain-search	fqdn	
vivco-suboptions	record	uint32,binary
vivso-suboptions	uint32	
pana-agent	ipv4-address	

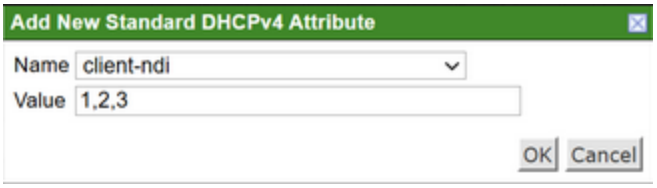
Attribute name	DHCP Option Value Type	Record Types (For “Record” Option Value Type)
v4-lost	fqdn	
capwap-ac-v4	ipv4-address	
sip-ua-cs-domains	fqdn	
rdnss-selection	record	uint8,ipv4-address,ipv4-address,fqdn
v4-portparams	record	uint8,psid
option-6rd	record	uint8,uint8,ipv6-address,ipv4-address
v4-access-domain	fqdn	

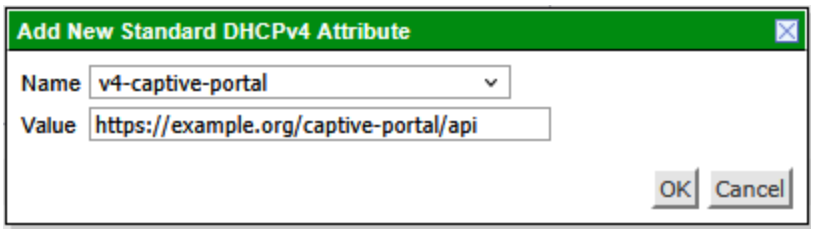
DHCP Option Value Definitions

Field	Definition & Notes	
Type	The type of this option. Possible values are:	
	binary	An arbitrary string of bytes, specified as a set of hexadecimal digits.
	boolean	A boolean value with allowed values true or false.
	fqdn	Fully qualified domain name (e.g. www.example.com).
	ipv4-address	IPv4 address in the usual dotted-decimal notation (e.g. 192.0.2.1).
	ipv6-address	IPv6 address in the usual colon notation (e.g. 2001:db8::1).
	ipv6-prefix	IPv6 prefix and prefix length specified using CIDR notation, e.g. 2001:db8:1::/64. This data type is used to represent an 8-bit field conveying a prefix length and the variable length prefix value.
	psid	PSID and PSID length separated by a slash, e.g. 3/4 specifies PSID=3 and PSID length=4. In the wire format it is represented by an 8-bit field carrying PSID length (in this case equal to 4) and the 16-bits-long PSID value field (in this case equal to "0011000000000000b" using binary notation). Allowed values for a PSID length are 0 to 16. See RFC 7597 for details about the PSID wire representation.
	record	Structured data that may be comprised of any type (except "record" and "empty"). The array flag applies to the last field only.

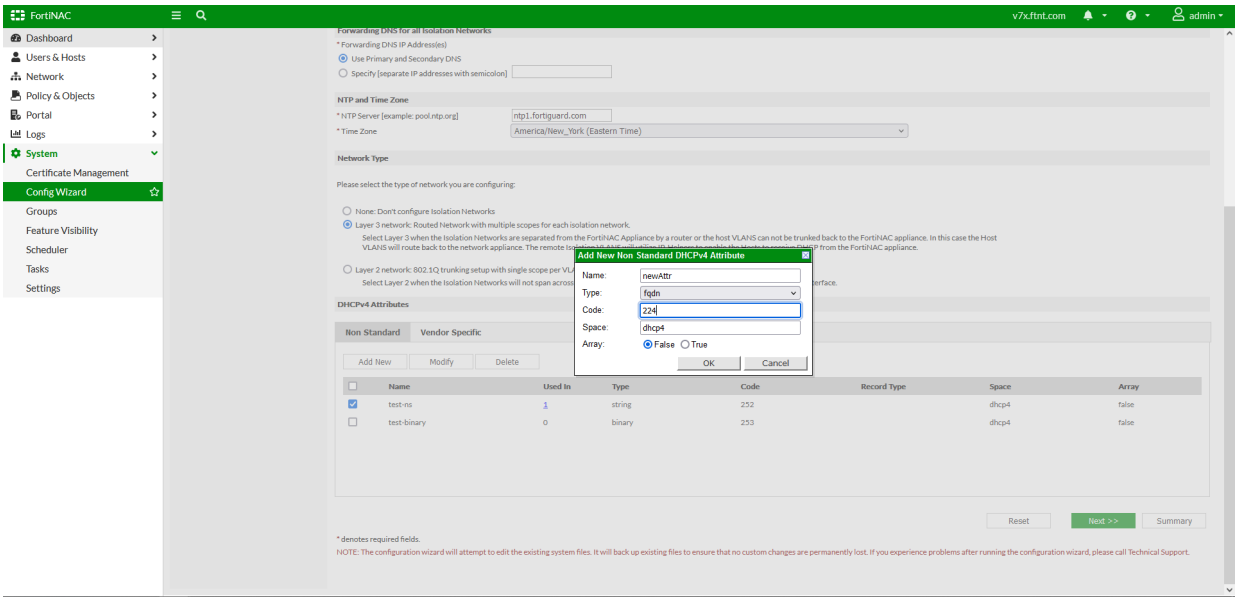
Field	Definition & Notes	
	string	Any text. Please note that Kea silently discards any terminating/trailing nulls from the end of "string" options when unpacking received packets. This is in keeping with RFC 2132, Section 2.
	tuple	A length encoded as an 8-bit (16-bit for DHCPv6) unsigned integer followed by a string of this length.
	uint8	An 8-bit unsigned integer with allowed values 0 to 255.
	uint16	A 16-bit unsigned integer with allowed values 0 to 65535.
	uint32	A 32-bit unsigned integer with allowed values 0 to 4294967295.
	int8	An 8-bit signed integer with allowed values -128 to 127.
	int16	A 16-bit signed integer with allowed values -32768 to 32767.
	int32	A 32-bit signed integer with allowed values -2147483648 to 2147483647.
Code	The code number of this option. The code number used by standard attributes can't be used here.	
Record Types	mandatory if type=record, otherwise it must be left blank Info icon to tell the user it is comma-separated, example "record-types": "ipv4-address, uint16, boolean, string",	
Space	An option space is a collection of DHCP options. Default is 'dhcp4'/'dhcp'.	
Array	Whether this option is an array. Default is false.	

Record exmples:





Define Non-Standard Attribute



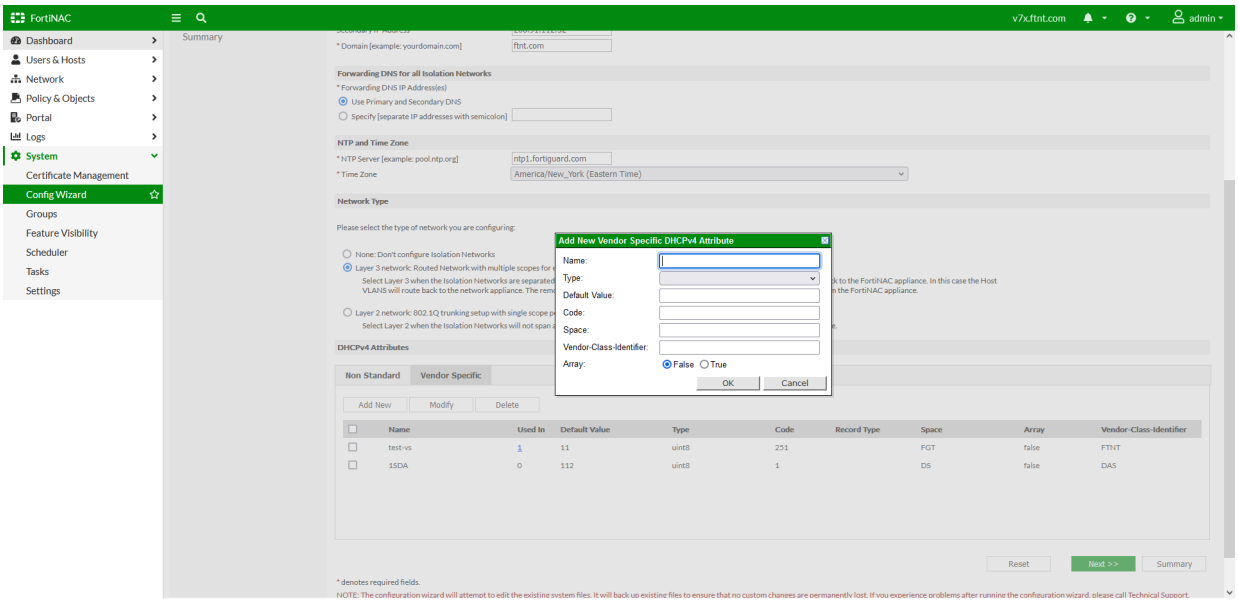
Here you can define non-standard attributes that will be included in DHCP messages to the hosts. Note that you will fill in the values of these attributes in isolation network configuration; here you only decide what Fields and attributes will be included.

You can also modify or delete non-standard attributes here, by selecting an attribute and clicking the “modify” or “delete” button. Please note that attributes in use cannot be deleted.

Field	Definition & Notes	
Name	The name of this option. The name used by standard attributes can’t be used here	
Type	The type of this option. Possible values are:	
	binary	An arbitrary string of bytes, specified as a set of hexadecimal digits.
	boolean	A boolean value with allowed values true or false.
	fqdn	Fully qualified domain name (e.g. www.example.com).
	ipv4-address	IPv4 address in the usual dotted-decimal notation (e.g. 192.0.2.1).
	ipv6-address	IPv6 address in the usual colon notation (e.g. 2001:db8::1).

Field	Definition & Notes	
	ipv6-prefix	IPv6 prefix and prefix length specified using CIDR notation, e.g. 2001:db8:1::/64. This data type is used to represent an 8-bit field conveying a prefix length and the variable length prefix value.
	psid	PSID and PSID length separated by a slash, e.g. 3/4 specifies PSID=3 and PSID length=4. In the wire format it is represented by an 8-bit field carrying PSID length (in this case equal to 4) and the 16-bits-long PSID value field (in this case equal to "0011000000000000b" using binary notation). Allowed values for a PSID length are 0 to 16. See RFC 7597 for details about the PSID wire representation.
	record	Structured data that may be comprised of any type (except "record" and "empty"). The array flag applies to the last field only.
	string	Any text. Please note that Kea silently discards any terminating/trailing nulls from the end of "string" options when unpacking received packets. This is in keeping with RFC 2132, Section 2.
	tuple	A length encoded as an 8-bit (16-bit for DHCPv6) unsigned integer followed by a string of this length.
	uint8	An 8-bit unsigned integer with allowed values 0 to 255.
	uint16	A 16-bit unsigned integer with allowed values 0 to 65535.
	uint32	A 32-bit unsigned integer with allowed values 0 to 4294967295.
	int8	An 8-bit signed integer with allowed values -128 to 127.
	int16	A 16-bit signed integer with allowed values -32768 to 32767.
	int32	A 32-bit signed integer with allowed values -2147483648 to 2147483647.
Code	The code number of this option. The code number used by standard attributes can't be used here.	
Record Types	mandatory if type=record, otherwise it must be left blank Info icon to tell the user it is comma-separated, example "record-types": "ipv4-address, uint16, boolean, string",	
Space	An option space is a collection of DHCP options. Default is 'dhcp4'/'dhcp'.	
Array	Whether this option is an array. Default is false.	

Define Vendor-Specific Attributes



Here you can define vendor-specific attributes that will be included in DHCP messages to the hosts. Note that you will fill in the values of these attributes in isolation network configuration; here you only decide what fields and attributes will be included.

You can also modify or delete vendor-specific attributes here, by selecting an attribute and clicking the “modify” or “delete” button. Please note that attributes in use cannot be deleted.

Field	Definition & Notes	Field
Name	The name of this option. The name used by standard attributes can’t be used here	
Type	The type of this option. Possible values are:	
	binary	An arbitrary string of bytes, specified as a set of hexadecimal digits.
	boolean	A boolean value with allowed values true or false.
	fqdn	Fully qualified domain name (e.g. www.example.com).
	ipv4-address	IPv4 address in the usual dotted-decimal notation (e.g. 192.0.2.1).
	ipv6-address	IPv6 address in the usual colon notation (e.g. 2001:db8::1).
	ipv6-prefix	IPv6 prefix and prefix length specified using CIDR notation, e.g. 2001:db8:1::/64. This data type is used to represent an 8-bit field conveying a prefix length and the variable length prefix value.

Field	Definition & Notes	Field
	psid	PSID and PSID length separated by a slash, e.g. 3/4 specifies PSID=3 and PSID length=4. In the wire format it is represented by an 8-bit field carrying PSID length (in this case equal to 4) and the 16-bits-long PSID value field (in this case equal to "0011000000000000b" using binary notation). Allowed values for a PSID length are 0 to 16. See RFC 7597 for details about the PSID wire representation.
	record	Structured data that may be comprised of any type (except "record" and "empty"). The array flag applies to the last field only.
	string	Any text. Please note that Kea silently discards any terminating/trailing nulls from the end of "string" options when unpacking received packets. This is in keeping with RFC 2132, Section 2.
	tuple	A length encoded as an 8-bit (16-bit for DHCPv6) unsigned integer followed by a string of this length.
	uint8	An 8-bit unsigned integer with allowed values 0 to 255.
	uint16	A 16-bit unsigned integer with allowed values 0 to 65535.
	uint32	A 32-bit unsigned integer with allowed values 0 to 4294967295.
	int8	An 8-bit signed integer with allowed values -128 to 127.
	int16	A 16-bit signed integer with allowed values -32768 to 32767.
	int32	A 32-bit signed integer with allowed values -2147483648 to 2147483647.
Default Value	The default value of this attribute. Cannot be left blank.	
Code	The code number of this option. Can be any number between 1 and 254, inclusive.	
Record Types	mandatory if type=record, otherwise it must be left blank Info icon to tell the user it is comma-separated, example "record-types": "ipv4-address, uint16, boolean, string",	
Space	An option space is a collection of DHCP options. This field accepts any alphanumeric string value.	
Vendor-Class-Identifier	Vendor Class Identifier is used to inform DHCP server of a particular vendor and/or model information. This vendor-specific attribute will be included in DHCP Offer or ACK messages from FortiNAC only if the Vendor Class Identifier option (option 60) in the DHCP Discover or Request message matches this field.	
Array	Whether this option is an array. Default is false.	

Step 4: Configure Network Type

No Isolation Network

1. Review the data on the Summary View to confirm the configured settings.
2. Click **Apply**. The Config Wizard writes the data to the files on the appliances. This process may take several minutes to complete. When completed, the Results page appears.
3. Review the Results. Errors are noted at the top of the Results page.
4. Scroll down through the results and note errors or warnings. Make changes and apply them until a successful configuration is written.
5. 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 port2 interface. Config Wizard will no longer be accessible from this interface.

   Port1 can now be connected to the network.

Re-run the Config 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.

Layer 3 Network

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 Additional Routes.

When you implement network access control, include at least one “isolation” Scope.

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

Layer 3 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, or Authentication) 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.

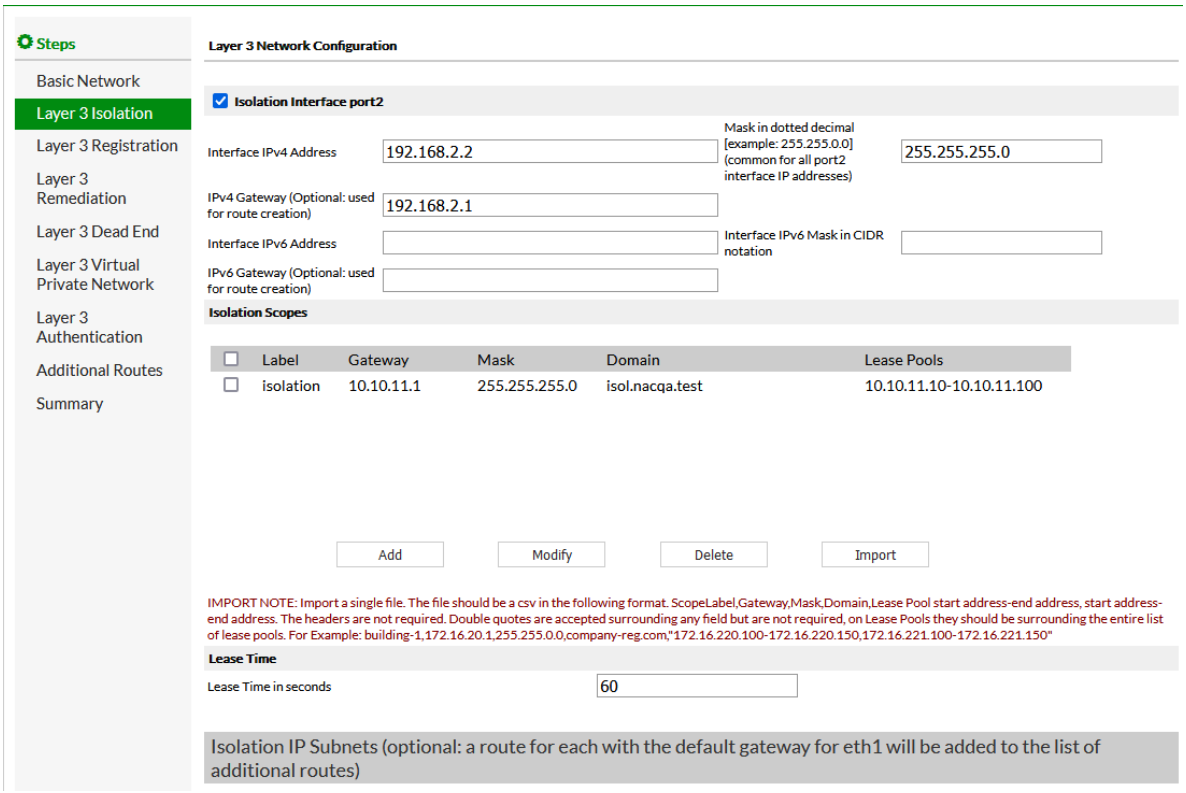
Configure interface port2

The configuration views for the Isolation, Registration, Remediation, Dead End, VPN and Authentication scopes are similar.

Note: When Isolation Interface port 2 is unchecked, and the system is rebooted, captive portal will be disabled.

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.

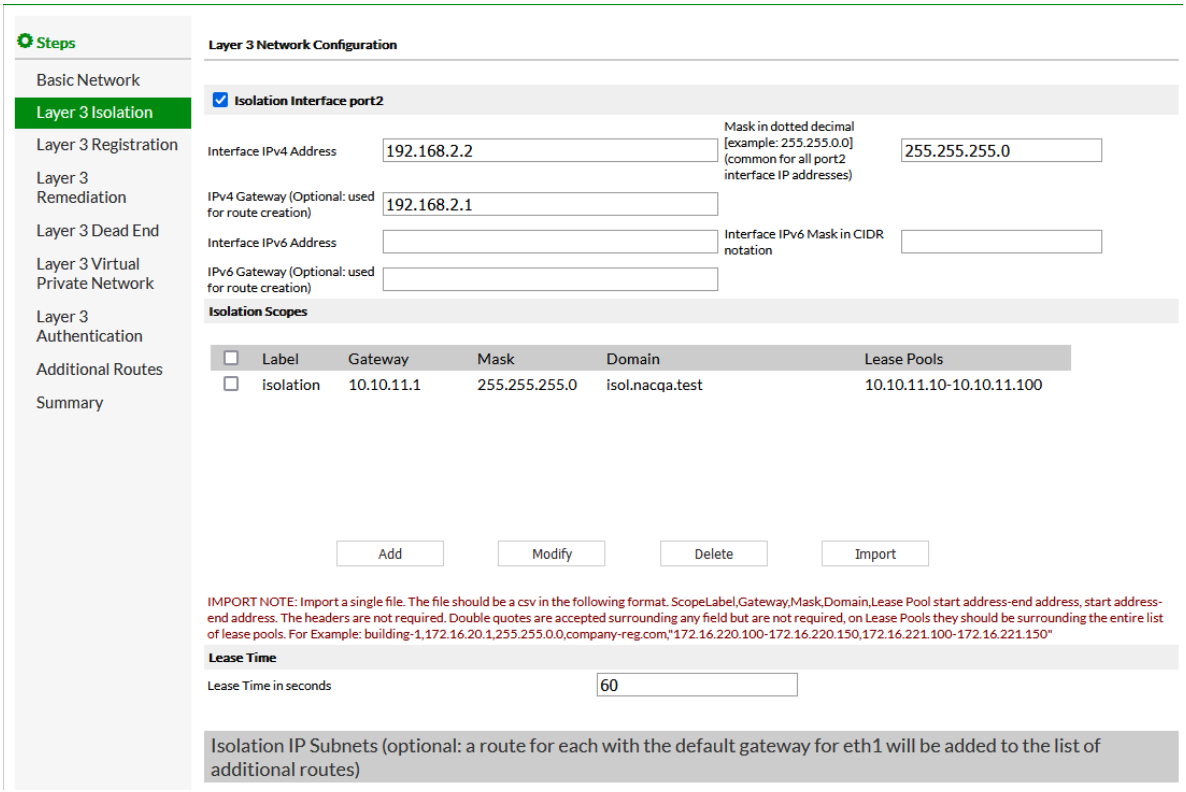


3. Under **Interface port2** section, configure using the table below.

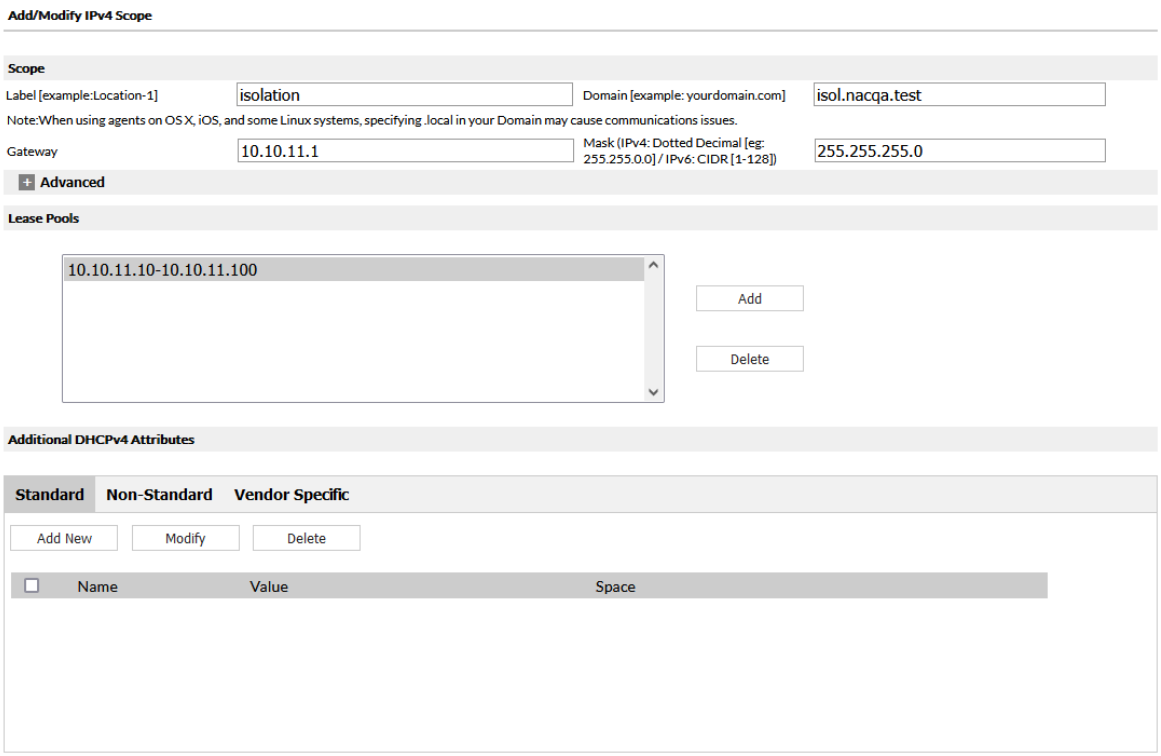
Field	Definition
Interface IP Address	IP address for the Route Scope interface on port2. Use a different IP for each route scope type you configure.
Mask	The subnet mask for the interface IP address. Note that the mask is shared between route scope types. If you modify the mask in one route scope, it changes in all others.
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 port2.

Configure scopes

1. Under **Scopes** section, click **Add** to add DHCP scope(s) or **Modify** to change existing information.



2. In the new window, configure the **Scope** section using the table below.

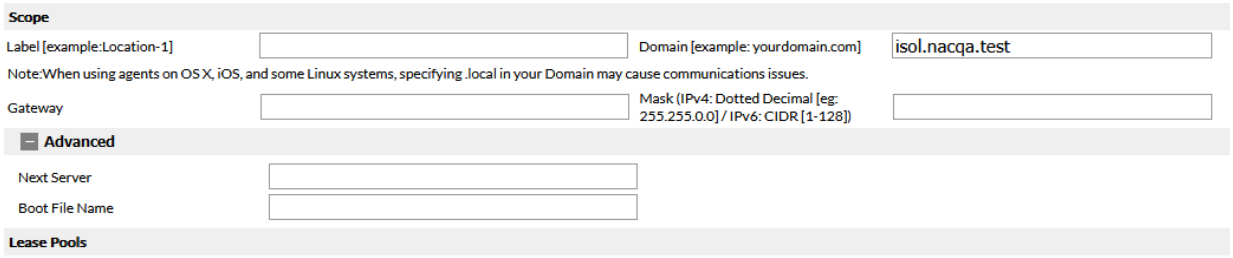


Field	Definition
Label	User specified name for the scope. Can be associated with a location, such as Building-B, or a function within the organization, such as Accounting. Note: When setting up Layer 3 Network Configurations in the Config wizard, labels of DHCP Scopes should not begin with any of these 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 port2.
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:**

Field	Definition
	Production domain is megatech.com For Isolation VLAN use **megatech-iso.com** For Registration VLAN use **megatech-reg.com**

Configure Advanced for PXE environments

Click **"+"** to expand the **Advanced** section. This is used to configure a Pre-boot Execution Environment (PXE). If not using PXE, skip this step.



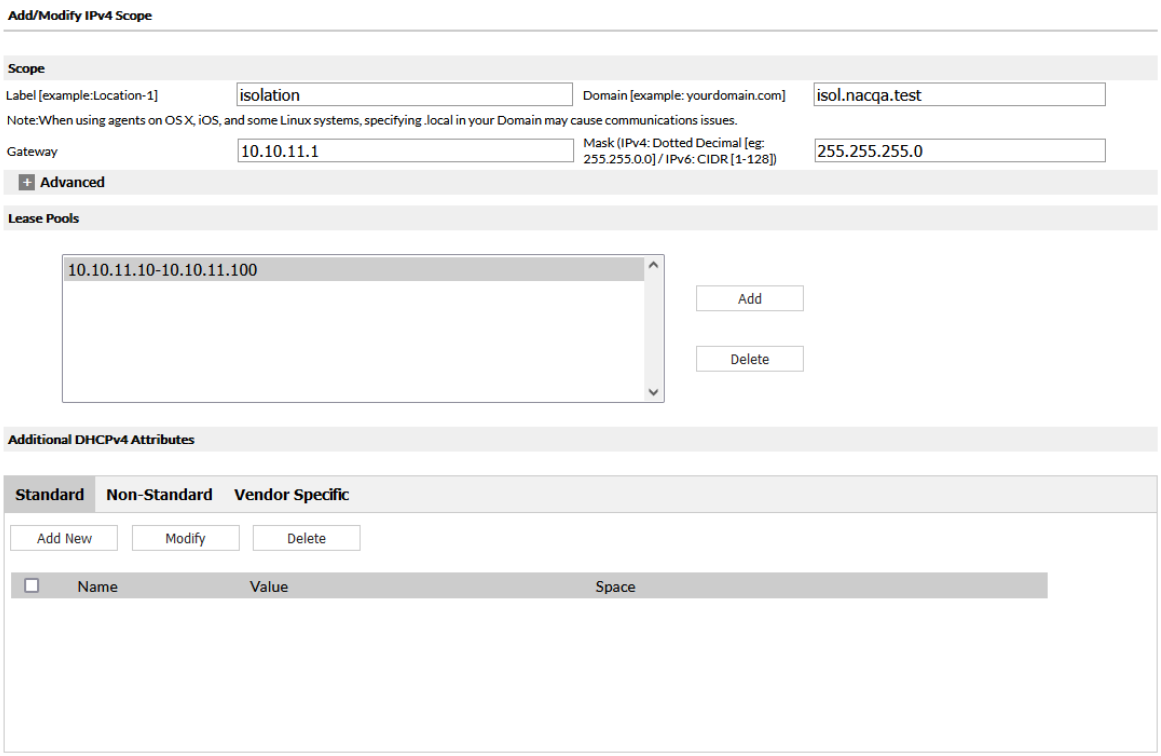
PXE is used for booting a client from an OS image stored in a file server. For users trying to set up a PXE, some hardware does not recognize tftp-server-name attribute (standard attribute 66) or boot-file-name attribute (standard attribute 67) but recognize legacy BOOTP server name and boot file name fields. The two BOOTP fields are not DHCP options and can only be configured in the "Advanced" menu. Refer to the DHCP Cookbook for details.

Field	Definition
Next server	The file server containing the boot image. The server should support TFTP.
Boot File Name	The absolute path to the OS image.

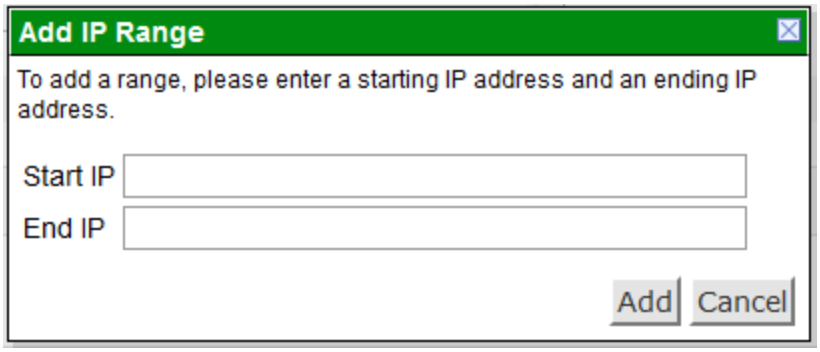
Configure lease pools

1. The **Lease Pools** section is used to configure the starting and ending IP addresses that delineate the range of IP addresses available on this route. Multiple ranges can be used.

   Click **Add** to add the lease pool information for the scope.



2. In the new window, enter the IP Addresses for **Start** and **End** of the lease pool range, then click **Add**.



3. Repeat steps 7 and 8 to create additional lease pools.

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

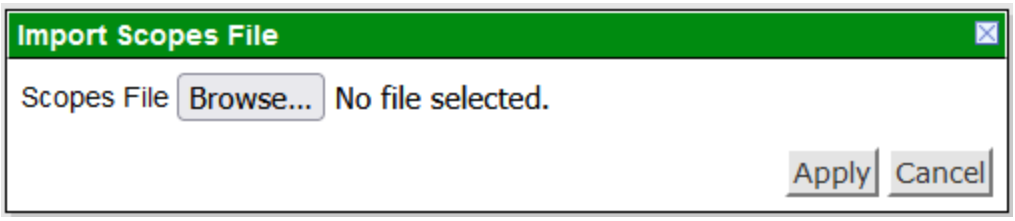
building-1,172.16.220.1,255.255.255.0,company- reg.com,"172.16.220.100-172.16.220.150,172.16.220.200-172.16.220.250"

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**.



Additional DHCP v4 Attributes

In L3 network settings, attributes are associated with isolation scopes and are configured in isolation scope settings. These attributes will be included in the DHCP response sent to hosts in this isolation network.

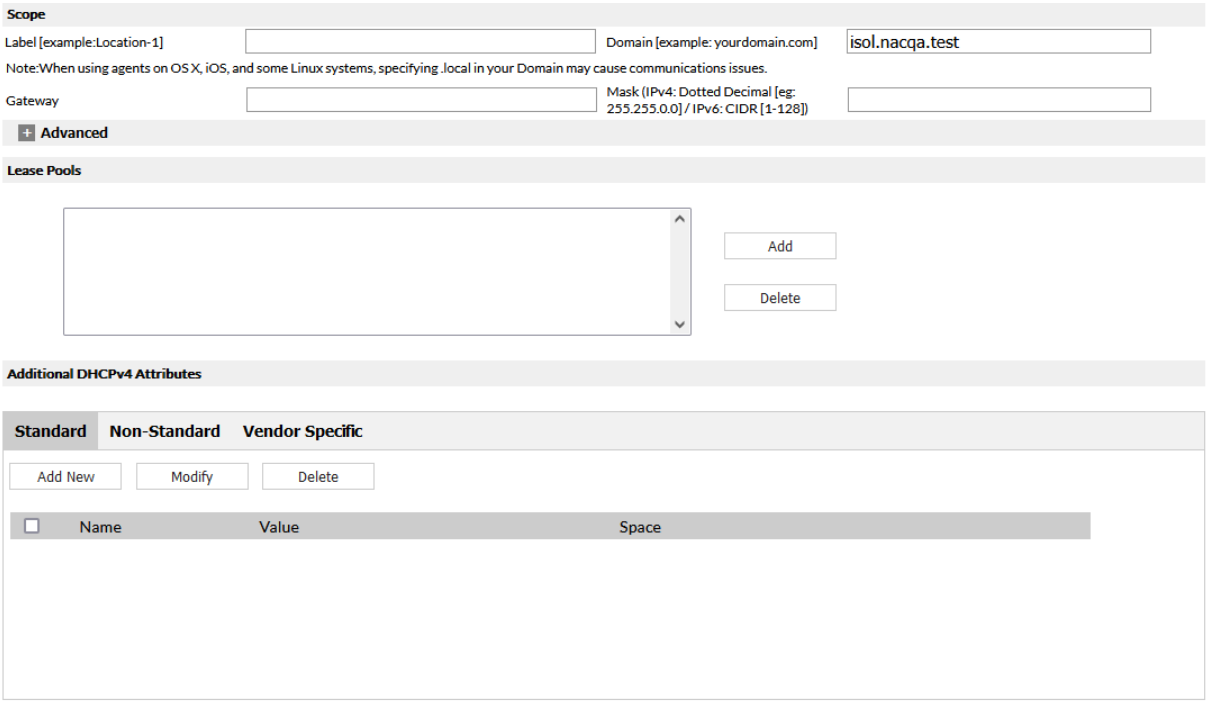
Three types of attributes can be configured:

Standard: For information about available standard attributes, refer to the chart entitled "List of Standard DHCPv4 Options" at the following link:

https://kea.readthedocs.io/en/kea-1.6.2/arm/dhcp4-srv.html#id2.

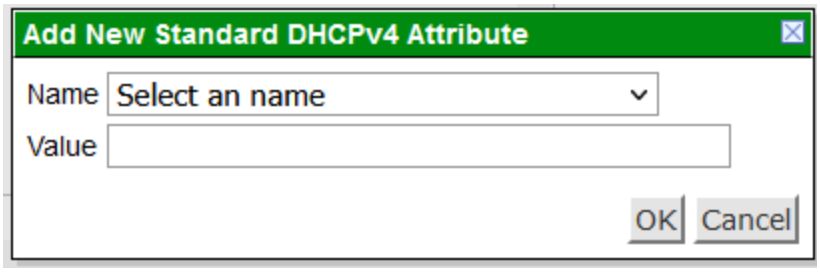
Non-Standard: Non-standard attributes are defined in the **Basic Network** settings. See Define DHCPv4 attributes for details.

Vendor Specific: Vendor Specific attributes are defined in the **Basic Network** settings. See Define DHCPv4 attributes for details.



Configure Standard Attributes

1. Under the **Standard** tab, click the **Add New** button.
2. In the new window, click the **Name** drill-down menu and select the option. For more information about available standard attributes, see https://kea.readthedocs.io/en/kea-1.6.2/arm/dhcp4-srv.html#id2.
3. Enter the associated value in the **Value** field.

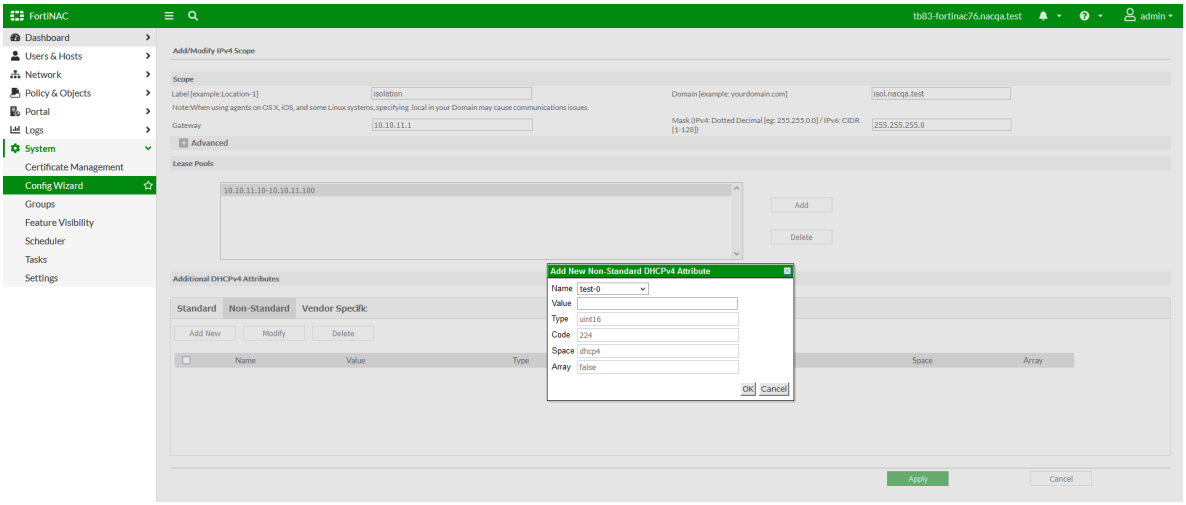


4. Click **OK** to save. The attribute will appear in the list under the **Standard** tab.

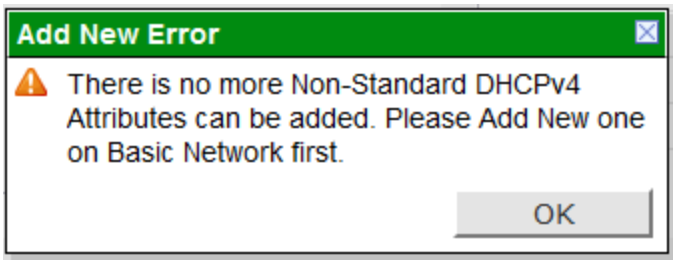
Use the **Modify** and **Delete** buttons to edit or remove an attribute from the list.

Configure Non-Standard Attributes

1. Under the **Non-Standard** tab, click the **Add New** button.
2. In the new window, click the **Name** drill-down menu and select one of the attributes defined in the Basic Network Settings.



If there were no attributes previously defined, the following message displays:

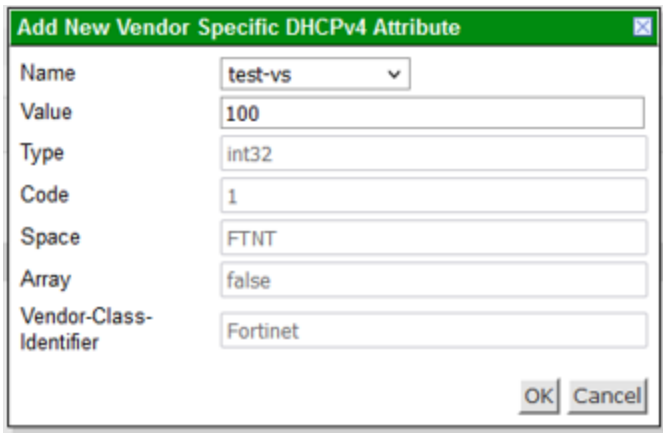


3. Enter the associated value in the **Value** field.
   (All other fields cannot be modified. They should be already defined).
4. Click **OK** to save. The attribute will appear in the list under the Non-**Standard** tab.

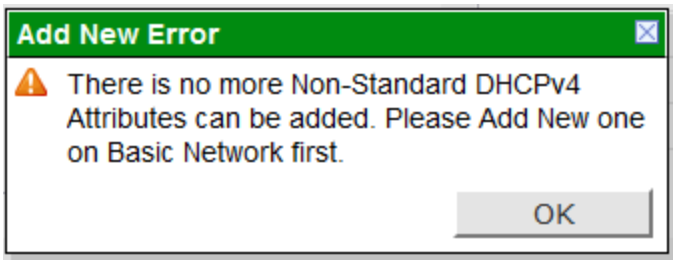
Use the **Modify** and **Delete** buttons to edit or remove an attribute from the list.

Configure Vendor-Specific Attributes

1. Under the **Vendor Specific** tab, click the **Add New** button.
2. In the new window, click the **Name** drill-down menu and select one of the attributes defined in the Basic Network Settings.



If there were no attributes previously defined, the following message displays:



3. Enter the associated value in the **Value** field.
   (All other fields cannot be modified. They should be already defined).
4. Click **OK** to save. The attribute will appear in the list under the **Vendor Specific** tab.

Use the **Modify** and **Delete** buttons to edit or remove an attribute from the list.

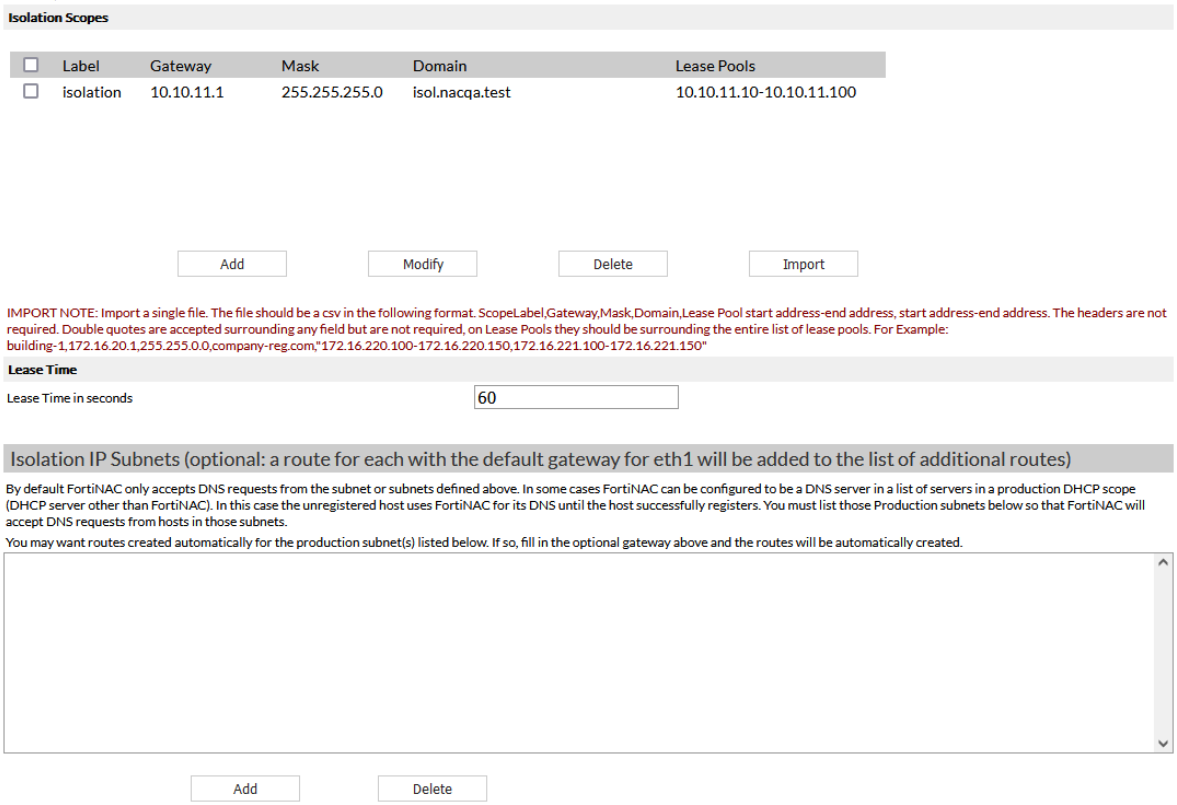
Isolation IP Subnets

By default, FortiNAC only accepts DNS requests from the subnet or subnets defined by the

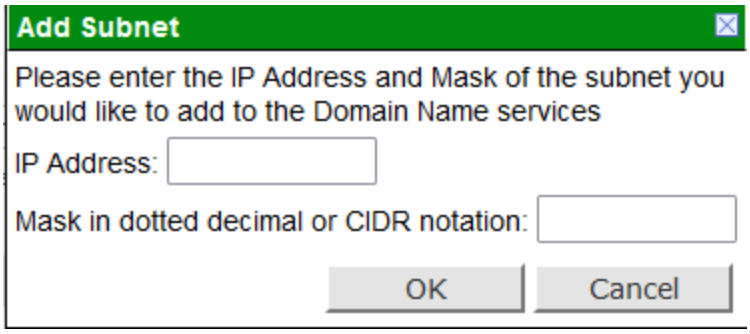
DHCP scope(s). In some cases, it may be desired for FortiNAC to respond to DNS requests from other subnets used for restricted access where FortiNAC is not acting as the DHCP server. Some examples include:

- FlexCLI,
- Roles only Aruba/Xirrus integration

- FortiGate with directly connected endpoints (see FortiGate Endpoint Management Integration Guide)



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

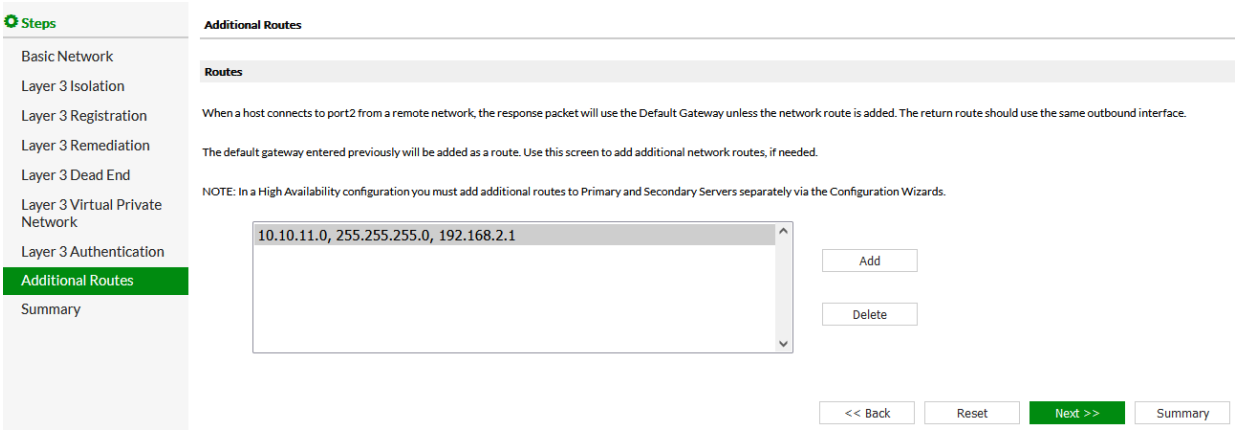


2. Define the network and mask for which FortiNAC will serve DNS then click **OK**.

Additional Routes

When a client connects on port2 from a remote network, the return packet uses the port1 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 port2.

As isolation network DHCP scopes are configured, static routes are automatically created for those networks, specifying the gateway for the corresponding port2 interface or sub-interface.



Important:

- 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 add a route:

1. Click **Add**.
2. Enter the Network IP Address, Mask, and Gateway, then click **Add**. Example:

   When port2 IP is 192.168.2.2 and the port2 gateway is 192.168.2.1 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 192.168.2.1	Identifies the gateway for port2. Do not use the gateway for the network.

3. Repeat step 1 and 2 to add additional routes.
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 Config 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.

Results

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 port2 interface. Config wizard will no longer be accessible from this interface.

Port1 can now be connected to the network.

Re-run the Config 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.

Layer 2 Network

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 Config wizard these additional VLANS are the Registration, Remediation, Dead End, VPN, Authentication and Isolation 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.

VLAN Type	Definition
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.

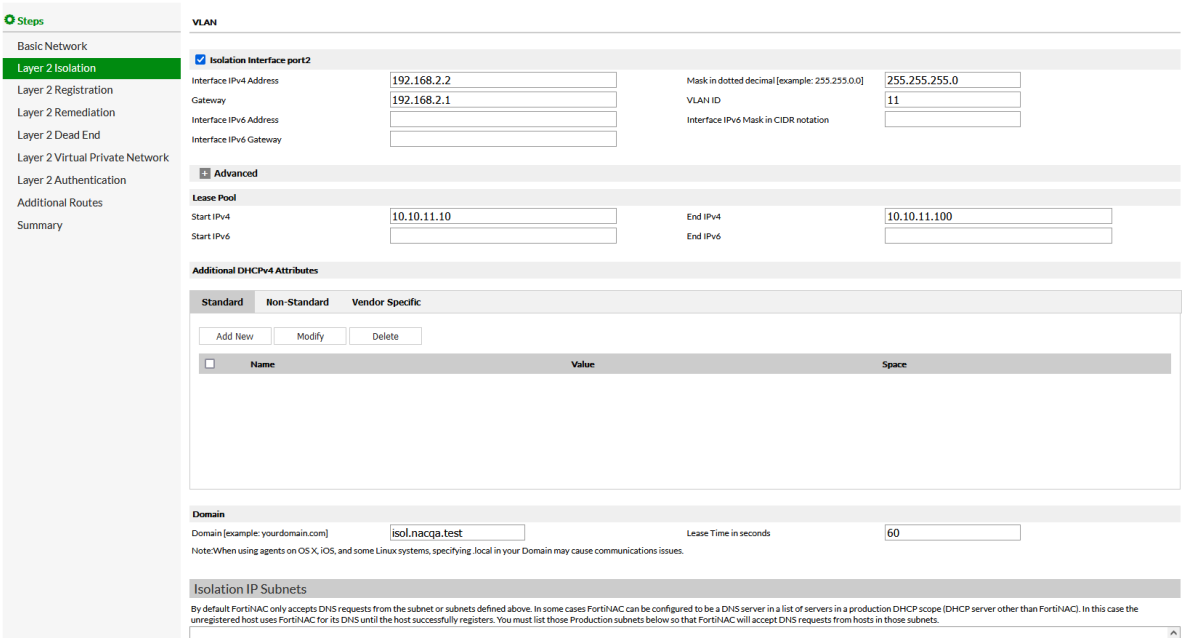
Configure interface port2

The configuration views for the Isolation, Registration, Remediation, Dead End, VPN and Authentication scopes are similar.

Note: When **Isolation Interface port 2** is unchecked, captive portal will be disabled.

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.

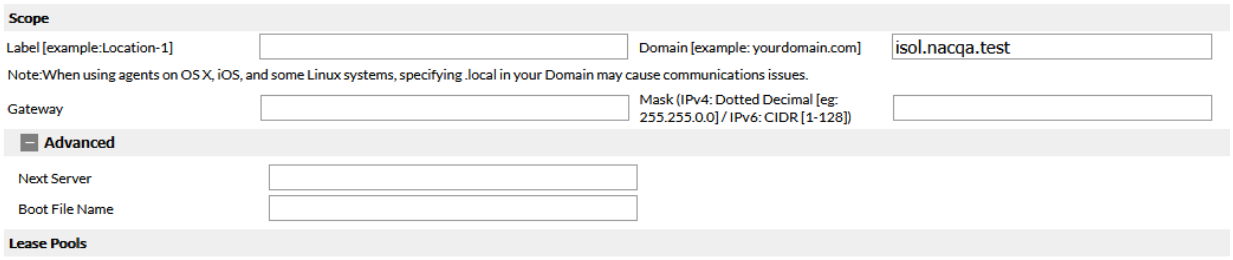


3. Under **Interface port2** section, configure using the table below.

Field	Definition
Interface IPv4 Address	IP4 address for the VLAN interface on port2. Use a different IP for each VLAN you configure.
Mask	The subnet mask for the interface IP address.
Gateway	Gateway for port2 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 port2. 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 port2 when clients connect through this VLAN.

Configure Advanced for PXE environments

Click **"+"** to expand the **Advanced** section. This is used to configure a Pre-boot Execution Environment (PXE). If not using PXE, skip this step.

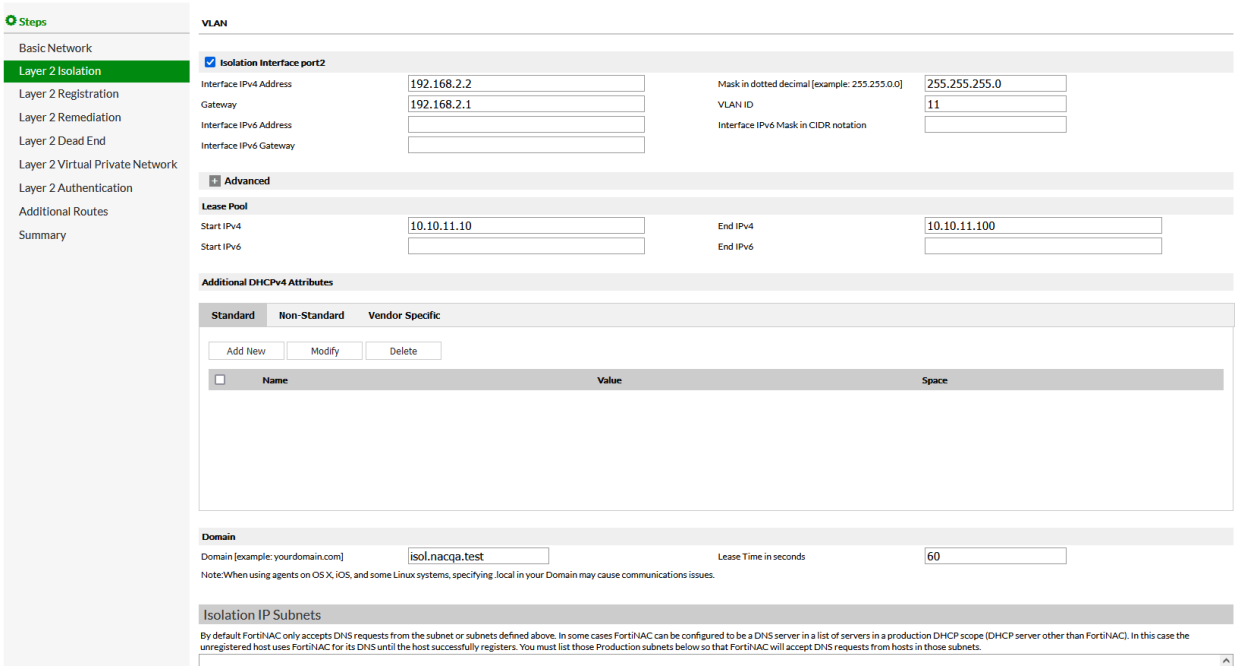


PXE is used for booting a client from an OS image stored in a file server. For users trying to set up a PXE, some hardware does not recognize tftp-server-name attribute (standard attribute 66) or boot-file-name attribute (standard attribute 67) but recognize legacy BOOTP server name and boot file name fields. The two BOOTP fields are not DHCP options and can only be configured in the "Advanced" menu. Refer to the DHCP Cookbook for details.

Field	Definition
Next server	The file server containing the boot image. The server should support TFTP.
Boot File Name	The absolute path to the OS image.

Configure lease pool & domain

The **Lease Pools** section is used to configure the starting and ending IP addresses that delineate the range of IP addresses available on this route.



Configure using the table below.

Field	Definition
Lease Pool Start	Starting IP address that delineate the range of IP addresses available on this VLAN.
Lease Pool End	Ending IP address that delineate the range of IP addresses available on this VLAN.
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

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 Isolation, Registration, Remediation, Authentication, Dead End and VPN is 60 seconds.

Additional DHCP v4 Attributes

In L2 network settings, attributes are configured in isolation network settings, since it doesn't have individual scope settings. These attributes will be included in the DHCP response sent to hosts in this isolation network.

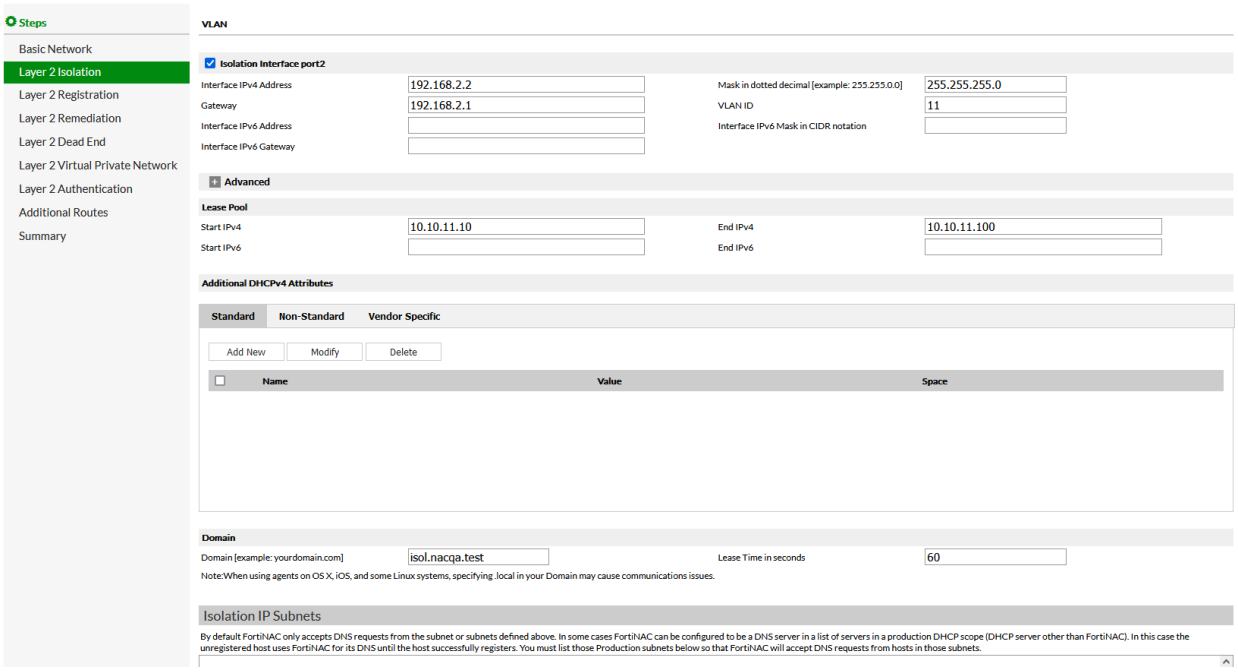
Three types of attributes can be configured:

Standard: For information about available standard attributes, refer to the chart entitled "List of Standard DHCPv4 Options" at the following link:

https://kea.readthedocs.io/en/kea-1.6.2/arm/dhcp4-srv.html#id2.

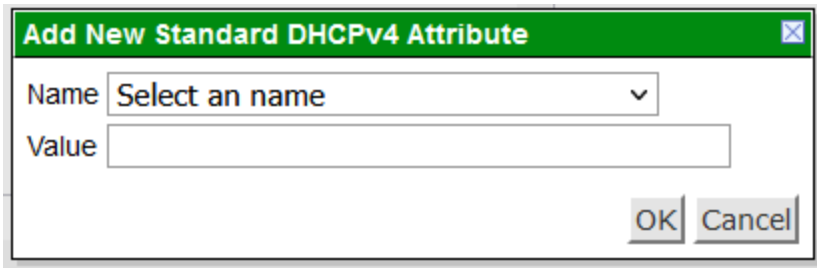
Non-Standard: Non-standard attributes are defined in the **Basic Network** settings. See Define DHCPv4 attributes for details.

Vendor Specific: Vendor Specific attributes are defined in the **Basic Network** settings. See Define DHCPv4 attributes for details.



Configure Standard Attributes

1. Under the **Standard** tab, click the **Add New** button.
2. In the new window, click the **Name** drill-down menu and select the option. For more information about available standard attributes, see https://kea.readthedocs.io/en/kea-1.6.2/arm/dhcp4-srv.html#id2.
3. Enter the associated value in the **Value** field.

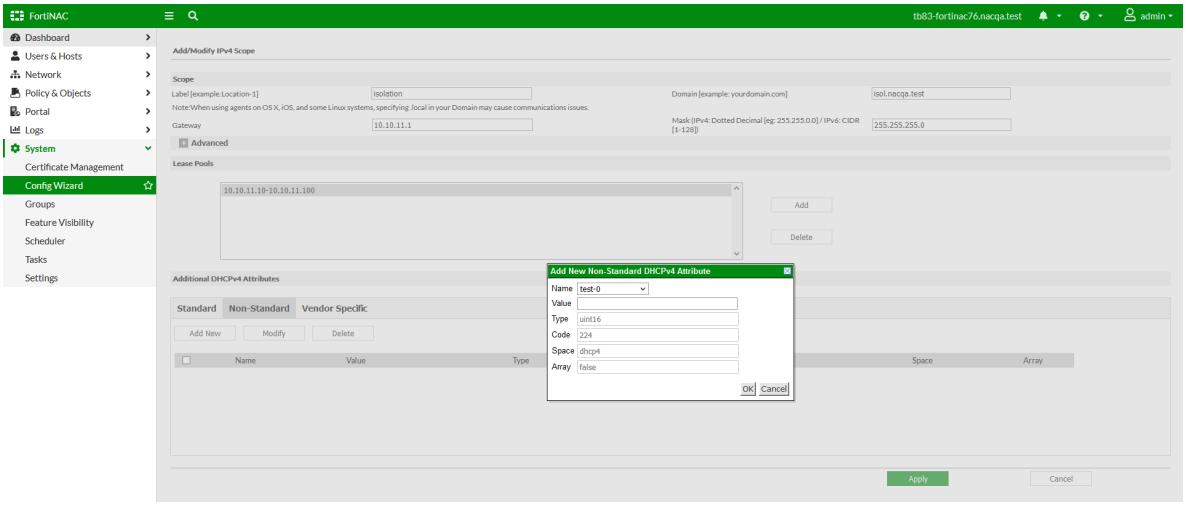


4. Click **OK** to save. The attribute will appear in the list under the **Standard** tab.

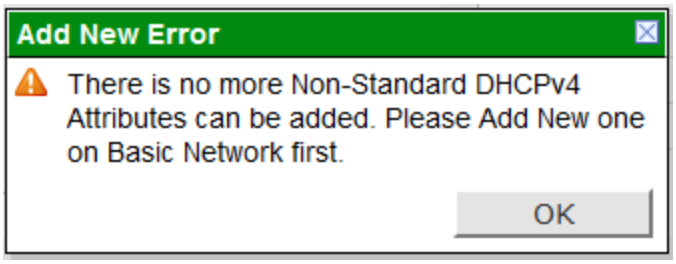
Use the **Modify** and **Delete** buttons to edit or remove an attribute from the list.

Configure Non-Standard Attributes

1. Under the **Non-Standard** tab, click the **Add New** button.
2. In the new window, click the **Name** drill-down menu and select one of the attributes defined in the Basic Network Settings.



If there were no attributes previously defined, the following message displays:



3. Enter the associated value in the **Value** field.

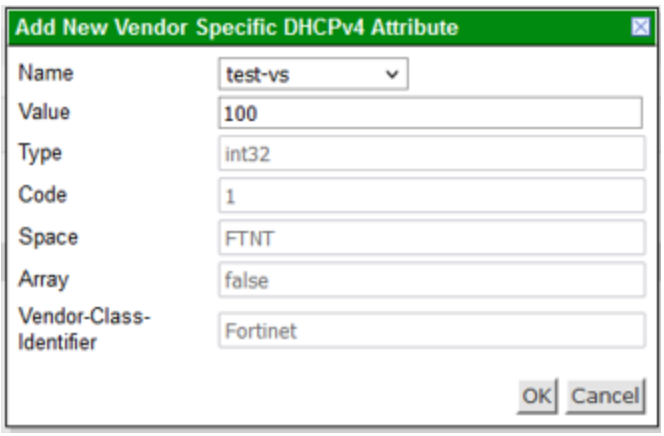
(All other fields cannot be modified. They should be already defined).

4. Click **OK** to save. The attribute will appear in the list under the Non-**Standard** tab.

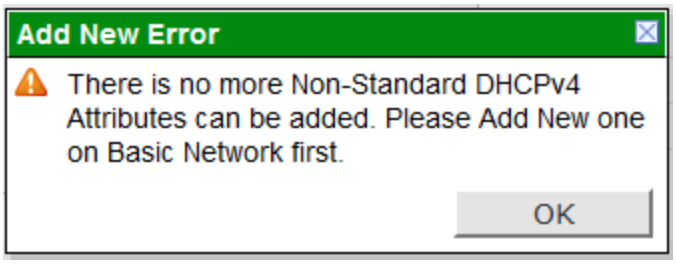
Use the **Modify** and **Delete** buttons to edit or remove an attribute from the list.

Configure Vendor-Specific Attributes

1. Under the **Vendor Specific** tab, click the **Add New** button.
2. In the new window, click the **Name** drill-down menu and select one of the attributes defined in the Basic Network Settings.



If there were no attributes previously defined, the following message displays:



3. Enter the associated value in the **Value** field.
   (All other fields cannot be modified. They should be already defined).
4. Click **OK** to save. The attribute will appear in the list under the **Vendor Specific** tab.

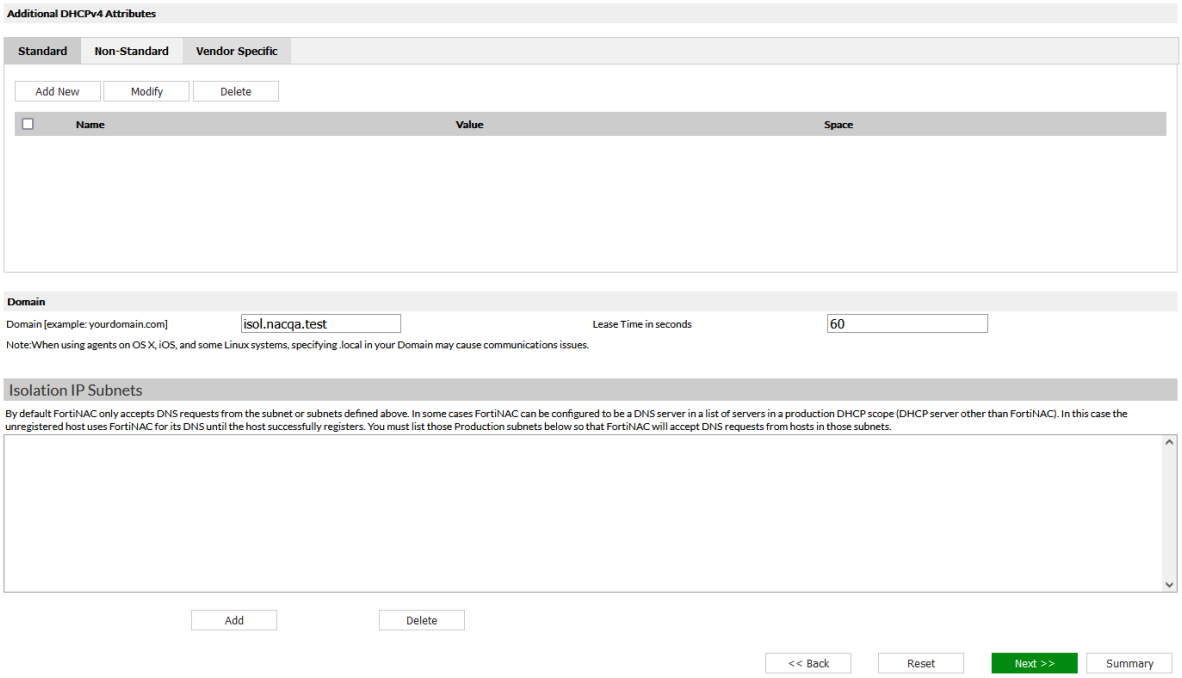
Use the **Modify** and **Delete** buttons to edit or remove an attribute from the list.

Isolation IP Subnets

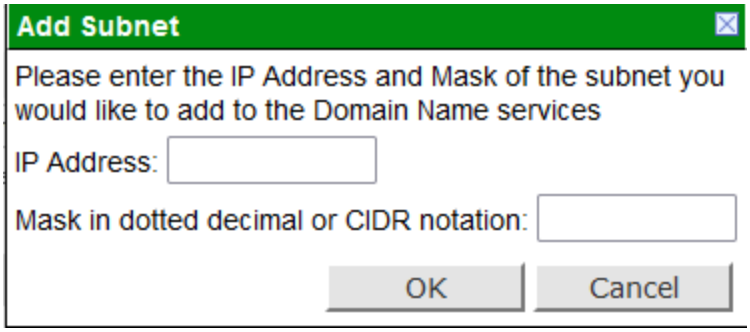
By default, FortiNAC only accepts DNS requests from the subnet or subnets defined by the

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:

- 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 IP Subnets** section.



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

Additional Routes

When a host connects to port2 from a remote network, the response packet will use the Default Gateway unless the network route is added. The return route should use the same outbound interface.

The default gateway entered previously will be added as a route. Use this screen to add additional network routes, if needed.

NOTE: In a High Availability configuration you must add additional routes to Primary and Secondary Servers separately via the Configuration Wizards.

1. To add a route, click the **Add** button.
2. Configure using the table below. Click **Add** to save.
3. Once all desired routes have been added, click **Next**.

Field	Definition
Network	Network
Mask	Subnet mask using dotted decimal notation
Gateway	Network gateway
Optional Sub Interface	Specify the sub interface (example - port2:3)

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 Config wizard writes the data to the files on the appliances. This process may take several minutes to complete. When completed, the Results page appears.

Results

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 port2 interface. Config wizard will no longer be accessible from this interface.

Port1 can now be connected to the network.

Re-run the Config 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.