DO NOT REPRINT
© FORTINET
Passdumps.com



FortiNAC

Study Guide

for FortiNAC 7.2

FORTINET
Training Institute

Vouchers & Dumps are Available | WhatsApp +201224665523

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

FORTINET

3/10/2023

Vouchers & Dumps are Available | WhatsApp +201224560923

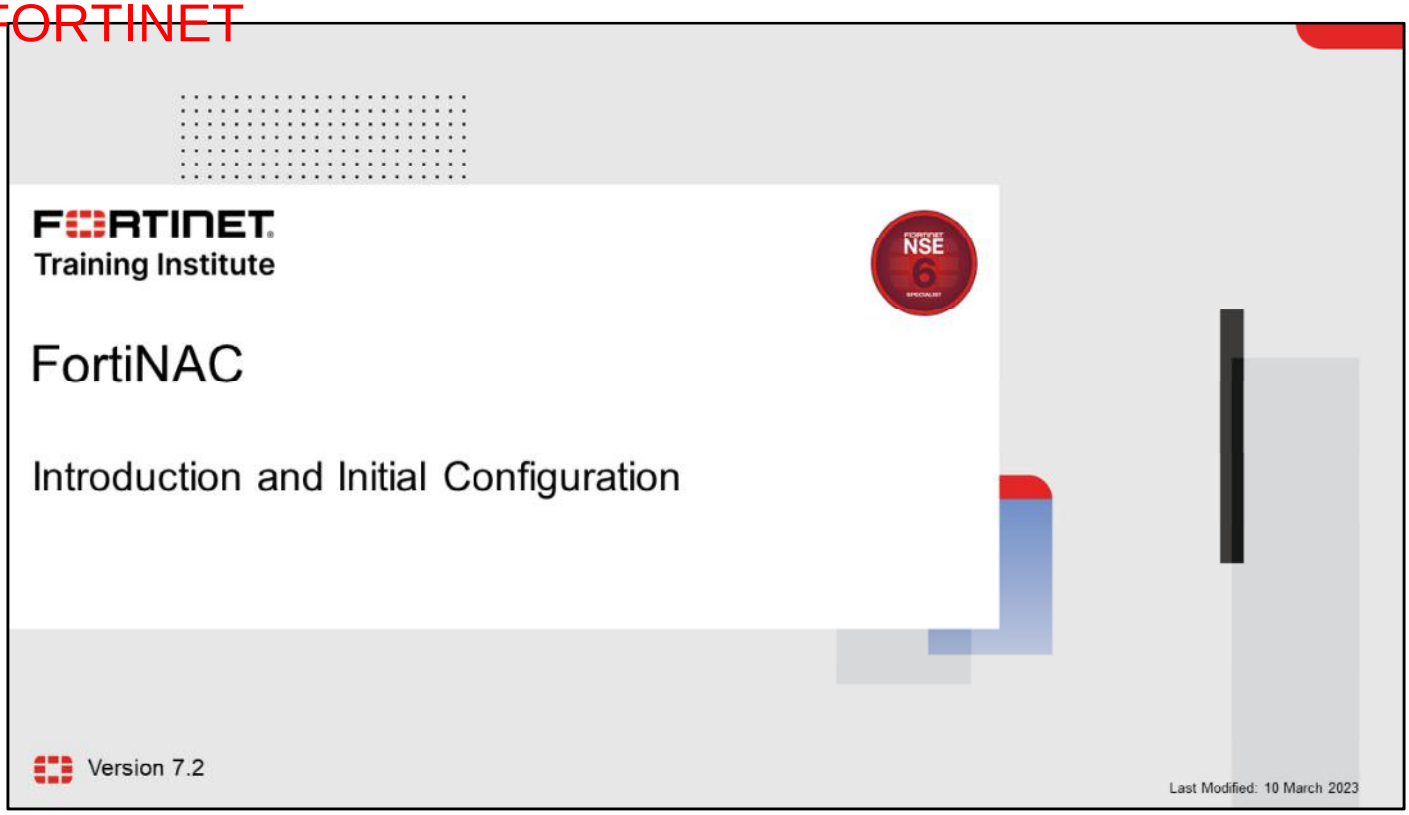
DO NOT REPRINT
© FORTINET
Brave-dumps.com

TABLE OF CONTENTS

01 Introduction and Initial Configuration 4
02 Achieving Network Visibility 65
03 Identification and Classification of Rogues 106
04 Visibility, Troubleshooting, and Logging 161
05 Logical Networks, Fortinet Security Fabric, and Firewall Tags 214
06 State-Based Control 240
07 Security Policies 281
08 Guest and Contractor Management 341
09 Security Device Integration and Automated Response 365
10 FortiGate VPN, High Availability, and FortiNAC Control Manager Integrations 402

Vouchers & Dumps are Available | WhatsApp +201224560923

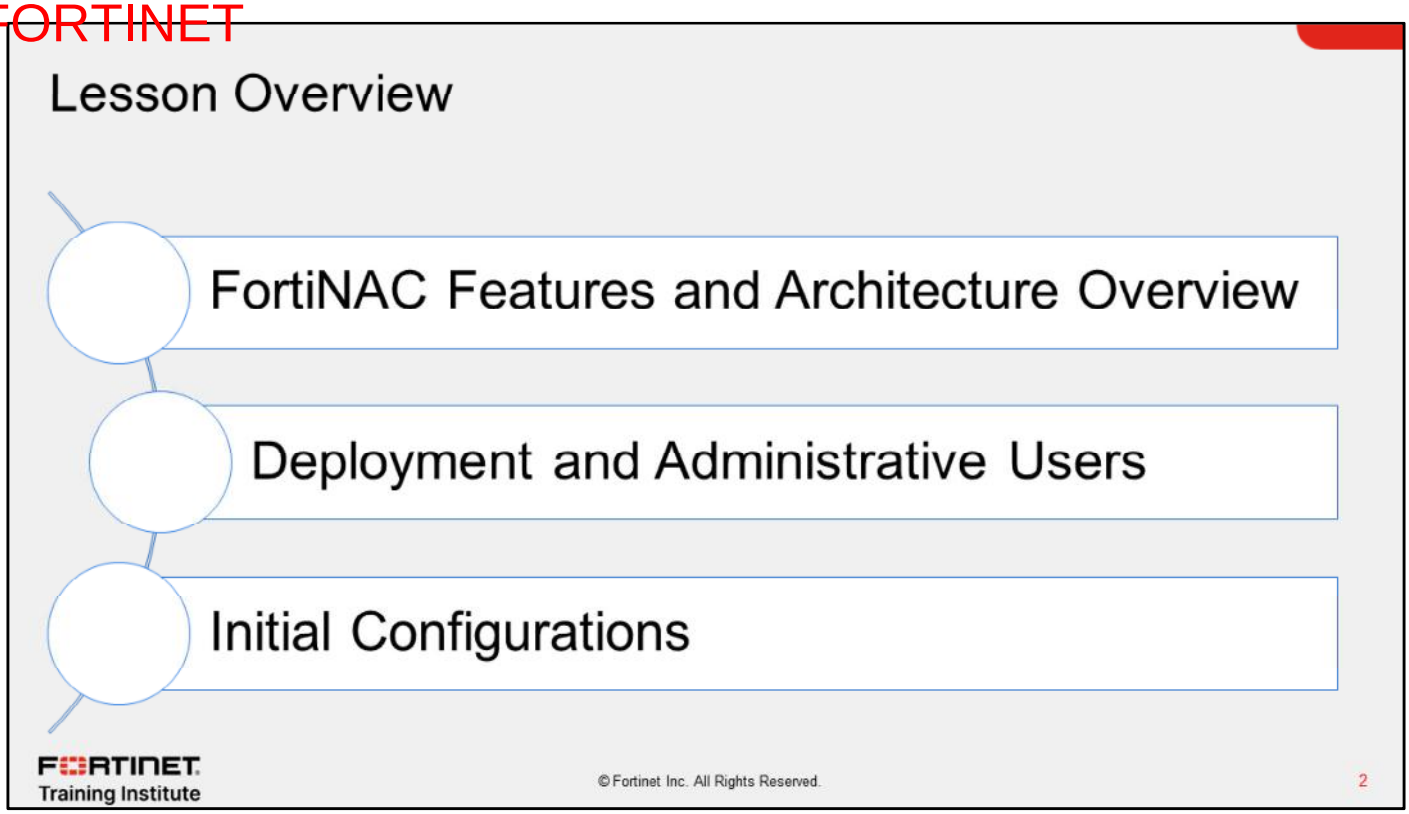
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will be introduced to FortiNAC and learn about the FortiNAC architecture, some initial configurations, and the administrative user interface framework. You will also learn about administrative users—how to set them up and delegate specific capabilities to them.

Vouchers & Dumps are Available | WhatsApp +201224560923

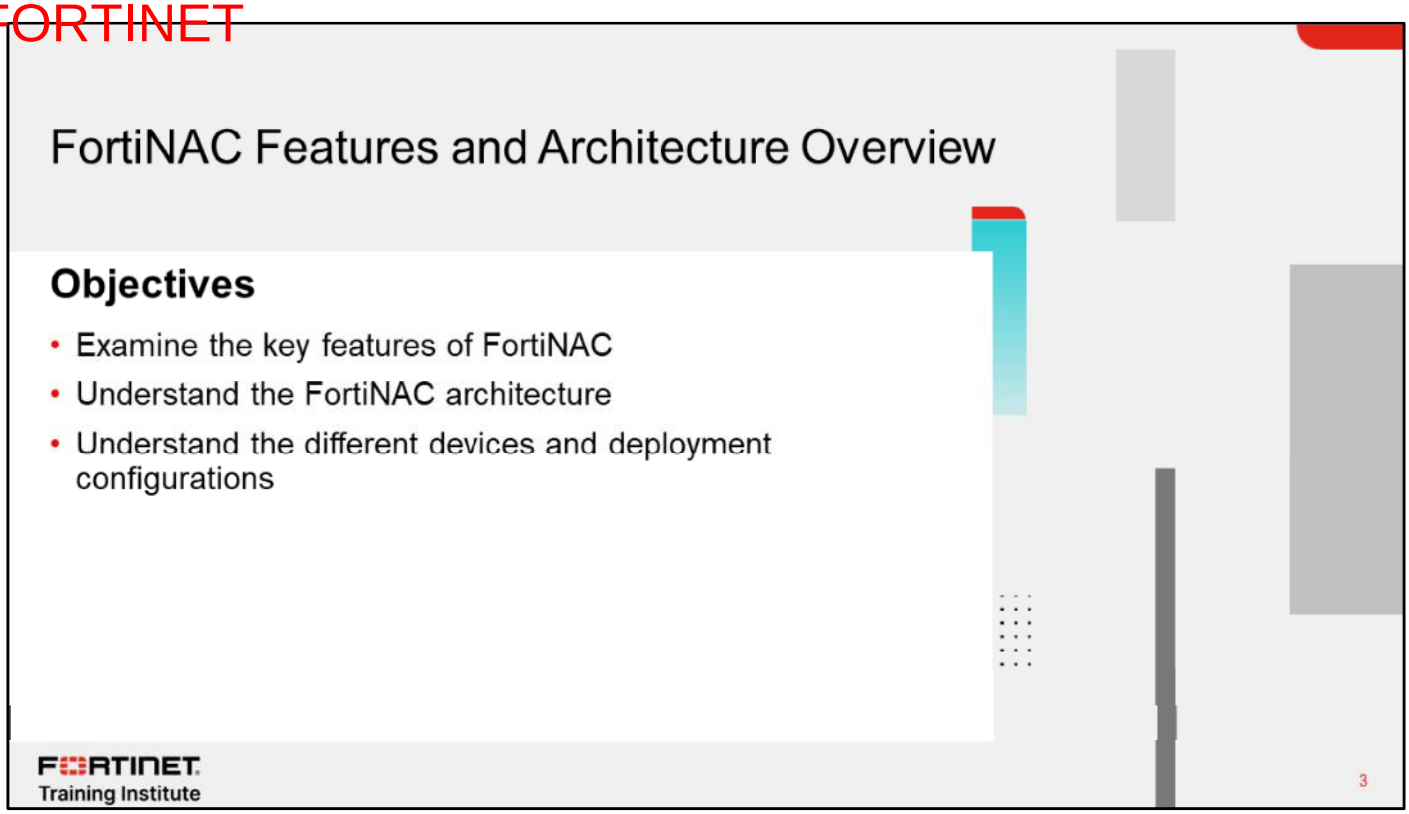
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

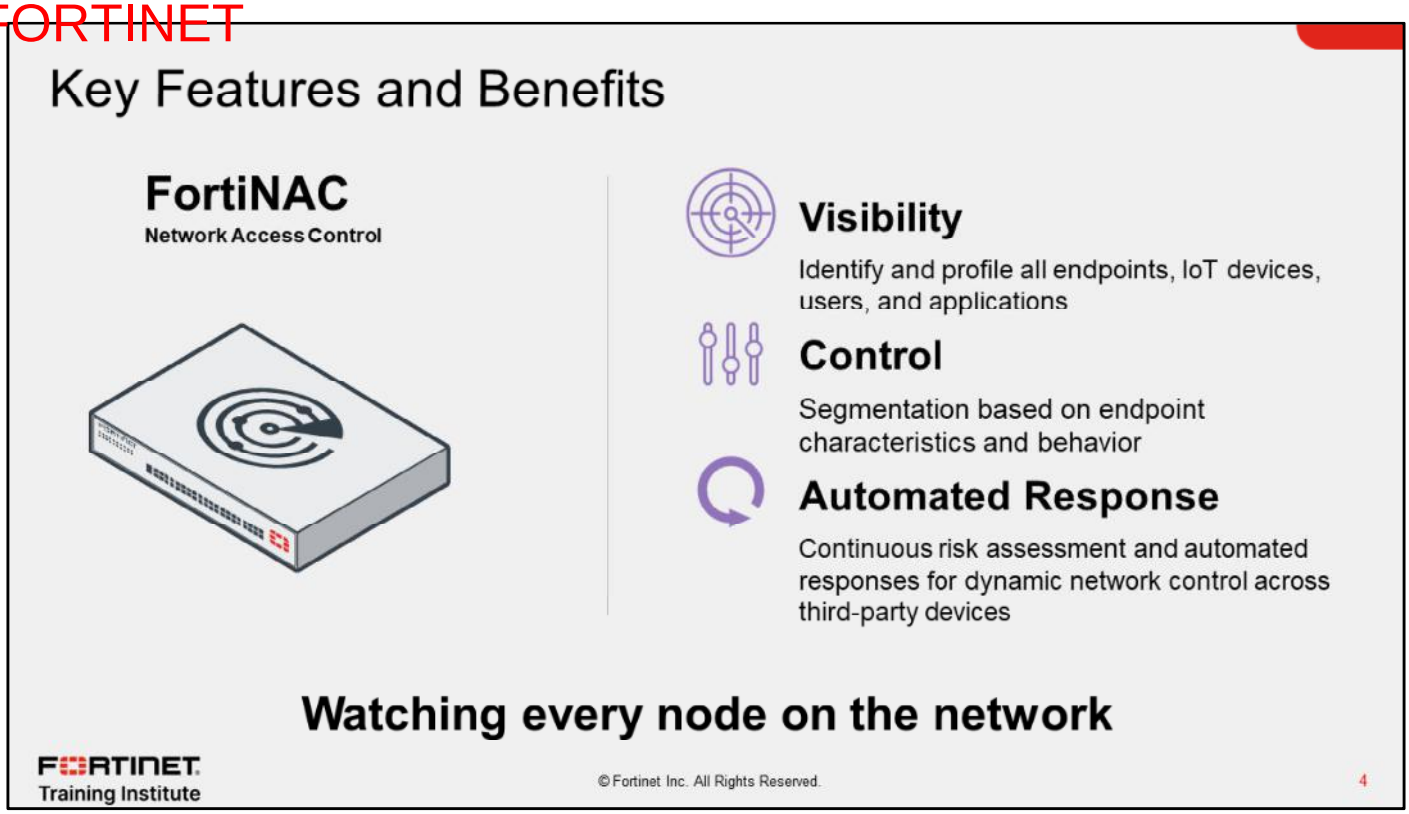


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of the FortiNAC architecture and initial configurations, you will be able to make appropriate decisions about FortiNAC deployment needs and options.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiNAC provides three pillars of comprehensive network security: visibility, control, and automated response.

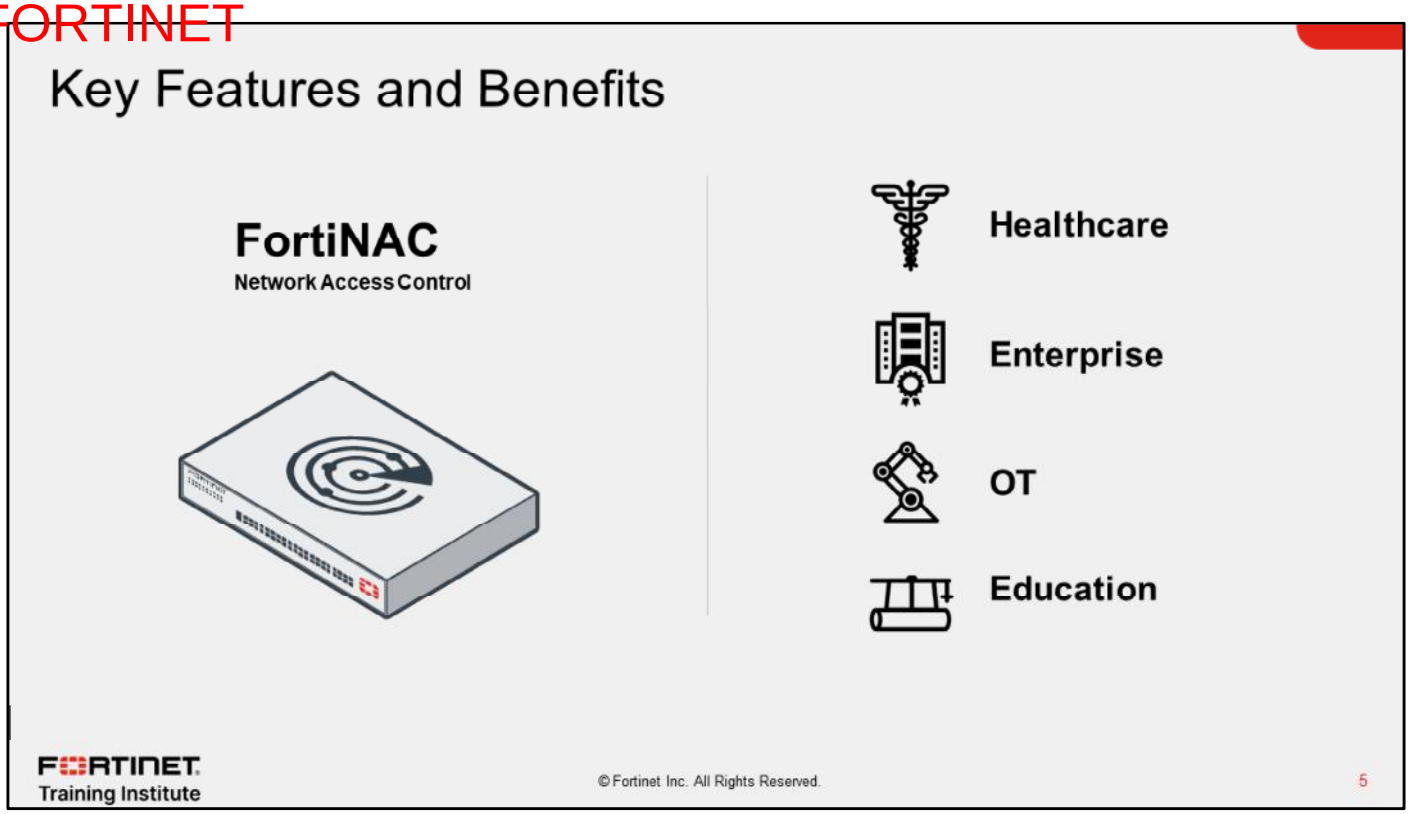
Visibility identifies and classifies all endpoints connected to the network. A complete, real-time inventory of who and what is connected, or has been connected, provides the foundation of control and response capabilities.

FortiNAC integrates with network infrastructure, providing control-like segmentation (VLAN assignment or custom configurations) and network access. The powerful combination of visibility and control ensures only trusted devices gain access to the network, and those devices are provisioned with only the access they need.

Automated response capabilities are achieved with the integration of security devices and systems, and the creation of response work flows. FortiNAC can receive real-time threat intelligence, and combining that with real-time visibility and control, instantly mitigate identified security threats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The flexibility built into FortiNAC provides a comprehensive security solution that can be applied across virtually every industry.

Enterprise customers leverage these capabilities to monitor assets, protect their networks, endpoints, data, and users. They provision endpoints appropriately and instantly respond to threats, preventing the spread of malicious software or data breaches.

Healthcare environments use these capabilities to ensure HIPAA compliance and to safeguard patient access.

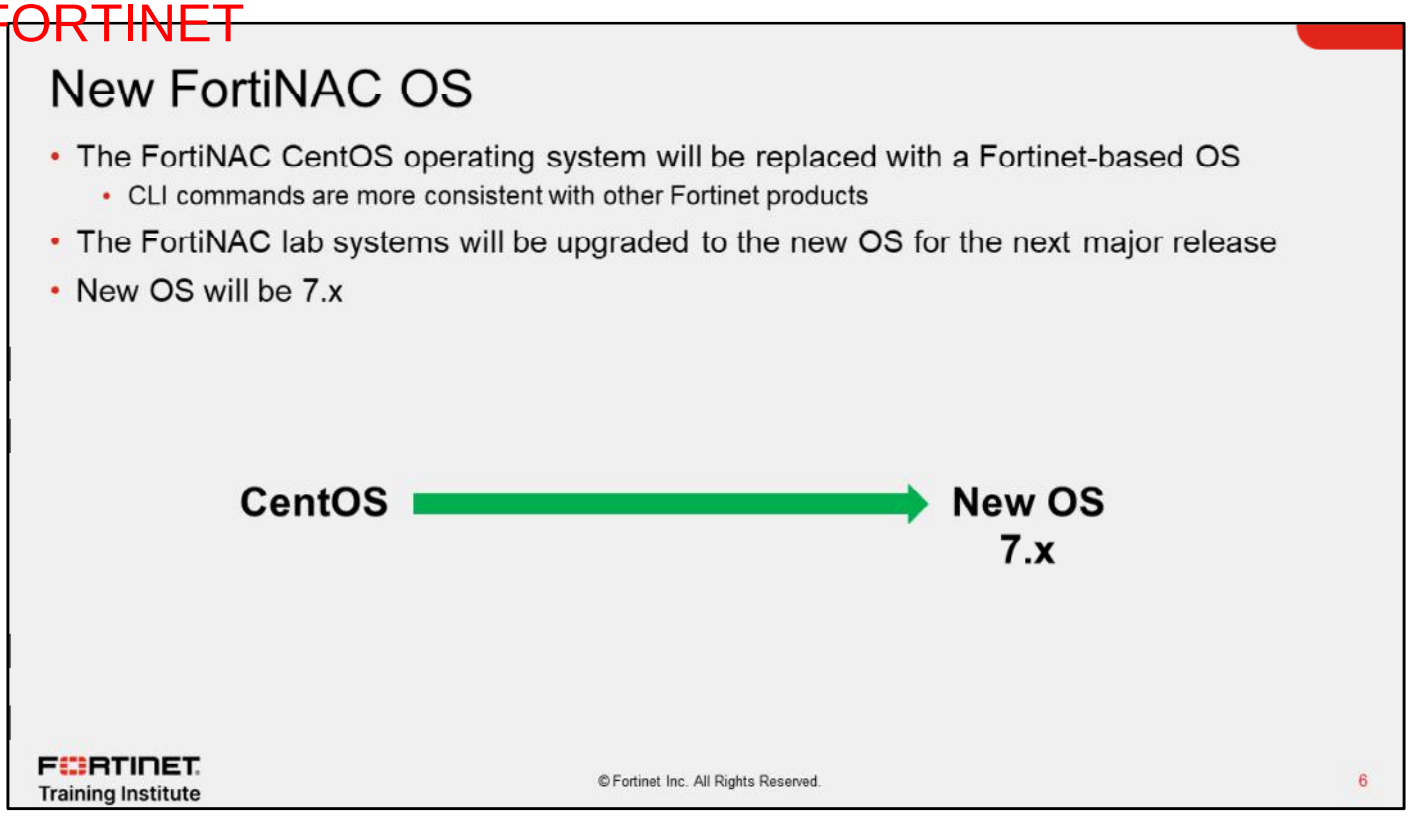
OT environments are extremely specialized, often with a diverse array of network-connected endpoints. FortiNAC can achieve visibility of endpoints passively, very often a requirement in these environments, and provides the flexibility to identify specialized endpoints, such as robotics, used on a manufacturing floor, or valve controls on an oil rig.

Education environments focus on provisioning and managing vast numbers of diverse BYOD devices, such as TVs, gaming consoles, phones, and so on. FortiNAC can allow students to onboard and manage their own devices.

These are just a few common examples.

Vouchers & Dumps are Available | WhatsApp +201224560923

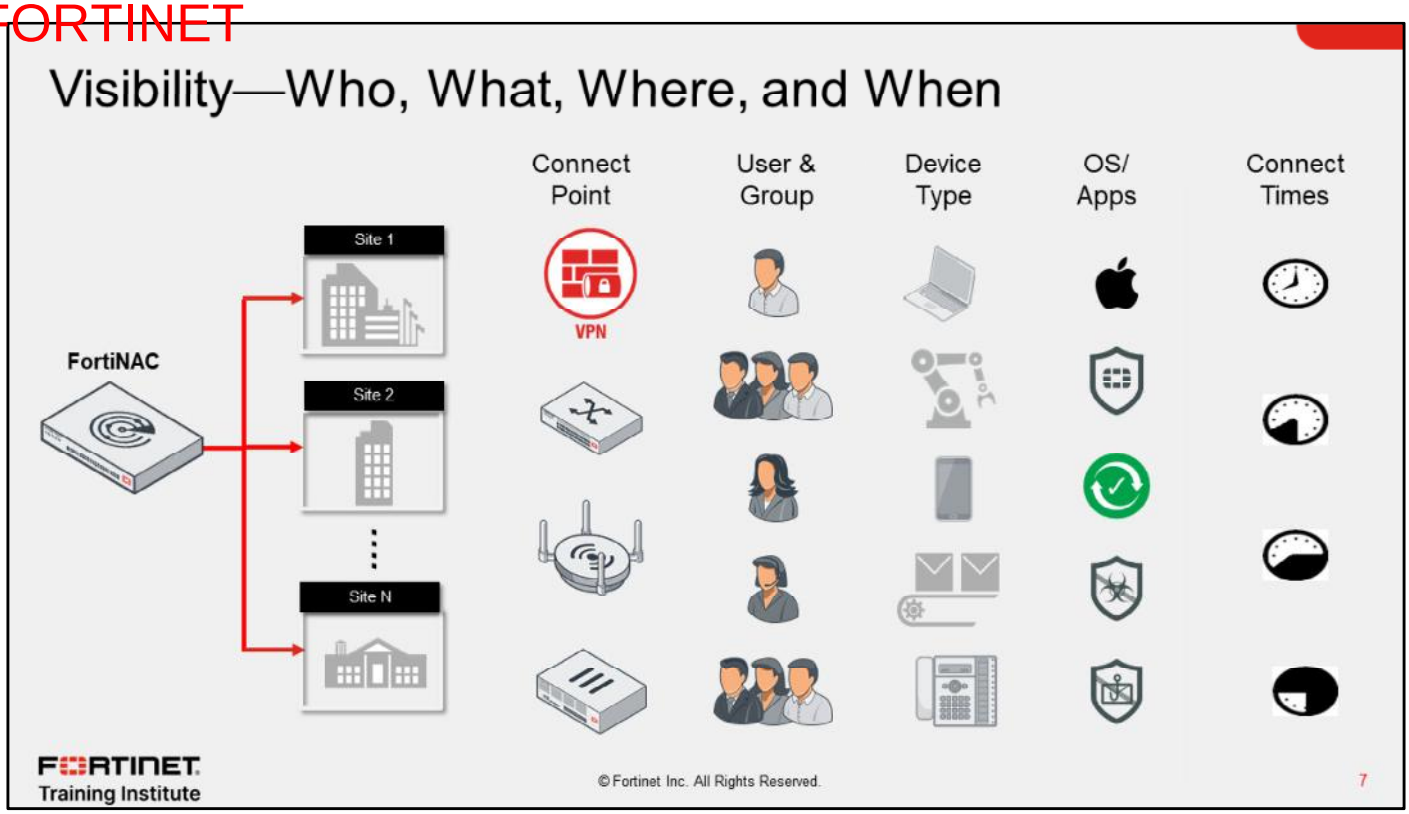
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The legacy CentOS, which has been the foundation of the FortiNAC OS, will be replaced with a Fortinet OS. This upgrade will make FortiNAC more consistent with existing Fortinet products, and features a new FortiOS-style CLI interface. The new OS will have updated versioning beginning with the 7.X release.

Vouchers & Dumps are Available | WhatsApp +201224560923

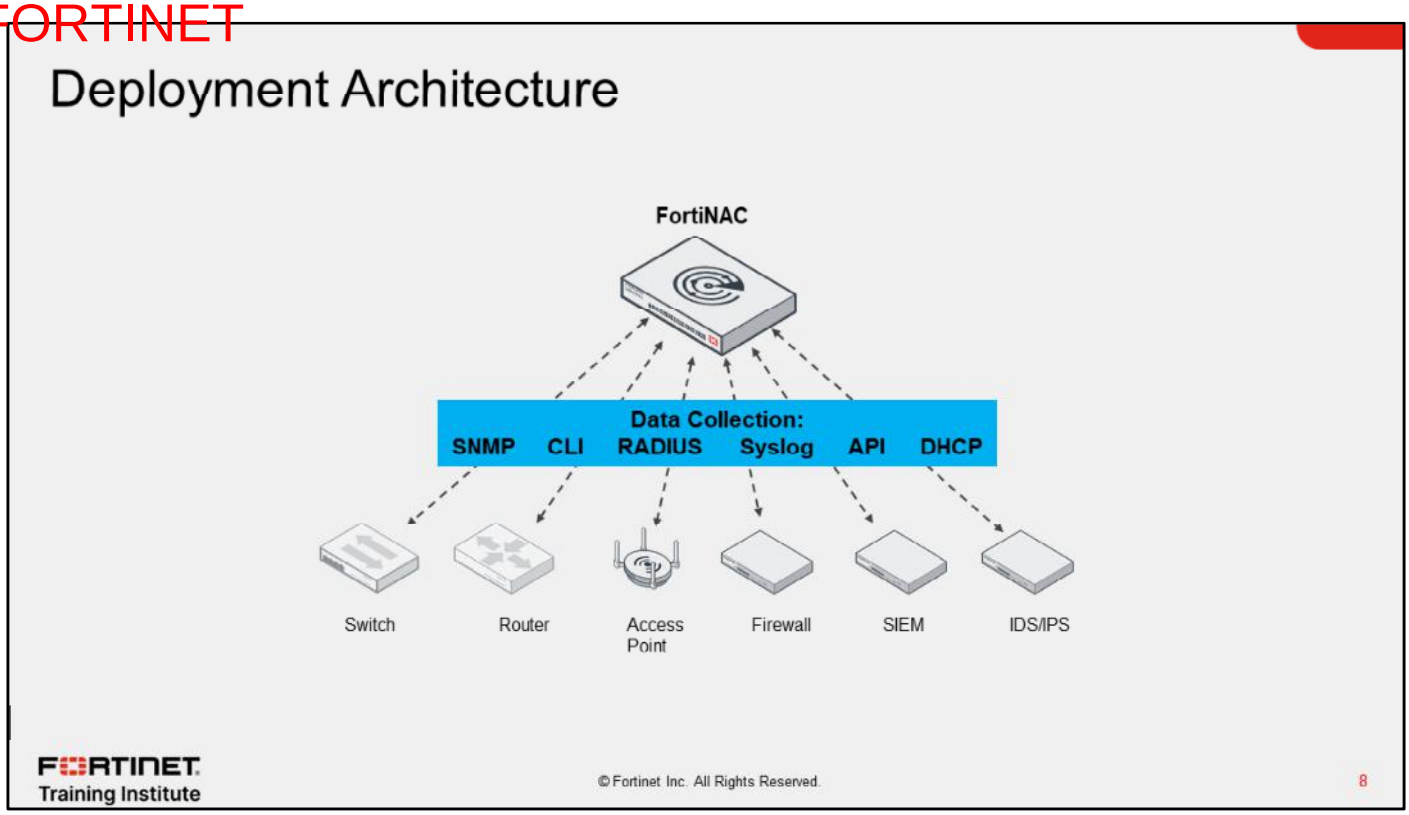
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can deploy FortiNAC as a physical device or as a virtual machine. FortiNAC communicates with infrastructure devices, such as wireless controllers, autonomous APs, switches, routers, and others. Because these infrastructure devices are inline, they can detect connected devices and connecting endpoints. They send this information back to FortiNAC, or FortiNAC gathers this information from them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



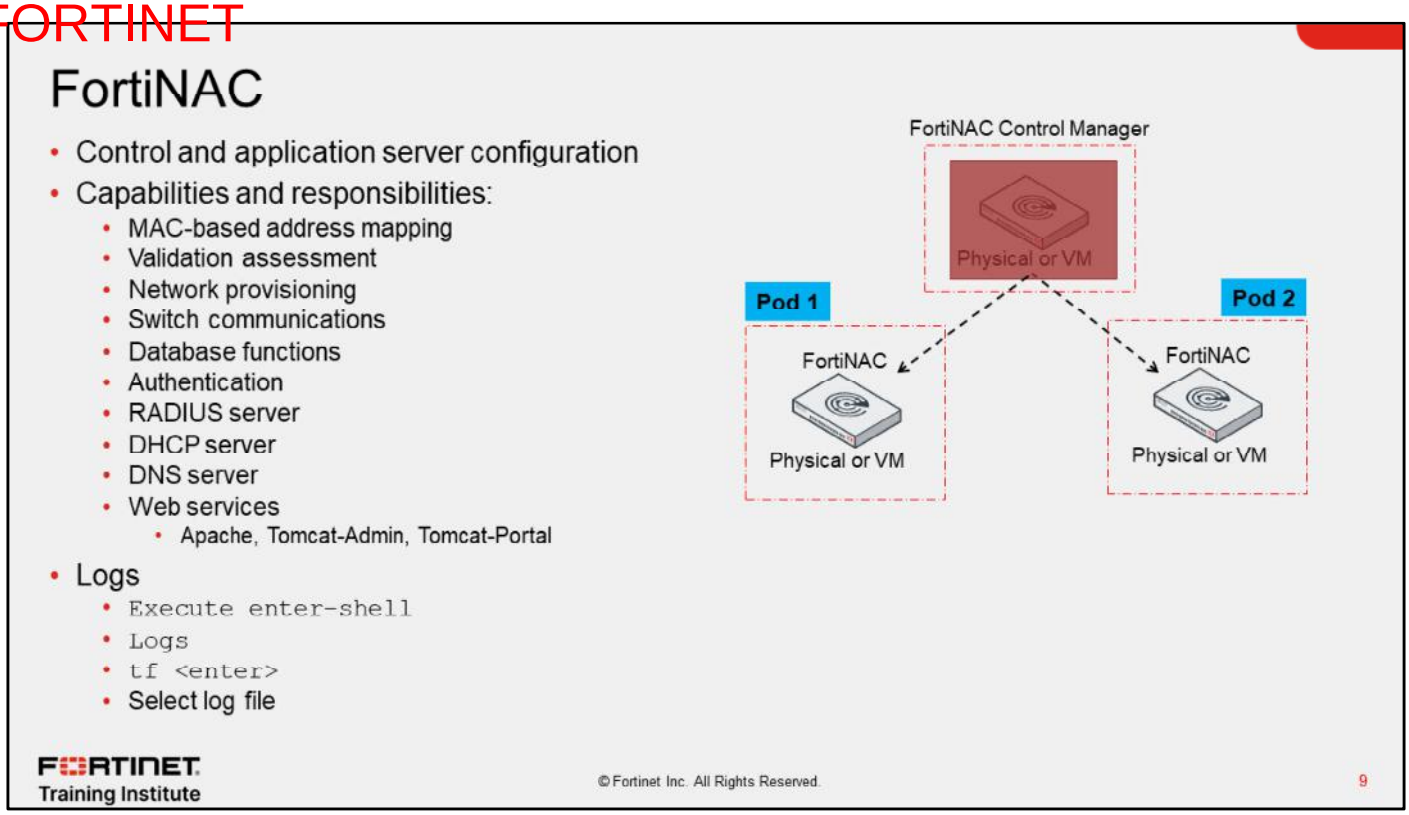
FortiNAC uses a variety of methods to communicate with and gather information from the infrastructure:

- FortiNAC uses SNMP to discover the infrastructure, complete data collection, and perform ongoing management.
- SSH or Telnet through the CLI is commonly used to complete tasks related to the infrastructure. For example, FortiNAC can use SSH to connect to a device and issue commands to gather visibility information or execute control functions.
- FortiNAC can also use RADIUS across a wired or wireless connection, to gather visibility information and control access.
- FortiNAC uses syslog to stay up-to-date on visibility details, such as hosts going offline. Syslog can also provide security device integration, giving FortiNAC the ability to log and react, if configured to do so, when it receives a security alert.
- Depending on the vendor of the infrastructure device, FortiNAC may leverage available API capabilities to enhance visibility and enforce control.
- FortiNAC can use DHCP, typically through fingerprinting, to identify connected devices and gain enhanced visibility.

The communication methods that FortiNAC uses depend on the vendor and model of the infrastructure device that FortiNAC is trying to integrate with. After FortiNAC knows the type of device it is communicating with, it determines and uses the appropriate methods and commands to gather information and maintain control.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiNAC leverages the built-in capabilities shown on this slide to maintain real-time visibility, and to enforce control and isolation responsibilities.

Some of the principle capabilities and responsibilities are:

- MAC-based address mapping: FortiNAC keeps track of where all the components in the network are connected. For example, if a laptop has a wired connection to switch 7 on port 5, or a wireless connection to an SSID, FortiNAC would have that information.
- Validation assessment: FortiNAC can provide endpoint compliance policy scanning using agents.
- Network provisioning: Network provisioning is a big part of what FortiNAC does. Security policies can automatically provision network access based on the who, what, when, and where information that it collects.
- Infrastructure communications: FortiNAC adjusts or changes the infrastructure configuration, as required, to ensure that all endpoints get appropriate access.
- Database functions: All the data that is collected about the infrastructure—visibility information, configuration details, adjustment, and so on—are stored in the FortiNAC database.
- Authentication services: FortiNAC performs authentication services, such as validating administrative users against Active Directory or the local database.
- RADIUS server: FortiNAC handles all RADIUS communications. Any wireless authentication or integration with a wireless controller uses the RADIUS server.
- DHCP and DNS servers: FortiNAC will act as the DHCP and DNS servers for hosts that have been isolated to a FortiNAC controlled captive portal network.
- Web services: Administrative users can access the administrative GUI through a Tomcat-Admin console.

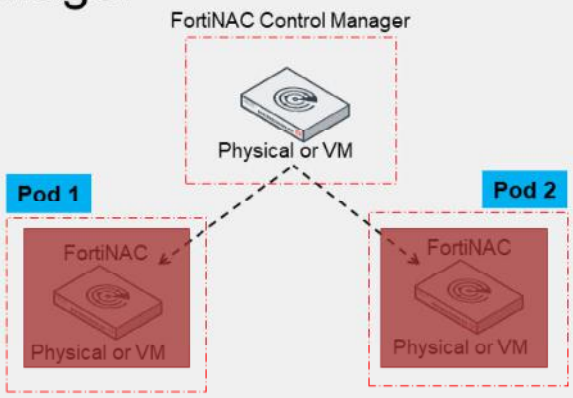
Output related to many FortiNAC functions is collected in log files that you can view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiNAC Network Control Manager

- Features and functionalities:
  - Seamless, network-wide registration
  - Global user identity database
  - Global version control
  - Global element management
  - Scalability
  - Web services
    - Tomcat-Admin



FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.
10

When deployed as a network control manager, FortiNAC manages other FortiNAC devices.

In the example shown on this slide, there are two FortiNAC servers deployed. This type of configuration could be deployed in an environment that is very large or geographically diverse. In any configuration that requires multiple FortiNAC devices, a FortiNAC network control manager is recommended. The network control manager ties together multiple FortiNAC devices in a distributed environment to allow for seamless, network-wide registrations, management, and visibility. For example, when a device is registered in a location that's managed by one FortiNAC, and then moves to a location managed by another, the move is seamless to the end user because the device is known and trusted in the first location and also known and trusted in the second location. The global user identity database combines select database elements from the distributed locations to make a single global database on the network control manager. It offers version control, so upgrades to the control manager can be distributed to all of the managed FortiNAC devices.

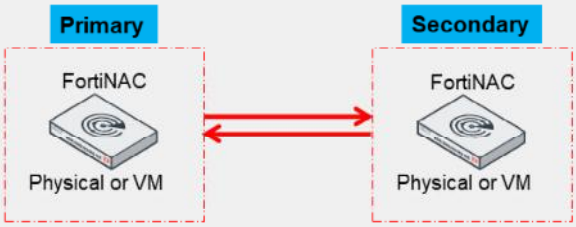
An additional capability is global element management. You can manage security policies, group management, and logical networks through the network control manager, and those changes or configurations can be pushed down to the FortiNAC devices. Synchronization can also be upstream from a managed FortiNAC, meaning work done at an individual FortiNAC level can be pushed up to the network control manager, and then the network control manager can distribute those changes to the other FortiNAC devices. This offers scalability for large deployments, so distributed management can fall back under a single user interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiNAC High Availability Deployment

- You can configure two FortiNAC devices (physical, virtual, or a combination) as an active-passive HA pair
- Database and configuration file replication keep the devices synchronized
- Administrative and control capabilities are maintained in the event of a failure
- Primary device fails over to a secondary device automatically
- Restoring control to a primary that has failed over is manual



FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.
11

For redundancy purposes, you can deploy FortiNAC in a high availability (HA) configuration. When configured in an HA configuration one FortiNAC device is designated the primary and the other is designated the secondary. After the initial configuration is complete, work is performed on the primary, and changes to the database and configuration files are synchronized with the secondary device. If the primary device or the means by which it connects to the network fail, the secondary device will assume control automatically. Restoration of a failed-over HA deployment is a manual process performed by an administrator.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which FortiNAC device provides DNS services?
   - ✓ A. The FortiNAC control and application server
   - B. The FortiNAC network control manager

2. How does FortiNAC know the point of connection for a host?
   - A. Through the GUI by an administrative user
   - ✓ B. Through communication with the network infrastructure

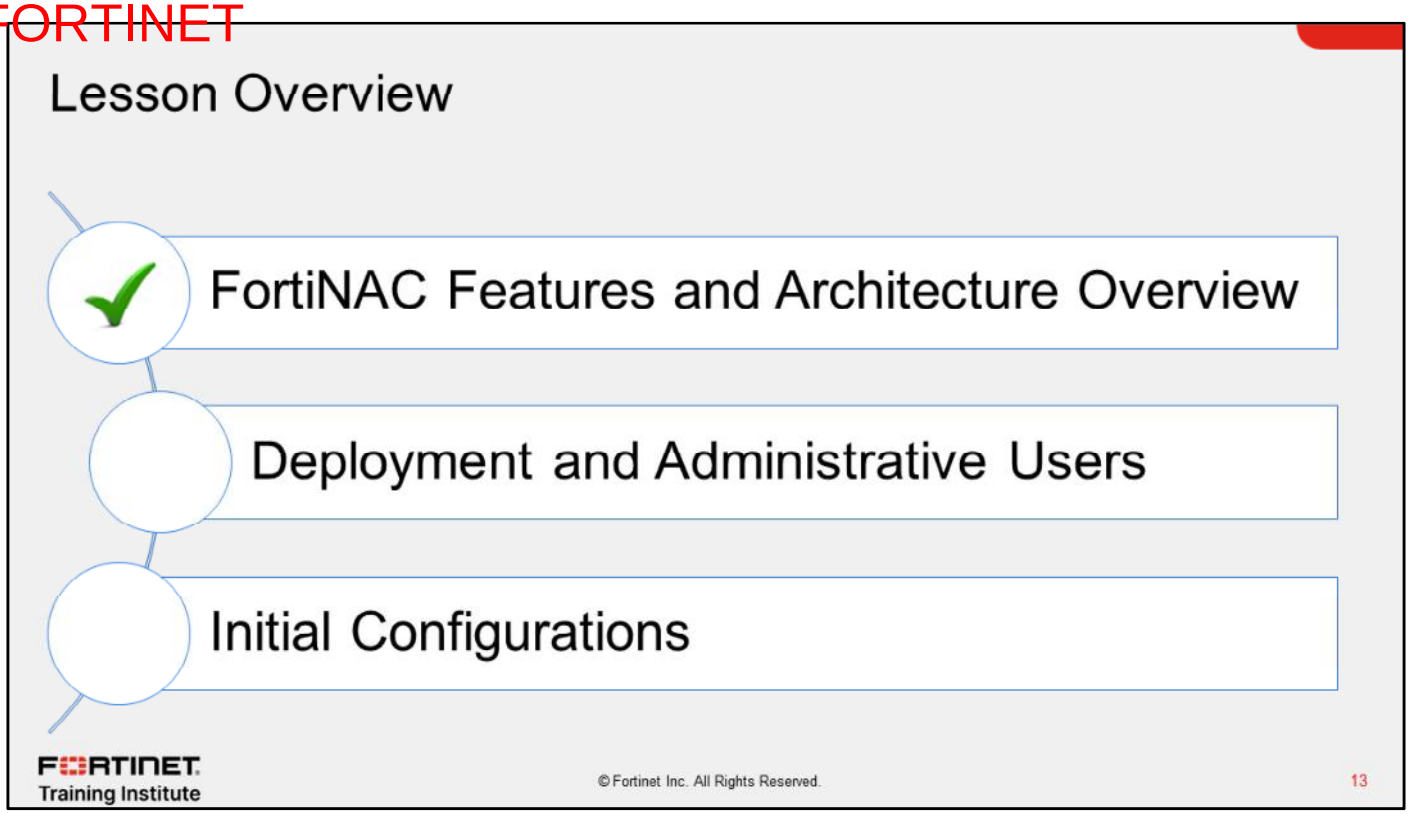
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

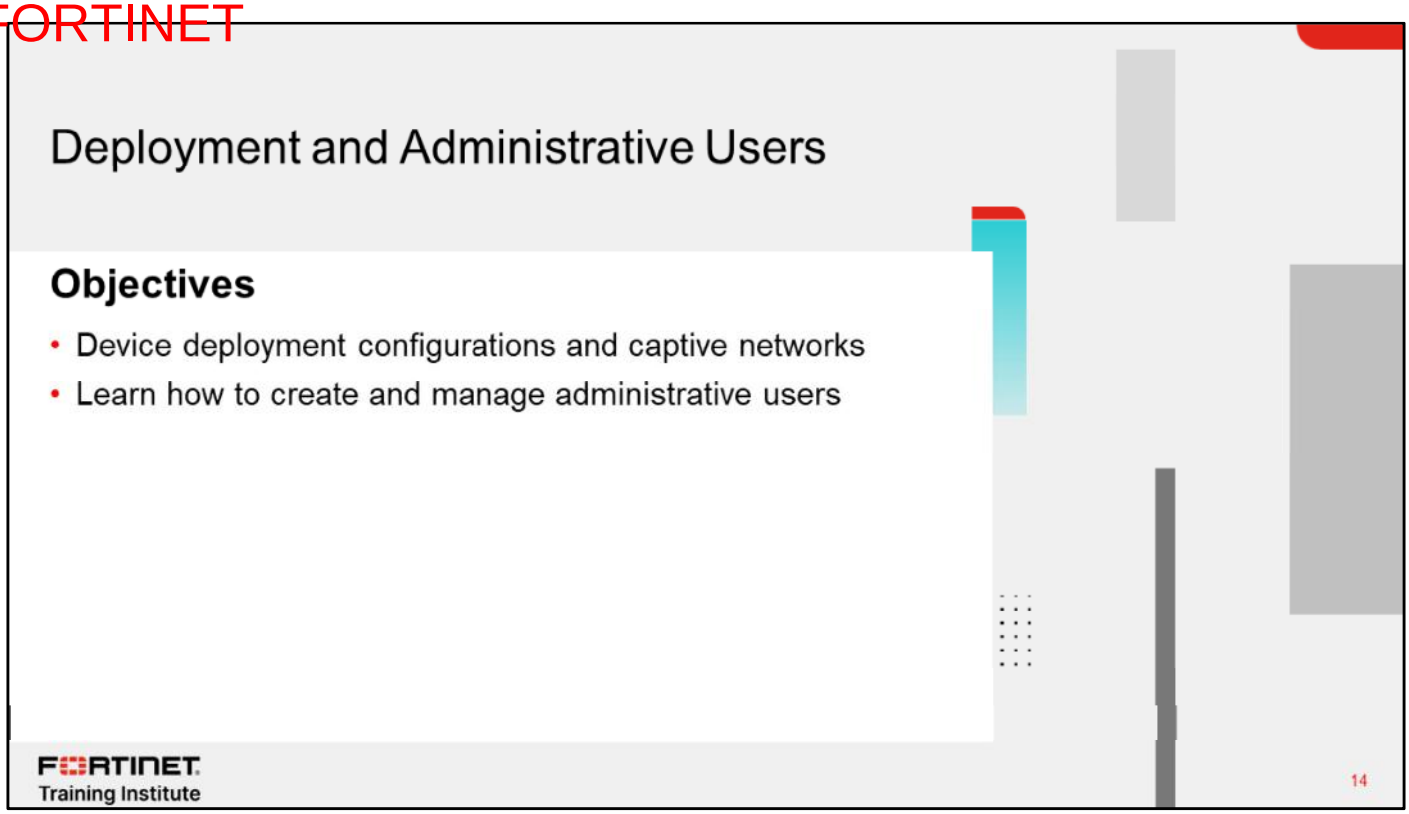


Good job! You now have a basic understanding of FortiNAC and the FortiNAC architecture.

Now, you will learn about the deployment and administrative users of a FortiNAC device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring the necessary initial deployment settings, understanding basic captive network operation, and creating and managing administrative users, you will be able to make informed decisions on FortiNAC deployment considerations in your environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Initial IP Configuration—Virtual Machine

- Install and power on the FortiNAC virtual machine
- Assign network interfaces
- Access the FortiNAC console and log in with the default CLI credentials
- Set the management interface IP address, mask, and gateway using the following commands:

```
config system interface
     edit port<#>
          set ip <ip address/mask>
          set allowaccess http-alt https-alt
     next
end
config system route
     edit 1
          set gateway <gateway IP address>
          set device <management interface port>
     next
end
```

- Validate the IP address by typing: `show system interface`
- Access the configuration wizard using a web browser by navigating to: `https://<management_IP_address>:8443/`

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

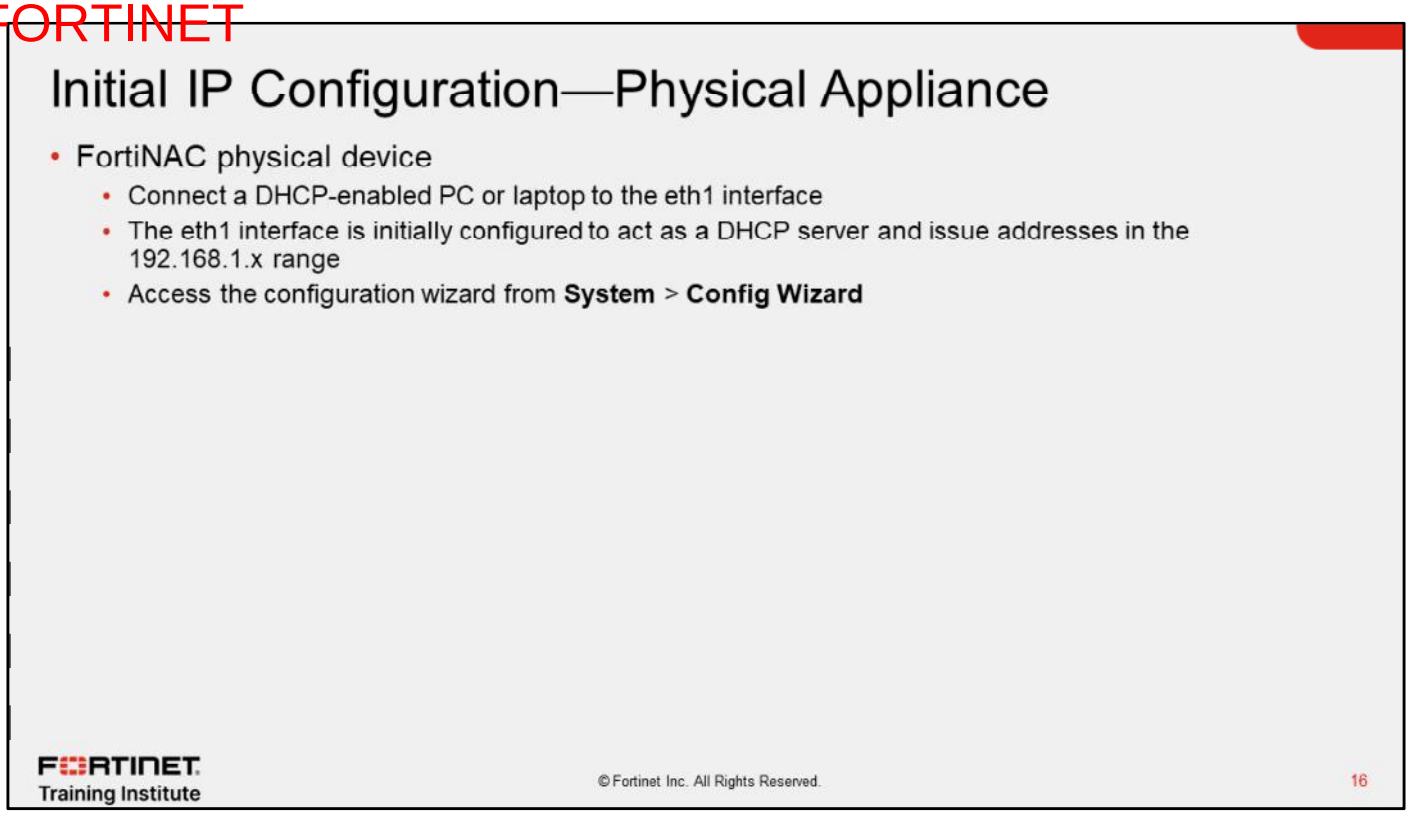
15

When you initially deploy a FortiNAC device, you must access the configuration wizard to make deployment setting configurations.

When deploying a virtual machine, you must assign the network interfaces to the appropriate networks and configure the management port IP address, mask, gateway, and allowed protocols for management access, as shown on this slide. You can validate the settings using the `show system interface` command. Access the configuration wizard using a web browser by entering the URL `https://<management_IP_address>:8443/`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

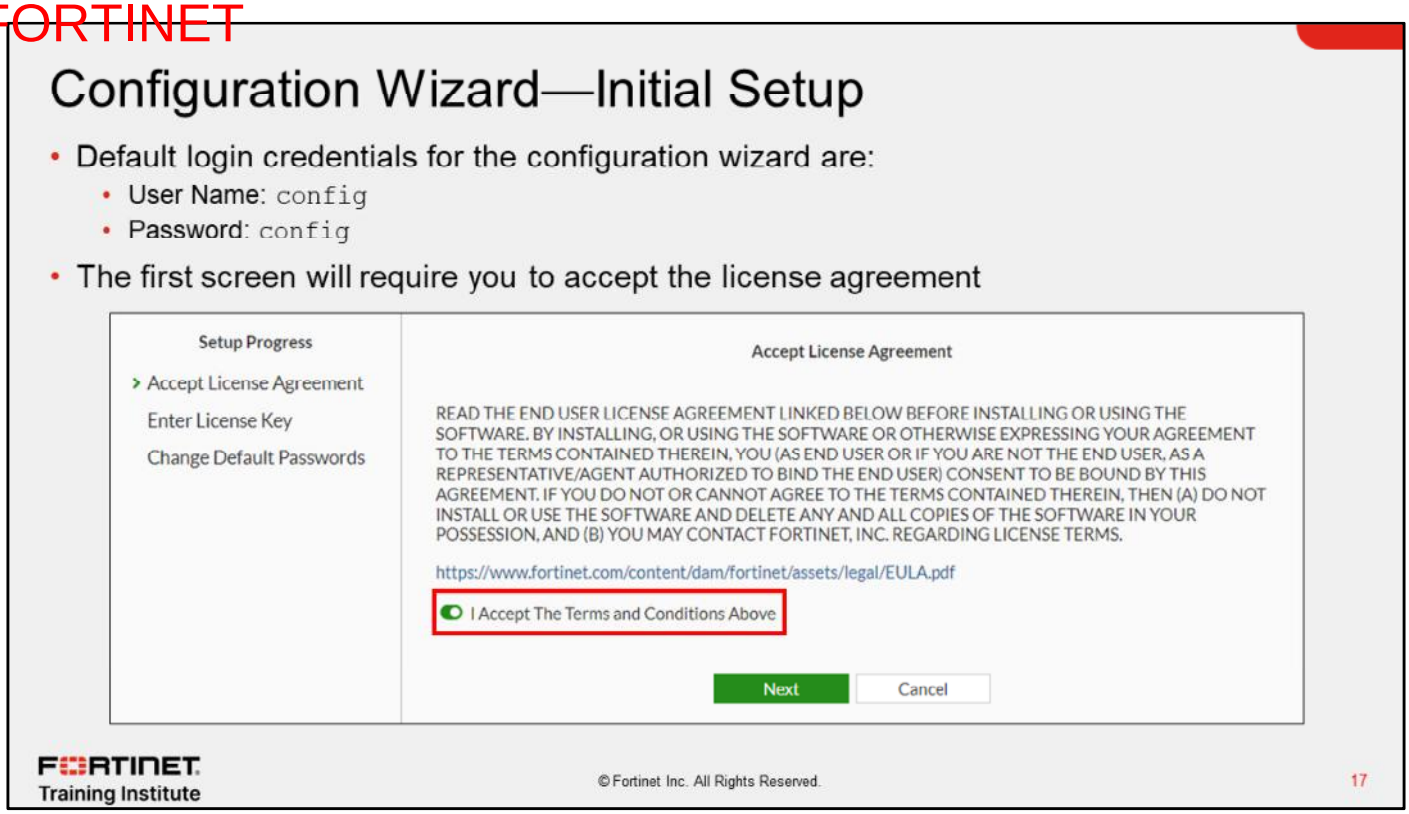


When deploying a physical device, you will configure the Ethernet 0 (eth0) interface IP address from the configuration wizard. After powering on the device, you will connect a DHCP-enabled system to the device interface labeled eth1. FortiNAC will assign an IP address in the 192.168.1.0/24 network. You can then access the configuration wizard from the administrative GUI.

You can access detailed deployment guides at docs.fortinet.com.

Vouchers & Dumps are Available | WhatsApp +201224560923

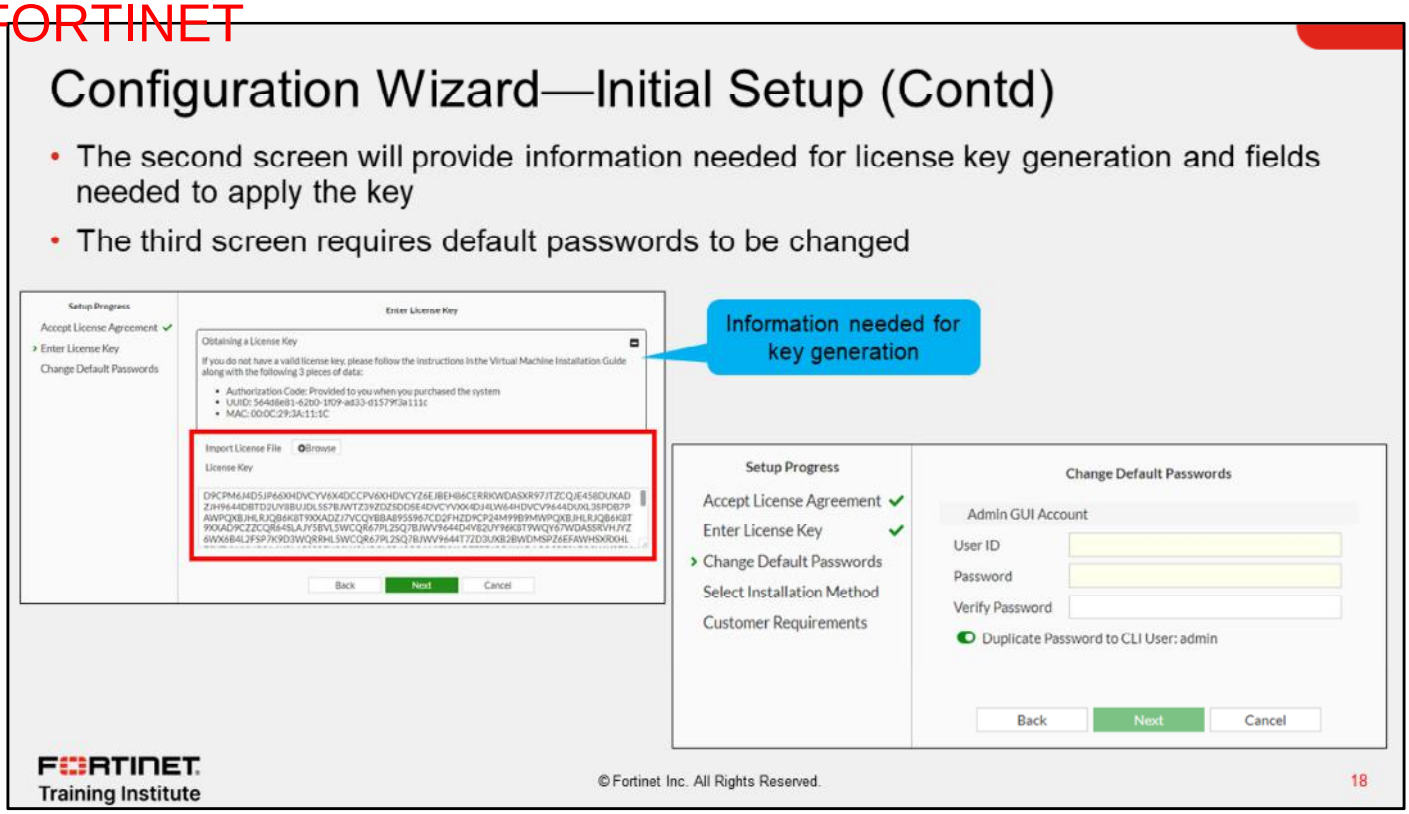
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The default username and password for access to the configuration wizard is `config`. The first configuration screen will present the license agreement and require the user to accept the terms and conditions of the license agreement before being able to proceed with the deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



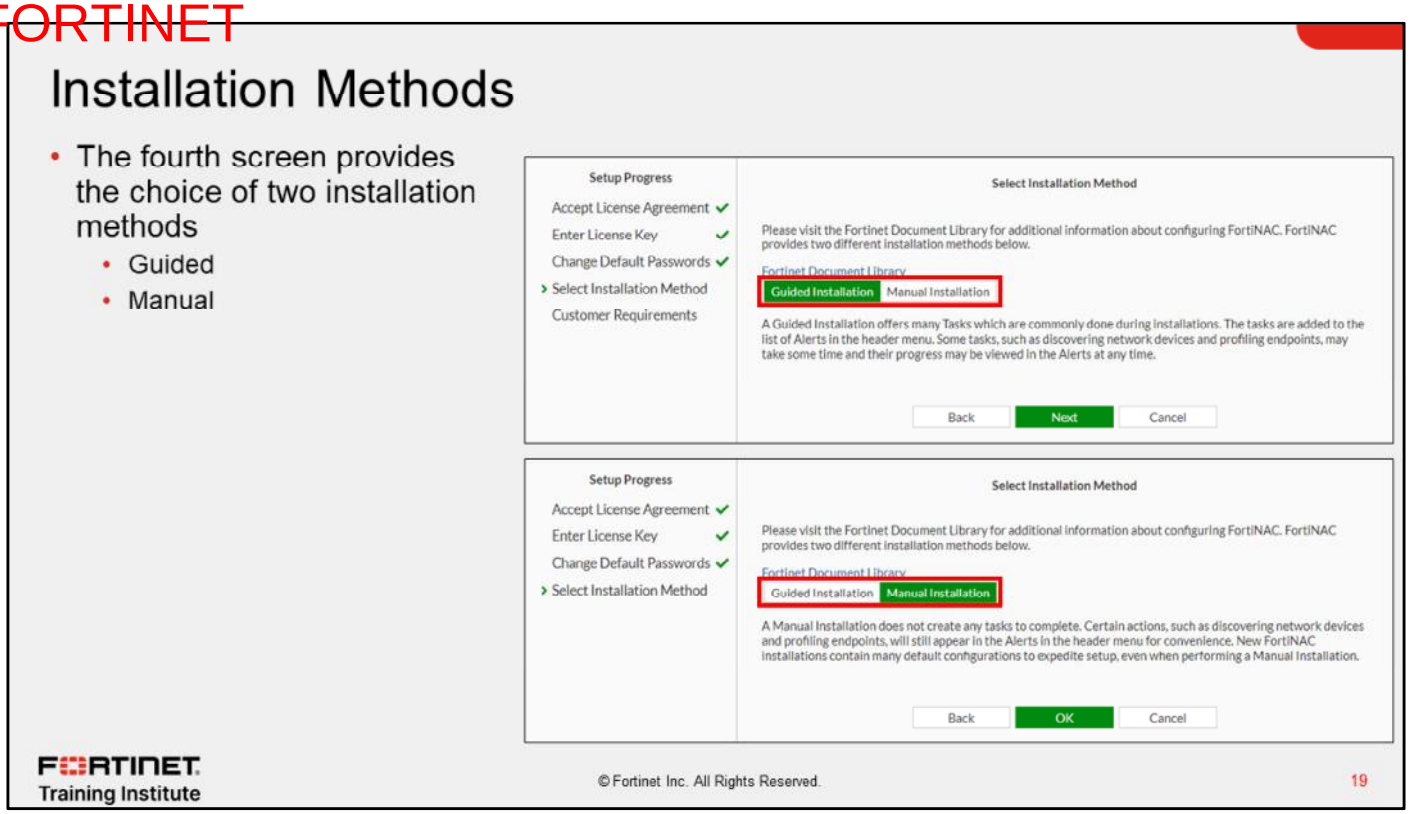
The second screen presents the necessary device-specific information needed to complete the Fortinet registration process and license key generation. You must upload a valid license key to continue.

The third screen is the **Change Default Passwords** page. You must define an administrator account for GUI access, and optionally, you can choose to have the same password you created for your GUI administrative account used for the `admin` CLI account.

Note that the GUI user ID does not have to be `admin`, but the CLI account is set by default to `admin`.

Vouchers & Dumps are Available | WhatsApp +201224560923

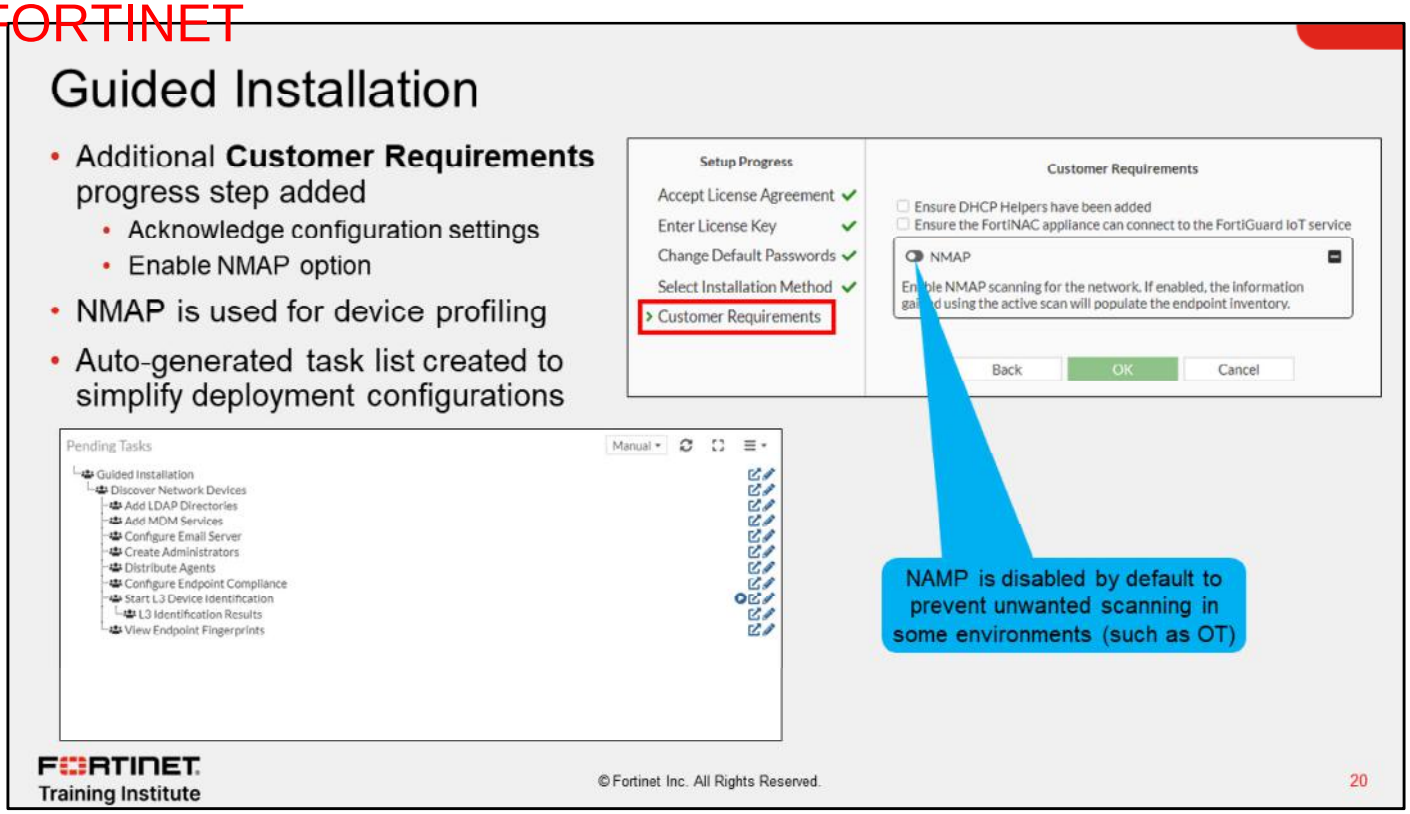
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The fourth screen is where you select the desired installation method. There are two installation method options: Guided and Manual.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

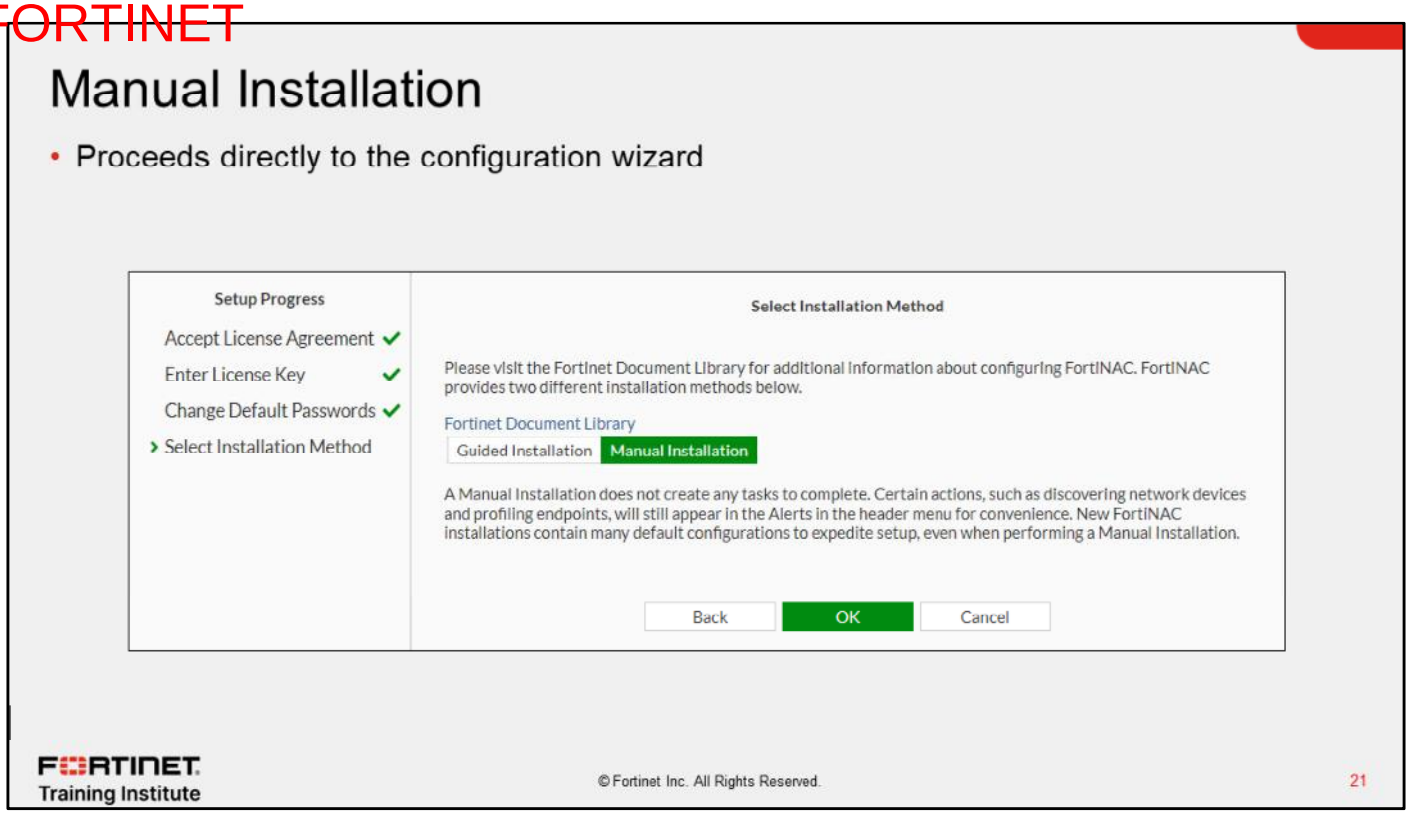


Selecting **Guided Installation** will add an additional **Customer Requirements** step. This forces the installer to acknowledge some important deployment configurations, and to choose to enable NMAP scanning for the network. NMAP scanning can be used by FortiNAC to gather visibility information and classify devices. Some environments do not allow NMAP scanning and performing them could trigger security alerts.

In addition to the customer requirements, FortiNAC will automatically generate a task list to assist with the tracking and assigning deployment responsibilities. You will learn about tasks later in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



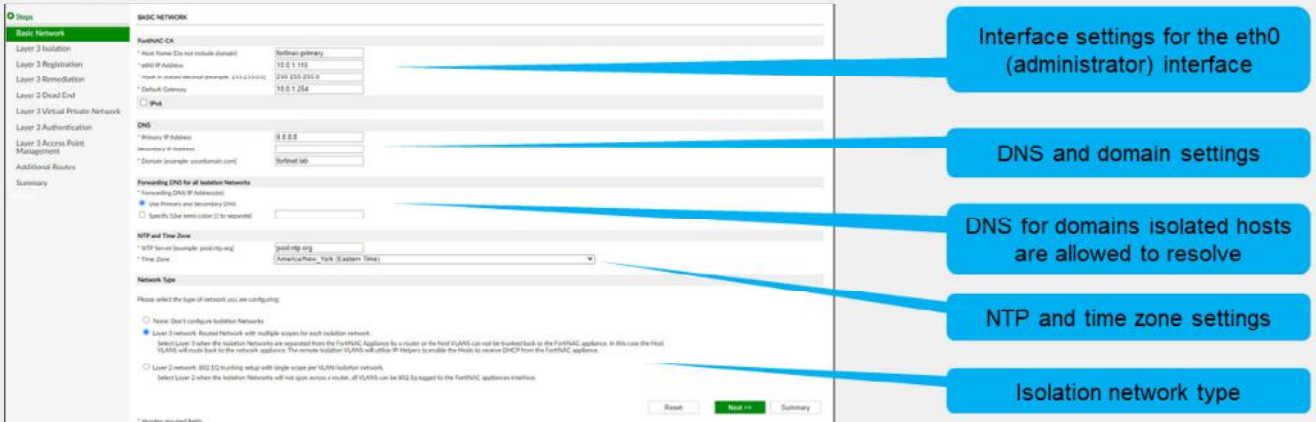
Select **Manual Installation** and click **OK** to go directly to the configuration wizard. A manual installation does not create installation tasks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuration Wizard—Basic Network

- The **Basic Network** configuration screen is where you configure the FortiNAC hostname, eth0 IP, mask, gateway, IPv6 details (optional), DNS information, forward DNS for isolation networks, NTP server, and time zone
  - The eth0 IP, mask, and gateway settings will already be set on VM appliances but may be changed here



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

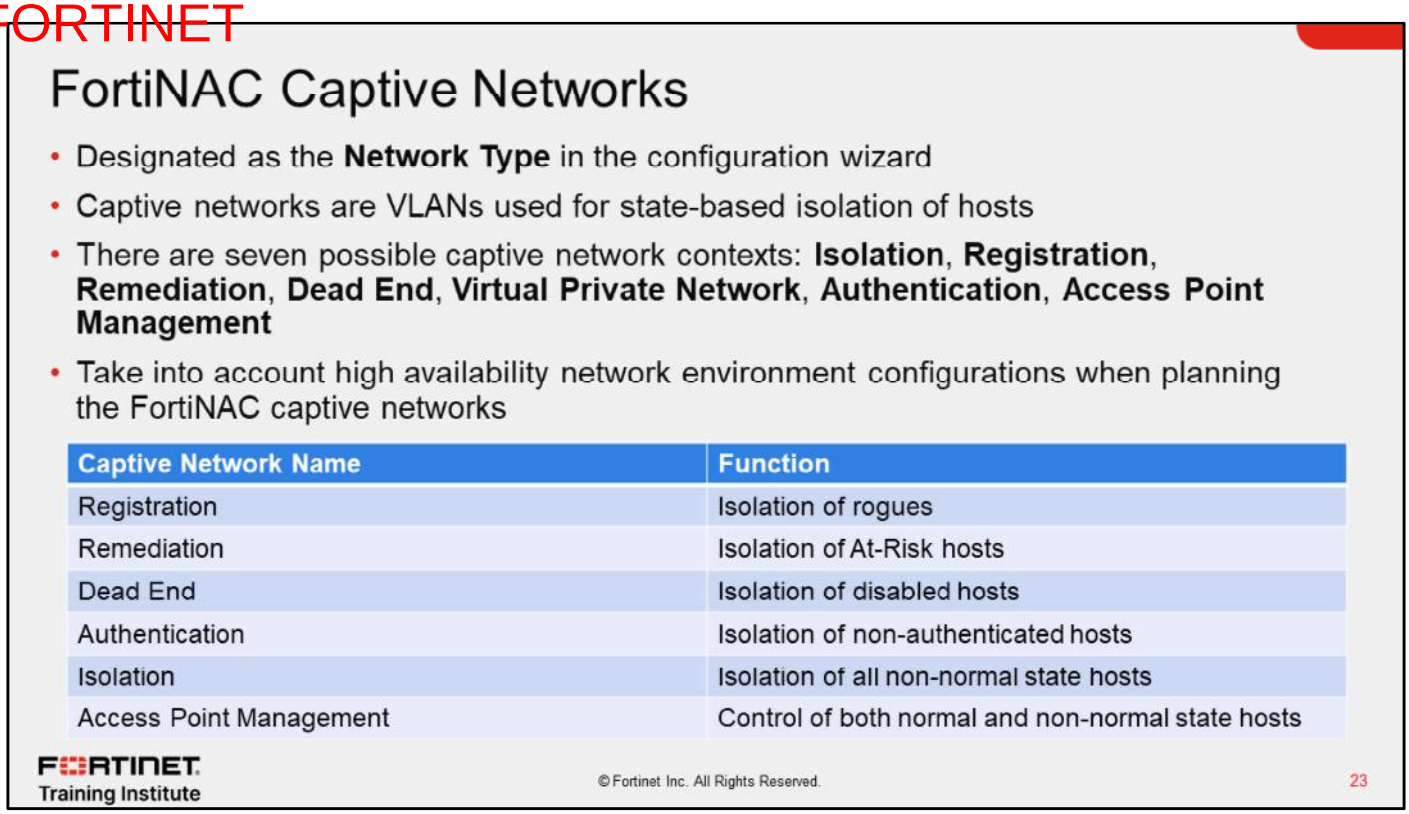
The **BASIC NETWORK** page is the first step of the configuration wizard. Here, you can configure the IP address, subnet mask, and default gateway for eth0. In a virtual machine deployment, the eth0 network settings are normally already completed using the `CLI` commands discussed earlier in this lesson. The primary and secondary DNS servers are configured here along with the FortiNAC domain.

The **Forwarding DNS for all Isolation Networks** settings are used by FortiNAC to resolve domains that have been added to an allowed list for hosts that are currently in a captive portal network. Details about how the captive portal networks operate will be covered in another lesson.

You will learn about the **Network Type** settings later in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiNAC captive networks are those networks used for the isolation of hosts, and the presentation of captive portals. You can provision hosts to captive networks for reasons that will be covered in another lesson.

There are seven different captive network contexts that can be defined in the configuration wizard: **Isolation**, **Registration**, **Remediation**, **Dead End**, **Virtual Private Network**, **Authentication**, and **Access Point Management**. The captive network contexts used will vary depending on need.

The **Network Type** designation in the configuration wizard will determine how the FortiNAC eth1 interface is configured, and define how host DHCP configuration will be performed by FortiNAC. For this reason, FortiNAC devices that will be deployed in a high availability configuration need to have the same network type designation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Layer 2 Network Type Captive Networks

- Each FortiNAC captive network (Registration, Remediation, and so on) will be configured as a single VLAN
- The FortiNAC captive networks interface will be configured as an 802.1Q interface with a sub-interface assigned to each configured FortiNAC captive network
- Each FortiNAC sub-interface will provide DHCP, DNS, and captive portal services for its associated captive network
- Consider network design for HA deployments using this network type



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

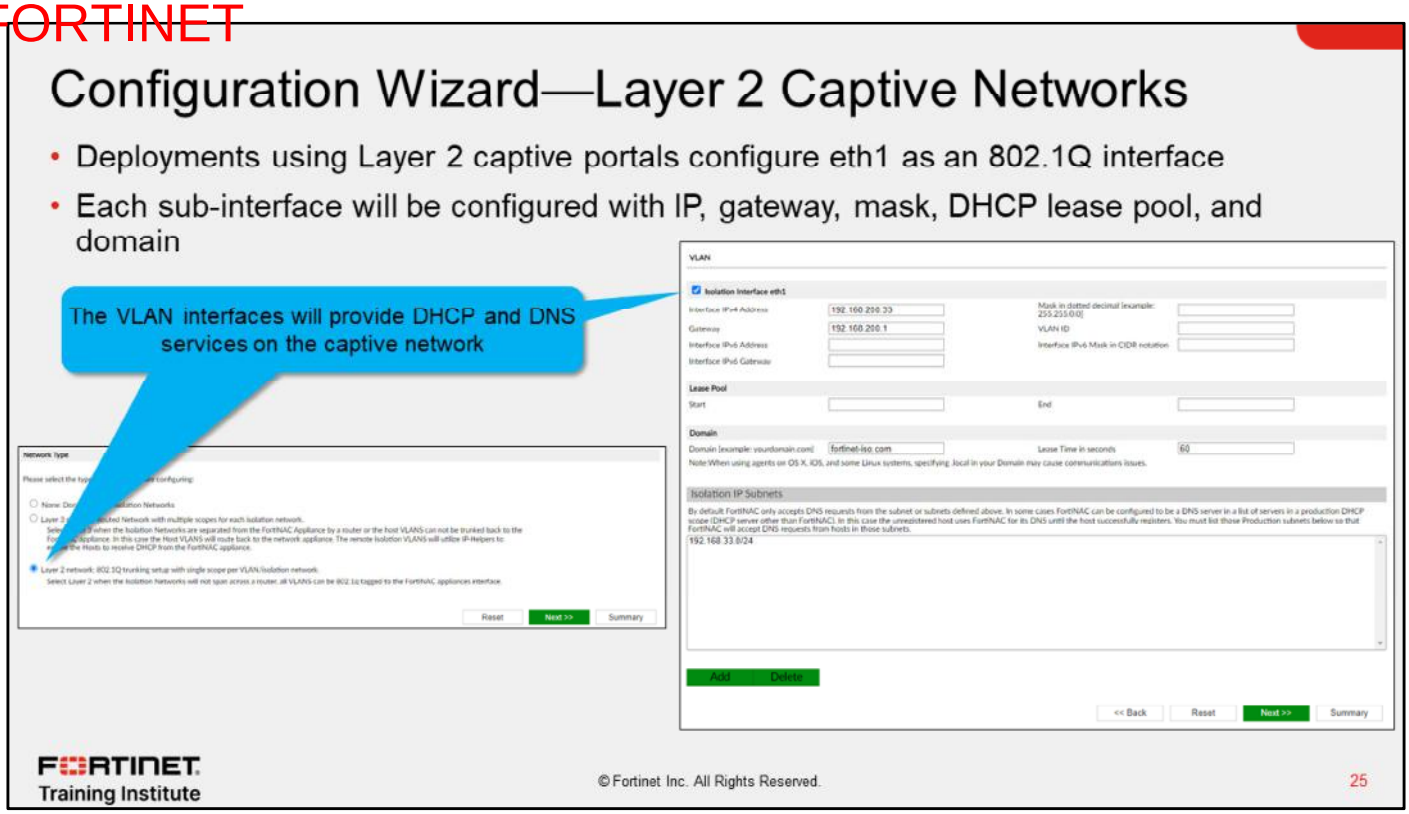
When selecting **Layer 2 network** in the configuration wizard **Network Type** section, the captive networks interface is configured as an 802.1Q interface, with a sub-interface assigned to each of the configured captive networks. The captive network is then configured as a single VLAN for each context (Registration, Remediation, Dead End, and so on) and FortiNAC provides DHCP services directly to the hosts provisioned to those networks. DNS and web services are provided by this interface.

When two FortiNAC devices are configured for high availability, each has sub-interfaces on each service network, so each service network VLAN is tagged back to each captive network interface. The interface on the device not in control is shut down by the HA process, and brought up only when the device assumes control.

Note that HA environments with the primary and secondary servers in separate locations and on different subnets might make it difficult to span the captive networks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The third step in the wizard is where you can designate the network type. This step, and almost all remaining steps, determine how the captive portal interface will function. These configurations are critical for proper host isolation and portal page presentation.

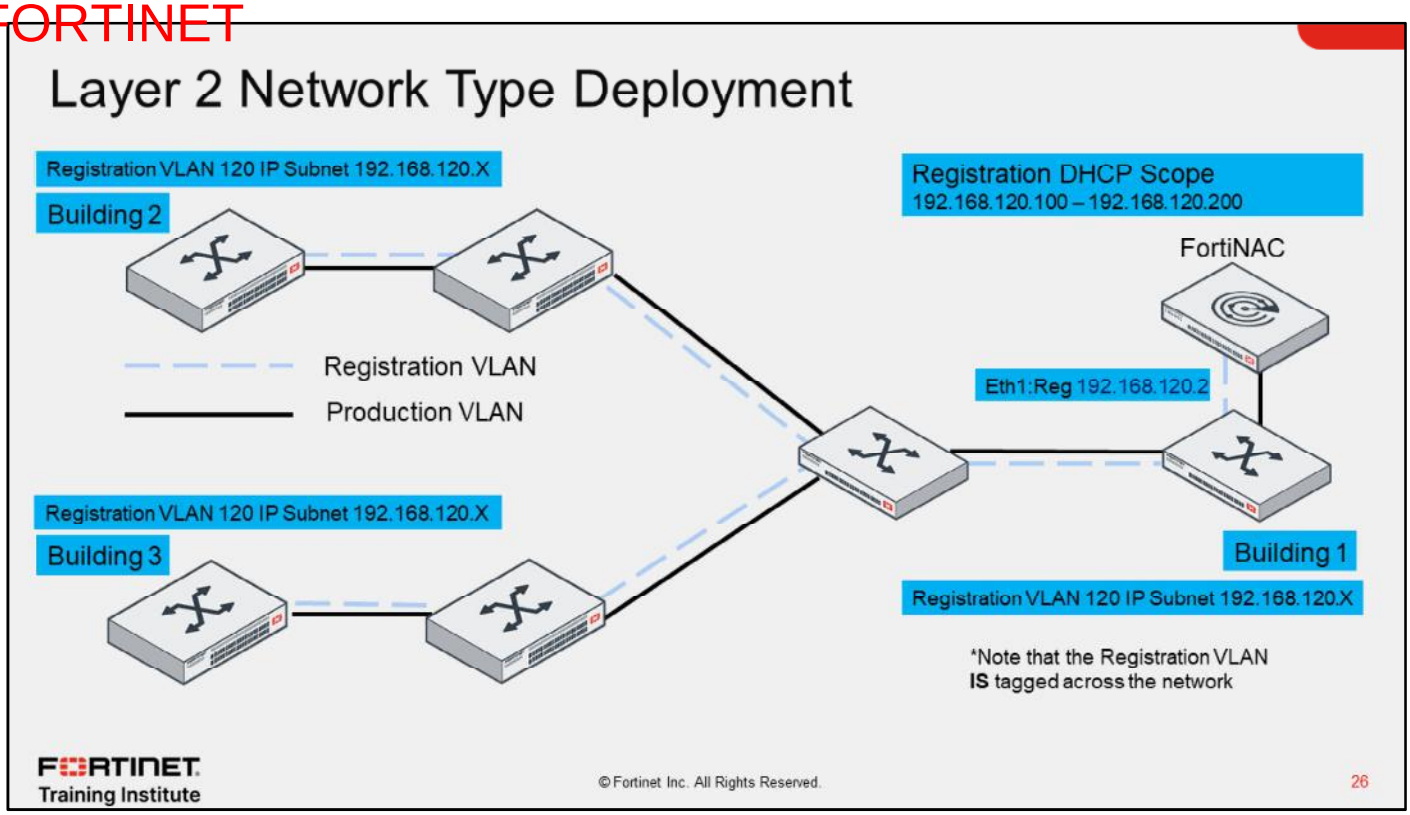
The captive networks are tagged throughout the environment so that any host assigned to a captive network (VLAN), is in the same broadcast domain as the corresponding FortiNAC VLAN interface.

The configurations for each of these captive network interfaces include the IP address, subnet mask, default gateway, and DHCP lease pool. The interface provides DHCP, DNS, and captive portal services to hosts assigned to the captive network.

An HA configuration with the primary and secondary devices configured on different subnets should *not* choose the Layer 2 network type for captive networks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows how a Layer 2 network type is configured on the network. Registration is the only captive network (VLAN) in this example, but it functions the same way for the other captive networks. Note that the registration captive network is portrayed by a broken light blue line.

The registration VLAN in Building 2 is 120. The registration VLAN in Building 3 is also 120. VLAN 120 is a flat network that spans the entire environment and exists in Building 1. Ethernet 1 on FortiNAC is configured with a sub-interface on VLAN 120, and has an IP address of 192.168.120.2.

In the configuration shown on this slide, a host that has been provisioned to the registration captive network in Building 1, 2, or 3 will be in the same broadcast domain as the FortiNAC sub interface for that VLAN.

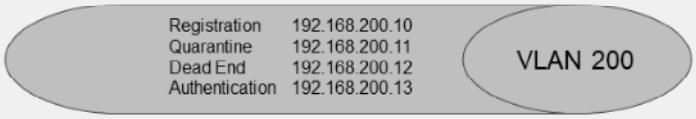
FortiNAC has a DHCP scope defined for VLAN 120, and it should be the only DHCP server available to hosts on that VLAN. The end result is that any host connected to VLAN 120 should get an IP address assigned by FortiNAC and a DNS server configuration of the FortiNAC IP for that VLAN, in this example, 192.168.120.2.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Layer 3 Network Type Captive Networks

- Each FortiNAC captive network (Registration, Remediation, and so on) is configured as one or more VLANs throughout the environment
- The FortiNAC eth1 interface is an access interface with an IP address (in the same subnet) for each type of captive network configured
- DHCP traffic is relayed to eth1 from the captive networks
- More appropriate configuration for HA deployments in large environments



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

A Layer 3 implementation differs from a Layer 2 implementation, primarily in the configuration of the eth1 interface and what needs to be configured on the network.

Ethernet 1 is still the captive portal interface on FortiNAC, just as it was with a Layer 2 implementation, but the configuration of the port is very different.

The interface exists on a single VLAN that is probably none of the captive network VLANs.

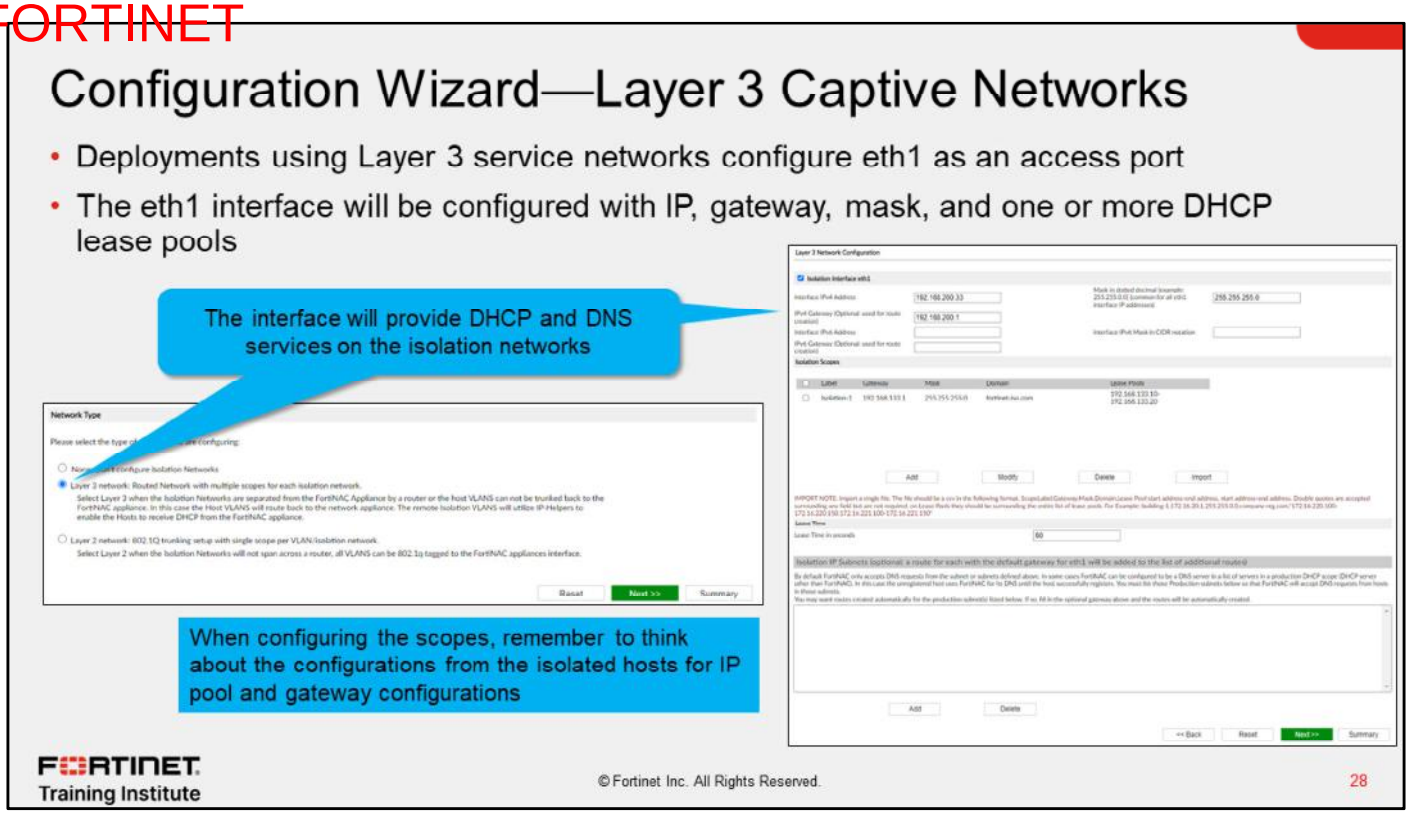
The captive portal interface is probably not within the same broadcast domain as a host assigned to the captive network, as it was with a Layer 2 implementation.

The captive portal interface has multiple IP addresses within the same subnet. The individual IP addresses are used when setting up the captive portal configurations during installation. This is the primary difference from a Layer 2 implementation, as far as the Ethernet 1 configuration goes. Instead of having several VLAN interfaces with IP addresses in separate subnets, it exists in a single VLAN with several IP addresses appropriate for that subnet.

DHCP relay addresses need to be configured on each isolation VLAN so that DHCP requests on those VLANs are forwarded to Ethernet 1. When configured as part of an HA deployment, multiple DHCP relays must be configured on each captive network so that DHCP traffic is passed to both the primary and secondary FortiNAC eth1 interfaces.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Selecting **Layer 3** as the network type will result in the Ethernet 1 (eth1) interface being configured as a typical access interface. Each subsequently configured captive network context (Registration, Quarantine, Dead End, and so on) will add an IP address to eth1, resulting in FortiNAC having multiple IP addresses on the interface. The captive networks will be configured throughout the environment with DHCP relays forwarding DHCP traffic back to the eth1 on FortiNAC.

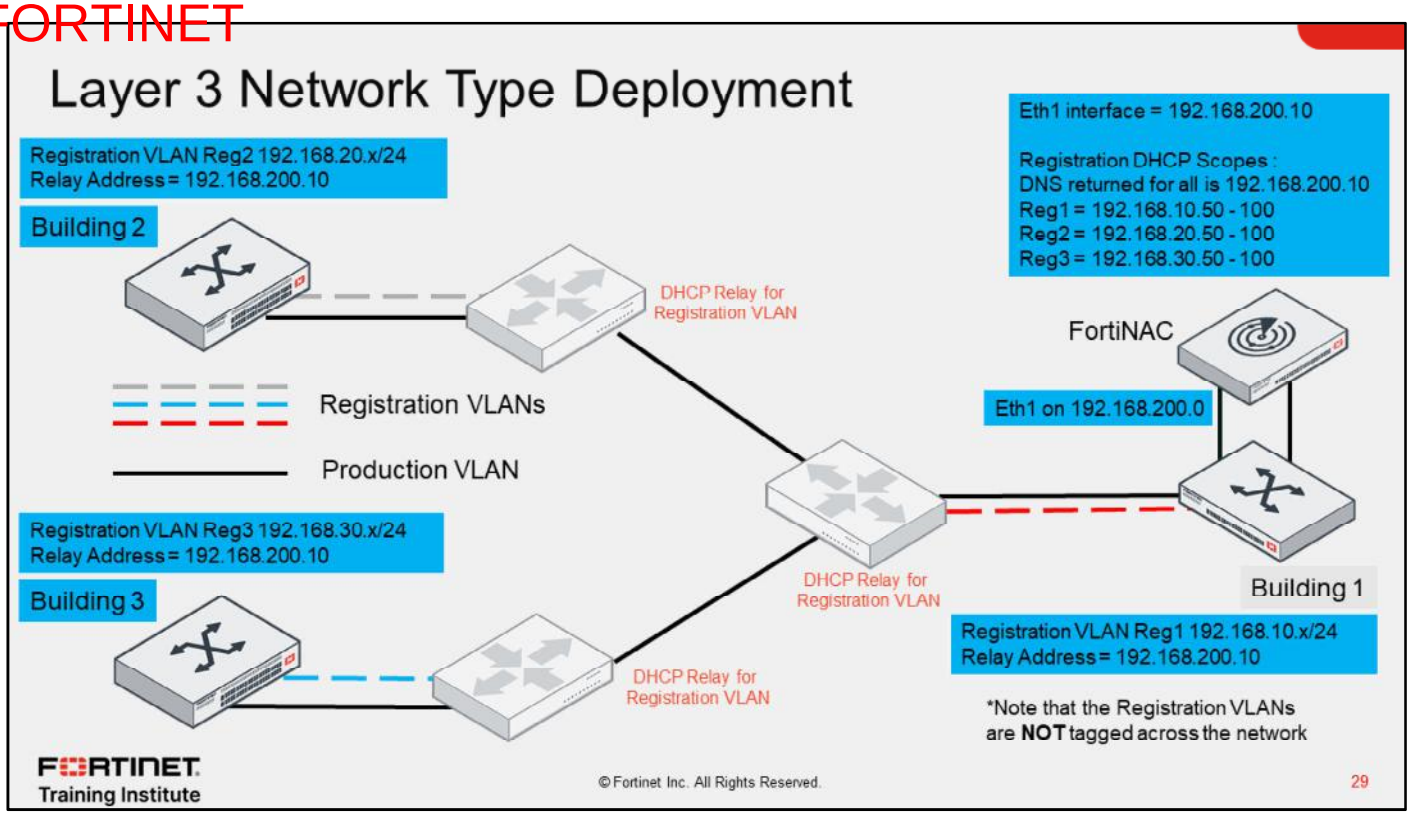
The configurations for each of these captive network interfaces include the IP address, subnet mask, default gateway, and one or more DHCP scopes. More than a single DHCP scope can be configured because there could be more than one network of each type. For example, a large environment could have a separate registration network in each building. Hosts assigned to the registration networks would all use eth1 but receive an appropriate IP address for their respective registration networks. The interface will provide DHCP, DNS, and captive portal services to hosts assigned to any of the captive networks.

An HA configuration with the primary and secondary devices configured on different subnets *should* choose the Layer 3 network type for captive networks.

You will learn about Layer 3 captive portal networks in more detail in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The example on this slide shows how a Layer 3 implementation functions. Registration is the only captive network context shown in this example, but it would work the same for the other captive network contexts.

Note that there are three different registration captive networks, one for each building.

Building 2 has captive network Reg2 designated for registration, and a DHCP relay has been configured on that VLAN to forward DHCP requests back to Ethernet 1 on FortiNAC. The captive network Reg2 does not exist beyond Building 2, meaning it is not tagged beyond that building, as it would have been in a Layer 2 implementation.

Building 3 has captive network Reg3 designated for registration. Just like in Building 2, a DHCP relay has been defined so DHCP requests get forwarded to, and serviced by FortiNAC. This captive network Reg3 exists only in Building 3.

Building 1 is configured in the same manner, with captive network Reg1 being designated for registration.

The FortiNAC Ethernet 1 interface is connected to a separate VLAN, often referred to as the FortiNAC service network, and has one of its several IP addresses defined as the DHCP relay address on the various registration VLANs.

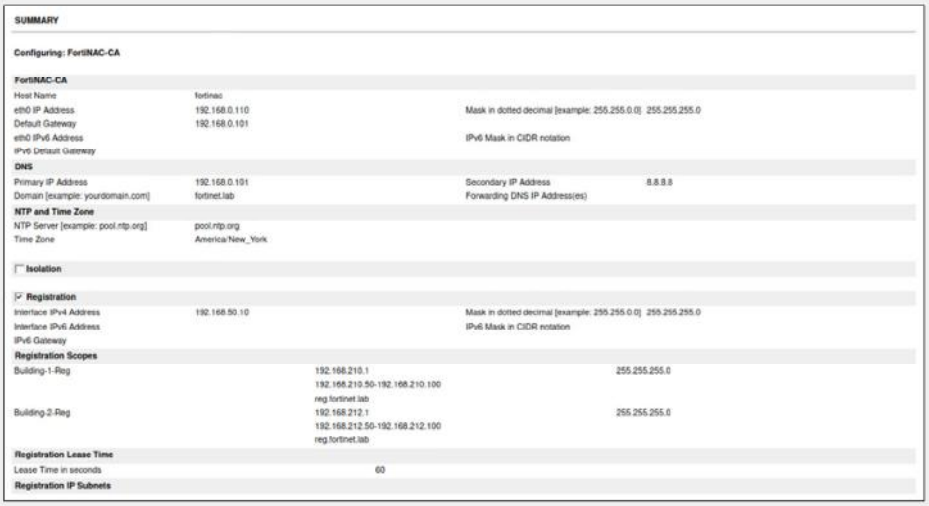
The DHCP configuration file on FortiNAC has scopes configured for each of the registration captive networks defined at each building. FortiNAC responds with an appropriate IP address, and a DNS server designation. The DNS server is one of the Ethernet 1 addresses. In this example, the address returned is 192.168.200.10.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuration Wizard—Summary

- **SUMMARY** view organizes all configuration settings into a single page for review
- After applying the configurations on the summary page the system will need to be restarted



SUMMARY

Configuring: FortiNAC-CA

FortiNAC-CA			
Host Name	fortinac		
eth0 IP Address	192.168.0.110	Mask in dotted decimal [example: 255.255.0.0]	255.255.255.0
Default Gateway	192.168.0.101		
eth0 IPv6 Address		IPv6 Mask in CIDR notation	
IPv6 Default Gateway			
DNS			
Primary IP Address	192.168.0.101	Secondary IP Address	8.8.8.8
Domain [example: yourdomain.com]	fortinet.lab	Forwarding DNS IP Address(es)	
NTP and Time Zone			
NTP Server [example: pool.ntp.org]	pool.ntp.org		
Time Zone	America/New_York		
☐ **Isolation**			
☑ **Registration**			
Interface IPv4 Address	192.168.50.10	Mask in dotted decimal [example: 255.255.0.0]	255.255.255.0
Interface IPv6 Address		IPv6 Mask in CIDR notation	
IPv6 Gateway			
Registration Scopes			
Building-1-Reg	192.168.210.1 192.168.210.50-192.168.210.100 reg.fortinet.lab		255.255.255.0
Building-2-Reg	192.168.212.1 192.168.212.50-192.168.212.100 reg.fortinet.lab		255.255.255.0
Registration Lease Time			
Lease Time in seconds	60		
Registration IP Subnets			

FORTINET Training Institute

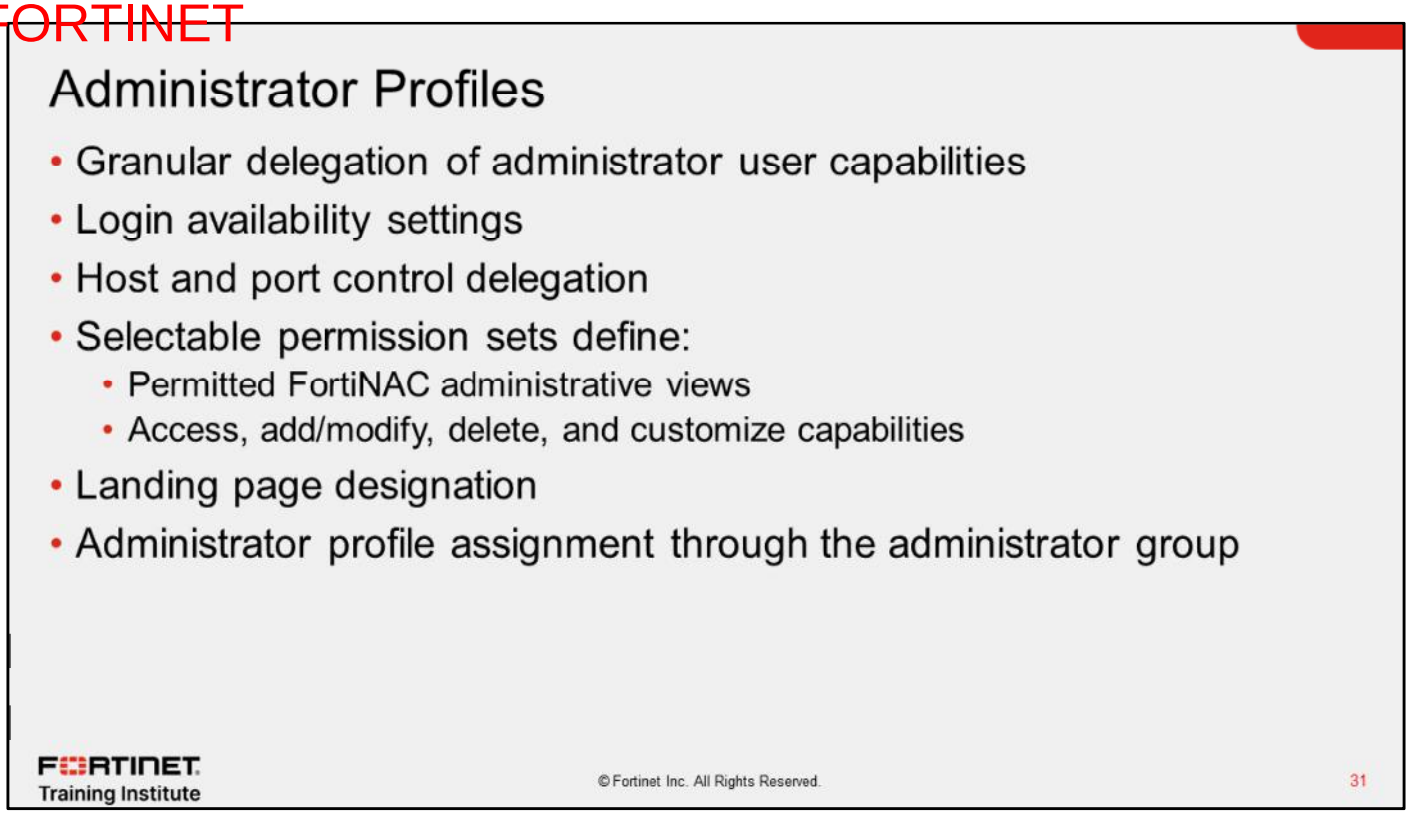
© Fortinet Inc. All Rights Reserved.

30

The final step in the configuration wizard is the **SUMMARY** page. Each configuration wizard step is detailed in its own section of the summary. You should review the **SUMMARY** page closely before applying the changes. After you apply the settings, the page will refresh with the settings to reboot or shut down FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



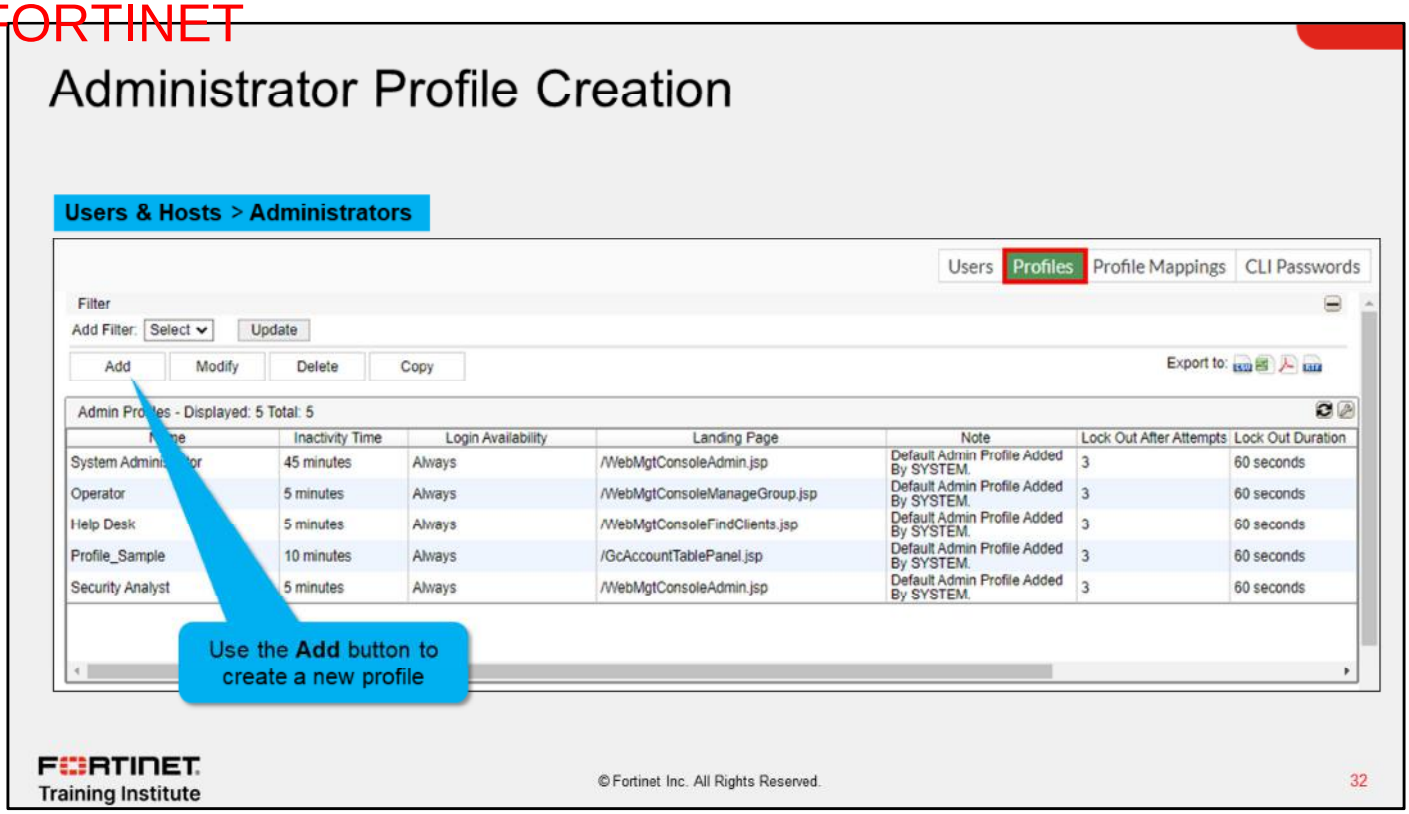
Administrator profiles are the mechanism for defining the specific capabilities of an administrative user. Every administrative user is required to have an administrator profile, and you can assign each administrator profile to more than one administrative user.

These profiles define inactivity timers to automatically log users off after a defined number of minutes of inactivity. Available login times are defined by days of the week and times of the day. They allow for landing page designation after login, and guest kiosk management capabilities.

Most importantly, these profiles define permission sets. A permission set is made up of one or more administrative views, as well as the administrative privileges within those views.

Vouchers & Dumps are Available | WhatsApp +201224560923

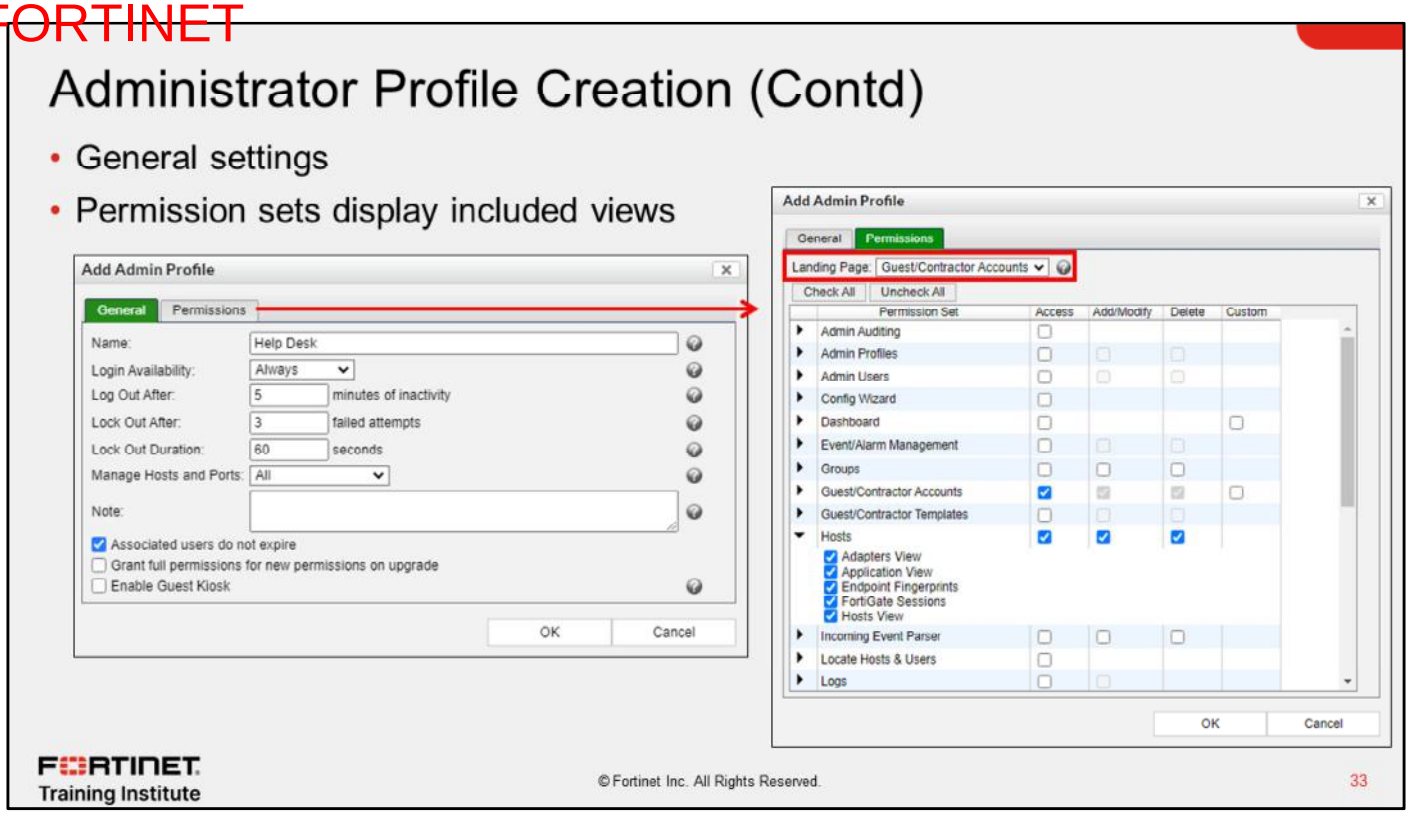
DO NOT REPRINT
© FORTINET
Brave-dumps.com



To create an administrator profile, select **Profiles** from the **Users & Hosts** > **Administrators** menu. This view displays all existing administrator profiles. You can perform administrator profile management using the buttons along the top of the view. When you click **Add**, the **Add Admin Profile** dialog box opens.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When you create or edit an administrator profile, there are two tabs that contain the profile properties and settings.
The **General** tab is where you give the profile a name, configure an inactivity timer, and define login availability. You can also use this tab to grant the ability to manage hosts and ports based on group membership. There are three additional settings that you can set:

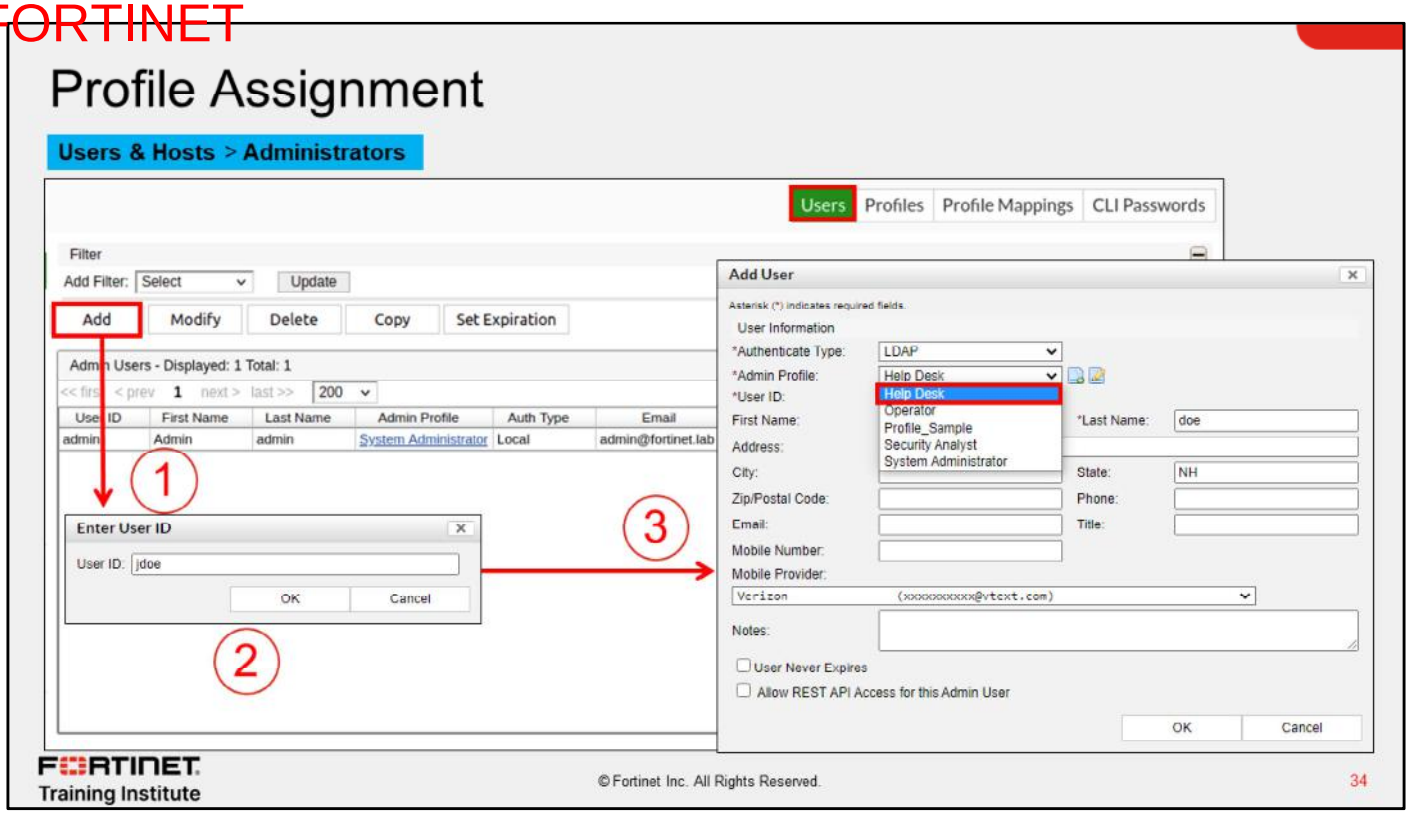
- **Associated users do not expire** prevents the administrative user from ever being purged from the FortiNAC database.
- **Grant full permissions for new permissions on upgrade** automatically grants administrative users full access to new permission sets added as the result of an upgrade.
- **Enable Guest Kiosk** makes the associated administrative users kiosk managers. They have no other capabilities other than opening a self-service kiosk for guests.

The **Permission** tab gives you access to all of the permission sets. This is where the administrator can select all the desired views to be included in the administrator profile. Each permission set includes these settings for administrative capabilities within that permission set: **Access** is read only, **Add/Modify** is read-write, **Delete** allows for the deletion of view entries. The permission sets also include one or more administrative views that you can remove individually from the permission set, if desired.

After selecting the desired permission sets, all available views will appear as settings in the **Landing Page** field. The administrative view selected from this field is the default initial page presented when the user logs in. If **Dashboard** is selected as the default landing page, and more than one dashboard exists, the highest-ranked dashboard will be the landing page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

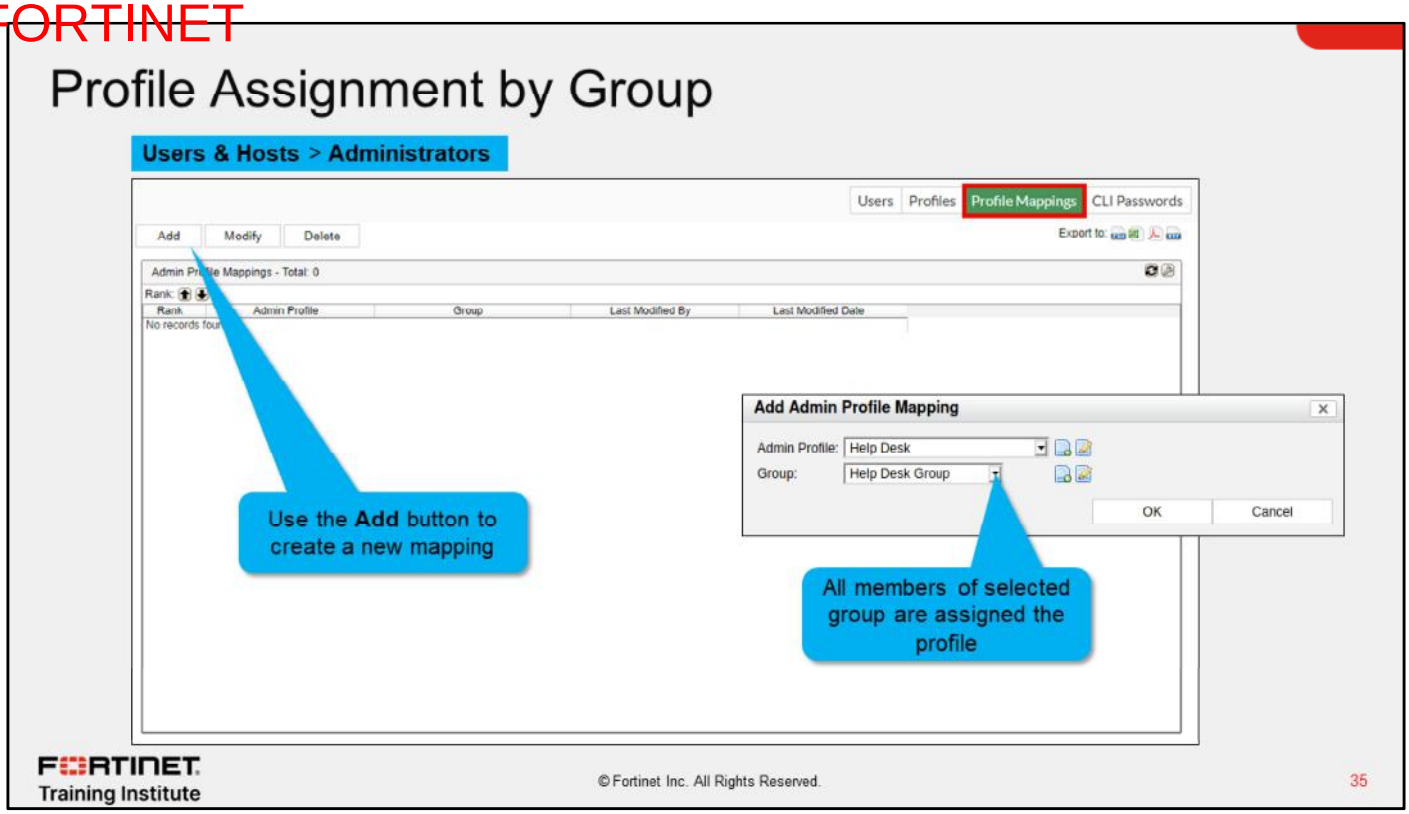


You can add new administrative users in the **Administrators** view. Clicking **Add** at the top of the window opens a dialog box where you can enter the new user ID. FortiNAC attempts to look up the user ID using LDAP, if an LDAP server is configured. If the ID is found, the new user property window is prepopulated with all mapped user attributes.

Each administrative user property window includes an **Admin Profile** field of all the existing administrator profiles. Selecting a profile assigns that profile and all of the permissions it grants.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can apply an administrator profile to all members of an administrative group on the **Add Admin Profile Mapping** window located under **Users & Hosts** > **Administrators**. You would do this in situations where you need to apply a single administrator profile to an entire group of administrative users. Create the administrator profile mapping by associating the desired administrator profile, selected from a drop-down list, to an administrator group.

In the example shown on this slide, all members of the group named **Help Desk Group** are assigned the **Help Desk** admin profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which type of deployment requires DHCP relays to be configured on the isolation networks?
   A. Layer 2
   ✓ B. Layer 3

2. What defines an administrative user's capabilities?
   ✓ A. Administrator profile
   B. The defined landing page

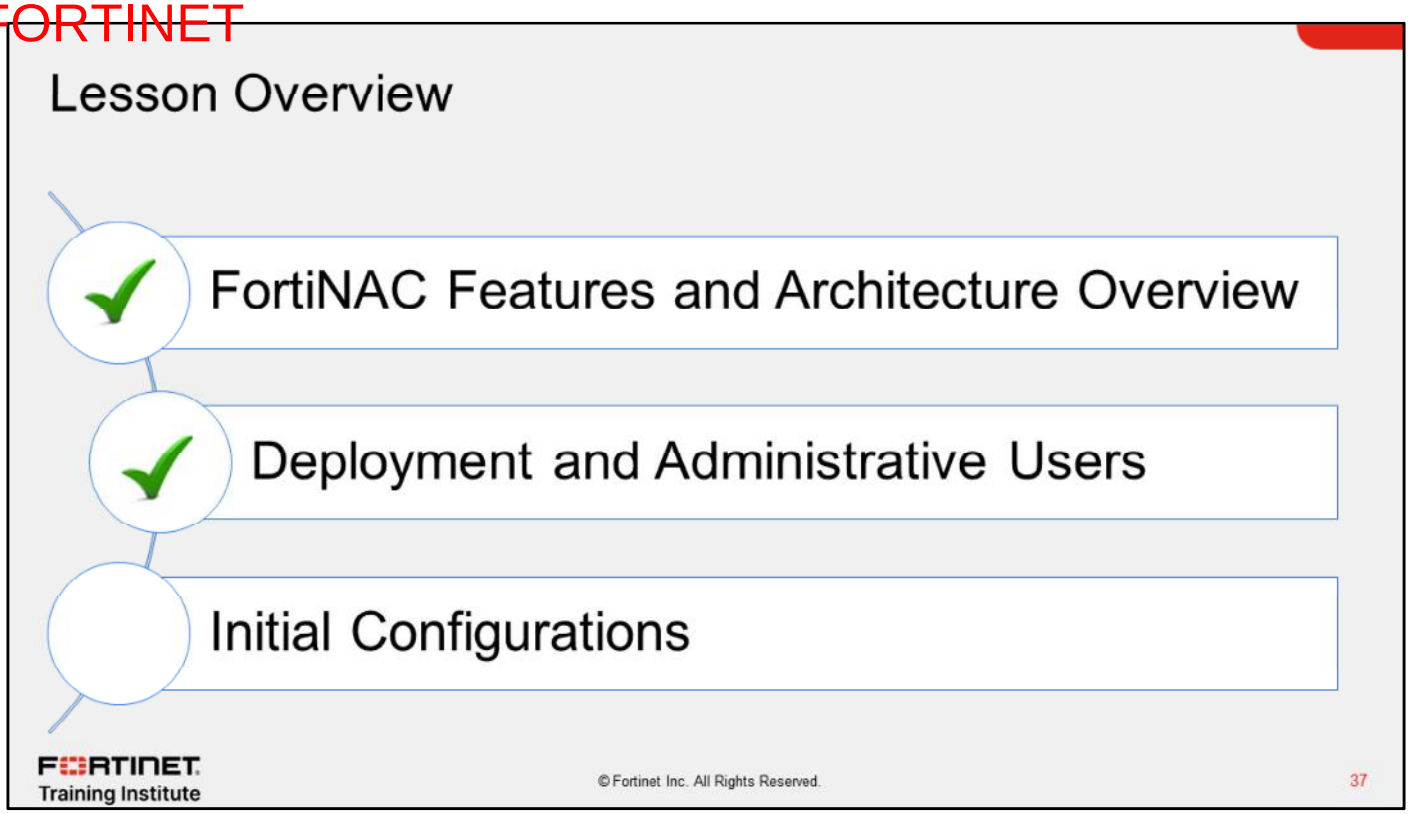
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

36

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

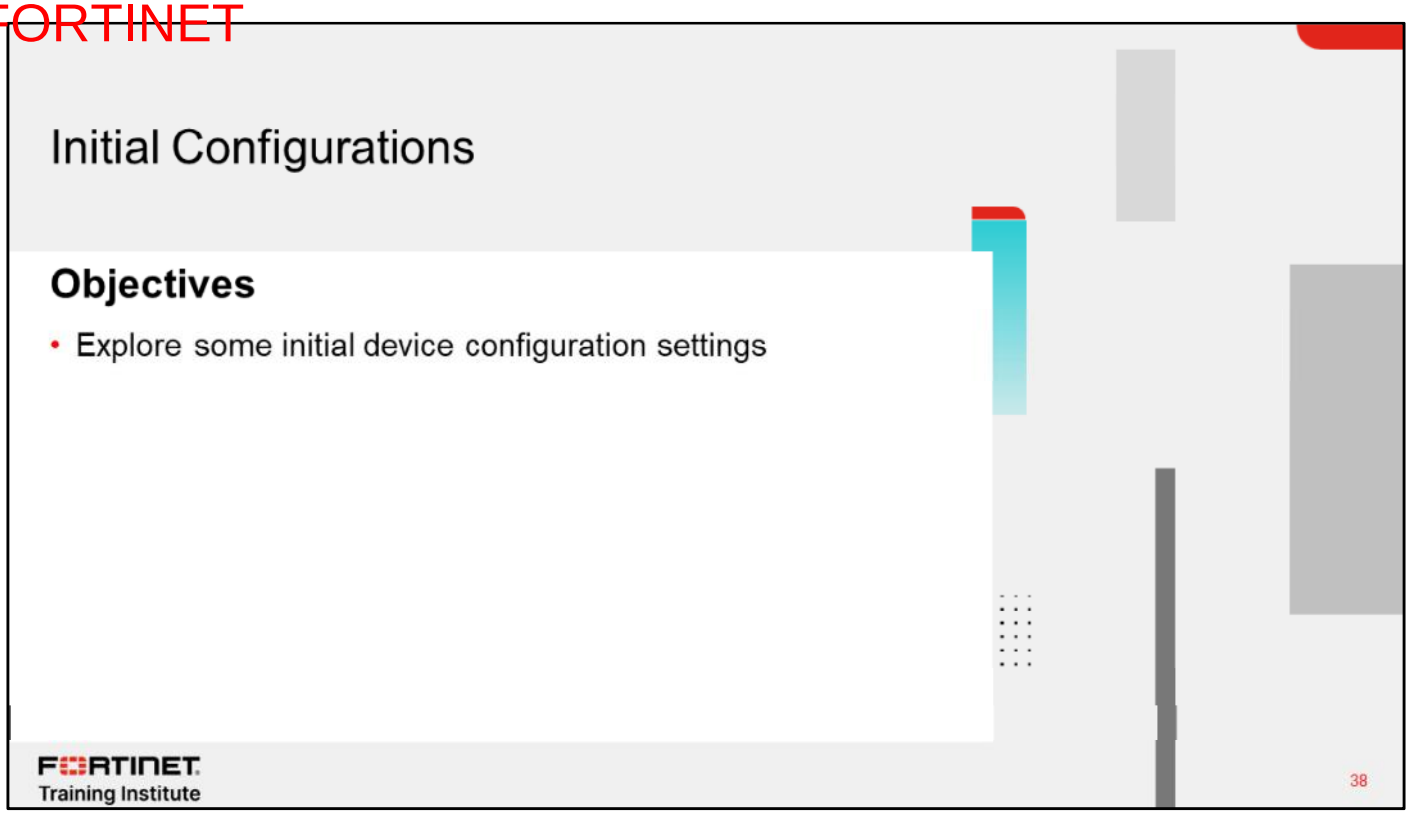


Good job! You now have a basic understand of FortiNAC deployment and initial configurations.

Now, you will learn about some FortiNAC initial configurations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

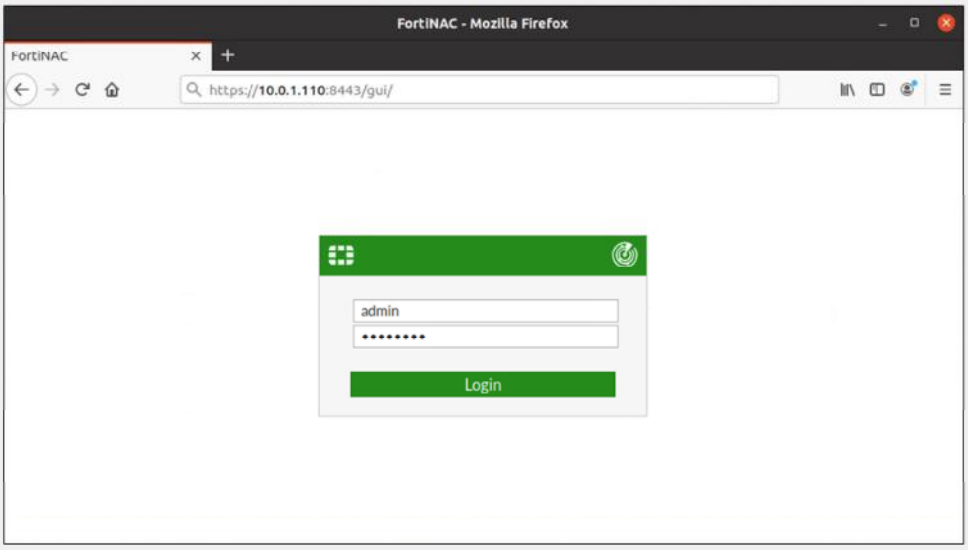
By demonstrating competence in configuring the most common initial configurations you will be able to successfully complete a FortiNAC deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Access to the Administrative GUI

- Access the administrative GUI login in screen at https://<FortiNAC_IP>:8443



FORTINET Training Institute

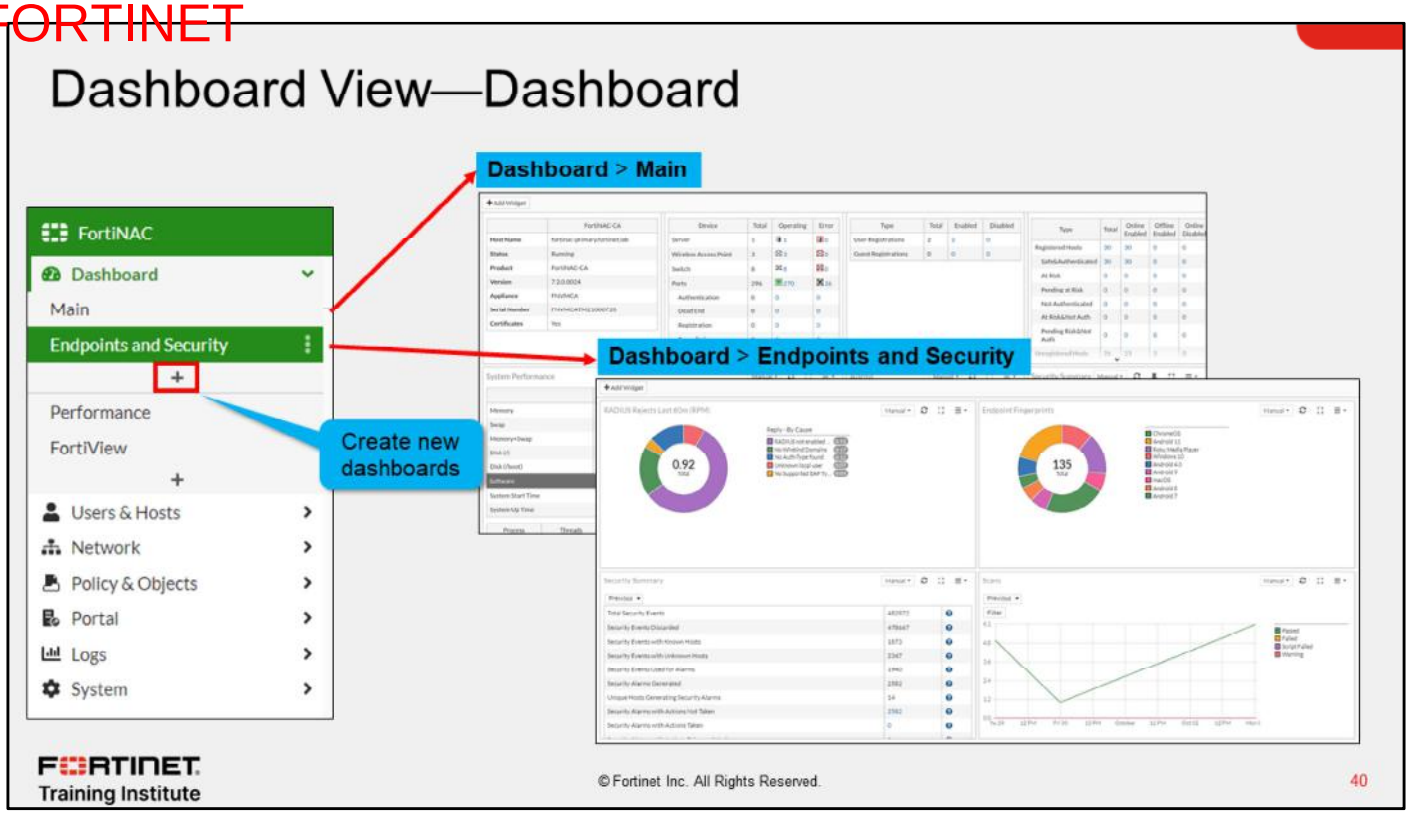
© Fortinet Inc. All Rights Reserved.

39

FortiNAC uses a simple browser-based administrative user interface to get username and password credentials. The credentials can be validated using a local administrative account or an LDAP or RADIUS server. FortiNAC administration access is handled by the device eth0 interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

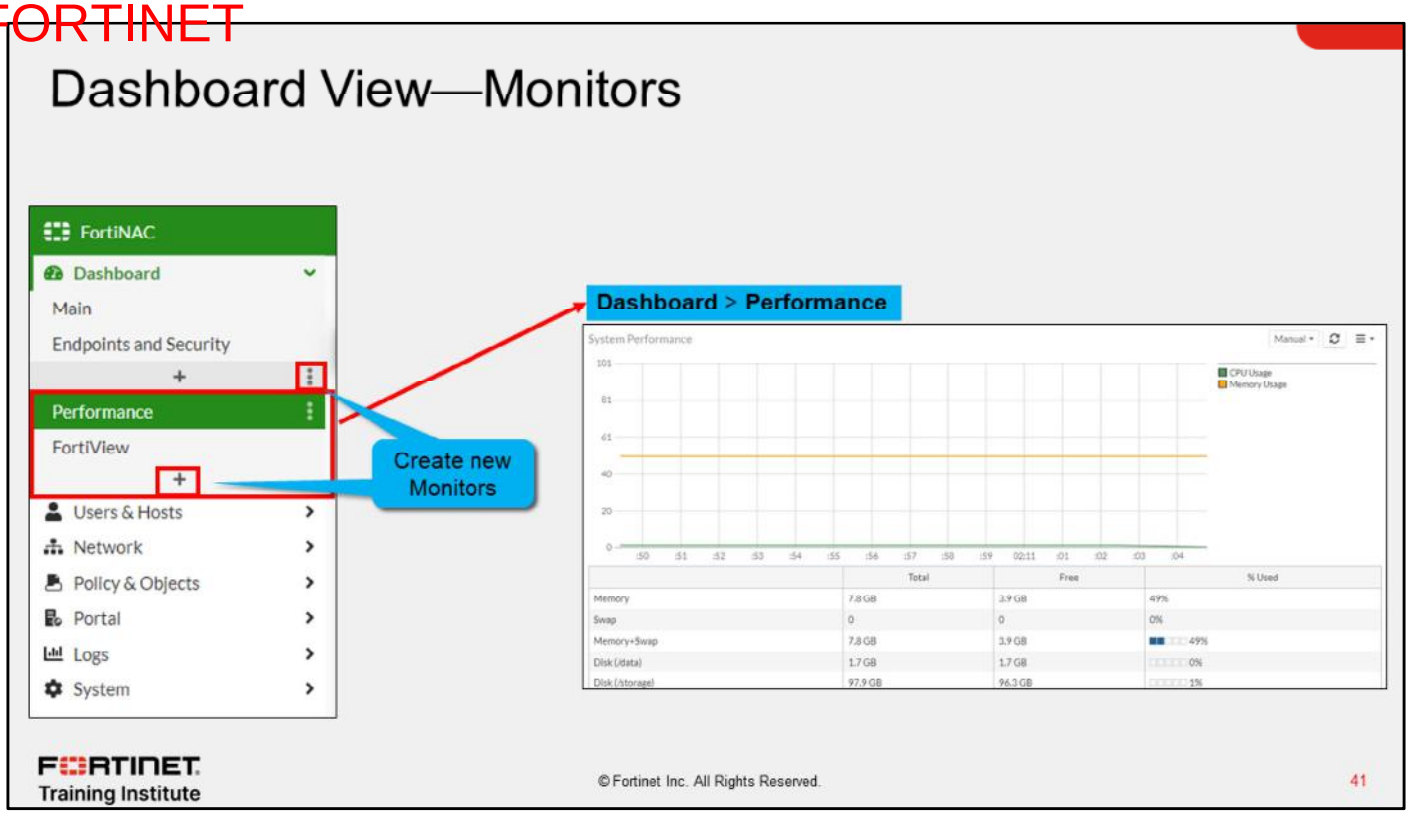
DO NOT REPRINT Brave-dumps.com
© FORTINET



The dashboard view is the default landing page for an administrative user. These dashboards play an essential role in presenting an administrative user with a detailed overview of vital information. Administrators can create as many individual dashboards as needed, and populate them with a wide variety of widgets. For example, an administrator could add a dashboard populated with widgets designed to monitor endpoint and security details. When more than one dashboard has been created, the highest-ranked dashboard will act as the default landing page.

Vouchers & Dumps are Available | WhatsApp +201224560923

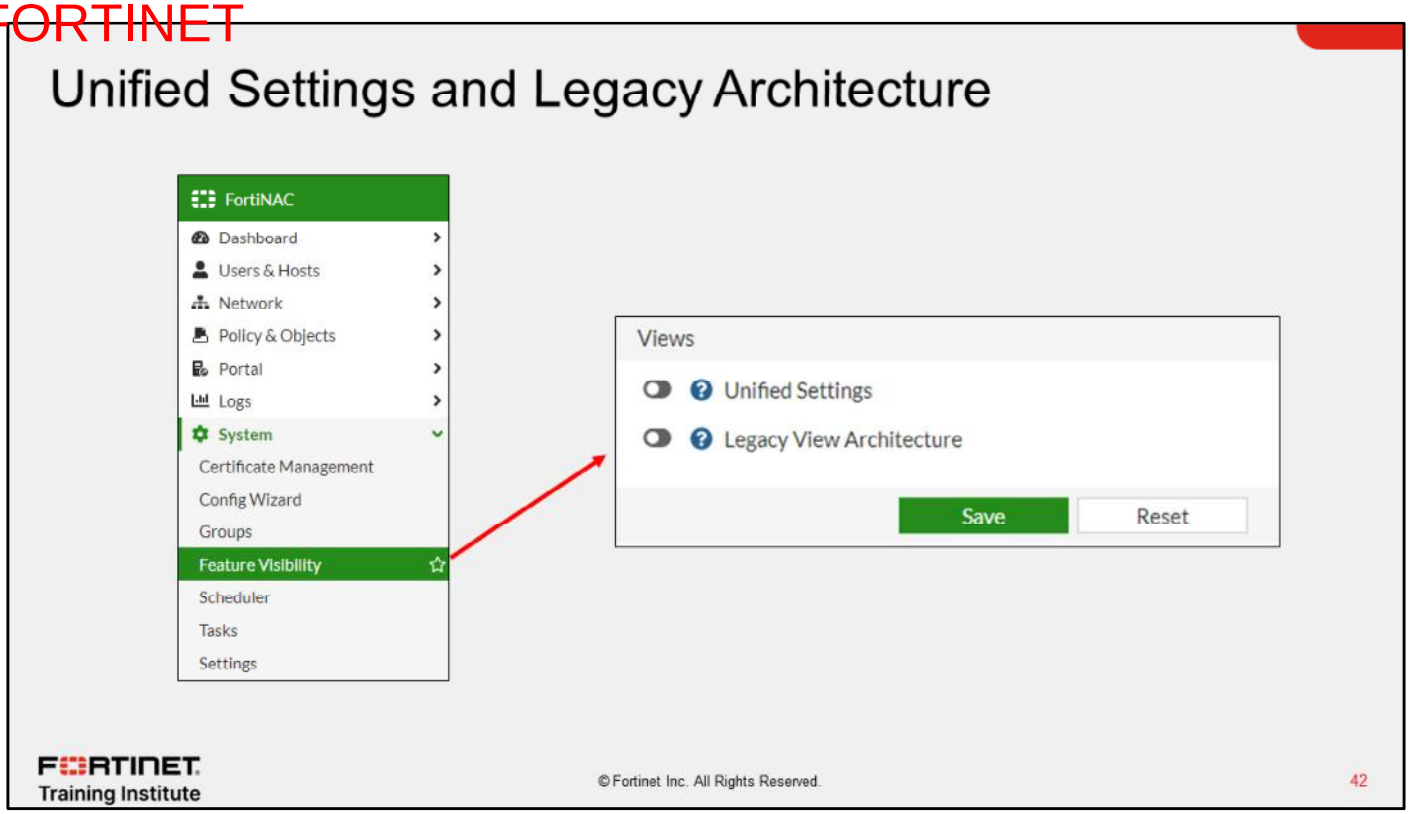
DO NOT REPRINT Brave-dumps.com
© FORTINET



In addition to the dashboard views, you can add monitor views. Monitors provide more detailed views of many dashboard widgets, such as system alarms, RADIUS server details, system performance, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



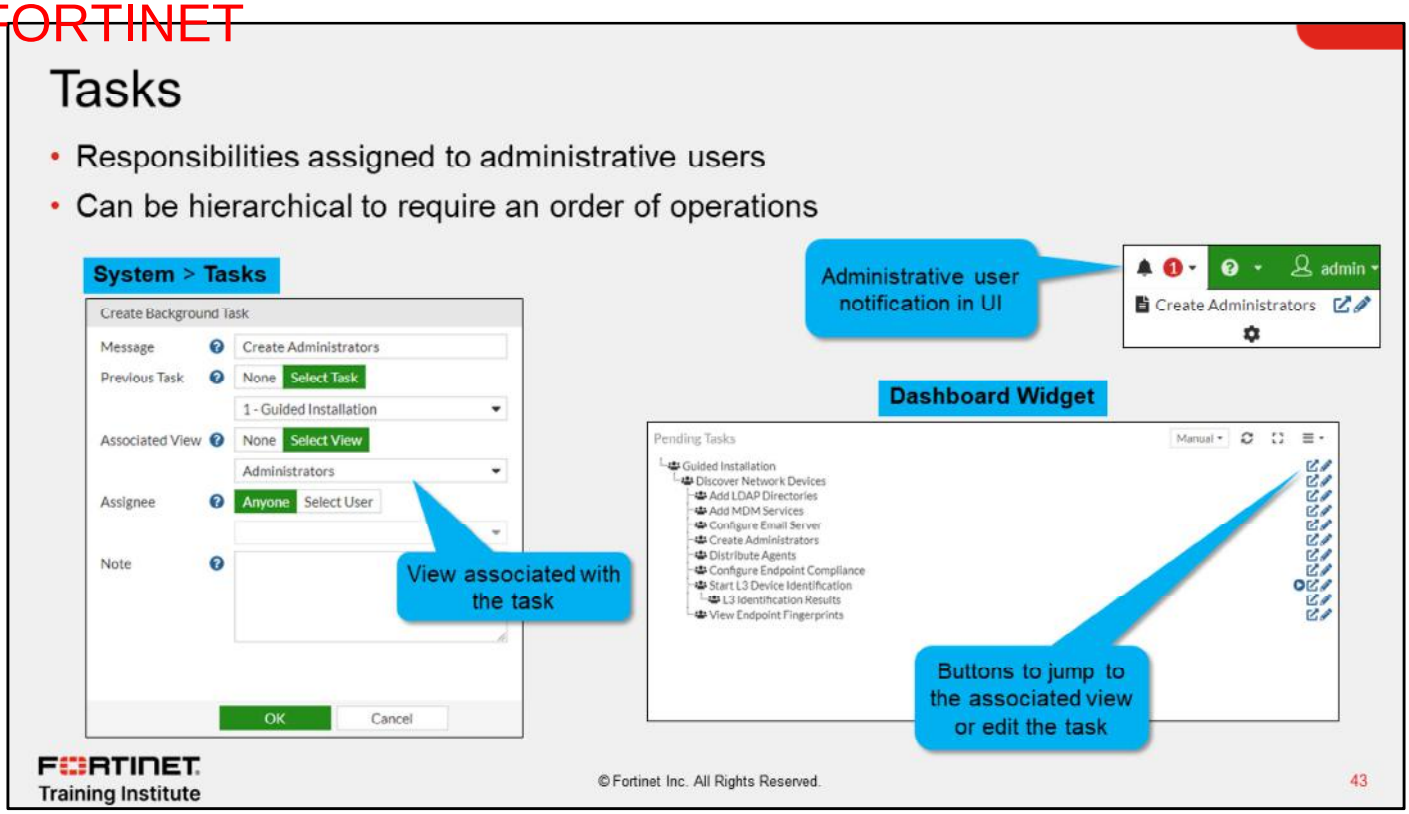
FortiNAC provides flexibility when displaying some UI components. The **Feature Visibility** view provides two settings for UI views and layout preferences.

By enabling **Unified Settings**, you can have all settings options condensed into a single settings view. If disabled, three more focused settings views appear under the **System**, **Network** and **Users & Hosts** menus.

Enabling **Legacy View Architecture** will revert updated views to the older FortiNAC style. Legacy views will not be available in future versions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

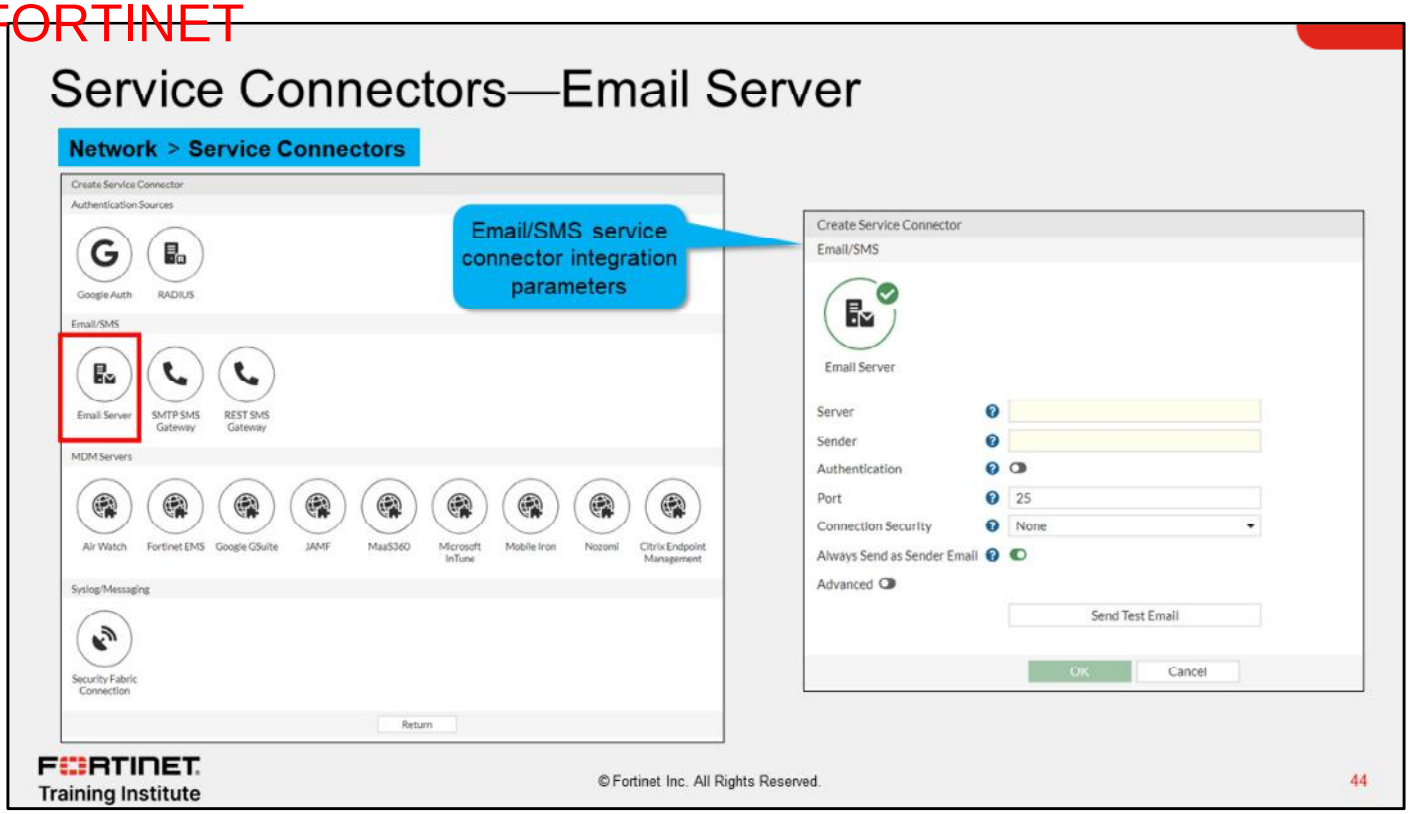


Administrators have many different responsibilities they must perform, using a wide array of tools. FortiNAC provides the ability to create tasks, organize them in a hierarchy and assign them to administrative users. A user who has been assigned a task will be notified under the bell notification menu on the taskbar. A **Pending Tasks** dashboard widget displays all existing tasks.

If tasks must be completed in sequence, you can organized them according to priority. Click **Open Link** to go to the administrative view associated with a listed task. This streamlines the process for the administrator. You can click **Edit Task** mark a task as complete.

Vouchers & Dumps are Available | WhatsApp +201224560923

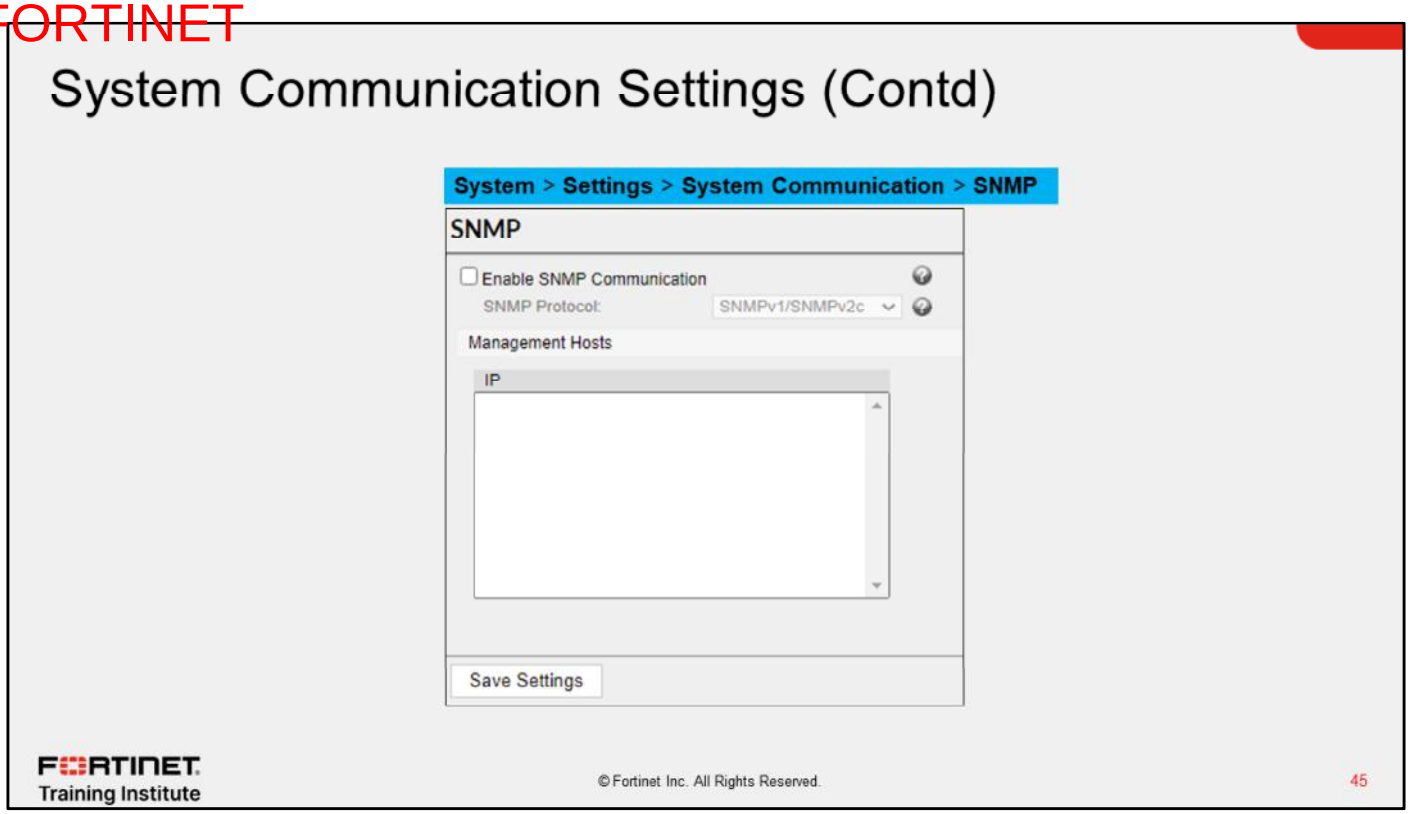
DO NOT REPRINT Brave-dumps.com
© FORTINET



Another important initial configuration is the setup of an email server. FortiNAC uses email to send notifications through email and SMS. In order for this to work, you must configure an email server. You perform an email server integration using a service connector. On the **Network** > **Service Connectors** page, create a new service connector, and then select the **Email Server** connector type. Then enter the email server parameters to complete the integration.

Vouchers & Dumps are Available | WhatsApp +201224560923

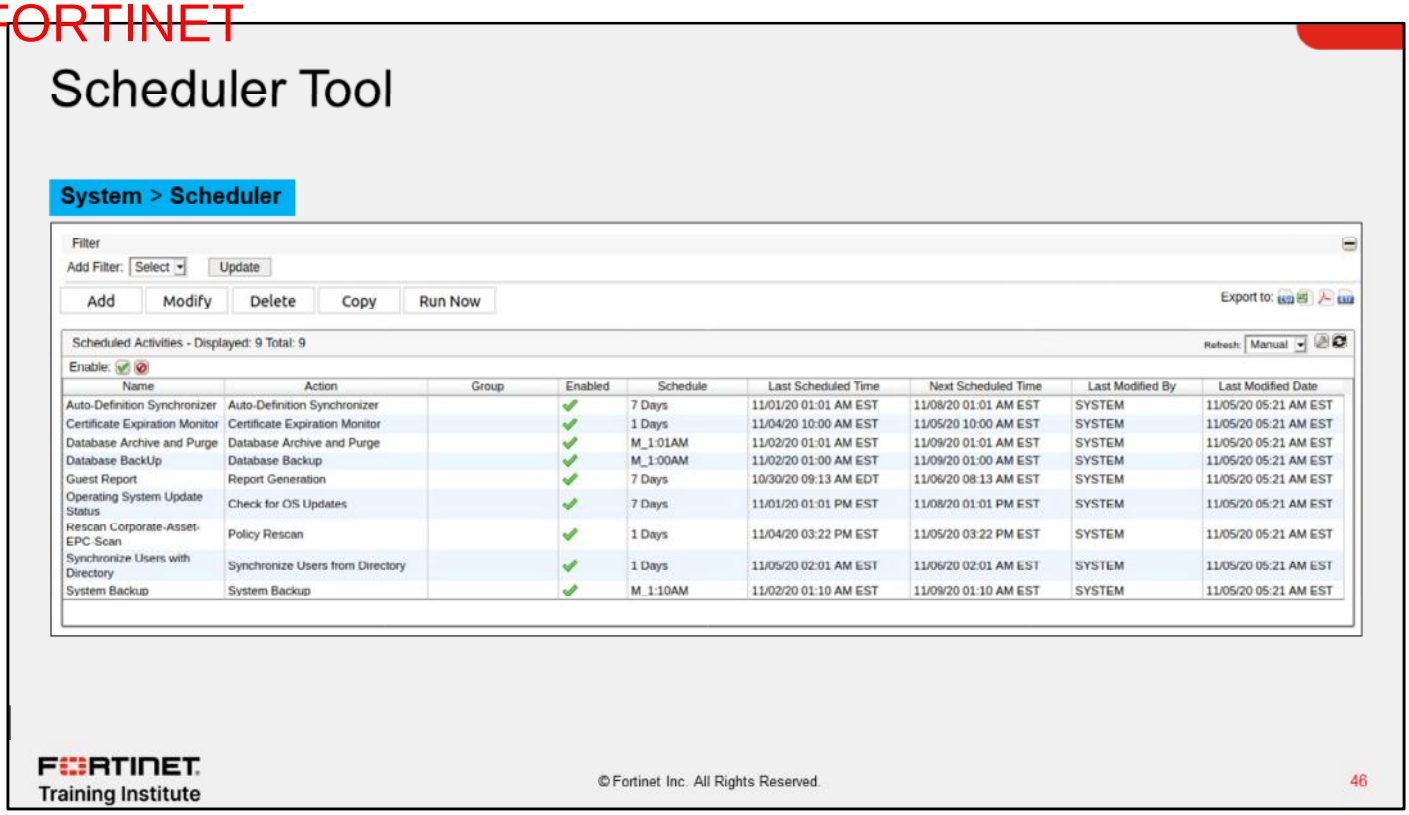
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Another configuration page contained in the **System Communication** folder is an SNMP agent configuration page that allows an administrative user to turn the FortiNAC onboard SNMP agent on. This allows other tools to query FortiNAC and gather SNMP information, such as license count, interface utilization, or the number of connecting hosts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiNAC has a built-in scheduler tool that allows administrative users to schedule the automated execution of actions. By default, there are a series of important actions already configured within the scheduler tool. These default actions and their purpose are as follows:

Auto-Definition Updates: Allows you to automatically update the virus definition or signature information for the antivirus software that is permitted in scans within your endpoint compliance policies. When new versions of operating systems and antivirus software are added using the **Auto-Definition Synchronization** settings, the updated versions are not automatically selected in existing scans. You must go to each scan and enable the new options if you choose to scan for them.

Certificate Expiration Monitor: Generates warning, critical warning, and expiration events for the certificates listed in **Certificate Management**.

Database Archive and Purge: Archives and purges event, connection, and alarm records that are older than seven days. You can configure the number of days on the **Database Archive** page within the **System Settings** menu, in the **System Management** folder.

Database Backup: Backs up the FortiNAC database.

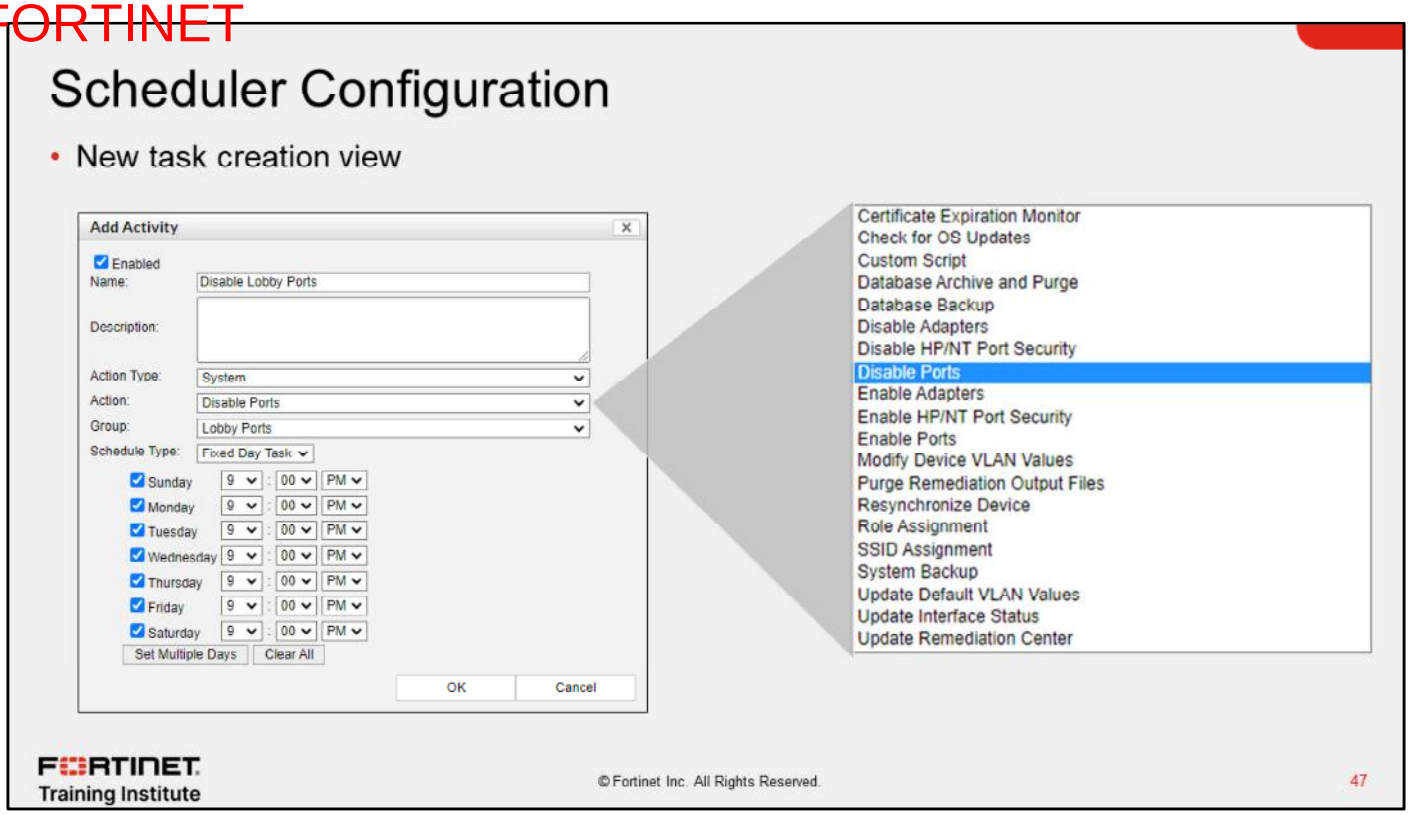
Check for OS Updates: Establishes a connection with the Fortinet FortiNAC FTP server to determine if the local system is up-to-date with current OS packages.

Synchronize Users from Directory: Writes the attributes mapped in the LDAP configuration of users in the directory to the corresponding user records in the FortiNAC database.

System Backup: Creates a backup of all system files that are used to configure FortiNAC, such as license key and web server configurations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

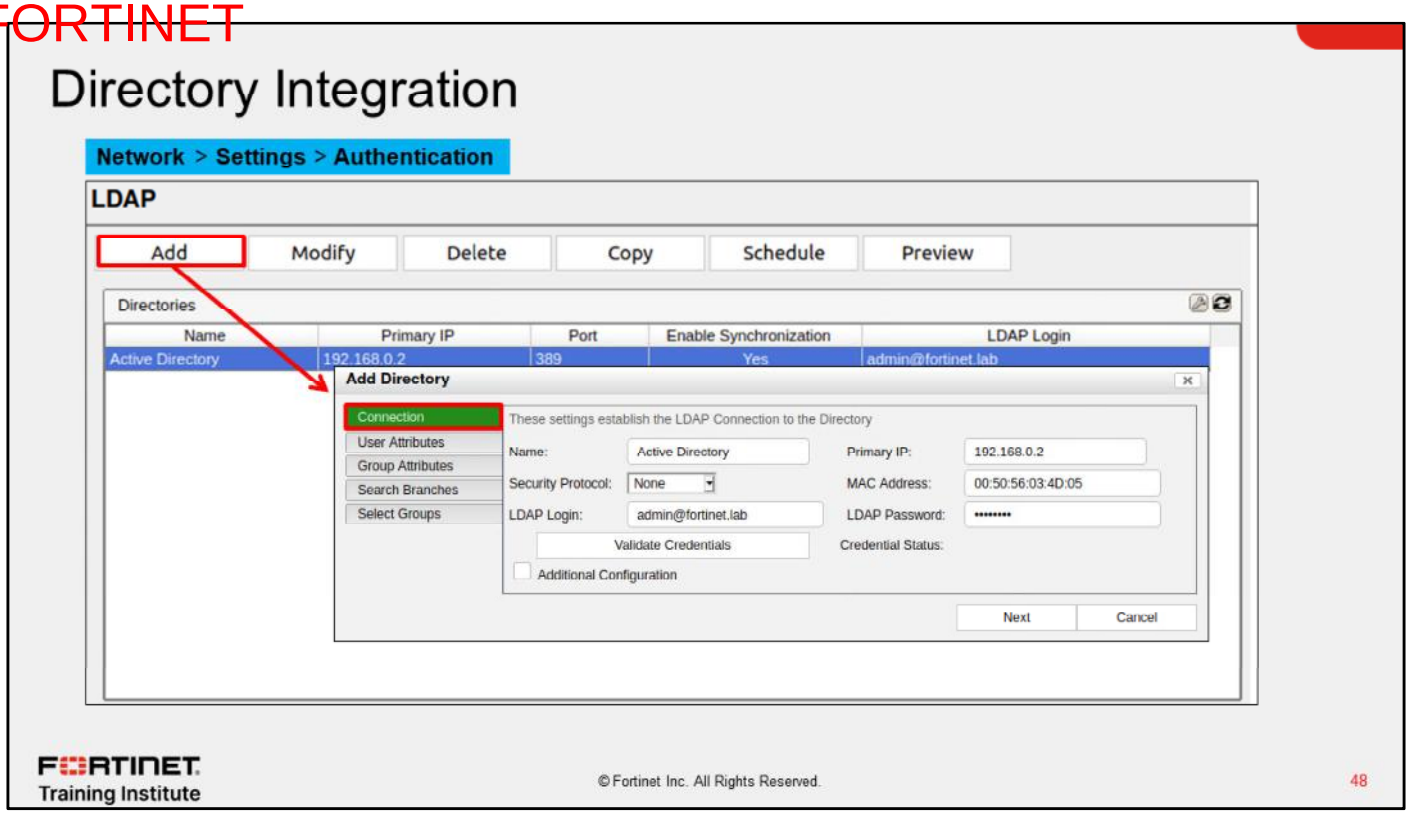


When you schedule an action, you can set it to execute at a specific time on designated days of the week, or as a repetitive task. Repetitive tasks are configured with a repetition rate (once, minutes, hours, or days) and a next scheduled time. The action will execute at the next scheduled time value and then continue to execute at an interval equal to the repetition rate. There are two types of actions that you can schedule: system and CLI. There is an extensive list of system actions that you can execute. Each system action is documented in the help for this view. CLI actions are user-created CLI configurations that you will learn about in another lesson.

Many scheduled actions or CLI configurations need to be targeted so that they are carried out on a specific group of elements. You can select the target group in the **Group** drop-down list. The groups available in the **Group** drop-down list are based on the group type defined by the selected action.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



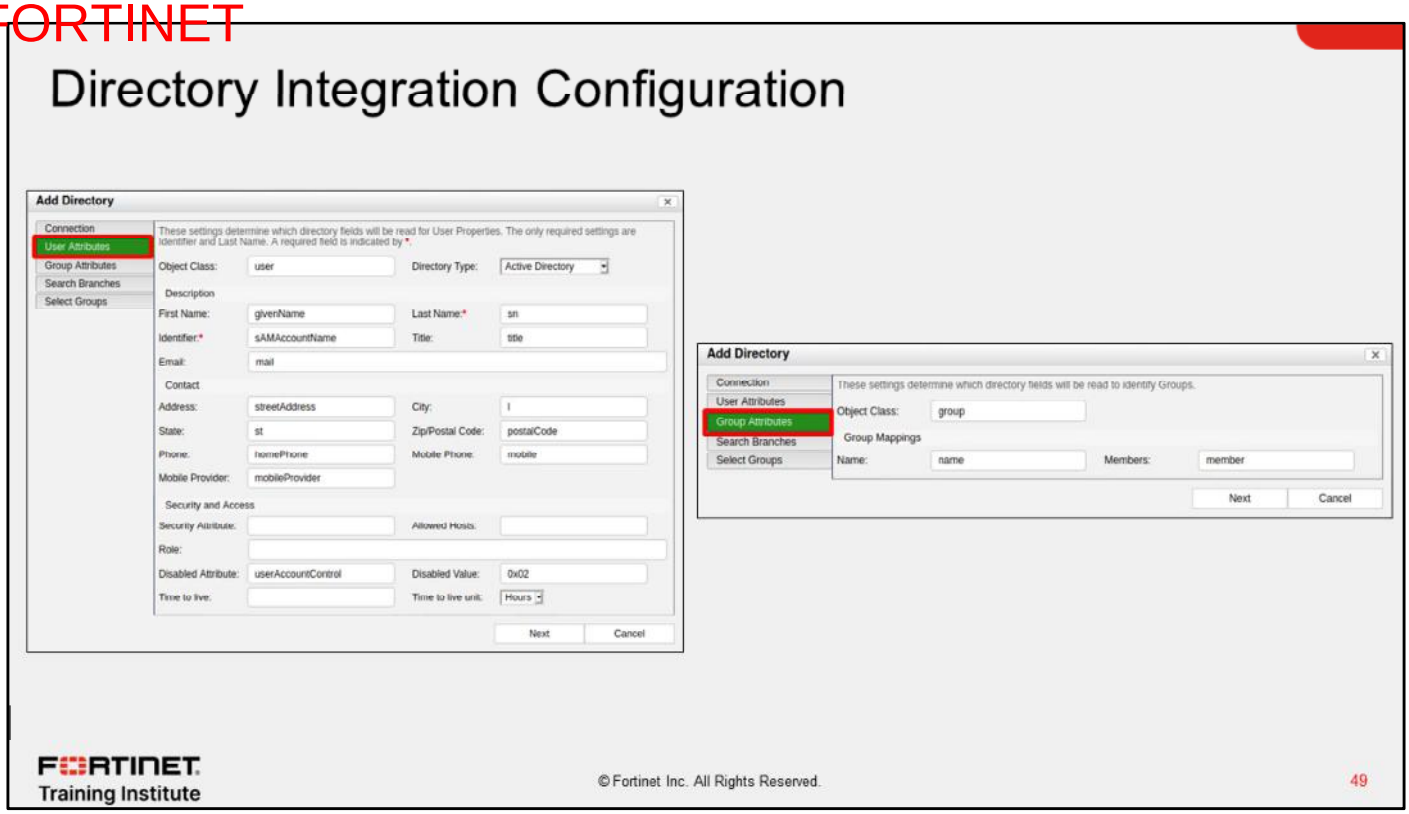
The **Directory Configuration** window allows you to configure the connection to an LDAP directory, the user attributes that you would like to import, the desired user search branches for validation of administrative users, or end-user on-boarding credentials, and the group search branches for finding groups that can be imported into FortiNAC. There is specific information that you must enter in each section to allow FortiNAC to connect with the directory and import users and groups.

To integrate with a new directory server, you will perform configurations across several tabs. FortiNAC automatically discovers existing directories, if there are SRV records for the directories in DNS.

The **Connection** tab contains the parameters required for communication with the directory. Not all fields are required. Be sure to enter information in only those fields that apply to your directory.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

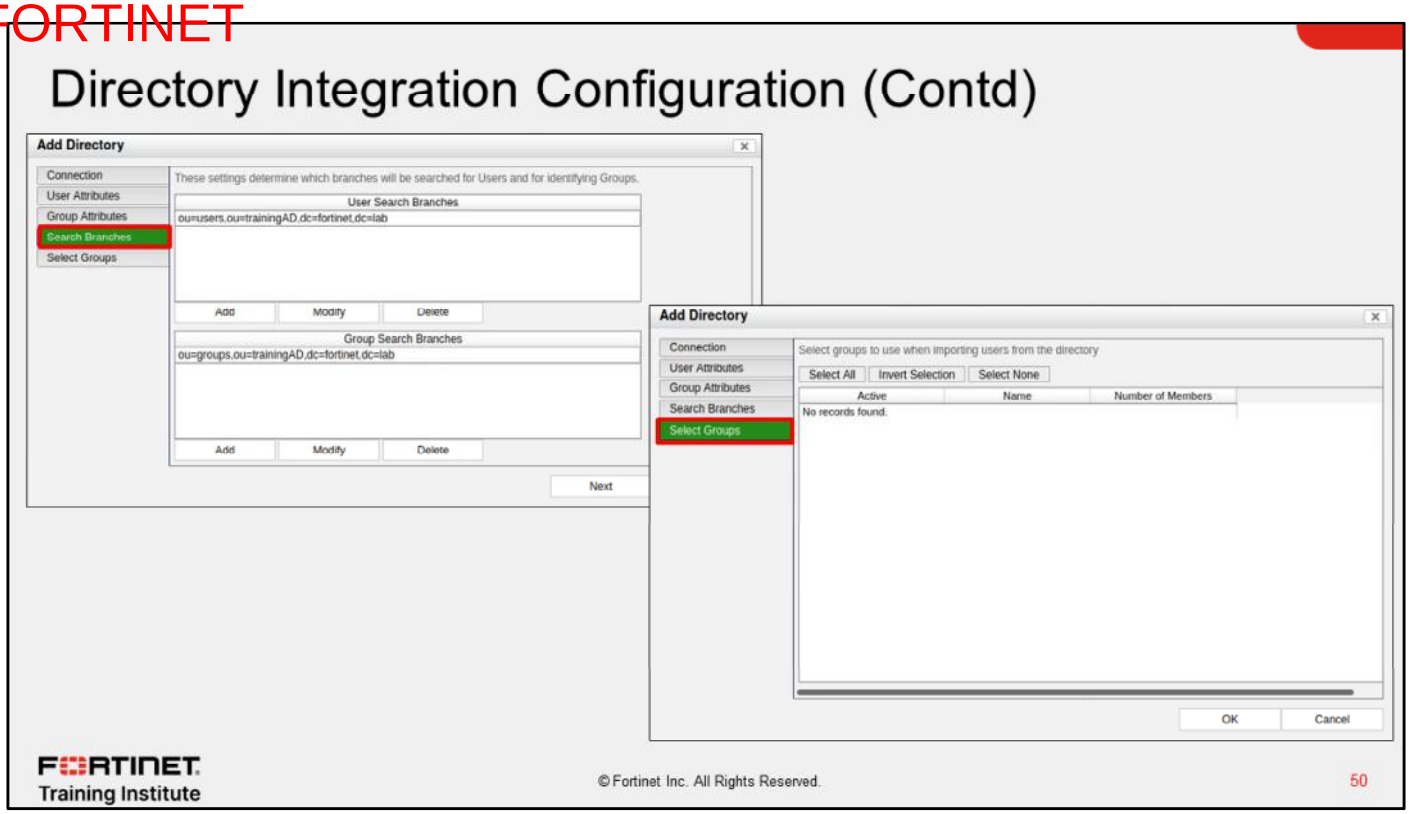


To map user attributes from an LDAP-compliant directory, you must map the user database schema to FortiNAC user data. If the directory type is included in the drop-down list, the default mappings for that directory type are automatically populated. The more complete these mappings are, the more detailed the user records will be in the database. You can also leverage these values within security policies.

Use the **Group Attributes** tab to create mappings for object class, group name, and members. This allows FortiNAC to retrieve the group information based on the **Group Search Branch** configured on the **Search Branches** tab. Groups you create in the directory are imported into FortiNAC each time the directory synchronization task is run, either manually, or by the scheduler.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

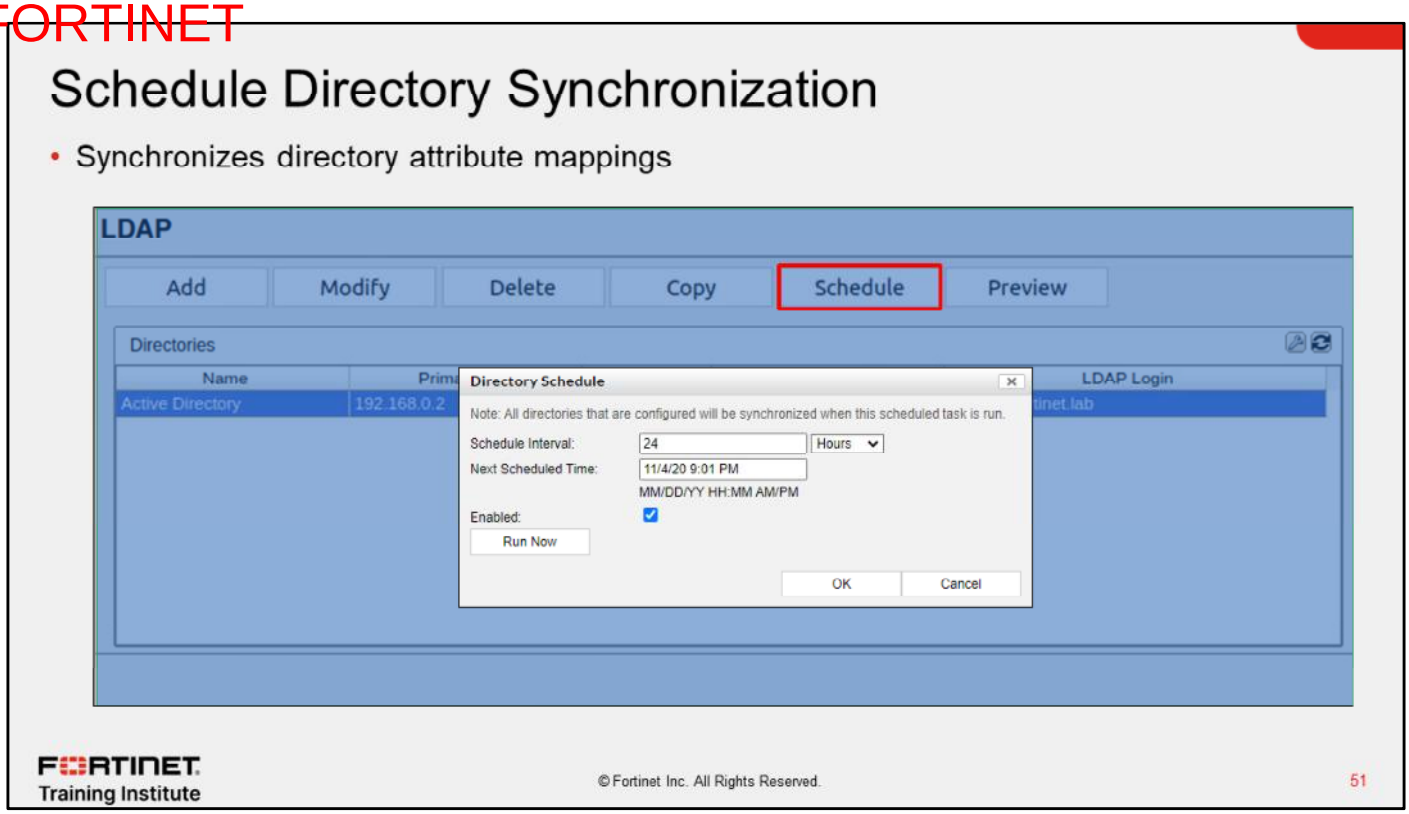


The **Search Branches** tab is where the administrator enters the specific user and group search branches information for the directory server. This tells FortiNAC where the user and group information is located in the directory. The more specific the branches are, the more quickly the lookups are preformed, and the less resource-intensive the process is.

Use the **Select Groups** tab to choose groups of users to be included when the directory and the FortiNAC databases are synchronized. Users that do not already exist in FortiNAC are not imported. However, user data for users already in the database is updated each time the synchronization task is run. Only the user records for users in the selected groups are updated. Users in the directory that are not in a selected group are ignored during synchronization.

Vouchers & Dumps are Available | WhatsApp +201224560923

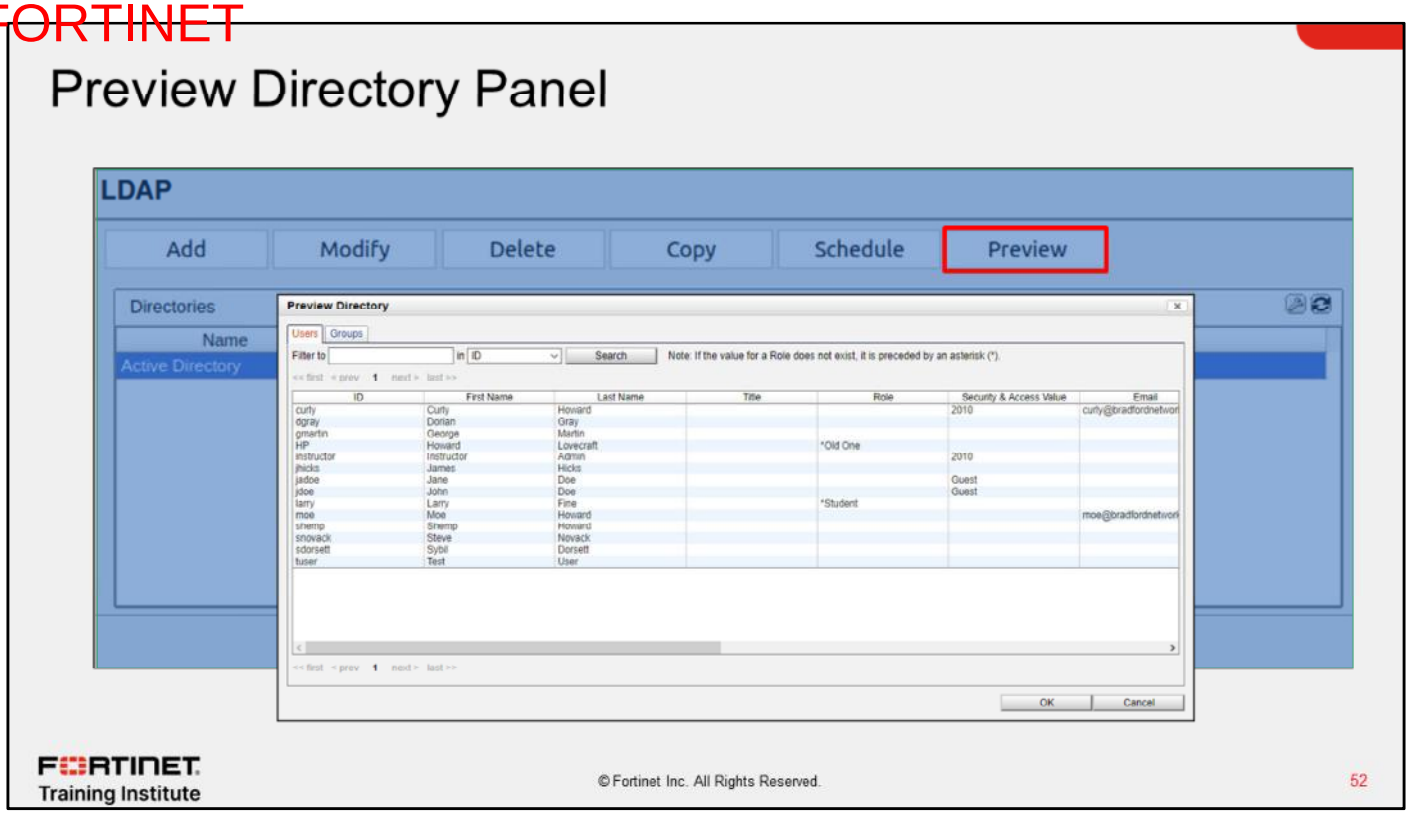
DO NOT REPRINT Brave-dumps.com
© FORTINET



Clicking **Schedule** in the **Directories** view allows the administrator to select a date, time, and poll interval for the directory synchronization task. The scheduled task may also be paused and run manually later. This process modifies the **Synchronize Users with Directory** task in the **Scheduler** view. When the directory and FortiNAC are synchronized, changes made to users in the directory are written to corresponding user records in the database. Keep in mind that when FortiNAC has to validate user credentials, the lookup to the directory is immediate. However, when changes are made to the mapped attributes of a user within the directory, the changes will not appear in the user's record on FortiNAC until the **Synchronize Users with Directory** task runs. Note that the directory is considered the system of record, so changes made there will overwrite changes made on FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

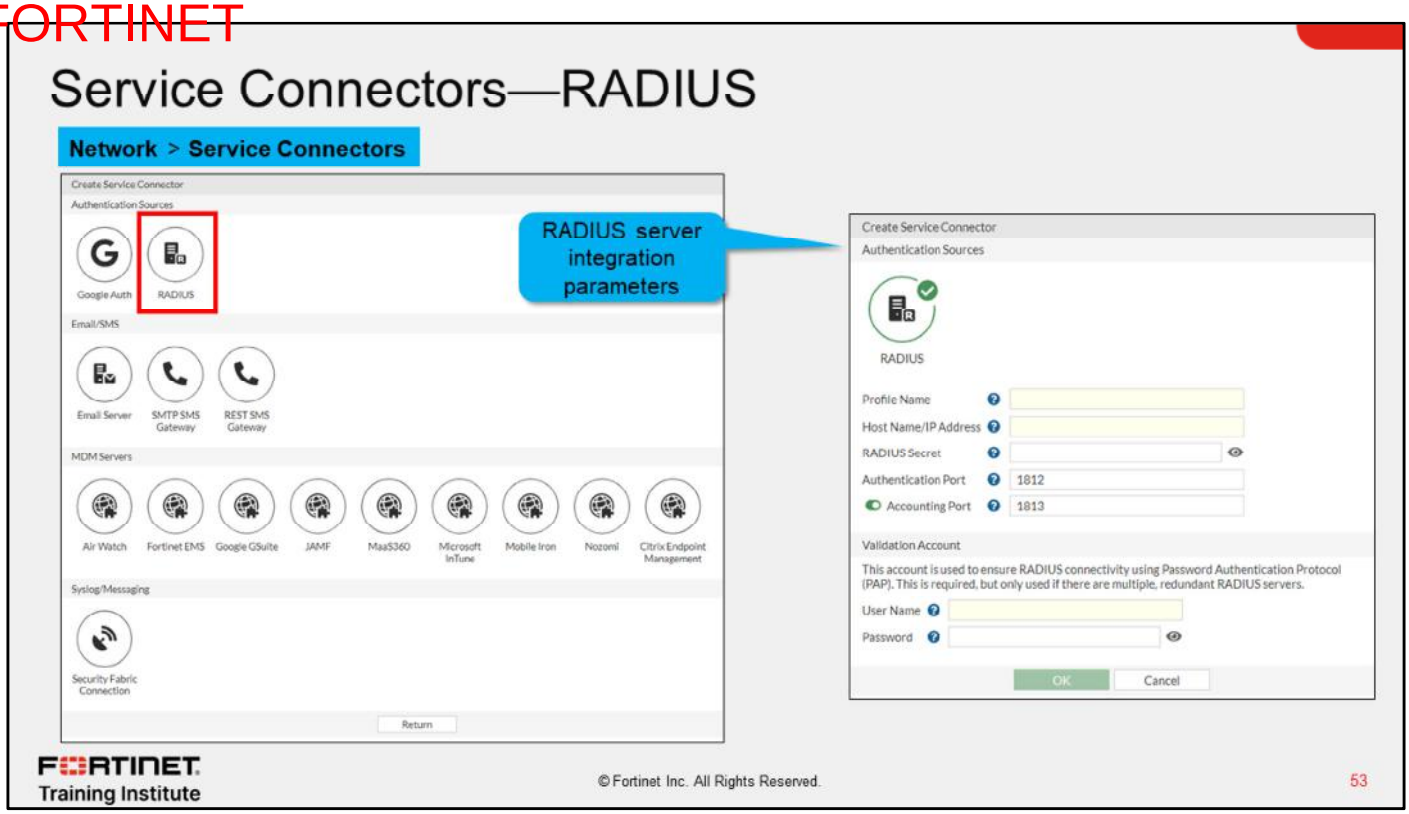
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Preview Directory** panel allows for a real-time lookup against the integrated LDAP server using a filter. This is a great way to verify successful LDAP server integration, as well as validate the attribute mappings. If a value appears in the **Role** column with an asterisk (*), it means that no role with a name equal to this value has been created on FortiNAC. This is a view-only list, and it is not imported into FortiNAC. The **Groups** tab will display identified LDAP groups and the number of members that exist in the directory for each group. You can select these groups for import into the FortiNAC **Groups** view. Note that group members are added into the corresponding FortiNAC group only as the user registers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In environments where FortiNAC manages devices configured for 802.1X, you can configure a back-end RADIUS server or servers.

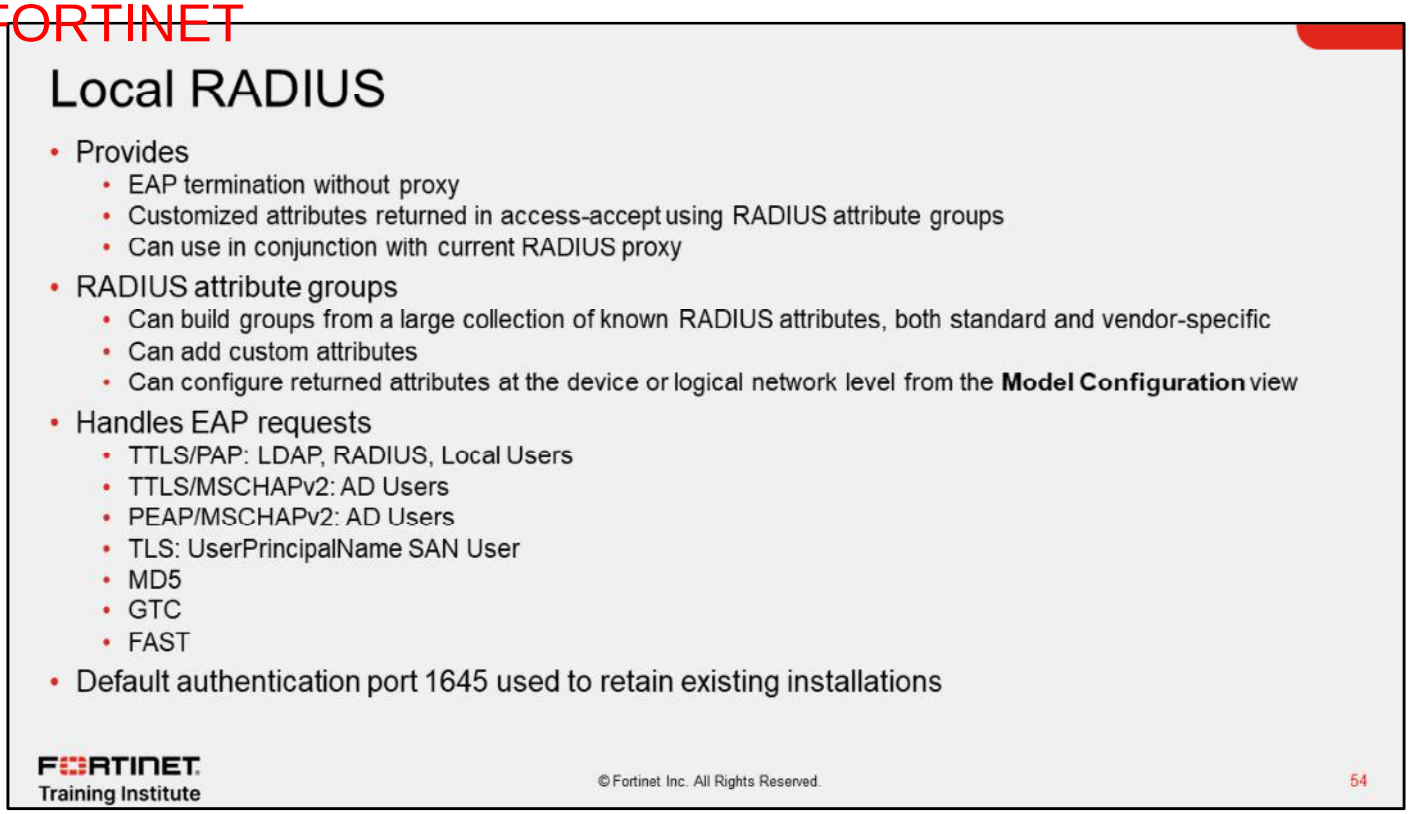
FortiNAC does not terminate 802.1x traffic by default, but instead acts as a proxy between the 802.1X controller, access point, or switch. You can also use RADIUS as the back-end authentication server for end users, guests, contractors, or FortiNAC administrative users.

Add RADIUS servers as service connectors by navigating to **Network** > **Service Connectors,** and then clicking **Create New**. You can add as many RADIUS servers as necessary to the list. You can designate the RADIUS servers for use on a device-by-device basis, and you can set them as a primary or secondary server for each device.

When you add a server, you must supply the host name or IP address, the RADIUS secret, and the authentication port. Optionally, you can configure the accounting port. You must have a validation account for the integration, but use it only if there is more than one RADIUS server configured. You must set the encryption method on the server to use the Password Authentication Protocol (PAP).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The FortiNAC local RADIUS server provides EAP termination for RADIUS authentication. You can customize the RADIUS access-accept packets returned to include RADIUS attributes. Customizable port settings allow for simultaneous use with proxy RADIUS capabilities for flexibility and gradual migration from existing proxy-based authentication.

RADIUS attribute groups can contain both standard and vendor-specific attributes. These attributes can be returned based on default attribute group settings defined at the model configuration level or as part of a logical network assignment. You will learn about these settings in more detail in another lesson.

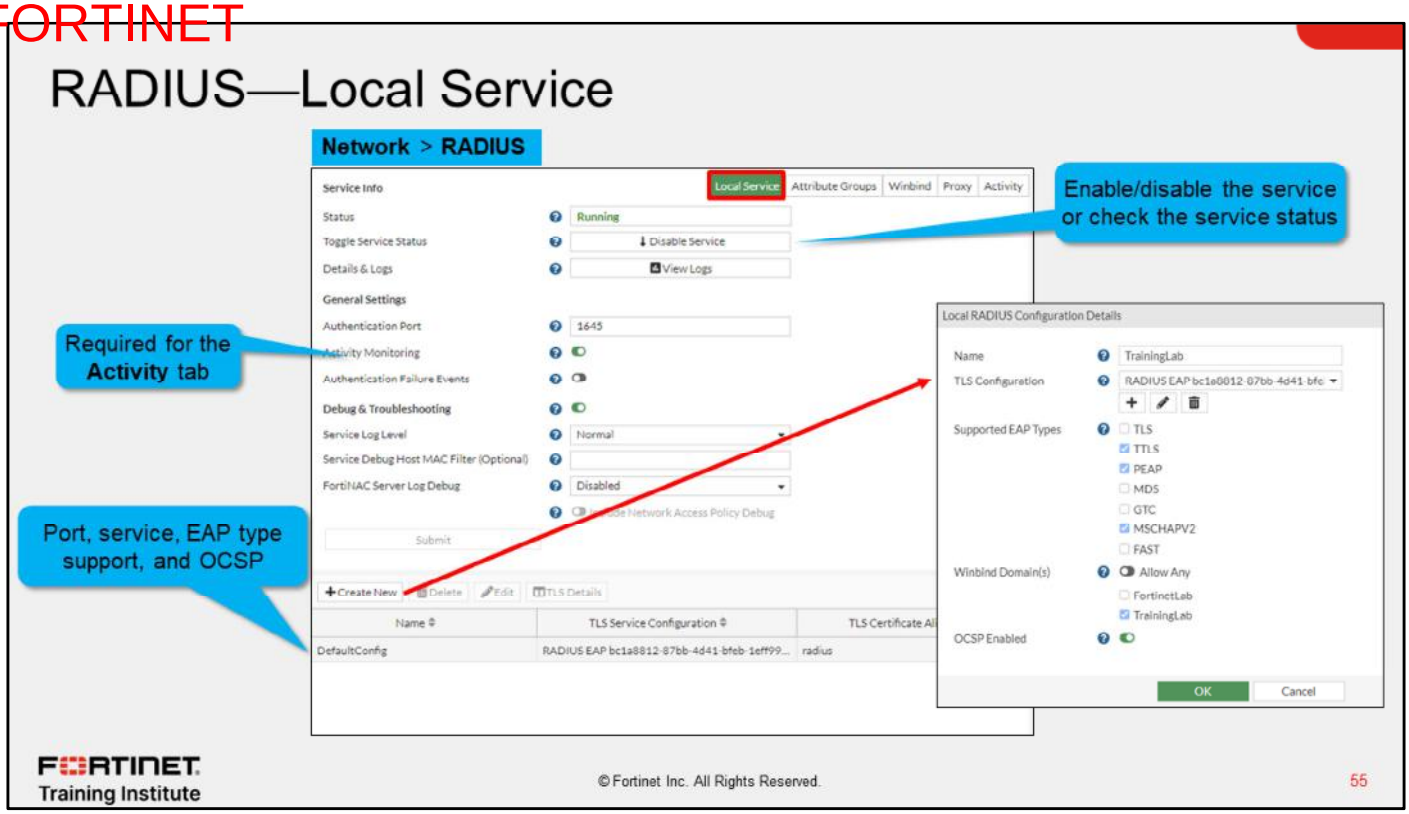
The local RADIUS server requires you to install a server certificate for EAP authentication. The following are the supported 802.1X EAP methods:

- TTLS/PAP: This method handles authentication requests through LDAP servers defined on FortiNAC, RADIUS servers defined on FortiNAC, and local users in the FortiNAC database. These local users include guest accounts.
- TTLS/MSCHAPv2 or PEAP/MSCHAPv2: These methods authenticate AD users only. You must join FortiNAC to the domain and this capability is currently limited to a single domain.
- TLS: This method authenticates UserPrincipalName SAN user from the certificate. This requires you to install the endpoint trust certificate so FortiNAC can validate the client-side certificate.
- MD5: This is a password-based authentication protocol common in wireless networks.
- GTC: This method leverages security tokens for authentication.
- FAST: This method leverages TLS to establish a mutually authenticated tunnel that is then used to send additional authentication data.

By default, the local RADIUS server uses port 1645 for communication.

Vouchers & Dumps are Available | WhatsApp +201224560923

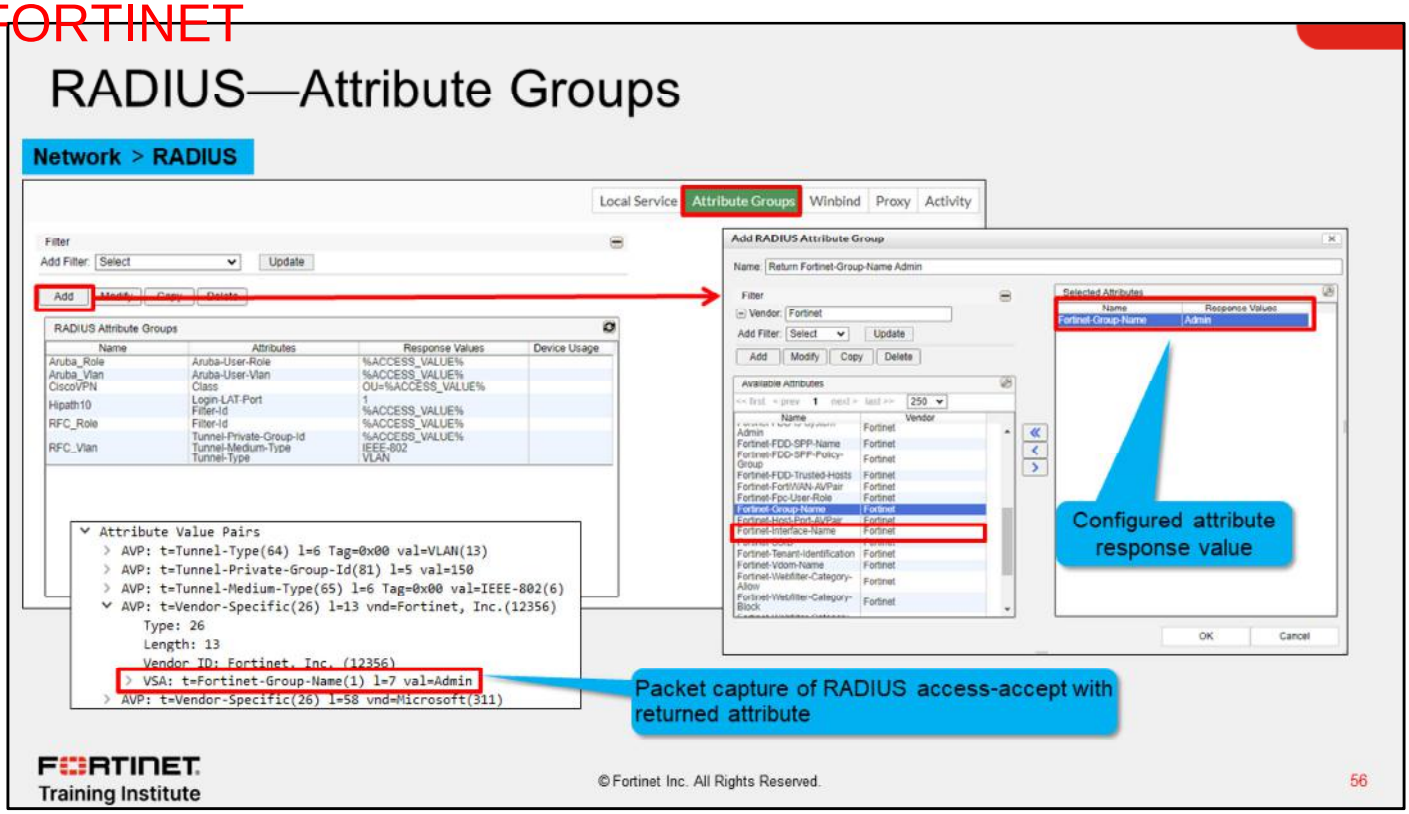
DO NOT REPRINT Brave-dumps.com
© FORTINET



Local RADIUS services are enabled and configured from the RADIUS view. RADIUS log information can be accessed directly from the RADIUS view, and debug and troubleshooting logs can be enabled and filtered. Multiple local RADIUS configurations can be created, each defining the TLS configuration, supported EAP types, winbind domains (winbind instances are managed in the **Winbind** tab), and OCSP settings. These RADIUS configurations can be selected on a device-by-device basis in the **Model Configuration** view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



RADIUS attribute groups allow administrators to control the RADIUS attributes FortiNAC returns in an access-accept packet. You can build these groups by selecting from a large list of standard and vendor-specific attributes.

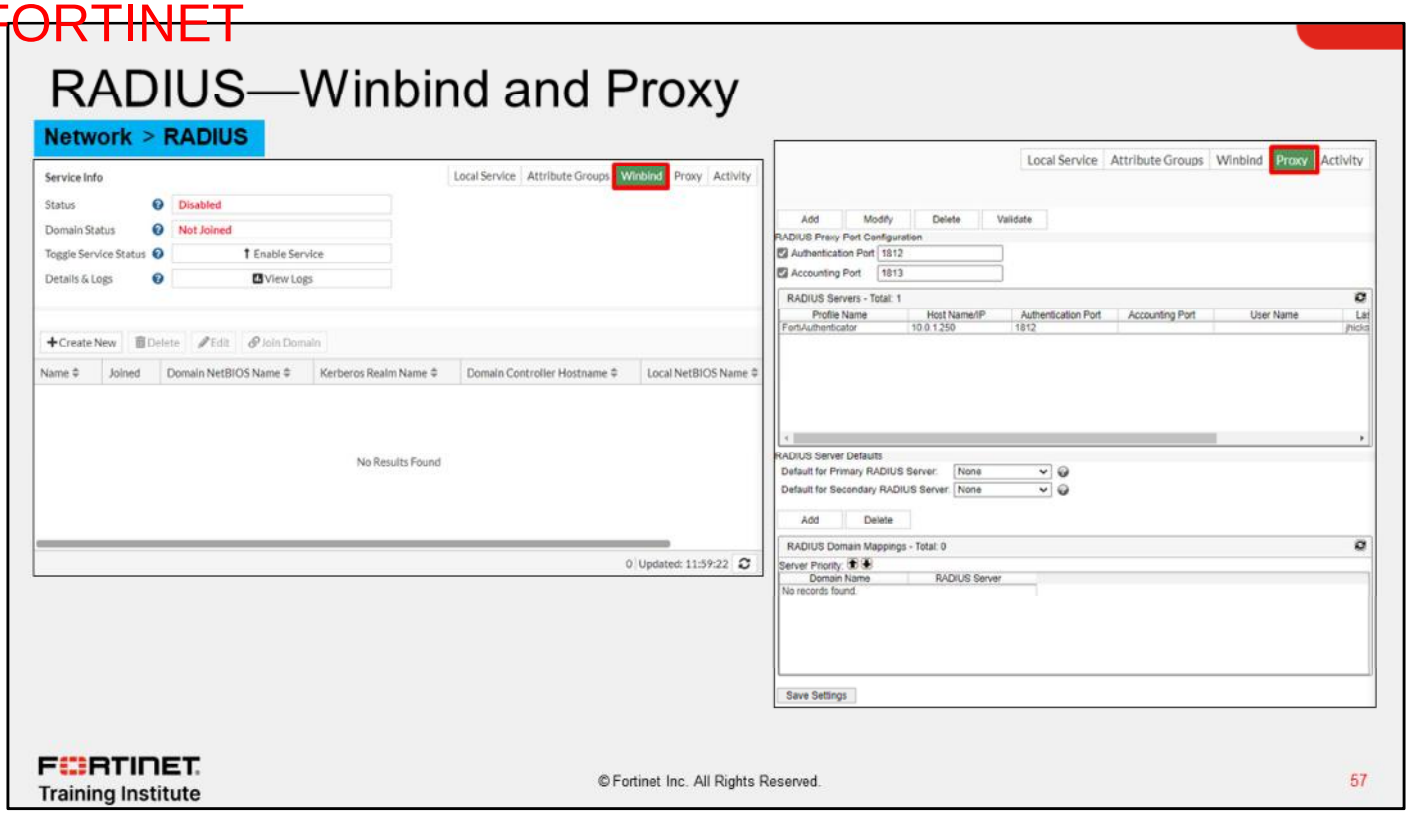
To build an attribute group, click **Add** in the **RADIUS Attribute Groups** window. You must provide a unique name for this attribute group. Next, select from the available attributes list (you can use a filter tool to locate specific attributes) and move the selected attribute to the **Selected Attributes** window. You can then define values for the attributes. You can select attribute lists to be returned as the default group of attributes for a user, or as an access policy-based group leveraging logical networks.

The example shown on this slide shows the RADIUS attribute **Fortinet-Group-Name** value set to `Admin`. The packet capture highlights the RADIUS access-accept packet, with the defined attribute value set.

You will learn about access policies and logical networks in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

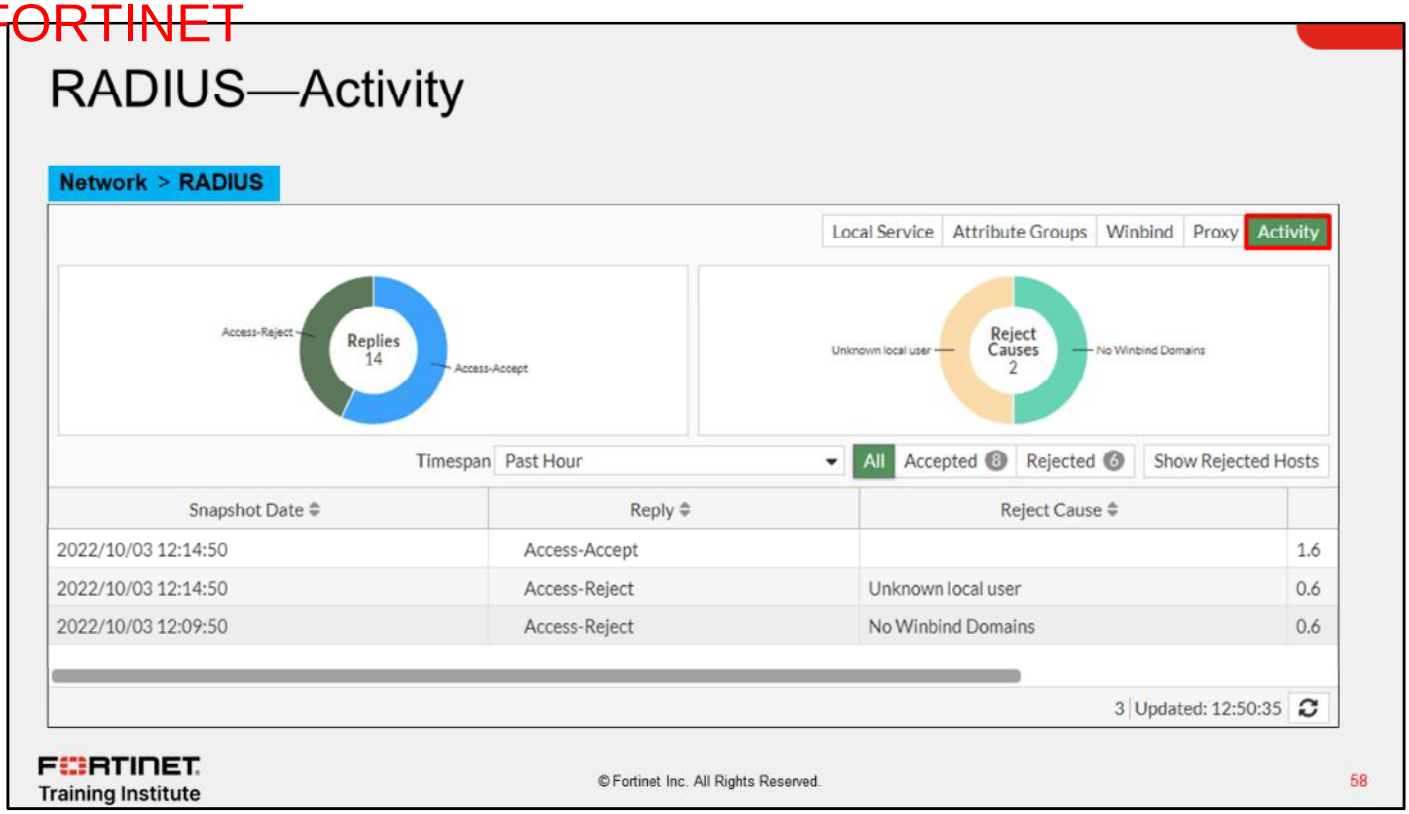


Winbind is used by the FortiNAC local RADIUS server for any MS-CHAP authentication, which requires FortiNAC to be joined to the domain. Multiple Winbind configurations can be added, and you can select one or more in a local RADIUS configuration.

You can configure external RADIUS servers, such as FortiAuthenticator, on the the **Proxy** tab. Once servers have been added you can define a default primary and secondary server. The RADIUS servers can be mapped for domain-specific authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can view RADIUS authentication activity on the **Activity** tab. All activity can be viewed in a single pane, or you can view accepted and rejected replies separately. Another setting will provide a list of rejected hosts. The **Activity** view is available only if the **Activity Monitoring** setting is enabled on the **Local Service** view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is the function of the **User Attributes** settings in an LDAP integration?

✓A. To map user information to FortiNAC user records

B. To define which LDAP-compliant server to use, based on user ID

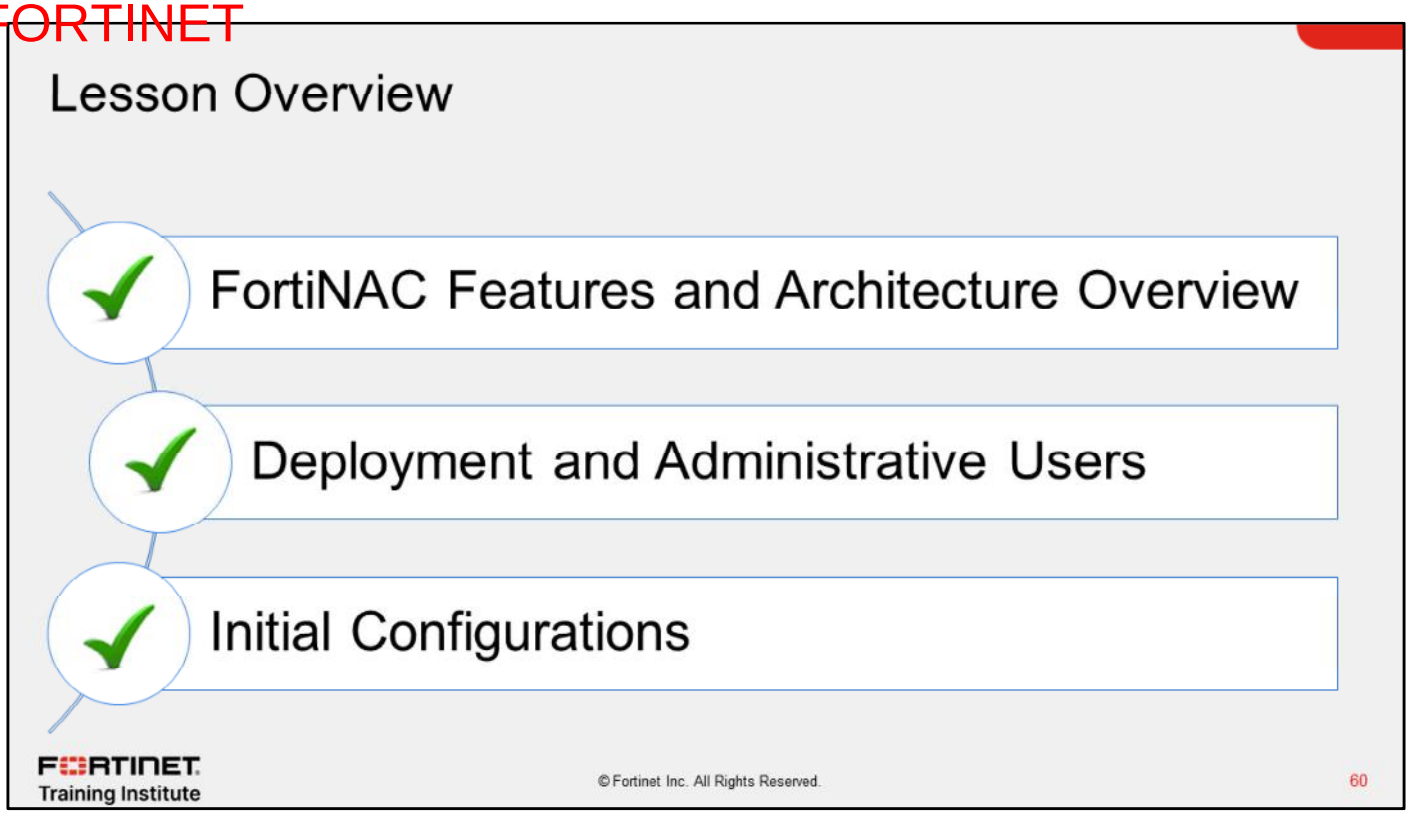
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

59

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

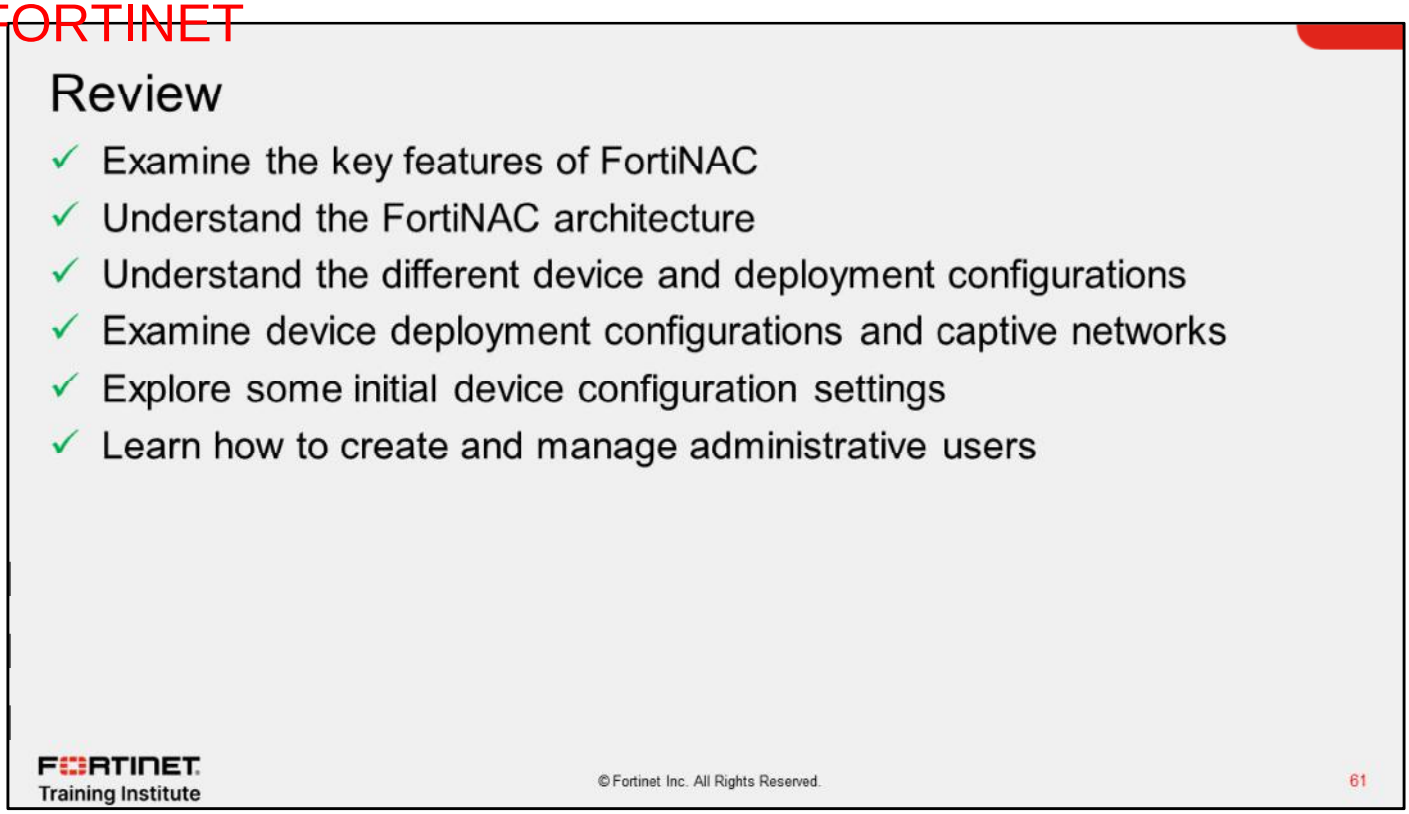


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

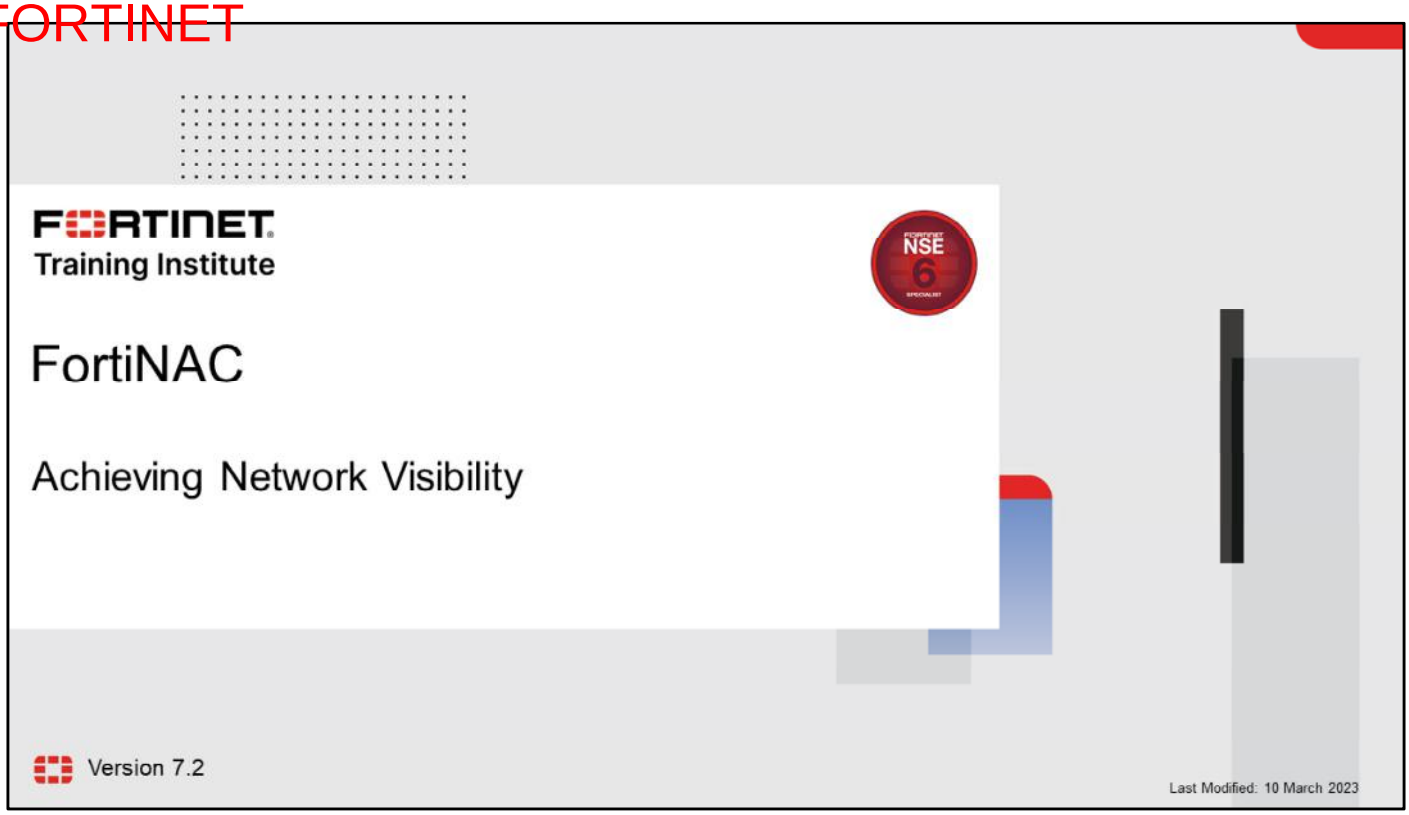


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the fundamentals of FortiNAC, its deployment configurations, and some initial deployment settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

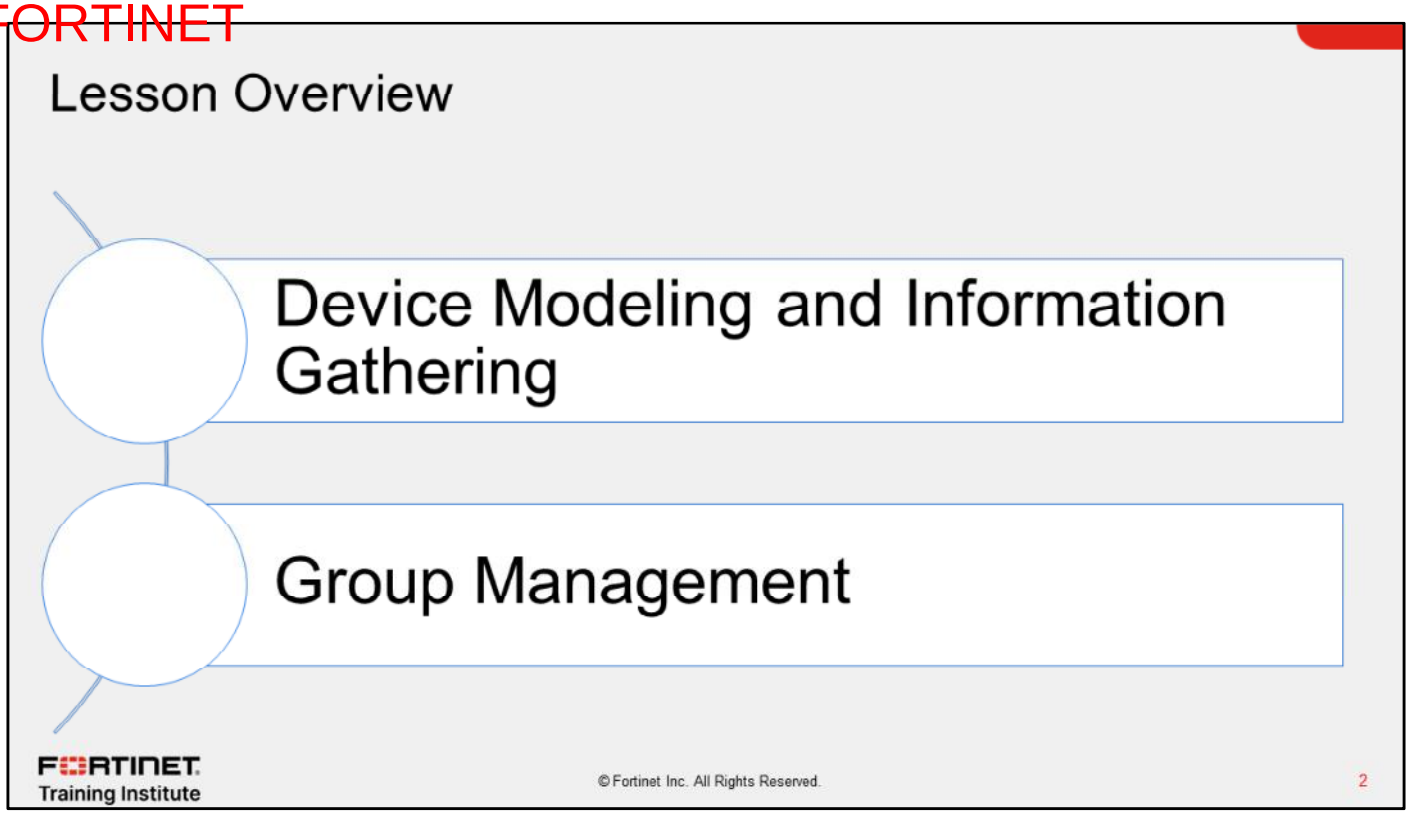
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to integrate FortiNAC with the network infrastructure.

Vouchers & Dumps are Available | WhatsApp +201224560923

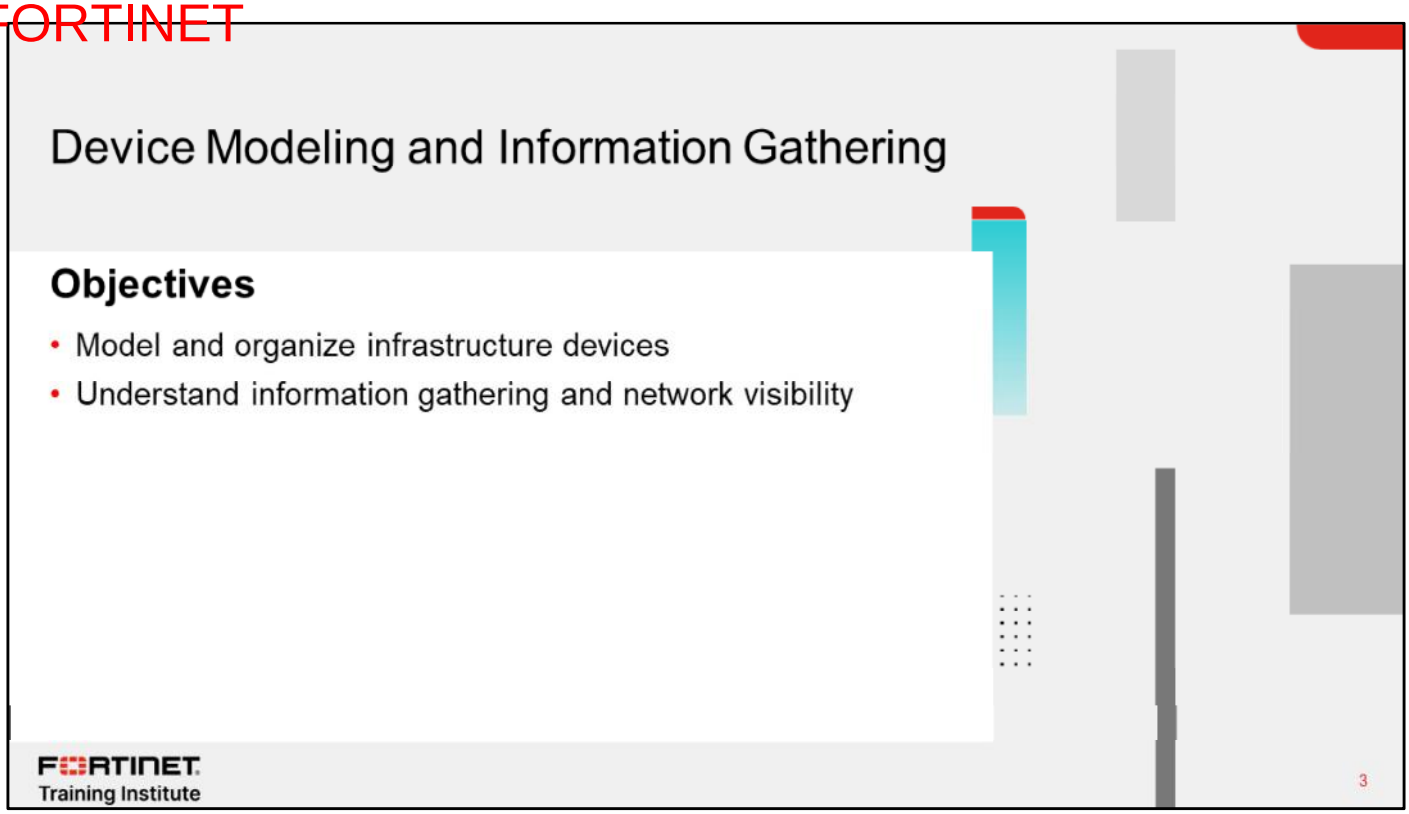
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

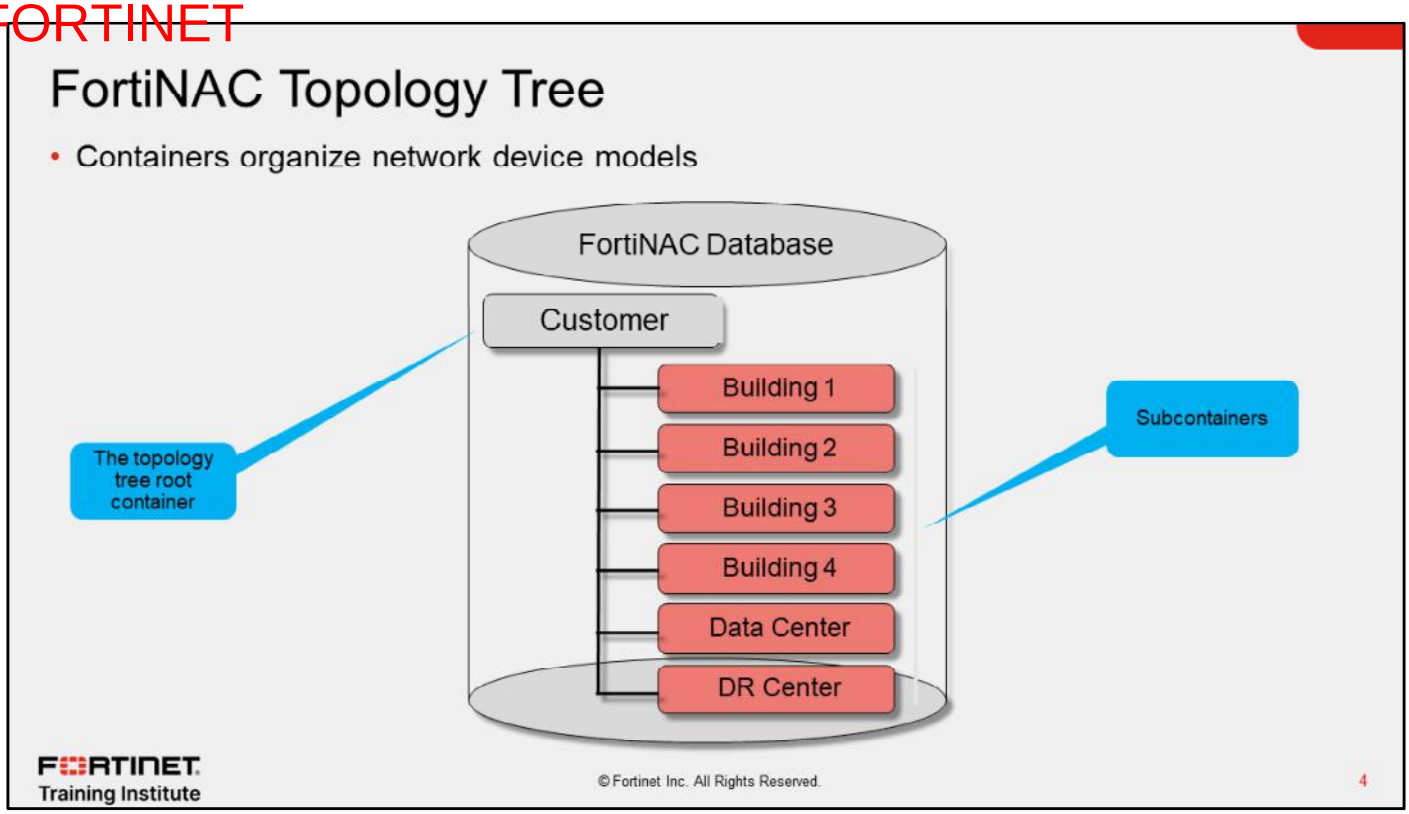


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in integrating FortiNAC with the network infrastructure to gather visibility information from endpoints and control the capabilities of the integrated devices, you will have a solid foundation for the implementation and ongoing administration of some of they key components of a FortiNAC deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

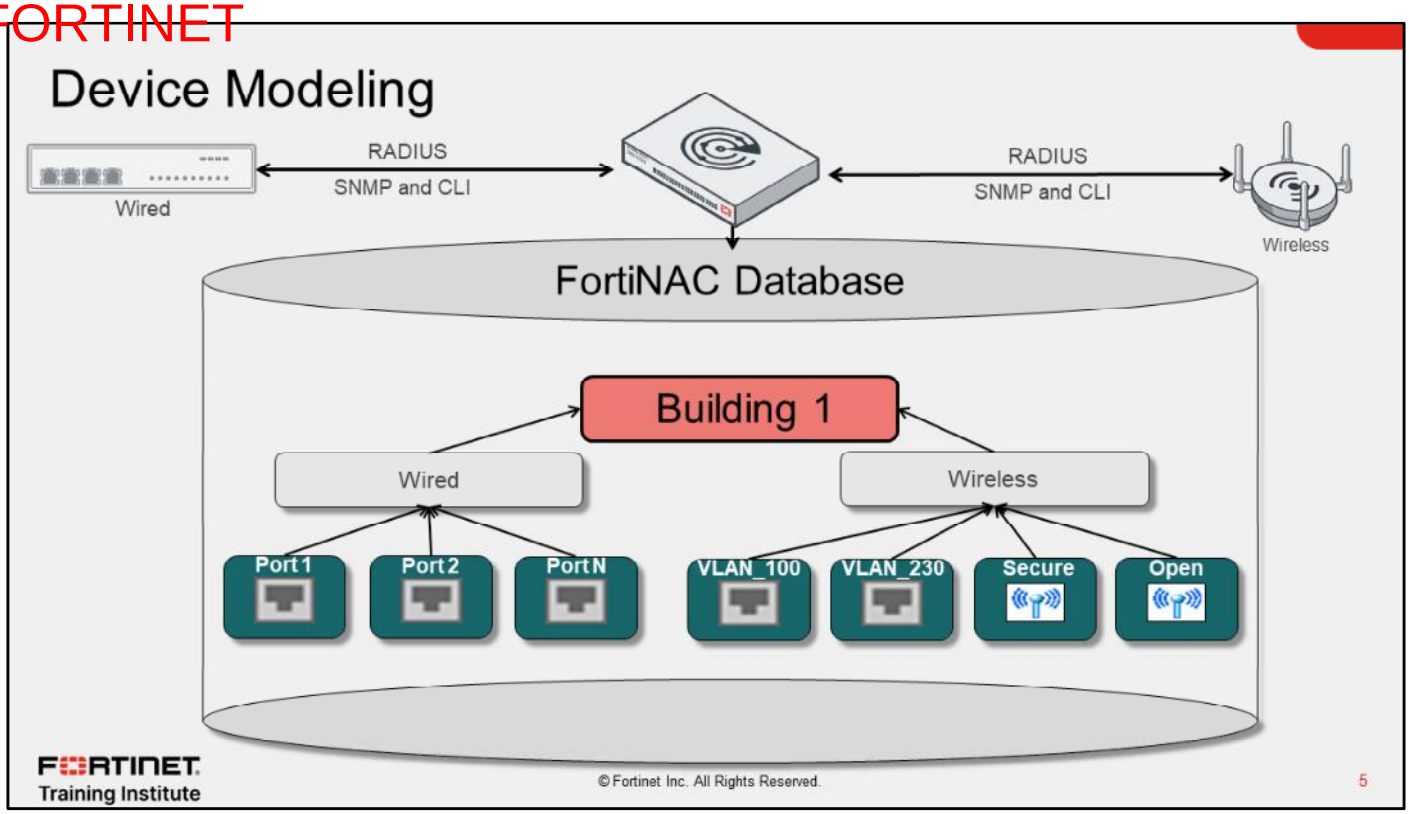
DO NOT REPRINT Brave-dumps.com
© FORTINET



Infrastructure devices, such as switches and routers, are organized within the topology tree panel of the **Inventory** view. A single root container that can have any number of subcontainers created within it. You can model devices only within the sub-containers. As a best practice, you should model infrastructure devices within the topology tree in a manner that makes it easy to locate any network port. You can add or remove containers at any point, and move modeled devices from one container to another at any time. Note that deleting a container will also delete any devices modeled within that container. You can use the containers that you build here in other parts of the product as a way to indicate location and as a way to provide additional information for adapter points of connection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

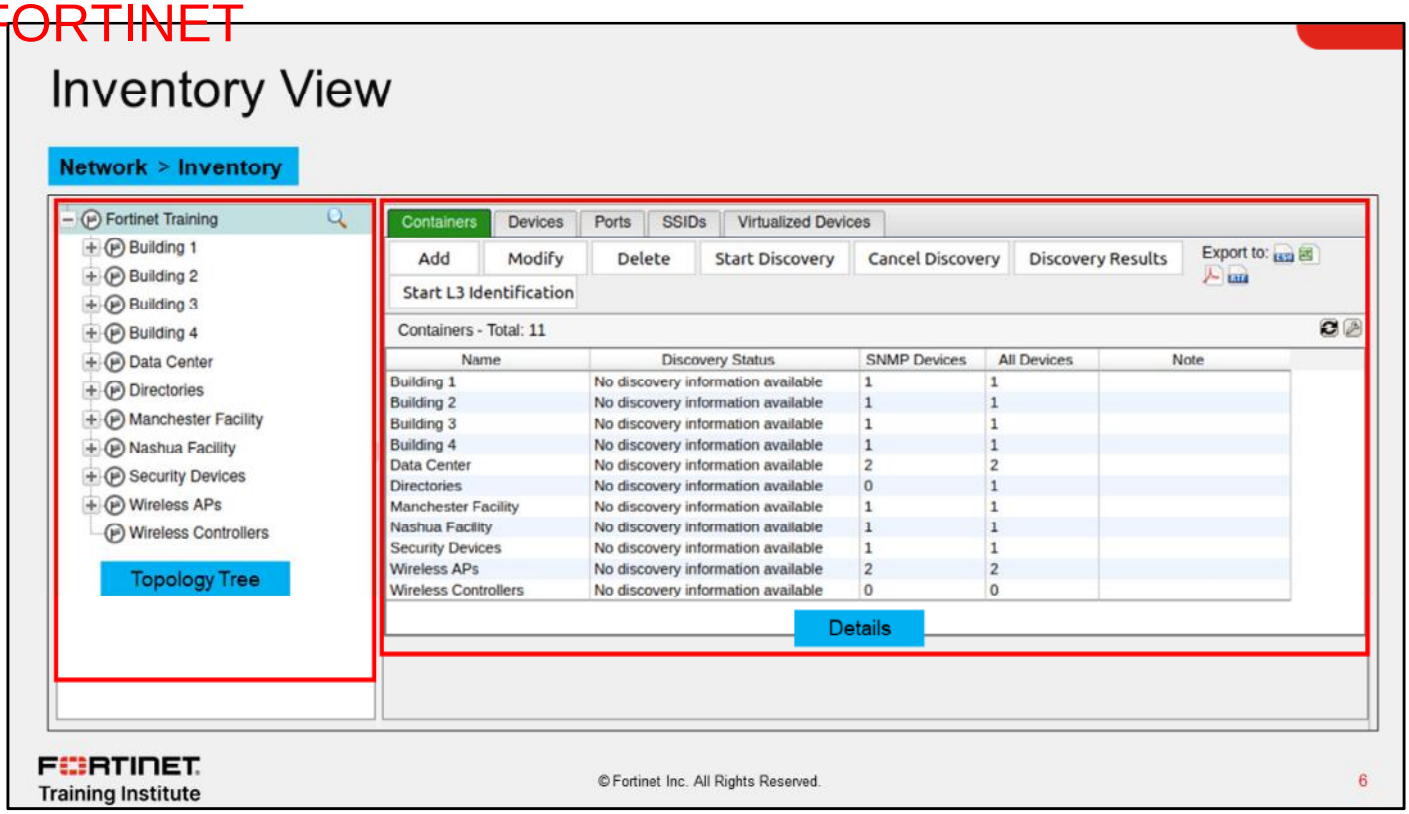


When you model a device, the FortiNAC system initially uses SNMP as a method of communicating with the device to identify the device type. Using the device sysObjectID, FortiNAC can identify the vendor and model of the device. This, in turn, identifies the necessary command sets and methods to be used when the CLI is used for visibility gathering and device control.

FortiNAC also uses collected MIB information to identify the number of ports, the administrative state of the ports, and the physical address of each port. On the FortiNAC GUI, RJ45 port icons represent each port on a wired infrastructure device. The same RJ45 port icons identify different things when it comes to wireless devices. For example, when a Fortinet wireless device is modeled, the RJ45 ports will be used to represent the different VLANs that are configured on the AP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

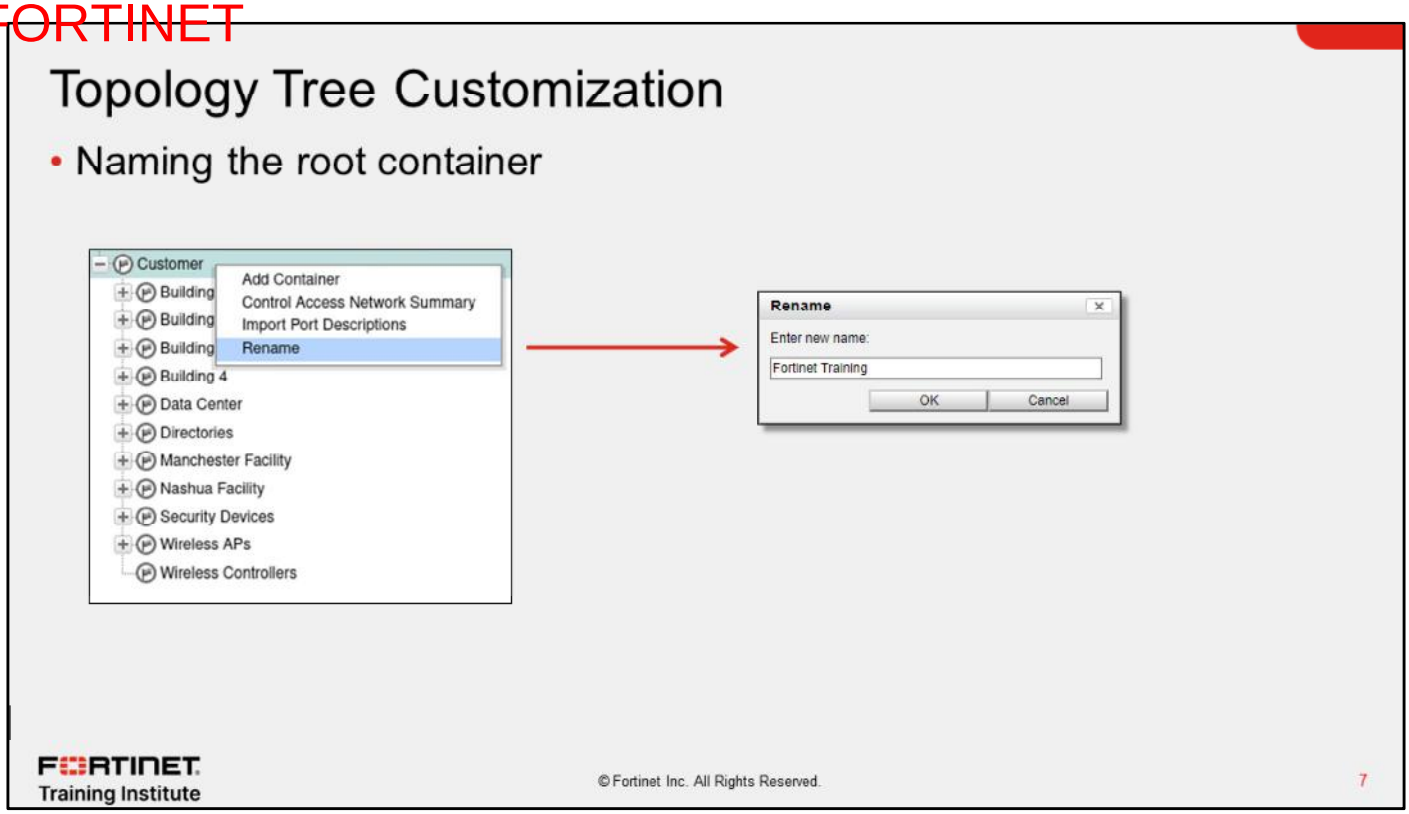


The **Inventory** view is broken into two sections. On the left side, the topology tree contains the root container and all subcontainers created within it. You can expand each container to show the devices modeled within it. On the right side is the details panel, which displays topology information across several tabs.

When you select a container, the possible tabs displayed are **Containers**, **Devices**, **Ports**, **SSIDs**, and **Logical Networks**. The tabs displayed will depend on the selected container. For example, the **Container** or **Logical Networks** tabs will appear only when you select the root container.

Vouchers & Dumps are Available | WhatsApp +201224560923

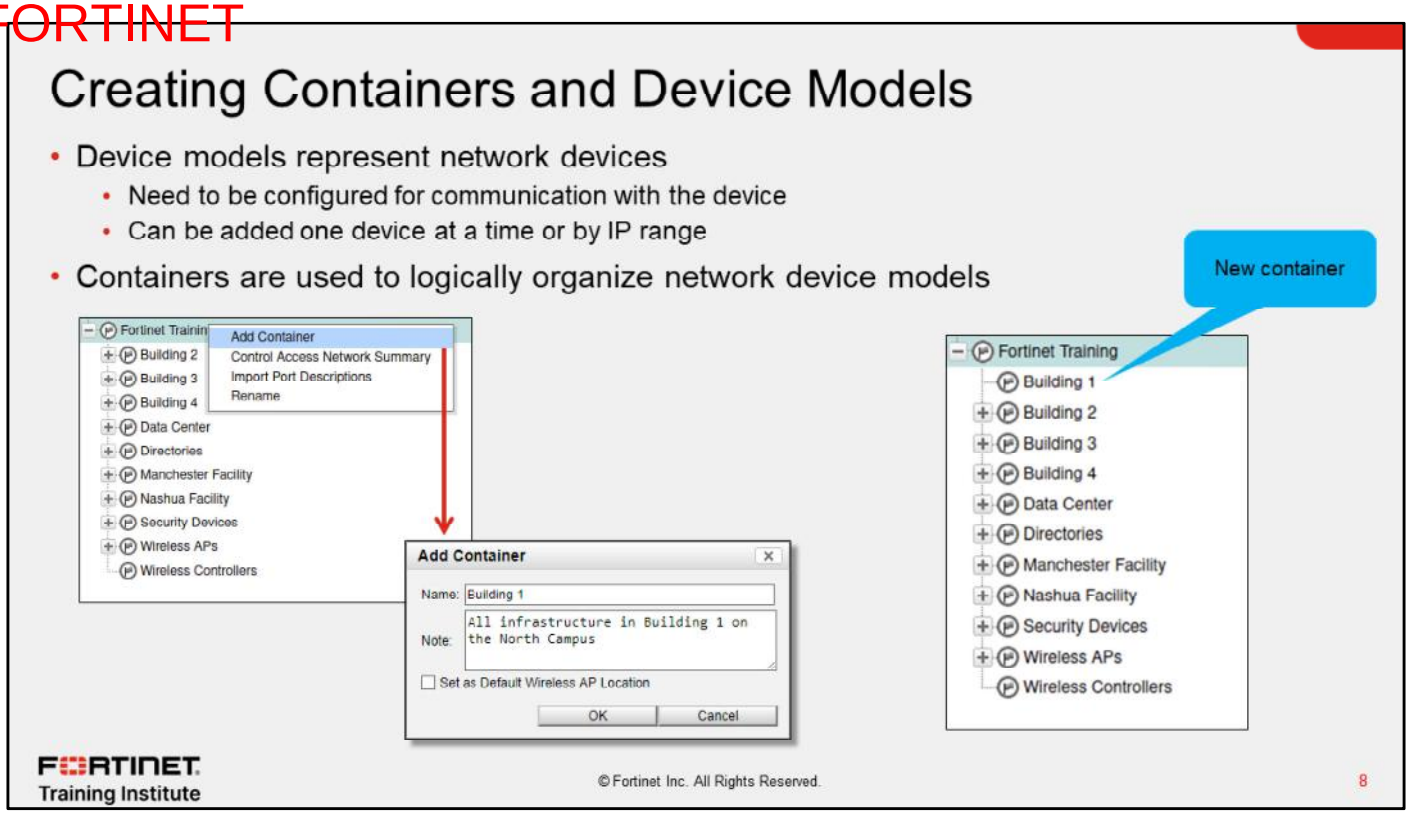
DO NOT REPRINT Brave-dumps.com
© FORTINET



To rename the root container, right-click the root container and then, in the drop-down list, select **Rename**. A dialog box opens and you can type the new name. After you click **OK**, the container updates to reflect the change.

Vouchers & Dumps are Available | WhatsApp +201224560923

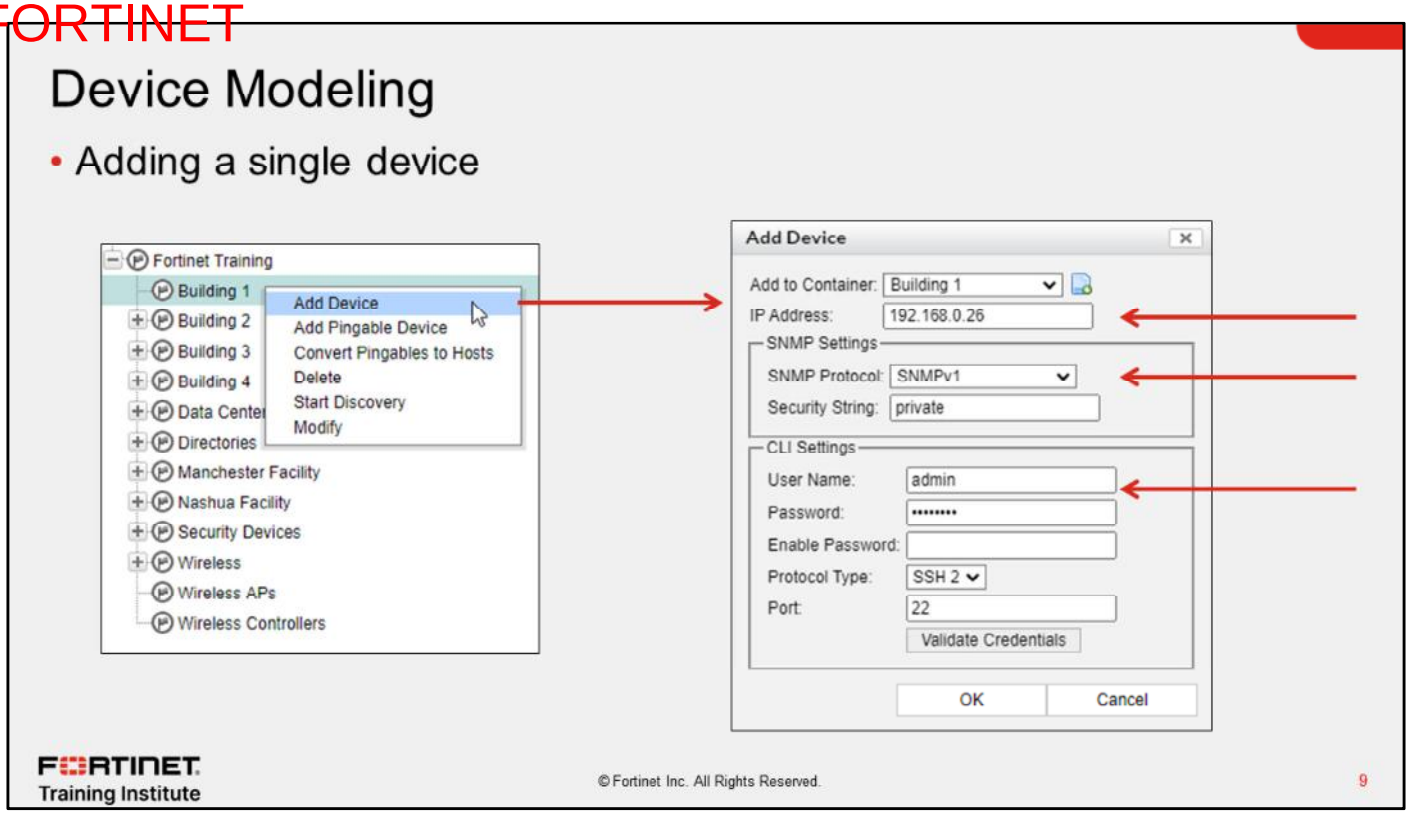
DO NOT REPRINT Brave-dumps.com
© FORTINET



To create subcontainers, right-click the root container and select **Add Container**. The **Add Container** dialog box opens, allowing you to give the container a name and add notes. After you click **OK**, the new subcontainer appears in the topology tree after a few seconds. The root container is the only container that allows the creation of subcontainers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To model a single SNMP-capable device, right-click the desired subcontainer and select **Add Device** in the drop-down list. The **Add Device** dialog box opens.

At the top of the dialog box, you can choose to change the container the device will be modeled in. By default, the device is modeled in the container that you right-clicked. Type the IP address of the device.

In the **SNMP Settings** section, select SNMP version 1 or version 3 and type the read/write security string.

In the **CLI Settings** section, configure the settings for **User Name**, **Password**, and **Enable Password** (if necessary) and select the appropriate protocol: Telnet, SSH1, or SSH2.

FortiNAC will use the SNMP and CLI settings to gather visibility information and for control purposes. If the username and password supplied do not grant access to configuration capabilities, then you must configure the **Enable Password** setting. If the username and password combination do grant access to the configuration capabilities, then you must leave the **Enable Password** field empty.

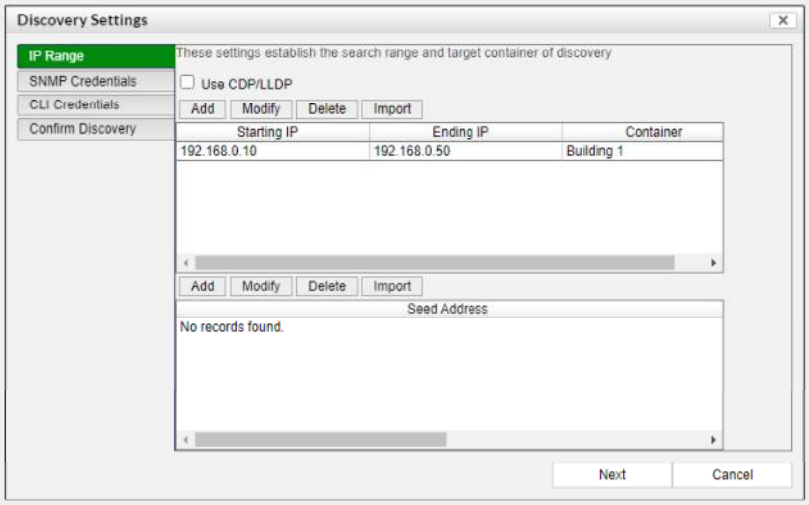
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Device Modeling (Contd)

- Discovering multiple devices





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

In large environments, individually adding devices can be a tedious task. Instead you can right-click a subcontainer and select **Start Discovery** to open the **Discovery Settings** dialog box.
On the **IP Range** tab, you can select Cisco Discovery Protocol (CDP), LLDP and/or address ranges. If you select **Use CDP/LLDP**, you must enter a seed device address.

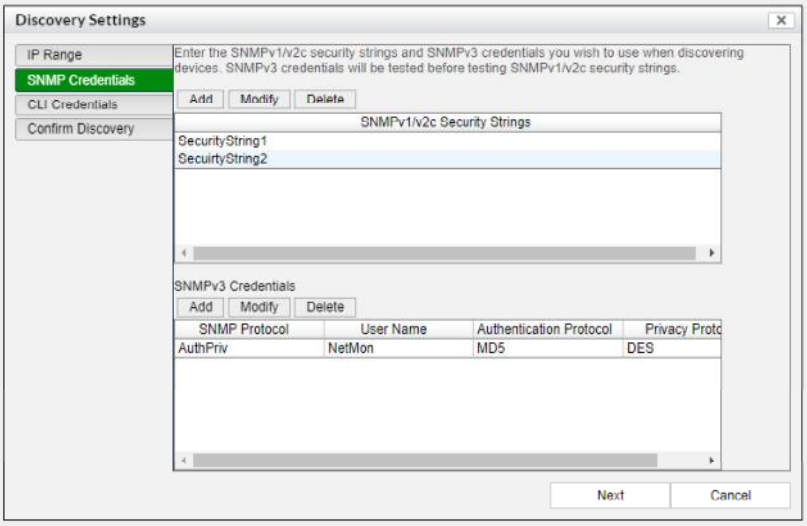
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Device Modeling (Contd)

- Discovering multiple devices





FORTINET Training Institute

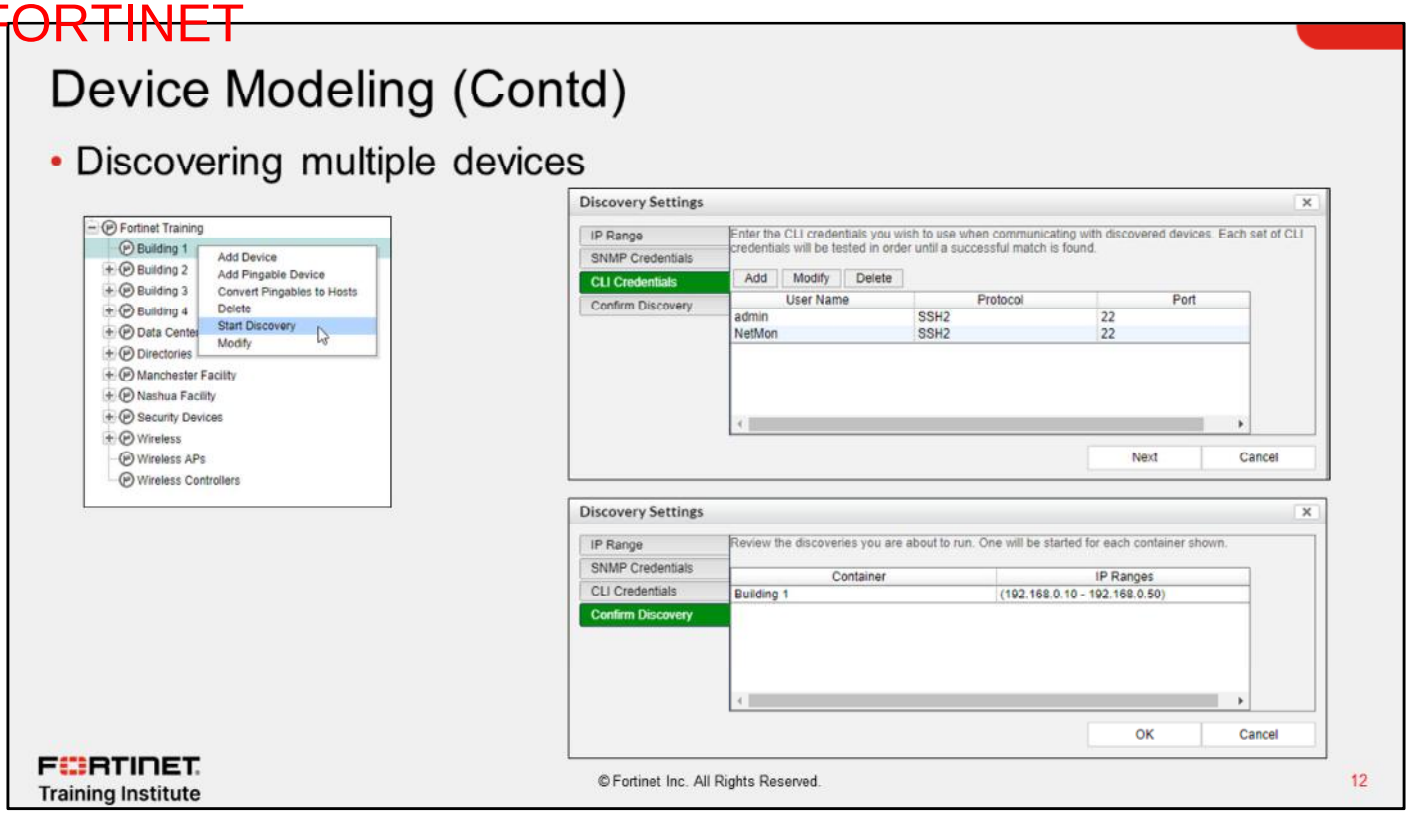
© Fortinet Inc. All Rights Reserved.

11

On the **SNMP Credentials** tab, you can add SNMP V1 or V2c security strings, as well as V3 credentials. FortiNAC tests each SNMP entry against each device, in order, until one is found that works or the list is exhausted.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

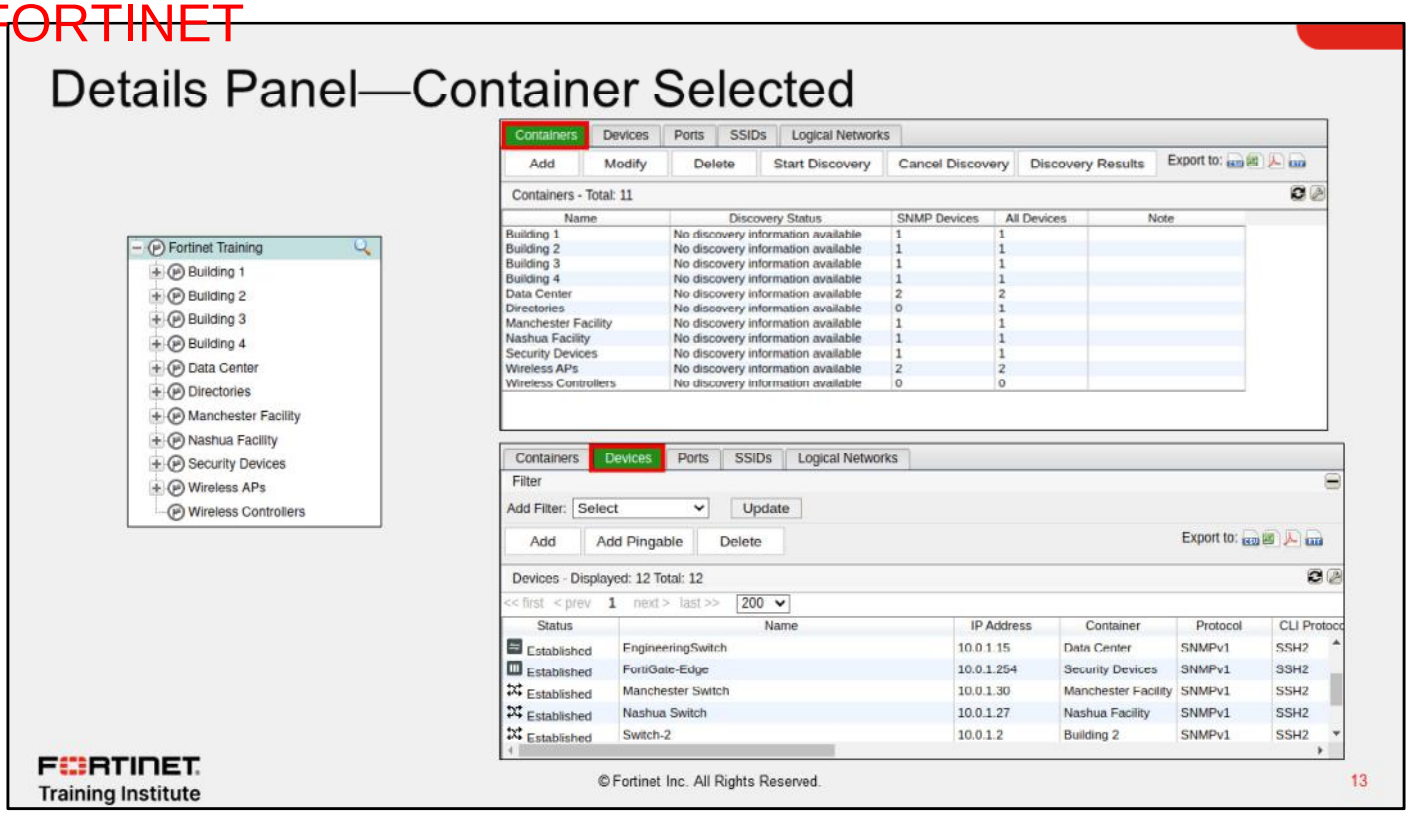


On the **CLI Credentials** tab, you can configure a list of user names, passwords, enable passwords settings, and protocol settings. FortiNAC attempts each entry in the list, in order, until valid credentials are found or the list is exhausted.

The **Confirm Discovery** tab summarizes all the container and IP range information you entered on the **IP Range** tabs. Click **OK** to initiate discovery.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

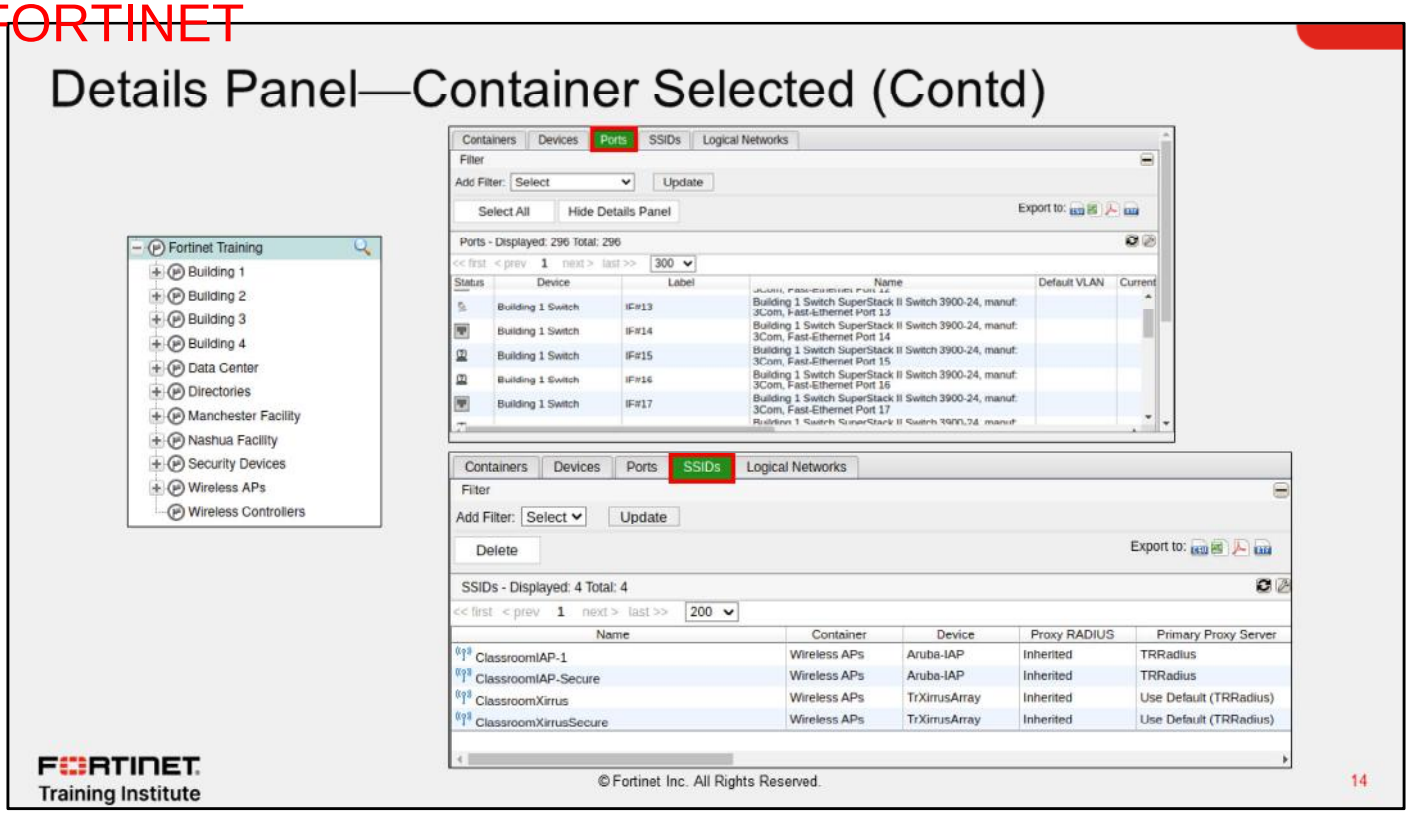


Selecting a container in the topology tree will provide access to several tabs of information. This slide shows the information displayed on the first two tabs.

The **Containers** tab shows a list of all sub containers that exist within the topology tree. This tab is displayed only if the root container is selected. The **Devices** tab displays all devices within a selected subcontainer.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



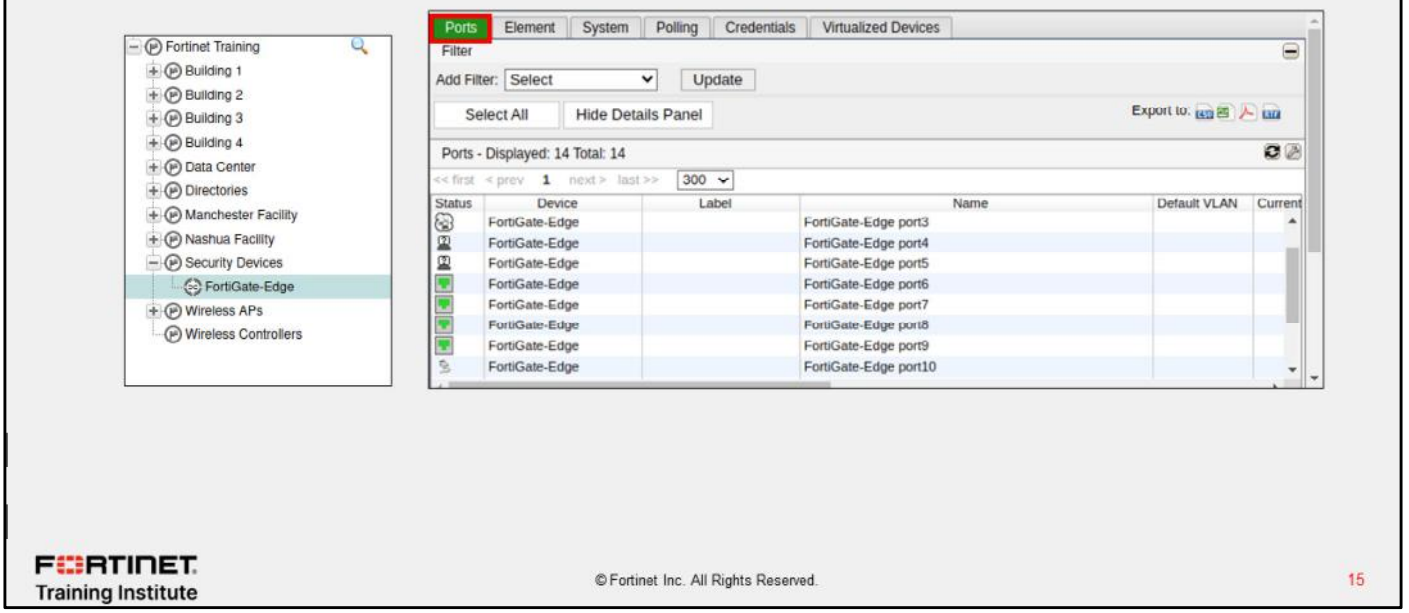
The **Ports** tab displays all ports of all devices within the selected container. The **SSIDs** tab displays all SSIDs from all devices within the selected container.

If you selected the root container, all elements of the inventory view will be displayed for each of the tabs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Details Panel—Device Selected



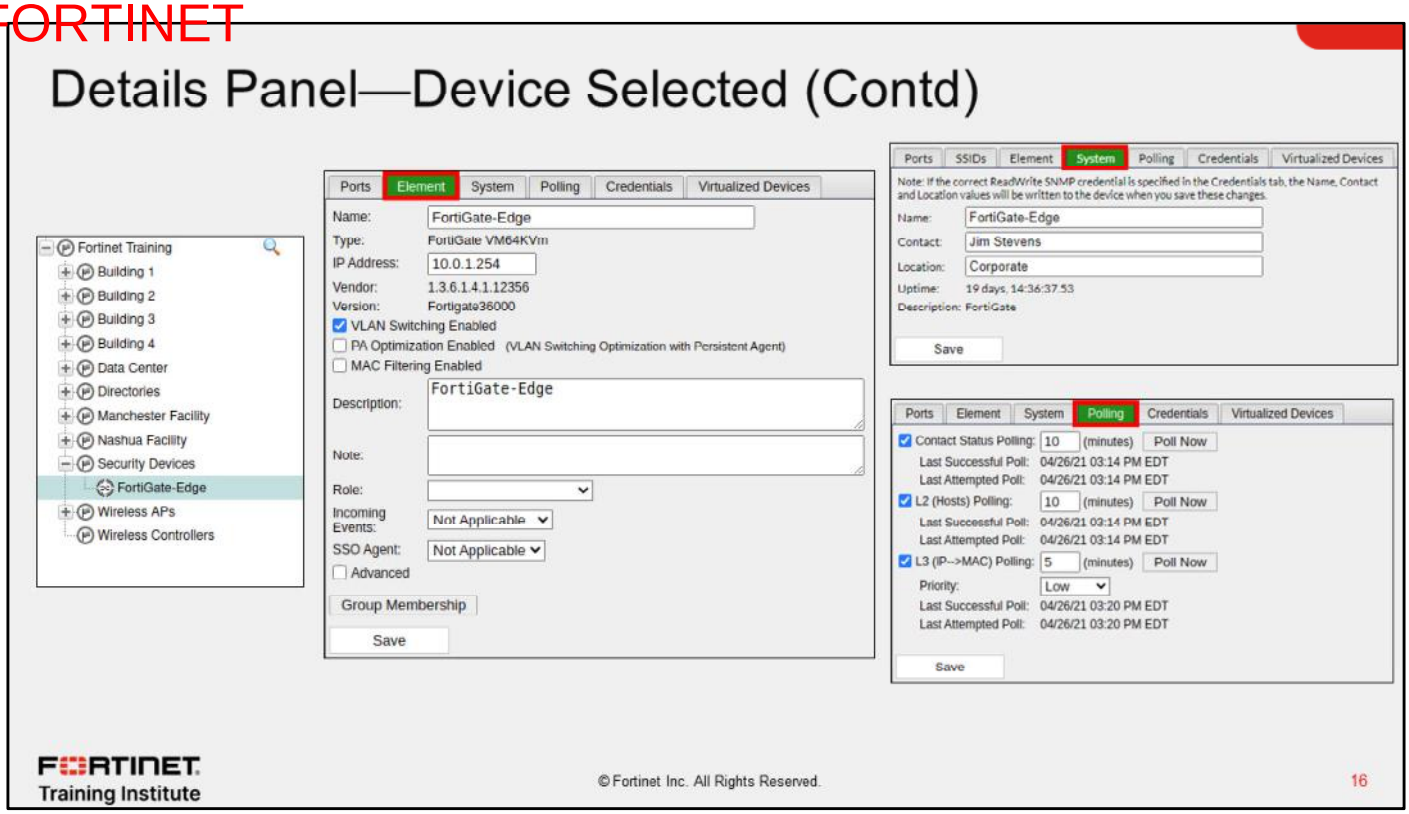
When you select an individual switch or router the following tabs will be displayed for most infrastructure devices:

- **Ports**
- **SSIDs** (if applicable)
- **Element**
- **System**
- **Polling**
- **Credentials**
- **Virtualized Devices** or **Model Configuration**

The **Ports** tab will display all ports that are associated with the selected device model as well as information about each port, including what is currently connected, the default VLAN, the current VLAN, and so on. When selecting a wireless device, such as an AP or a FortiGate managing an AP, port icons will be used to represent more than just physical wired ports, such as VLANs, roles, or groups, depending on the wireless vendor.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Element** tab provides detailed information about the selected device and configuration options. You can set the following from the **Element** tab:

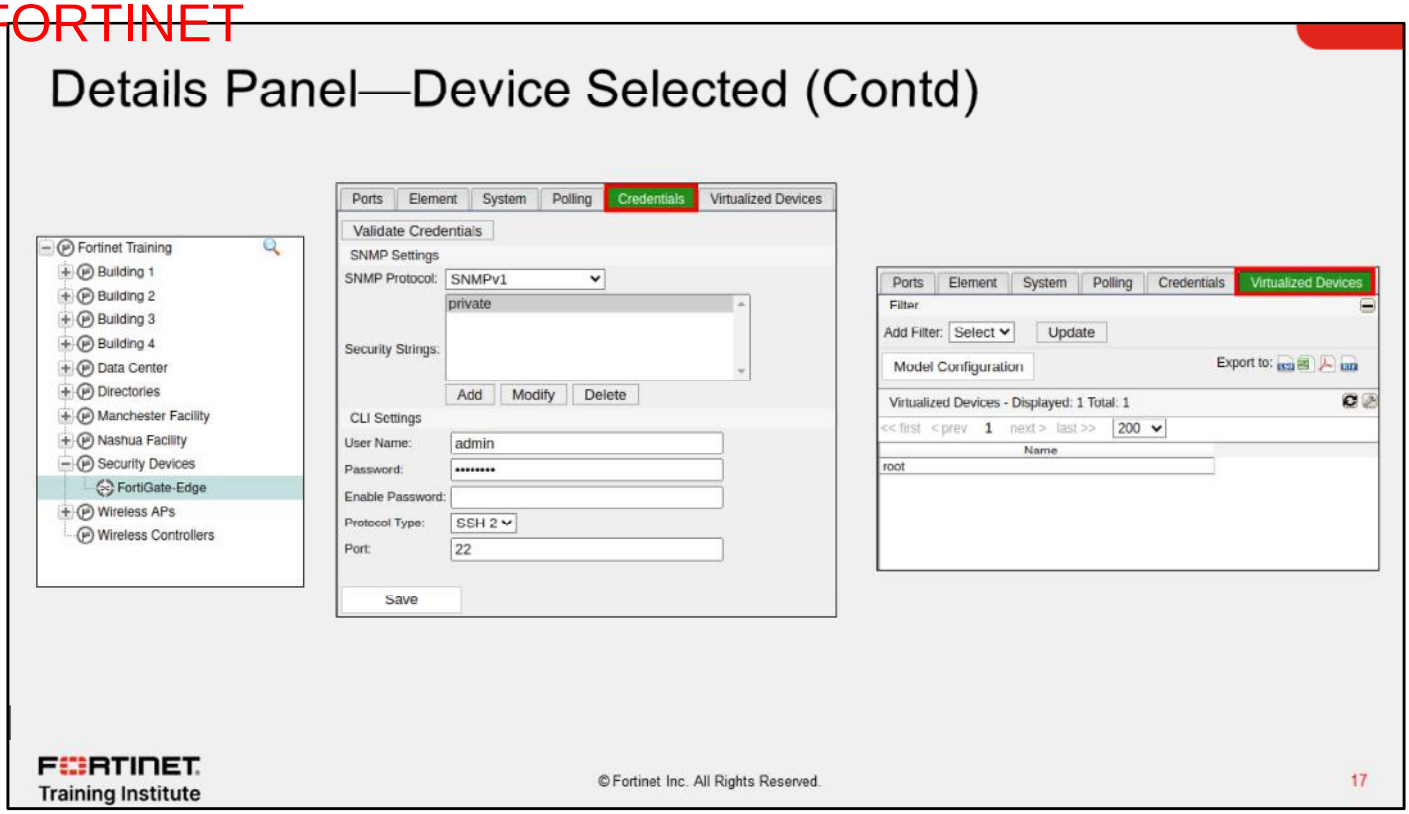
- **Name**: This is the name that will be displayed in the inventory tree.
- **IP Address**: This is the IP address of the device
- **VLAN Switching Enabled**: If selected, FortiNAC will change VLANs for connecting hosts based on policy or status.
- **PA Optimization Enabled**: If selected, FortiNAC will change VLANs for hosts running the persistent agent more efficiently.
- **MAC Filtering Enabled**: If enabled, a host that has been disabled on FortiNAC will have its MAC address filtered at the switch.
- **Role**: A FortiNAC role can be assigned to the device.
- **Description** and **Note**: These are fields for identifying information about the device.
- **Incoming Events**: You can select for incoming event type and parser for automation and integration.
- **SSO Agent**: Selecting an SSO agent from the drop-down list will allow FortiNAC to send user ID and IP address information to specific devices types, such as FortiGate, Palo Alto, and iBoss.
- **Advanced**: Selection provides access to advanced management options, such as managing as a generic SNMP device or device type override.
- **Group Membership**: This button displays all groups the device is currently a member of and allows for group management.

The **System** tab displays the sysName, sysContact, and sysLocation information retrieved from the device. The information is updated automatically.

The **Polling** tab displays supported polling types and their current settings. **Poll Now** buttons for each type allow for manual polling.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



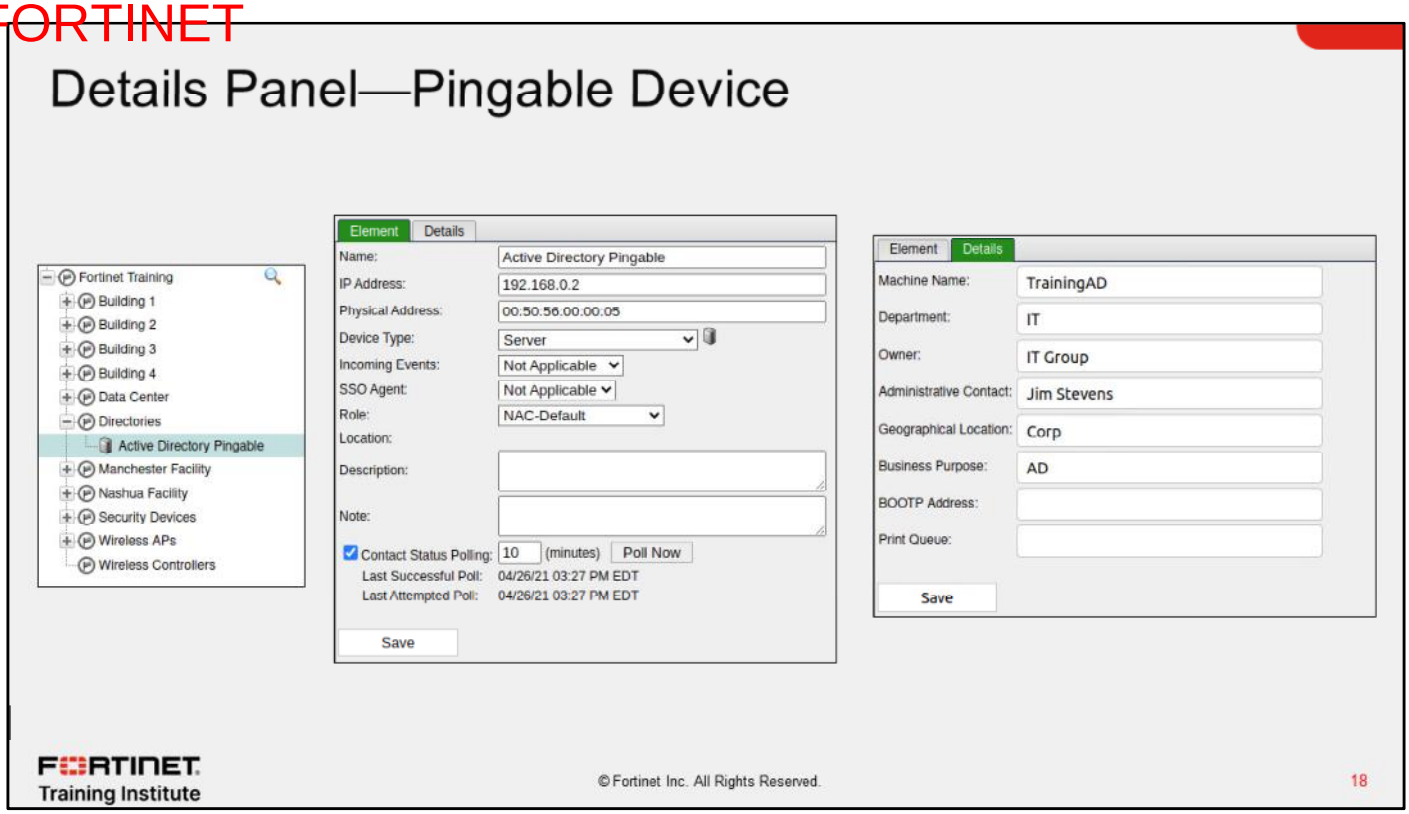
The **Credentials** tab shows and allows you to modify the SNMP and CLI credentials that FortiNAC uses for communication with the selected device.

The **Virtualized Devices** tab appears when the selected device is a FortiGate with VDOMs configured. Each configured VDOM appears in the **Virtualized Devices** list and has its own **Model Configuration** screen. Other devices each have a **Model Configuration** tab with the model settings. Model configuration settings are covered in another lesson.

You can also configure the settings on each tab from the Properties view. Right-click a device name to access the **Properties** view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



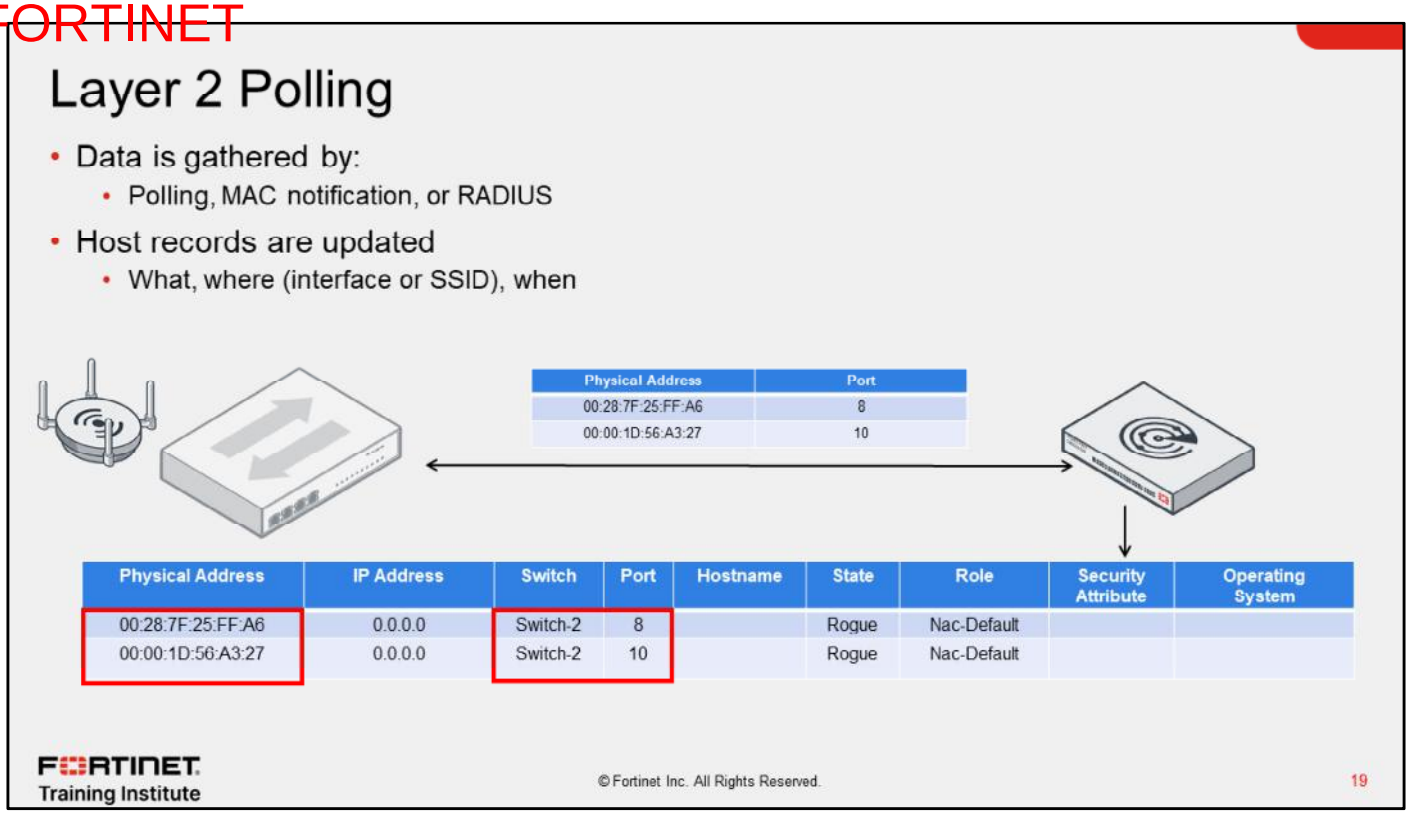
When you select a device that is modeled as a pingable device, two tabs for the device are displayed.

The **Element** tab displays detailed properties of the selected device, such as the name, IP address, physical address, and device type. It also provides some configuration options for the processing of incoming events or integration with an SSO agent. You can assign a role value to the device from a drop-down list. The location of the device is displayed (if it is known), and you can modify the description and note fields with additional details. Contact status allows you to enable or disable the polling, set the interval for polls, and displays the last successful poll as well as the last attempted poll.

The **Details** tab provides a location for you to add important device-specific information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Because each physical address is unique, FortiNAC can identify hosts as they connect to the network. FortiNAC uses the information that it gathers when it identifies a host to fill in the physical address and location information in the database.

The information is gathered through polling of the infrastructure device acting as the point of connection for the endpoint, or through the receipt of a MAC notification trap or RADIUS request sent to FortiNAC from the device that an endpoint has connected to.

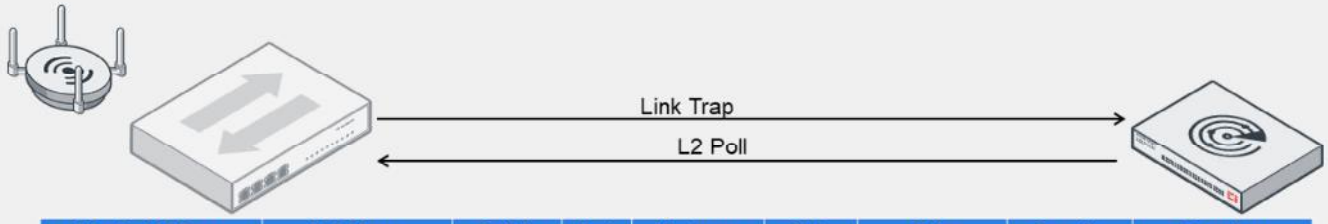
The physical address that was learned, the time it was learned, and where it was learned from, provide the beginnings of endpoint visibility in the form of what, where, and when information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Layer 2 Data Collection

- Layer 2 data polling can be triggered by:
  - Manual polling
  - Scheduled tasks
  - Link traps
- Layer 2 data can be received by MAC notification traps



Physical Address	IP Address	Switch	Port	Hostname	State	Role	Security Attribute	Operating System
00:28:7F:25:FF:A6	0.0.0.0	Switch-2	8		Rogue	Nac-Default		
00:00:1D:56:A3:27	0.0.0.0	Switch-2	10		Rogue	Nac-Default		

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

The three ways that Layer 2 polling is triggered are:

- Manual polling: Manual polling is initiated when an administrative user right-clicks the device in the topology tree and selects **Poll for L2 (Hosts) Info**, or clicks **Network** > **L2 Polling**.
- Scheduled: Layer 2 polling is scheduled in the **Network** > **L2 Polling** view. You can change the default scheduled intervals.
- Link Traps: Link traps received from an edge device trigger FortiNAC to perform a Layer 2 poll to update its awareness of devices that are connected on that edge device. The traps that trigger the poll are: Linkup, Linkdown, WarmStart, and ColdStart. This trigger keeps FortiNAC up-to-date in real time as devices connect to and disconnect from edge devices.

You can also collect Layer 2 data from MAC notification traps. When an edge device issues a MAC notification trap to FortiNAC, the notification contains the MAC address that was just learned or removed from the MAC address table of the edge device, as well as the port that MAC address was associated with. FortiNAC can then update its database with the new information.

MAC notification traps are the preferred method for learning and updating this Layer 2 information and you should always use them when they are an option. Receiving and processing MAC notification traps is much less resource intensive than having to contact and query an edge device.

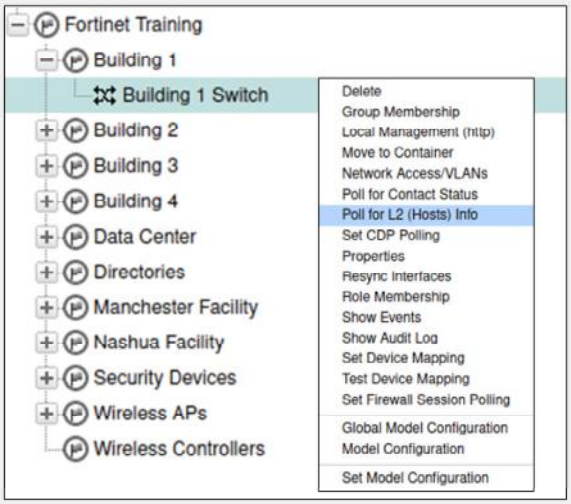
You should not configure link traps to be sent to FortiNAC on devices that have MAC notification traps configured. You should not configure MAC notification traps on interfaces that are uplinks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Manual Layer 2 Polling

- Topology tree Layer 2 polling
  - Right-click the device and select **Poll for L2 (Hosts) Info**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

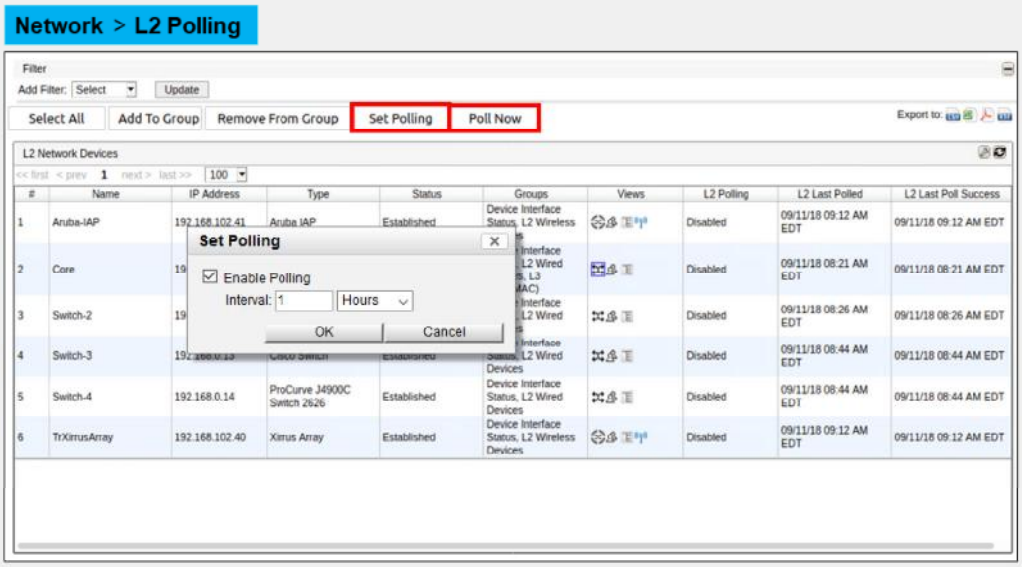
To manually initiate a Layer 2 poll on a single device, right-click the device in the topology tree and select **Poll for L2 (Hosts) Info**. FortiNAC will immediately perform a Layer 2 poll and update the host's entries in the database.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configure Layer 2 Polling

- Use **Poll Now** or **Set Polling**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

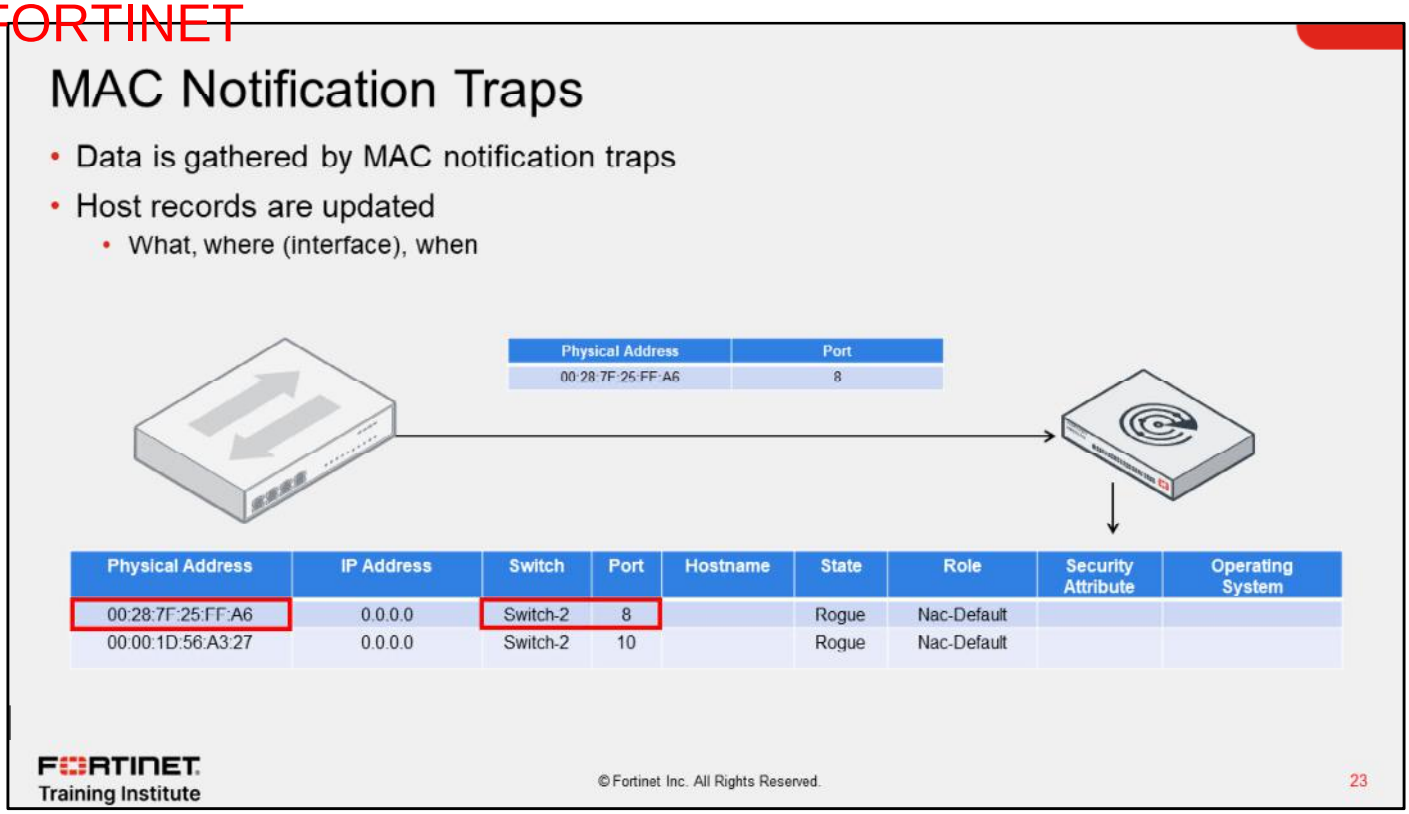
22

To schedule FortiNAC to perform Layer 2 polls or manually perform a Layer 2 poll on one or more devices, use the **L2 Polling** view. This view contains a list of all Layer 2-capable devices that have been modeled in the topology tree. These devices are displayed here because they exist in the **L2 Network Devices** system group.

You can manage these Layer 2-capable devices using the buttons at the top of the screen. The **Add To Group** and **Remove From Group** buttons allow for group management of all selected devices. Use **Set Polling** to enable and schedule automatic polling intervals for selected devices, and **Poll Now** to trigger an immediate poll of all selected devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



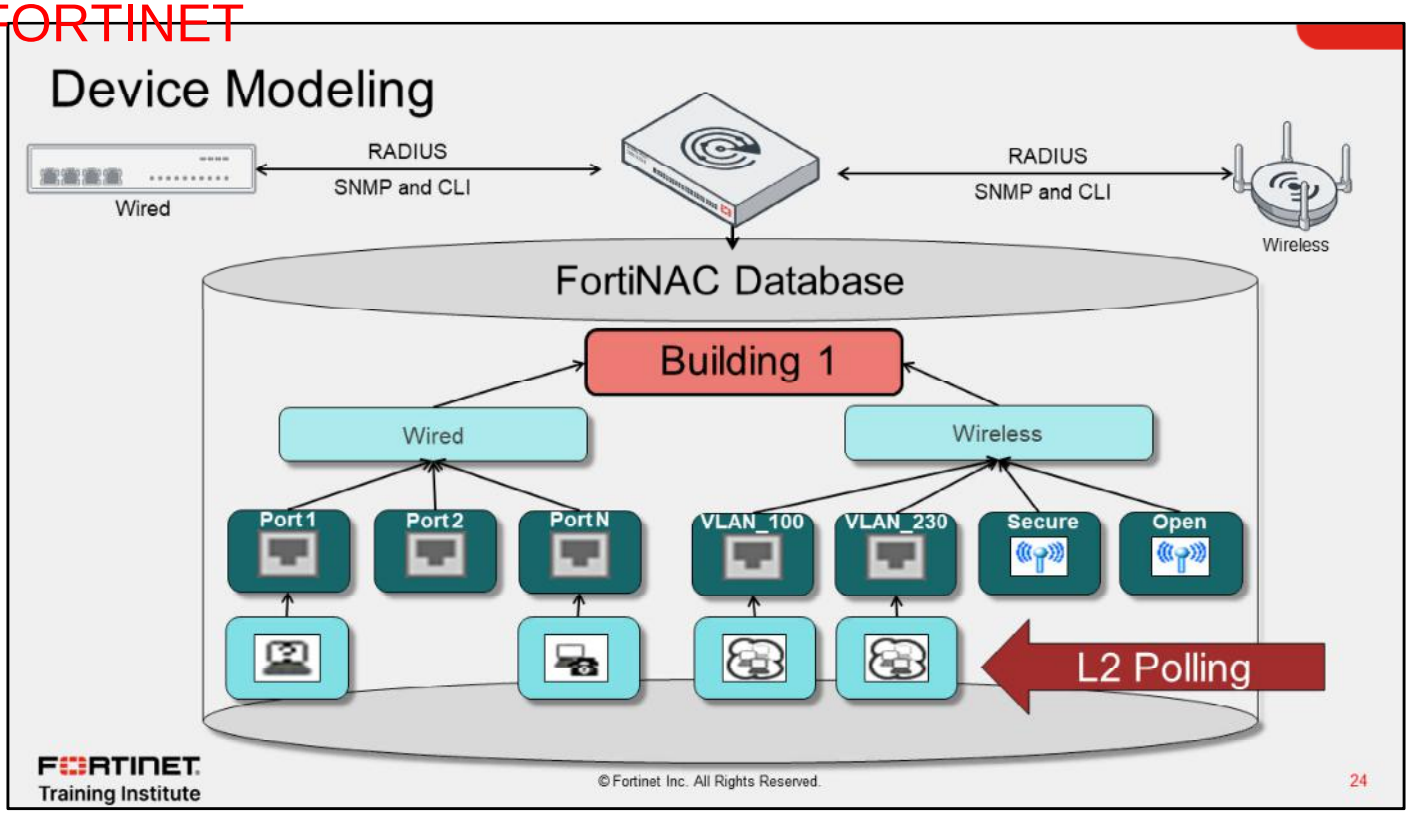
MAC notification traps offer, with specific vendors, an alternative and preferred method of Layer 2 data gathering. A MAC notification trap is generated by the infrastructure device when a new MAC address is learned or removed from its MAC address table.

There are a couple of reasons why MAC notification traps are preferred over link up and link down traps and why you should always use them whenever possible:

- First, FortiNAC no longer needs to establish a connection to the infrastructure device each time a link up or link down trap is received because the required information is included in the MAC notification trap. This makes database updates faster and demands fewer resources.
- Second, hosts and devices that connect through hubs or IP phones will be seen immediately, even if the device they connected to can’t generate link up or link down traps.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

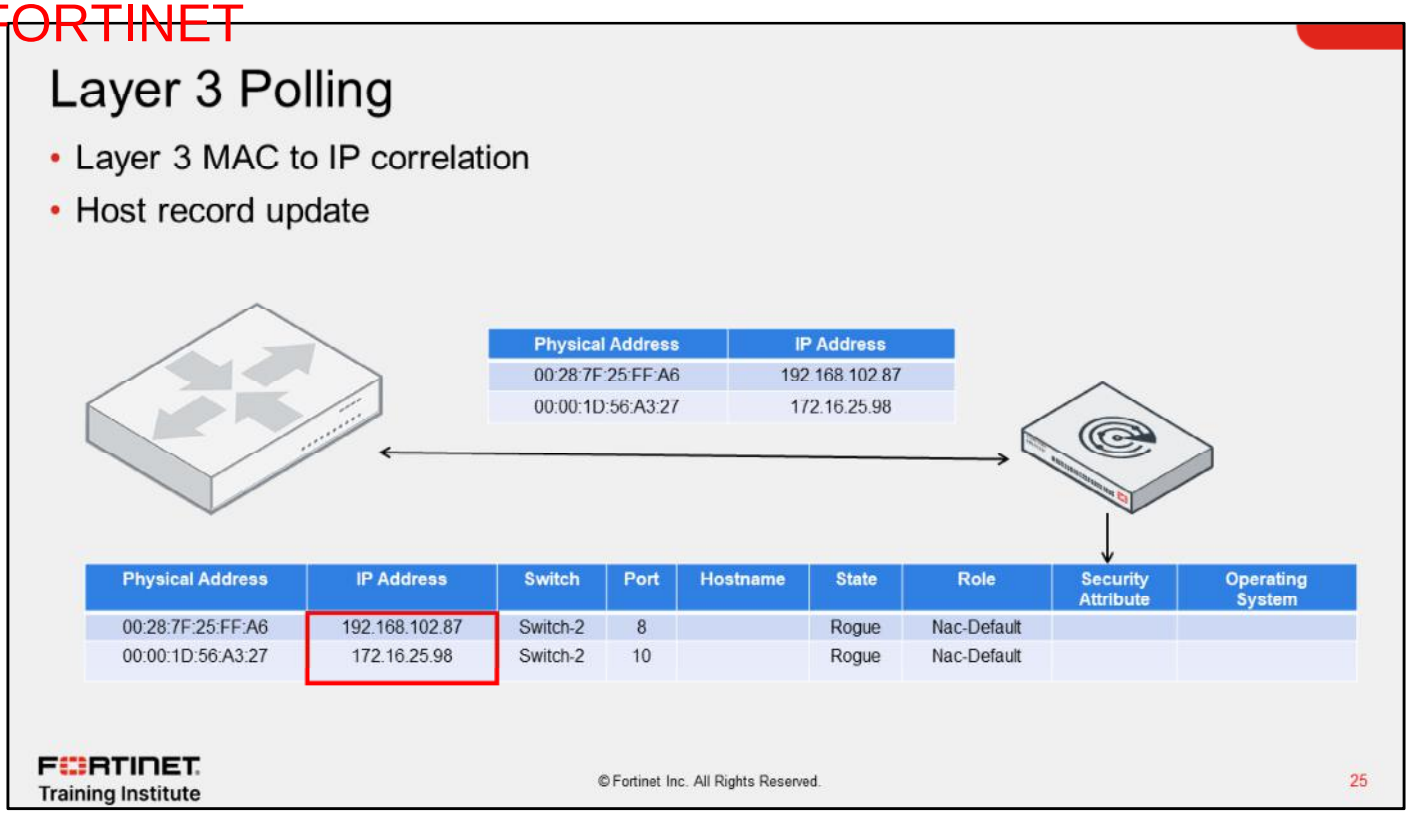


Regardless of the method used, once Layer 2 information is gathered or received, FortiNAC can update the device locations by point of connection. There are any number of different icons that can be used to display what is connected. Some of the common default icons are shown on this slide. On the far left, you can see an icon representing an unknown device connected to port 1. On port N, you see an icon representing a single host in addition to a connected IP phone.

The two wireless ports representing VLAN_100 and VLAN_230 are showing a cloud icon, which is used by FotiNAC to indicate that more than a single host connected. When represented in the inventory view, you can click these clouds to see each element that makes up the cloud.

Vouchers & Dumps are Available | WhatsApp +201224560923

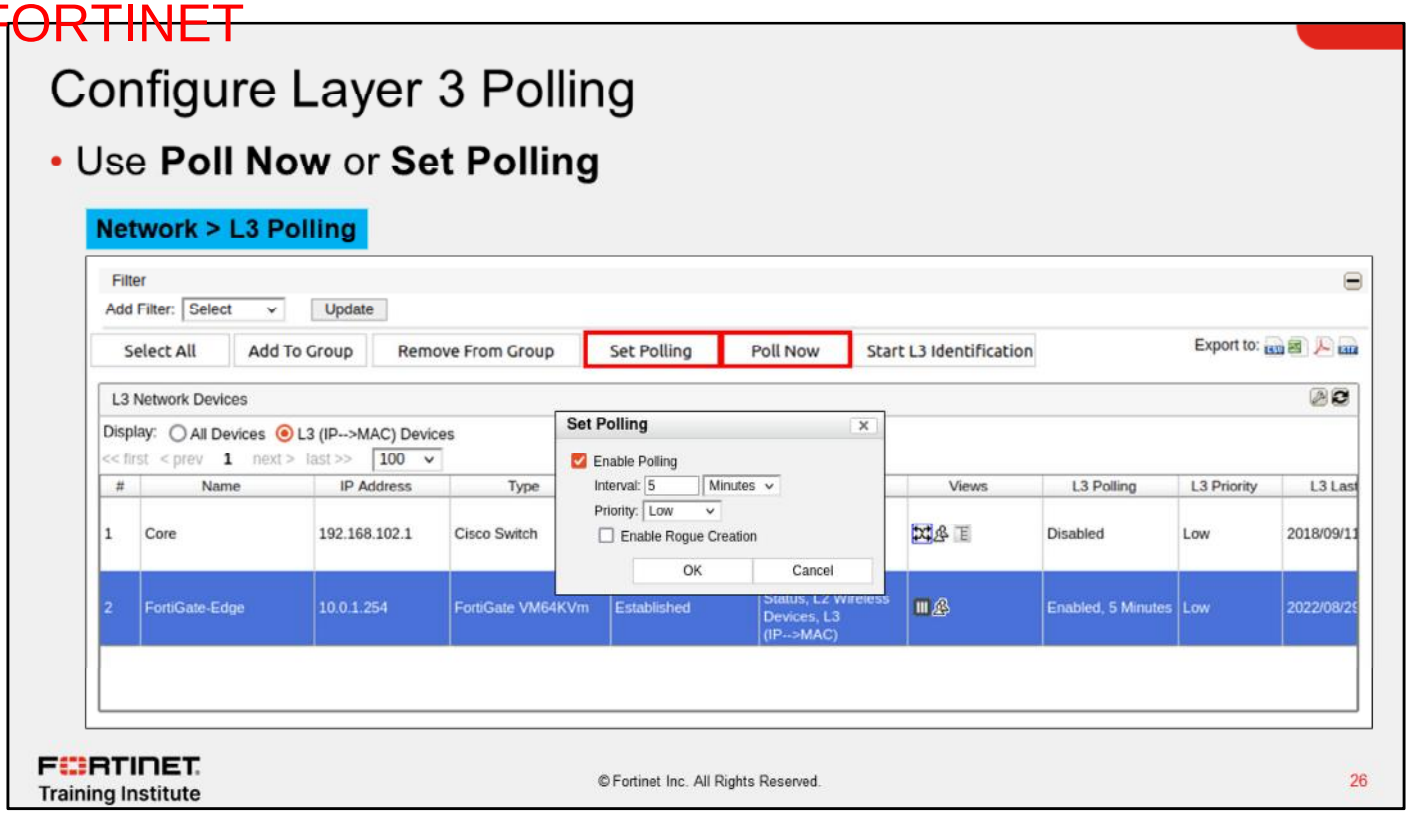
DO NOT REPRINT Brave-dumps.com
© FORTINET



L3 IP address information is a critical piece of network visibility and is a necessary component for some FortiNAC capabilities. As devices are added or discovered, they are automatically added to the **L2 Wired Devices** or **L2 Wireless Devices** groups. These groups are nested as subgroups of the **L2 Network Devices** group. A default **L3 (IP --> MAC)** group is created by FortiNAC, but may not be automatically populated, so you may need to add your Layer 3 devices to this group. The polling of devices in the Layer 3 device group is performed on a scheduled basis, and the correlated IP address is added to the database record for the corresponding MAC address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



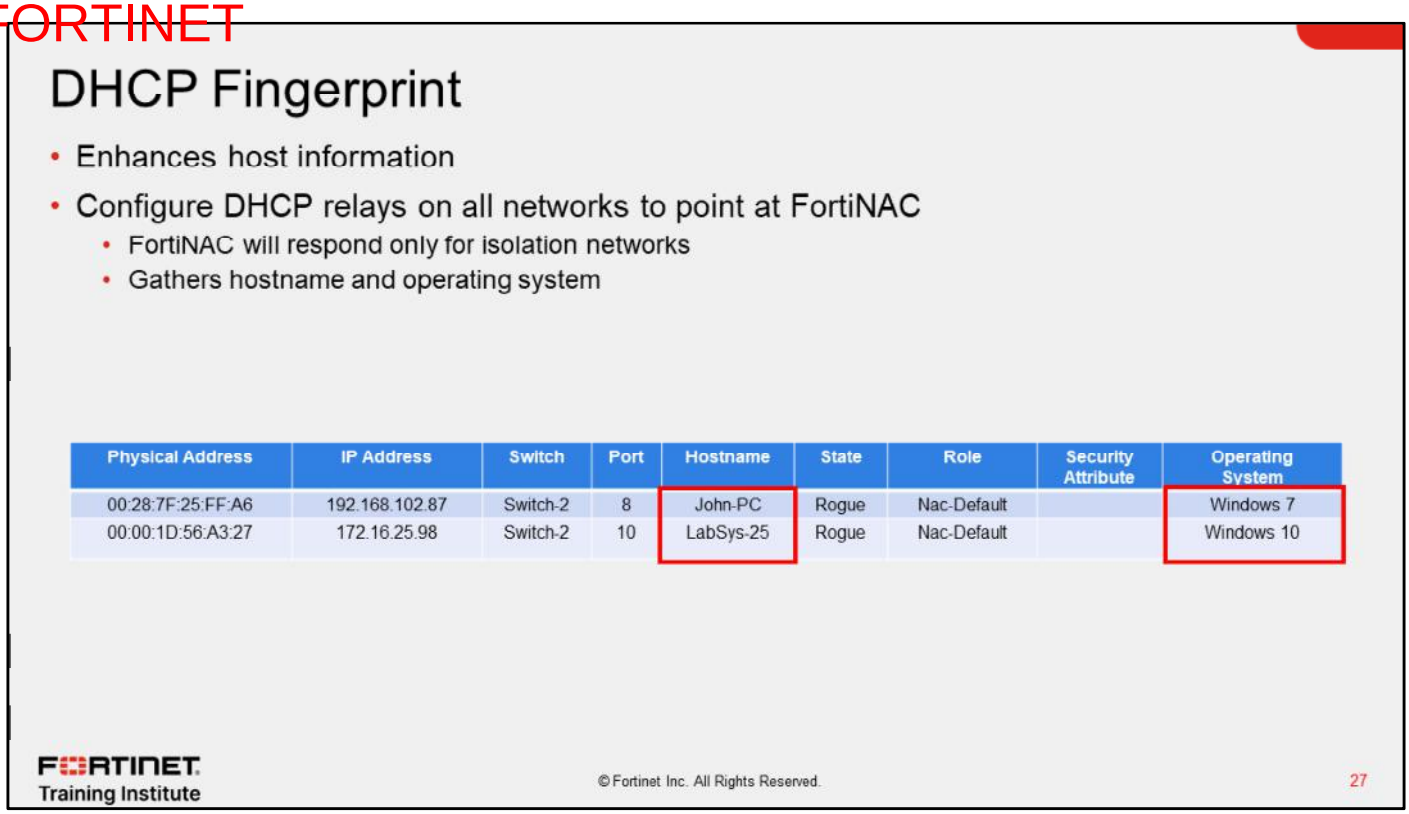
To schedule FortiNAC to perform L3 polls, click **Network** > **L3 Polling**. This where you can manually perform or schedule the poll.

Only devices that are members of the **L3 (IP→MAC)** system group appear in this window. Buttons along the top of the window allow you to add devices to that group from this view.

Use **Set Polling** to enable and schedule automatic polling intervals for selected devices and **Poll Now** to trigger an immediate poll of all selected devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



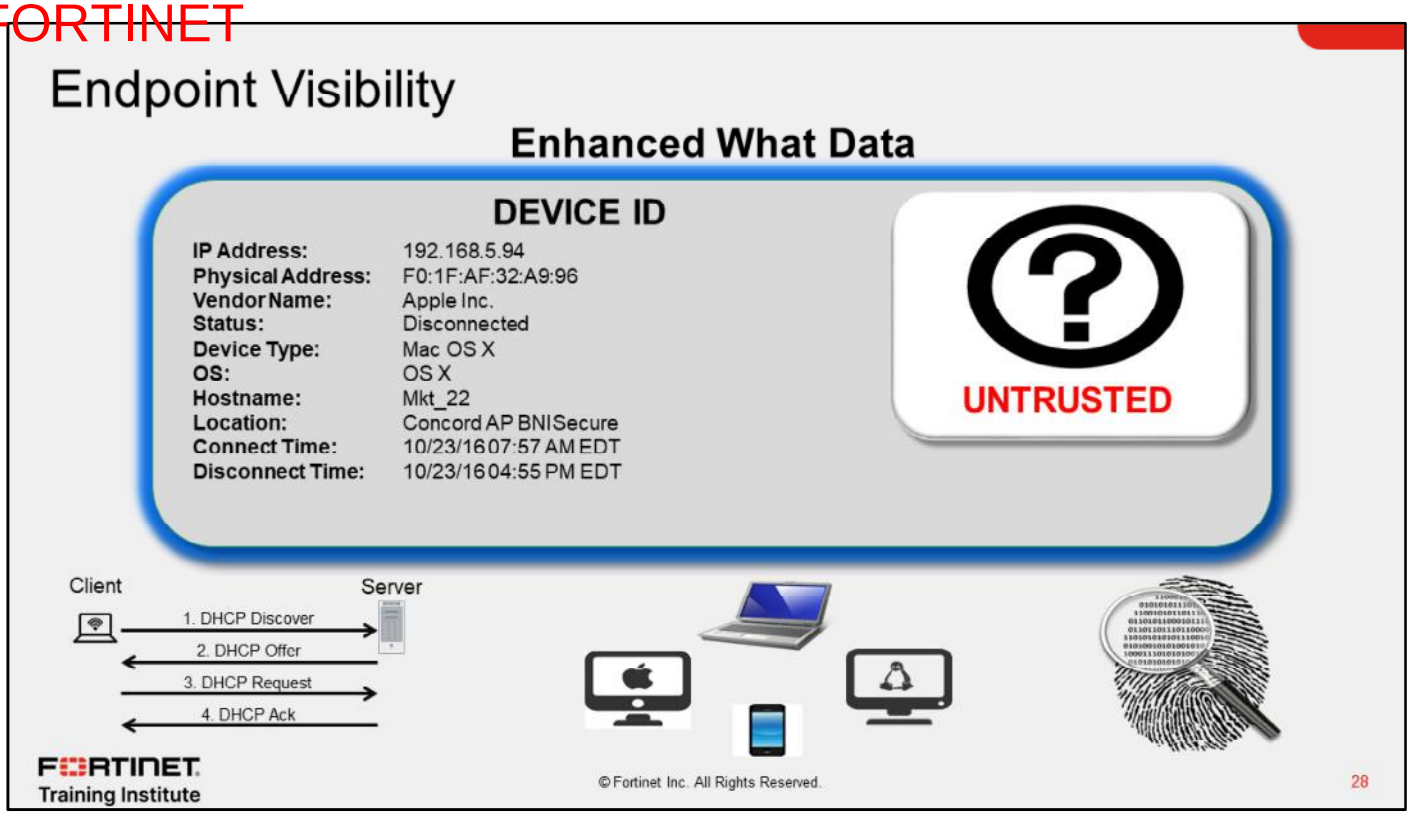
Configuring FortiNAC as an additional DHCP server using DHCP relays throughout an environment will result in FortiNAC receiving copies of DHCP discovery and request packets. FortiNAC will never respond to the packets forwarded to it from production networks because it should never have DHCP scopes configured on it for those networks. Once received, FortiNAC can parse the contents of each DHCP discovery or request and identify, based on parameters in the packet, the originating host's hostname and operating system. This information will be used to update and enhance the visibility information stored in the database.

This added visibility can also be used to generate notifications when hostnames or host operating systems change.

In deployments that use control and application servers, these DHCP relays should be targeted to **Eth1** on the application server. For single appliances or VMs, the relays should target **Eth1**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Endpoint visibility is the information gathered about endpoints connected or previously connected to the network. Endpoint visibility information usually includes all or some of following information:

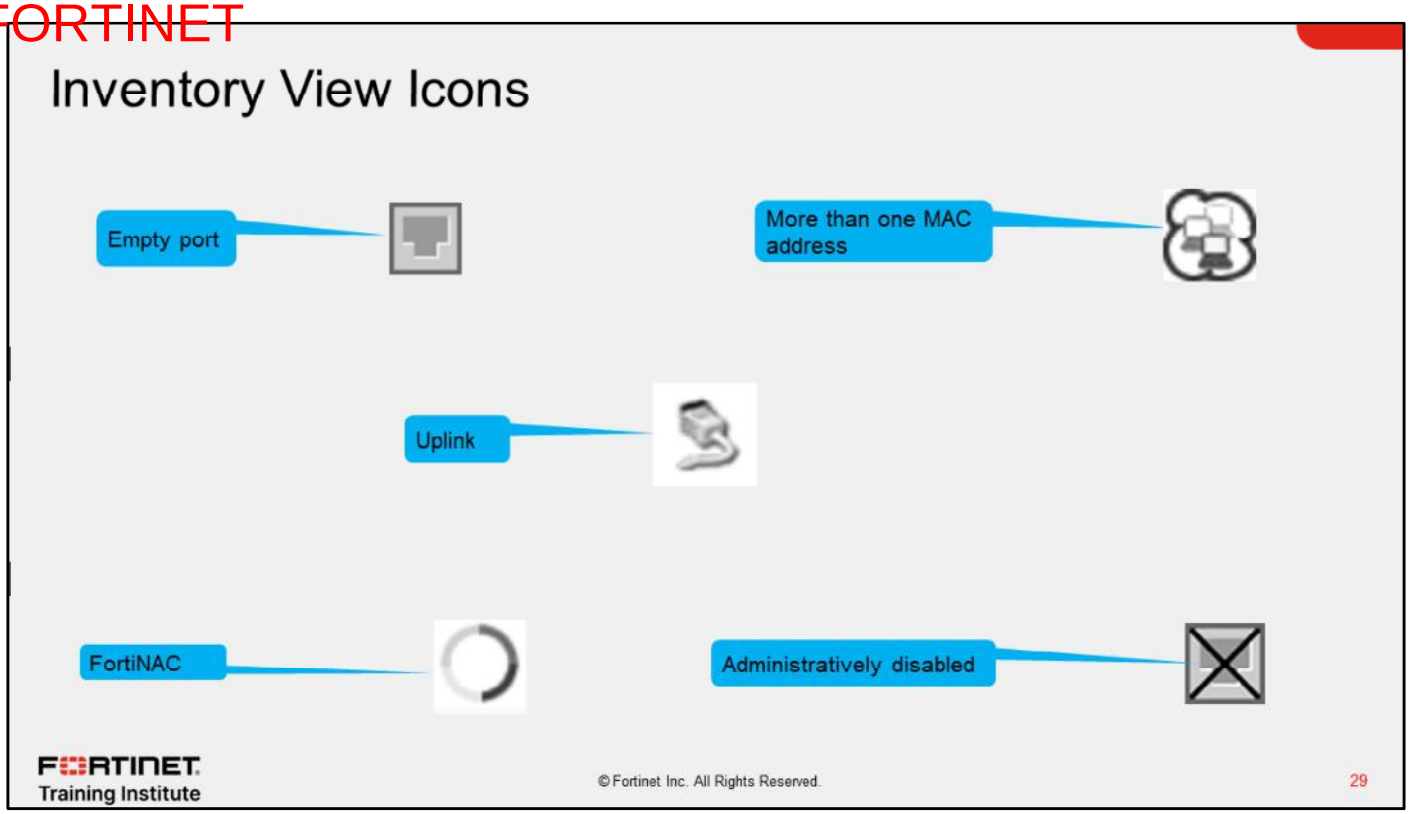
- The MAC or physical address, which is gathered using Layer 2 polling or MAC notification traps.
- The network or IP address, which is gathered using Layer 3 polling.
- Its current or last location on the network, which is known through Layer 2 polling.
- Connection status (connected or disconnected) and the connect and disconnect times, which is based on Layer 2 polling.
- The vendor name, which is based on the vendor OUI of the MAC address. FortiNAC has a current list of vendor OUIs in the database.
- The hostname and operating system, which is gathered from DHCP fingerprinting.

Endpoint visibility and details do not define device trust. Trust is defined through the classification of each endpoint. You will learn more about methods and process for classification in another lesson.

Note that you can also gather most of this information using FortiNAC agent technology. You will explore agents in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows some common port icons that you will see in the inventory view. In the upper-left corner there is an RJ45 port icon. RJ45 ports are used to represent physical ports on wired devices. An empty port, like the one shown here, indicates that, based on Layer 2 poll results, no devices are physically connected. If the port icon is green, it indicates that, when the interfaces were originally read from the switch, the port was in an administrative link-up state. The same RJ45 port icons are used for wireless devices, but may represent different things, such as an access group or a VLAN.

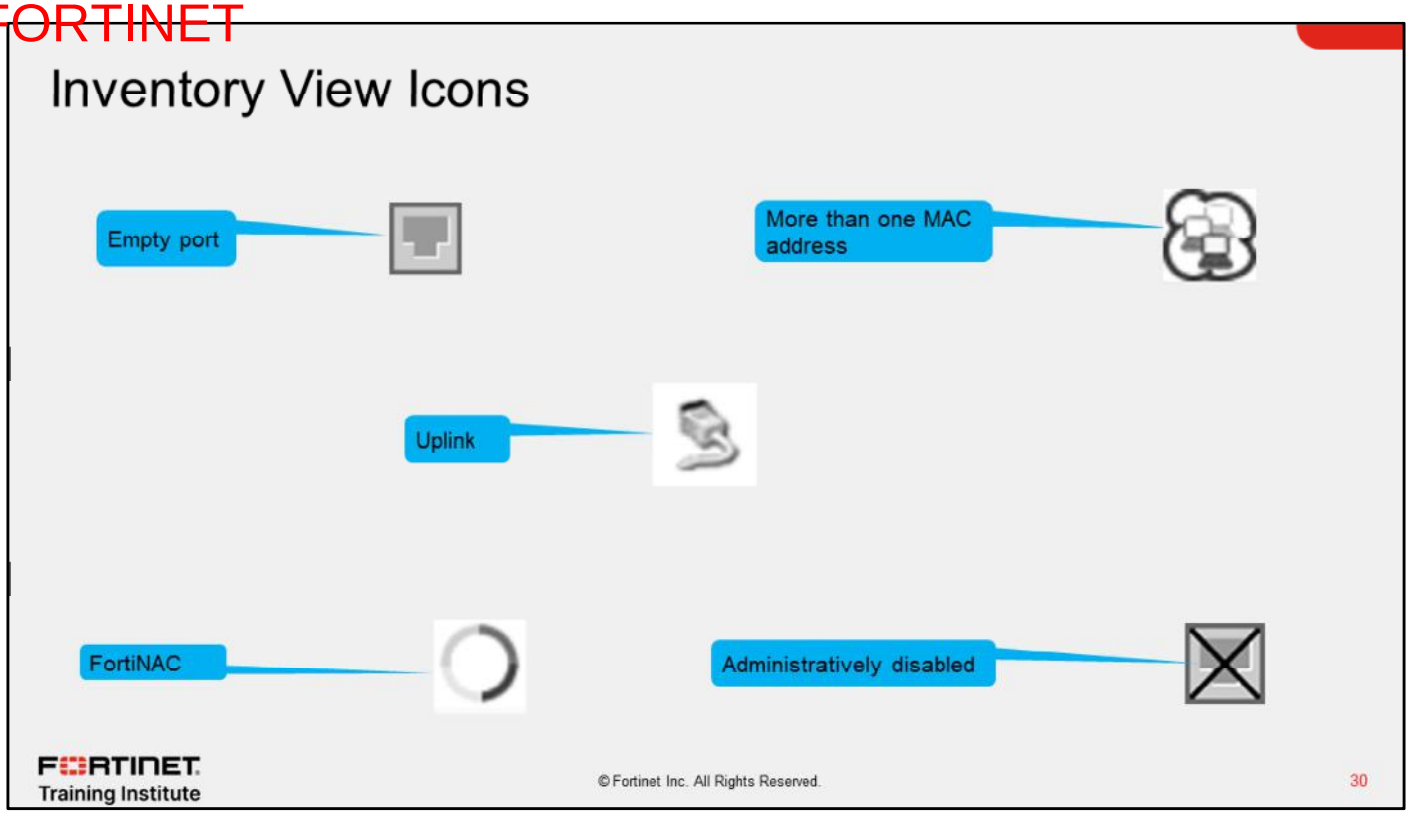
The icon on the lower-left identifies FortiNAC. FortiNAC will recognize its own physical address when it performs an L2 poll.

The icon on the upper-right indicates multiple devices on the same port. If a Layer 2 poll determines that more than one MAC address is concurrently connected to a single port in a wireless network, or more than one MAC address is connected as part of the same group or on the same VLAN, FortiNAC represents the multiple connected devices as a cloud. You can view all connected hosts individually using the **Adapters** tab. If one of the connected devices has been classified as an IP phone, a small IP phone icon will be shown in the cloud icon.

Administratively disabled RJ45 ports are represented by the port icon with an X through it, as shown on the lower-right corner.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



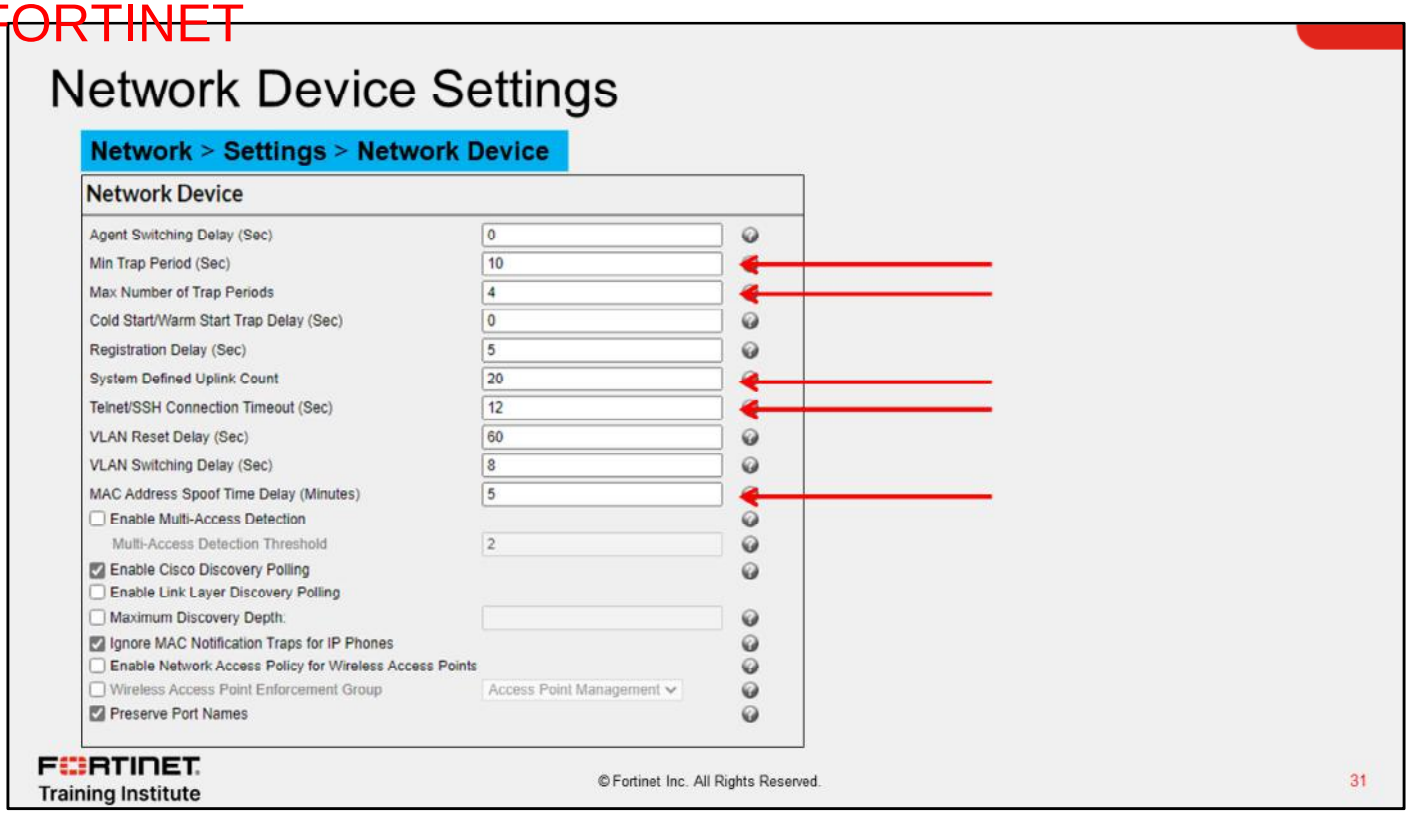
The icon shown in the center of the slide is called an uplink. Uplink ports are represented by a small RJ45 cable. Uplink ports change the way FortiNAC gathers information from the port and how it controls the port. During L2 polling, all physical addresses learned on an uplink port will be ignored because they aren't actually connected on that port. FortiNAC will not perform any control operations (changing VLANs, changing port state, and so on) on a port that is designated as an uplink.

There are three ways a port can be designated an uplink:

- A physical address that is owned by a port on another infrastructure device is shown as being learned on the port being polled.
- More than 20 (default setting) physical addresses are seen as being concurrently connected to a port.
- An administrative user manually designates a port as an uplink.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Network Devices** settings allow you to configure global properties that are specific to network devices and VLANs. Only some of the settings are covered on this slide.

Min Trap Period (Sec): This is the number of seconds FortiNAC waits after receiving a linkup trap before reading the forwarding table from the switch associated with the trap. The default is 10.

Max Number of Trap Periods: This is the maximum number of trap periods that the appliance waits before reading the switch forwarding tables.
If the switch does not have the MAC address information for the port that generated the linkup trap, the appliance places the switch back into the queue. Once **Min Trap Period** has expired, the forwarding table on the switch is read again. If another linkup trap is generated by the same switch, the trap period time is reset. The default is 4.
For example, if **Min Trap Period** is set to 20 seconds and **Max Number of Trap Periods** is set to 2, the longest the appliance will wait to read the switch forwarding tables is 40 seconds.

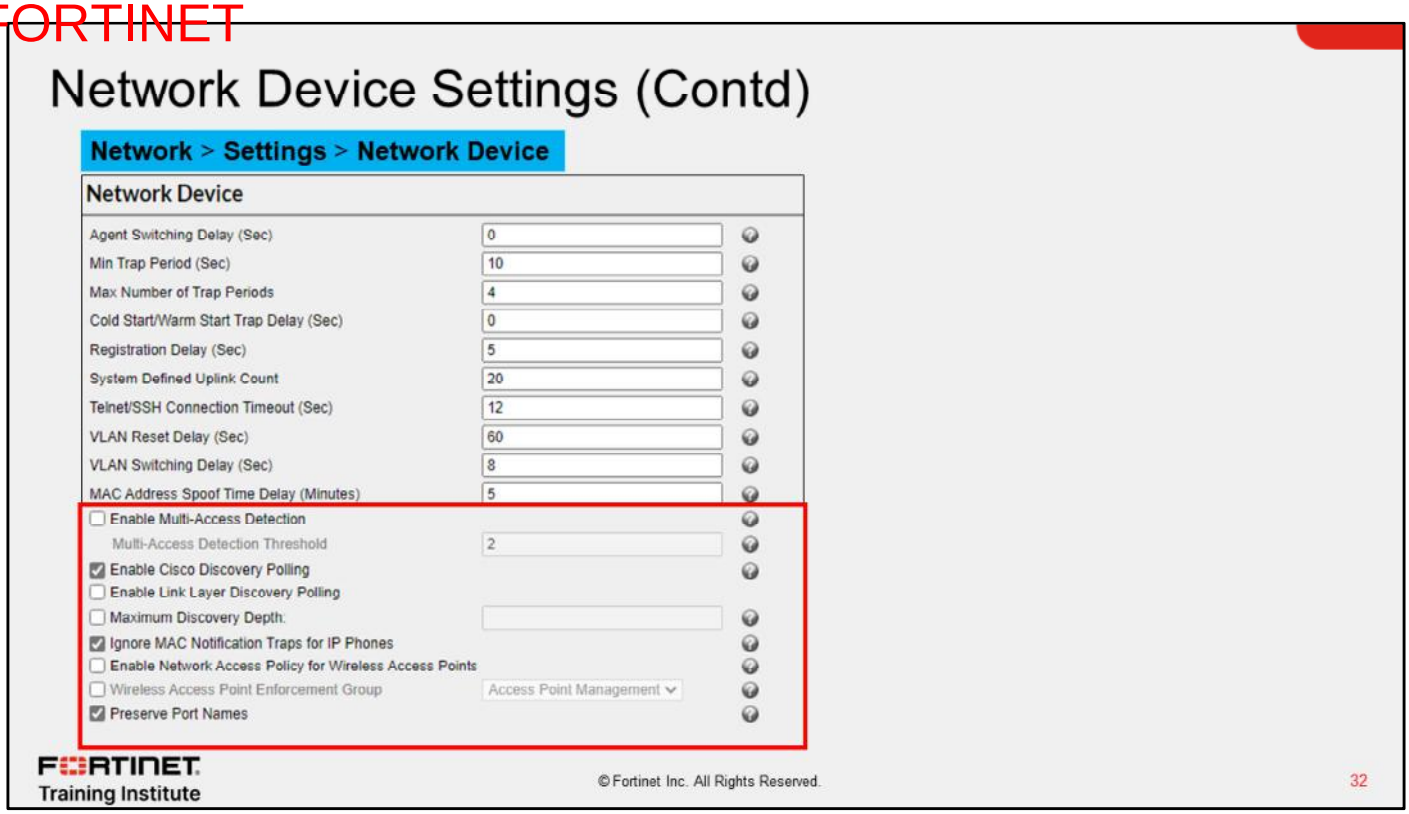
System Defined Uplink Count: When the number of MAC addresses on a port exceeds this value, the port is changed to an uplink. Setting this value to a higher number can help to indicate multi-access points. For example, setting this value to 7 changes the port to an uplink if a minihub with eight ports is connected on the port. The default is 20.

Telnet/SSH Connection Timeout (Sec): When you use telnet to contact devices, this setting determines how long the server waits for a response from the device before timing out. The default is 12 seconds.

MAC Address Spoof Time Delay (Minutes): This is the number of minutes after which, if the same MAC address has been detected on two devices/ports simultaneously, the possible MAC address spoof event is generated. The default is 5 minutes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Enable Multi-Access Detection: When this option is enabled, the appliance looks for multiple MAC addresses on ports each time a switch is read. This setting is disabled by default. To generate an event when multiple MAC addresses are detected on a port, you must also enable **Multi-Access Point Detected**; however, if the detected port is in the **Authorized Access Points** group, an event is not generated.

Enable Cisco Discovery Polling: When enabled, this option allows FortiNAC to query devices about other connected devices on the network using Cisco Discovery Polling (CDP). This setting is enabled by default. If this discovery protocol is enabled on a device, it gathers and stores information about devices it manages and devices it can contact on the network. Only devices with **Enable Cisco Discovery Polling** will respond to a CDP query. This is a global setting for the system. If this setting is enabled, devices can be set individually on the **Polling** tab of the **Device Properties** view. If this setting is disabled, the device setting is ignored and CDP is not used when polling a device. Devices that have the capacity for CDP must have the feature configured on the device firmware.

Maximum Cisco Discovery Depth: This setting limits the number of layers from the original device that will be queried using CDP.

Ignore MAC Notification Traps for IP Phones: When this setting is enabled, FortiNAC will not process MAC notification traps for IP phones. This setting is enabled by default.

Network access policies are applied to wireless access points using the Enable Network Access Policy for **Wireless Access Points** option.

Preserve Port Names will prevent port names or labels changed on a switch from being updated in the FortiNAC database.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which statement about uplink ports is true?
   - ✓ A. Learned endpoint MAC addresses are ignored.
   - B. The physical port is managed before non-uplink ports.

2. If a device can send both linkup/linkdown traps and MAC notification traps, which is the recommended choice?
   - A. Linkup/linkdown traps
   - ✓ B. MAC notification traps

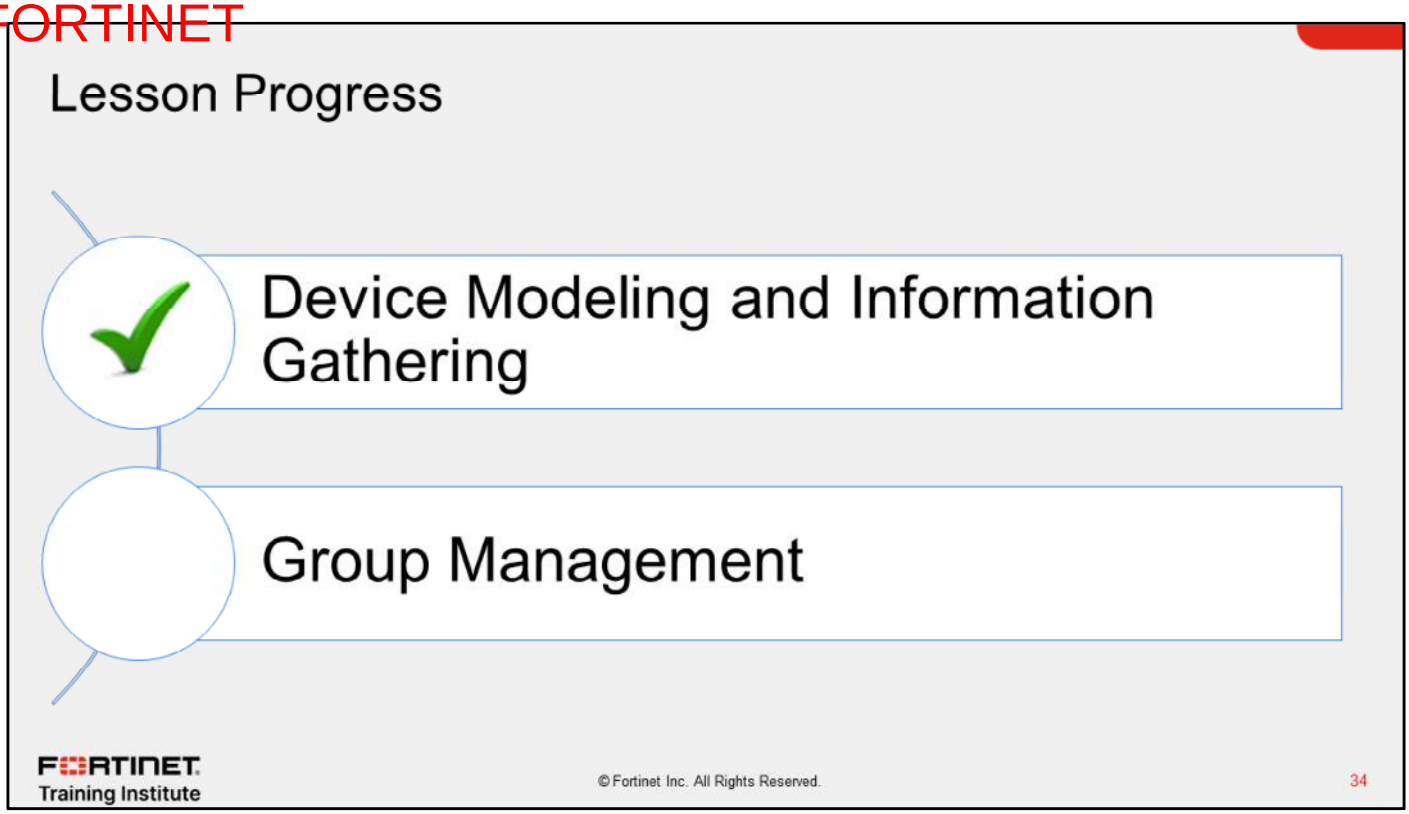
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

33

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

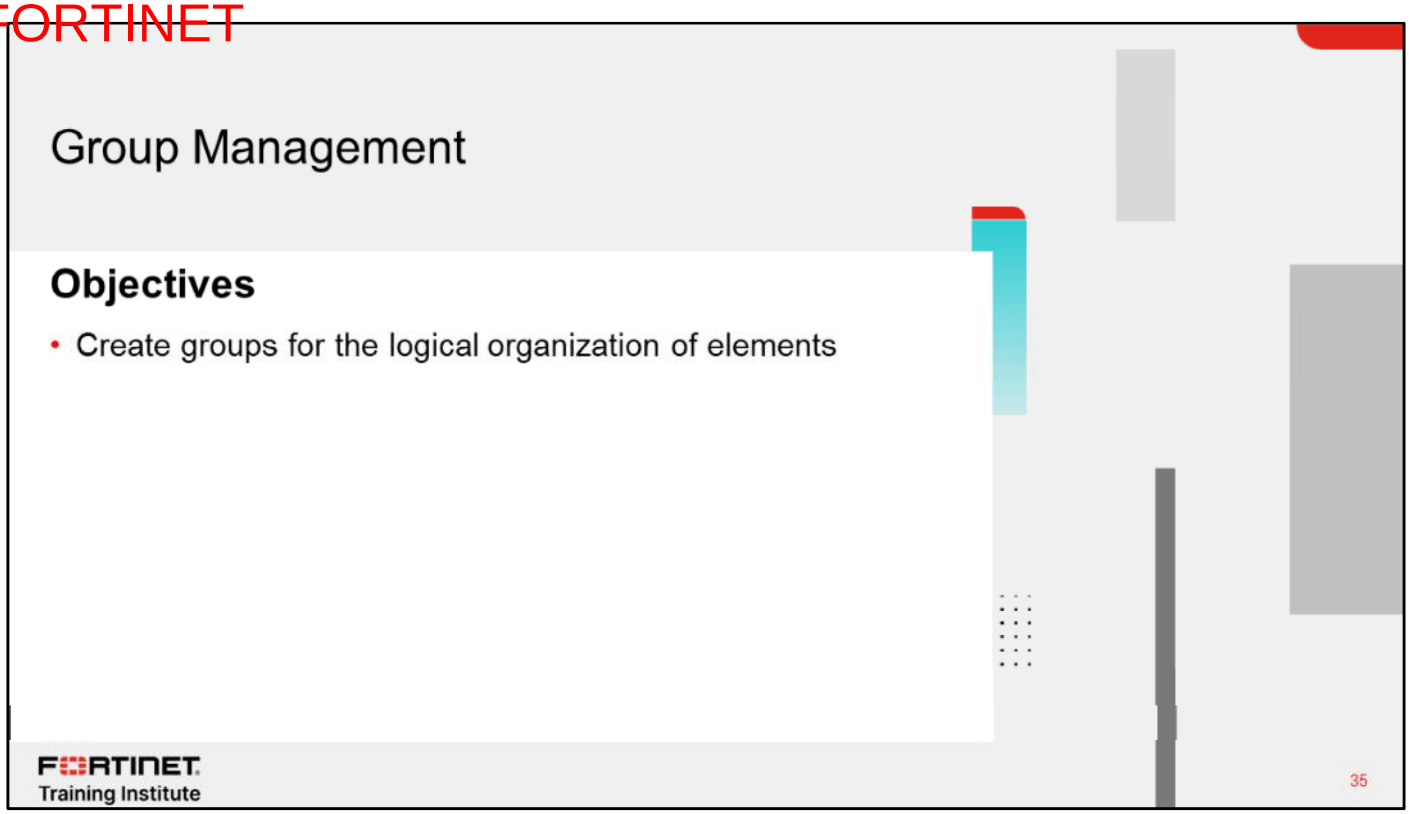


Good job! You now understand the modeling of network infrastructure devices.

Now, you will learn how to manage FortiNAC groups.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

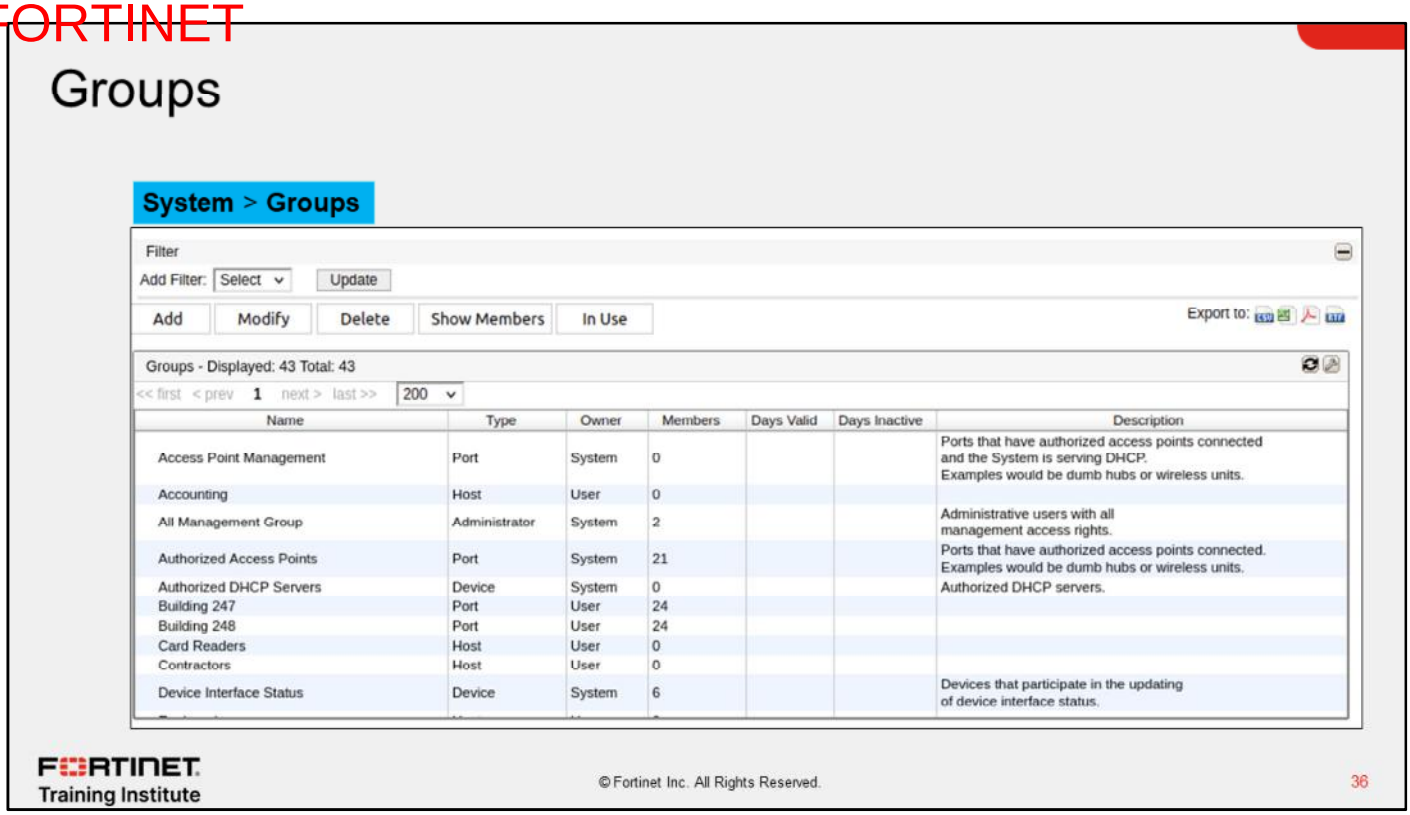


After completing this section you should be able to achieve the objective shown on this slide.

By demonstrating competence working with groups, you will be able to appropriately plan and use them to achieve your deployment and management goals.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Groups are collections of elements. Groups are a fundamental part of FortiNAC operations. There are six different types of groups and the groups type defines what can be a member of that group. The different group types are: administrator, device, host, IP phone, port, and user.

A set of preconfigured groups, called system groups, are identified by an owner type that is set to **System**. Most of these groups enforce some form of control or enable some functionality on all members.

Any groups created by administrative users, or imported as a result of an LDAP integration, will be assigned an owner of **User**. These groups are used to organize elements and do not enforce any type of control or functionality directly.

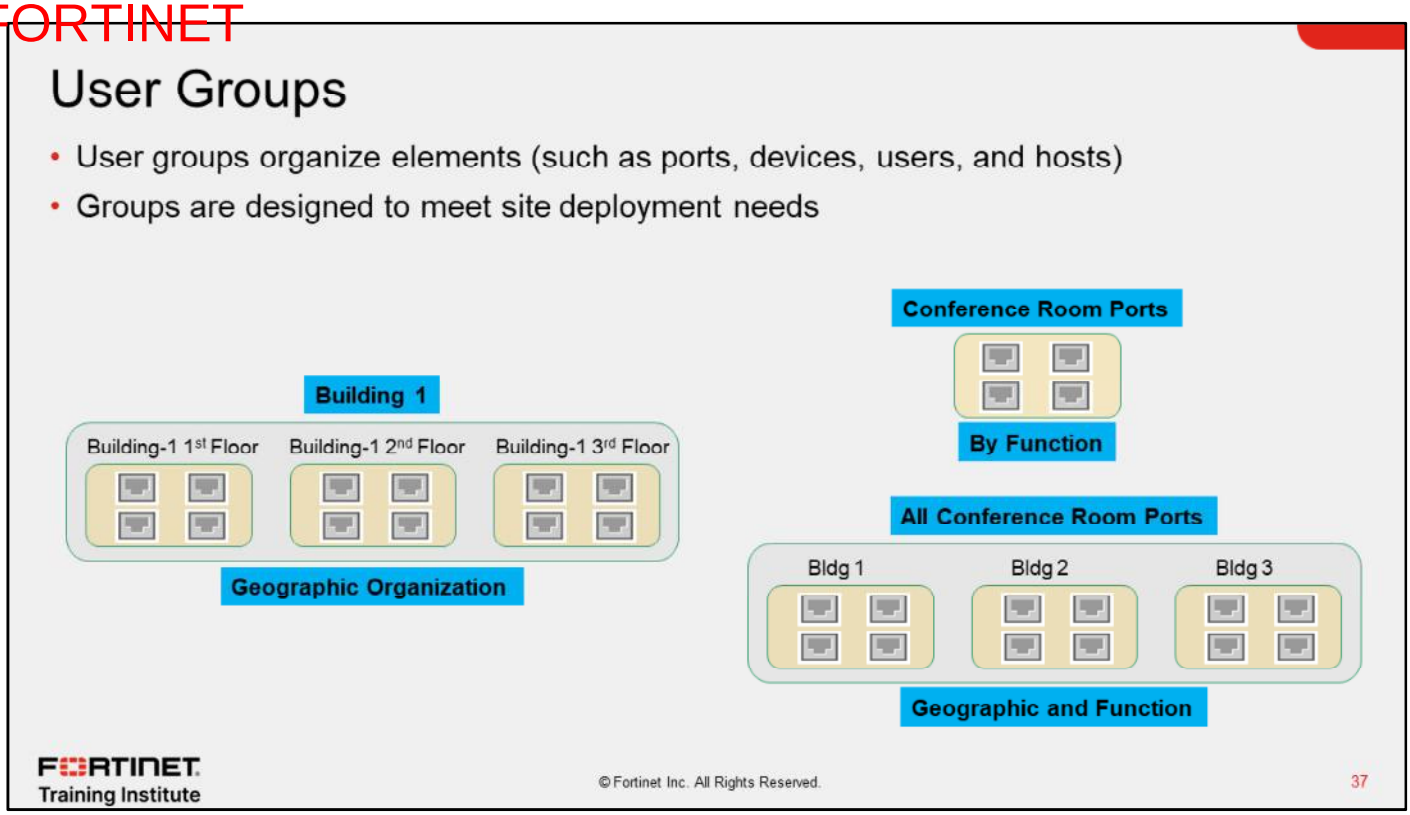
Groups of the same type can be nested within one another. As a best practice, administrative users create groups to identify elements in a way that allows them to nest those groups into appropriate systems groups, to satisfy enforcement needs.

There are more than 25 different system groups on FortiNAC, and several of the most commonly used groups are covered in another lesson. You can find a definition for each system group in help.

A small set of system groups are automatically populated. These groups are:
- Rogue hosts
- Registered hosts
- Layer 2 wired devices
- Layer 2 wireless devices

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The examples on this slide show some common methods for organizing ports. The first example is a simple geographical organization of ports through the use of four individual port groups. The first three groups have ports directly added to them as members and are named **Building-1 1st floor**, **Building-1 2nd floor**, and **Building-1 3rd floor**. These three port groups are added as subgroups to the fourth group called **Building 1**. This organization of ports provides the ability to enforce control on a floor-by-floor basis or by the building as a whole.

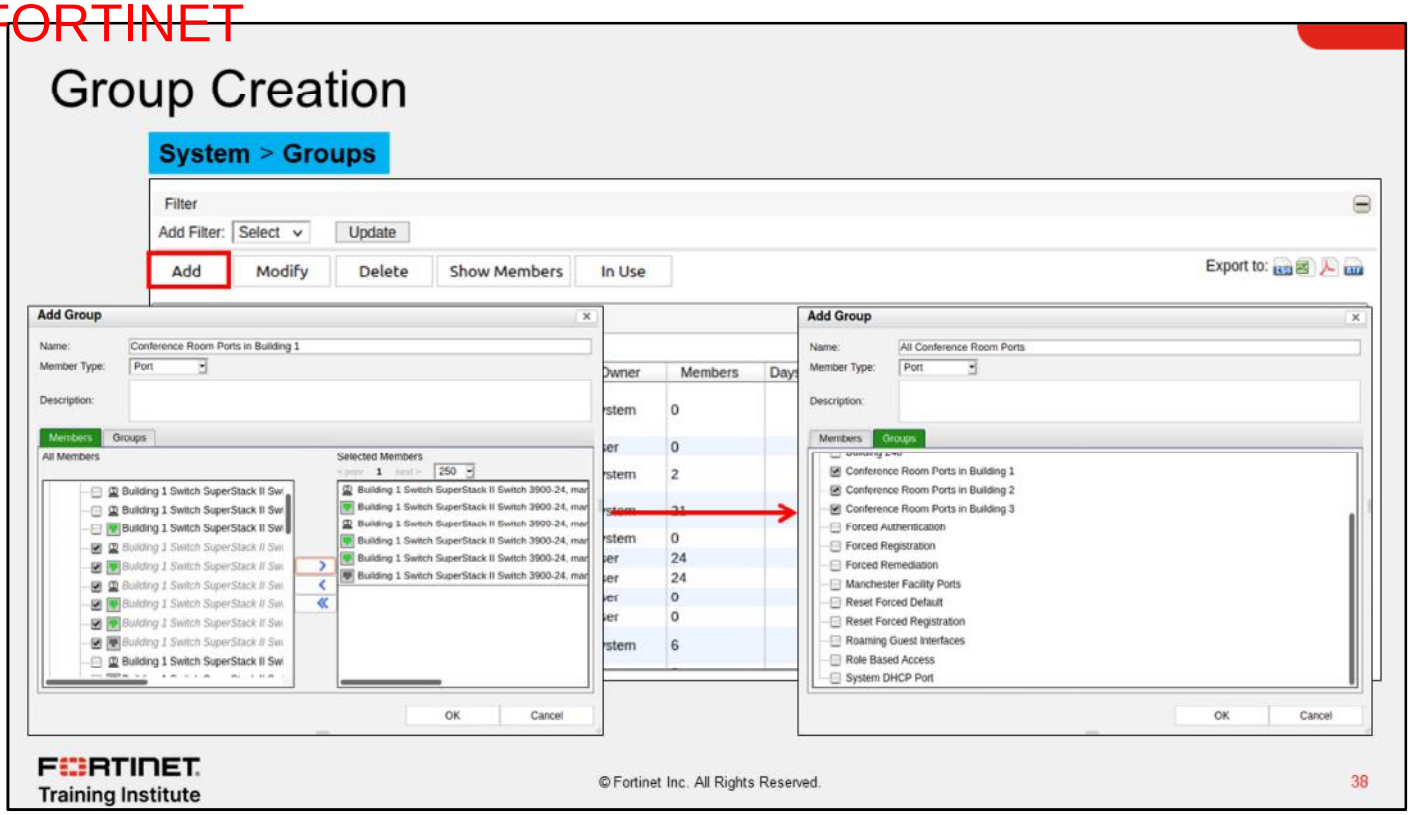
The second example shows a group of ports organized by function. The conference room ports contained within the group named Conference Room Ports may have no geographic similarities at all; however, they all serve the same function and can now be managed together.

The final example shows a combination of the previous two examples. In this example, the conference room ports are organized based on a geographic location, and the ports are named **Bldg 1**, **Bldg 2**, and **Bldg 3**. As a group based on function, the group is named **All Conference Room Ports**. These ports can now be managed by function, all conference room ports, or by function and location, building 1 conference room ports.

The FortiNAC method of management through groups allows for an extremely granular means of control, down to the exact point of connection in these examples.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To create a port group that is a combination of geographic location and function, click the **System** tab and select **Groups** to open the **Groups** administrative view.

Click **Add** to open the **Add Group** dialog box. Type a group name that indicates the group contents, such as `Conference room ports in building one`. In this example, you would set the **Member Type** to **Port**. Remember that the group type defines what can be a member of that group. The **Members** tab displays the topology tree from the inventory view, which highlights the importance of setting up the topology tree in a logical way that makes sense for your environment. In this example, the **Building 1** container has been expanded and a switch has been selected. Each port that is a conference room port in this building is selected. Use the arrow button to move ports from **All Members** to **Selected Members**. Click **OK** to make the ports members of the **Conference Room Ports in Building 1** group. Repeat this process two more times, for the second and third buildings. There will now be three individual port groups representing each of the three buildings.

You can create a fourth group, called **All Conference Room Ports**, and, in place of ports being added directly to the group, the previously created groups could be added from the **Groups** tab.

Groups are a critical part of any FortiNAC deployment and the ability to nest the groups provides both granularity of management, as well as the ability to scale to any size environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When you nest groups, what must be true about each group?
   - A. The two groups cannot have a common member.
   - ✓ B. The two groups must be of the same type.

2. Which type of group would you use to group SSIDs?
   - ✓ A. Port
   - B. Device

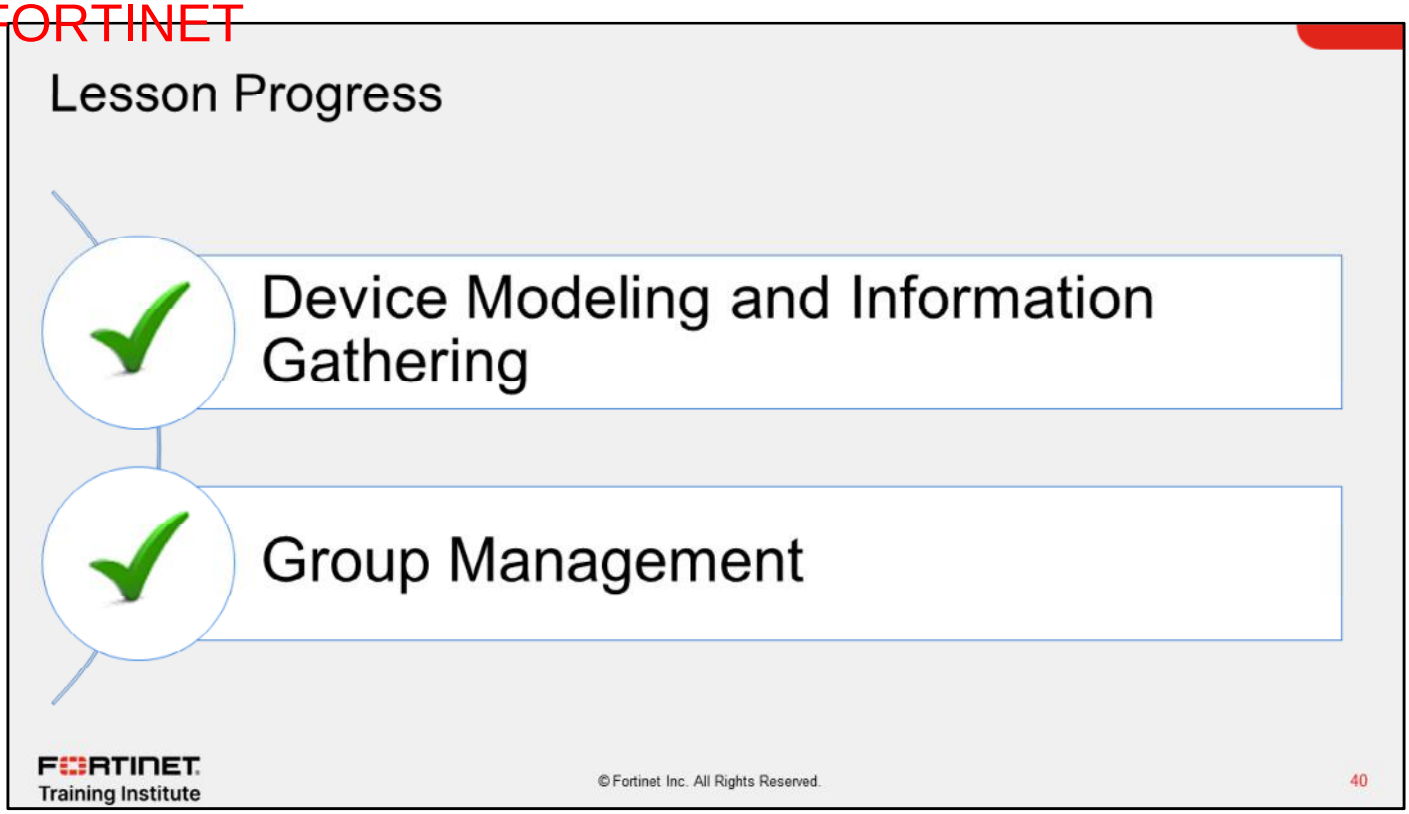
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

39

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

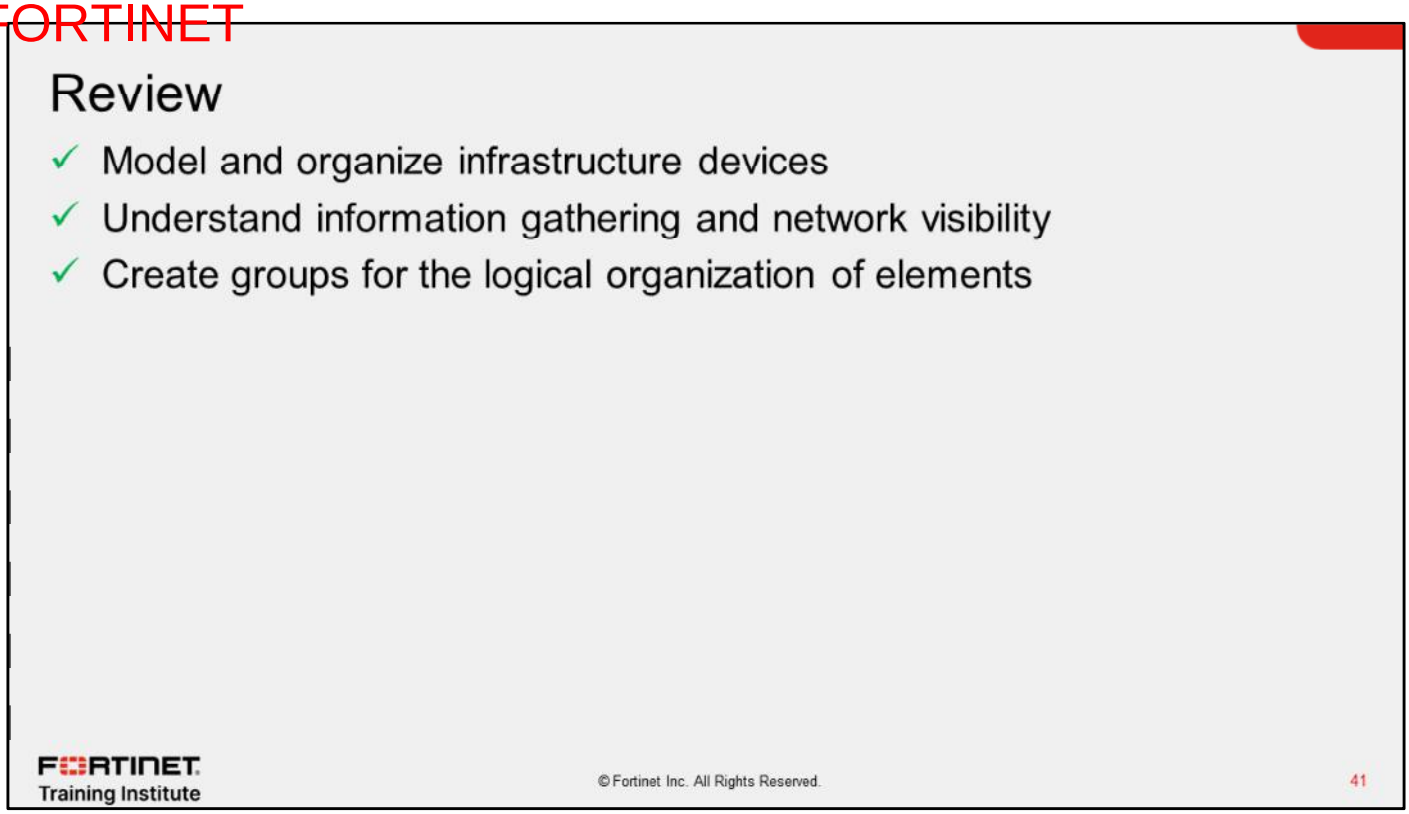


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

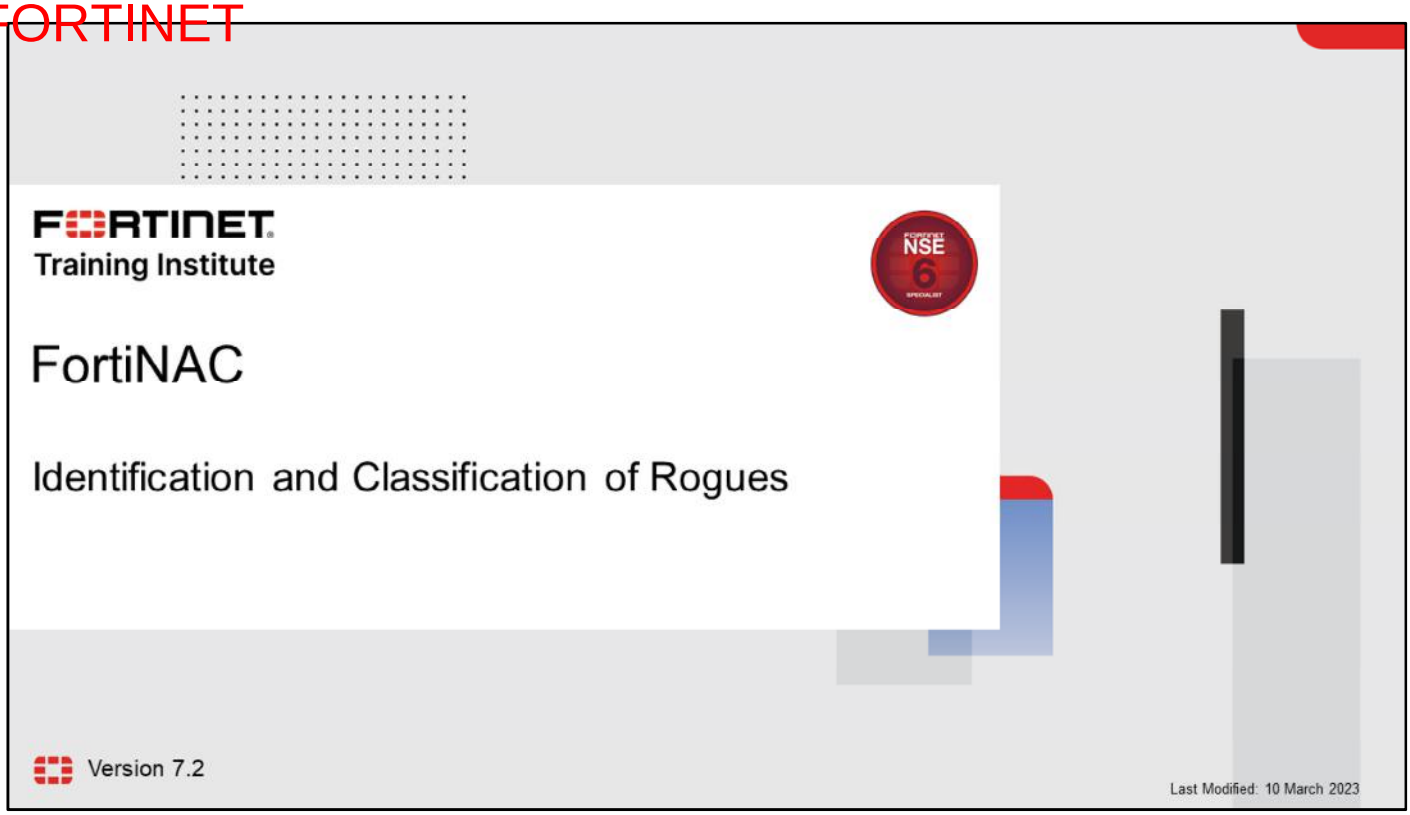


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to integrate FortiNAC with the network infrastructure, how information is gathered from the infrastructure, and how to create and manage groups.

Vouchers & Dumps are Available | WhatsApp +201224560923

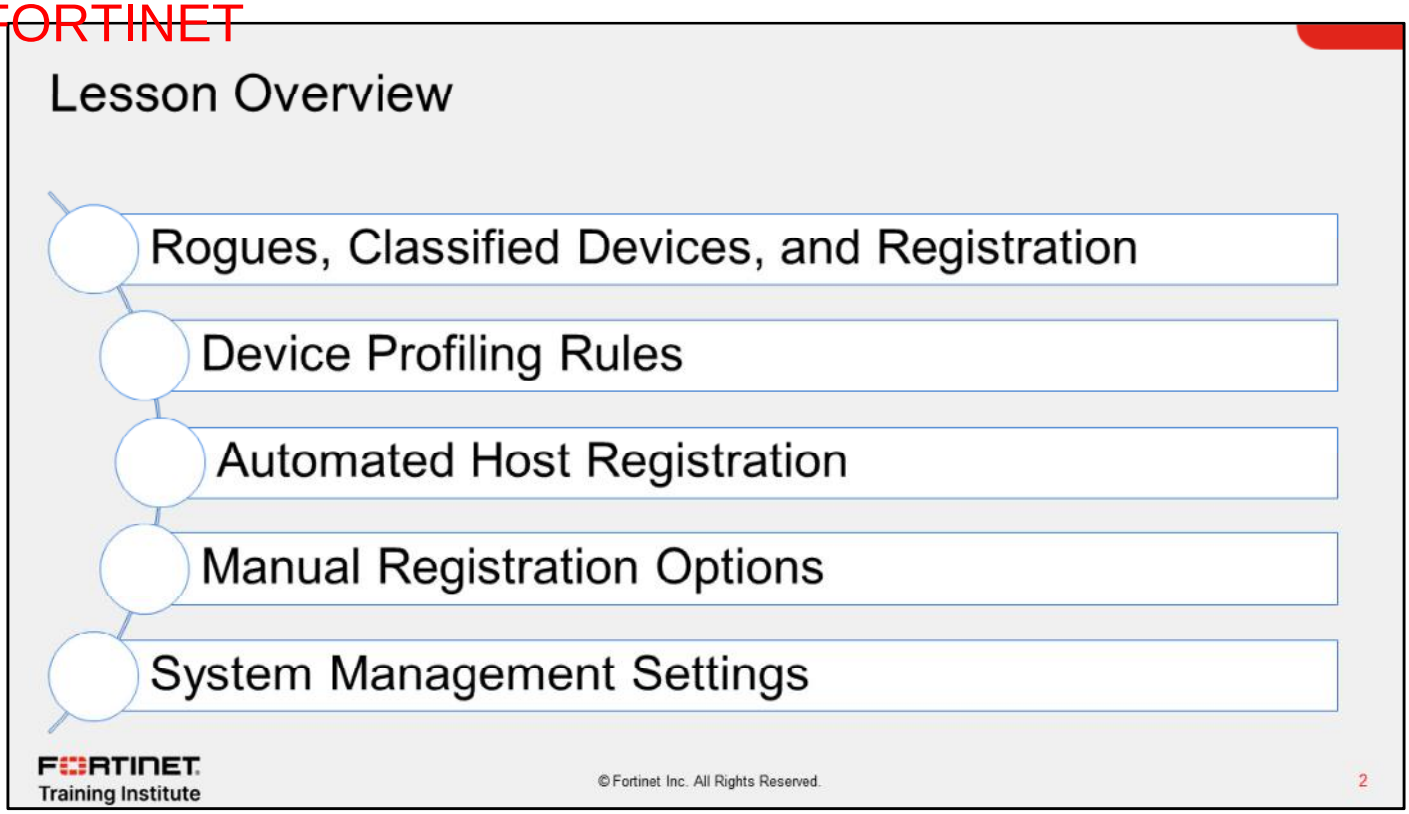
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the endpoint identification and classification process as well as the tools and methods used to expedite the process.

Vouchers & Dumps are Available | WhatsApp +201224560923

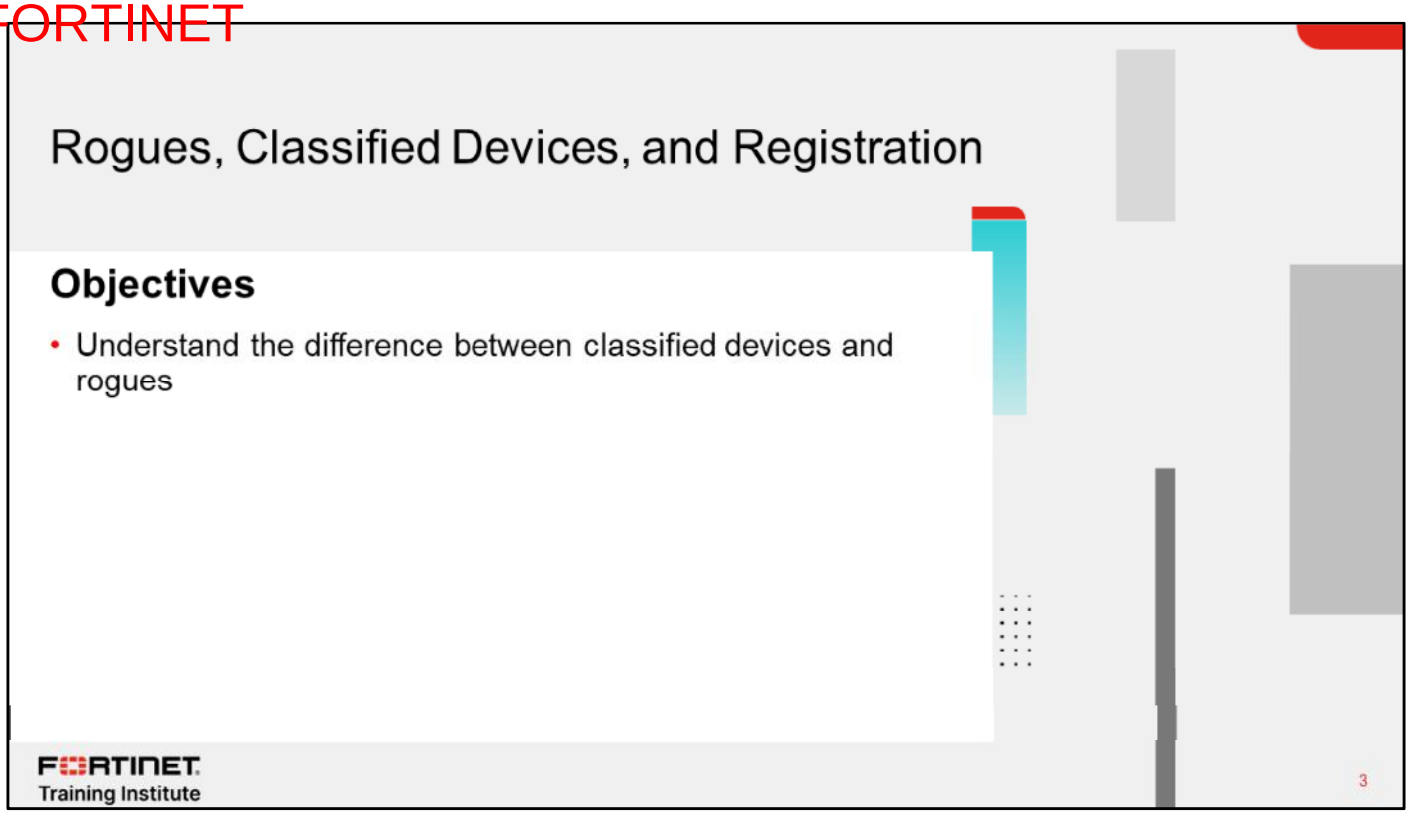
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating knowledge of the difference between rogues and classified devices, you will be able to better understand the process used, as well as the need for classification.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Rogue Devices

- Any device that has not been classified within FortiNAC
- Displayed as a PC with a question mark on the screen
- A host state enforced with the Forced Registration port group



FORTINET Training Institute

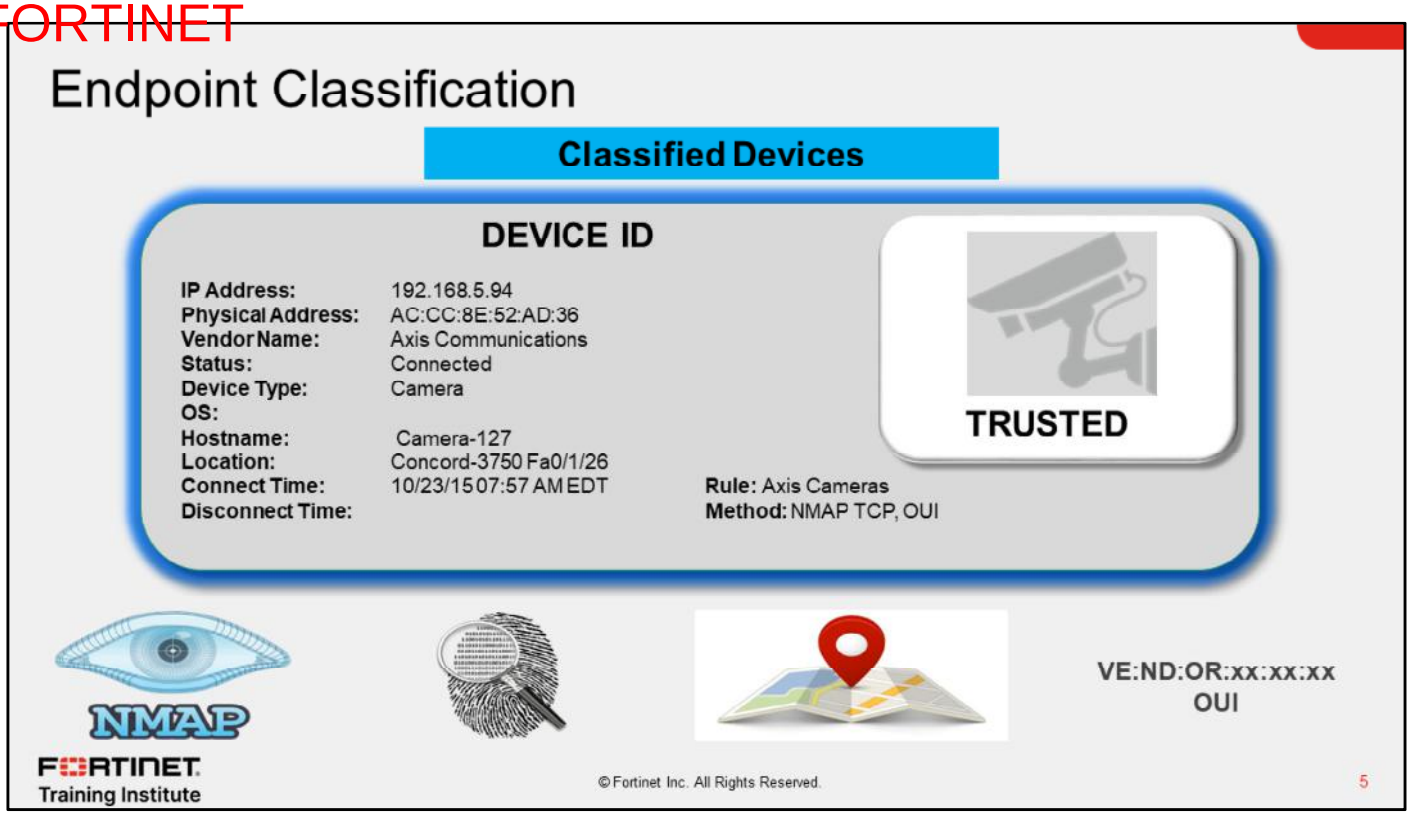
© Fortinet Inc. All Rights Reserved.

4

A rogue device is a physical address that has been seen on the network but has not been associated with an existing known host and is therefore considered unknown. On the GUI, FortiNAC represents a rogue device as a laptop image with a question mark on the screen. Rogue devices are often referred to as *unknown* or *untrusted* endpoints. The default logical network called **Registration** is the method used to isolate rogue hosts at the point of connection when enforcement is enabled.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



A foundation of visibility is created from the information that FortiNAC gathers from endpoints. Endpoints are a collection of elements: IP addresses, physical addresses, vendor names, statuses, and so on. However, having this information about endpoints does not classify them as trusted devices. One method used to classify connected devices is the device profiling tool. The device profiling tool uses administratively created rules that identify what's connected to the network using one or more methods that identify the type of device. In the example shown on this slide, there is a rule called printers that uses NMAP to scan open TCP ports. This scans devices as they connect to look for specific open TCP ports, and allows you to change the classification of an unknown rogue device to a trusted device, in this case, a printer.

You can create rules, as needed, for each different type of device that requires classification. An IP phone rule, for example, may use NMAP active, which means an NMAP scan looks at the operating system details for matched values. When FortiNAC evaluates the gathered information it compares it to a pre-set list in the database to determine if it is a match for the selected device type. You can also enter a user-defined value to allow for detailed device-specific customizations.

You can use multiple methods for more robust rule creation. For example, the rule shown on this slide uses both open TCP port and vender OUI requirements.

Endpoints that are classified are also known as registered hosts, because they are now considered registered in the system and trusted.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is a rogue device?
   A. Any device that connects to an unauthorized location
   ✓B. Any device that has not been registered with FortiNAC

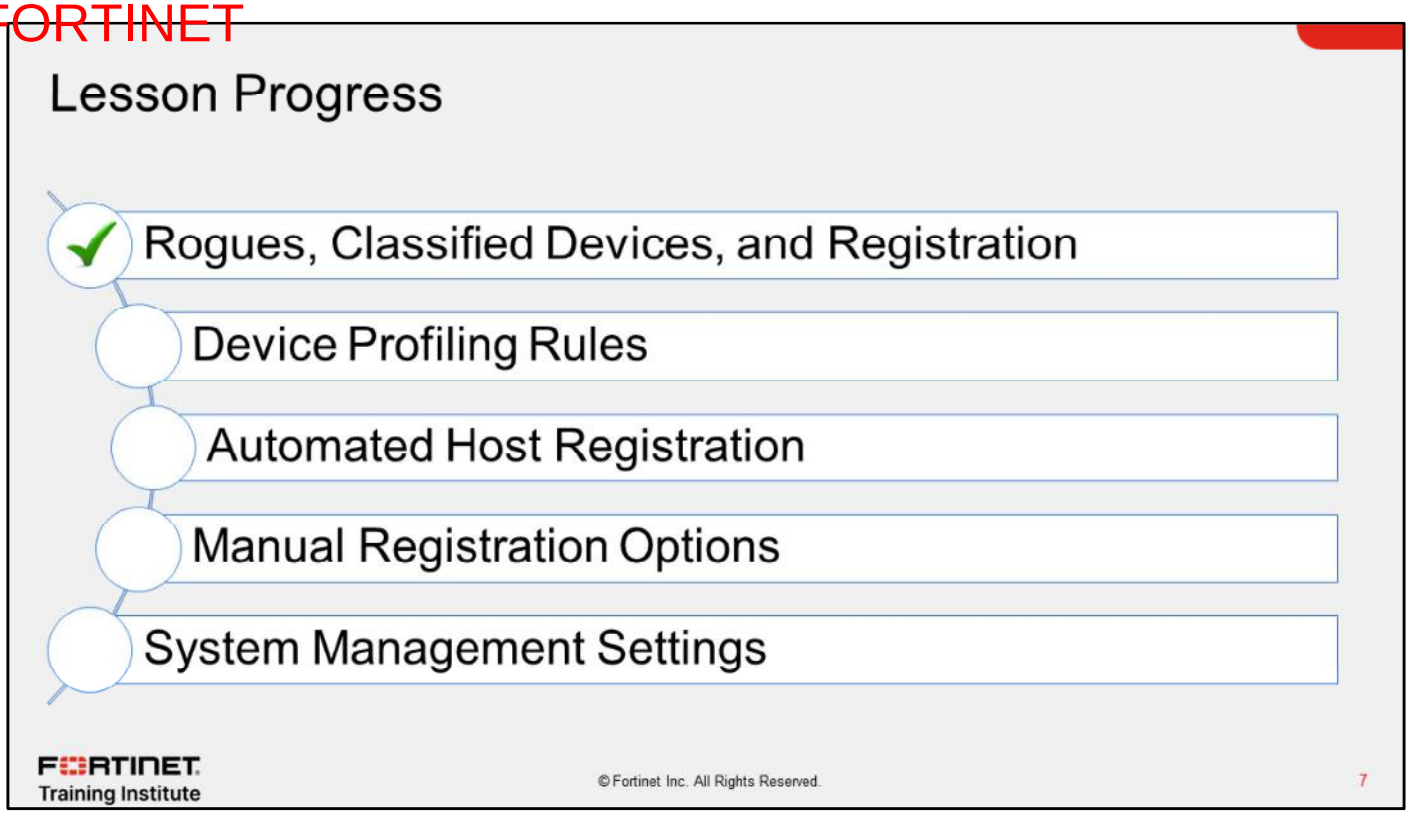
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

6

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

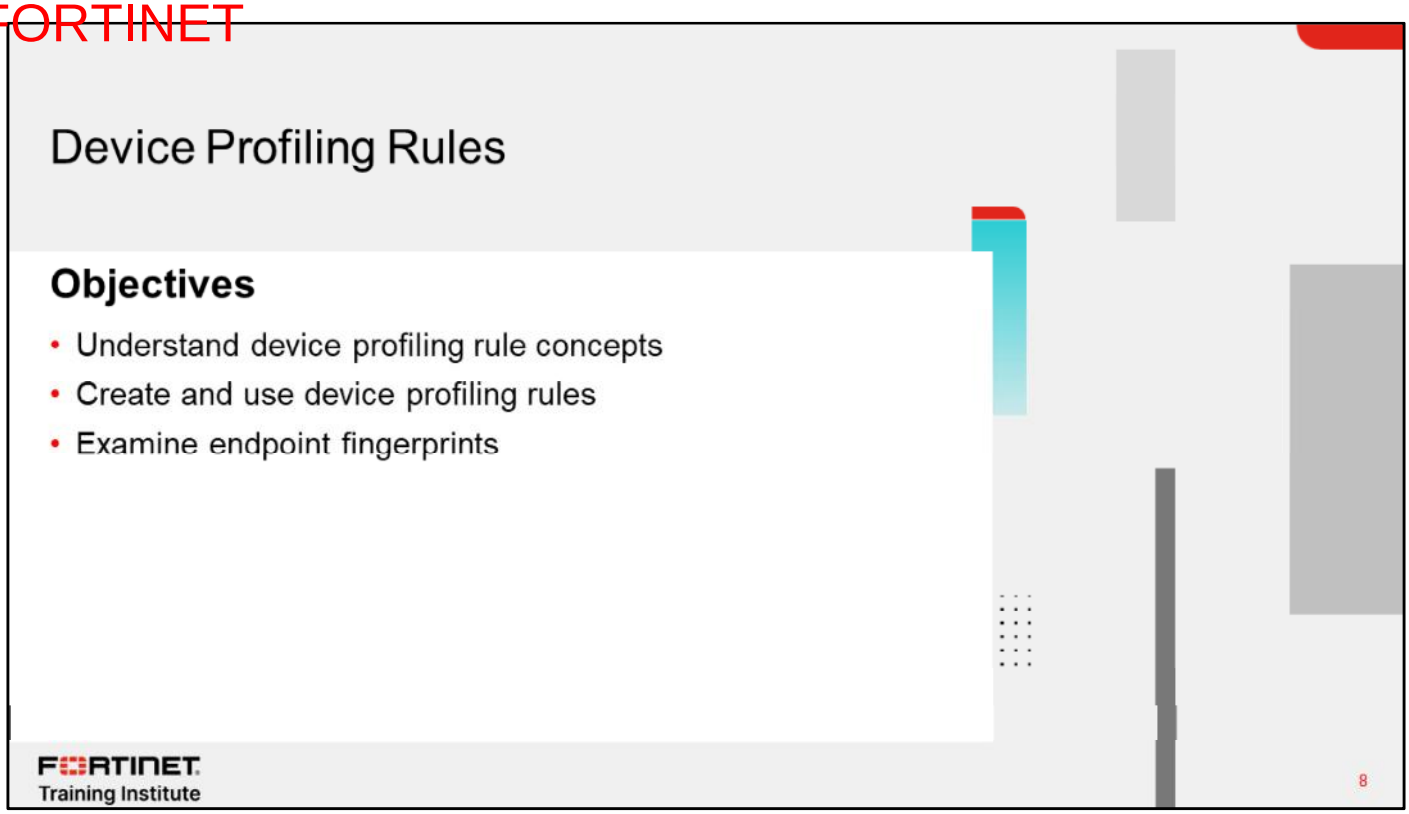


Good job! You now understand the difference between rogue devices and classified (registered) devices.

Now, you will learn how to create device profiling rules to identify and classify rogue devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

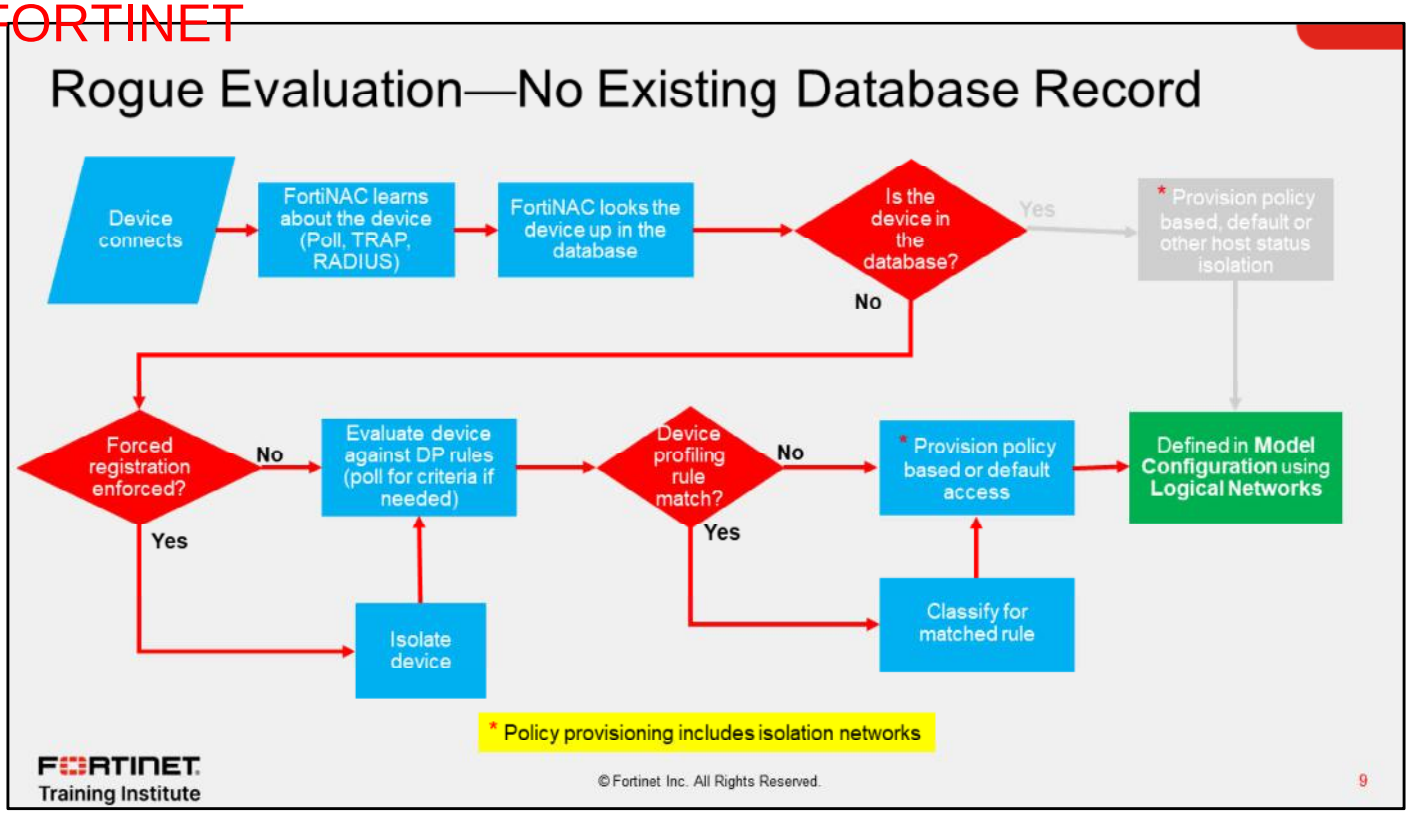
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



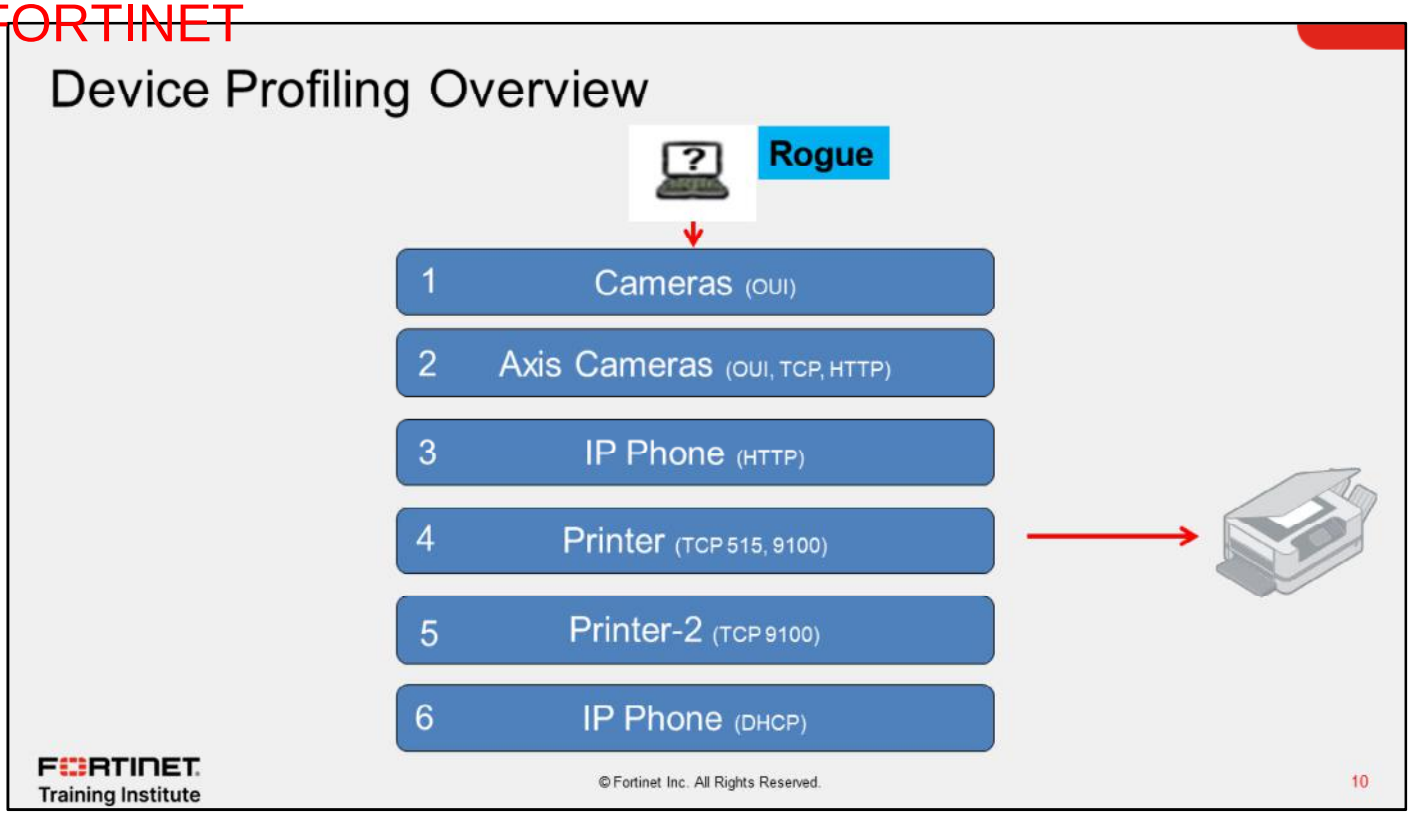
This slide shows the rogue evaluation processes and order of actions that FortiNAC performs the first time a rogue device connects to the network.

1. The rogue device connects.
2. FortiNAC learns of the connection. This is often done using Layer 2 polling, MAC notification traps, and RADIUS. Other methods may be used, depending on the vendor of the infrastructure.
3. FortiNAC queries the database for the connected device.
4. If the device is not in the database, FortiNAC adds it to the database, and determines if the point of connection is in the **Forced Registration** port group. If it is, the device is isolated and then evaluated against the device profiling rules. If the point of connection is not in the **Forced Registration** groups the device is evaluated against the device profiling rules from the current VLAN. Note that devices are initially evaluated against device profiling rules only if they do not exist in the database. This prevents unnecessary rule evaluation for devices that already exist in the database.
5. If no rule is matched, the device remains in the current policy-defined VLAN.
6. If the host matches a device profiling rule, the classification settings for that rule are applied and access is provisioned based on policy (default or network access policy).

How the device is provisioned is based on logical networks and how they are defined for each infrastructure device. The definition for these logical networks is set in the **Model Configuration** view of the infrastructure device. Provisioning based on policy includes isolation networks. For example, the policy to isolate a rogue host is based on the device status and the point of connection (the port is in the Forced Registration group).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When a rogue device record is created, the device is evaluated against the enabled device profiling rules. FortiNAC evaluates a device against each rule in ranked order until one of the following results is achieved:

- Pass: The device matches all necessary criteria defined in the rule.
- Fail: The device fails to match all necessary criteria defined in the rule.
- Insufficient data: The necessary criteria cannot be evaluated due to an inability to gather device information.

If a rule evaluation ends with an insufficient data result, the device profiling process stops all evaluation, and the device is added to the database as a rogue. It is for this reason that selected methods of evaluation should be taken into consideration when determining rule order.

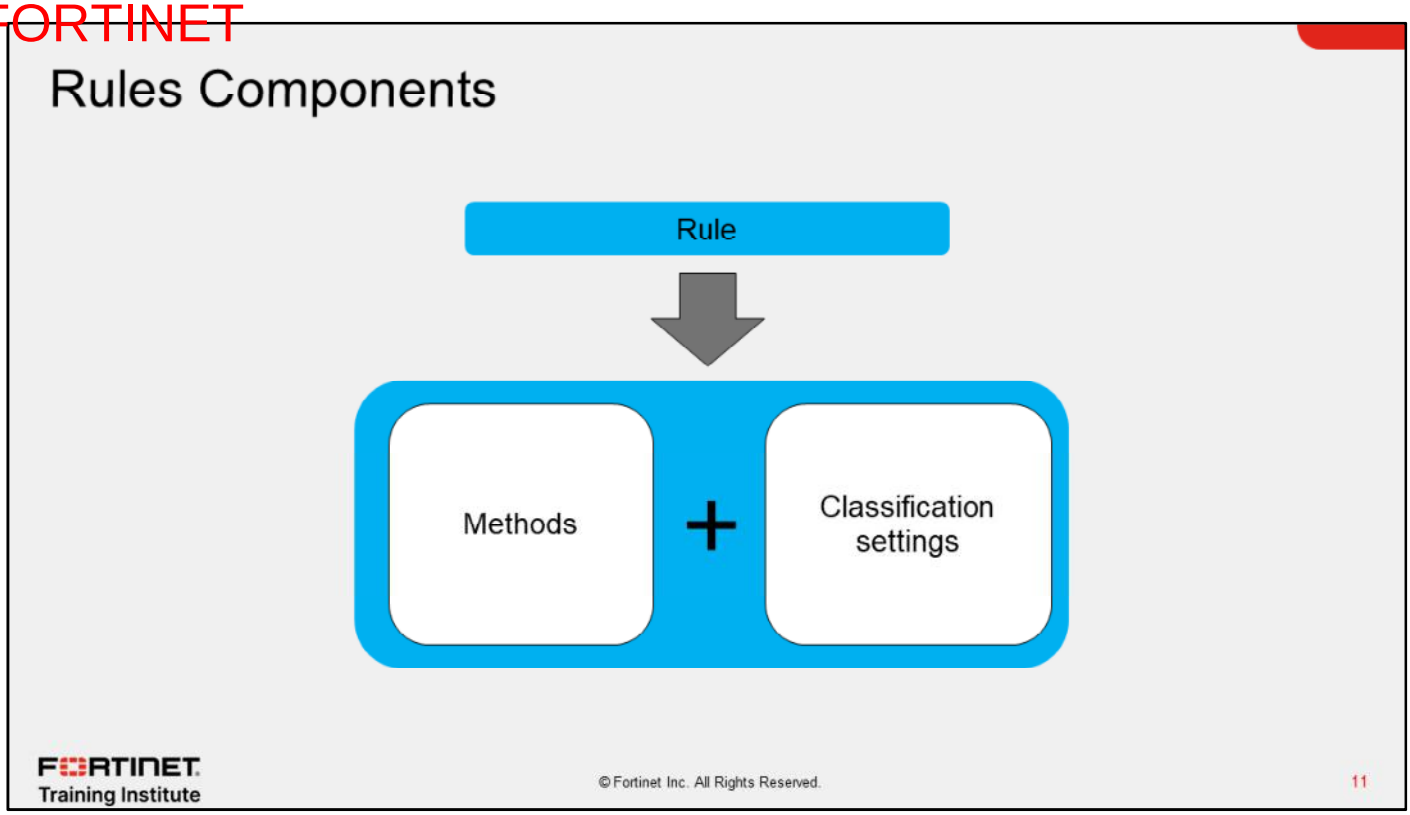
The following is an example list of rules and the methods used to validate each rule. They are prioritized for efficient processing and specific identification:

- Rule 1, called Cameras, uses a single validation method: Vendor OUI.
- Rule 2, called Axis Cameras, uses three methods: Vendor OUI, open TCP ports, and an HTTP query.
- Rule 3, called IP Phone, uses a single method: HTTP query.
- Rule 4, called Printer, uses a single method: TCP ports and is keying upon two ports being open: 515 and 9100.
- Rule 5, called Printer-2, uses a single method: TCP ports and is keying upon a single port being open: 9100.
- Rule 6, called IP Phone, uses a single method: DHCP fingerprint.

Next, you will take a closer look at the components of a device profiling rule.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



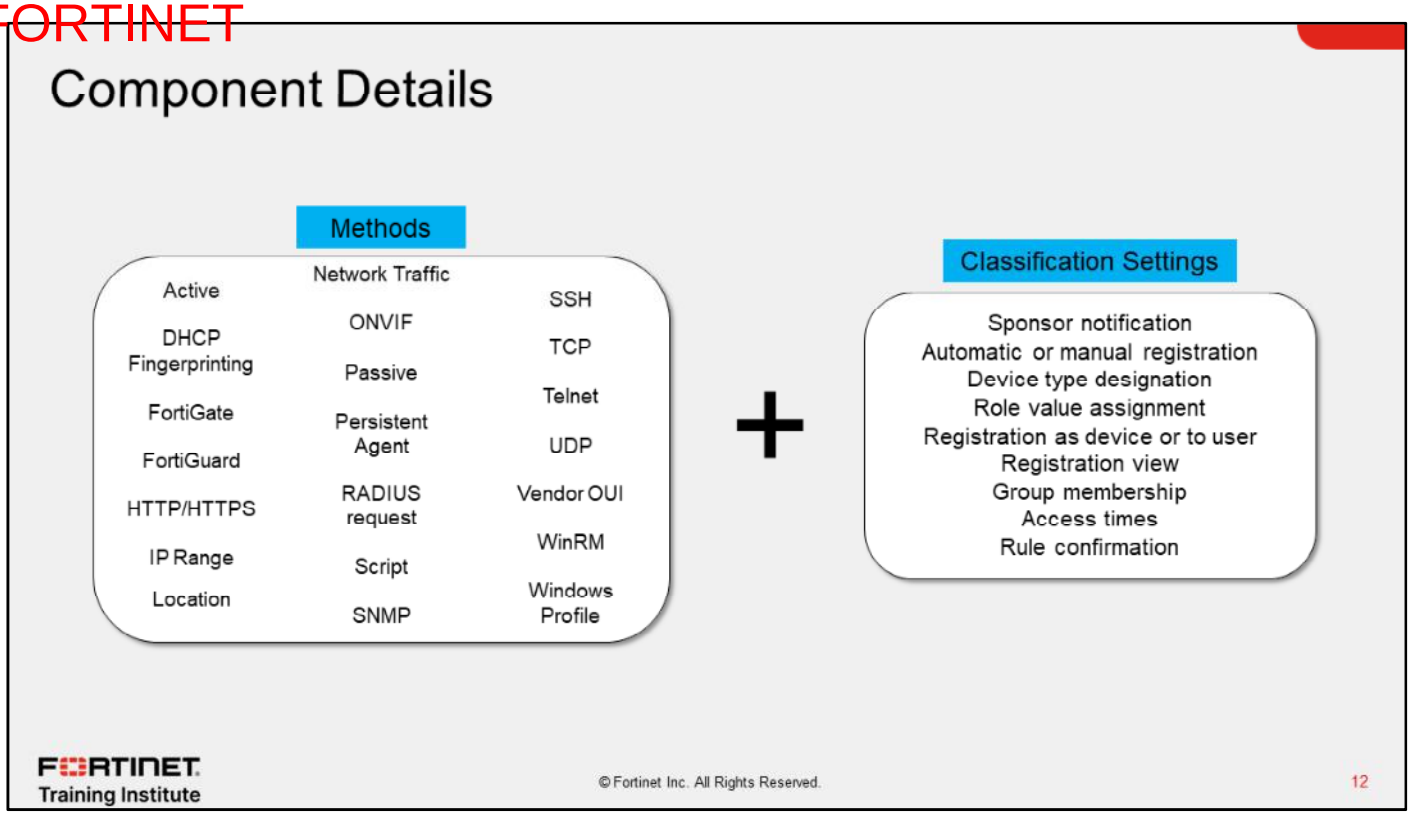
Device profiling rules are used to evaluate and classify rogue devices. You can configure profiling rules to automatically, manually, or through sponsorship, evaluate and classify unknown, untrusted devices as they are identified and created.

Device profiling leverages rules comprising classification settings and methods used for evaluation.

FortiNAC uses the rule methods to evaluate devices to test for a pass or fail result. If all selected methods result in a pass result, then FortiNAC applies the rule-defined classification settings of device type, grouping, and attribute values.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

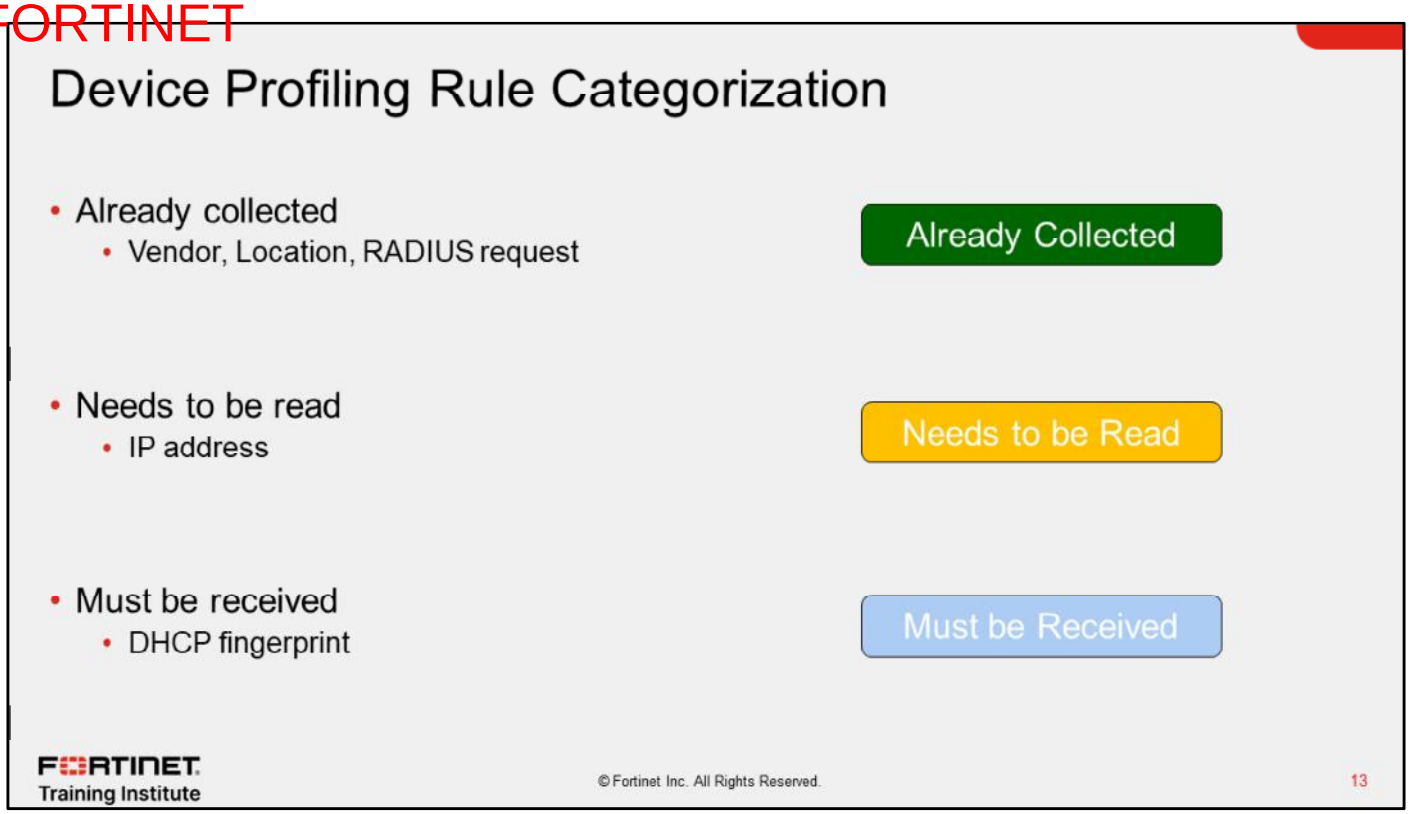


The methods shown on this slide are used to evaluate connected rogue devices. If more than one method is selected, the selected methods are logically anded when determining if the rule is matched. Match criteria are configured for each method, as the methods are selected.

The classification settings outline how FortiNAC will configure the connected device and how it will appear in the GUI. You can leverage the device type, role, and group membership for policy enforcement. You can use access availability settings to grant networks access during specific days and times, and the **Rule Confirmation** option to revalidate previously profiled devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Efficient and specific ranking of the rules is required so that a device is evaluated against all of the available rules.
FortiNAC evaluates a device against each rule until a pass, fail, or cannot evaluate (because of insufficient data) result is reached.

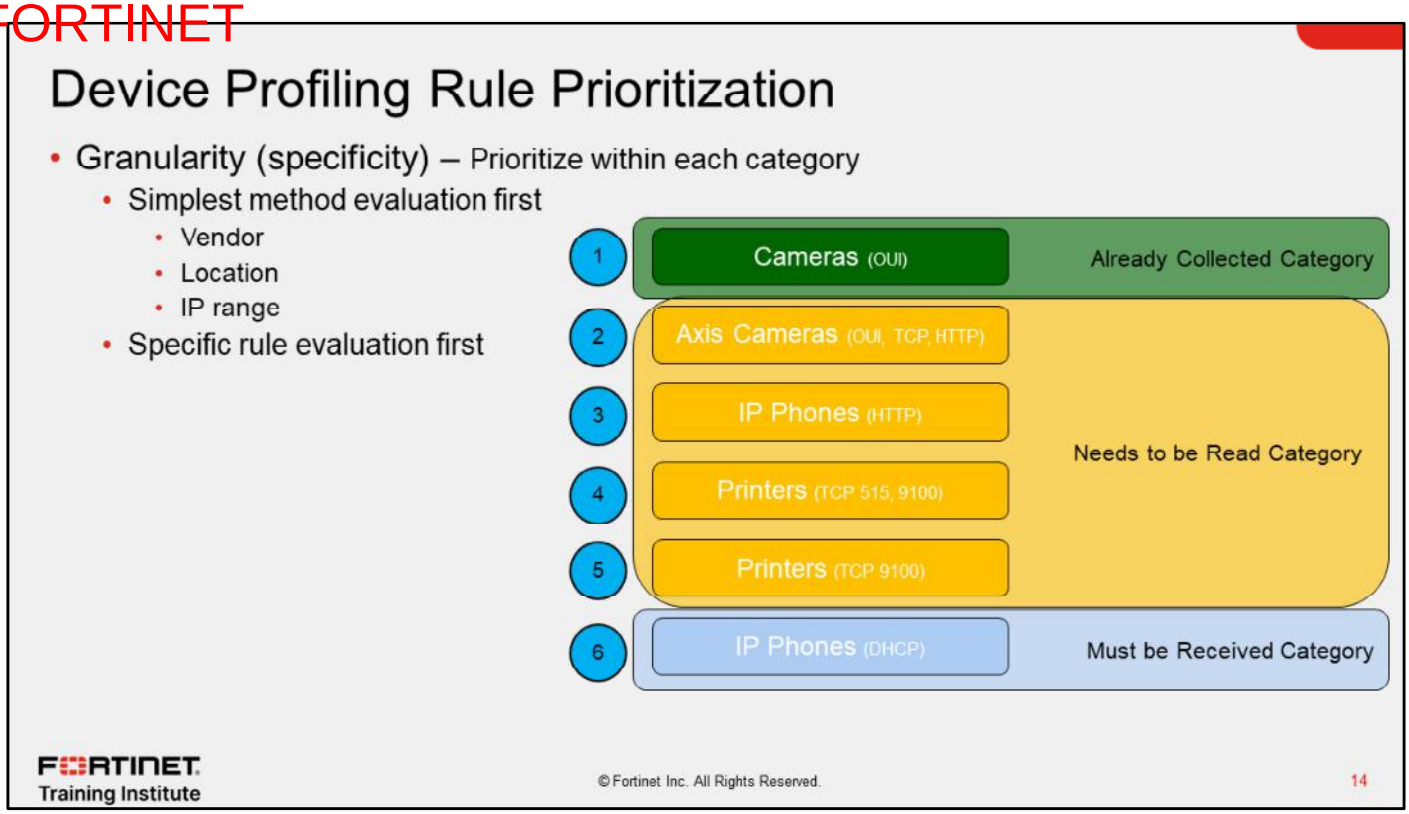
- A rule evaluation result of pass classifies the device as defined by the rule classification settings.
- A rule evaluation result of fail continues the device evaluation process with the next ranked rule.
- A rule evaluation result of cannot evaluate stops the device evaluation process. This occurs when a method within the rule requires data that is not available or able to be validated as current.

As a best practice, categorize rules fall into the three prioritized groups, which should, in most cases, follow these guidelines:

- Place rules with vendor OUI and/or location methods only in the Already Collected group.
- Place rules with one or more IP-based methods in the Needs to be Read group.
- Place any rules that use DHCP methods in the Must be Received group.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



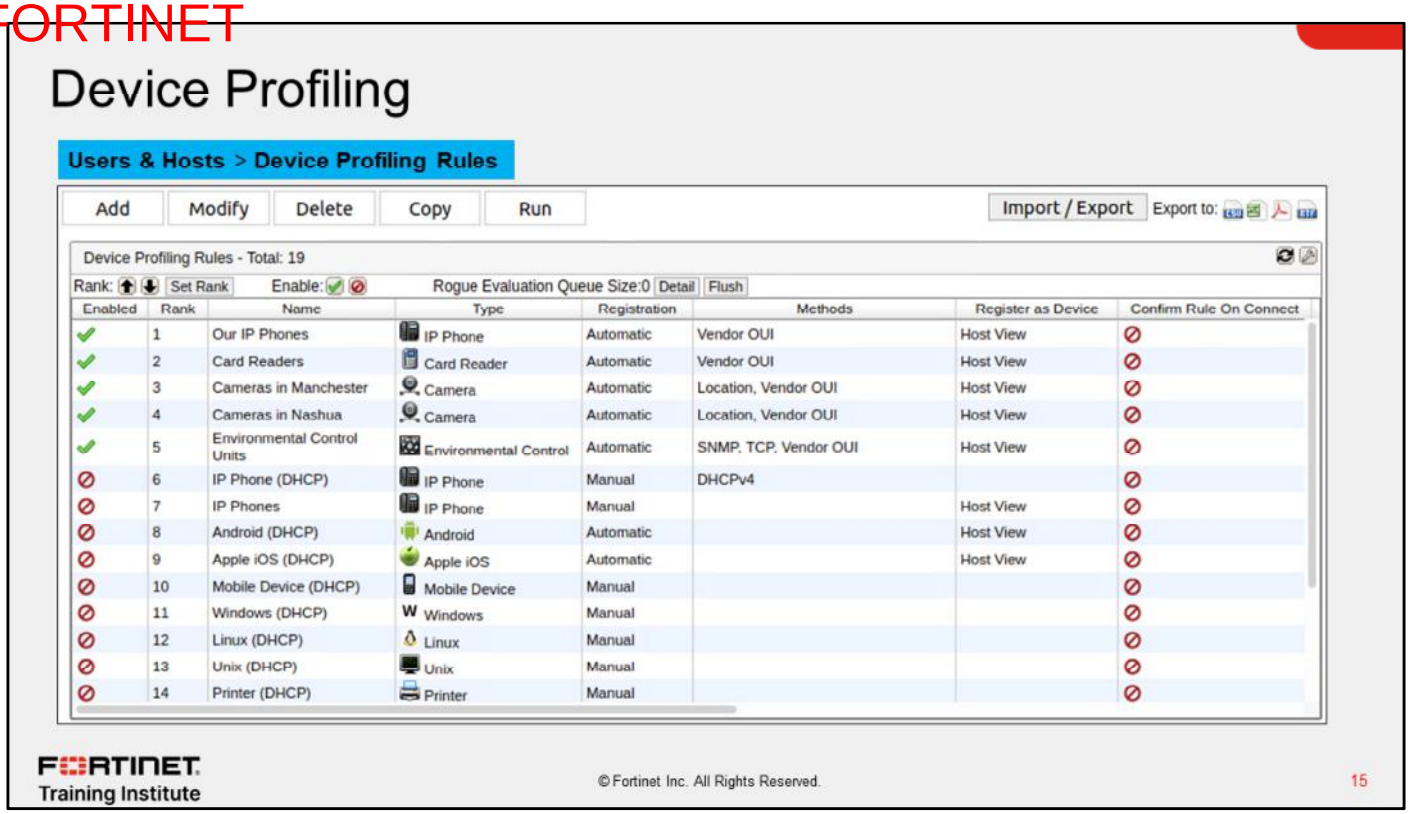
Within each group, organize the rules based on granularity.

Here is the result of following those guidelines with these example rules:

- Rule 1 OUI evaluation result is the simplest path to failure, resulting in the lowest overhead to validate.
- Rule 2 Evaluation of TCP ports and HTTP is done only if OUI matches. This prevents unnecessary processing of devices that don't have the correct vendor OUI.
- Rule 3 uses a single IP-reliant method.
- Rule 4 and 5 are specifically ordered with the most granular rule first. If a host has only TCP port 9100 open, it will fall through to rule 5.
- Rule 6 is efficiently ordered because DHCP fingerprint receipt is not controlled by FortiNAC and could stop rule evaluation if no fingerprint is received.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can access the **Device Profiling Rules** window by clicking **Users & Hosts** > **Device Profiling Rules**.

The **Device Profiling Rules** view displays the default set of rules provided. Use this window to modify the default rules or to create your own set of rules. Default rules vary depending on the version of the software and the firmware installed. Upgrading to a newer version of the software does not add or modify default rules.

In multimethod rules, evaluate OUI, location, and IP range before any other methods. This is so you can write profiling rules to specifically target specific devices while excluding others.

Disabled rules are ignored when processing rogues. Device profiling rules are disabled by default and are set not to register devices. When you are ready to begin profiling, enable the rule or rules you want to use.

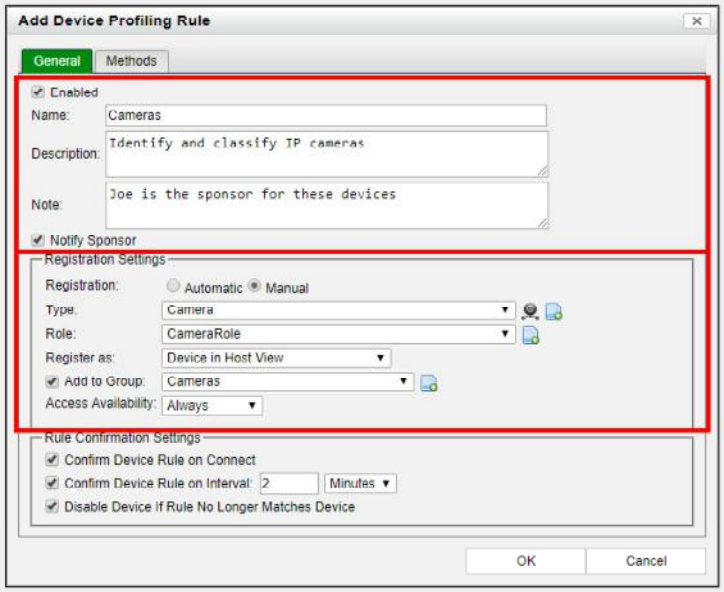
Notice that the rules are ranked, which you can modify, for the order in which the rules should be applied.

Run the rules to evaluate rogues that already exist in the database.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

General Rule Information



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

16

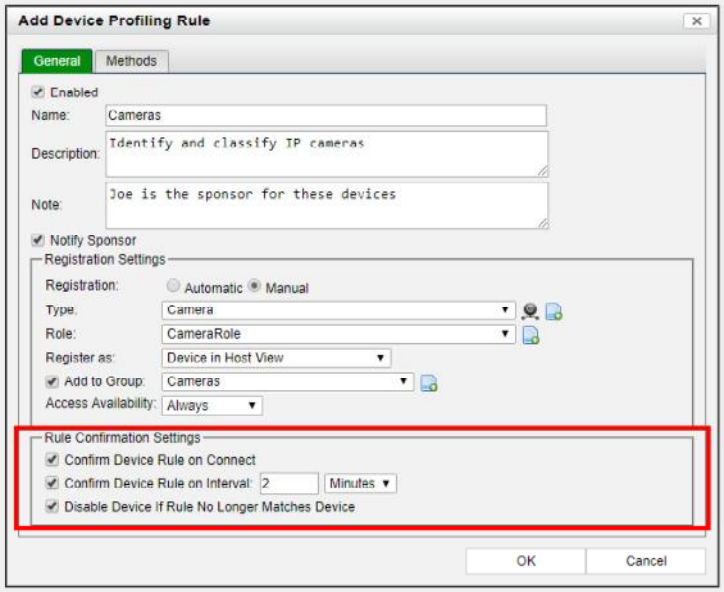
Creation of a device profiling rule begins with configuring the general settings that define the registration settings, rule confirmation settings, and other general attributes. At the top of the **Add Device Profiling Rule** window, there is an option to enable the rule. Only rules that are enabled will process rogues to see if they match. The rule needs a name and can also have an optional description. At the bottom of the selected area, there is an option to notify a sponsor. Any rule can be set up so that a sponsor is notified when a rule is matched. A sponsor is an administrative user. This can be configured on a rule-by-rule basis and is configured within an administrator profile.
The middle section is where you configure the registration settings. The very first option is to have the settings carried out automatically or as a manual process. If set to **Automatic**, FortiNAC will carry out all the following registration steps as soon as the rule is matched. If set to **Manual**, the rule is still matched, the device is profiled, however, the registration settings are not processed until a sponsor logs in to the GUI and manually registers the device. The next setting to configure is the device type. There are many pre-existing device types. However, administrative users can also create their own types, which provides complete flexibility, regardless of the types of devices in any given environment. A role can be assigned to a device and this value could then be leveraged in a policy. For example, there could be a network access policy configured to provision devices with a role of camera to a particular network, depending on the point of connection. The **Register as** field is where you can define were the device is placed. The options are, in the host view, the topology view, or both. The most common option is the host view.

You can also assign device ownership for BYOD devices if user information is known. For devices that are in the host view, they can automatically be added to a host group. However, for devices that are in the topology view, you need to select a topology container. The **Access Availability** option lets the administrative user define specific days and times the profiled device is allowed on the network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

General Rule Information (Contd)



FORTINET Training Institute

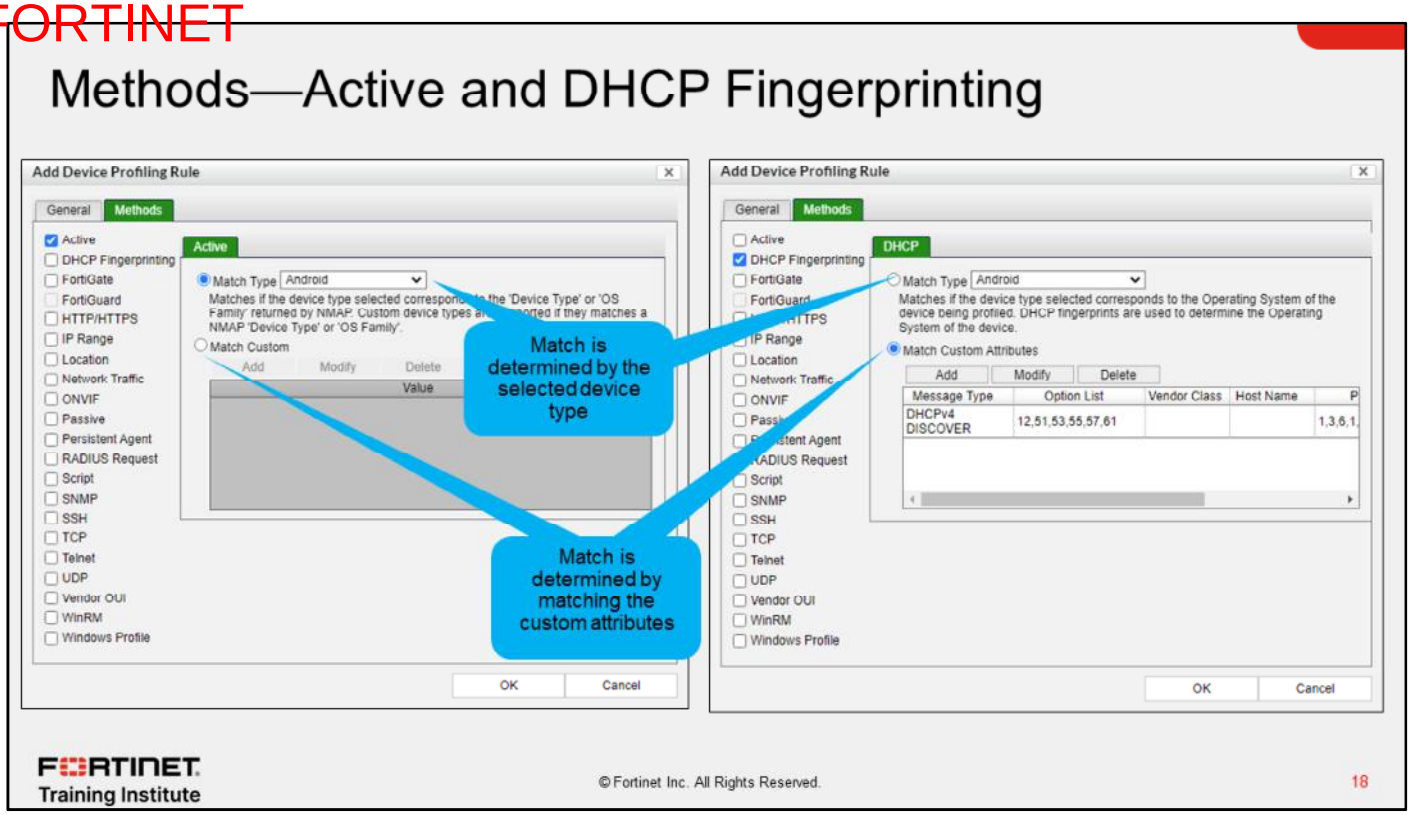
© Fortinet Inc. All Rights Reserved.

17

When a rogue device is processed by a rule and found to be a match, FortiNAC remembers the matching rule. Going forward, FortiNAC revalidates that the device still matches the rule, each time the device connects to the network, and/or at a user-defined time interval. If the device fails to match the rule on revalidation, you can configure FortiNAC to automatically disable the device. This is a safeguard against impersonation of a previously-profiled endpoint.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This lesson covers some of the most common methods. You can find details about all methods in the *FortiNAC Administrator's Guide*.

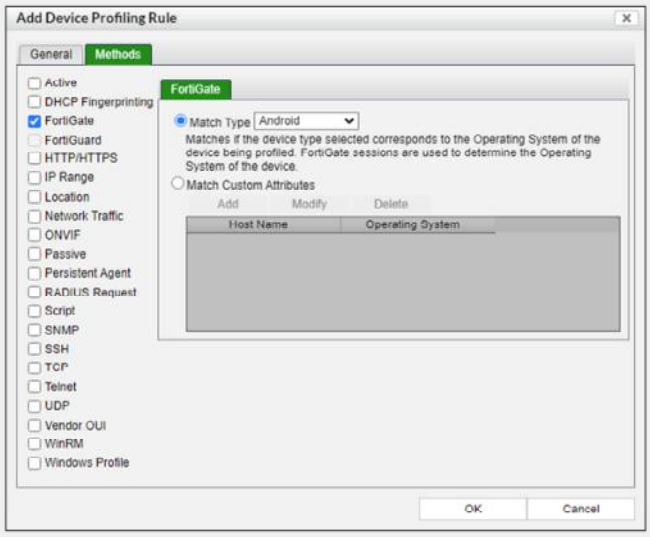
The active method is an NMAP scan of a connected host. There is a device database that will match on the operating system detail information that is gathered during the NMAP scan. There is a second option to match a custom value. You can use the key values that you find in the NMAP scan results instead of using the existing database entries. Therefore, you can use an exact string match or regular expression, which lets you customize the active method for almost any environment.

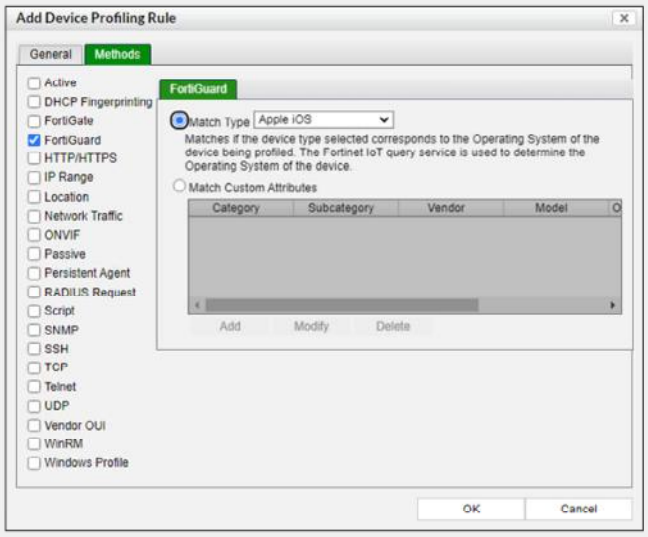
The DHCP fingerprinting method evaluates a DHCP discovery or request packet that was received by the FortiNAC device. Similar to the NMAP scan, the FortiNAC device has a DHCP fingerprint database that contains a large list of fingerprints. These fingerprints are identified using option lists and parameters seen in the DHCP discovery or request. When using **Match Custom Attributes**, option fields that are left blank are ignored. The custom attributes supported are: DHCP message type, option list, vendor class (DHCP option 60), host name (DHCP option 12), parameter list (DHCP option 55), and operating system.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Methods—FortiGate and FortiGuard





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

19

The FortiGate method leverages firewall session information to determine a match. The **Match Type** option will return a pass for this method if the session information indicates a matching operating system. The **Match Custom Attributes** option will use the firewall session information and evaluate it against the defined host name or operating system values. The values can be an exact string match or a regular expression.

Firewall session polling must be set up to use this method. You do this by right-clicking on the FortiGate device in the **Network** > **Inventory** view, and then selecting **Set Firewall Session Polling**.

The FortiGuard method uses the Fortinet IoT query service to determine the OS of the device. When you use the **Match Type** option, you will get a match if the device type selected corresponds to the operating system of the device being profiled. The **Match Custom Attributes** option can be used to match against one or more of the following attributes:

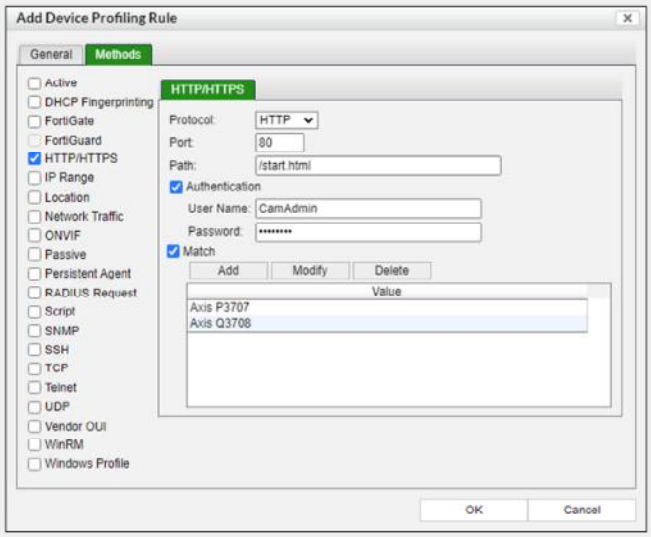
- Category
- Subcategory
- Vendor
- Model
- Operating System
- Sub Operating System

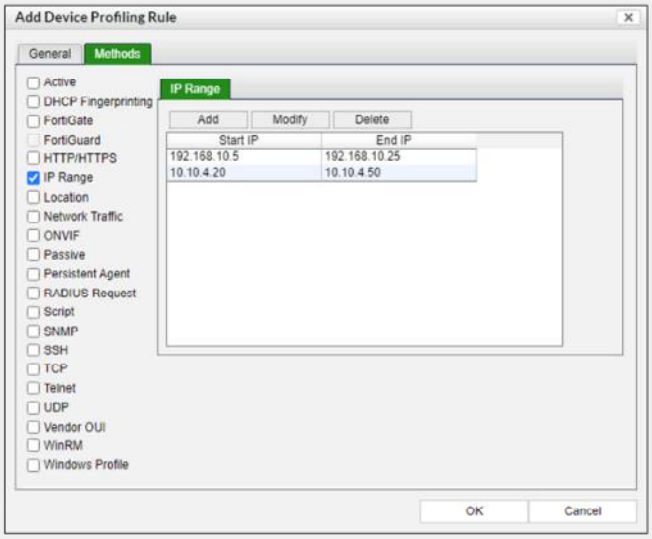
Note that a FortiCare support contract is required to enable the FortiGuard device profiling method; otherwise, the method will be grayed out.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Methods—HTTP/HTTPS and IP Range





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

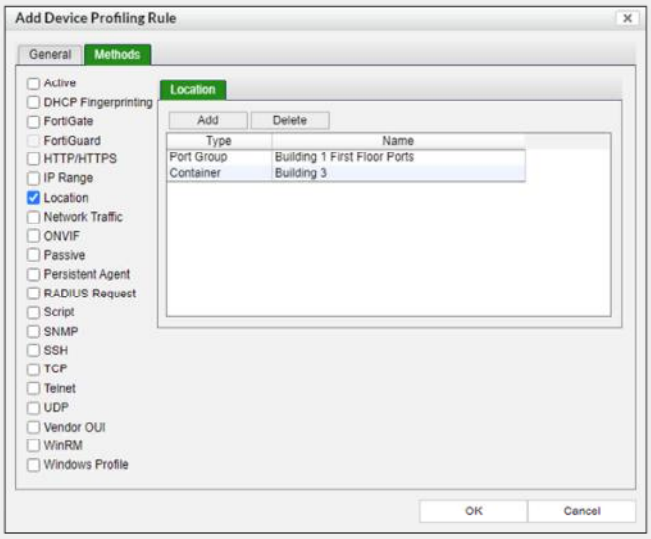
The HTTP/HTTPS method configures the FortiNAC device so that it attempts to open a connection with the device it is trying to profile on a particular port of your choosing, and using the selected protocol. Optionally, it can attempt to load a page and/or enter designated credentials. A matching value is specified and the page contents are parsed for those values. If multiple response values are entered, FortiNAC will attempt to match any of them.

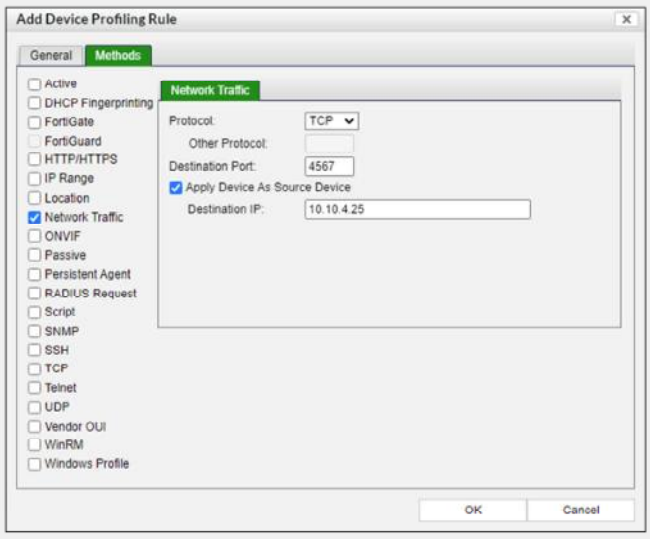
The IP range method results in a match if the IP address of a device falls within one of the ranges. You must specify at least one IP range. This method requires the FortiNAC device to know the current IP address of the device that is profiled, and will trigger a Layer 3 (IP to MAC) poll to gather this information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Methods—Location and Network Traffic





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

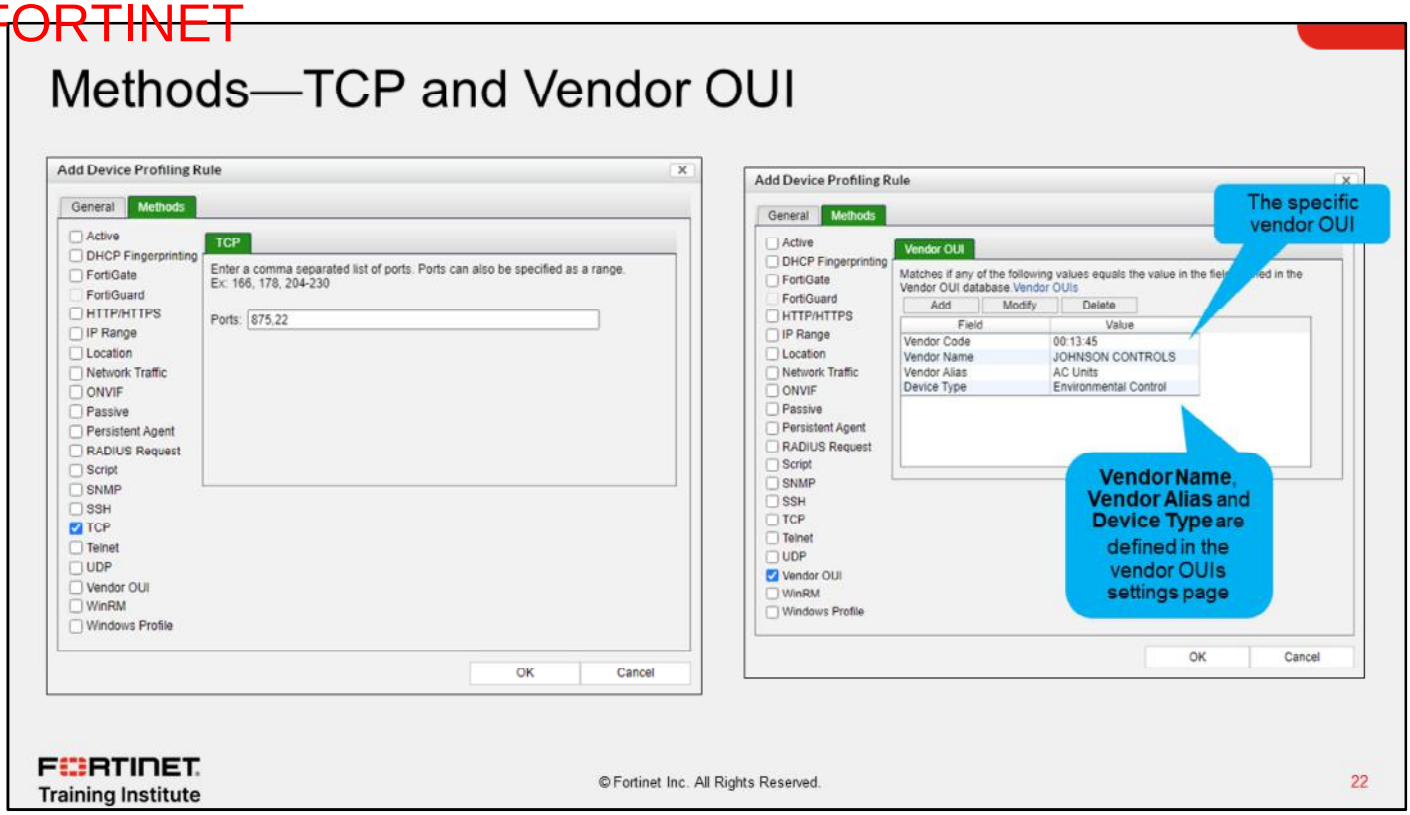
21

The location method finds a match if the device connects to the selected location on your network. The options are: anything within a container in the inventory view, anything in a port group, or anything in a device group. In the example shown on this slide, if the endpoint being evaluated is connected to a port in the **Building 1 First Floor Ports** group or any port of any device in the **Building 3** container, then it satisfies the location criteria.

The network traffic method evaluates network traffic generated or received by the device being profiled by protocol, destination port, and destination IP address. Firewall session polling must be enabled to leverage firewall session information. Firewall session polling is configured by right-clicking a device in the topology tree and selecting **Set Firewall Session Polling**. The network traffic information can also be received using Netflow. Netflow source devices must be configured so that the export destination for the device is the IP address of FortiNAC, and the listener port is set to 2055.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The TCP method matches if the device provides a service on all of the ports specified. You must specify at least one port, but all specified ports must match. Multiple ports are entered, separated by commas, such as, `162, 175, 188`. A range of ports are entered using a hyphen, such as `204-215`. The FortiNAC device uses NMAP to perform the port scan.

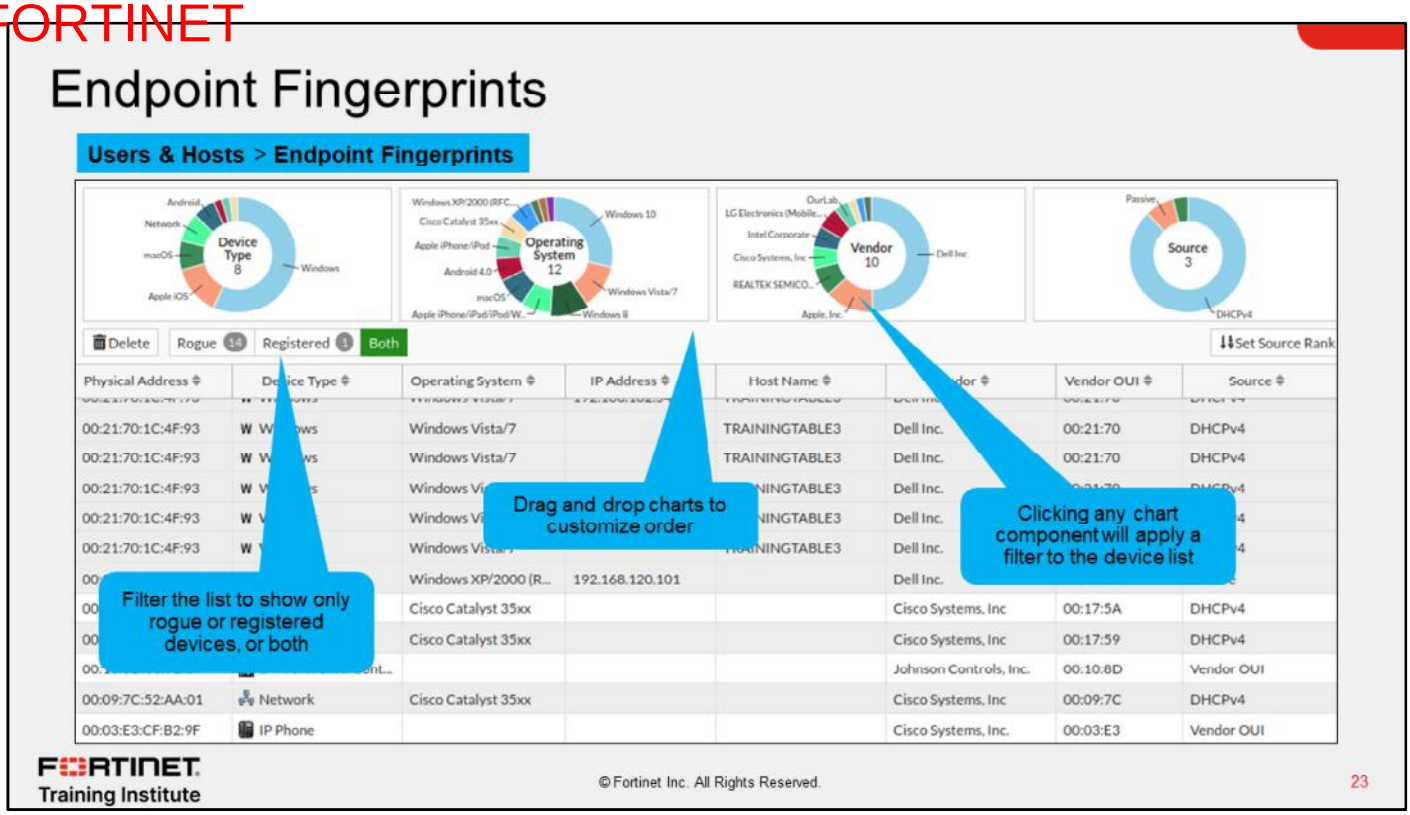
The vendor OUI method matches if the vendor OUI for the device corresponds to the OUI information selected for the method. At least one vendor option must be specified. If there are multiple entries, the device only has to match one entry to match this rule. Options include:

- **Vendor Code:** A specific vendor OUI selected from the list in the FortiNAC database. To select the OUI, begin typing the first few characters. A list of matching OUIs is displayed in a drop-down list.
- **Vendor Name:** A single vendor name selected from the list in the FortiNAC database. To select the name, begin typing the first few characters. A list of matching vendors appear in a drop-down list. You can use an asterisk as a wildcard at the beginning and/or end of a vendor name to match all variations of a name.
- **Vendor Alias:** A vendor alias is an administratively-defined string that you can assign to one or more vendor OUIs, across multiple vendors. You can define the alias values in the **Vendor OUI** settings page, located in the **Identification** folder, which you can find in the system settings.
- **Device Type**: Select a device type from the drop-down list provided. Includes items such as Alarm System or Card Reader. If this option is selected, the device type associated with the vendor OUI of the connecting device must match the device type for the OUI in the FortiNAC vendor database. You can see the device type in the vendor database, and override it in the vendor OUIs settings page, located in the **Identification** folder in the system settings.

Note that it is a best practice to use the vendor OUI method in conjunction with other methods to avoid undesired matches due to MAC address spoofing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

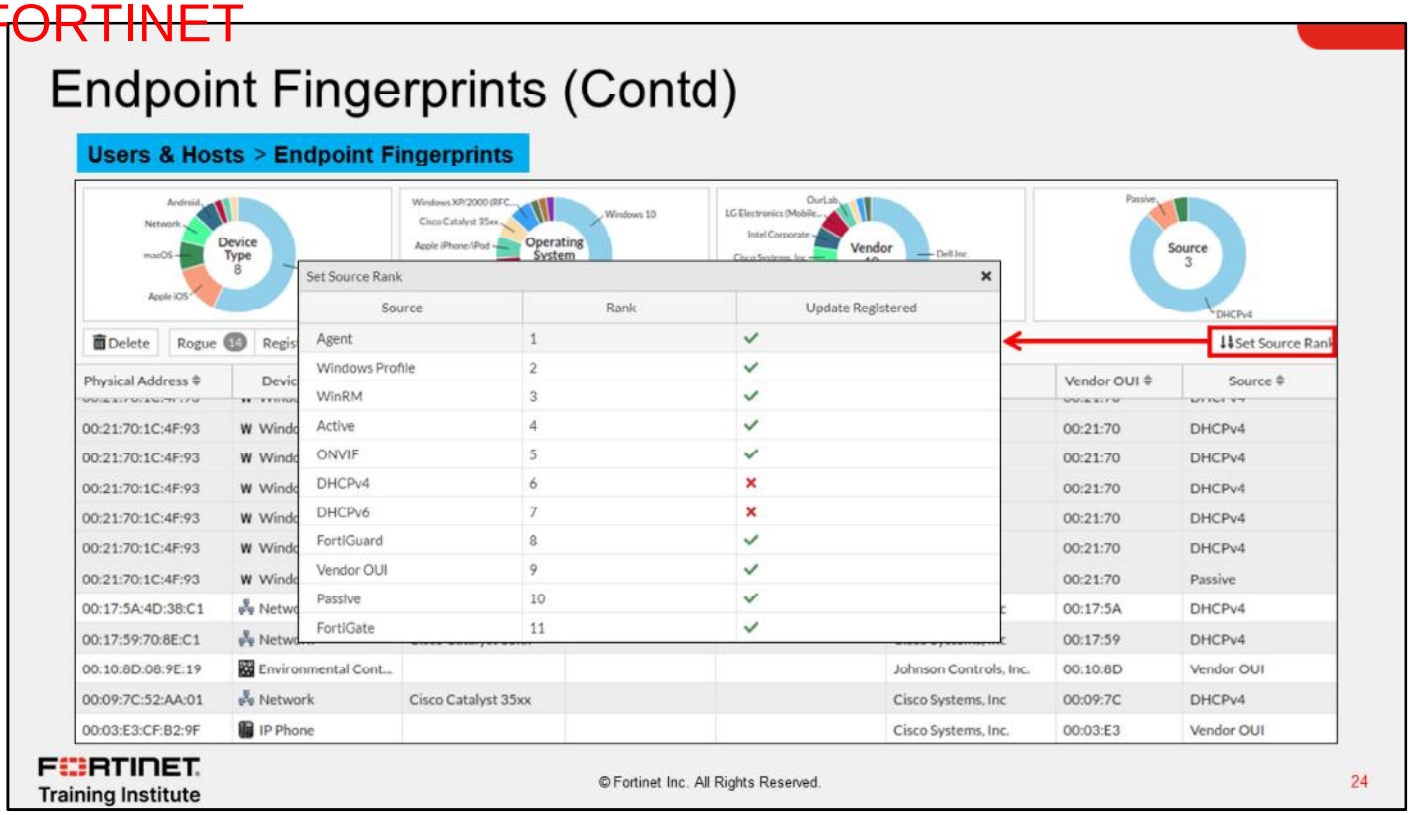


FortiNAC uses a list of sources to gather fingerprint information about all devices (rogue and registered) that are connected or have previously connected to the network. Charts across the top of the view break down the devices by device type, operating system, vendor, and source. You can drag and drop the graphs to customize the order, and you can click any component of a chart to apply a filter to the device list. The button at the top of the device list allows you to filter the list to display only rogue or registered devices, or both.

The same device may have several fingerprint entries in the list. This is because a new entry is made for each unique fingerprint. For example, a fingerprint may show a different set of DHCPv4 options or parameters from two DHCP discovery messages, or between DHCP discovery and request messages. The same host with multiple fingerprints identifying different operating systems is most likely a dual-boot host.

Vouchers & Dumps are Available | WhatsApp +201224560923

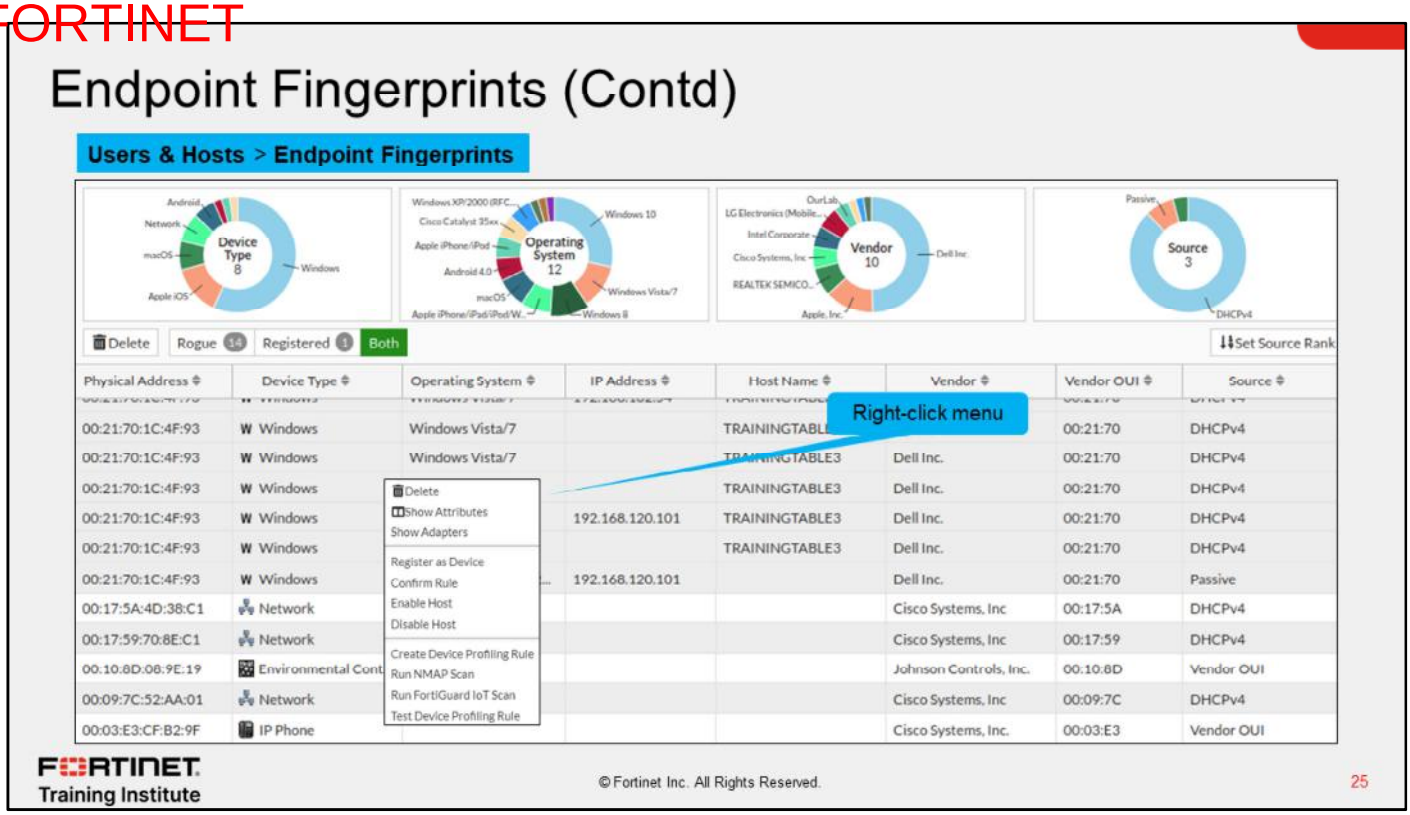
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The set source rank list will display the sources of data collection used to gather the fingerprints. These sources can be ranked for situations where a device has conflicting data. For example, if the **Vendor OIU** source fingerprints it as one type of device and **Active** another, FortiNAC will represent it in the list as the device type associated with the higher ranked source.

Vouchers & Dumps are Available | WhatsApp +201224560923

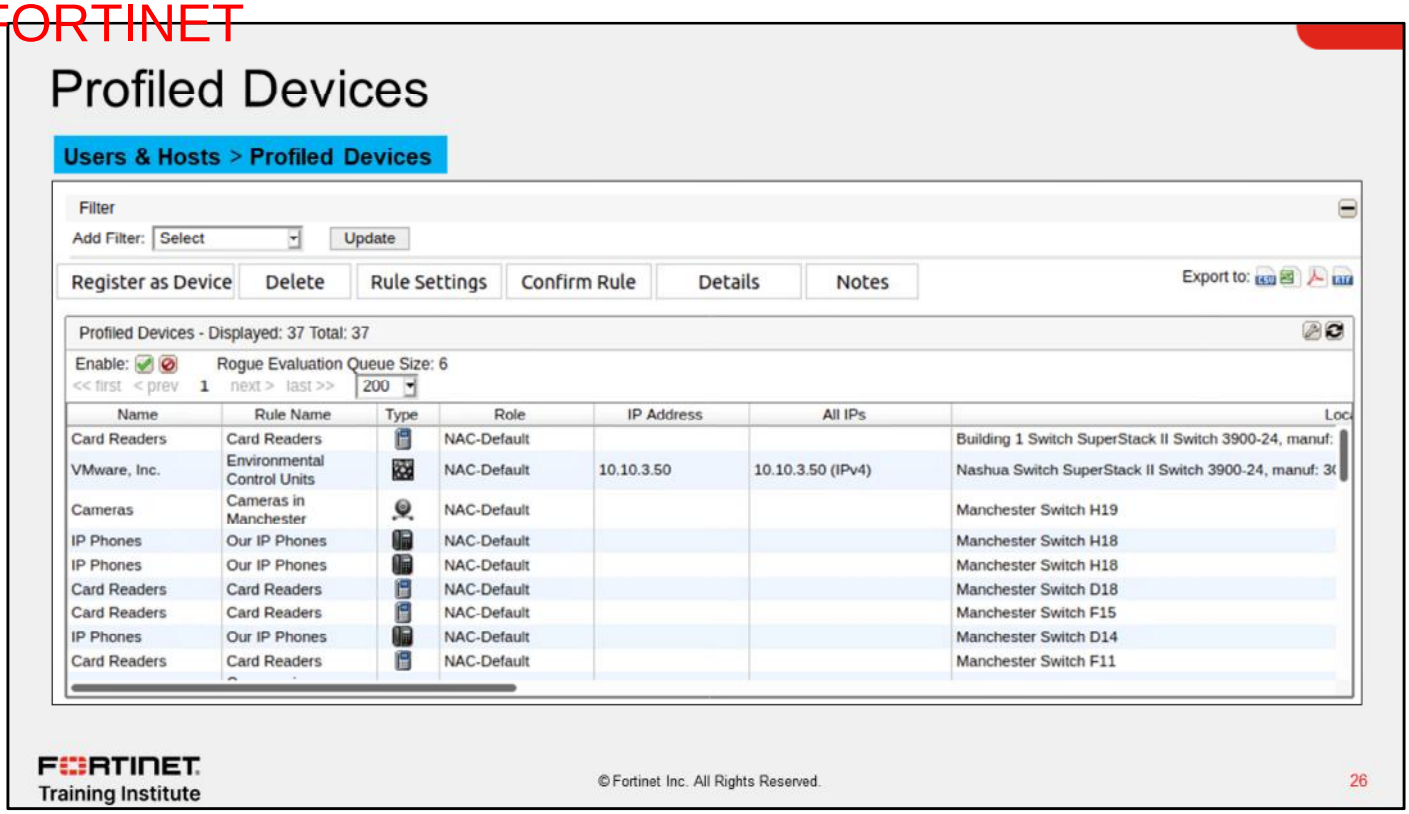
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Right-click options are available for any host in the list. The options are:
Delete: deletes the selected fingerprint(s).
Show Attributes: displays the fingerprint attributes information.
Show Adapters: displays the adapter information associated with the device.
Register as Device: registers the host as a device.
Confirm Rule: if the device has matched a device profiling rule, the device is re-evaluated against that rule.
Enable Host: enables the host, if it has been disabled.
Disable Host: disables the host.
Create Device Profiling Rule: displays the **Add Device Profiling Rule** window with any methods known as a result of the fingerprint enabled and populated.
Run FortiGuard IoT Scan: attempts to identify the device using FortiGuard.
Test Device Profiling Rule: evaluates the device against an existing profiling rule.

Vouchers & Dumps are Available | WhatsApp +201224560923

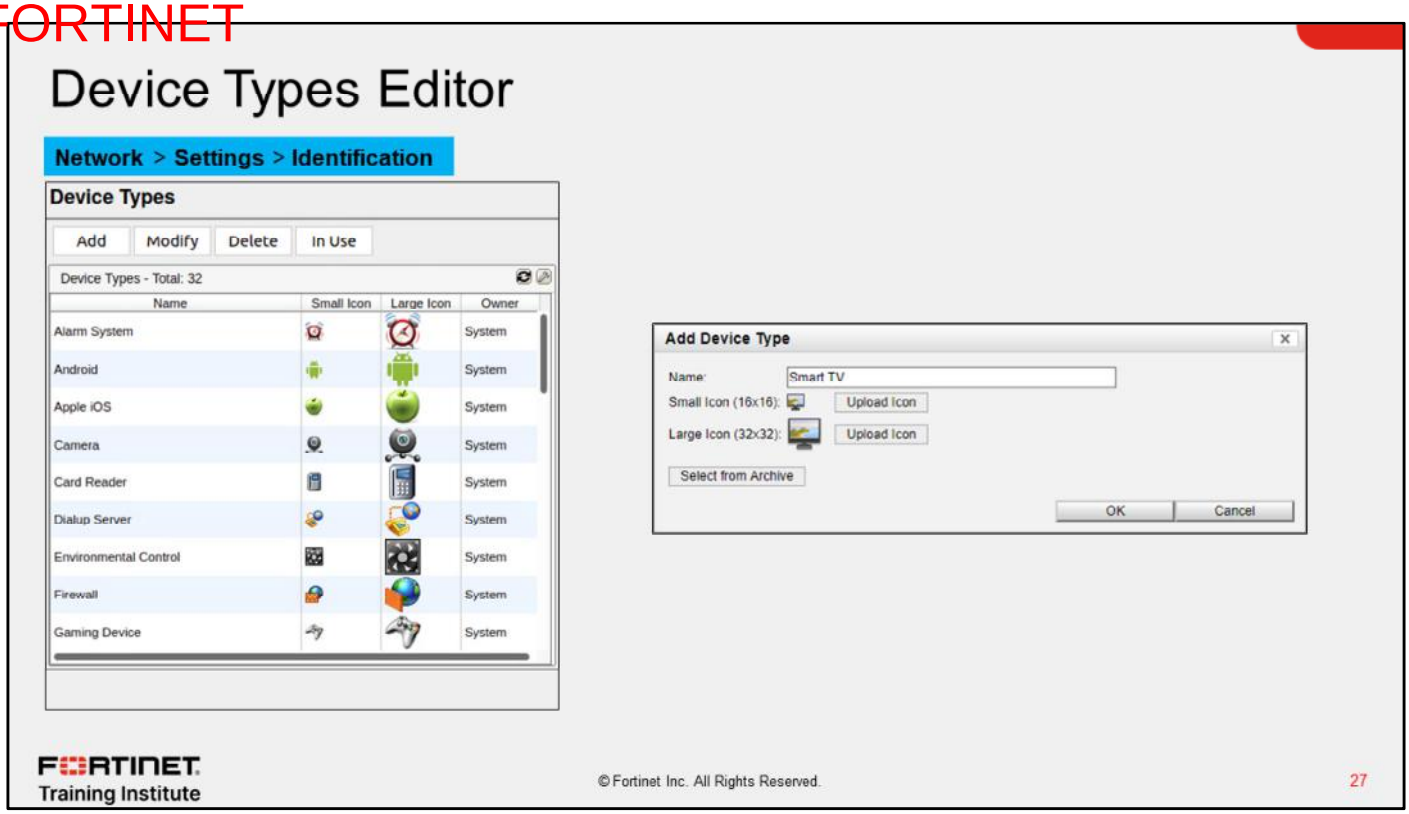
DO NOT REPRINT
© FORTINET
Brave-dumps.com



When a device matches a profiling rule, the device appears in the **Users & Hosts** > **Profiled Devices** view. This view displays the device name, profiling rule that was matched, type of device it is or will be registered as, role assignment, IP address and physical address, location, and several other pieces information. If the rule was configured to automatically register the device, there is nothing more you need to do. It appears as registered in the **Registered** column. If the rule was set for manual registration, it also appears in the **Registered** column. However, an administrative user or sponsor needs to select the device in the **Profiled Devices** view, and click **Register as Device** to complete the process.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



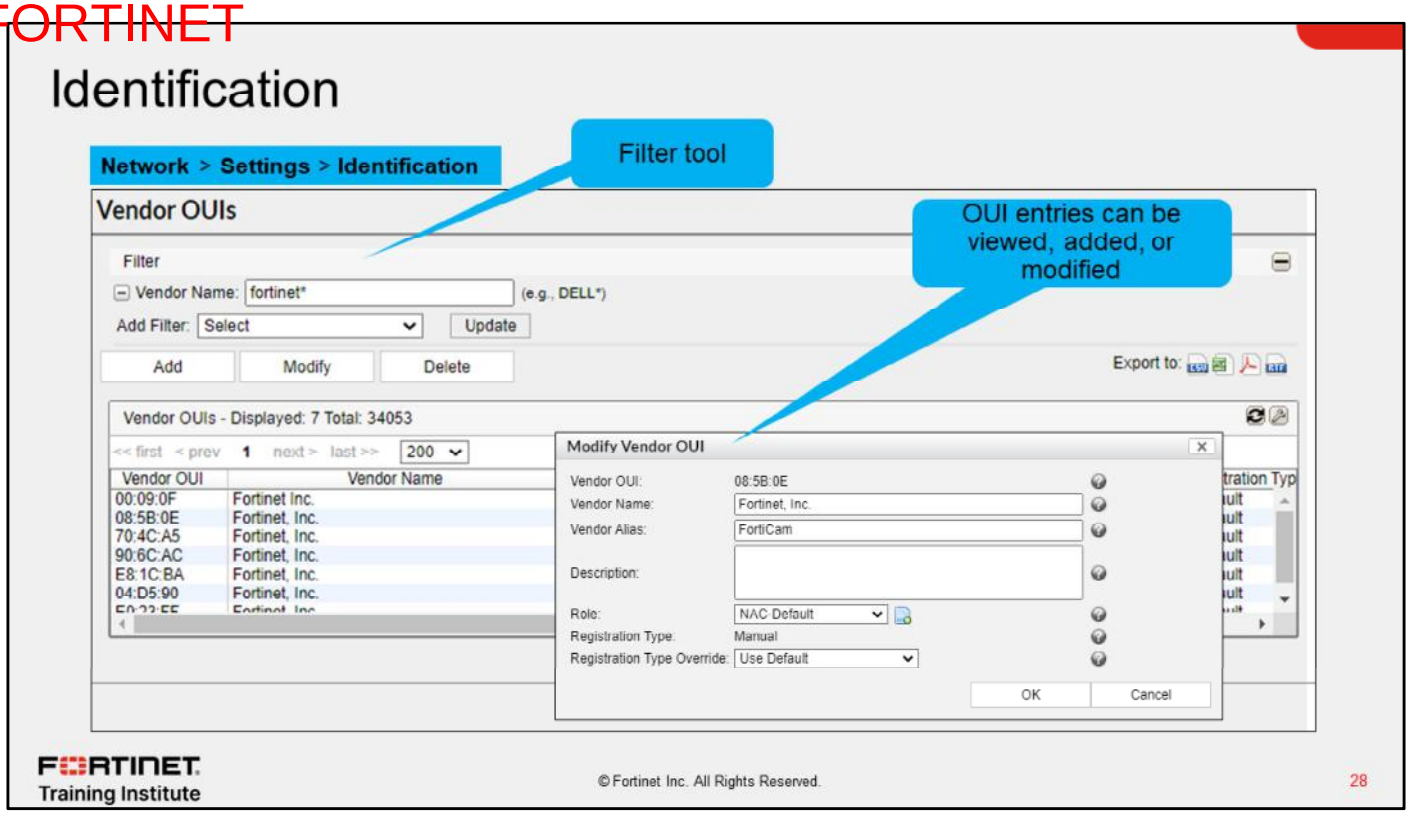
Access the **Device Types** editor by clicking **Network** > **Settings** and expanding the **Identification** folder.

An important part of classifying devices is to accurately portray the many diverse endpoints that connect to an environment. Device type is commonly used for running inventory reports or creating security policies. There is a default set of pre-existing device types that you can use during the classification process. You can view the list from the **System Settings** menu, within the **Identification** folder. Use the **Device Types** editor to modify or create new device types. This helps you to customize device types to fit any environment.

To create a new device, click the **Add** button. Give the device type a name. Then upload icons of the appropriate size, or select a small and large icon pair from the archive list of almost 2,000 icon pairs. After you create a new device type it appears in the list and works exactly like the default device types.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Access the vendor OUIs view by clicking **Network** > **Settings** and expanding the **Identification** folder. From this view you can locate specific vendor OUIs using the filter, and you can modify specific attributes of the selected OUI. To configure an alias, select an entry and click **Modify**. You learned about alias attributes when you learned about device profiling configurations.

You can set the alias in the **Vendor Alias** field. You can also make configuration changes for default role assignment and registration type. The default role assignment is the value assigned if the device is registered using a portal page. The registration type is a default device type association and is used with the vendor OUI method of a device profiling rule. You can override the registration type when the type set by the FortiNAC device does not reflect what is seen in a specific environment.

Vendor OUI information is kept up-to-date by the auto-definition synchronizer scheduled task that exists in the scheduler tool.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When more than one profiling method is selected for a single rule, what is the logic between those methods?
   - ✓ A. AND
   - B. OR

2. What can you do if there are no FortiNAC device types that accurately classify a profiled device?
   - A. Use a generic device type.
   - ✓ B. Create a new device type.

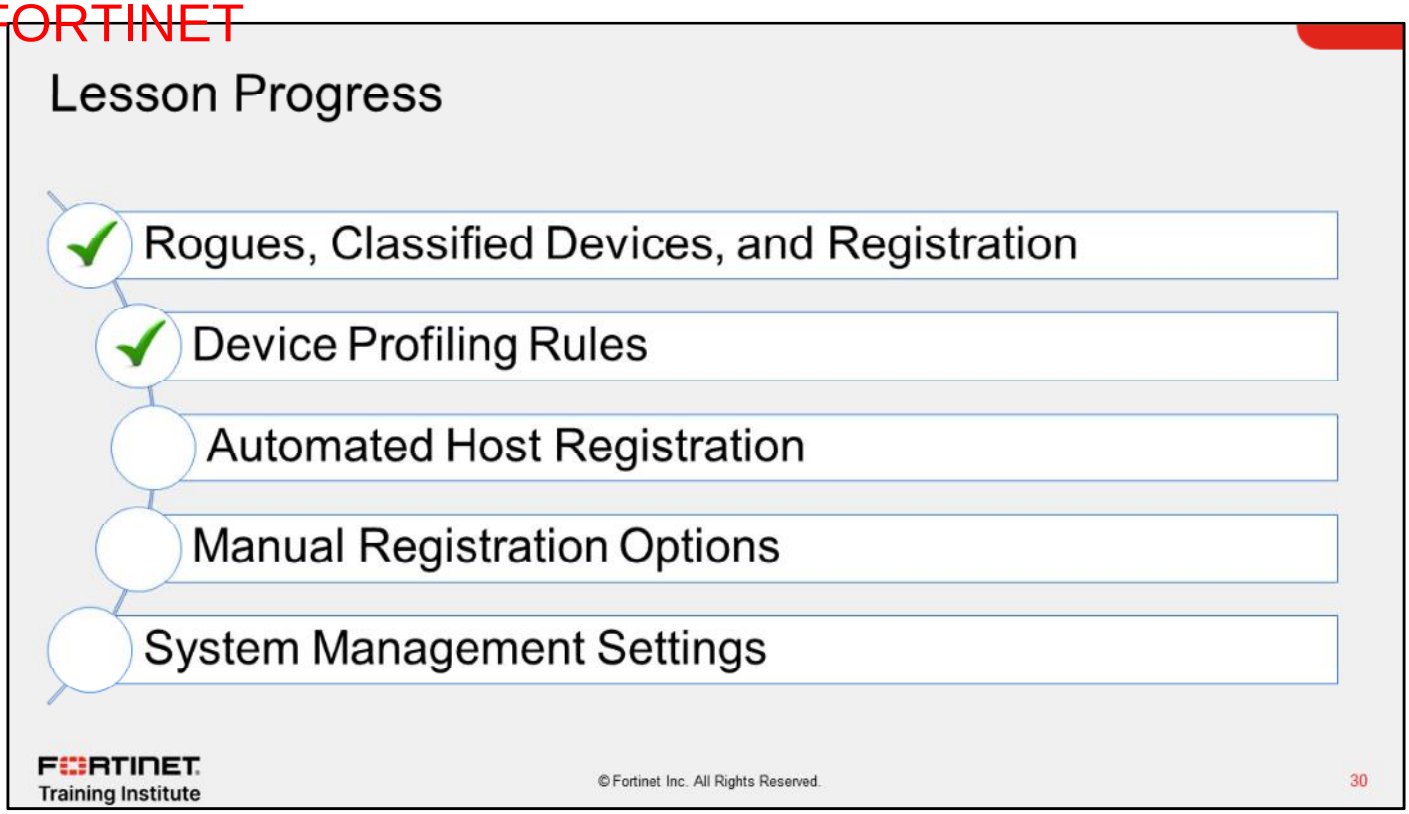
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

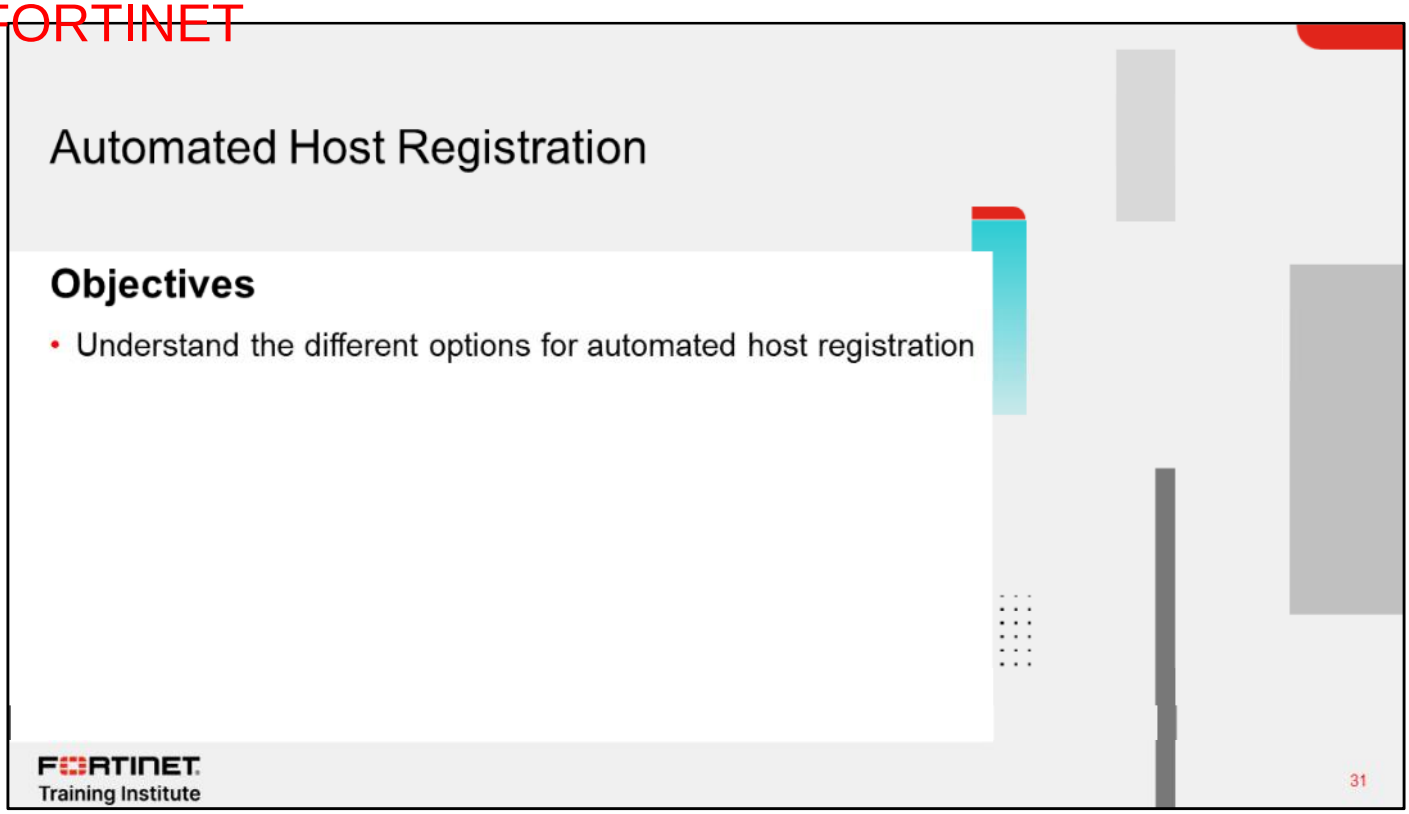


Good job! You now understand how to create and use device profiling rules.

Now, you will learn about automated host registration options to assist in the classification of rogue devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

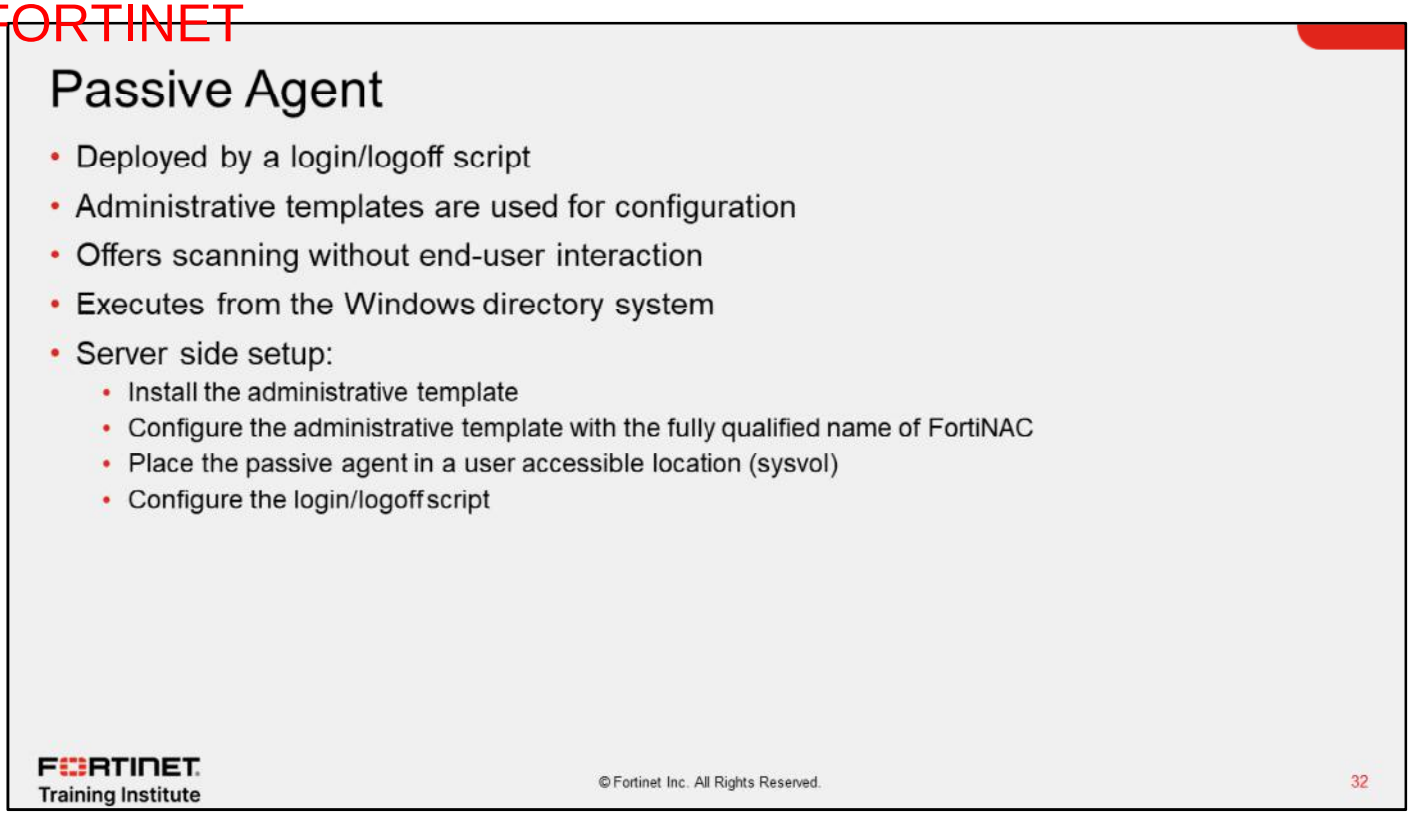


After completing this section you should be able to achieve the objective shown on this slide.

By understanding the ways that you can use different tools to securely register endpoints, you will be able to use appropriate options for registration.

Vouchers & Dumps are Available | WhatsApp +201224560923

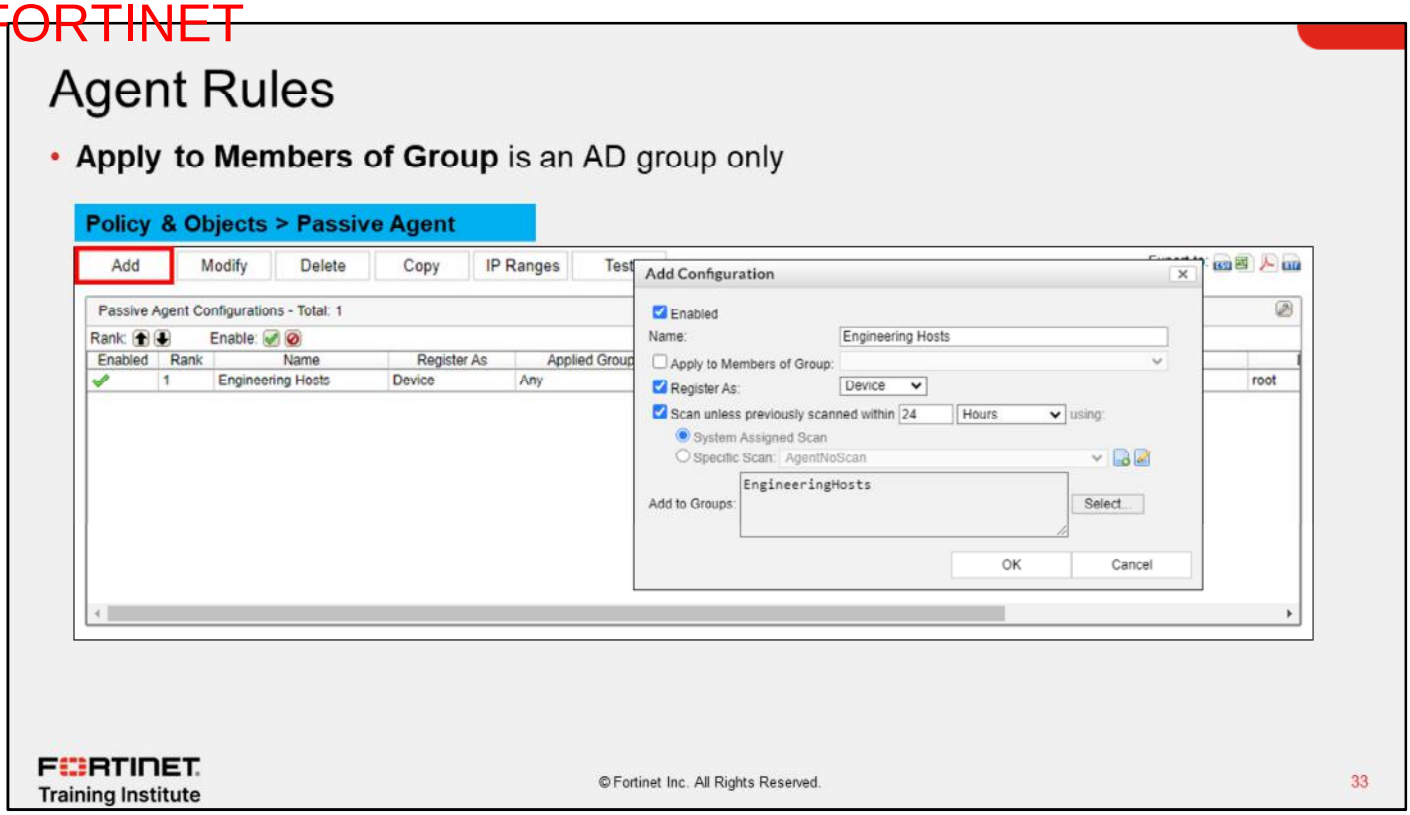
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The passive agent registers and scans end stations that are joined to a domain when a domain user logs in. You can deploy the agent using a login script and use administrative templates to configure it. The administrative templates are installed and configured on the domain controller with the fully qualified domain name of the FortiNAC device. As a result, when the agent runs, it knows where to send the results. Place the agent executable in a user accessible location, and configure the login/logoff script to execute the agent. If the end station is configured to register at login, it registers the first time and remains registered until it expires based on configurable aging timers. You can also use the passive agent to track users as they log in and out of domain machines.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Access the passive agent rules from the **Security Configuration** > **Passive Agent** view.

Passive agent registration helps you create customized configurations that register and scan hosts that are associated with network users contained in your LDAP or active directory. Scanning requires an agent, however, the agent does not need to be installed by the user. The agent is provided using an external method, such as group policy objects, and launched when the user logs in to the domain.

When a user connects to the network and logs in, FortiNAC determines the directory group to which the user belongs. Based on that group, a passive agent configuration is used. The configuration registers the user and the associated host in FortiNAC. If enabled, the agent scans the host to verify that it is in compliance with the appropriate endpoint compliance policy. You can specify the scan in the configuration, or FortiNAC can determine it, based on the user/host profile of the user or host.

You can also use a passive agent configuration to track user login and logoff on hosts with the persistent agent installed. To create a passive agent configuration that does not apply to any domain group members, leave the check box unselected. The different configurations can be ranked with the more specific ones first.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The FortiNAC persistent agent is an install and stay resident agent. There are several different types of persistent agents for use, depending on the method of deployment. The .exe, .dmg, .deb, and .rpm are normally deployed from within the captive portal environment during end station on-boarding. This enables the configuration of the agents through server communication, as they are installed. The .msi is typically deployed as part of the group policy or by some other software distribution mechanism. When an agent is deployed as part of the group policy, the administrative templates can be installed on the active directory for agent configuration. When being deployed by other means, a set of registry key entries must be deployed or configured as well.

The behavior of the agent, and the FortiNAC server it communicates with, is configured in the registry on Windows systems. Similar configurations are used on Mac systems and DNS SRV records can be used. Installation scripts can be run on Linux systems for configuring these values.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Persistent Agent (Contd)

- Communicates with FortiNAC
- Background scanning
  - No user interaction or VLAN switching unless scan failed
- System messaging
  - With queue and timers
  - By group
  - By host



FORTINET Training Institute

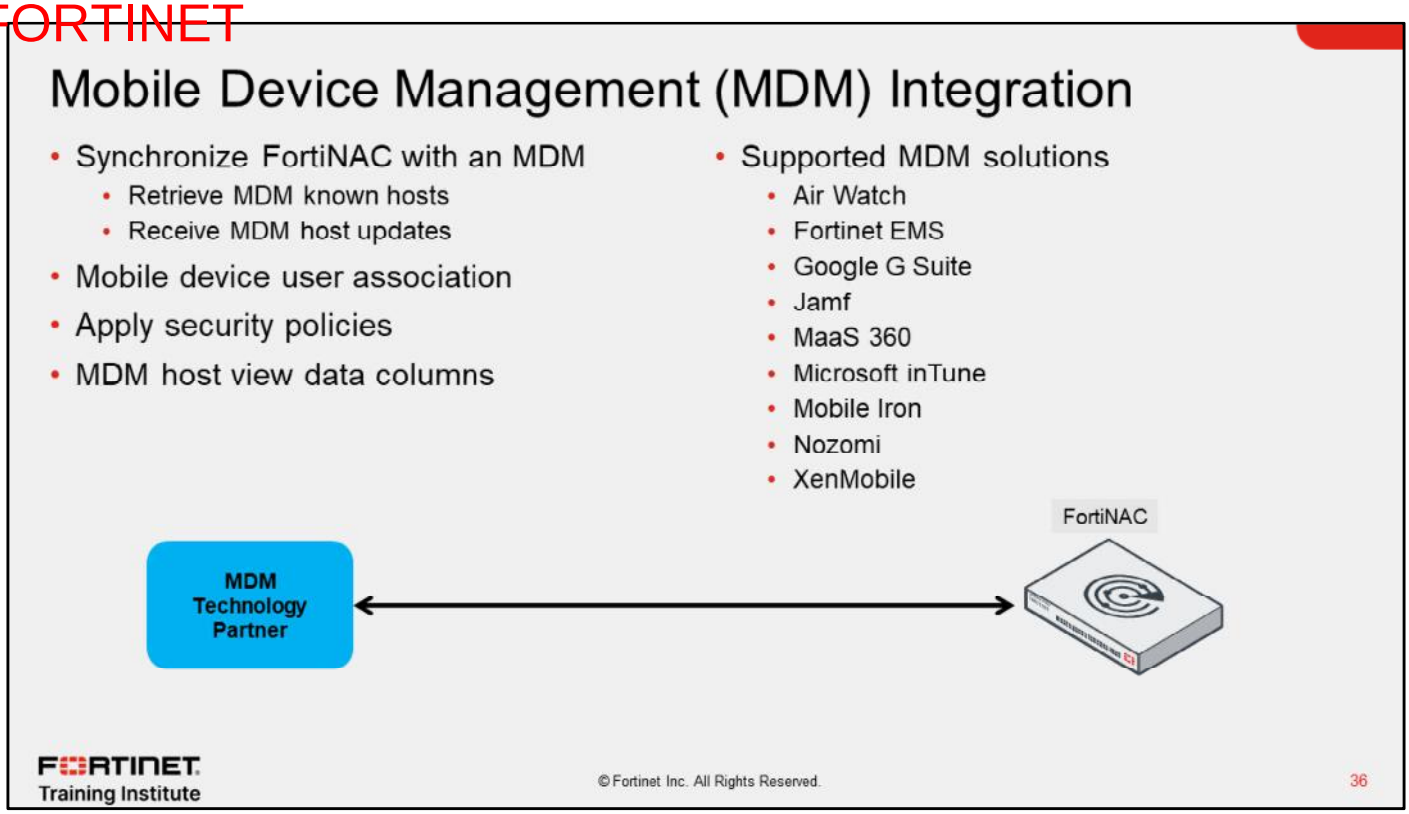
© Fortinet Inc. All Rights Reserved.

35

After the persistent agent is deployed, it initiates communication back to the FortiNAC server every 15 minutes. The persistent agent performs scheduled scans in the background that are transparent to the end user. To use system messaging, go to the **Bookmarks** menu, or you can right-click a specific host in the host view and select **Send Message**.

Vouchers & Dumps are Available | WhatsApp +201224560923

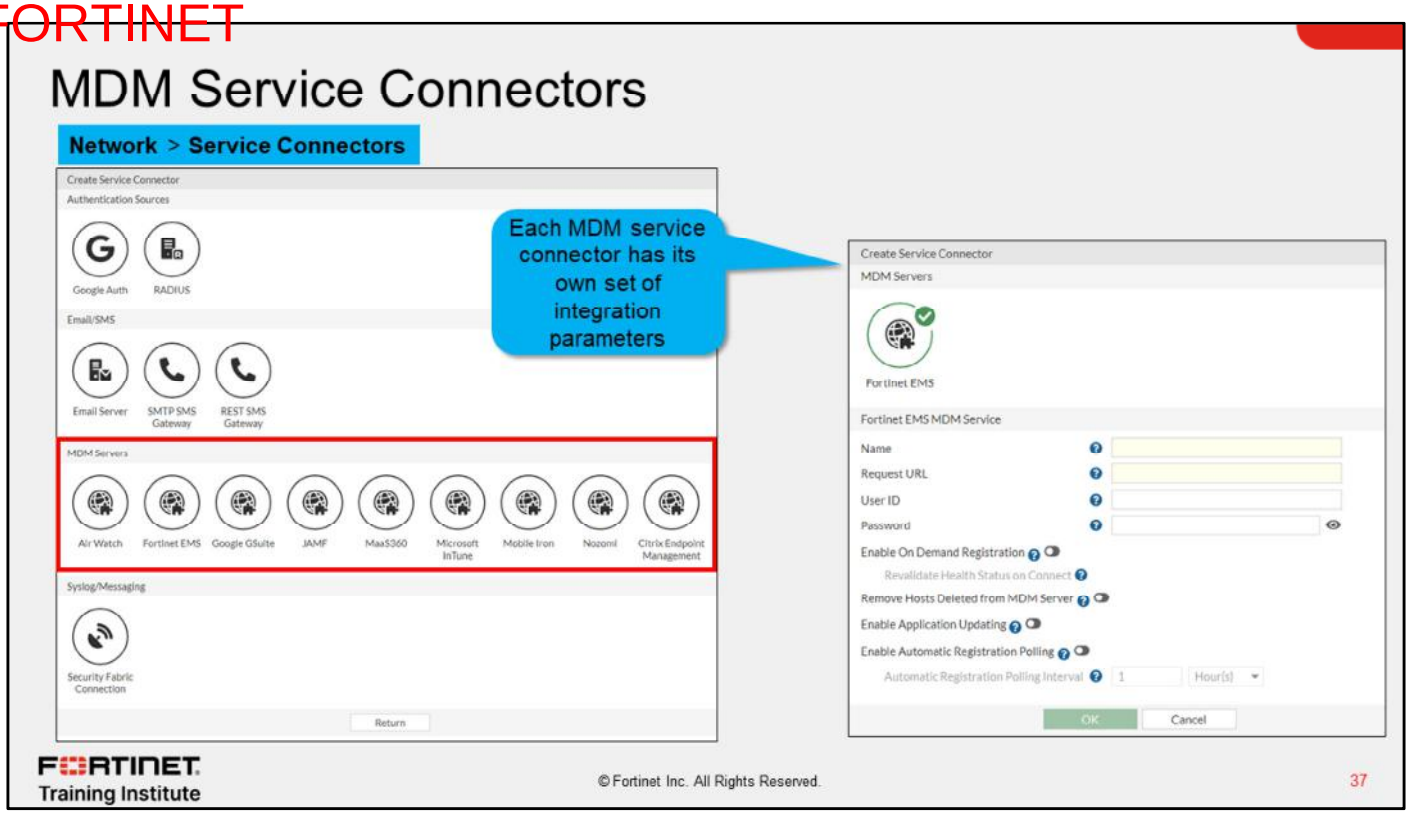
DO NOT REPRINT
© FORTINET
Brave-dumps.com



MDM services helps you configure the connection or integration between FortiNAC and an MDM system. The FortiNAC device and the MDM system work together to share data through an API to secure the network. FortiNAC leverages the data in the MDM database and registers hosts using that data as they connect to the network. You can pull down device application inventories from some MDMs to enhance the visibility of connecting mobile devices. You can use email addresses to make user associations between existing users and newly added devices. You can also leverage security policies by matching on attributes that are passed down from the MDM, and see additional host information that is available within the host view.
The supported vendors are: AirWatch, FortiClient EMS, Google G Suite, Jamf, MaaS360, Microsoft In Tune, Mobile Iron, Nozomi, and XenMobile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

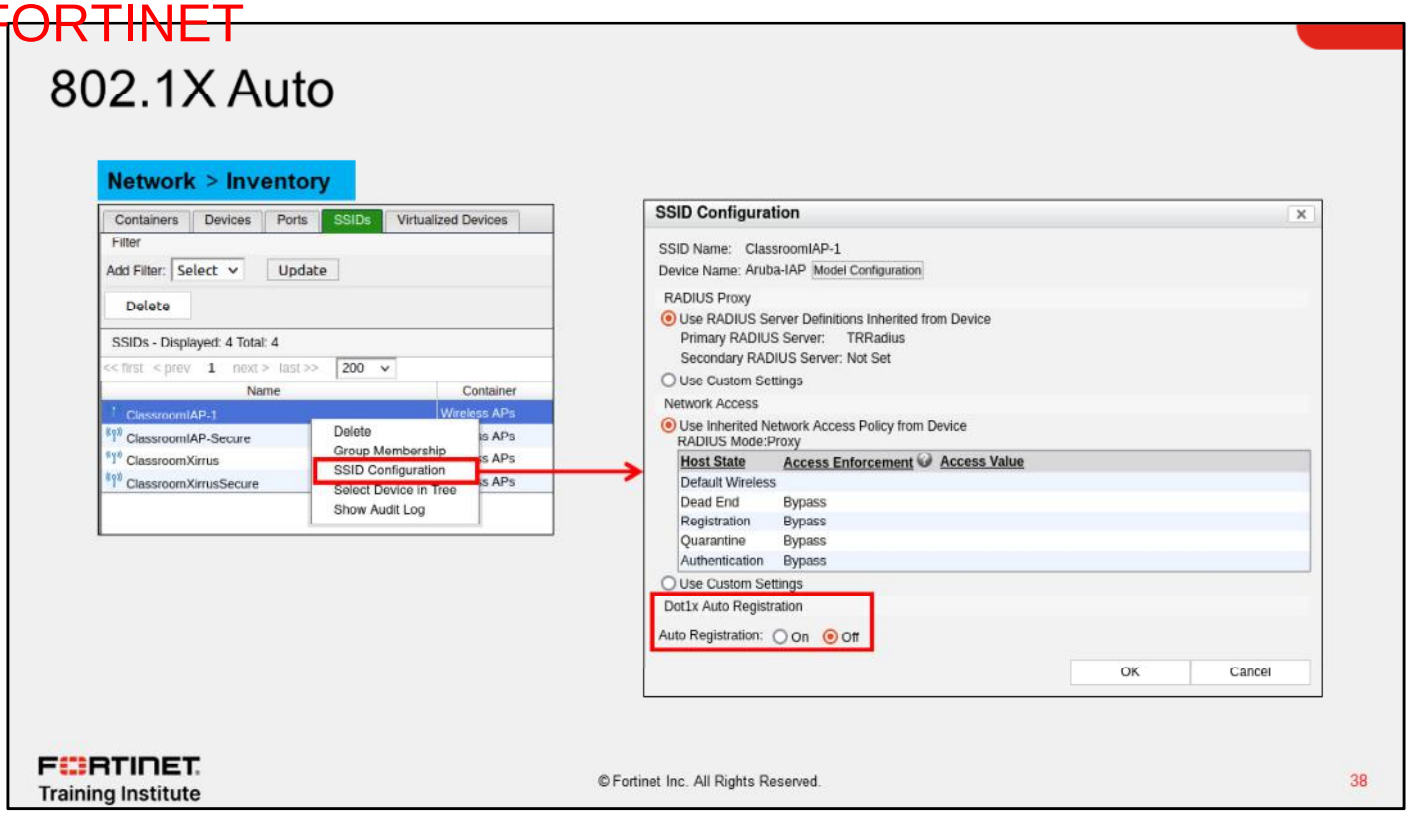


The MDM integration is performed from the **Network** > **Service Connectors** view. Click **Create New** to create a new MDM integration. Select the vendor from the **MDM Servers** list, name the integration and fill in the appropriate communication parameters for your MDM.
Use the appropriate behavioral options for the integration:

- **Enable On Demand Registration** triggers FortiNAC to query the MDM whenever a host reaches the captive portal for onboarding. If the host is found in the MDM, it is registered using the data obtained from the MDM.
- **Revalidate Health Status on Connect** prompts FortiNAC to query the MDM for host compliance whenever hosts connect to the network. This is disabled by default, and can generate a lot of overhead for the MDM.
- **Remove Hosts Deleted from the MDM Server** prompts FortiNAC to remove hosts from its database, if they have been deleted from the MDM server.
- **Enable Application Updating** prompts FortiNAC to retrieve and store the application inventory for hosts that are in the FortiNAC database.
- **Enable Automatic Registration Polling** sets the time interval for MDM server polling by FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can configure FortiNAC to automatically register a host based upon the user's 802.1X authentication with the RADIUS. You enable this feature in the **SSID Configuration** view of the controller or access point model in **Network** > **Inventory**. Once the user credentials have been successfully validated, the host will be registered to the user, and the user will appear as logged on to the host.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. If a mobile device is added to the FortiNAC database as the result of an MDM integration, how could you associate it with an existing user record on FortiNAC?
   - A. User ID
   - ✓ B. User email address

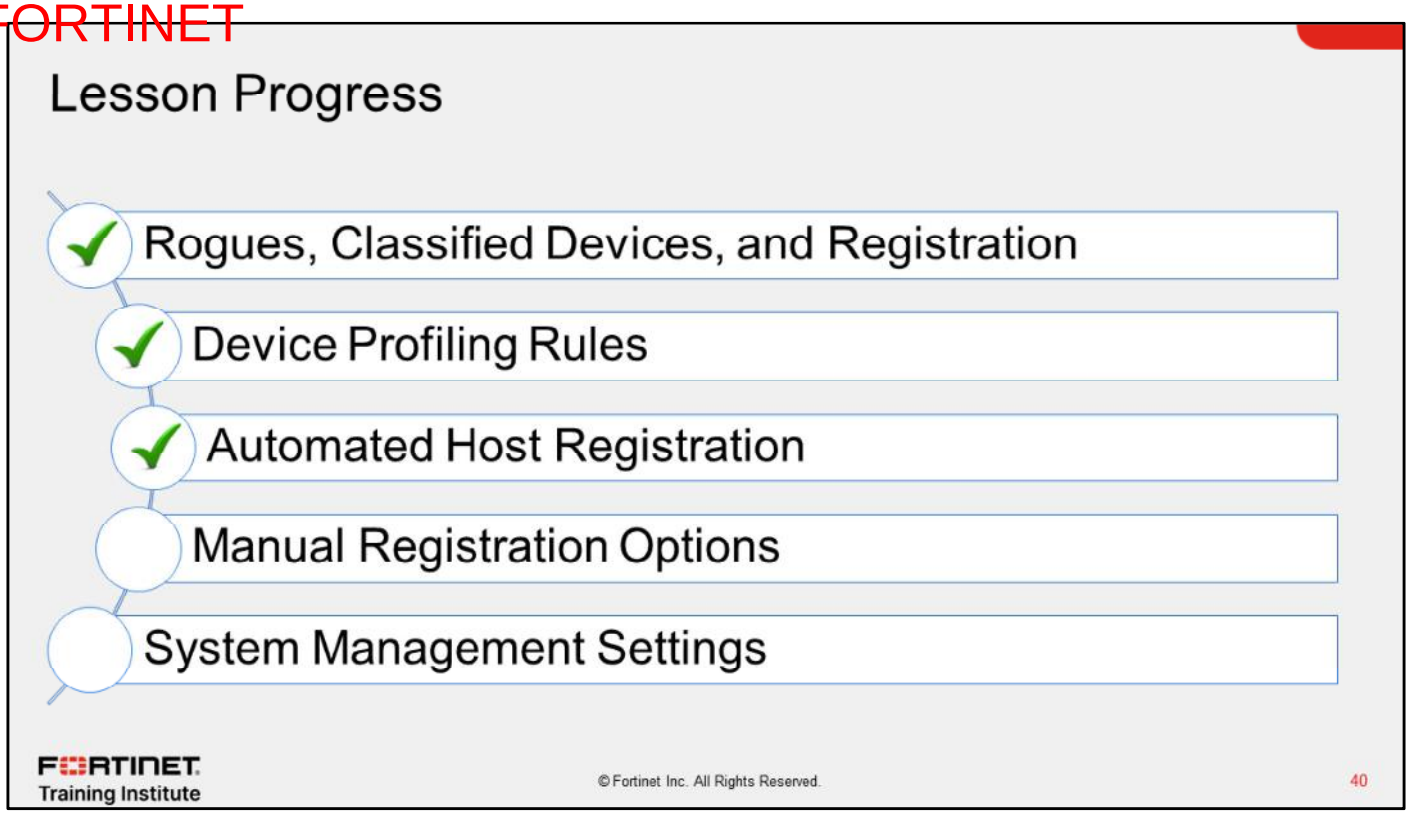
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

39

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

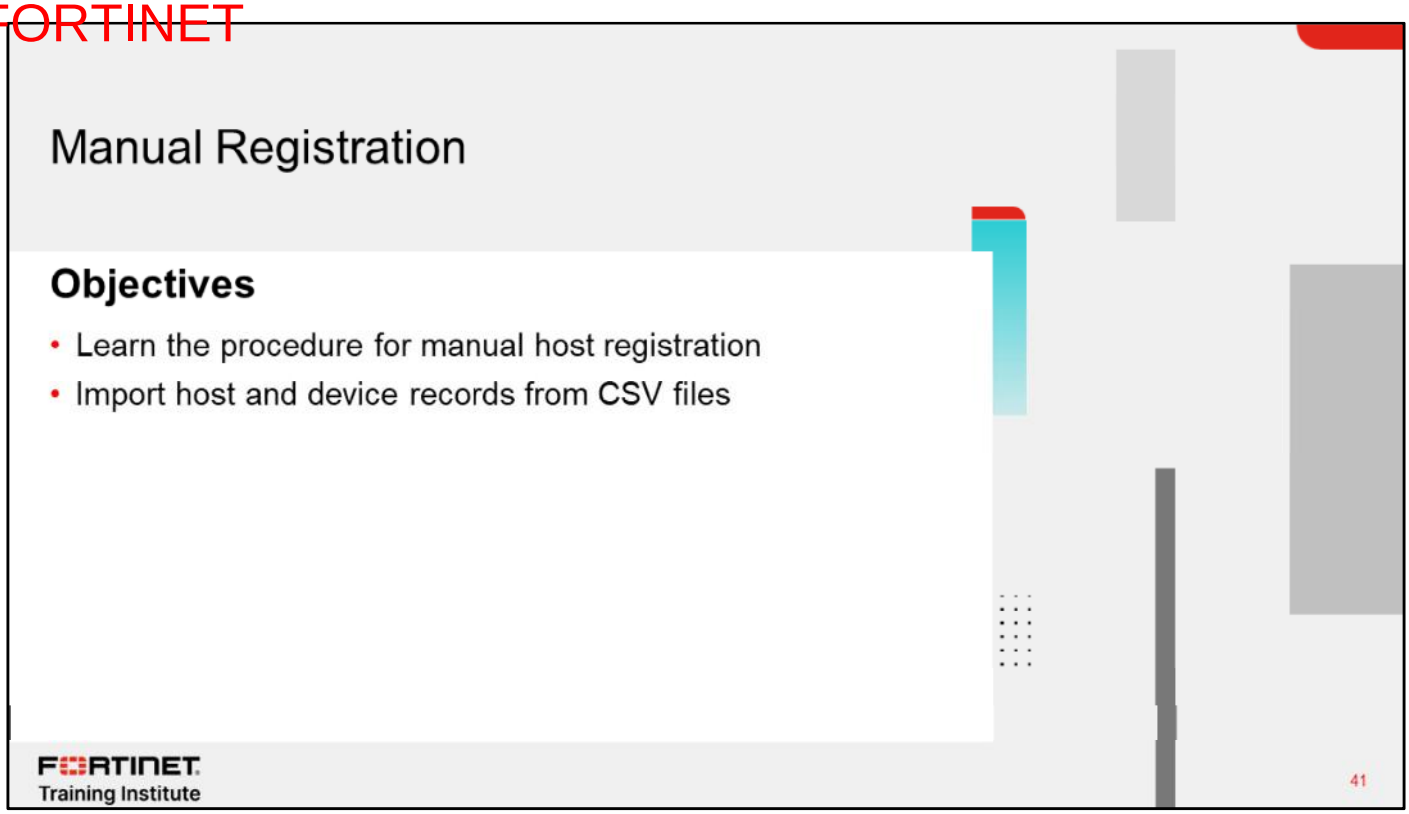


Good job! You now understand how you can use MDM integration to define trust and enhance visibility.

Now, you will learn how you can use manual registration to assign trust to endpoints.

Vouchers & Dumps are Available | WhatsApp +201224560923

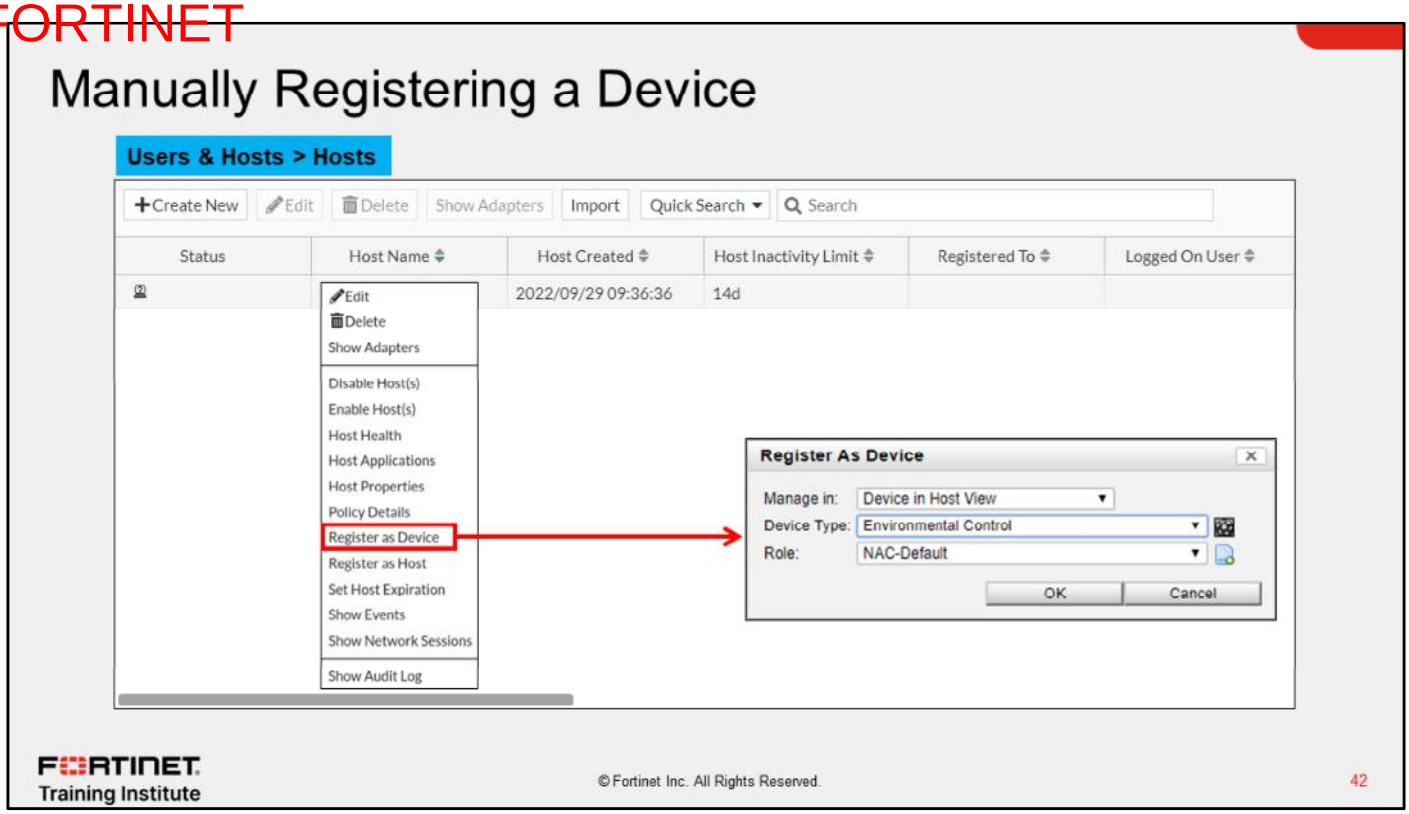
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objectives shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

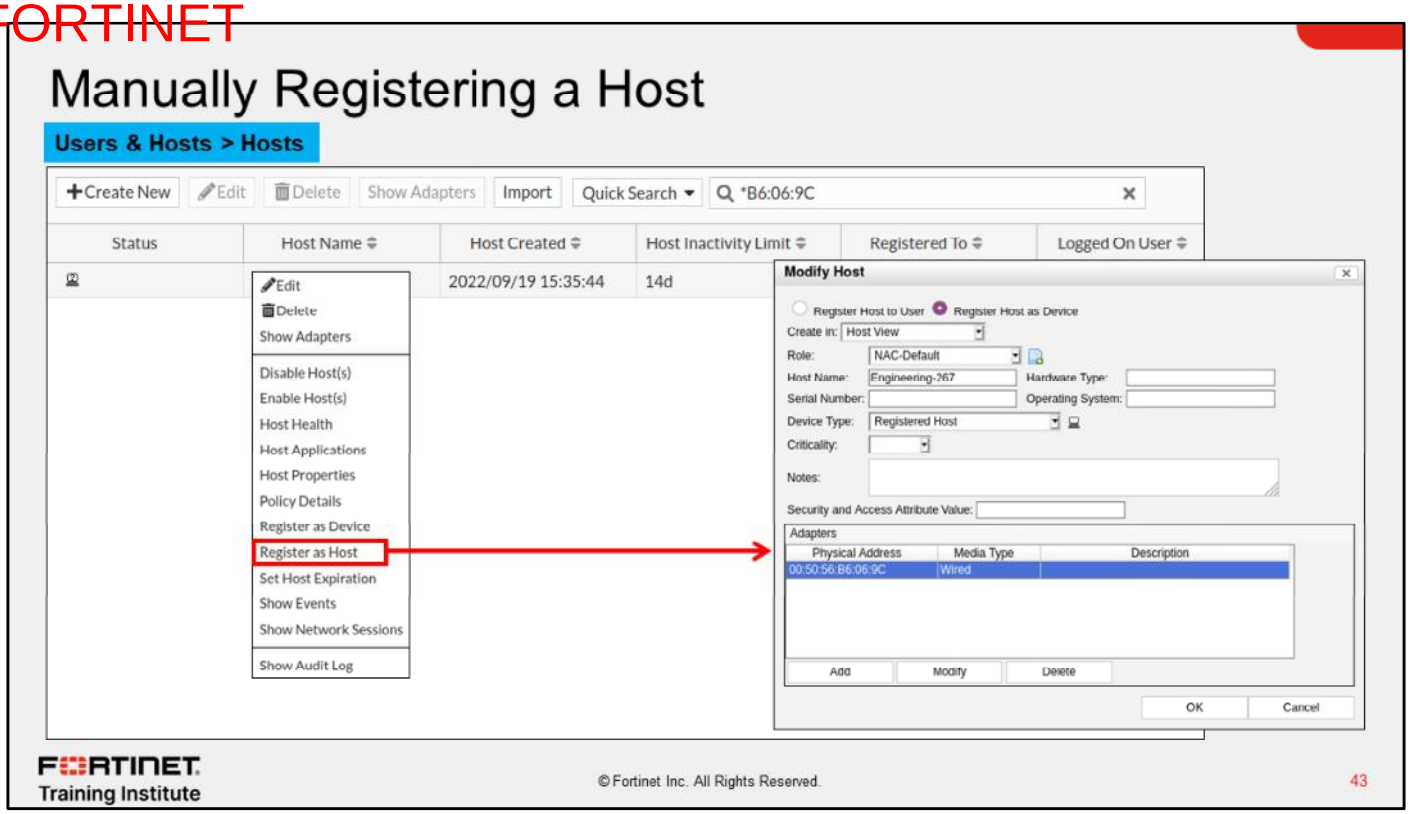


To manually register a host as a device, locate the host in the **Users & Hosts** > **Hosts** view, and then select the option from the right-click menu. The **Manage in** drop-down list helps the administrative user decide how the registered device is viewed and managed after registration.

- The **Device in Host View** option will model the device as a host, and it will appear and be managed in the host view.
- The **Device in Topology** view will display the host in the topology tree. Note that security policies are not applied to devices modeled using the **Device in Topology** option.
- The **Device in Host View and Topology** option will display the device in both locations.
- The **Device Type** drop-down list is used to manually assign the device type and will include all default and administratively created device types.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



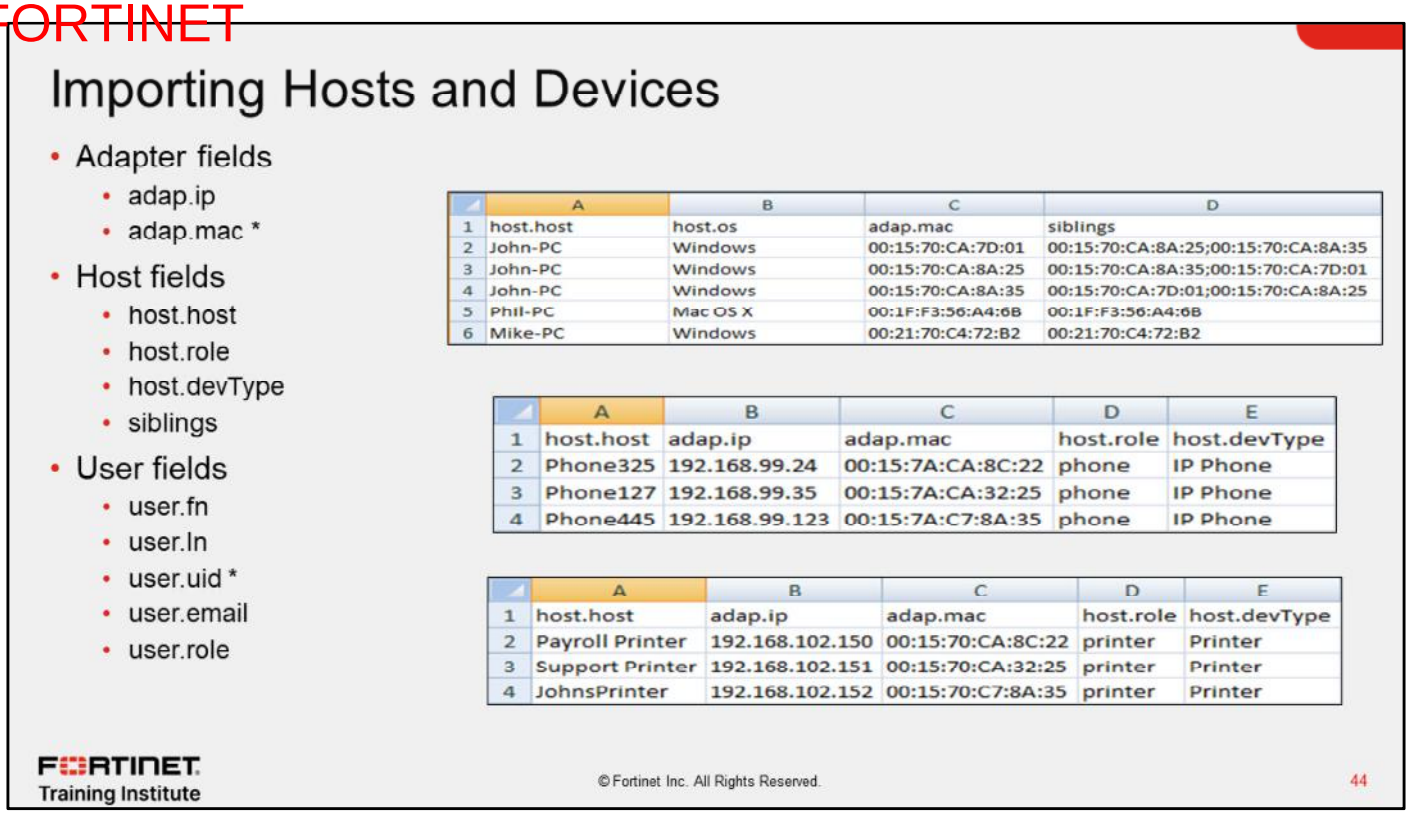
Another option for manual registration is the **Register as Host** option, which is available from the right-click menu.

Use the filter to locate the device you want to register, right-click the device, and select **Register as Host**. **Register Host to User** is the default option and should be selected if the host and a user record need to have a permanent association. This is normally the case in BYOD situations, such as guests and contractors.

The **Register Host as Device** option does not make a permanent association between a particular user and the host, and this is typically used for corporate assets or IoT devices. This is equivalent to the **Device in Host View** option from the previous slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To add hosts, users, devices, or IP phones, create a comma-separated value (CSV) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records.

You can mix the types of records you are importing. For example, you can import hosts, users, and IP Phones in the same file as long as you have all of the appropriate fields in the header row.

The first row in the file is a header row and must contain a comma-separated list of the database field names that are included in the import file. The order of the fields does not matter. For example, to import hosts and their corresponding adapters, the header row could have the following columns:
adap.mac, **adap.ip**, **host.owner**, **host.host**, and **siblings**.

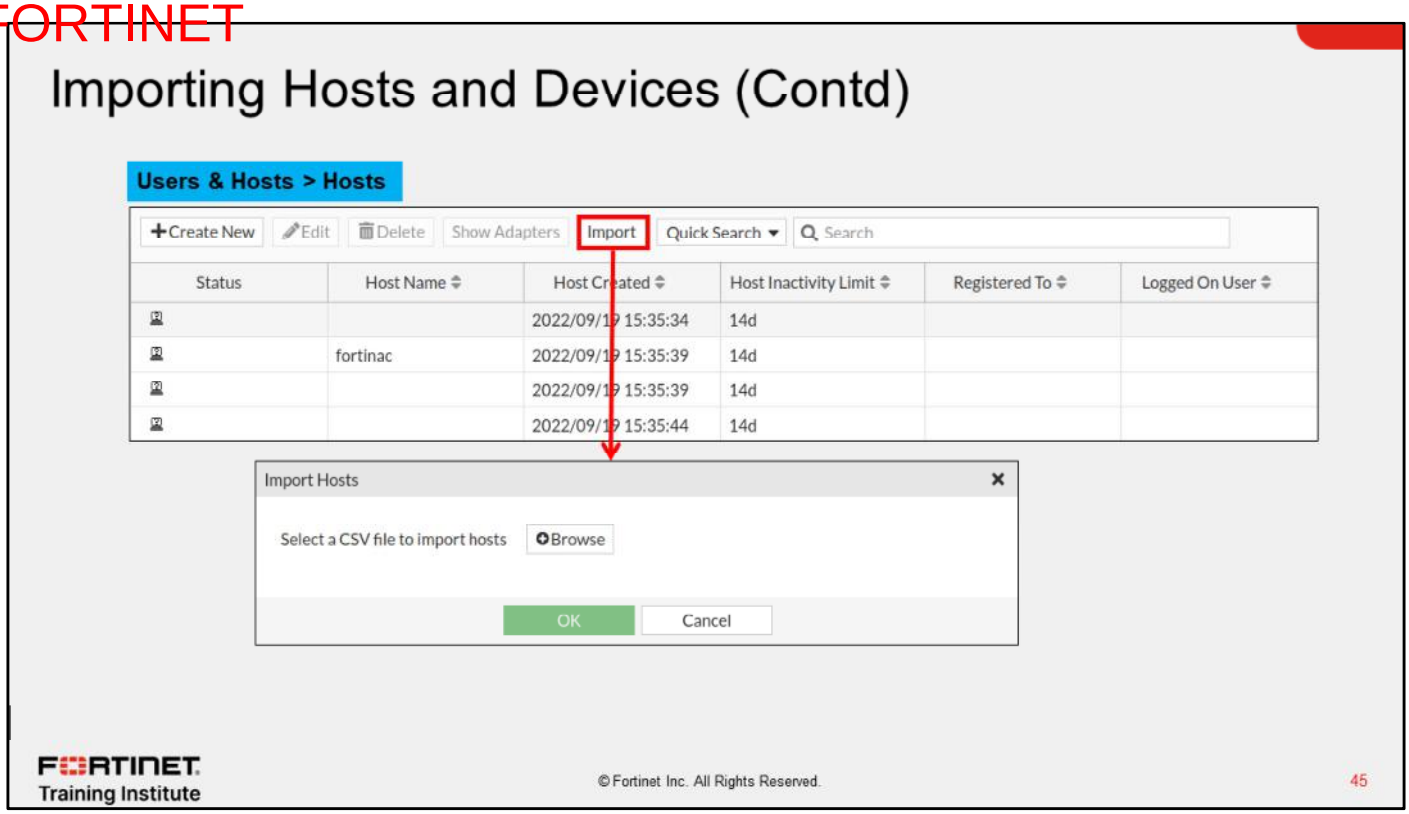
There are a couple required columns, depending on what is being imported.
For hosts, the **adap.mac** column is required, and for users, the **user.uid** column is required.

Note that fields are case sensitive, and if you import something that already exists in the database, the existing record is updated with the new data from the import.

The fields displayed on this slide are some of the most commonly used. A more complete list exists in the help.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you create a CSV file with all the required fields and entries, you can import it into the database from the **Users & Hosts** > **Hosts** view by clicking **Import** and then clicking **Choose File**. Navigate to and choose the CSV file and click **OK**. The entries will appear in an **Import Results** window. Click **OK** to close the window. The imported records will now be searchable within the different visibility views.

Note that the **Import** option is only visible after the **Legacy View Architecture** option is enabled under **System** > **Feature Visibility**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

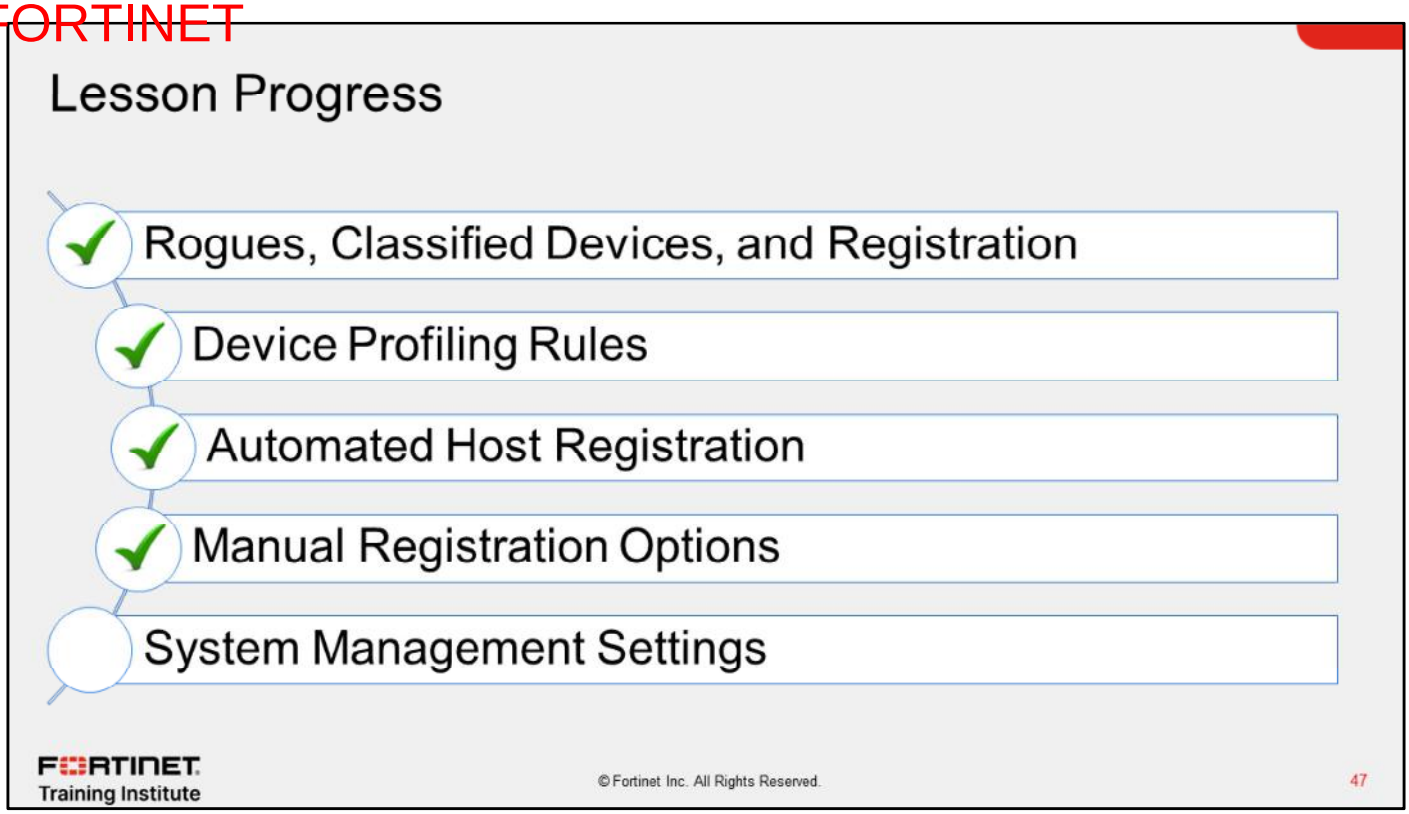
Knowledge Check

1. When importing host records, which field is mandatory?
   - A. adap.ip
   - ✓ B. adap.mac

FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

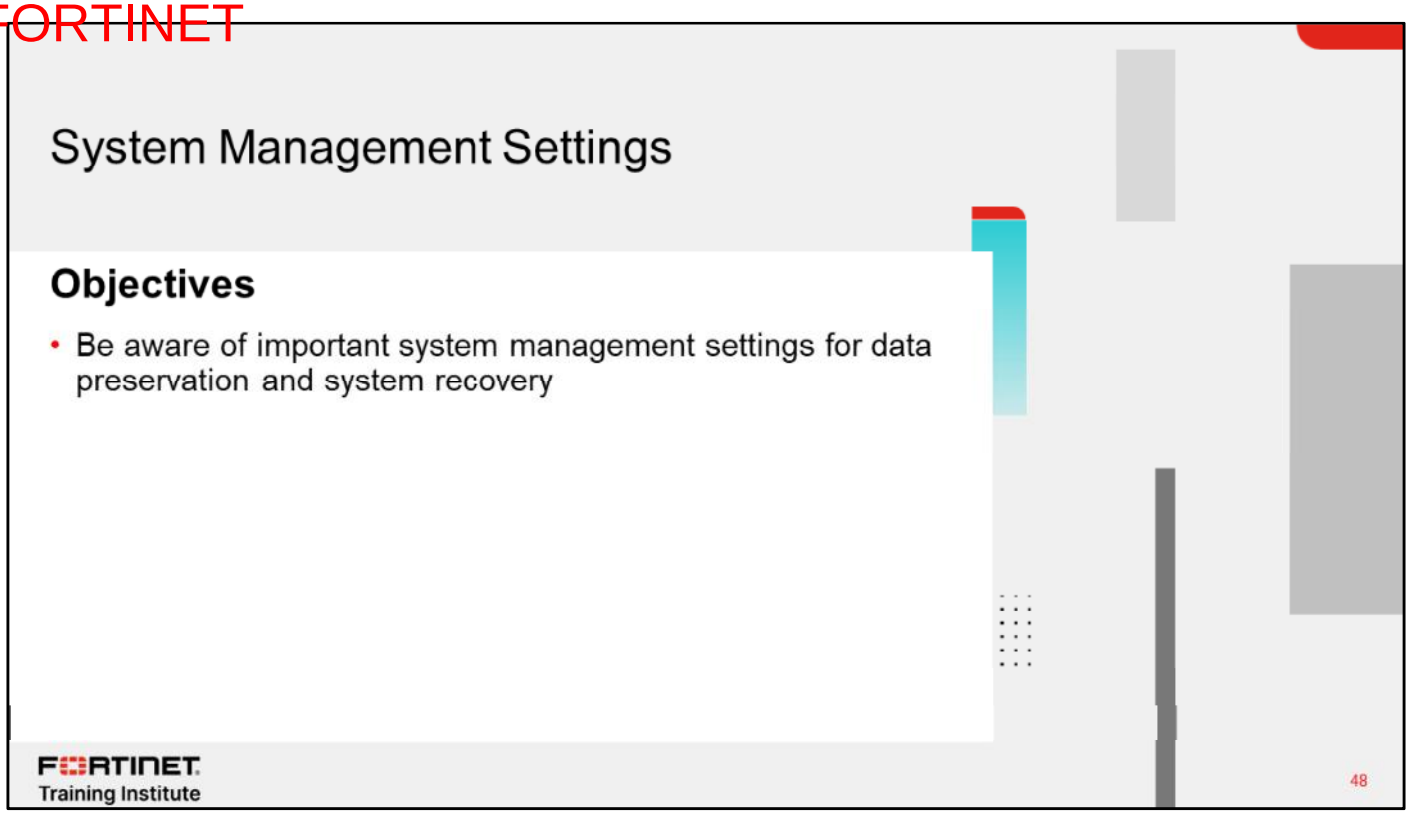


Good job! You now understand how you can use importing to classify devices.

Now, you will learn about the system management settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

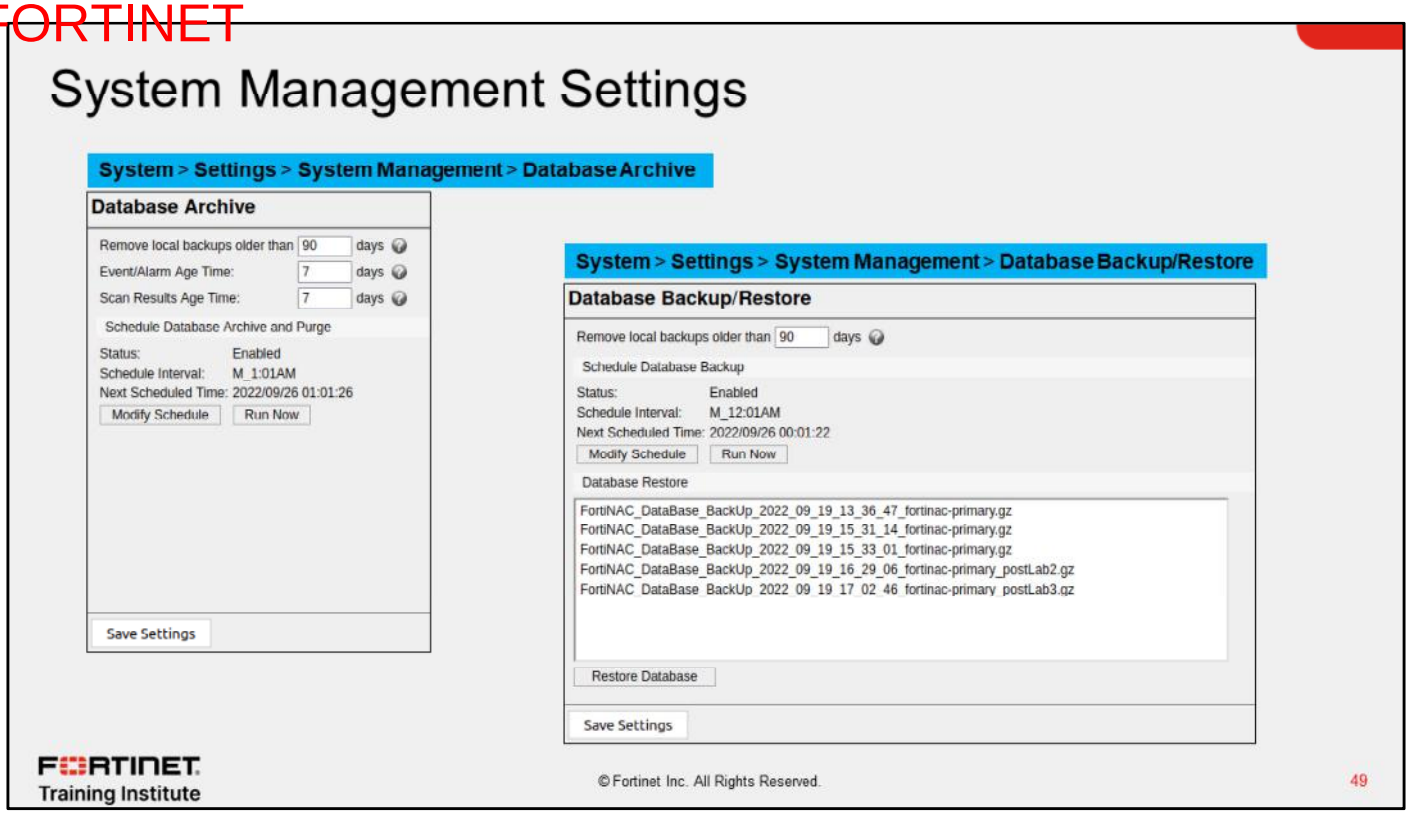
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section, you should be able to achieve the objective shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The system management settings are located in the **System** > **Settings** view. The individual settings pages are contained in the **System Management** folder. The first settings are for database archive parameters. These settings help preserve disk space and help specific administrative views to load more quickly. This is achieved by removing the data that is stored for the indicated views from the database and archiving it to local files.

The first option sets how long the FortiNAC device will keep the local copy of the archived data. The default is 90 days.
The next three options define at what age the data is removed from those views and archived. The listed views are: connections, events, alarms, and scan results. They tend to fill very quickly with entries. If those entries aren't removed periodically, the views may take a long time to load.

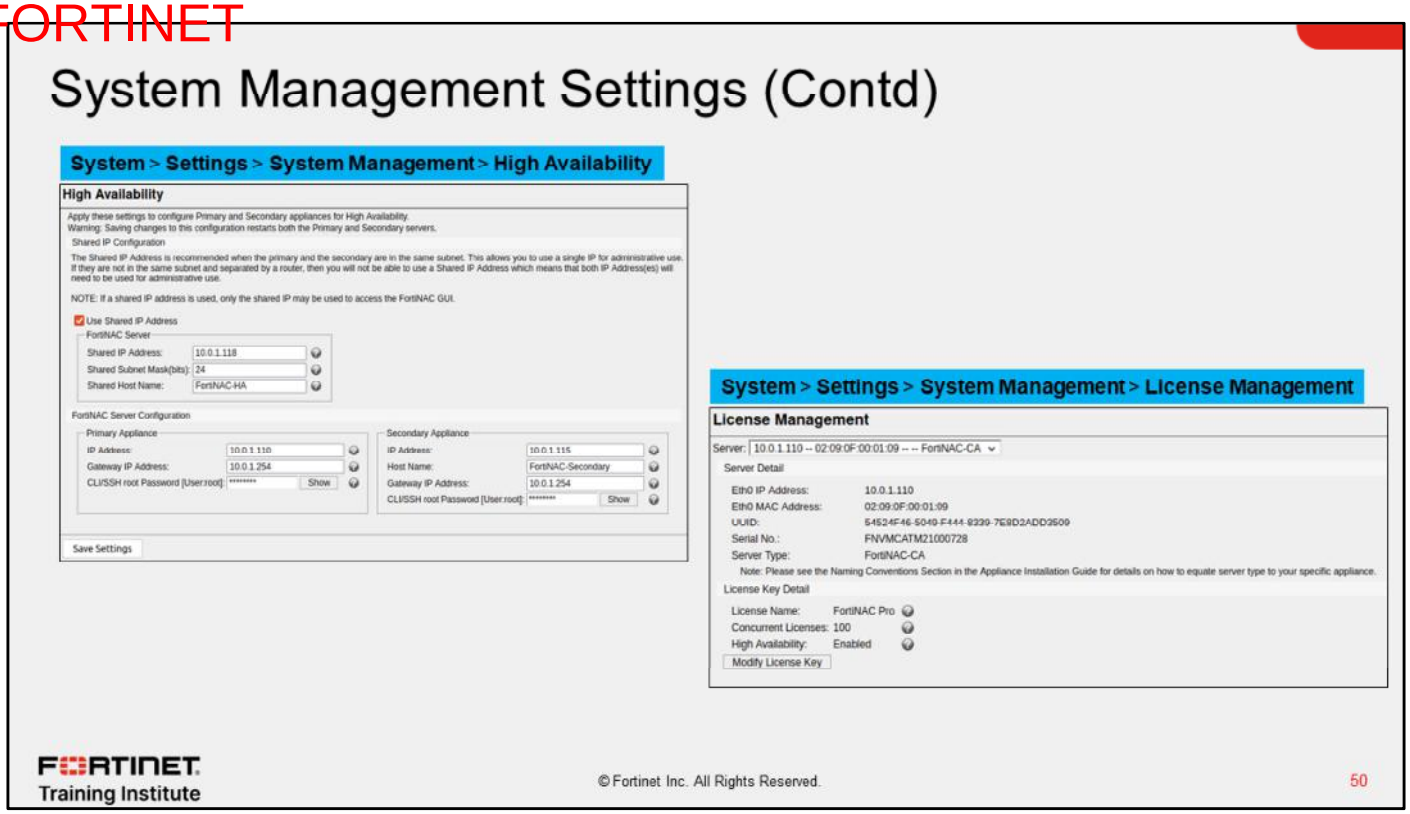
The **Schedule Database Archive** and **Purge** settings help an administrator perform the archive manually (use the **Run Now** button) or modify the scheduled interval (use the **Modify Schedule** button). Modifying the schedule will update the scheduled entry in the scheduler tool for the **Database Archive** and **Purge** action.

The **Database Backup/Restore** settings window is where you can define the following:
- Length of time that local backup copies of the database are kept
- The interval by which the database is backed up

This is also where existing copies of database backups are restored. When a backup copy of the database is restored, a current backup is made automatically.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **High Availability** settings view is for the configuration of FortiNAC high availability (HA) installation settings. You can configure high availability deployments in a Layer 2 manner using a shared IP address with both the primary and the secondary system on the same subnet. You can also configure an HA deployment in a Layer 3 configuration whereby the two systems are separated by a router. The Layer 2 option allows for management to be performed using a single interface address, whereas the Layer 3 option uses two different interface addresses: one for the primary, and one for the secondary. The secondary interface is available for administrator access only after a failover.

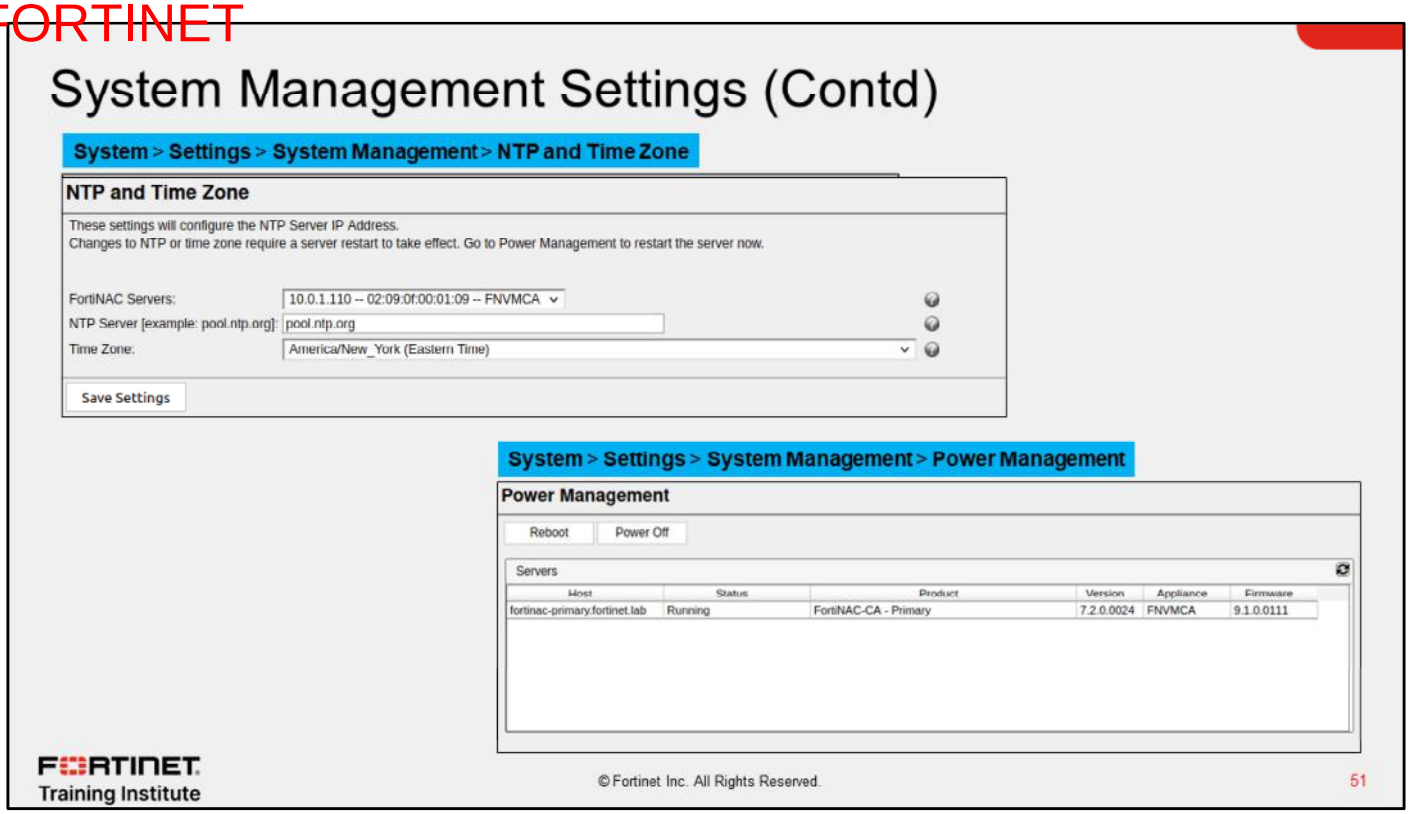
The **License Management** view displays the following information about the FortiNAC server:

- Eth0 IP address
- Eth0 MAC address
- UUID
- Serial number
- Server type

The **License Key Detail** section displays the license name, such as **Fortinet Base**, **Plus**, or **Pro**. It also displays the number of concurrent licenses and any additional licensed features. Click **Modify License Key** to install a new license.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

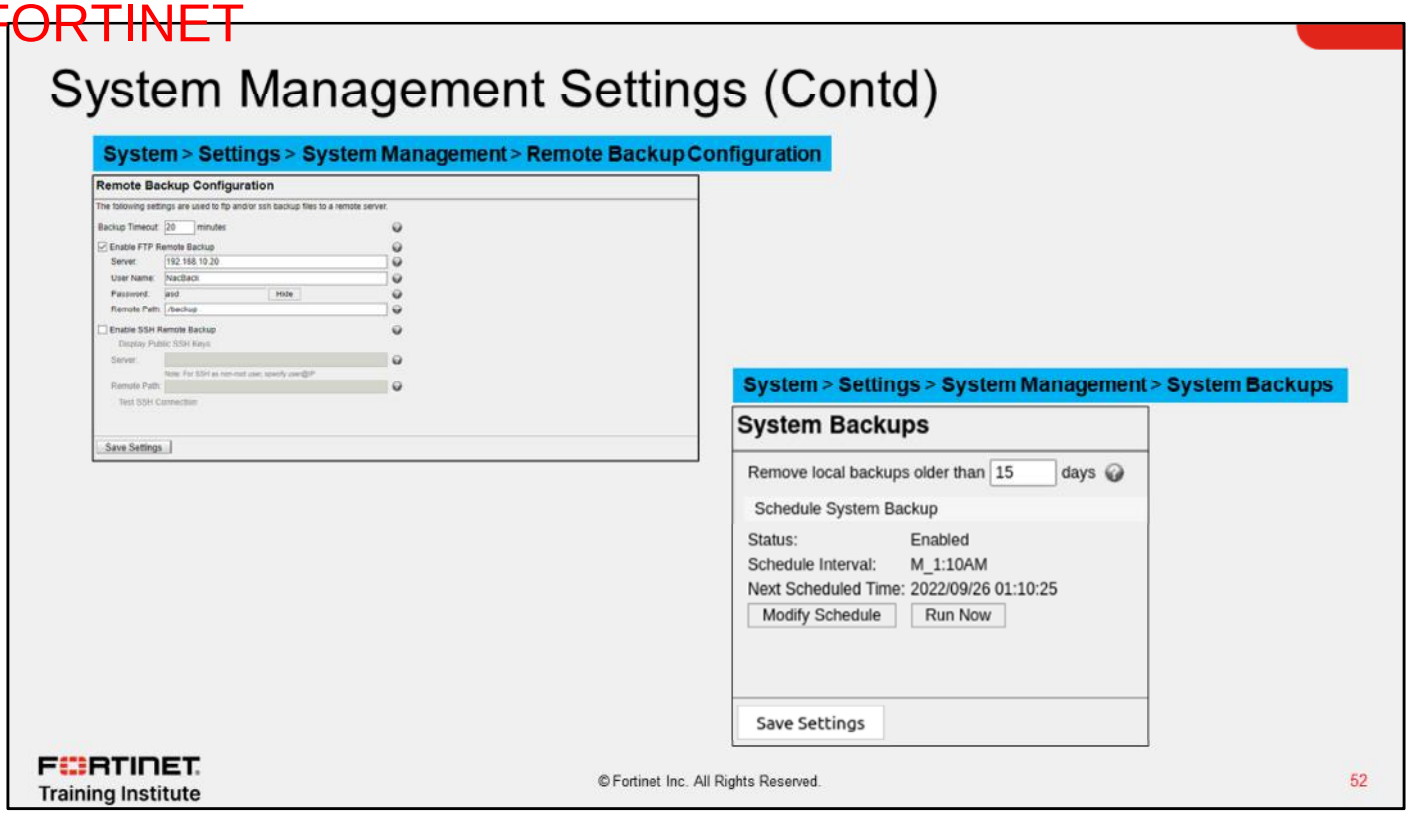


The **NTP and Time Zone** settings view is where you can configure the NTP server and time zone for each appliance, depending on the deployment. If you have a control server and an application server pair, both servers appear in the list. In an HA environment, this includes up to four servers, two control servers, and two application servers.

Use the **Power Management** view settings to properly reboot or power off the appliance.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



An extremely important part of data preservation is to keep important data backed up on remote systems. By default, the FortiNAC device backs up the database and other important configuration files locally. The **Remote Backup Configuration** window helps you set up a remote system or systems. Using FTP or SSH, the FortiNAC device transfers a copy of the backed-up data each time the database or system backup tasks are run.

Use the **System Backups** configuration view to set the backup frequency of system information that is not included in the database set. This will update the **System Backup Action** task in the scheduler tool.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

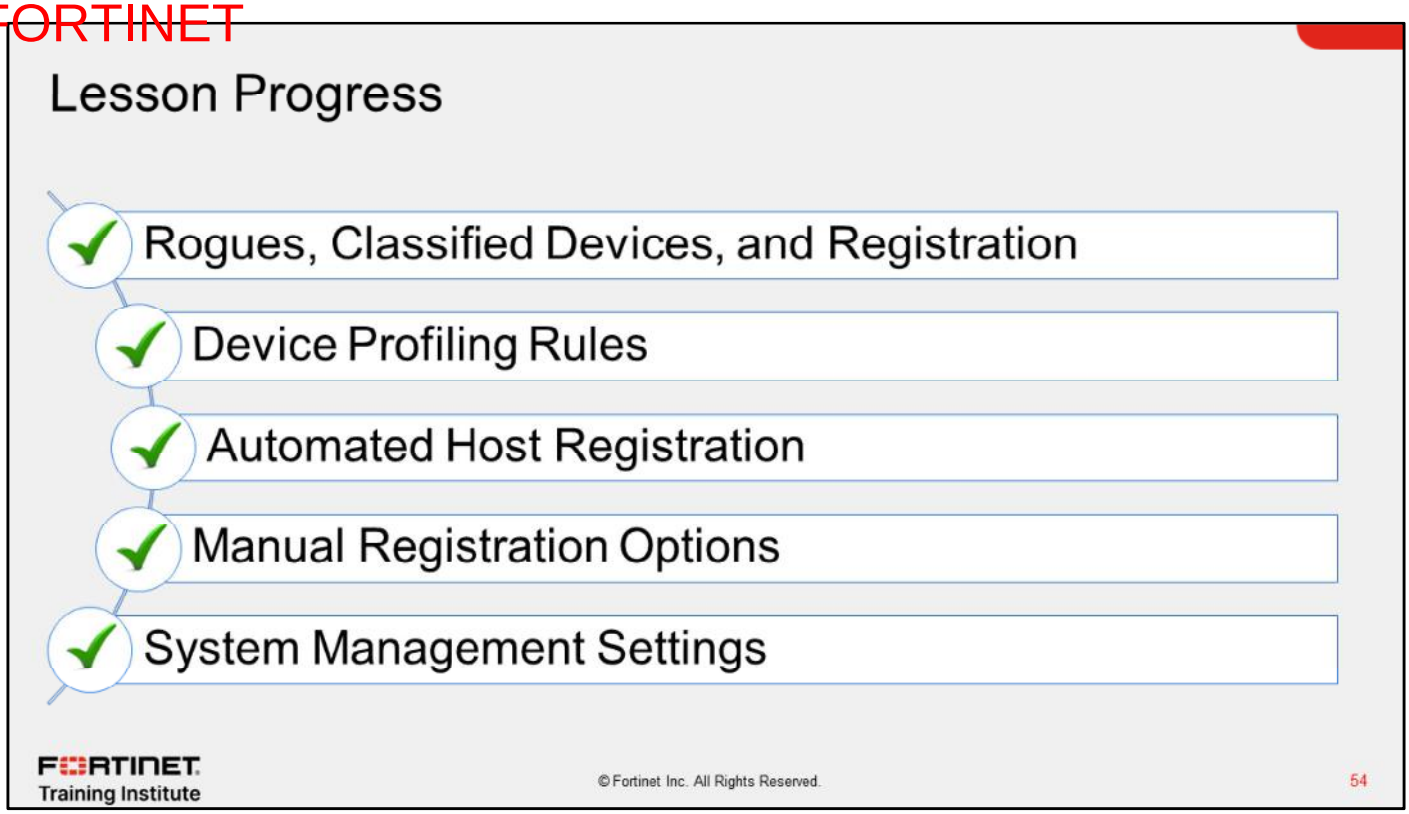
Knowledge Check

1. By default, how long are local database backups kept on FortiNAC?
   A. 7 days
   ✓ B. 90 days

FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.
53

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

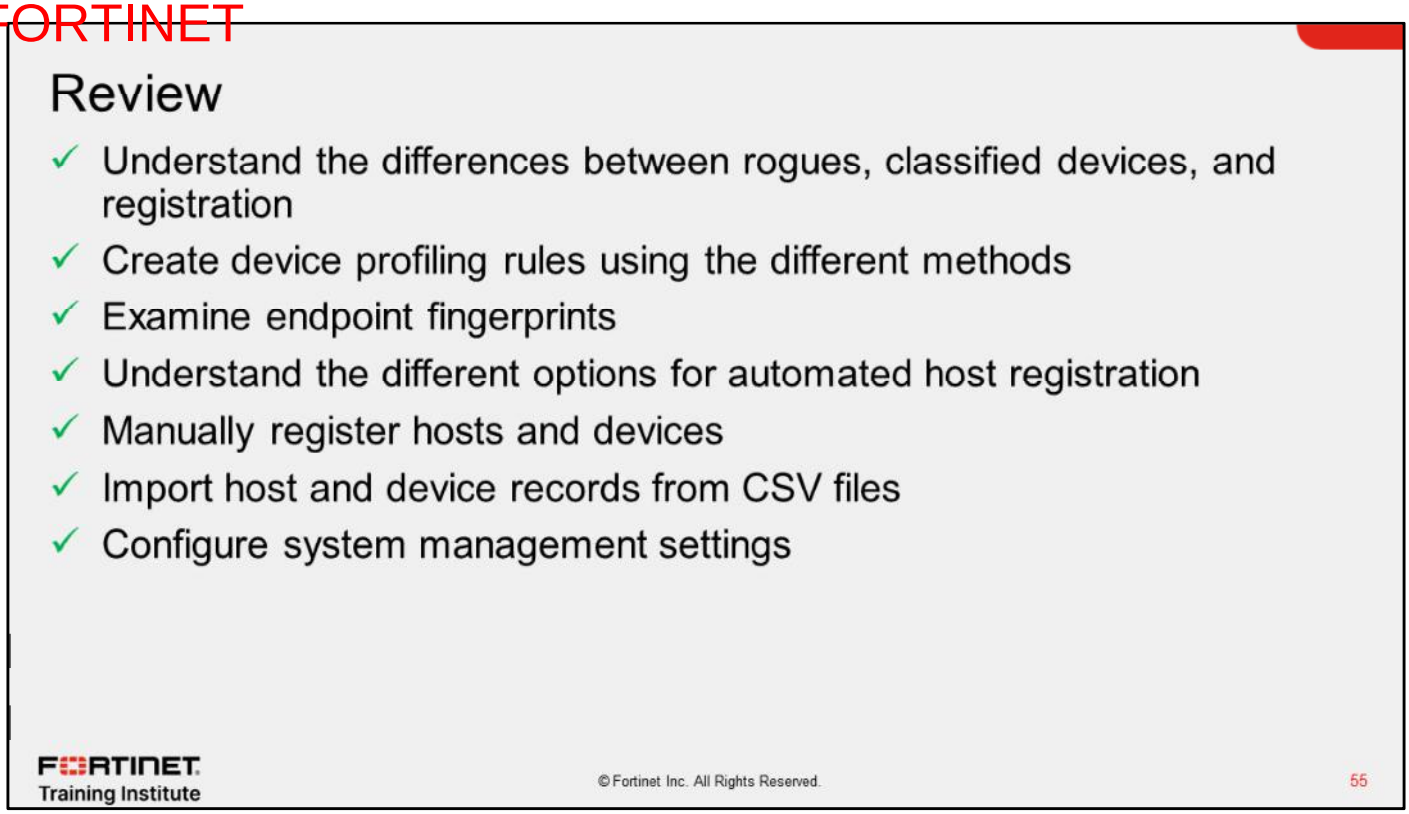


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

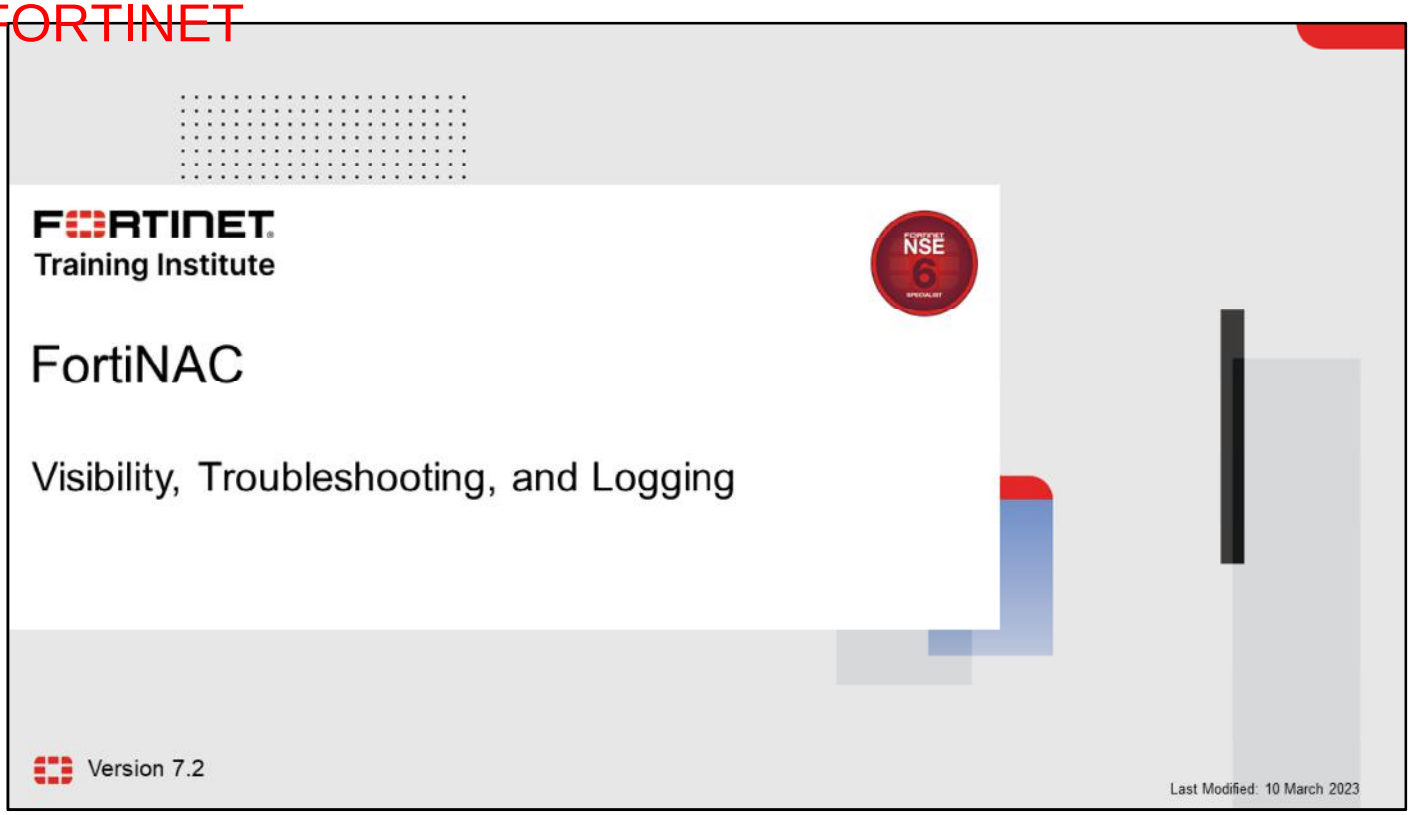


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about the endpoint identification and classification process, as well as the tools and methods used to expedite the process.

Vouchers & Dumps are Available | WhatsApp +201224560923

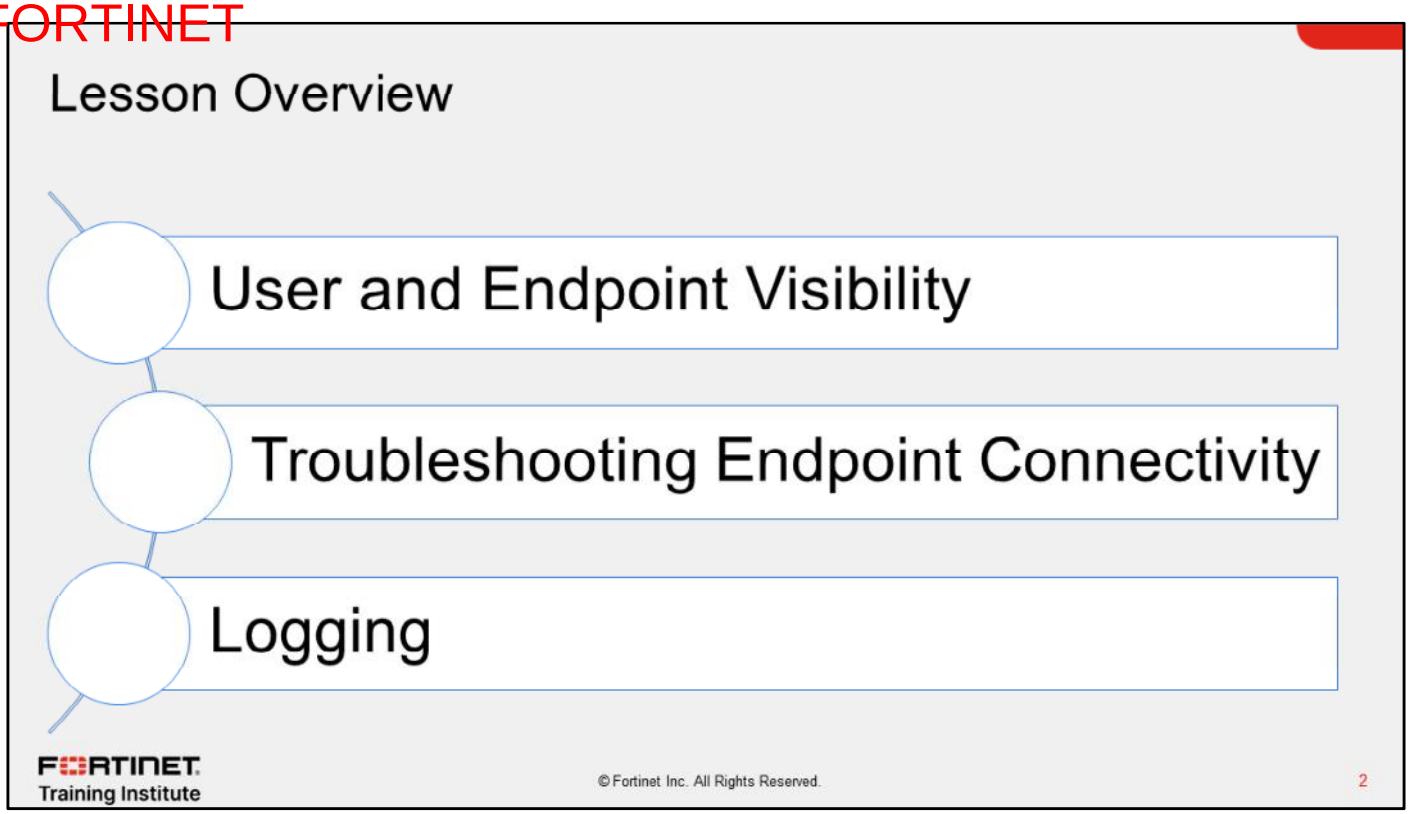
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to access and manage user and endpoint information quickly and efficiently. You will understand the basic visibility hierarchy that the FortiNAC uses to organize and relate different elements.

Vouchers & Dumps are Available | WhatsApp +201224560923

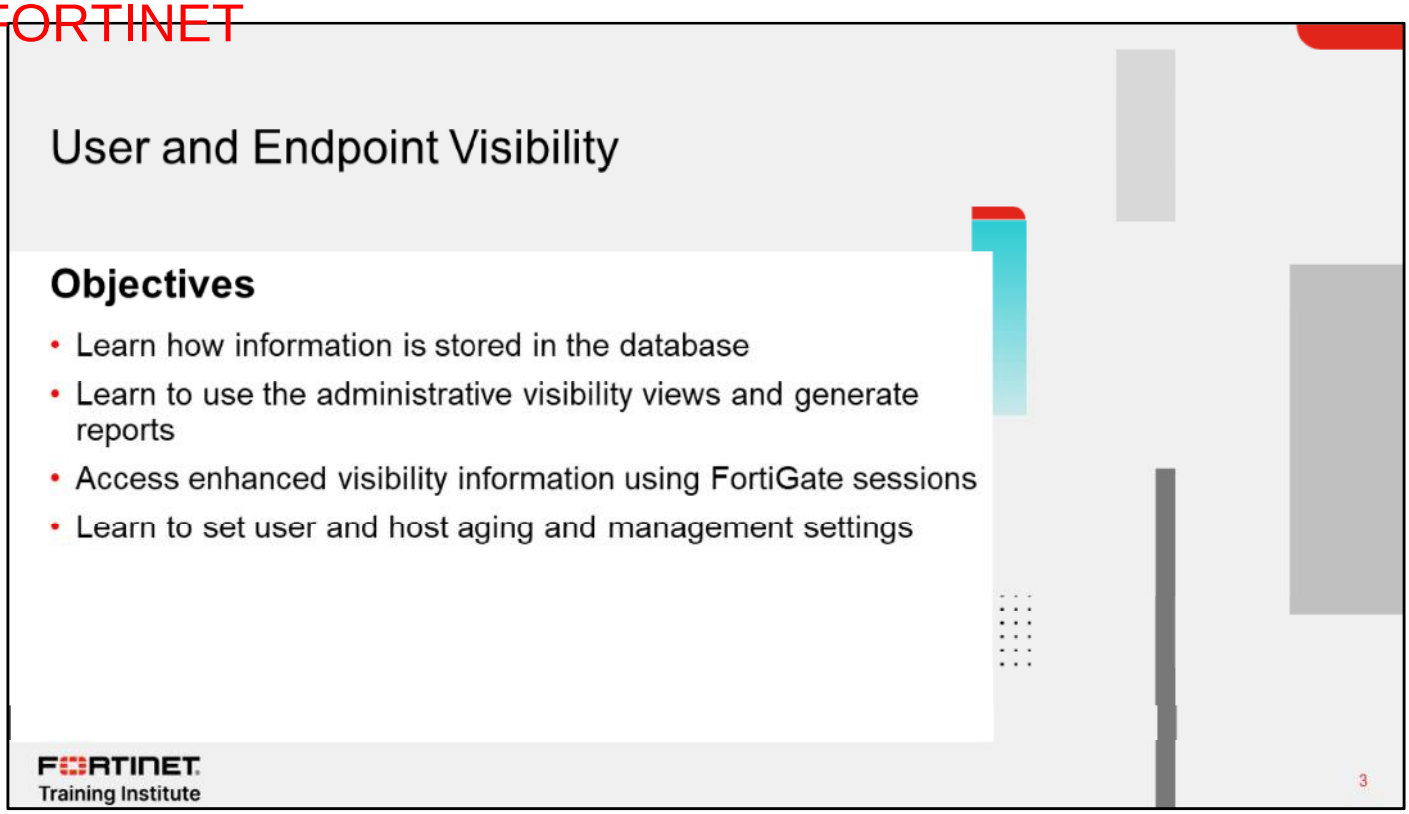
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

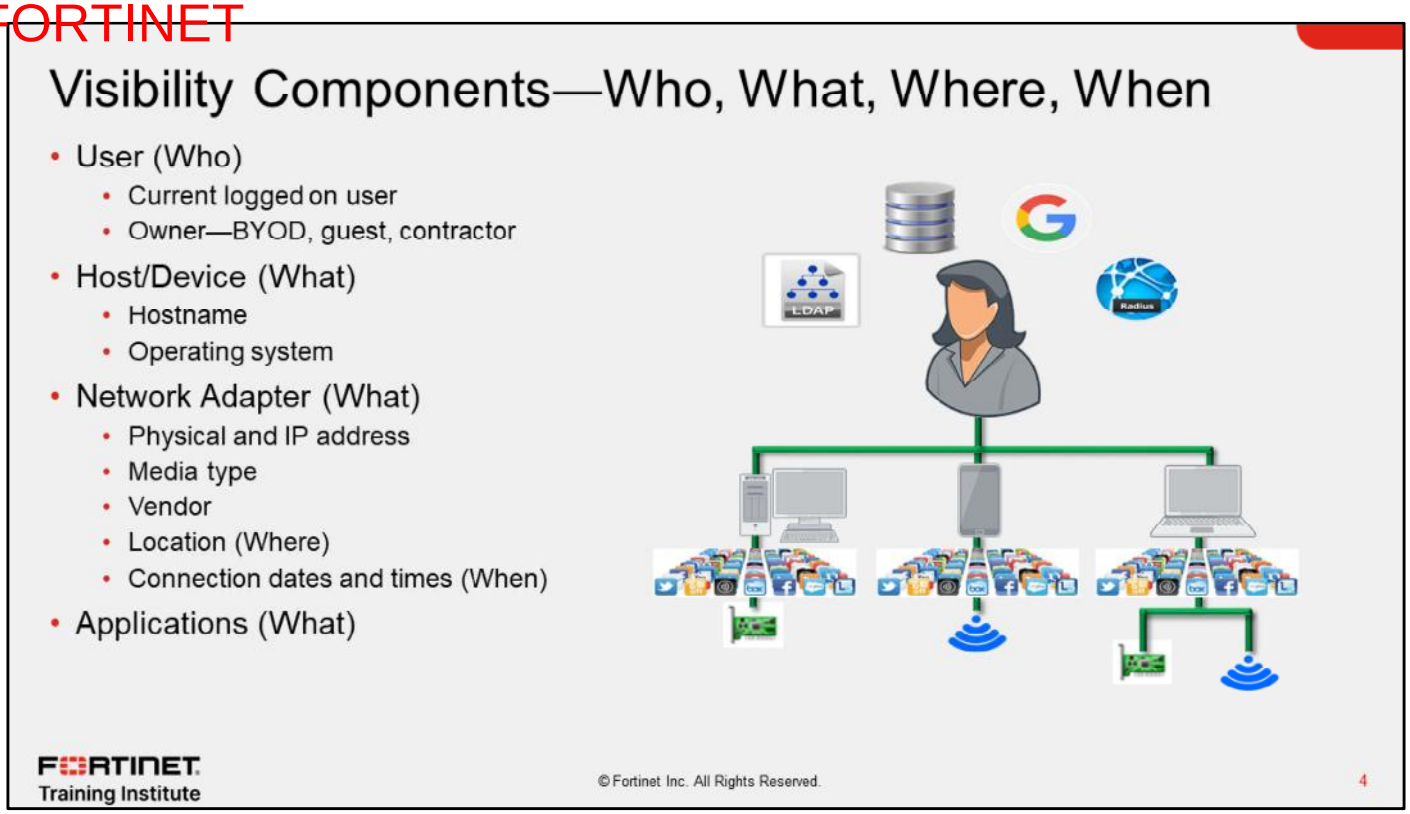


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competent understanding of how information is stored, how to use views and filters, and how to access the information available in those views, you will be able to view and use the information in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Network visibility is the first step to building a comprehensive network security solution that will profile and track all the endpoints accessing your network.

User information is gathered through integrations with LDAP or RADIUS servers, or stored locally in the FortiNAC database. Users can be associated with hosts as the current logged in user, in the case of user tracking, or as the owner of a particular device, in the case of BYOD. The user records contain a variety of user property information and this makes up the who component of visibility.

Host and adapter information is gathered from communication with the infrastructure, DHCP fingerprints and agent technology. Hosts will have associated adapters and a variety of host properties, such as host name, operating system and expiration dates. This host information makes up part of the What component of visibility.

Adapters are associated with hosts and contain a set of properties as well, such as physical address and IP address information. This adds additional information to the what component. Communication with the infrastructure adds where a particular adapter is connected and historic information is retained to track where it was connected in the past. This fills in the where and when information.

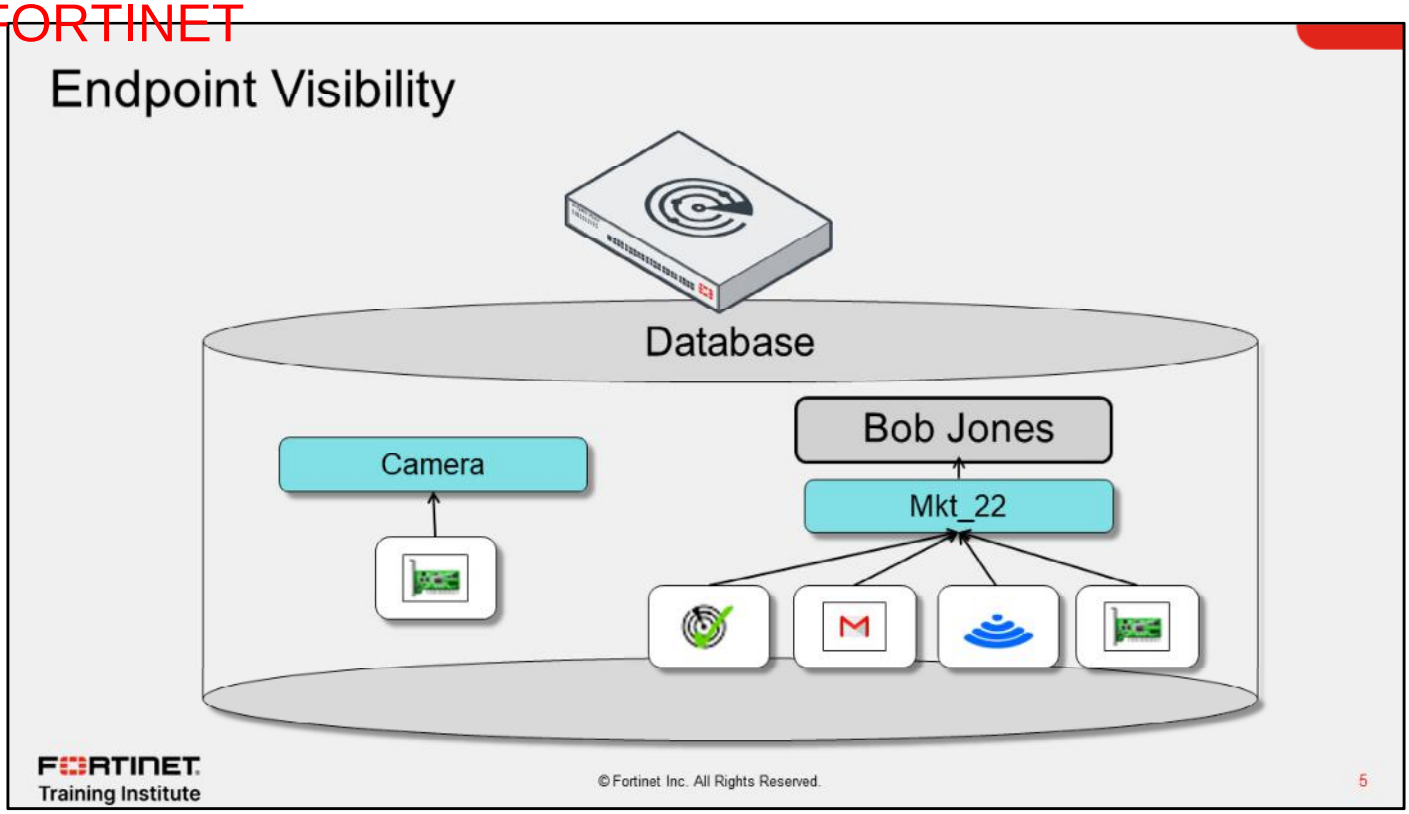
Application information is gather from agent communication or MDM integrations.

The gathered information can then be enhanced by information contained in the database, such as vendor identification based on adapter OUI. This information is organized and stored as attributes of the entities they are associated with. There are four levels of visibility available within FortiNAC, arranged as a visibility hierarchy, and there is a dedicated visibility view for each: users, hosts, adapters, and applications.

Application details, such was what applications are installed and their versions, enhances the what information further. You will explore each of these views in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

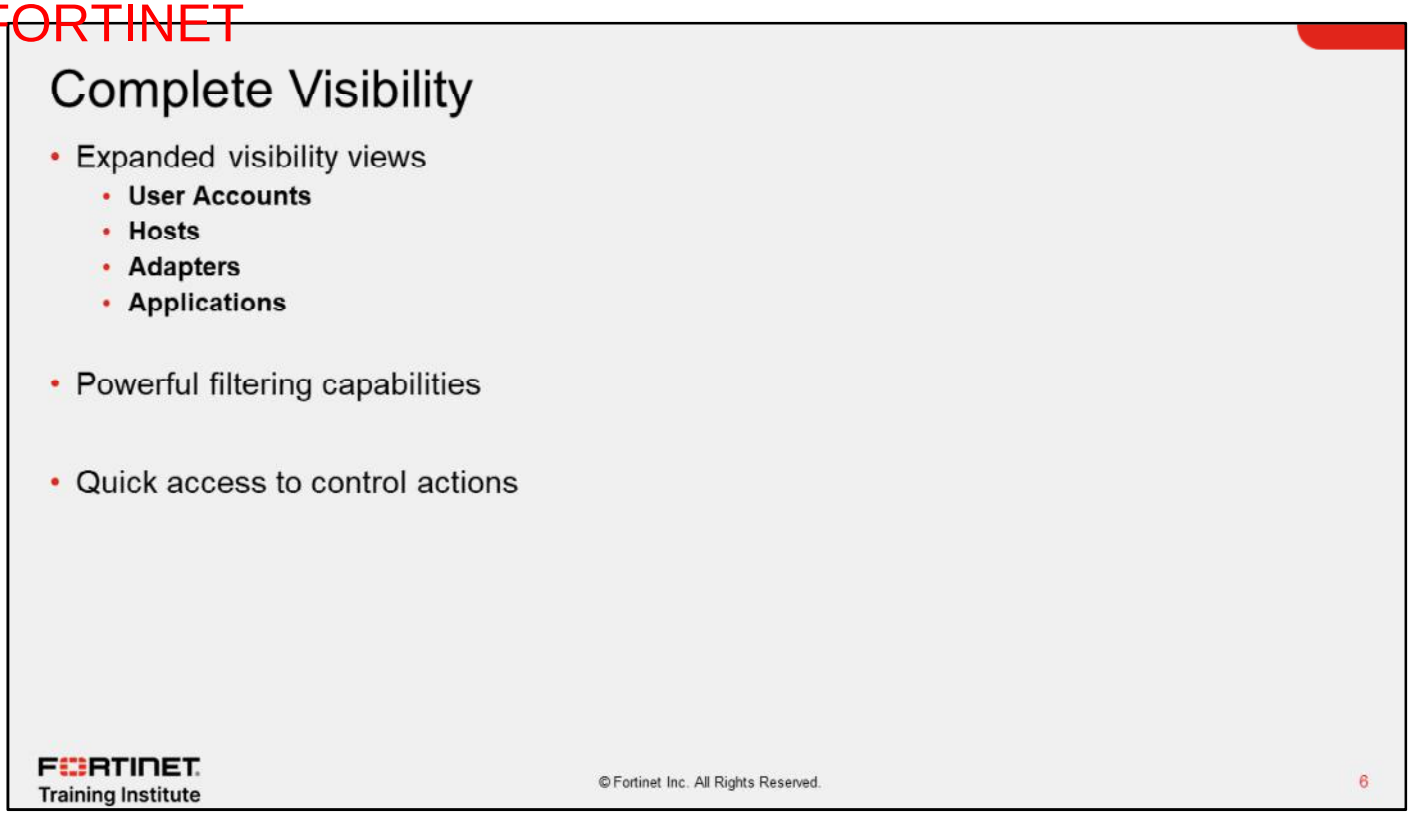
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Endpoint devices represented in the database can have varying levels of attributes. A simple headless IoT device, for example, may have nothing more than an adapter associated with it. An end station, however, may have a user associated with it, either as an owner, in the case of BYOD, or as the current user of a corporate asset. It may have applications such as web browsers, mail clients and agents. It may have wired, wireless adapters, or both. These two examples are most often displayed in the **Hosts** view with the IoT device being referred to as a device, and the end station as a host. This visibility can be broken down into four simple categories: users, hosts (this includes the IoT devices), adapters, and applications.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are four expanded visibility views for users, hosts, and devices not shown in the network inventory view:

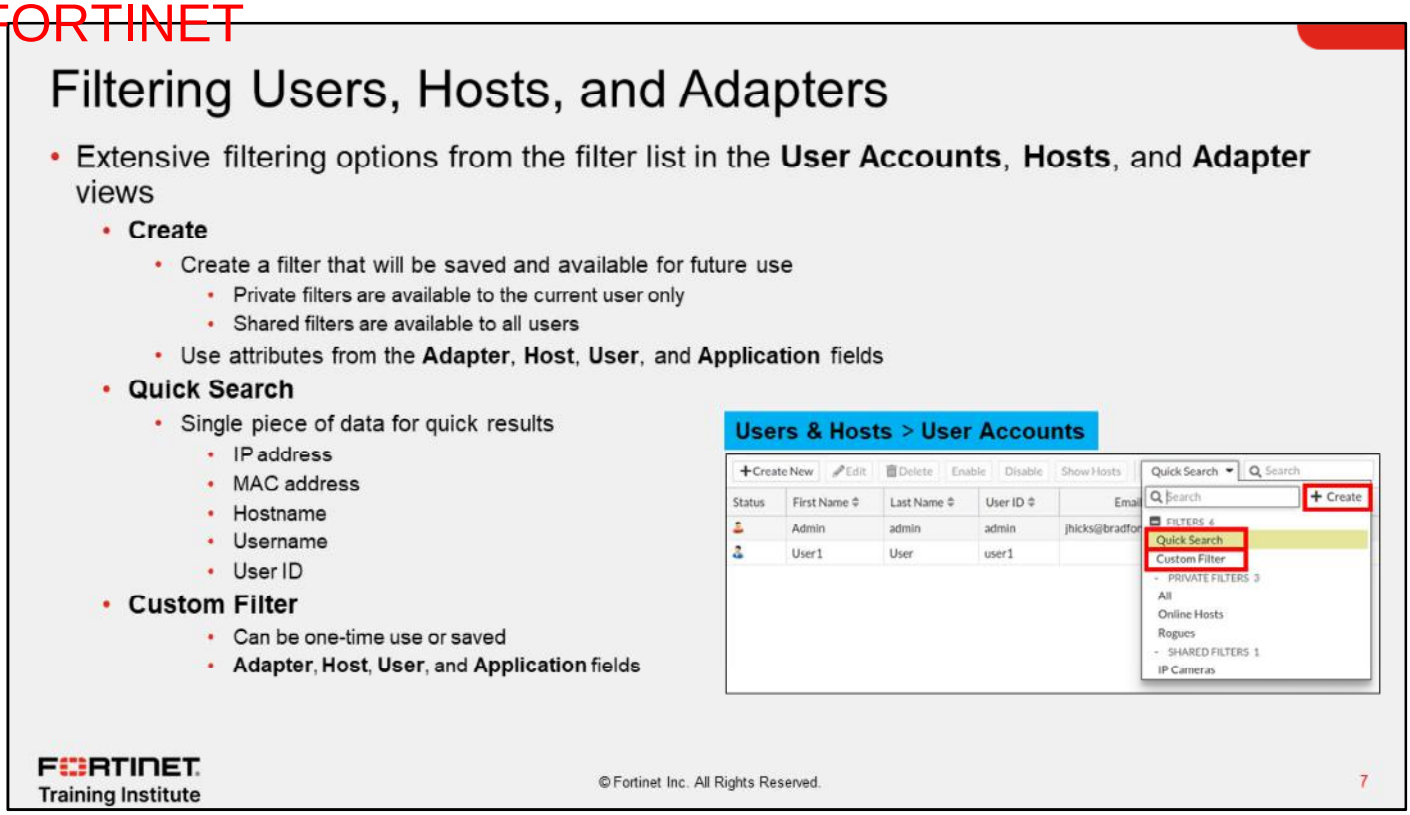
- **User Accounts**
- **Hosts**
- **Adapters**
- **Applications**

These views are all located under the **Users & Hosts** menu.

A very important feature of each view is the filtering capabilities. In a typical environment, there are thousands or tens of thousands of users, hosts, and so on. It is crucial that you are able to find what you're looking for as quickly and easily as possible. Another important component is easy access to control actions. When an administrative user is searching for a user, host, or adapter, it's normally because they need to gather information about that entity or take action on that entity, such as disabling a host and denying it network access. Control actions provide that capability.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The filtering tool that is available in the **User Accounts**, **Hosts**, and **Adapters** views looks and works the same way in each view.

In each view, the filter tool is located above the results panel. The **Create** button opens a filter configuration window that allows for the creation of extremely granular filters. These filters will be designated as **Private** or **Shared**. Private filters will only appear in the drop-down list when the user that created them is logged in. Shared filters will appear in the list for all users. Shared filters can be scheduled to produce report output in CSV format. The filter criteria can be selected from any of the attributes associated with user accounts, hosts, adapters, or applications. Logic, such as `AND` and `OR` can be incorporated in these filters.

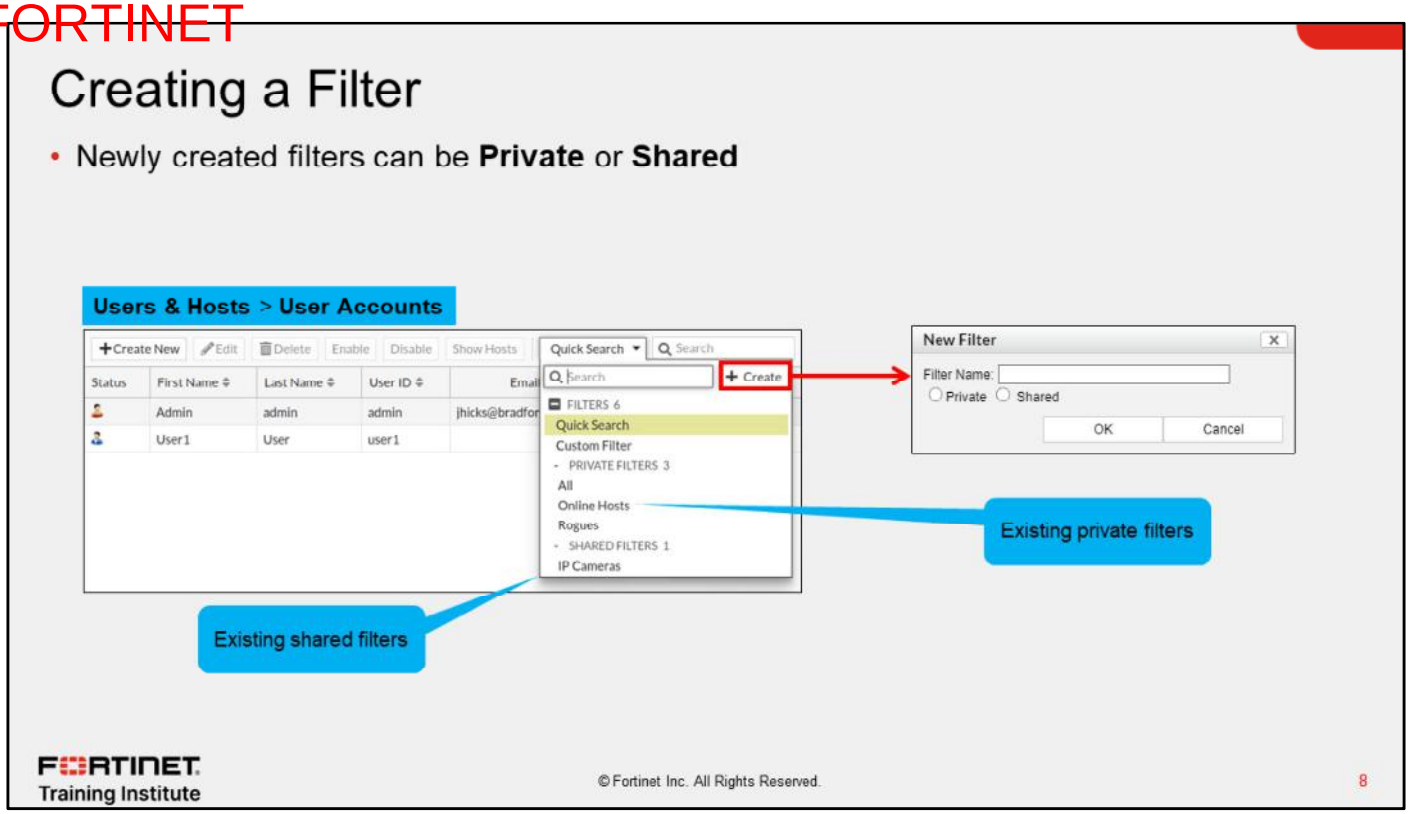
This default option is **Quick Search**. Any values entered as a quick search will be searched against the IP address, MAC address, host name, username, and user ID of all users, hosts, and adapters. Wild cards can be used in the quick search. For example, a value of `192.168.102.*` would return all adapters or hosts, depending on the current tab, with those numbers as the first 24 bits of their IP address. There are additional ways to customize filter criteria. For example, [attribute1, attribute2, attribute3] will return results that match any of the three attributes listed. Wildcards can be used within each of the attribute options and an ! (exclamation point) at the front of any search will invert the search to display all entities that do *not* match the parameters.

A **Custom** filter can be a one-time use filter or can be saved as a shared or private filter, with the same configuration options as the **Create** button.

The filter for applications uses a different style of filter, like the one seen in most of the other views, built one criteria at a time in the upper-left of the view.

Vouchers & Dumps are Available | WhatsApp +201224560923

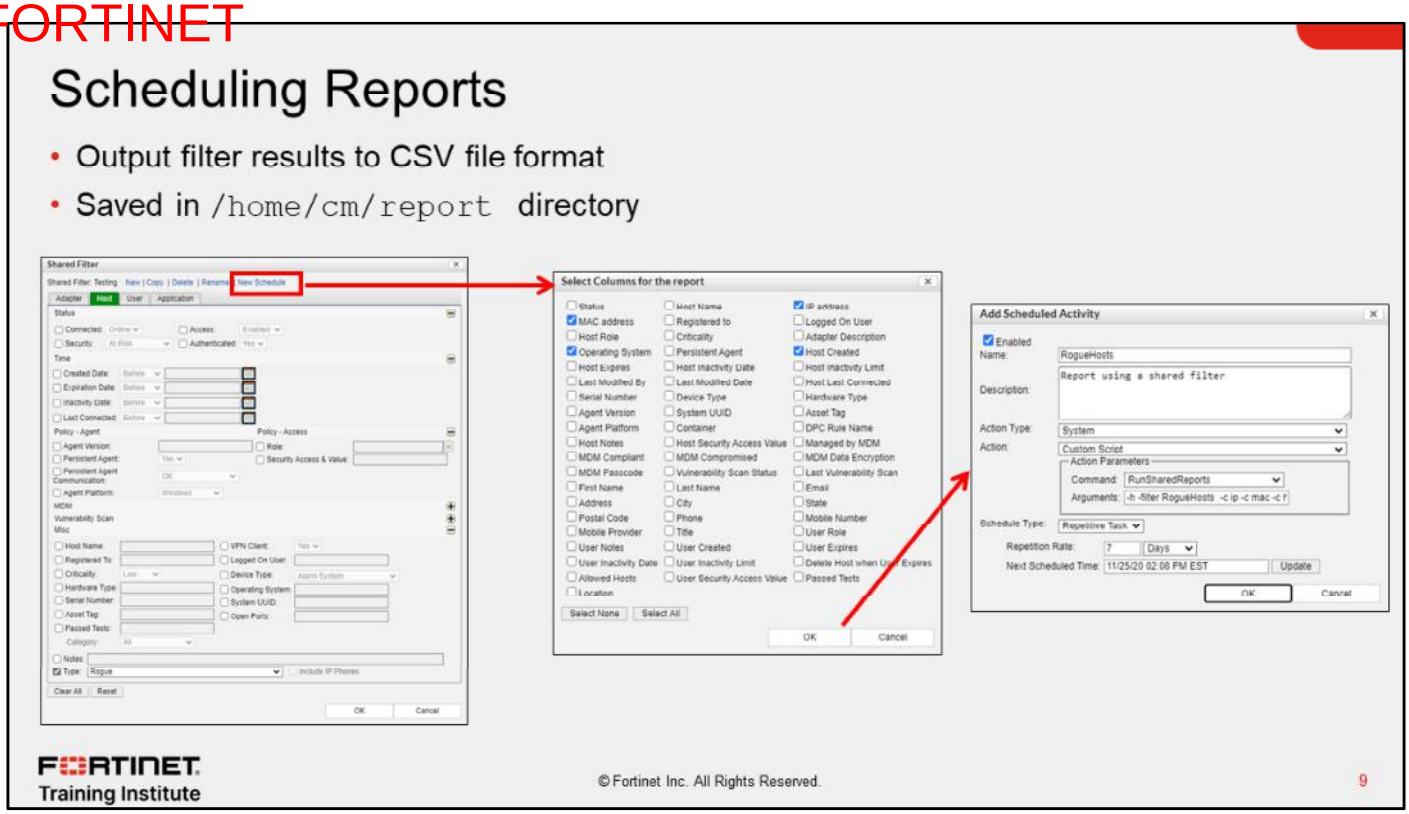
DO NOT REPRINT Brave-dumps.com
© FORTINET



When creating a new filter, you must assign a name to the filter, and designate the filter as shared or private before the filter configuration window opens.

Vouchers & Dumps are Available | WhatsApp +201224560923

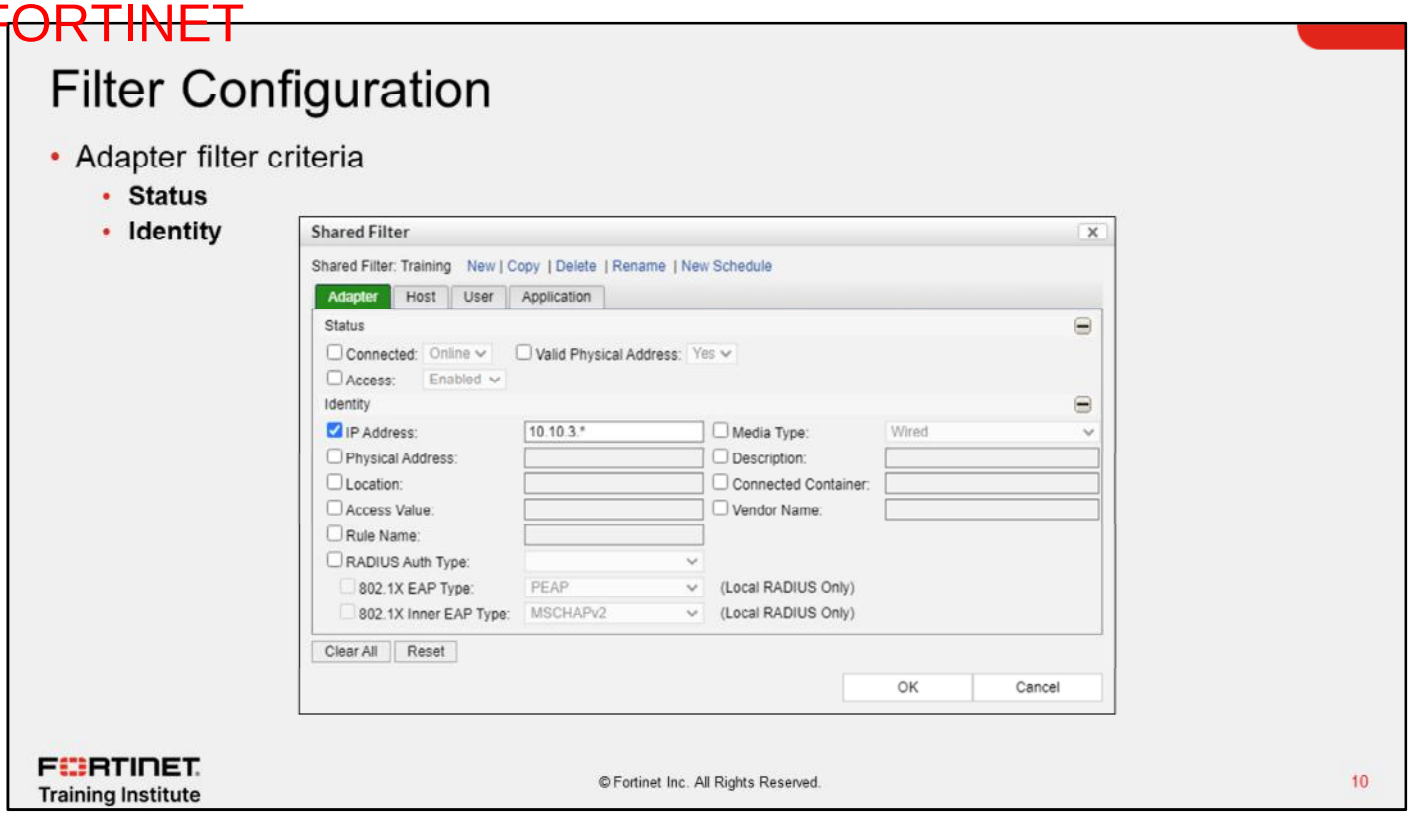
DO NOT REPRINT Brave-dumps.com
© FORTINET



When you create a shared filter, use the **New Schedule** option to add an entry to the **Scheduler** tool. Select the columns of information to include in the CSV output file and click **OK**. Each time the scheduled task runs, the output file will be stored in `/home/cm/report` with a date and time stamp.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The filter configuration window consists of four tabs, each focused on the attributes of the four different levels of visibility: **Adapter**, **Host**, **User**, and **Application**.

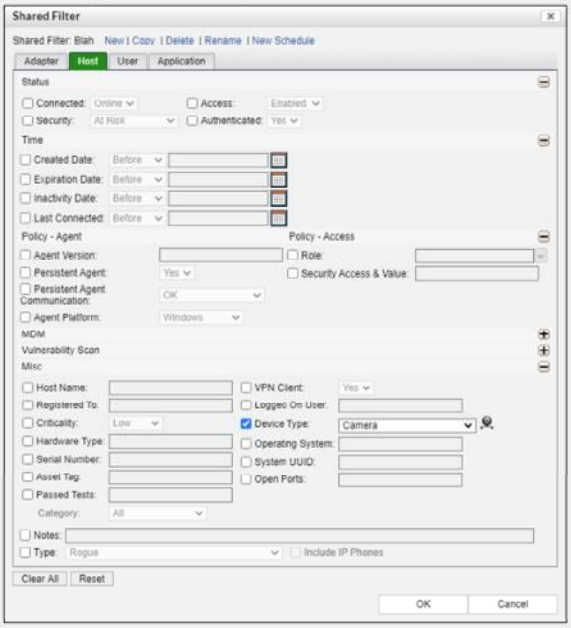
The **Adapter** tab allows you to select the attributes that will be filtered on and specify the values desired for those attributes. In some cases, when the options are finite, you can select the values from a drop-down list. In other cases, you will type the values into the fields. When you type the values, you can also use the wildcard and other options that were available in the quick filter. All selected attributes are logically ANDed together.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Filter Configuration (Contd)

- Host filter criteria
  - **Status**
  - **Time**
  - **Policy—Agent**
  - **Policy—Access**
  - **Misc**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

Configuring the host filter options works the same way as the adapter options. Attributes with finite options have drop-down selections and the other attributes require manual configuration. When values are entered manually, the wildcard and other options that were available in the quick filter are also available here. All selected attributes are logically ANDed together.

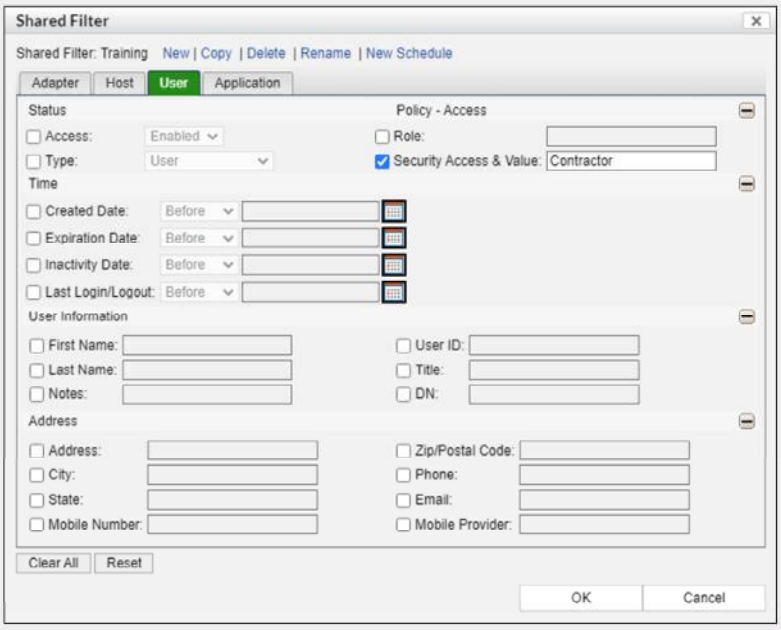
A simple, yet useful, function shown on this slide is the ability to create a filter to return a specific type of device, in this case, a camera. This capability allows you to create quick and easy real-time inventory reports based on device type. As you can see in the **Status** section, you can customize the reports to display the total number of cameras or just online or offline cameras.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Filter Configuration (Contd)

- User filter criteria
  - **Status**
  - **Policy - Access**
  - **Time**
  - **User Information**
  - **Address**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

12

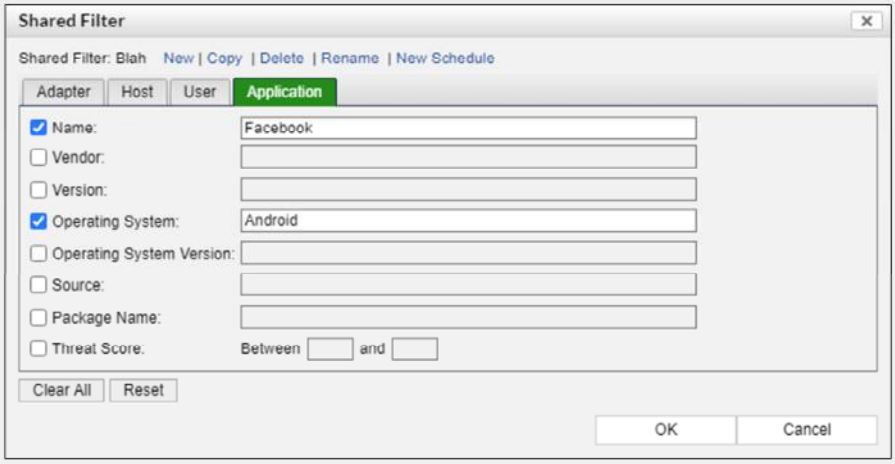
The filter attribute options on the **User** tab are specific to user record attributes, often information synchronized from LDAP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Filter Configuration (Contd)

- Application information:
  - MDM integration
  - Agent



FORTINET Training Institute

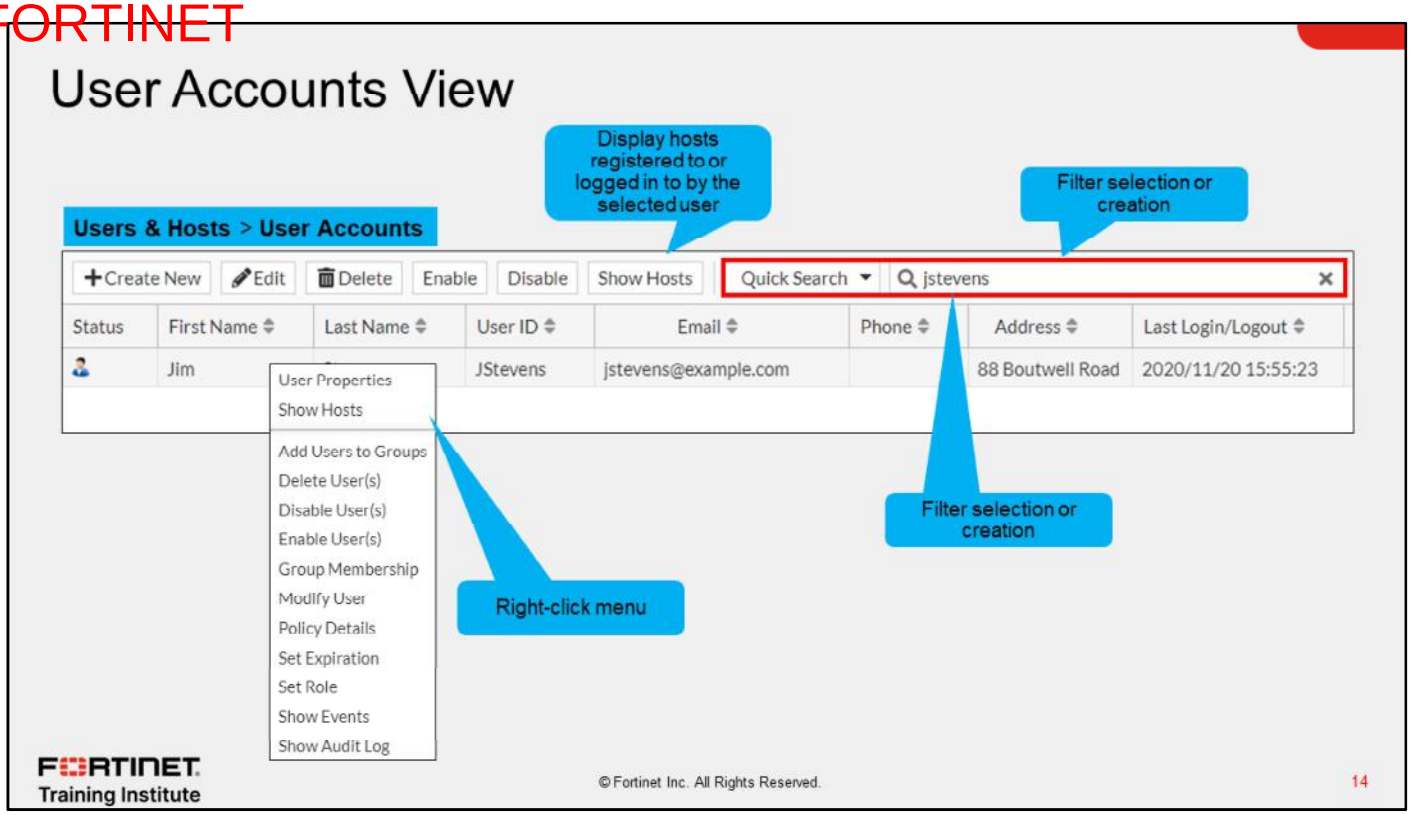
© Fortinet Inc. All Rights Reserved.

13

The **Application** tab stays consistent with all the other tabs in the way that it functions. There are no drop-down options, so you must type each value.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



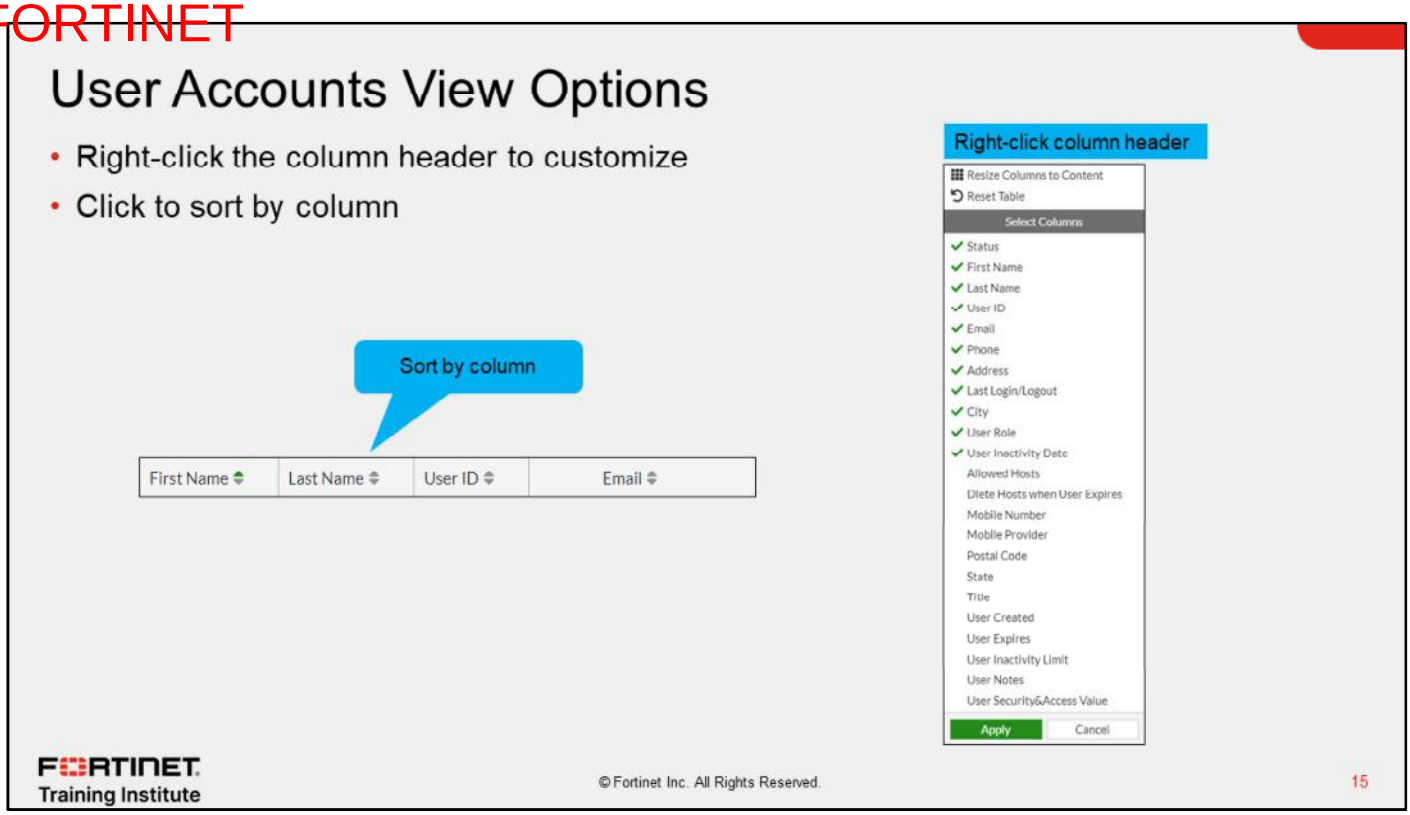
The **User Accounts** view is the first of the four visibility views you will learn about in this lesson. Notice the filter is located in the upper-right of the view. You can use the **User Accounts** view to add, delete, edit, locate, and manage users on your network. Users include network users, guest or contractor users, and administrative users. Administrative users can also be managed from the **Administrators** view. Administrative users may also be network users; therefore, they are included in the **User Accounts** view with a slightly different icon: a person wearing a red jacket. The normal network users are represented with almost the same icon, except with a blue jacket. Guest users are represented by a small notepad and pencil icon, and contractors are represented by a briefcase.

The **Show Hosts** button is used to display all hosts currently registered to the selected user, or currently logged in to by the user. A registered designation indicates ownership of that device to that user, typically BYOD devices. A designation of logged in demonstrates user tracking.

Right-click a user record to access management options such as, disable user, view or edit user properties, view or edit group memberships, delete the user from the database, view events associated with the user record, set a role value, and show administrative changes made to the user in the audit log. In the example shown on this slide, the user record was found using the **Quick Search** filter and filtering for the user ID.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

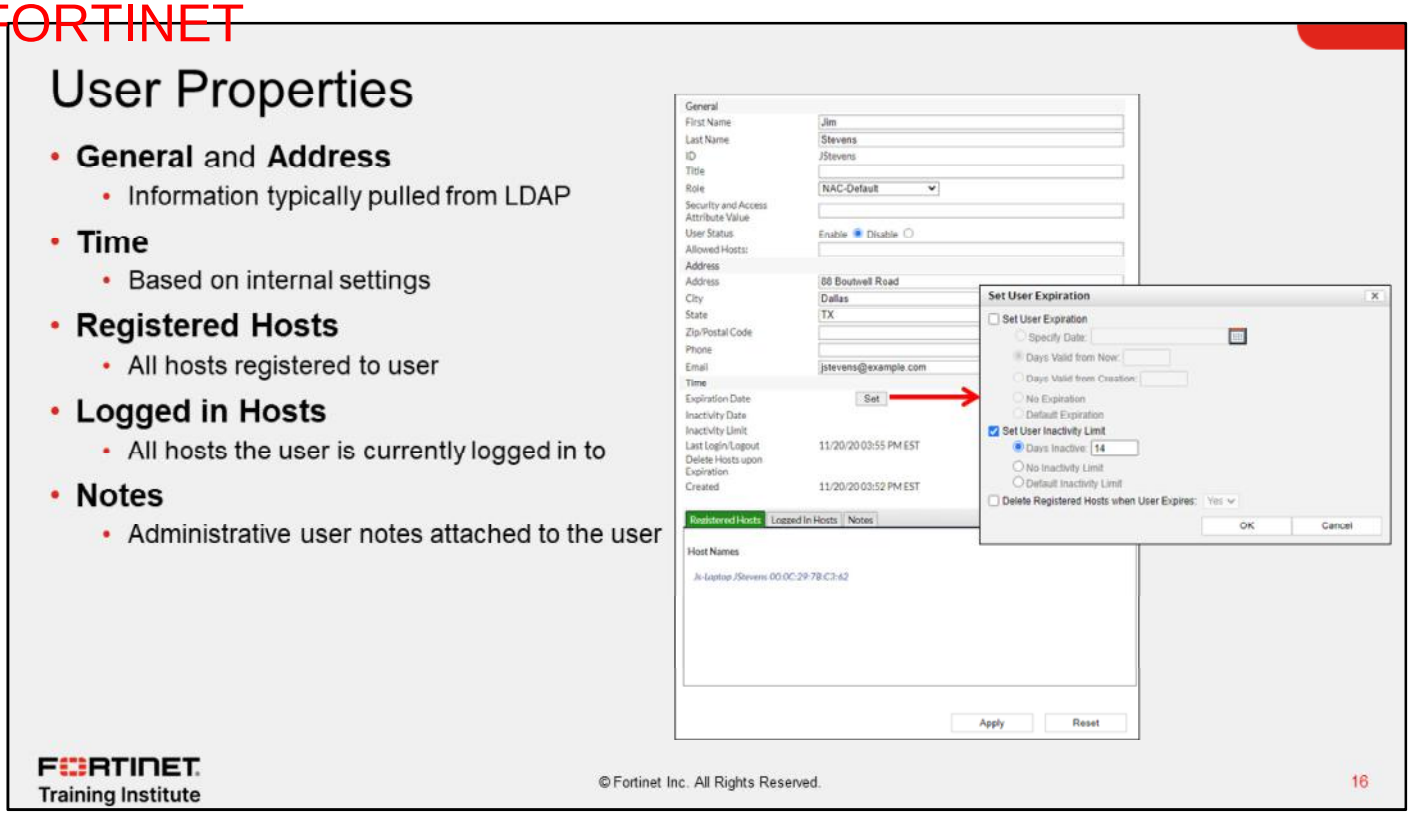


You can right-click any column header in the **User Accounts** view to select which columns will be displayed in the view.

You can click any column header to sort on that column.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

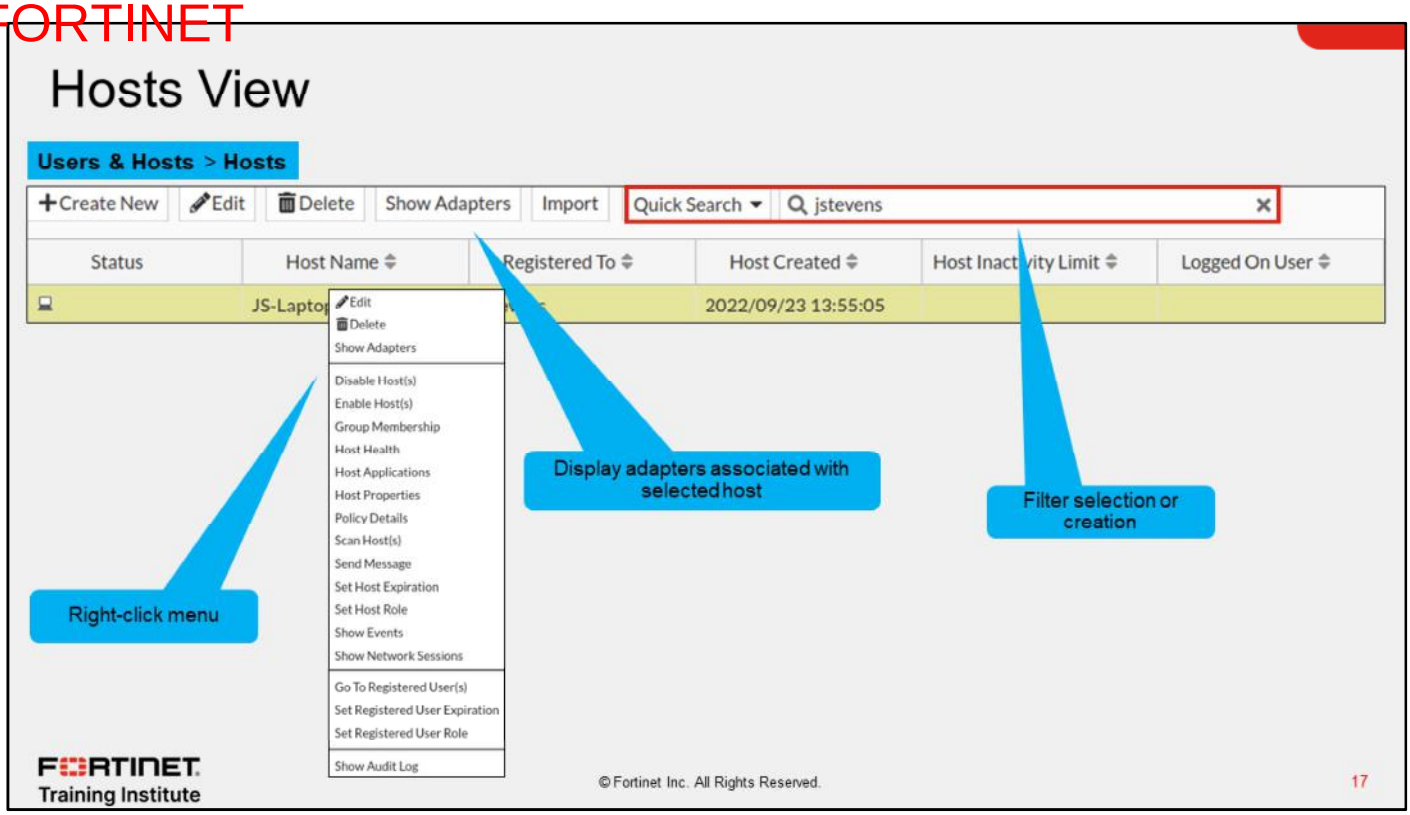


The user properties view provides access to detailed information about a single user. You can update user information in this view but, keep in mind, if the original information was populated from an LDAP server, the updated information that you entered will be overwritten the next time the directory synchronization scheduled task runs.

You can also configure expiration settings for the user here as well. You can access associated host properties clicking the adapter's physical address, displayed in the **Registered Hosts** or **Logged In Hosts** tabs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



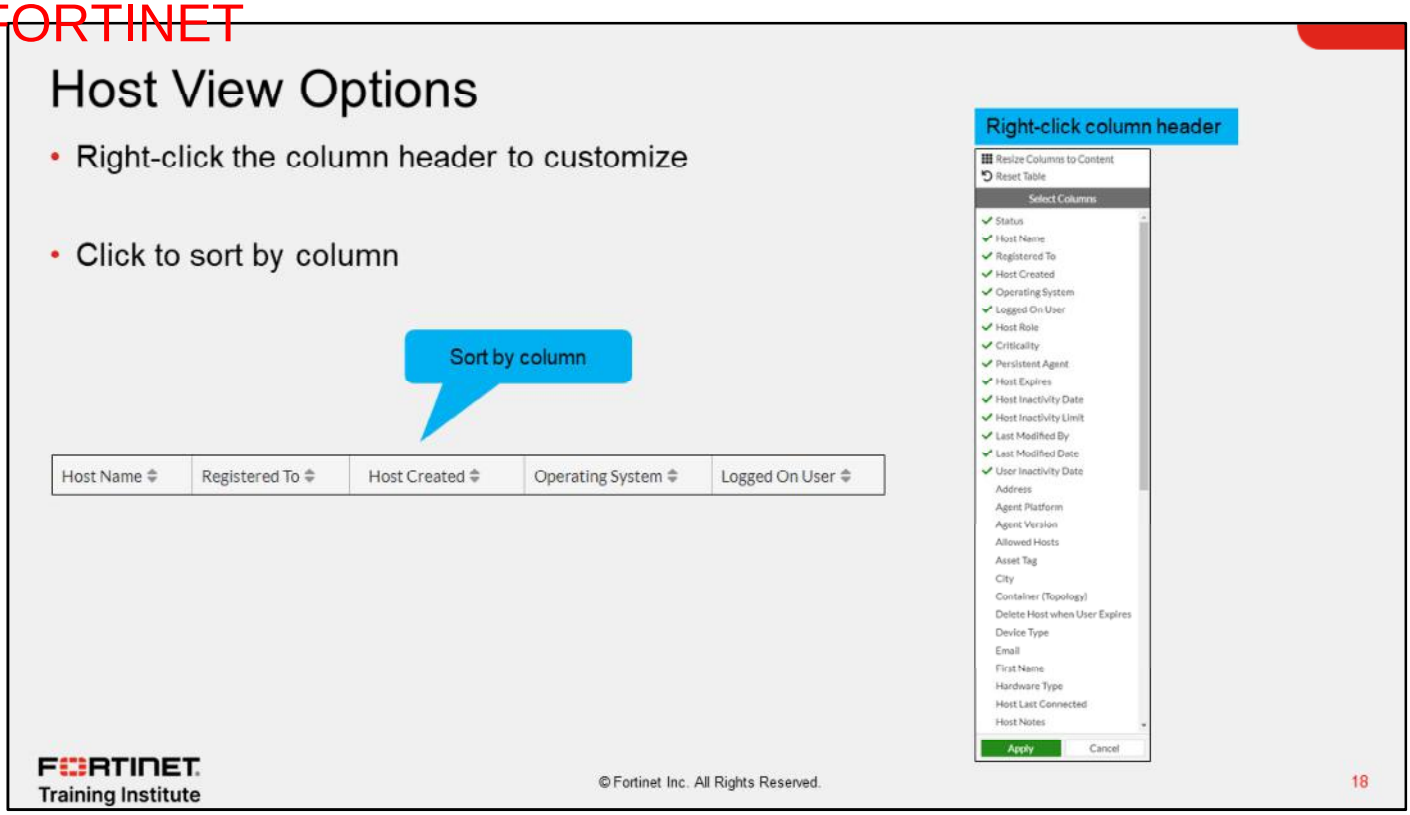
The **Hosts** view is laid out in the same way as the **User Accounts** view. The filter tool is located in the upper-right portion of the window. The **Hosts** view can be used to add, edit, delete, enable, or disable hosts. Hosts include virtually all network connected devices not modeled in the topology tree. This includes everything from endstations, like laptops and desktops, to mobile devices, like phones and tablets, to service type systems, like cameras, environmental units, IP phones, and so on. The systems seen here will be represented with a variety of different icons, even ones administratively created using the device type editor.

Selecting a host and clicking the **Show Adapters** button will display all adapters currently associated with that host. Remember, there is a hierarchy of relationships; users own or log in to hosts, and hosts have associated adapters. If you hover over the icon in the **Status** column, a pop-up window opens, displaying details about that host. The remaining columns are configurable by the administrative user and can include any of the available host properties.

Right-click a host record to access management options such as, disable host, view or edit host properties, view or edit group memberships, delete the host from the database, view events associated with the host record, set a role value, and show administrative changes made to the host in the audit log. In the example shown on this slide, the host record was found using the **Quick Search** filter and filtering for the user ID.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

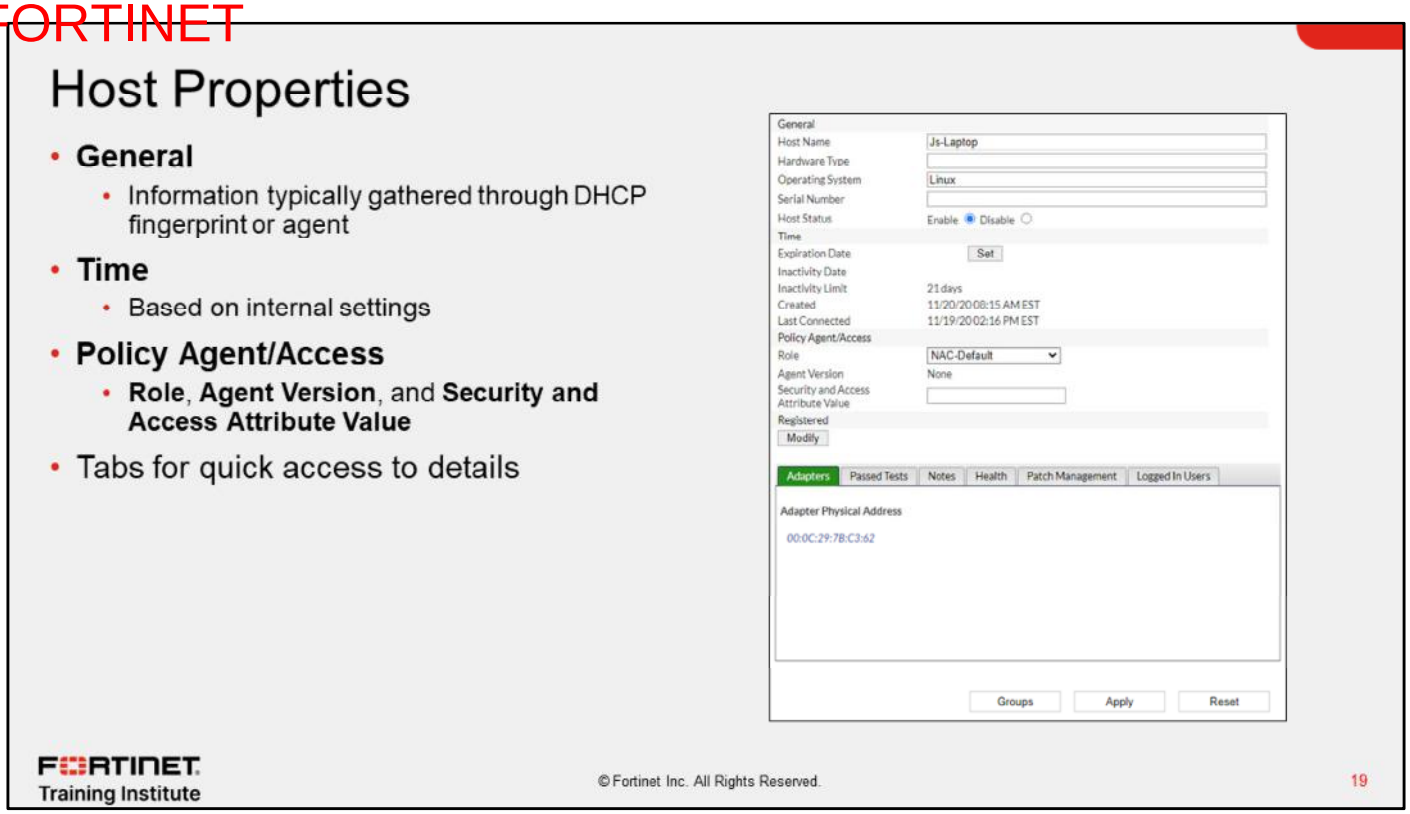


Right-click any column header in the **Hosts** view to select which columns are displayed in the view.

Click any column header to sort on that column.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The host properties view provides access to detailed information about a single host. You can update host information in this view, but, keep in mind, if the information was populated from communication with an agent, the updated information that you entered is overwritten the next time the agent communicates. Expiration settings for the host can be configured here as well.

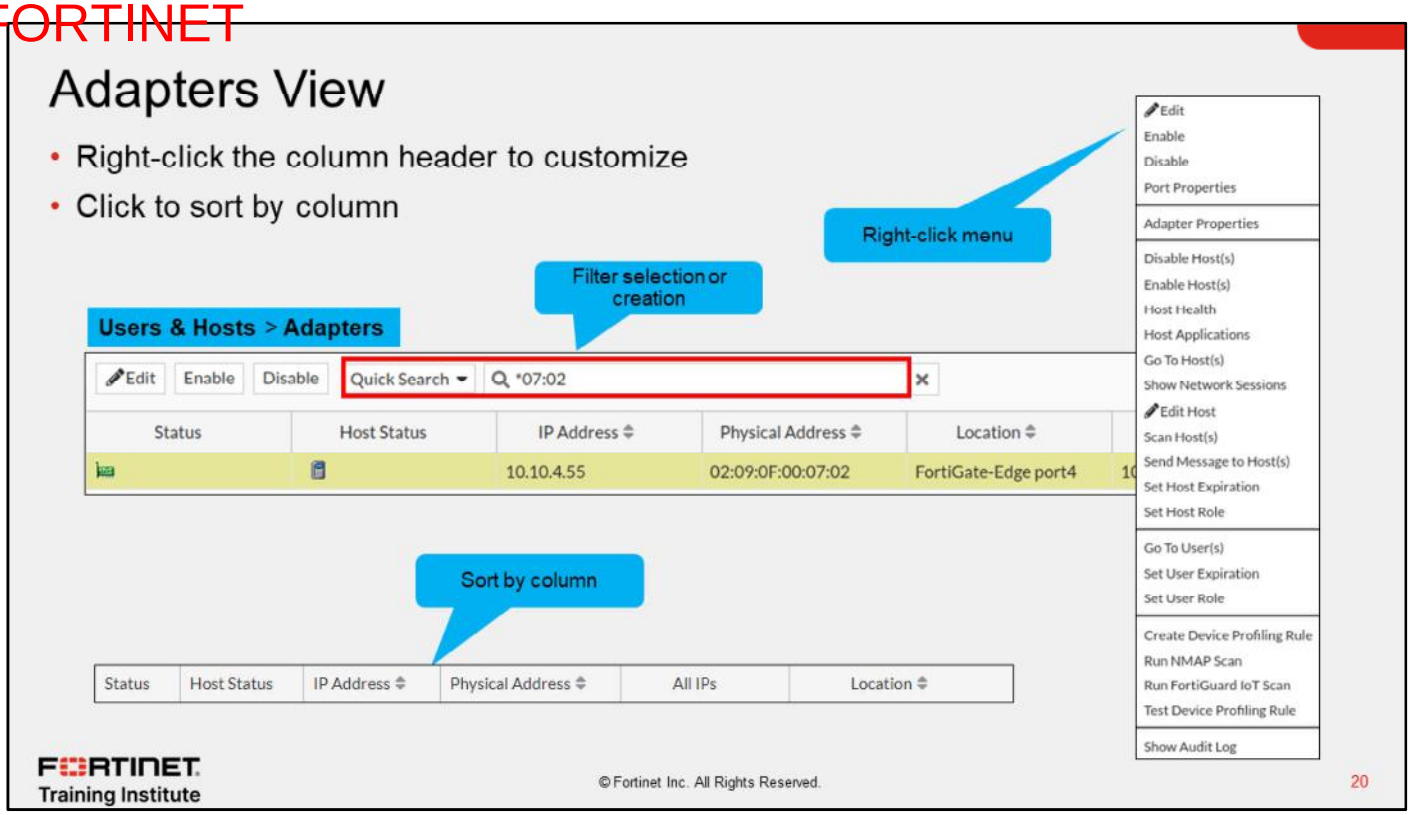
Tabs across the bottom of the view provide access to the following information:

- **Adapters**: Show adapter properties when you click the adapter physical address.
- **Passed Tests**: Show the details of any successful policy scans.
- **Notes**: A notes field for administrative notes about the host.
- **Health**: Show all the possible policy and administrative scans that could be or have been performed or assigned, and the results.
- **Patch Management**: Display information on patches that have been applied to the host by its associated patch management server, patch manager vendor name, and ID number of the most recently applied patch.
- **Logged In Users**: Display the user name of any user logged in to this host. User tracking must be ongoing for this information to be available.

If the host has a persistent agent installed, a **Send Message** button will be available for sending messages to the host. The **Groups** button allows an administrative user to view and modify host group membership. The **Apply** button commits any changes, and the **Reset** button undoes any changes made since the last commit.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Adapters** view behaves in the same way as the **User Accounts** view and **Hosts** view. The filter tool is located in the upper-right portion of the window. You can use the **Adapters** view to enable, disable, or edit adapter records. Adapters are represented with a network interface card (NIC) icon that is green if the adapter is online. The icon is gray if the adapter is offline.

The host that is associated with this adapter is represented with its device type icon in the **Host Status** column. Hovering over the icon in the **Status** column opens a pop-up window that displays details about that adapter.

The administrative user can configure the remaining columns and include any of the available adapter properties.

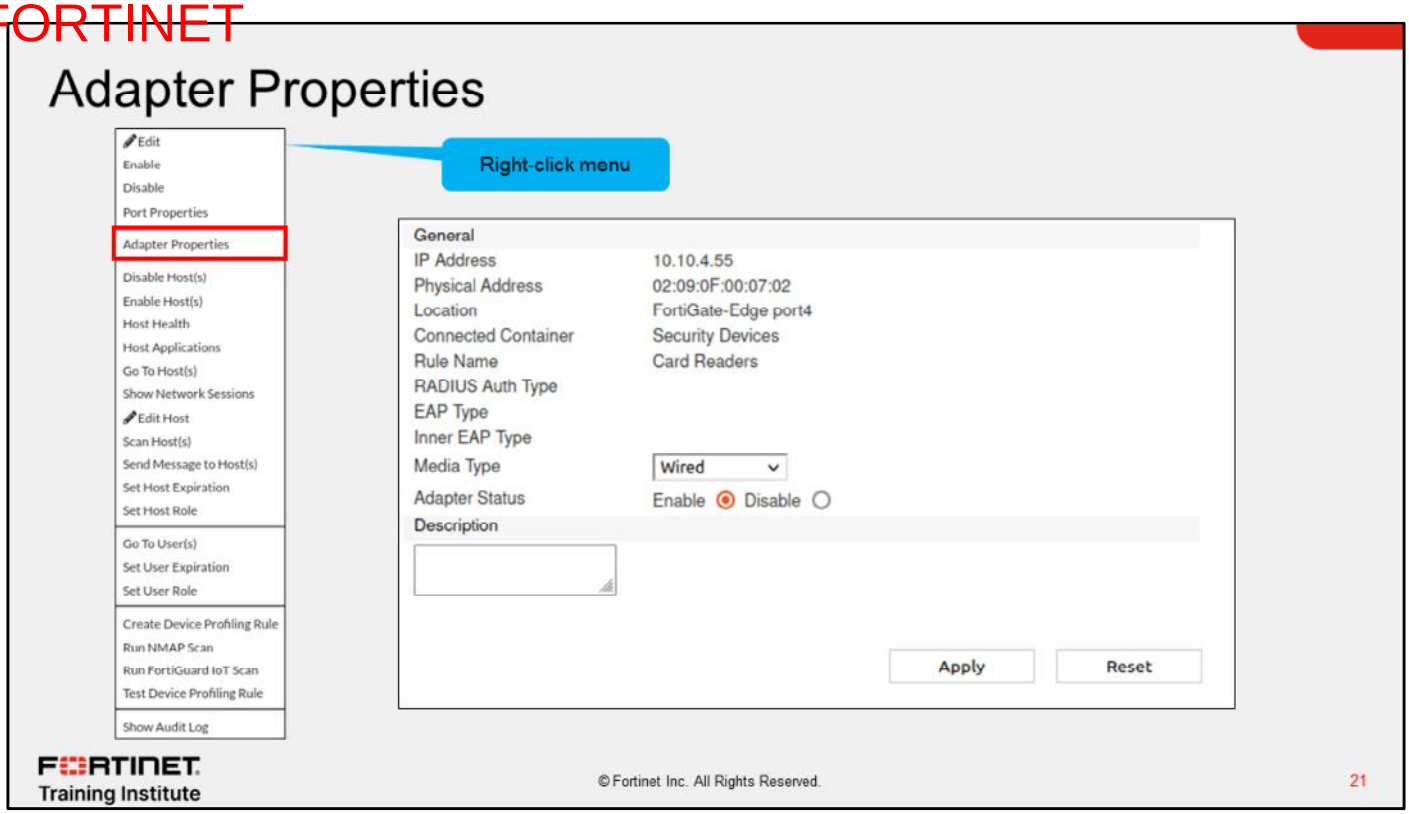
Right-click an adapter to access adapter properties and all administrative actions that can be taken on that adapter, such as disable, enable, modify, view connected port properties, and so on. You can also move backwards up the hierarchy and view or modify information on the associated host.

The right-click menu includes the following options that can be useful when developing and testing device profiling rules:

- **Create Device Profiling Rule**: This option opens the **Add Device Profiling Rule** window, which is populated with information known about the device, as well as any known method information—most often vendor OUI and DHCP fingerprint.
- **Run NMAP Scan**: FortiNAC runs an NMAP scan against the endpoint and displays the results in a window. This can help with determining values that can be used with the active method.
- **Run FortiGuard IoT Scan**: This option will show the results of a FortiGuard IoT scan of the selected device.
- **Test Device Profiling Rule**: This option allows an administrate user to validate the selected adapter and its corresponding host against an existing device profiling rule with a **Match** or **Does Not Match** result.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The adapter properties view displays detailed information about the selected adapter, including:

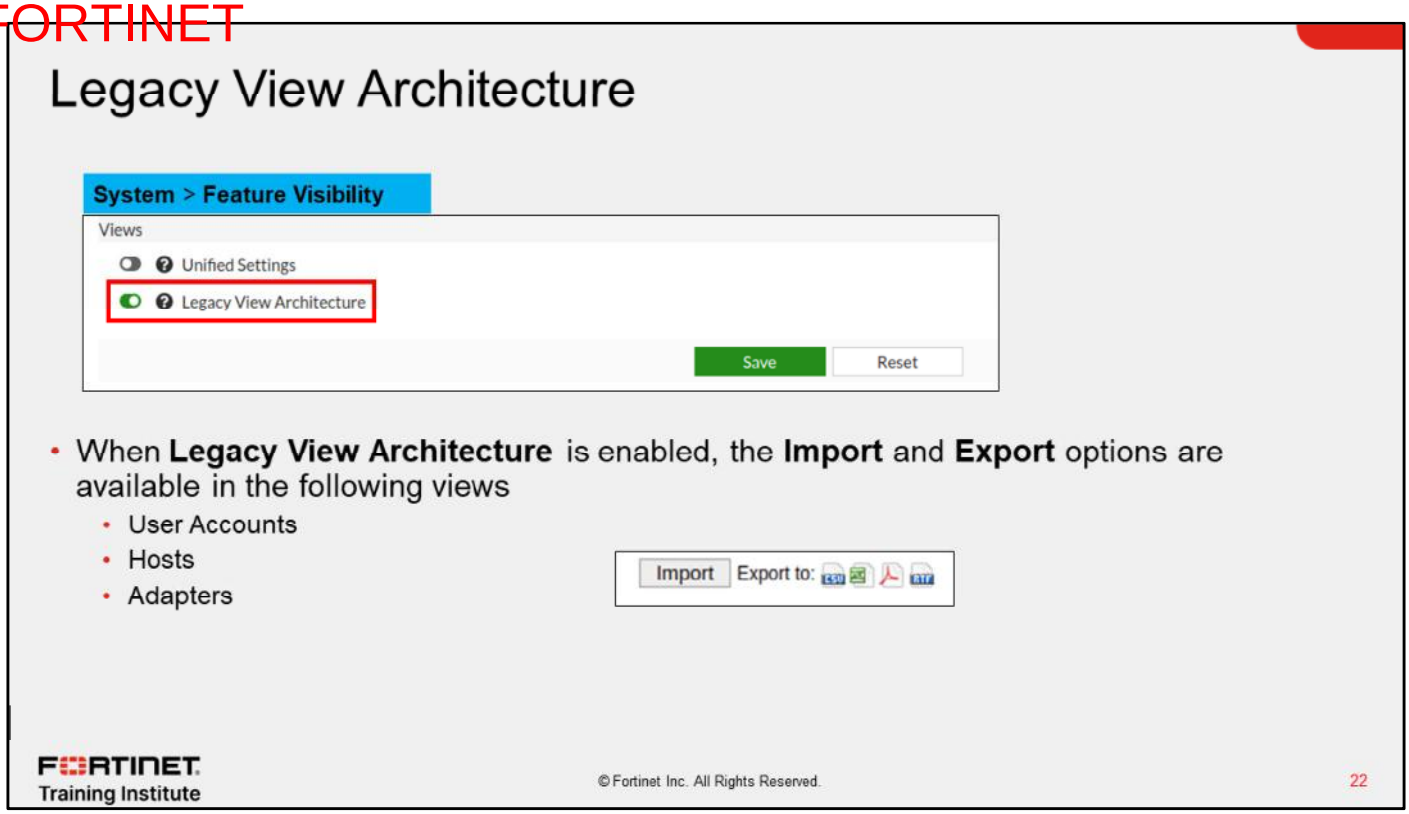
- IP address
- Physical address
- Location
- Connected container
- Rule name (matched device profiler rule if applicable)
- RADIUS and EAP information
- Media type
- Adapter status
- Description

In the **Media Type** drop-down list, you can select **Wired**, **Wireless**, **Virtual** (the host is a VM), **Virtual Guest** (the host is a VM running on a registered host), or **Unknown**. In the **Adapter Status** field, you can select **Enable** or **Disable**. You can type a description in the **Description** field.

Click **Apply** to commit any changes and **Reset** to undo any changes made since the last commit.

Vouchers & Dumps are Available | WhatsApp +201224560923

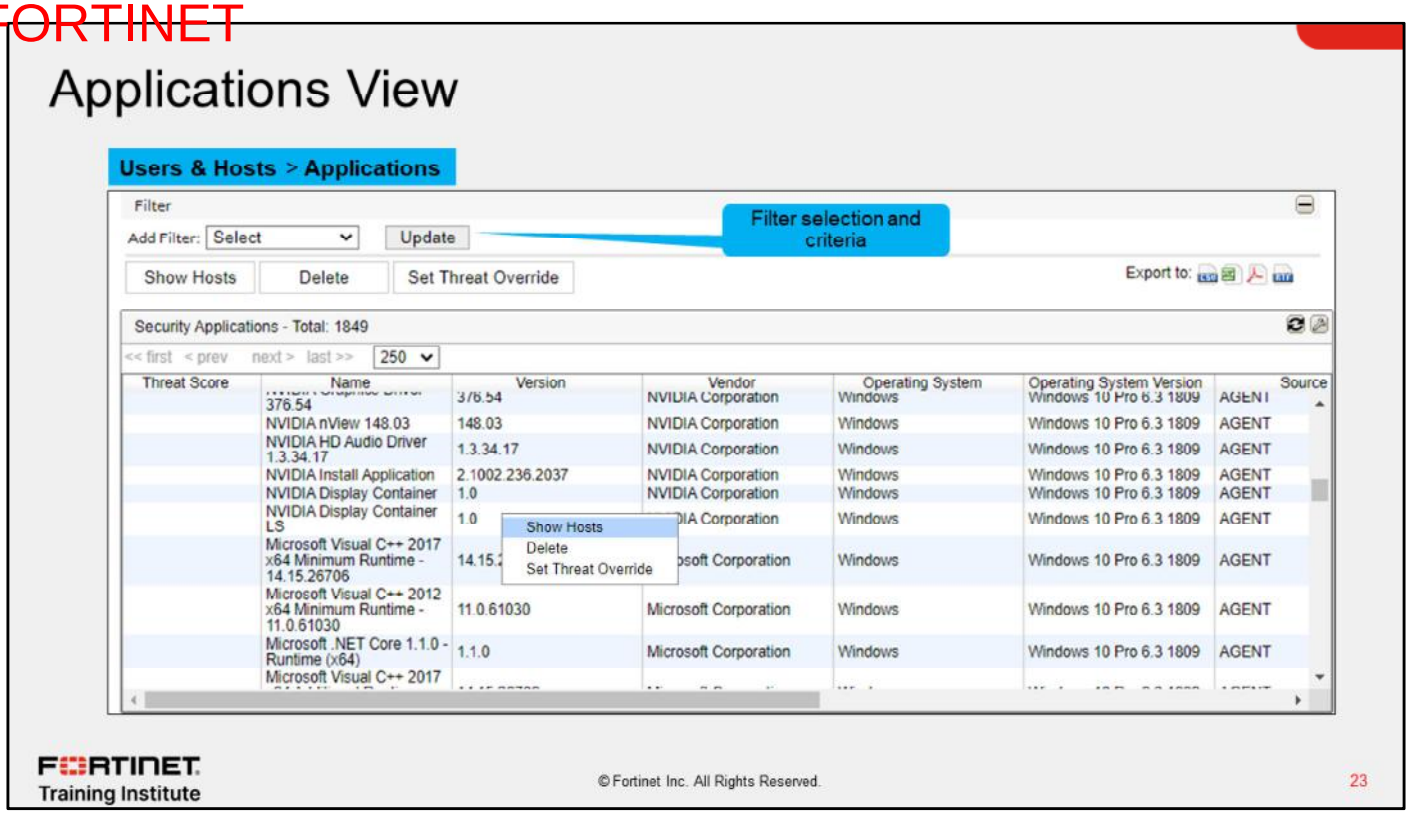
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Import and **Export** options are available from the **User Accounts**, **Hosts**, and **Adapters** views when **Legacy View Architecture** option is enabled in the **System** > **Feature Visibility** view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Applications** view is set up a little differently than the other views. One of the most notable differences is how you add a filter. To add a filter, use the **Add Filter** field to select and then add one criterion at a time. The criteria are the information available across the columns.

Another difference is that, even if you remove all hosts that have a particular application from the system, the application remains in the view until you delete it. This function can be useful when you want to leverage application information in situations where an existing host with that application is not needed, as part of a security policy, for example. Each application gets a unique entry if any portion of its details make it unique. So, for example, you may have the same version of a particular application, but the applications were learned from systems with different operating systems. This allows for maximum visibility granularity.

You can click the buttons along the top, or right-click an entry, to provide the following options:

- **Show Hosts**: Changes the view to the host view, prefiltered, to display only hosts with the selected application installed.
- **Delete**: Removes the selected applications from the database.
- **Set Threat Override**: Allows you to designate an application as trusted and safe or untrusted and dangerous.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate Session Information

- Enable firewall polling from the right-click menu of the firewall model
- Session information will begin to populate after polling has been enabled
- Device profiling rules can be created from session information

Users & Hosts > Network Sessions

Delete

Firewall	Protocol	Device	Country	Country ID	Hostname	Source Address	Source MAC Address	Source Port	Destination Address
10.0.1.254	udp	Linux	United States	21333		10.10.3.50	02:09:0F:00:02:03	40653	8.8.8.8
10.0.1.254	tcp	Linux	United States	21333		10.10.3.150	02:09:0F:00:02:02	48200	104.16.248.249
10.0.1.254	udp	Linux	United States	21333					
10.0.1.254	udp	Linux	Canada	16707	BPMonitor				
10.0.1.254	tcp	Linux	United States	21333					
10.0.1.254	udp	Linux	United States	21333	BPMonitor	10.0.1.2	02:09:0F:00:01:08	57345	8.8.8.8
10.0.1.254	udp		Canada	16707		100.64.1.1	02:09:0F:00:04:01	2316	208.91.112.52
10.0.1.254	udp		Canada	16707		100.64.1.1	02:09:0F:00:04:01	2316	208.91.112.53
10.0.1.254	udp	FortiManager	Canada	16707		10.0.1.106	02:09:0F:00:01:03	123	208.91.112.61
10.0.1.254	udp	FortiManager	Canada	16707		10.0.1.106	02:09:0F:00:01:03	37473	208.91.112.52

Delete
Create Device Profiling Rule

Right-click to begin profiling rule creation

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

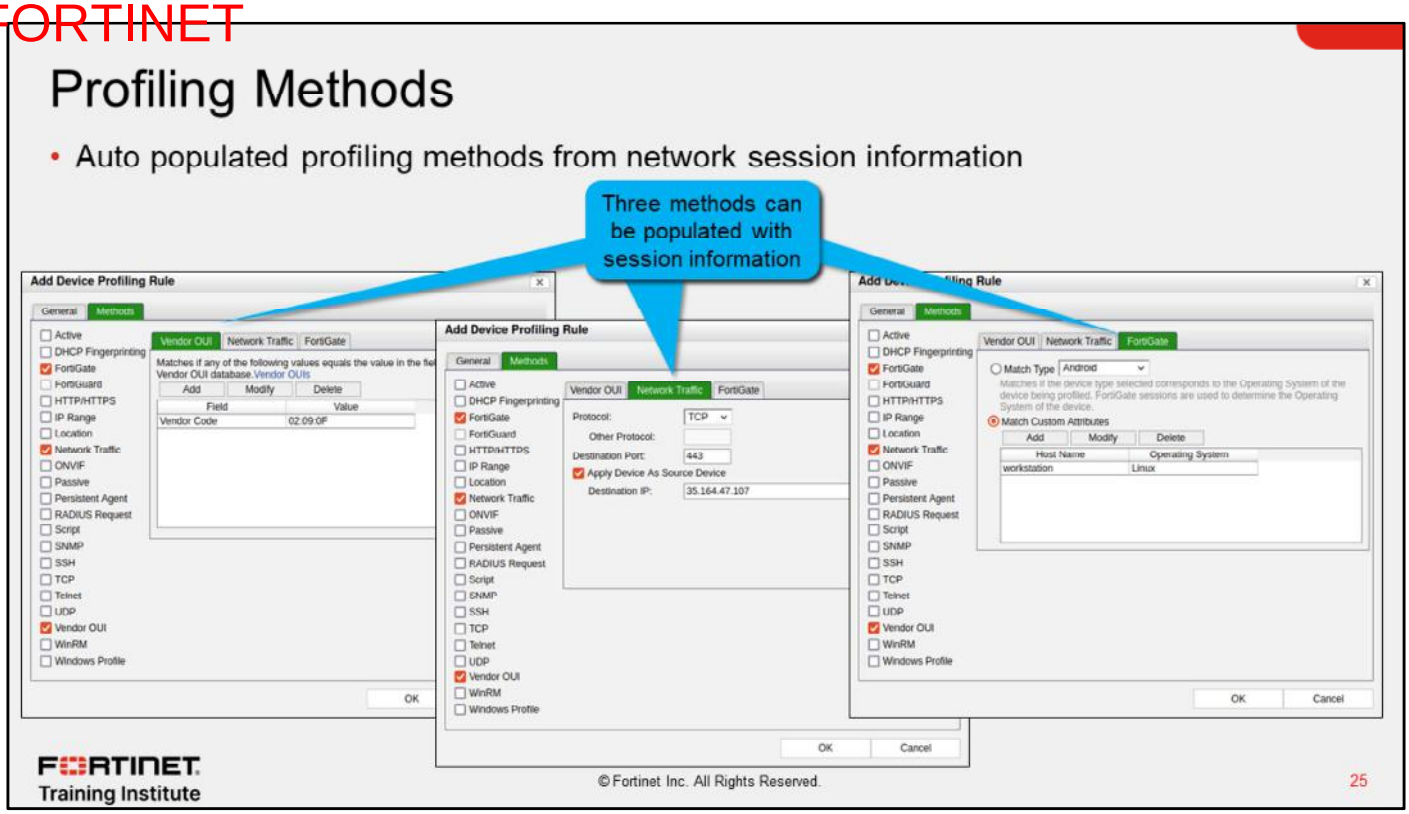
FortiGate session information is pulled and saved based on endpoint models in FortiNAC.

Rogue host records can now be created based upon the presence of the endpoint MAC address in the FortiGate session table or a router ARP table. See FortiGate sessions in the Administration Guide for more information.

The **FortiGate Sessions** view allows you to view endpoint connections and to build profiling rules from the information by selecting an entry and right-clicking and selecting **Create Device Profiling Rule**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

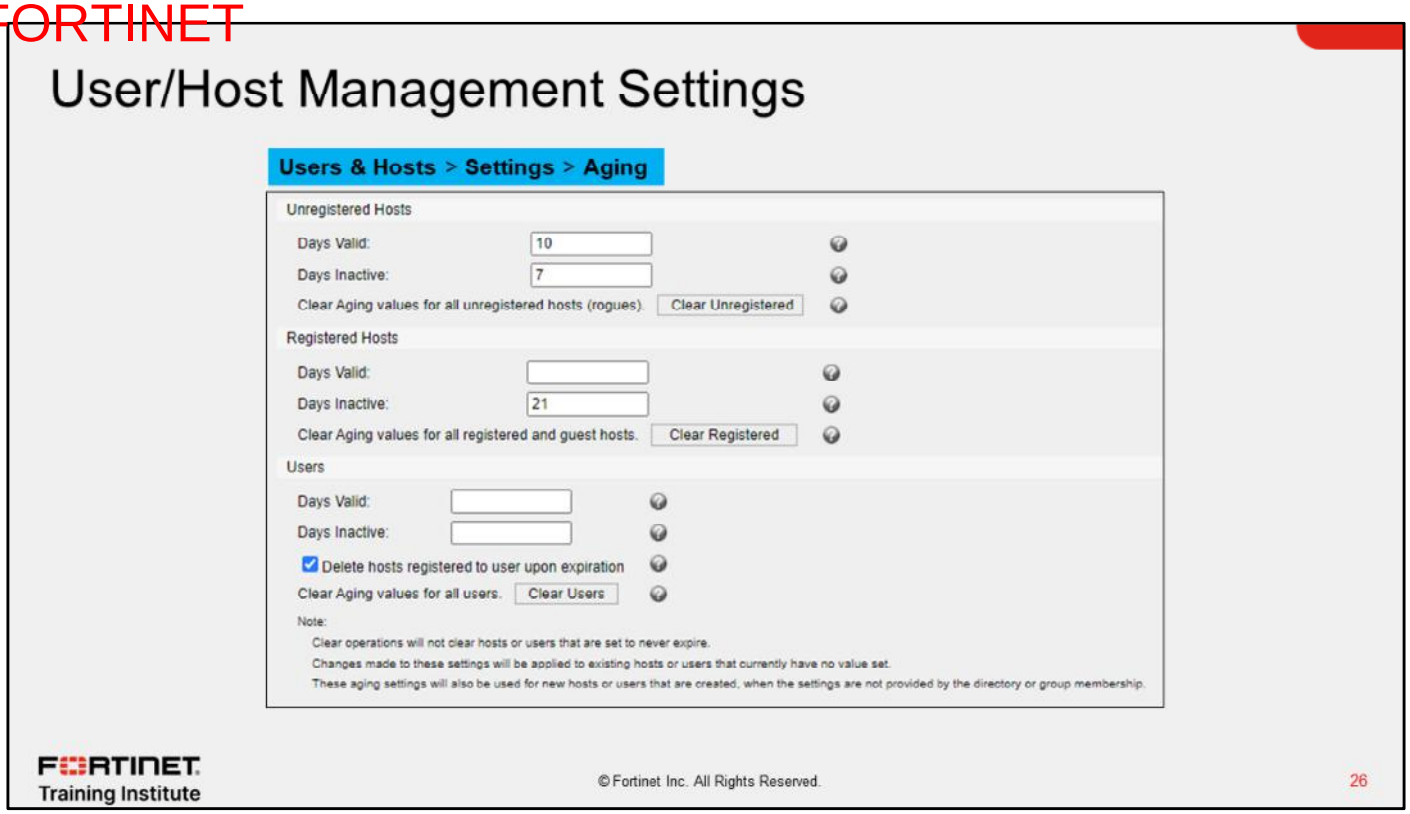


Creating a device profiling rule from a selected session entry will automatically populate the following two device profiling methods:

- **Vendor OUI**: Classify based on the vendor OUI of the adapter.
- **Network Traffic** (network flow): Identify or classify a device based on traffic protocol, application, source IP address or destination IP address.
- **FortiGate**: Classify based on the device type returned by FortiGate or host name.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Aging users and hosts from the database can be an important part of database management. Located under **Users & Hosts** > **Settings**, aging values can be set for three different database elements:

- **Unregistered Hosts**: These settings apply to unknown end points, also called rogues.
- **Registered Hosts**: These settings apply to registered or known endpoints.
- **Users**: These settings apply to users.

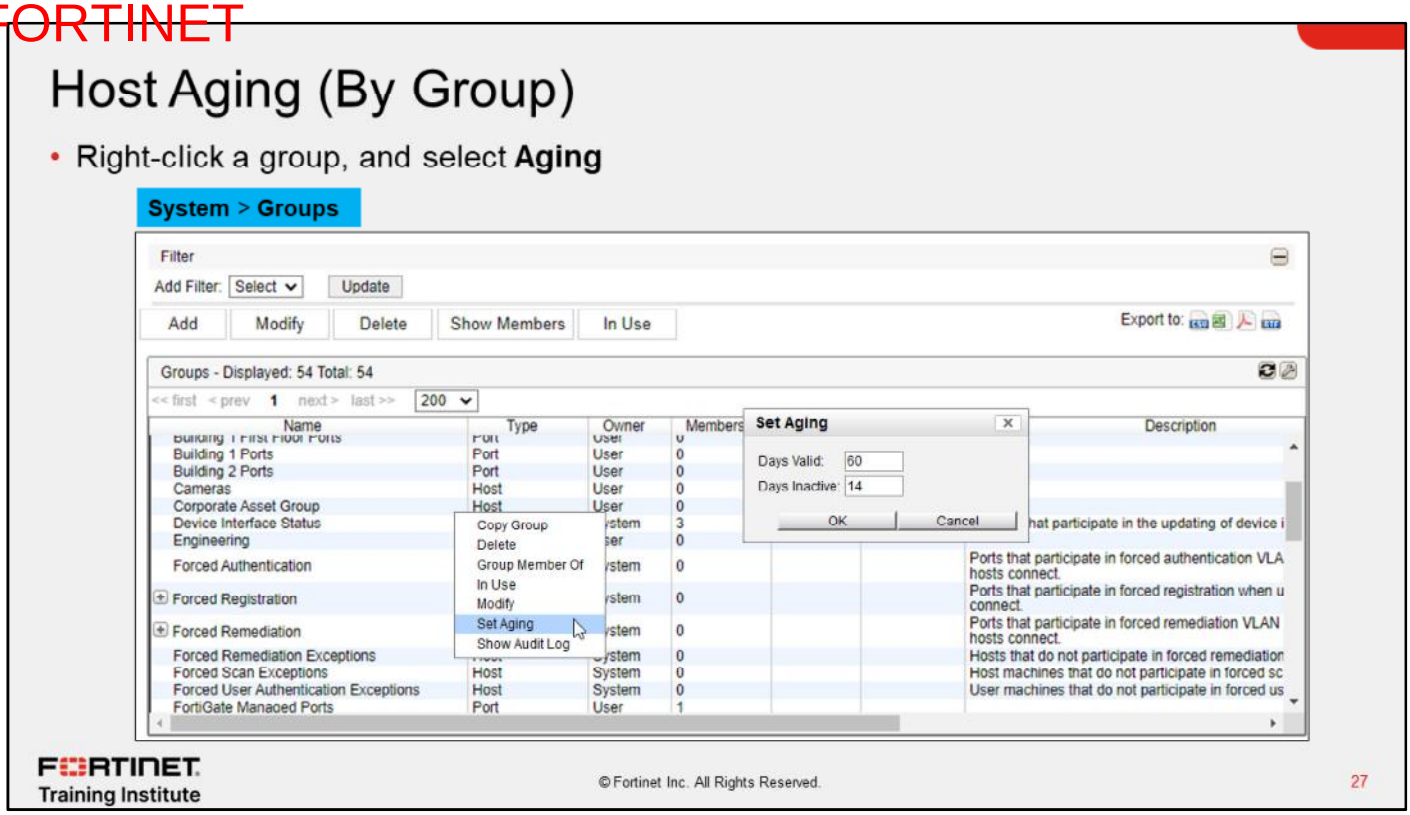
When you apply aging to users, you can remove all hosts that are registered to an expiring user with the user.

The settings for each user are:

- **Days Valid**: Number of days a record remains in the FortiNAC database before it is deleted.
- **Days Inactive**: Number of days a user or host can be inactive before the record is deleted from the database.

Vouchers & Dumps are Available | WhatsApp +201224560923

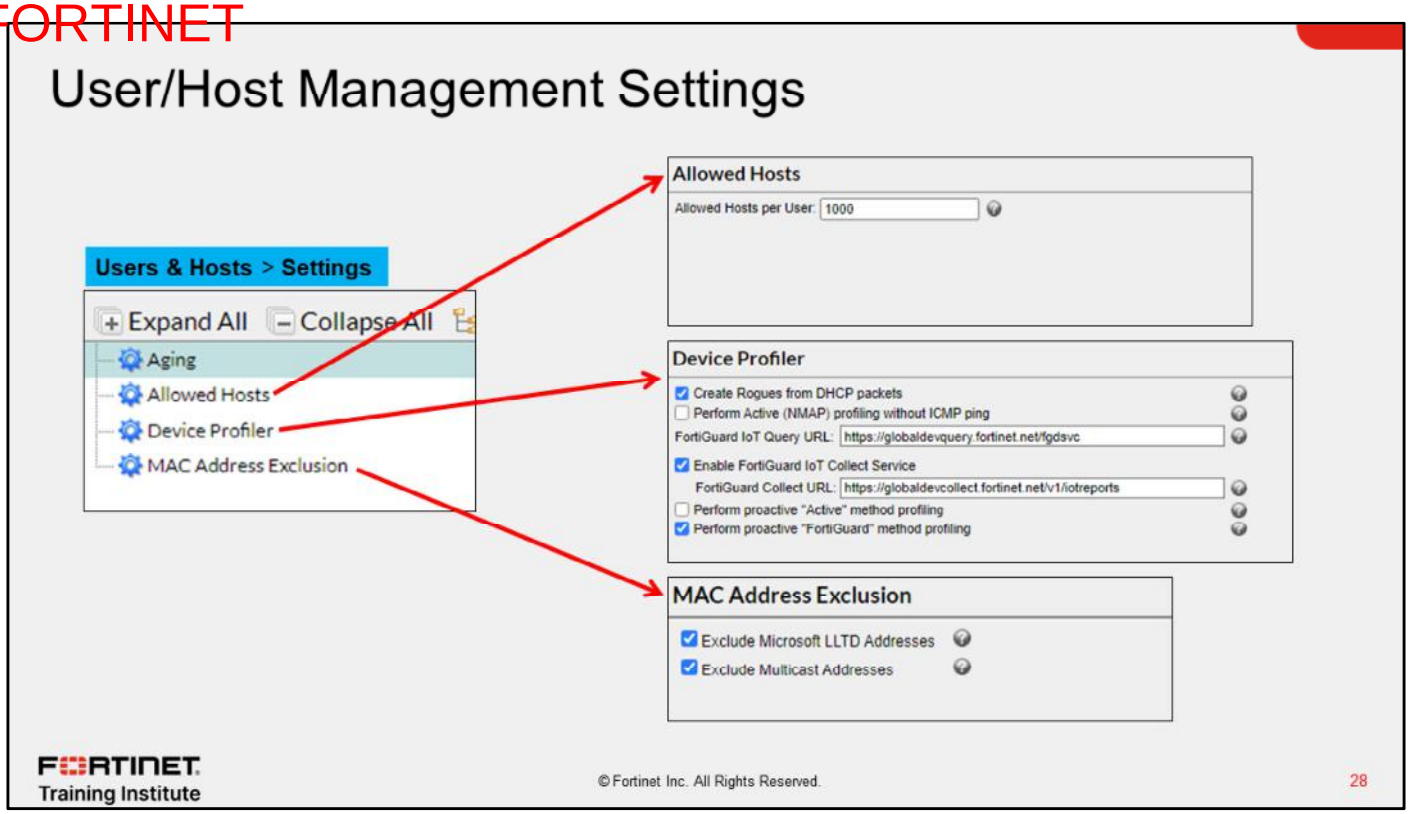
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The same aging settings can be configured on a group-by-group basis. Right-click a host or user group to select the **Set Aging** option. Aging set at a group level overrides the global settings for all members of that group.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



A few other user and host-related settings are located under **Users & Hosts** > **Settings**.

The **Allowed Hosts** settings define the number of registered hosts a single user can have associated with their user account.

The **Device Profiler** settings change the way FortiNAC handles the rogue creation and profiling. **Create Rogues from DHCP packets** will create a rogue host record using information learned from DHCP packets seen on the network, even if the host's point of connection is unknown, such as when a host is connected to a non-modeled switch. The **Perform Active (NMAP) profiling without ICMP ping** setting will configure FortiNAC to perform NMAP scans (active profiling method) without first performing an ICMP ping of the host. The **FortiGuard IoT Query URL** setting defines the URL for the API FortiNAC must query for IoT data. The **Enable FortiGuard IoT Collect Service** configures the feature and URL for FortiNAC to send IoT data it has collected.

The **MAC Address Exclusion** settings configure FortiNAC to do the following when a MAC address that falls within either the Microsoft LLTD or multicast address range connects:

- Creates a Found Microsoft LLTD or Multicast Address event and an alarm alerting the administrator that FortiNAC has seen a Microsoft LLTD or multicast address on the network for the first time. This critical alarm warns administrators that if these addresses should continue to be ignored, they must configure the MAC Address Exclusions list or the MAC addresses will be treated as rogues.
- Sets a timer that expires in 48 hours. While that timer is active, continues to ignore Microsoft LLTD and multicast MAC addresses. Events and alarms continue to be created for each connection from one of these MAC addresses. If the administrator has not configured the MAC Address Exclusions list when the 48-hour timer expires, FortiNAC no longer ignores Microsoft LLTD and multicast MAC addresses. FortiNAC creates rogues for each MAC address that connects, just as it would any other MAC address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Can a quick filter be used to locate a host using a partial MAC address?
   - ✓ A. Yes
   - B. No

2. To find a host based on a partial IP address and an installed application, which filter option would you use?
   - A. Quick filter
   - ✓ B. Custom filter

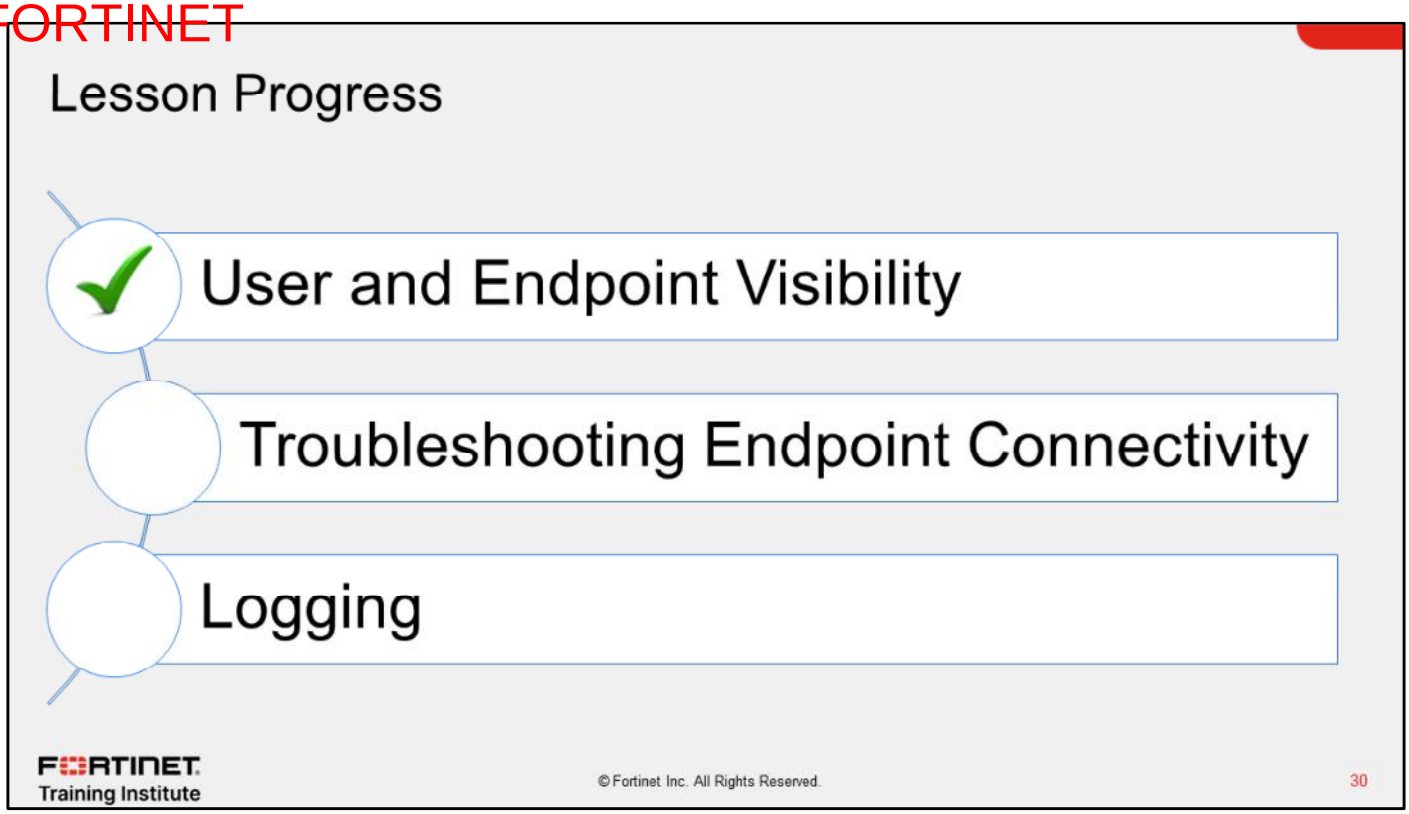
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

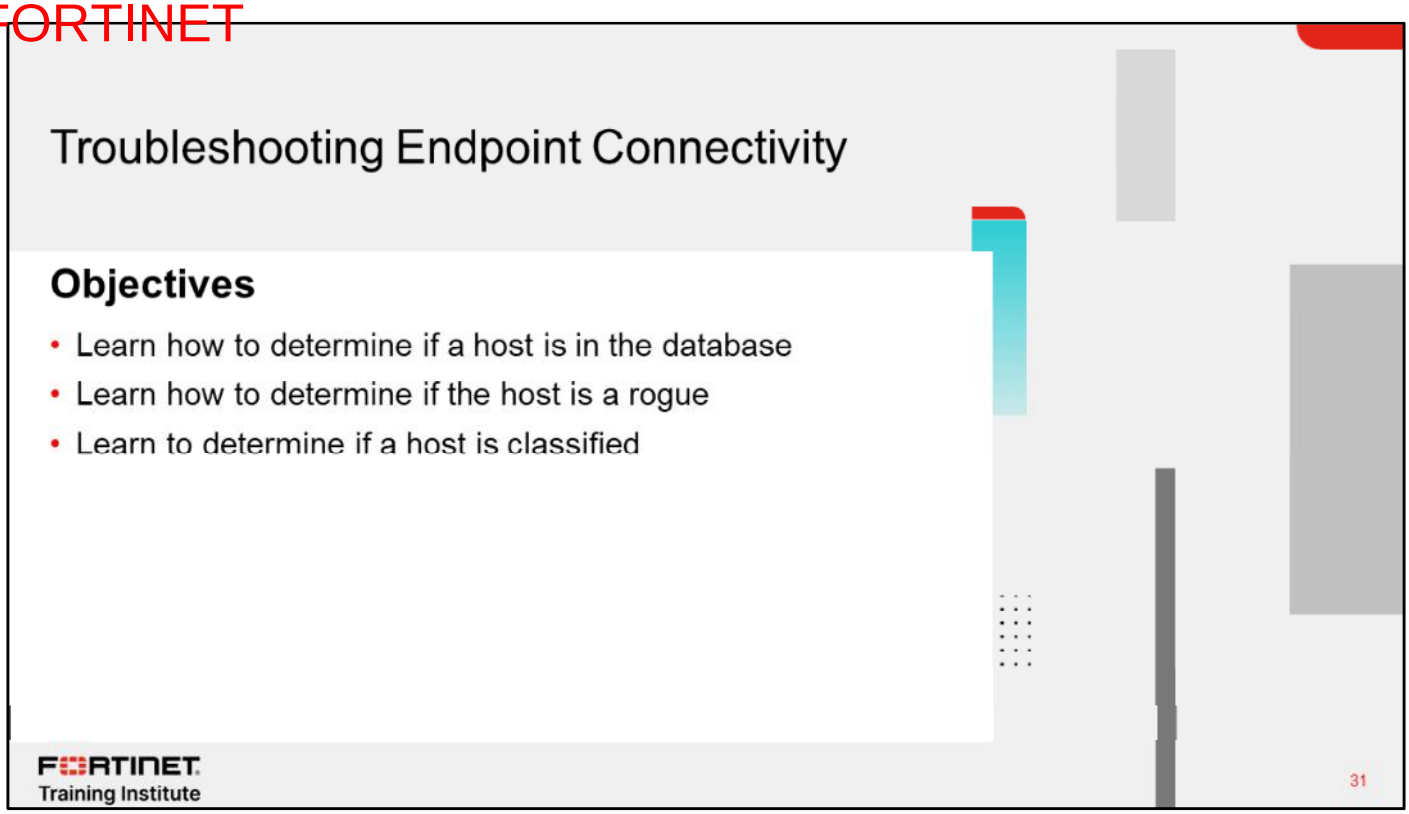


Good job! You now understand user and endpoint visibility, the administrative views dedicated to that visibility, and the management of those users and endpoints.

Now, you will learn about the different logging and reports views available on FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

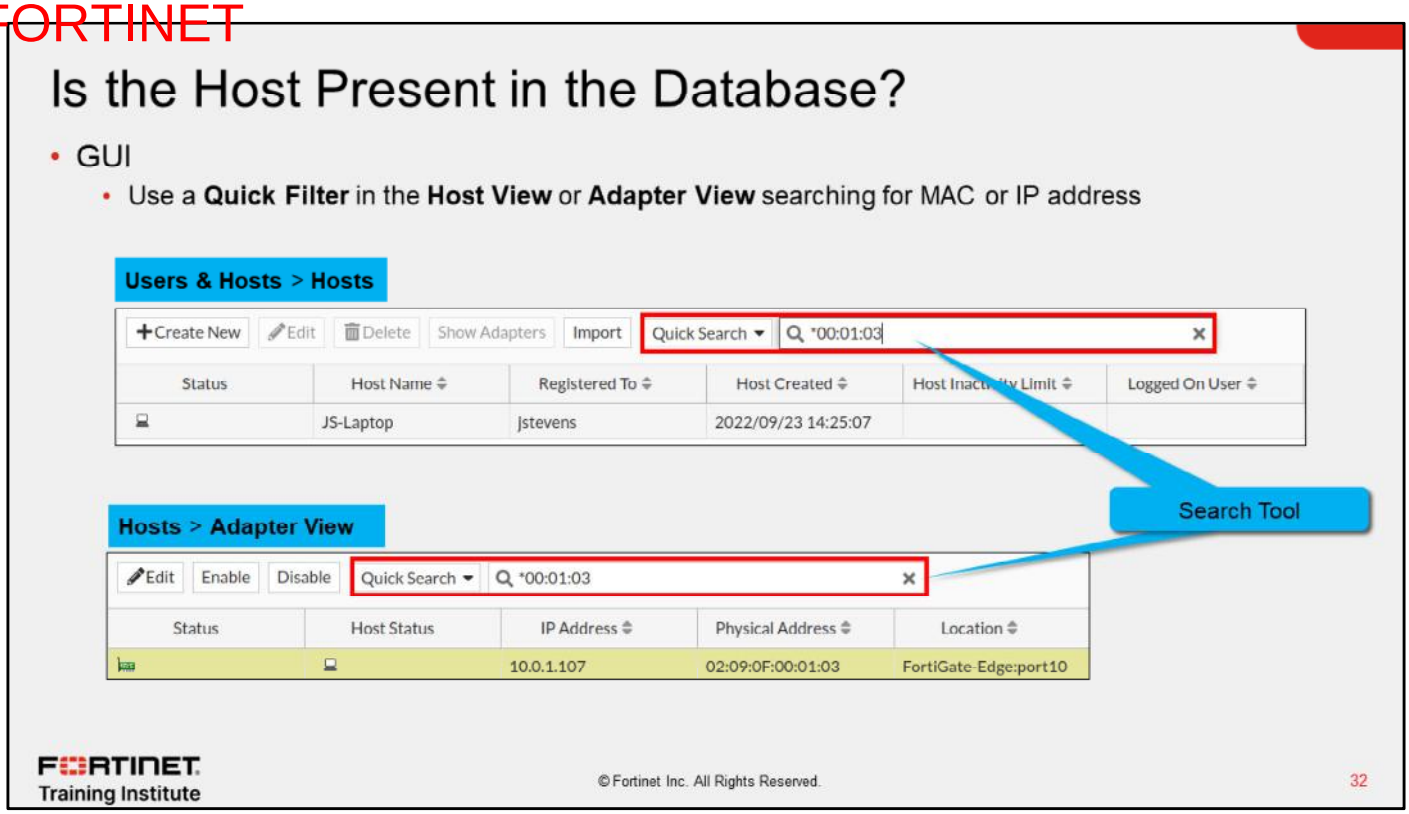


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in basic troubleshooting techniques, you will be able to troubleshoot host connectivity problems in your environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

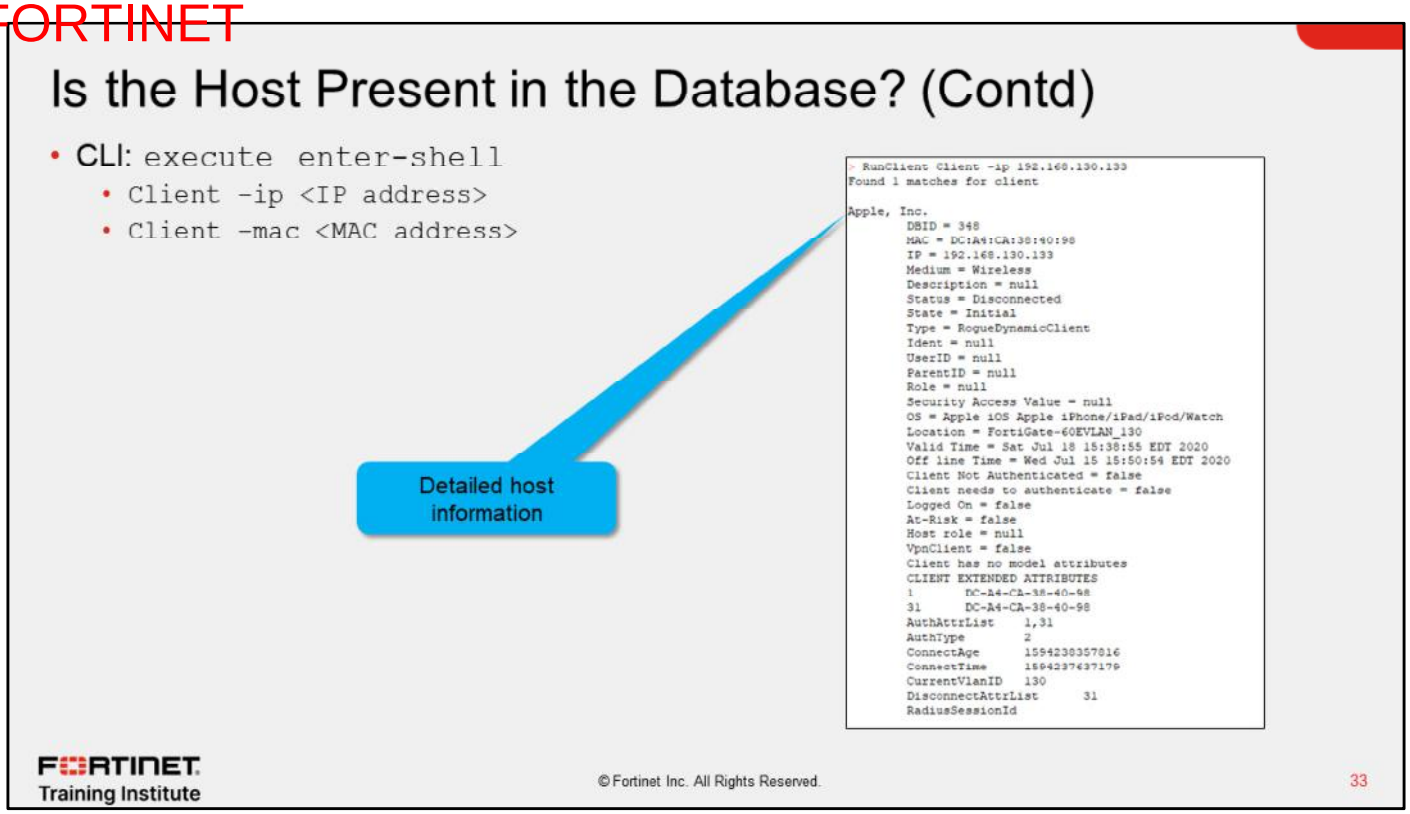
DO NOT REPRINT Brave-dumps.com
© FORTINET



In the example shown on this slide, the host record is found using the **Quick Search** tool and a partial MAC address in both the hosts and adapters views. Any of the filtering capabilities can be used for locating the host or adapter.

Vouchers & Dumps are Available | WhatsApp +201224560923

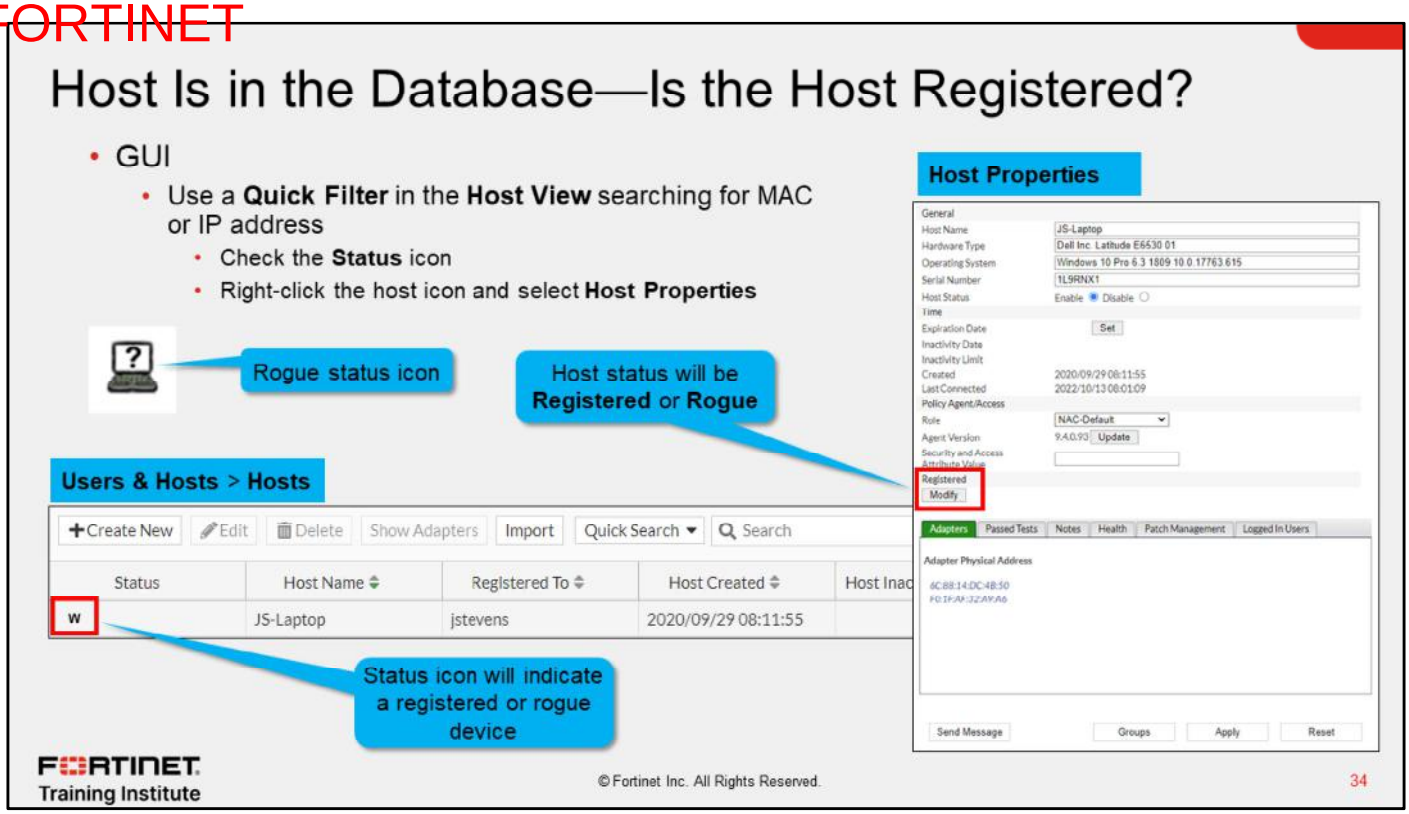
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Using the CLI, you can use the commands shown here to determine if there is a matching host record in the database.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



If the host is present in the database, you can look at the icon in the hosts view to determine if the host is a rogue. You can also access the **Host Properties** view. If the host is registered, the page section bar will be labeled **Registered**, and the button just bellow will be labeled **Modify.** If the host is a rogue, the page section title bar will be labeled **Rogue,** and the button label will be **Register**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Host Is in the Database—Is the Host Registered? (Contd)

- CLI: `execute enter-shell`
  - `Client -ip <IP address>`
  - `Client -mac <MAC address>`
- Check the `Type` field

```
> RunClient Client -mac 6C:88:14:DC:4B:50
Found 1 matches for client

DESKTOP-FHS1QIU
        DBID = 17
        MAC = 6C:88:14:DC:4B:50
        IP = 192.168.150.10
        Medium = Wireless
        Description = Intel(R) Centrino(R) Advanced-N 6205
        Status = Connected
        State = Initial
        Type = DynamicClient
        Ident = null
        UserID = null
        ParentID = 357
        Role = NAC-Default
        Security Access Value =
        OS = Windows 10 Pro 6.3 1809
        Location = FortiGate-60EVLAN_150
        Client Not Authenticated = false
        Client needs to authenticate = false
        Logged On = false
        At-Risk = false
        Host role = NAC-Default
        VpnClient = false
```

Type designated as `DynamicClient` is registered

Type designated as `RogueDynamicClient` is not registered

```
> RunClient Client -ip 192.168.130.133
Found 1 matches for client

Apple, Inc.
        DBID = 348
        MAC = DC:A4:CA:38:40:98
        IP = 192.168.130.133
        Medium = Wireless
        Description = null
        Status = Disconnected
        State = Initial
        Type = RogueDynamicClient
        Ident = null
        UserID = null
        ParentID = null
        Role = null
        Security Access Value = null
        OS = Apple iOS Apple iPhone/iPad/iPod/Watch
        Location = FortiGate-60EVLAN_130
        Valid Time = Sat Jul 18 15:38:55 EDT 2020
        Off line Time = Wed Jul 15 15:50:54 EDT 2020
        Client Not Authenticated = false
        Client needs to authenticate = false
        Logged On = false
        At-Risk = false
        Host role = null
        VpnClient = false
        Client has no model attributes
        CLIENT EXTENDED ATTRIBUTES
        1       DC-A4-CA-38-40-98
        31      DC-A4-CA-38-40-98
        AuthAttrList    1,31
        AuthType        2
        ConnectAge      1594238357816
        ConnectTime     1594237637179
        CurrentVlanID   130
        DisconnectAttrList      31
        RadiusSessionId
```

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

35

The example shown on this slide uses CLI to determine the status (rogue or registered) of a host. A host with a `Type` value of `DynamicClient` is a registered host. A host with a `Type` value of `RogueDynamicClient` is not registered.

Vouchers & Dumps are Available | WhatsApp +201224560923

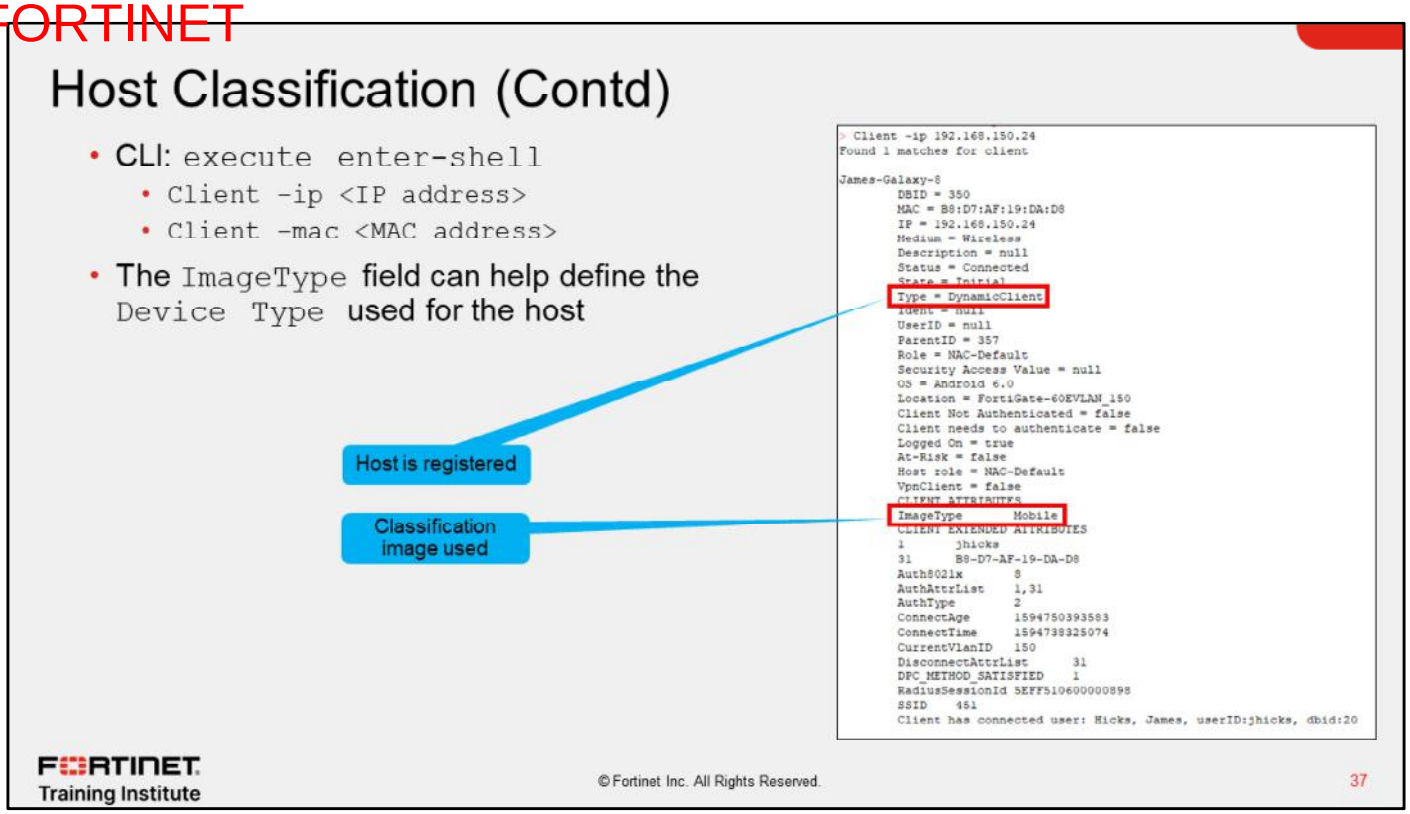
DO NOT REPRINT
© FORTINET
Brave-dumps.com



A host that has been classified (registered) will have an icon in the **Status** field of the **Host View** associated with the device type set for the host. The example shown on this slide depicts a host that has been classified as a mobile device and the icon associated with that device type.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can also obtain host classification information using the CLI commands shown on this slide. The command output displays `Type` and `ImageType` information. The example shown on this slide is a registered host classified as a mobile device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When using the CLI command `client -mac <MAC address>` what would be the `Type` value for a registered host?
   A. RegisteredHost
   ✓ B. DynamicClient

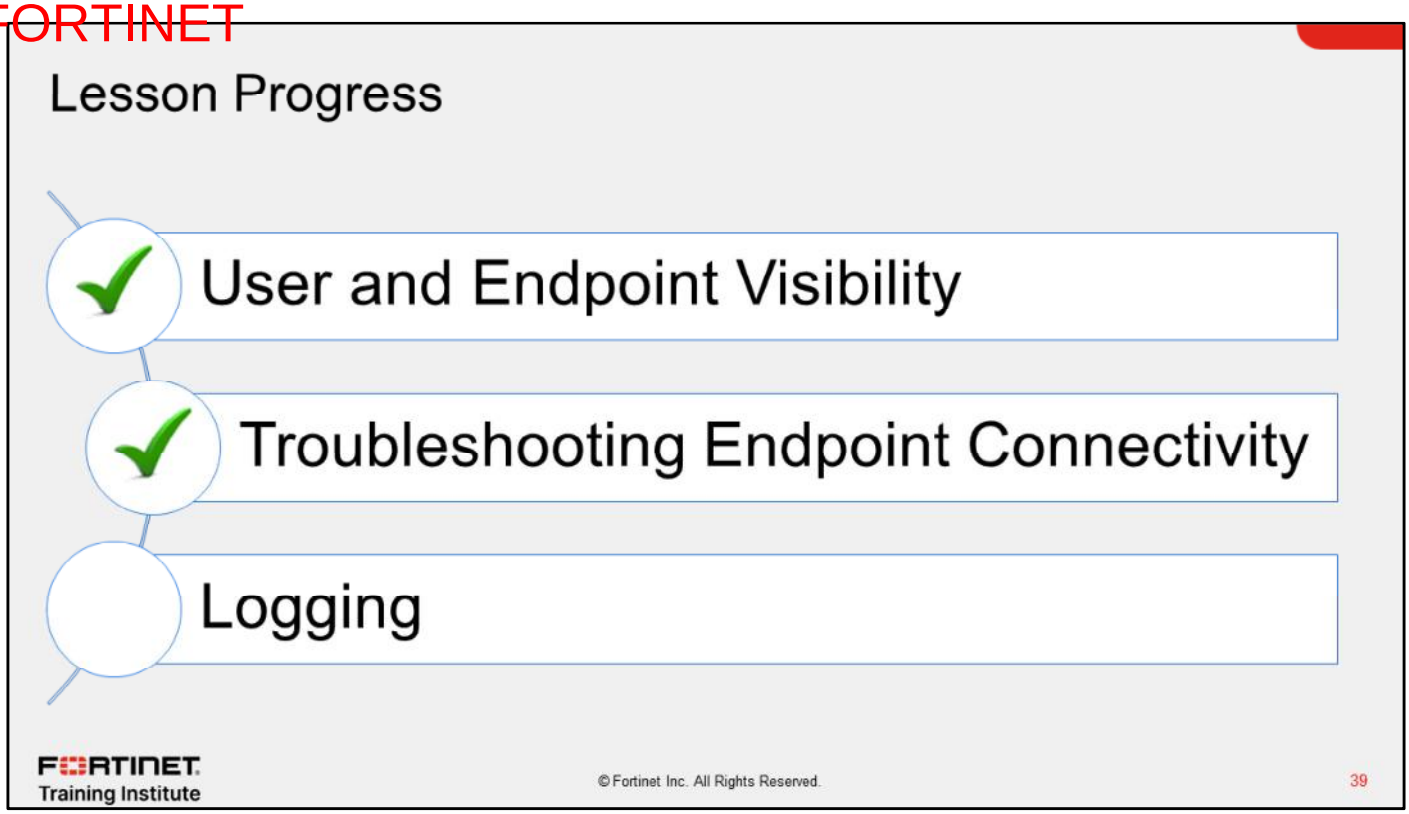
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

38

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

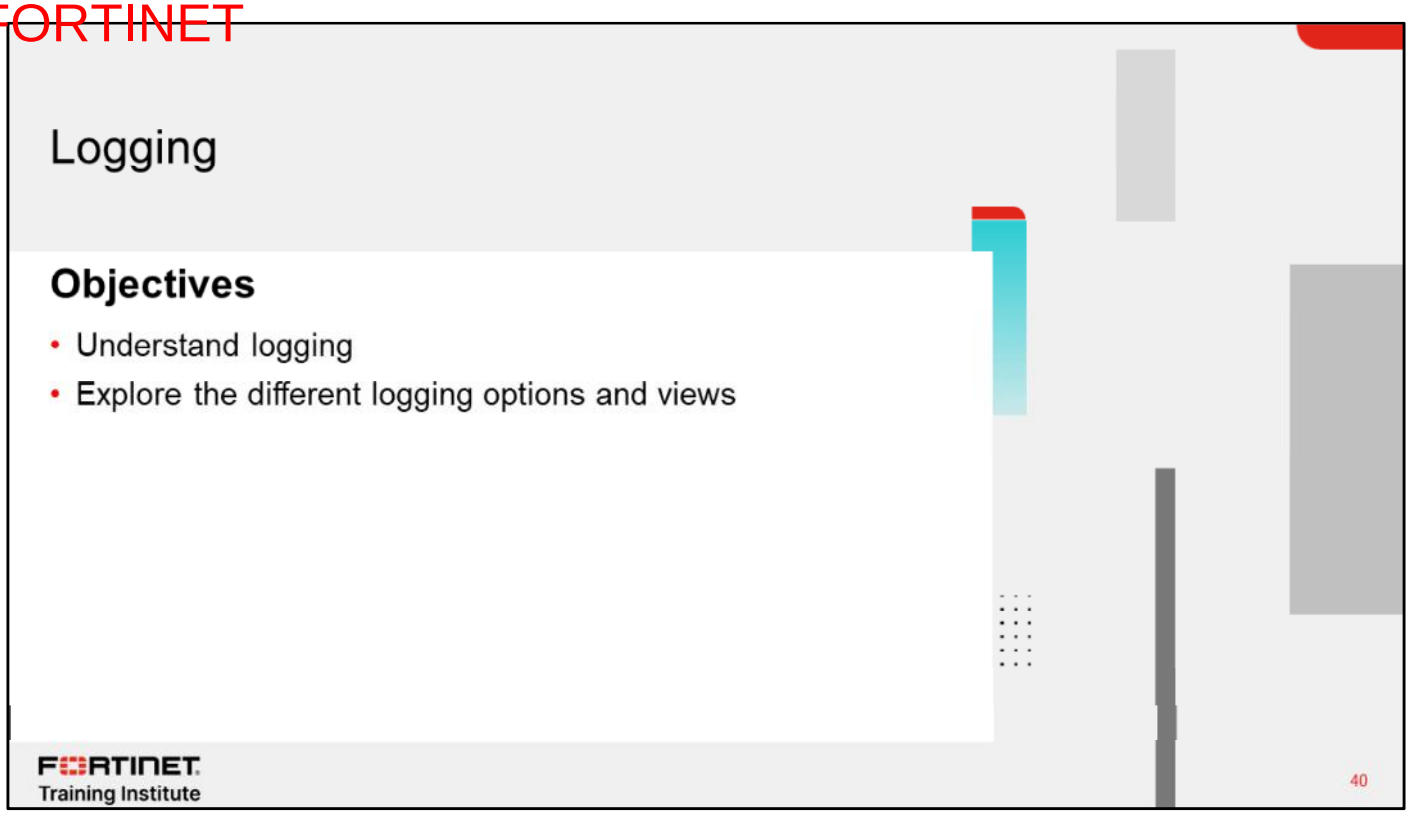


Good job! You now understand how to troubleshoot endpoint connectivity issues using the FortiNAC GUI or CLI.

Now, you will learn about the different logging and reports views available on FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

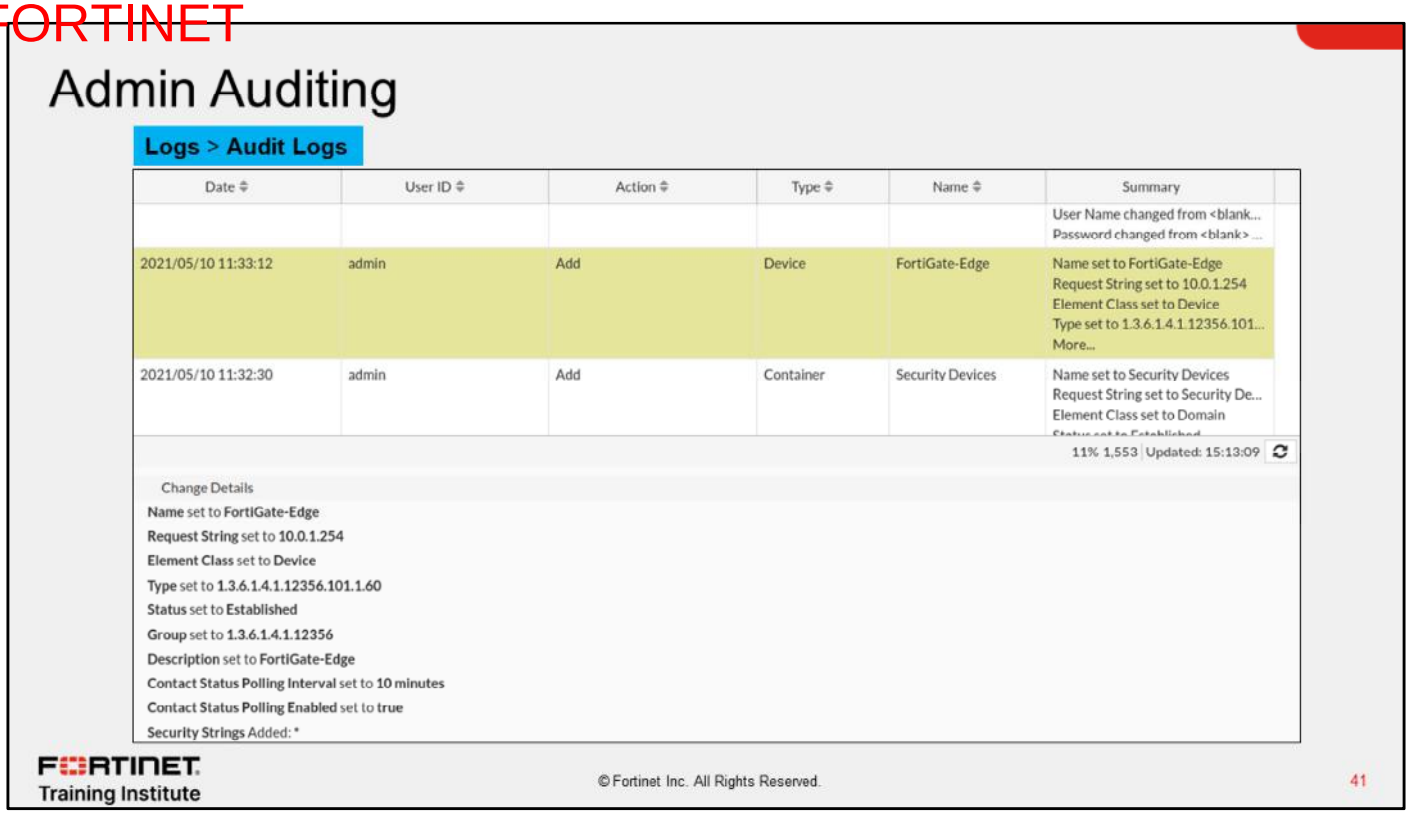


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in viewing, using, and understanding logs, you will be able to use logs to better understand and solve issues in your network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



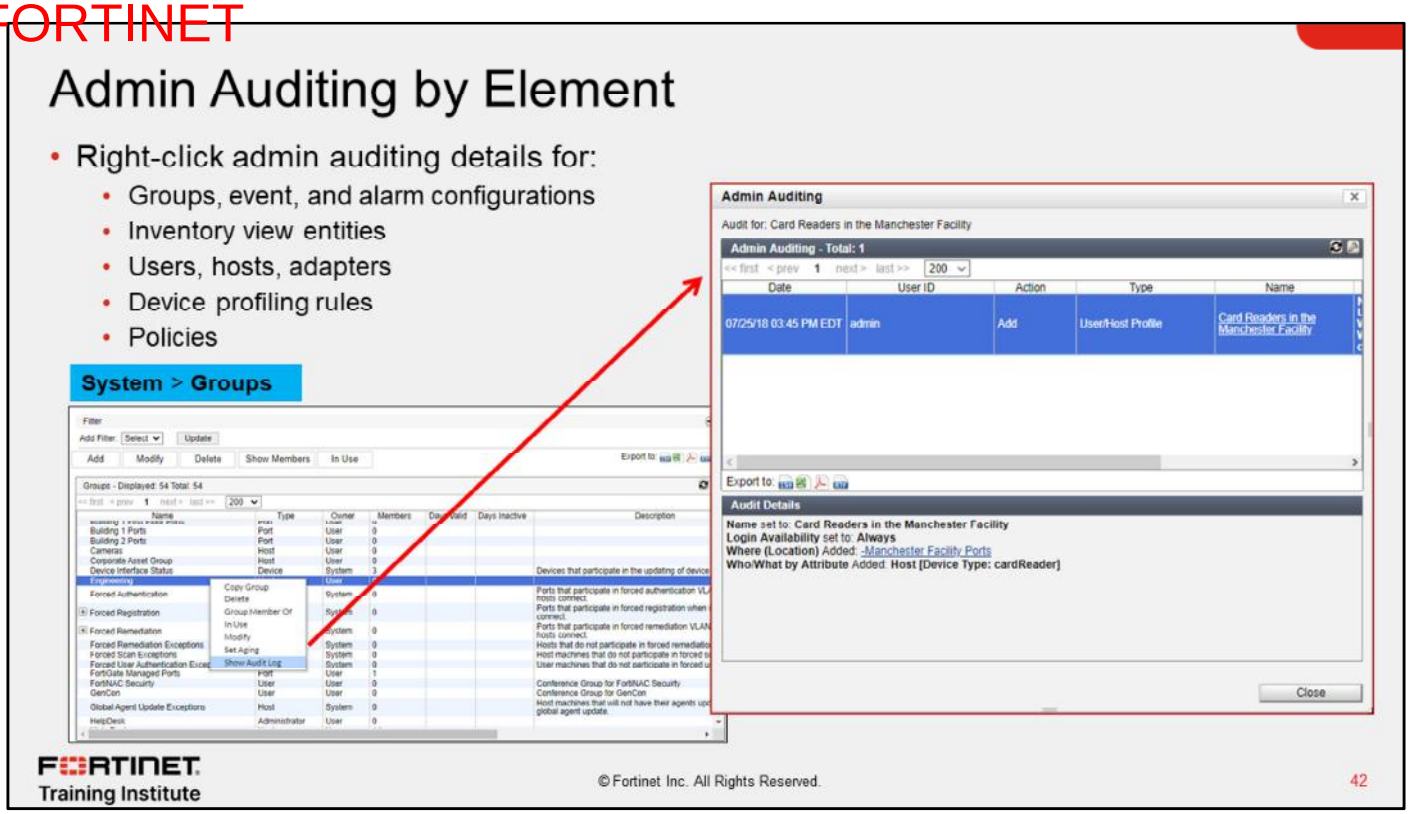
The ability to track changes made to a system by administrative users can be vital.

The admin auditing log, located under **Logs** > **Audit Logs**, tracks all changes made to an item in the system. Users with admin auditing permissions will see a change in the admin auditing log whenever data is added, modified, or deleted. Users can see what was changed, when the change was made, and who made the change. Changes can be filtered by the name of the item that was changed, the action taken, the date when the change occurred, the user ID for the user who made the change, and the type of item that was changed.

Changes made through the CLI are also tracked in the admin auditing log; however, the user ID for the user who made the change will appear as **CLI Tool**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In addition to the admin auditing view located under **Logs** > **Audit Logs**, administrative users with the appropriate permissions, can access admin auditing information directly from elements within the GUI.

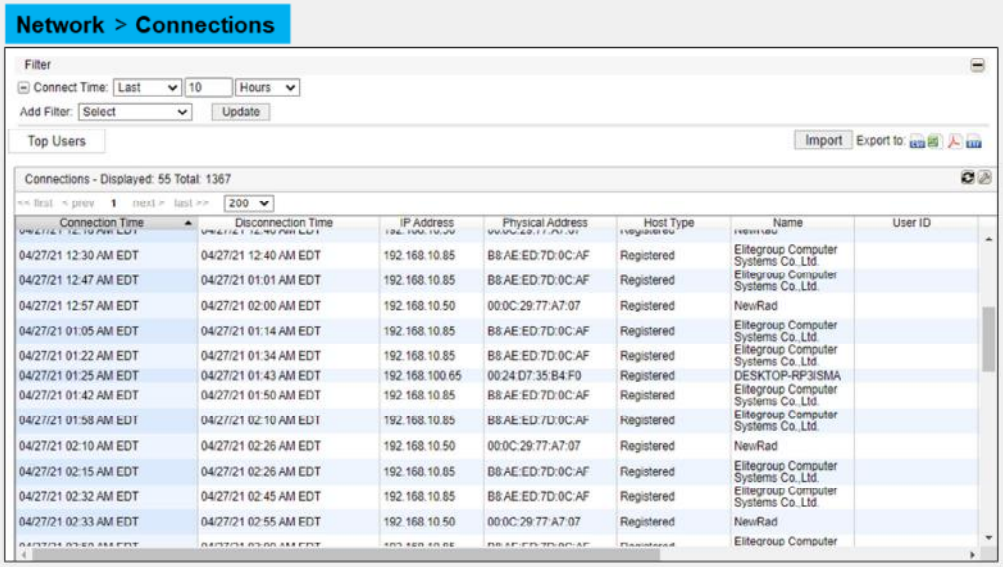
By right-clicking a supported element type, such as groups, alarms and events, inventory view components, users, hosts, adapters, device profiling rules, and security policies, the administrative user can view a prefiltered admin auditing log displaying changes made to only that particular element. This tool quickly identifies who made a change and when.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Connections

- Historic connection information for each host



FORTINET Training Institute

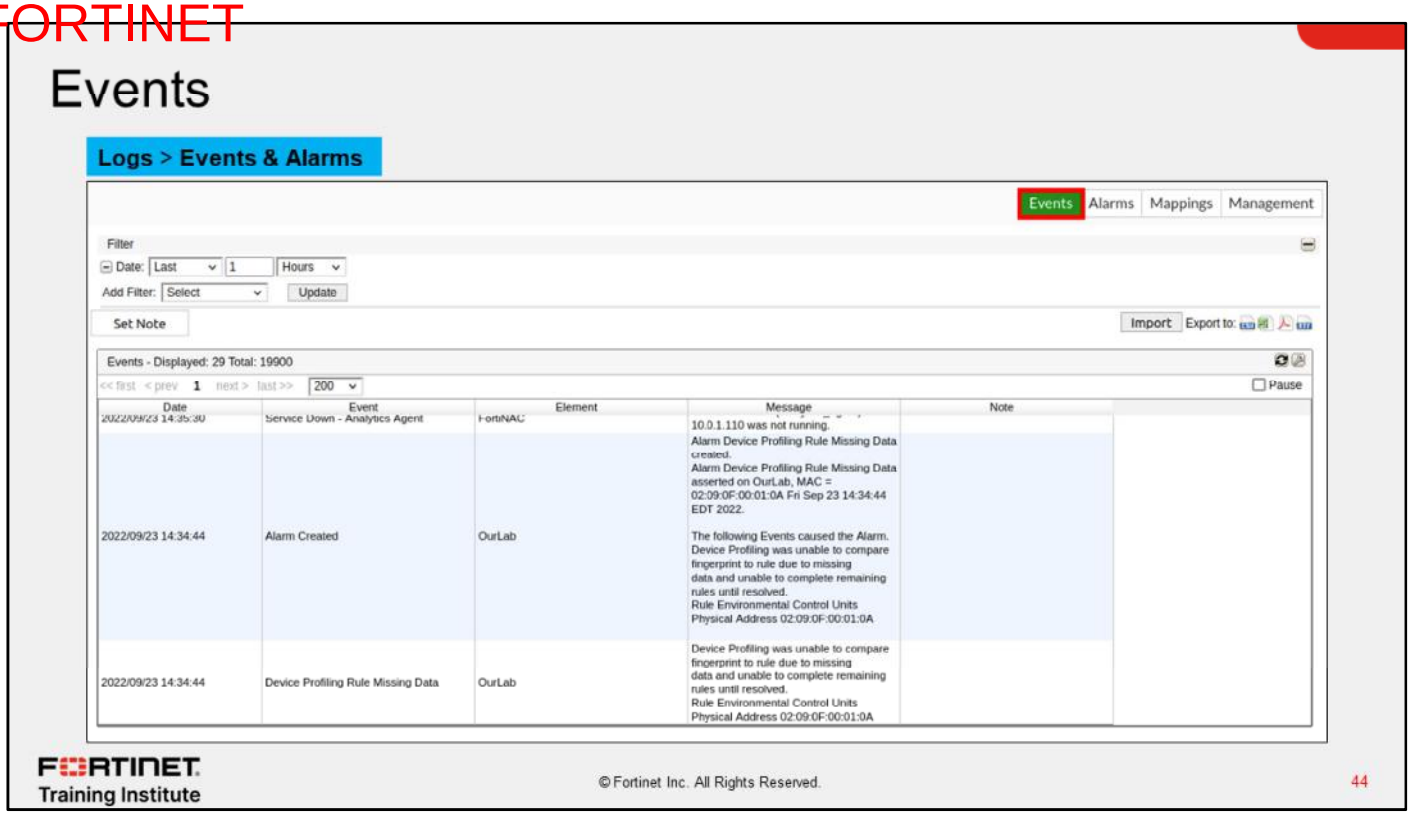
© Fortinet Inc. All Rights Reserved.

43

The **Connections** view, displays the contents of the connection log. The connection log contains a list of historical host and user connections to the network. Each time a host or user comes online, a connection record is started. When that host or user goes offline, the connection record is completed. The information contained in the log includes date and time of the connection and disconnection, the user ID (available with user tracking), the owner ID (BYOD devices), host name, physical address, and MAC address. The filter tool allows for specific searches based on any of the displayed criteria, providing information centered around who, what, where, and when. For example, you can quickly determine what host had a particular IP address at a particular date and time and where that host was connected. Connection data that is older than the defined database archive age time is removed from the database (and subsequently, the view), and stored to file each time the **Purge Events** task runs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

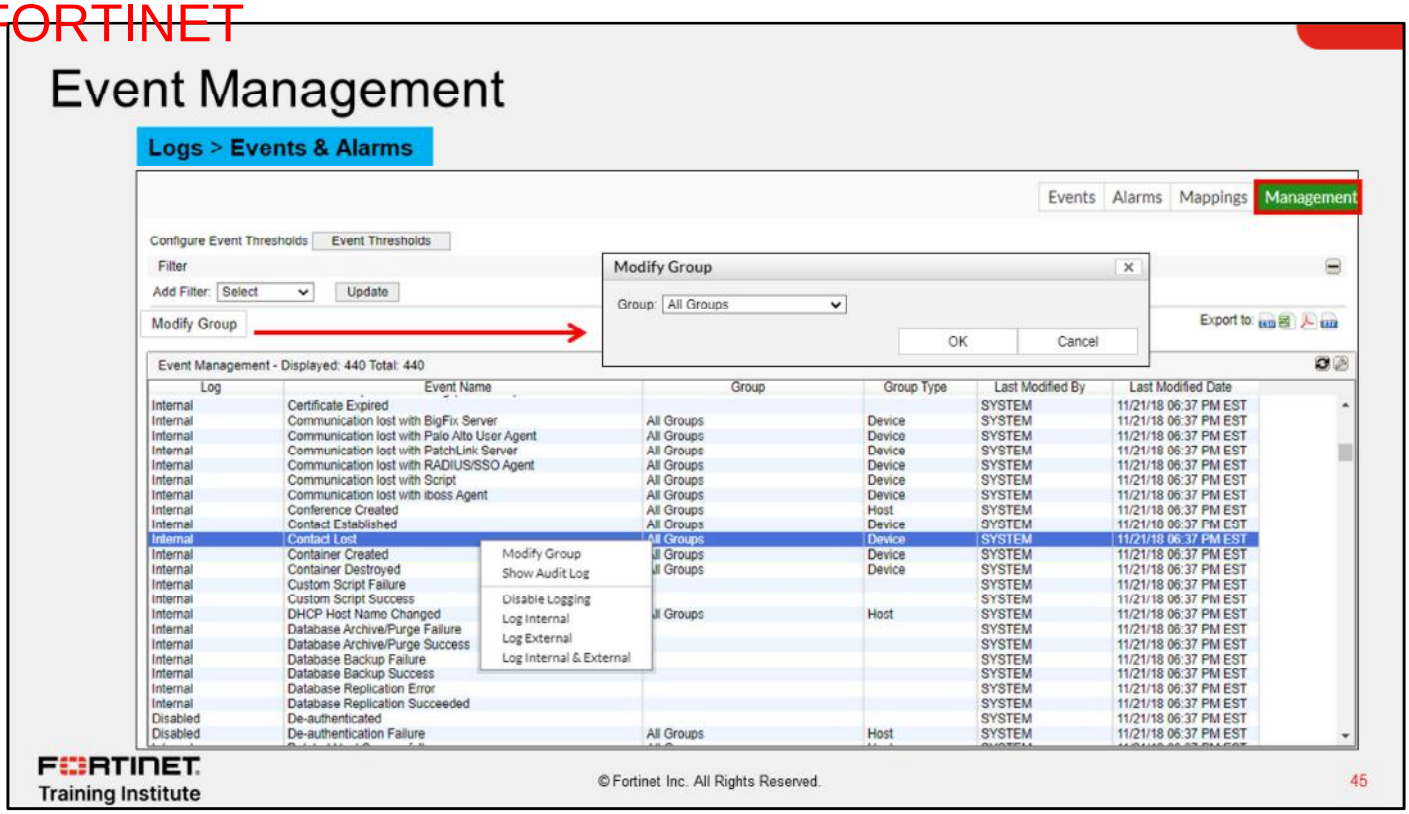


The **Events** view is accessed from **Logs** > **Events & Alarms** and displays the contents of the events log. The events log is an audit trail of significant network and FortiNAC incidents. Events are logged when they are enabled in the events **Management** view. These events can provide important details to an administrator about the FortiNAC device, or the environment it's deployed in. There are more than 400 events that can be generated on current FortiNAC servers. Event information includes the date and time the event was generated; the element, such as the host, device or user that caused the event to be generated; and the specific event message. Notes can be added to any event by an administrative user, and events can be exported.

There is a filter tool in the upper-left of the event log to assist in quickly locating logged events.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **Management** view is accessed from **Logs** > **Events & Alarms**. Event management allows you to specify which of the more than 400 available events to generate, and whether to log the event records on another server, in addition to the local appliance.

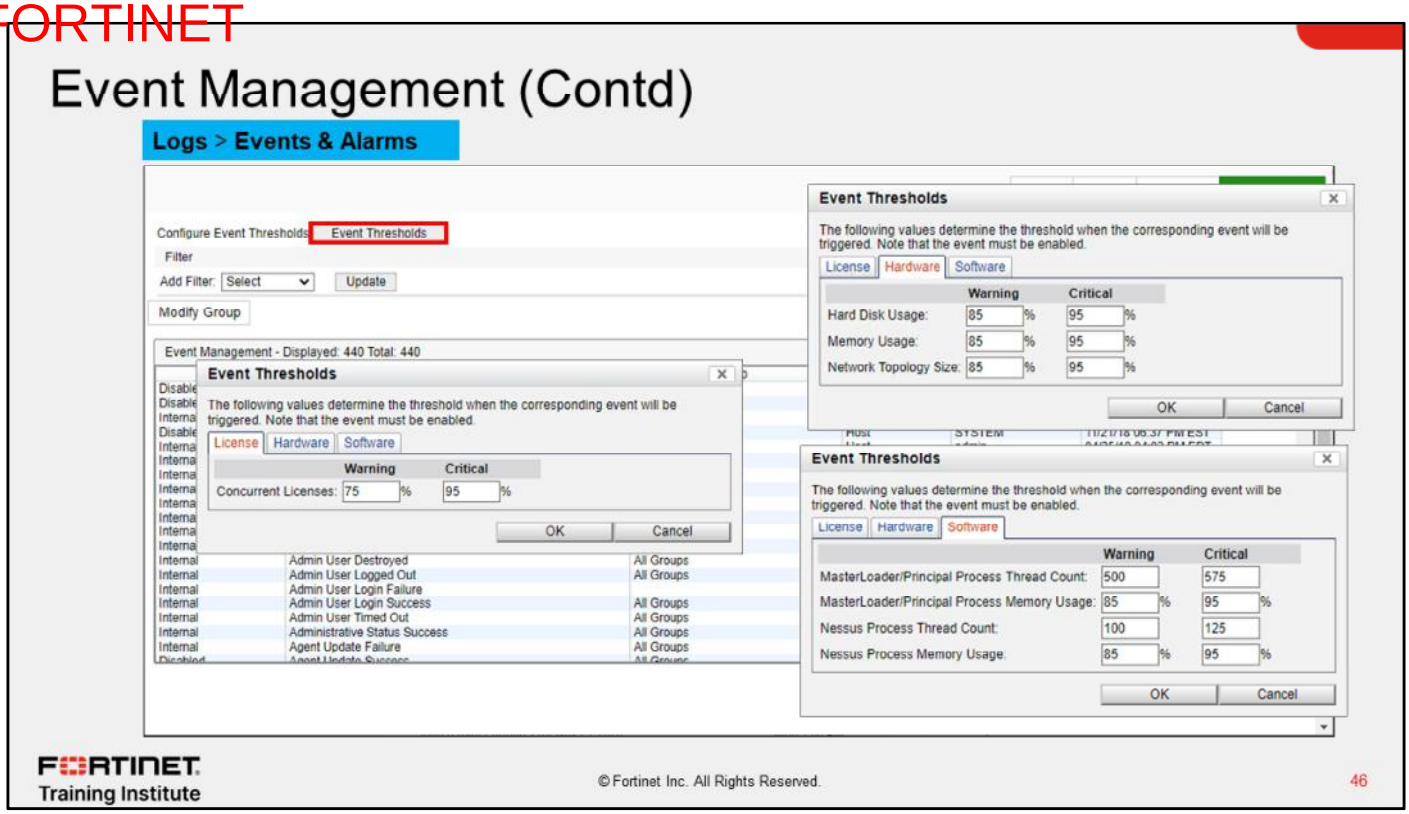
Right-click one or more events to set the logging designation for a selected event, and access the following options:

- **Disable Logging**: The event will not be generated.
- **Log Internal**: The event will be logged only to the FortiNAC event view.
- **Log External**: The event will be logged to external systems defined on the **Log Receivers** settings page.
- **Log Internal and External**: The event will be logged in both the FortiNAC event view and the designated external systems.

You can limit the number of events generated by selecting a group for each event. Event messages are created only when the event is generated by an element within the specified group. This feature is commonly used to locate missing assets. For example, the **Host Connected** event could be configured to generate only when the connecting host is a member of a specific host group, such as a group called **Missing Assets**. The event will include the point of connection for the host.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



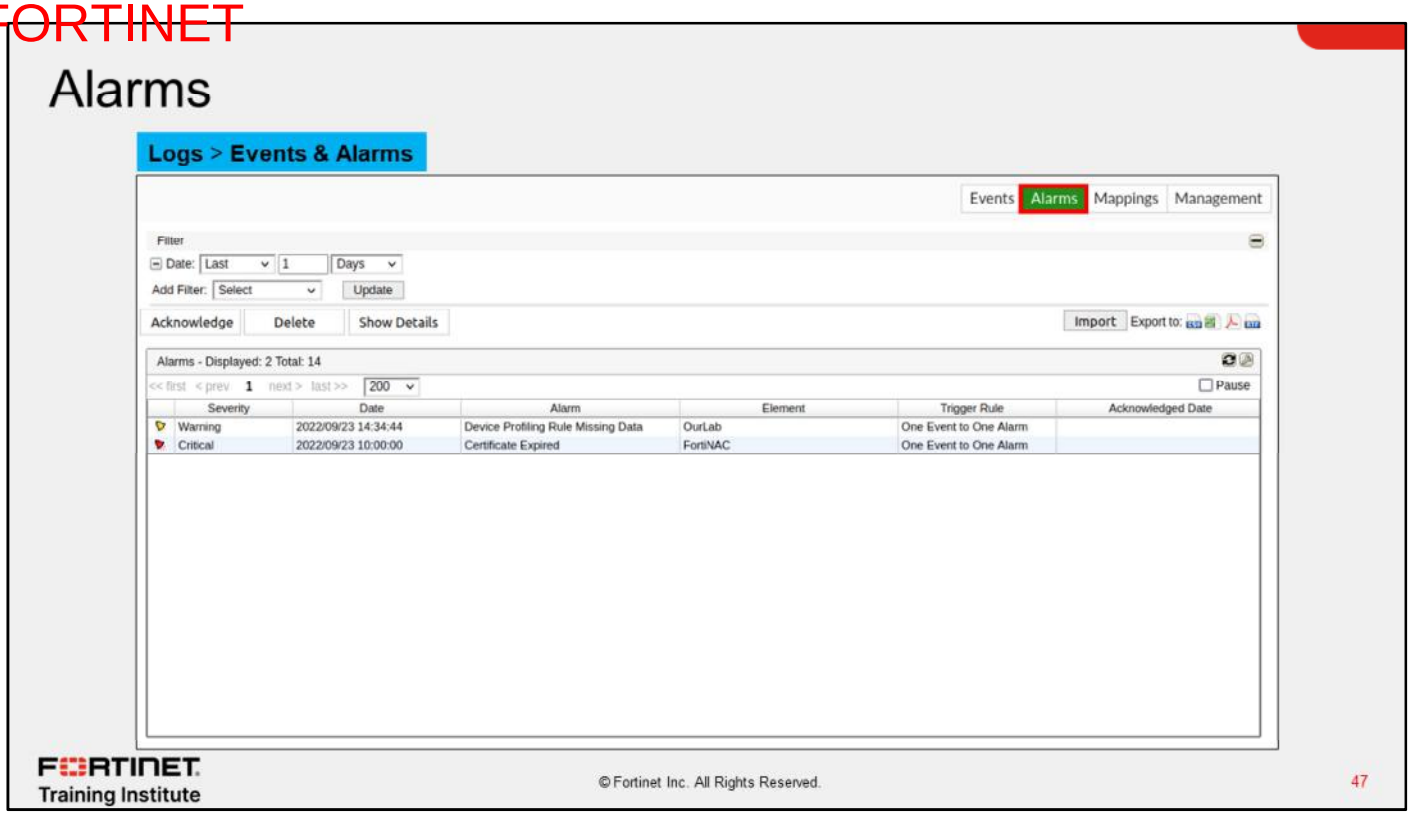
Specify threshold values for self-monitoring events by clicking **Event Thresholds**. The different types of thresholds are displayed on these three tabs:

- **License**: This tab displays warning and critical threshold values for the current license usage thresholds.
- **Hardware**: This tab displays warning and critical threshold values for hardware-specific parameters, such as hard disk usage and memory usage.
- **Software**: This tab displays warning and critical threshold values for software-specific parameters, such as specific process thread counts or memory usage.

These thresholds affect the **Performance** panel on the **Dashboard**. You can edit them here or from the **Performance** panel. Some events are generated frequently and may not be necessary for day-to-day operations. Review the list of events and determine which ones to enable to provide you with the most useful feedback.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Alarms** view is accessed from **Logs** > **Events & Alarms**. The **Alarms** view is used to view and manage the contents of the alarm log, which is a list of all current alarms. Alarms are generated as a result of an event being generated, so every alarm that is generated has a trigger event that was mapped to generate the alarm.

You will learn more about how these events are mapped in this lesson. The alarm view can display the following information about an alarm:

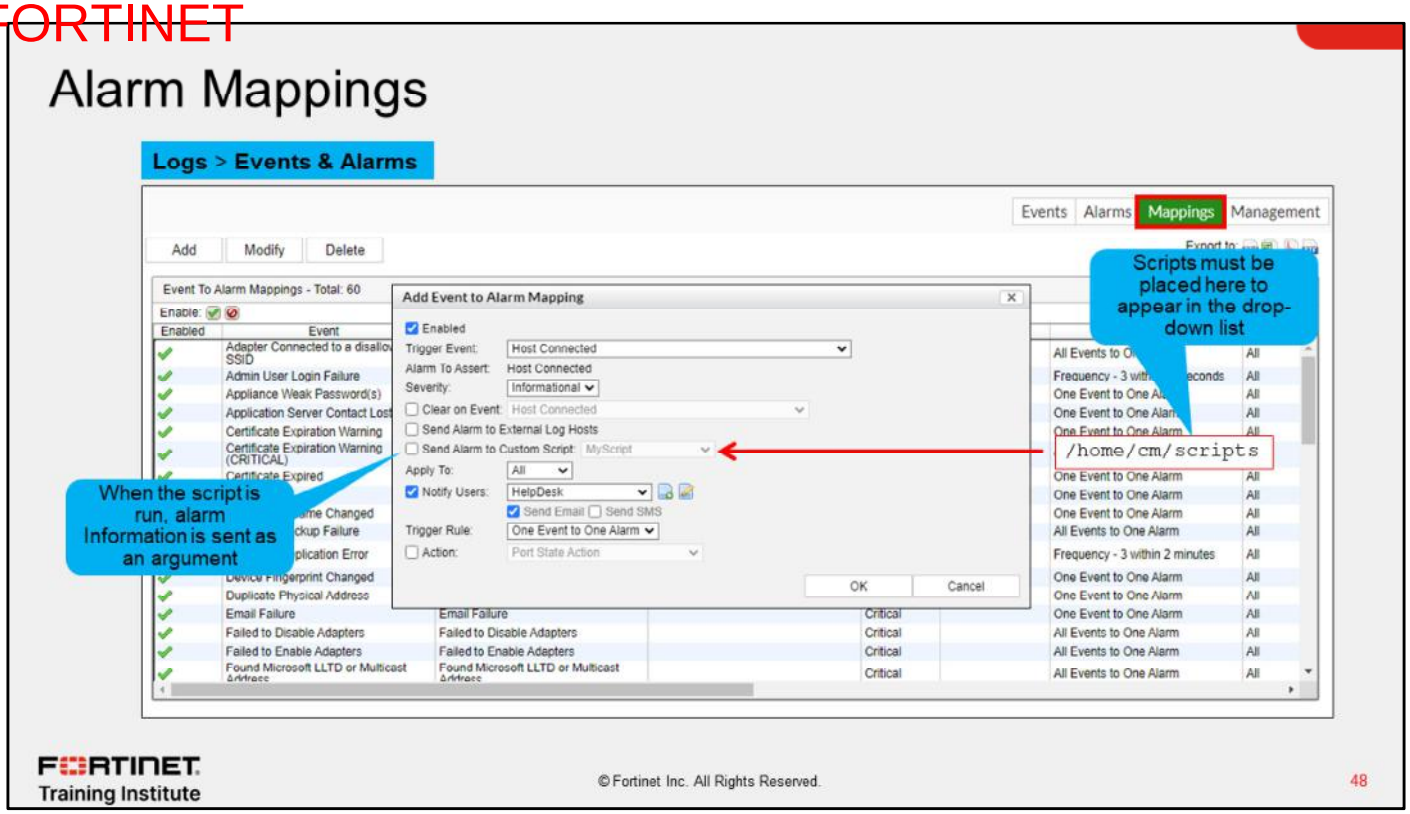
- **Severity**: Indicates how serious the alarm is. Severity levels include: critical, minor, warning, and informational.
- **Date**: The date and time the alarm was generated.
- **Alarm**: The alarm listed by name.
- **Element**: The device, administrative user, server, or process that triggered the event that generated the alarm.
- **Trigger Rule**: The rule that determines the conditions under which an alarm is triggered based on an event. The options are: **One Event to One Alarm**, **All Events to One Alarm**, **Event Frequency**, and **Event Lifetime**. These options are detailed on the *Alarm Mappings* slide.
- **Acknowledge Date**: The date and time an alarm was acknowledged, if an administrator has chosen to acknowledge the alarm.

Alarms can be removed from the log in two ways:

- Manually: when an administrative user selects an alarm and clears it using the right-click menu or the button above the alarm list.
- Automatically: when the clear event defined in alarm mapping occurs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Mapping events to alarms is the process of configuring an alarm to be generated when a particular event is generated and the trigger rule is satisfied. If an event is mapped to an alarm, the alarm notification system and other automated actions can be triggered. Some events are mapped to alarms by default. Events are mapped to alarms from the **Event to Alarm Mappings** view, accessed from **Logs** > **Events & Alarms** and selecting the **Mappings** tab.

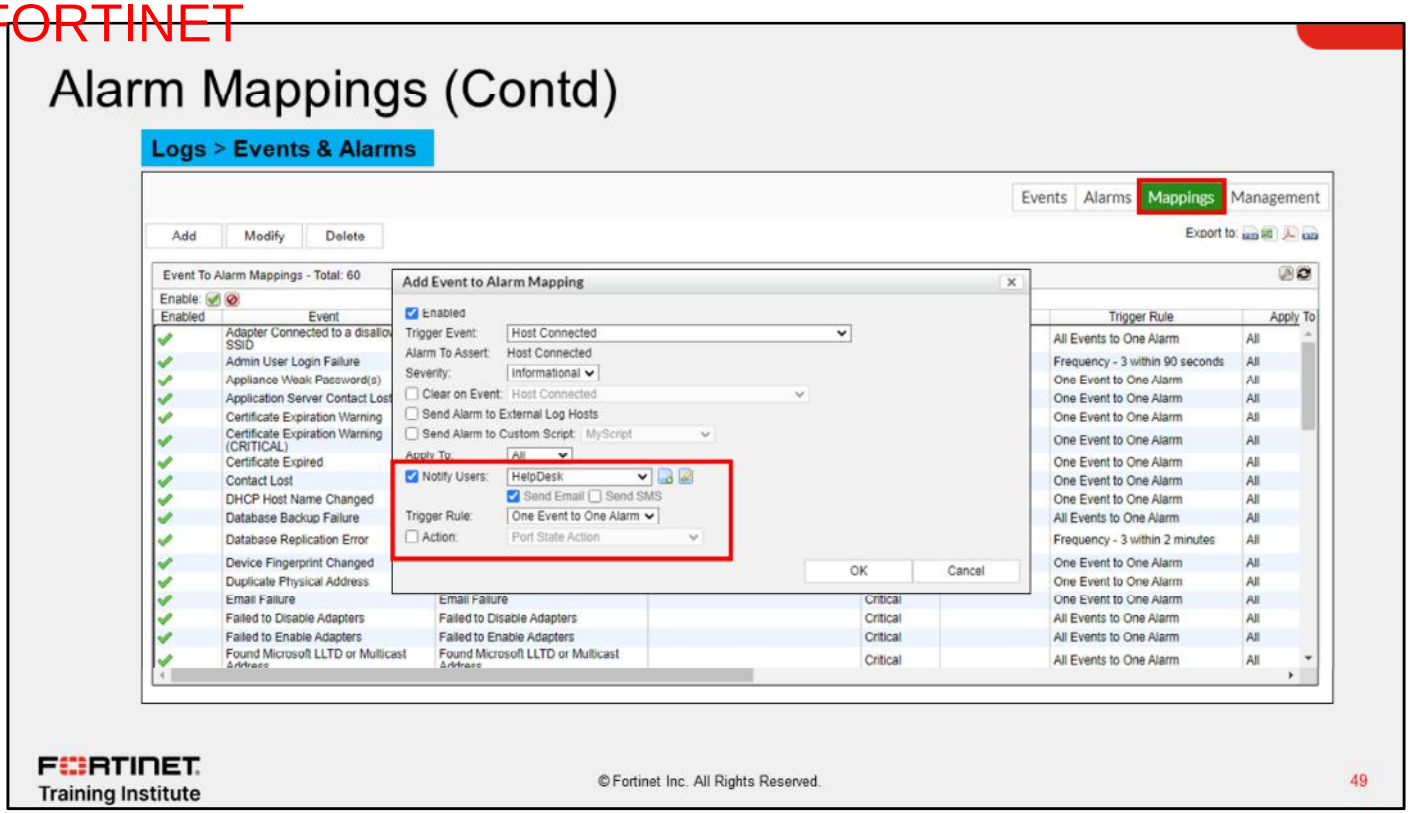
The view will display all current event-to-alarm mappings and give the ability to add new mappings, modify existing mappings, or delete existing mappings. Click **Enable** or **Disable** to quickly enable or disable a mapping. To add a new event-to-alarm mapping, click the **Add** button. The **Add Event to Alarm Mapping** window will open.

On the **Add Event to Alarm Mapping** window, select **Enable** to enable mapping. The **Trigger Event** drop-down list contains all 400+ available events seen in the event management window. The **Alarm to Assert** field contains the name automatically assigned by **FortiNAC**. In the **Severity** drop-down list, select the alarm severity: **Informational**, **Minor**, **Warning**, or **Critical**. The **Clear on Event** option instructs FortiNAC to automatically clear an existing alarm if a specific event occurs on the same element. The **Send Alarm to External Log Hosts** option works like the event option for logging externally. The **Send Alarm to Custom Script** option executes a selected command line script, such as a Perl script, and passes the alarm information as an argument to the script. A script must be located in the `/home/cm/scripts` directory to be available in this drop-down list.

The **Apply To** option works the same way as the **Filter by Group** option on the **Event Management** window. The alarm will be generated only if the element responsible for its generation is a member of a selected group or has been selected individually.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Use the options in the **Notify User** drop-down list to configure the alarm details that are sent, select whether they are sent by email or text, and select the administrator group that they are sent to.

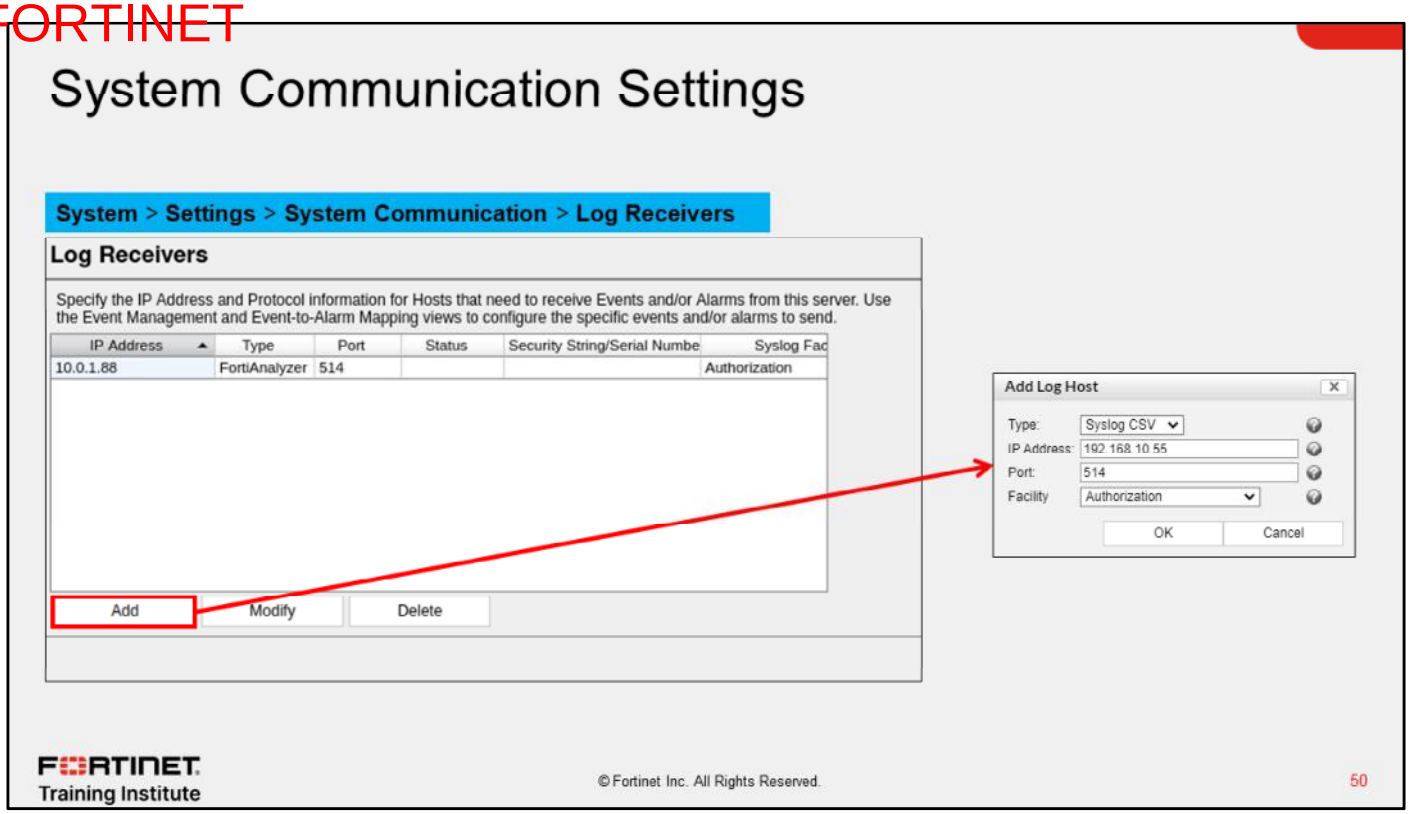
The **Trigger Rule** drop-down list contains the following options:

- **One Event to One Alarm**: A unique alarm is generated on every occurrence of the event.
- **All Events to One Alarm**: An alarm is generated the first time the event occurs.
- **Event Frequency**: An alarm occurs only if the trigger event is generated a specified number of times within a specified time frame.
- **Event Lifetime**: An alarm is generated when a trigger event is generated and no clear event is generated within a user-specified period of time.

Select **Action** to allow automated actions to run when the selected alarm is generated. The action options vary depending on the trigger event, but can include host state actions, CLI script actions, notification actions, port state actions, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Sending event information, alarm information, or both to an external system, such as a FortiAnalyzer, syslog server, or SIEM, is a valuable capability. The configuration settings page for these external systems, called log receivers, is located under **System** > **Settings** in the **System Communication** folder.

To configure a new log receiver, define the following settings:

- **Type**: The format the message should be sent in. Supported formats in the drop-down list are: **Syslog CSV**, **Syslog CEF**, **SNMP Trap**, and **FortiAnalyzer**.
- **IP Address**: The IP address of the server that will receive event and alarm messages.
- **Port**: The connection port on the server. For syslog CSV and syslog CEF servers, the default is port 514. For SNMP trap servers, the default is 162.
- **Facility** (for syslog options): The syslog facility. The default value is **Authorization**.
- **Security String** (for SNMP trap and FortiAnalyzer): The security string sent with the event and alarm messages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When sending information upstream to external log receivers, which three message types can be sent?

✓A. Syslog, SNMP, FortiAnalyzer

B. ICMP, SNMP, IMAP

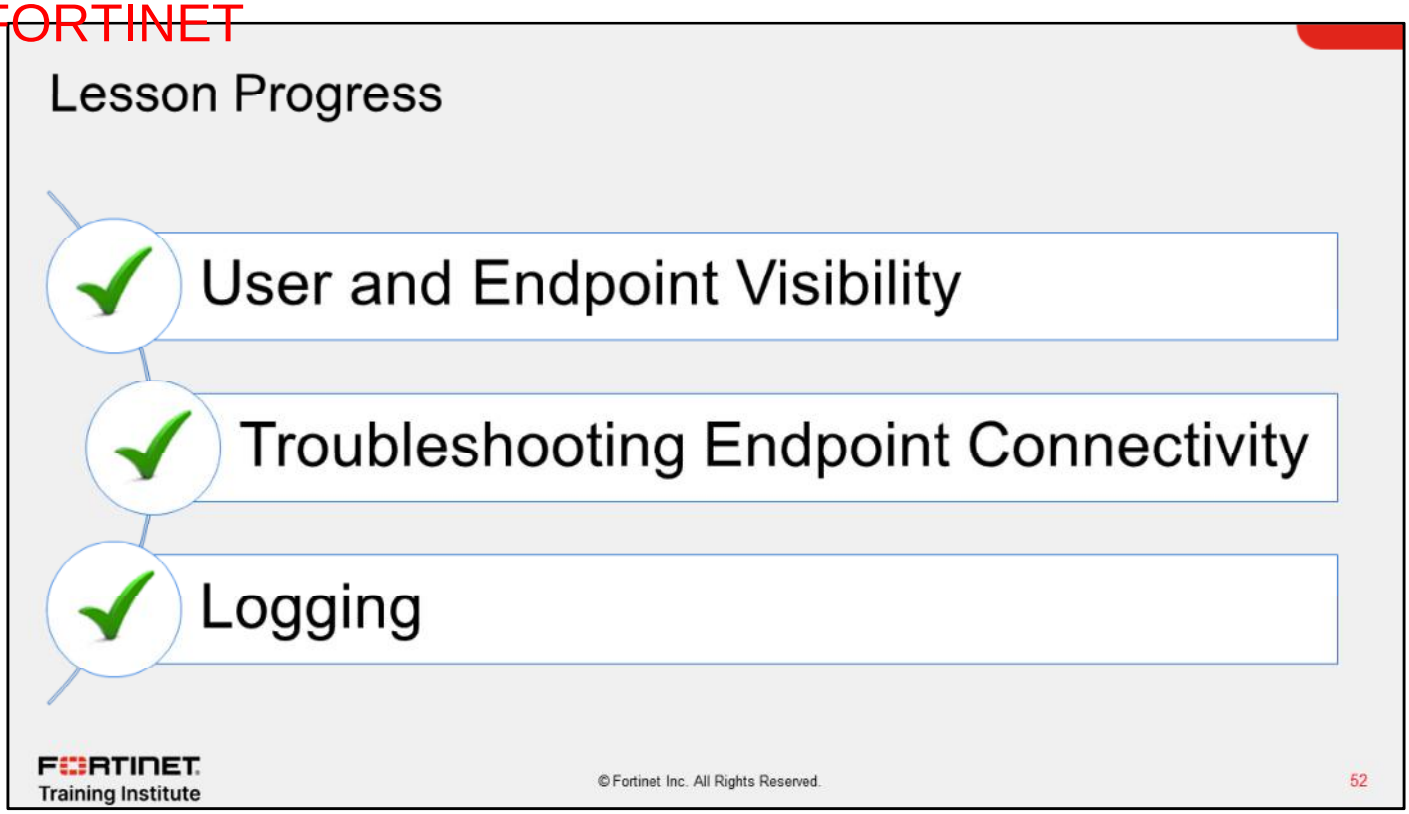
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

51

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

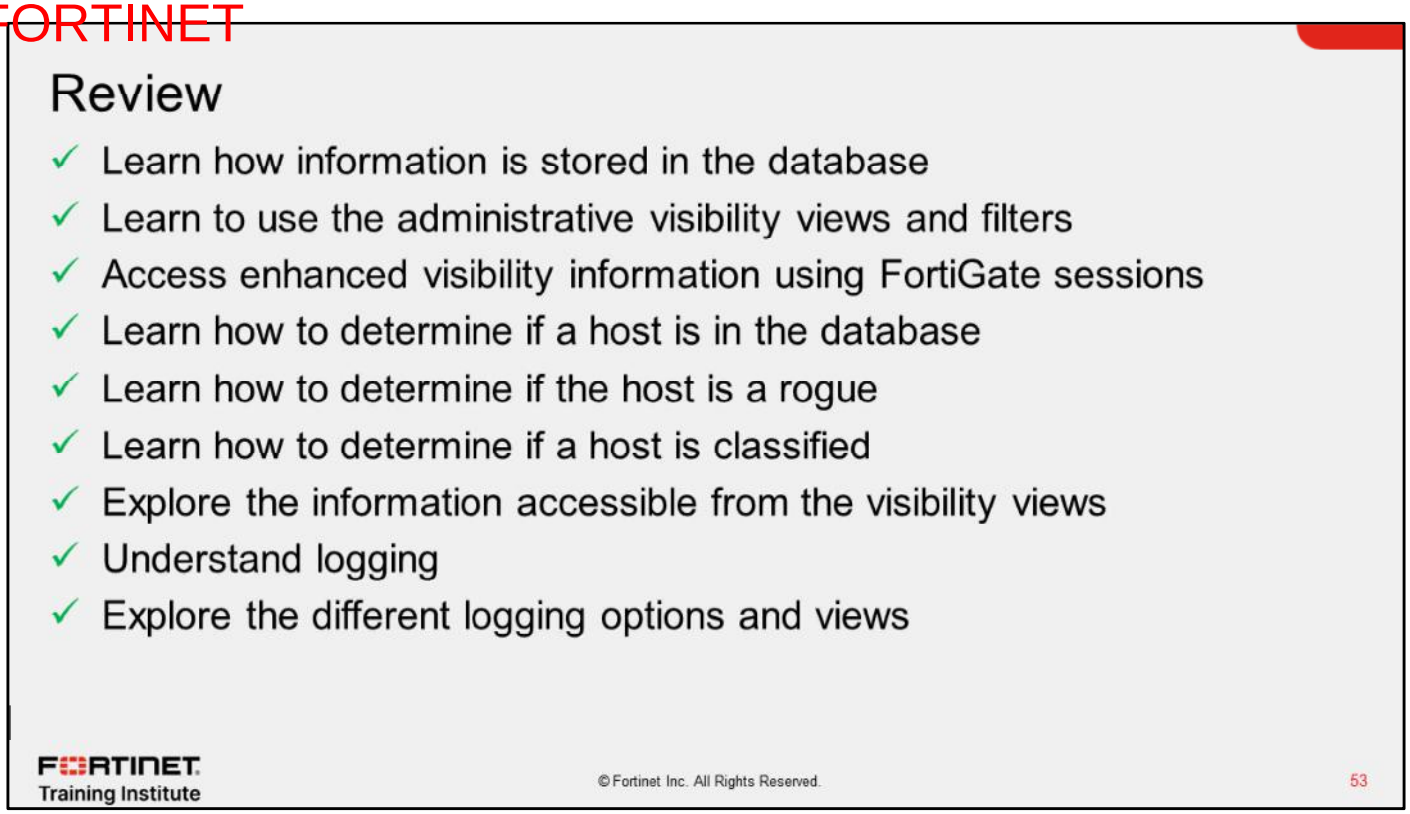


Congratulations! You've completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

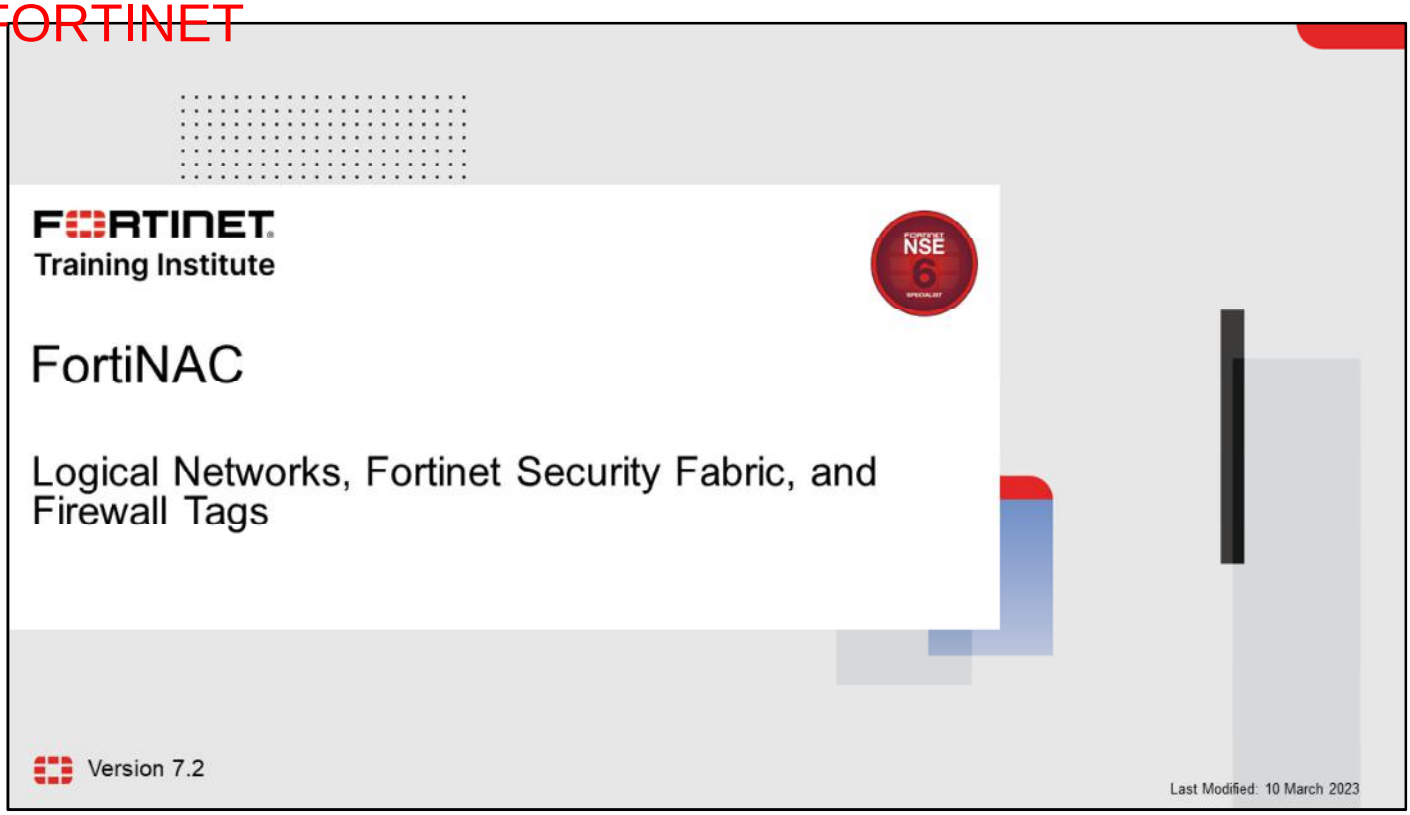
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide lists the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned how to access and manage user and endpoint information quickly and efficiently.

Vouchers & Dumps are Available | WhatsApp +201224560923

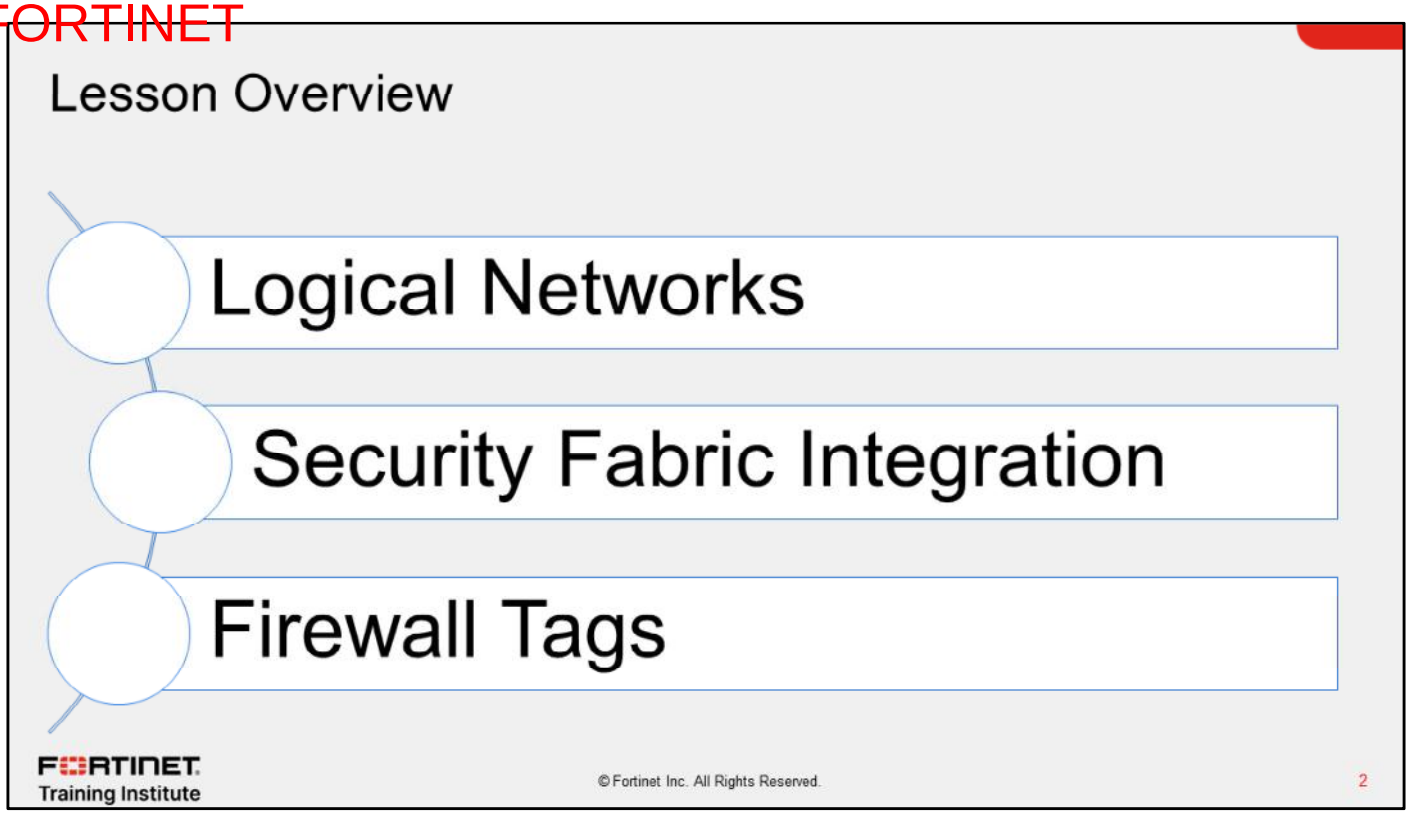
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiNAC logical networks, how to integrate FortiNAC in to the Fortinet Security Fabric for dynamic access control, and how to create and configure firewall tags.

Vouchers & Dumps are Available | WhatsApp +201224560923

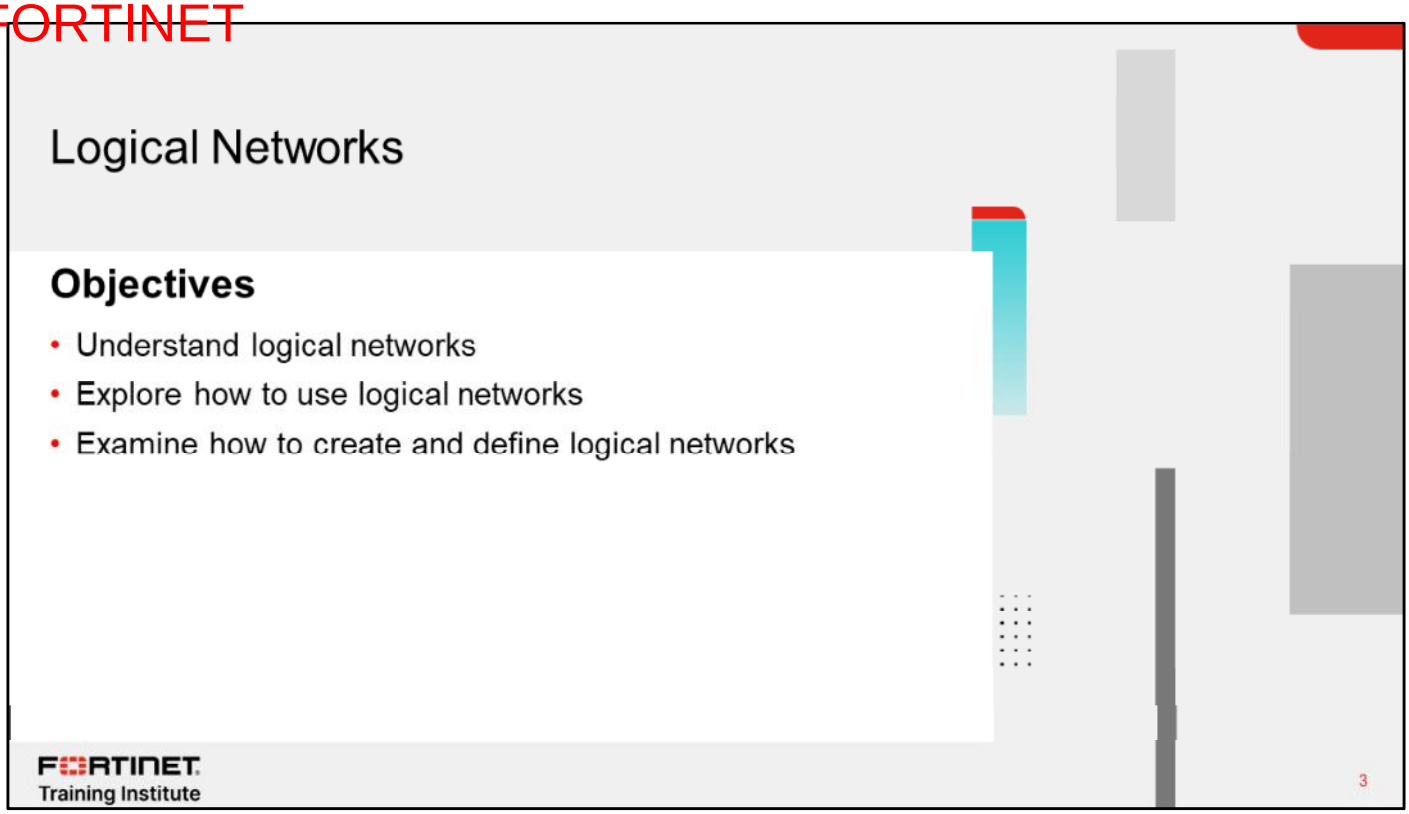
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

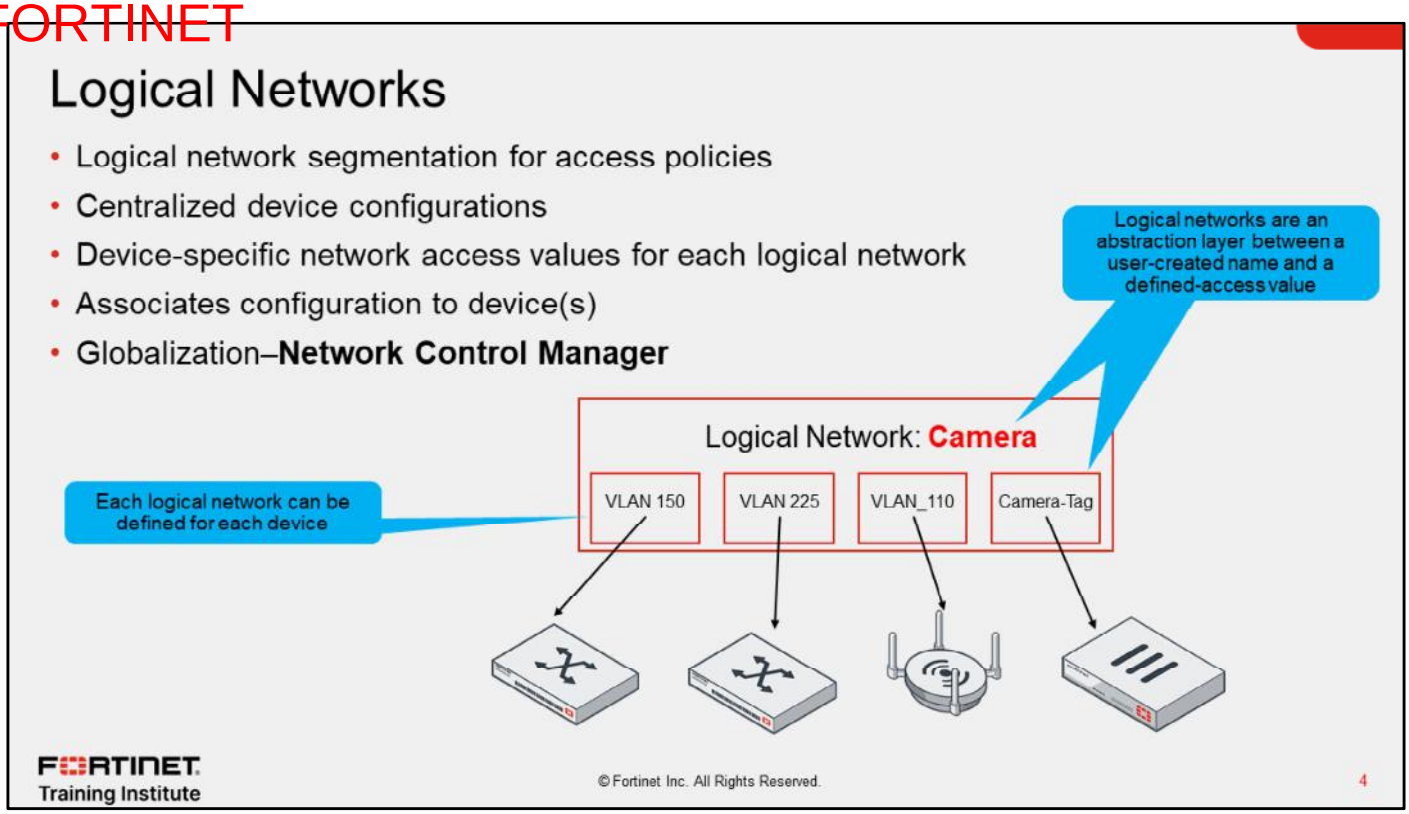


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiNAC logical networks, you will be able to explain what a logical network is, describe how to use logical networks, and create and define logical networks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



On FortiNAC, logical networks are representations of network configurations. Logical networks can represent different physical configurations for different infrastructure devices.

Logical networks are used to apply network access policies. Logical networks also translate logical access values to the physical values of infrastructure devices, decoupling policies from network configurations.

FortiNAC then uses the decoupled configuration values to provision the appropriate network access. One logical network can represent <N> physical network segments. This simplifies the configuration of network access policies.

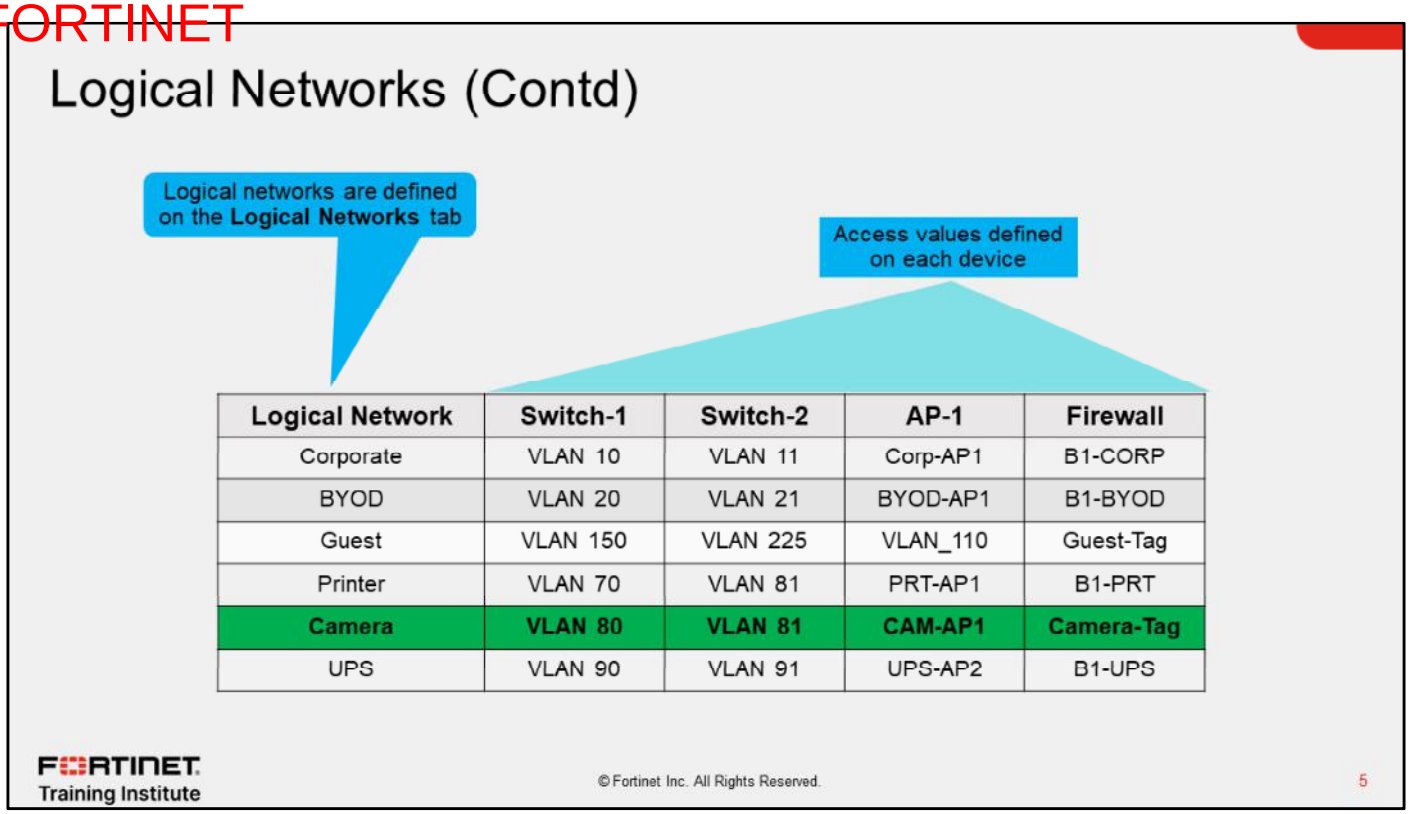
Device-specific configurations for network infrastructure devices are performed on the device, or sets of devices, that associate the configuration values with the devices. This simplifies network access policy management by reducing the number of policies.

Logical networks allow network access policy support in the **Network Control Manager**, enabling global administration in distributed environments.

In the example shown on this slide, the logical network **Camera** defines three different access values for three different points of connection, as well as an access tag to be sent to the firewall. This logical network defines the Layer 2 access (VLAN) and the firewall policies that will be enforced (firewall polices applied because of the tag) from a single access policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows an example of how logical networks can be used.

In the example, six network access policies have been developed to support the required endpoint-based segmentation on four infrastructure devices.

As you can see, a device identified as a camera and assigned to the logical network **Camera** is provisioned to **VLAN 80**, if it connects to **Switch-1**; is provisioned to **VLAN 81** if it connects to **Switch-2**; and so on. The values designated in the **AP-1** column are access values that may be vendor specific, depending on the vendor of the wireless access point (AP) or controller. These values could also be VLAN names, groups, roles, interfaces names, and so on.

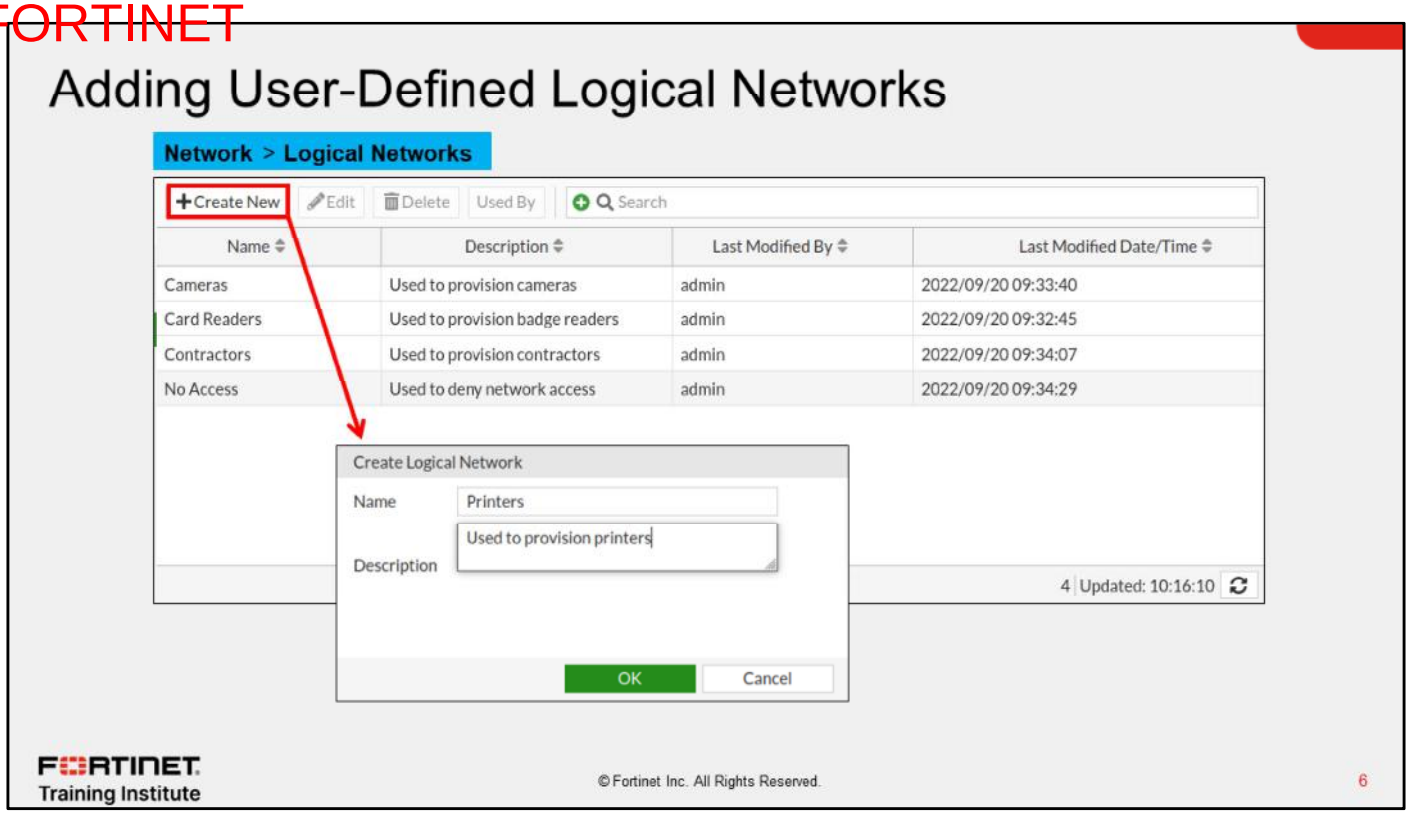
The **Firewall** column could represent a firewall tag that would result in the camera matching a specific firewall policy.

You can use logical networks to greatly decrease the number of network access policies, resulting in simplified policy creation and management.

These same network access policies work for small, medium, or large environments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



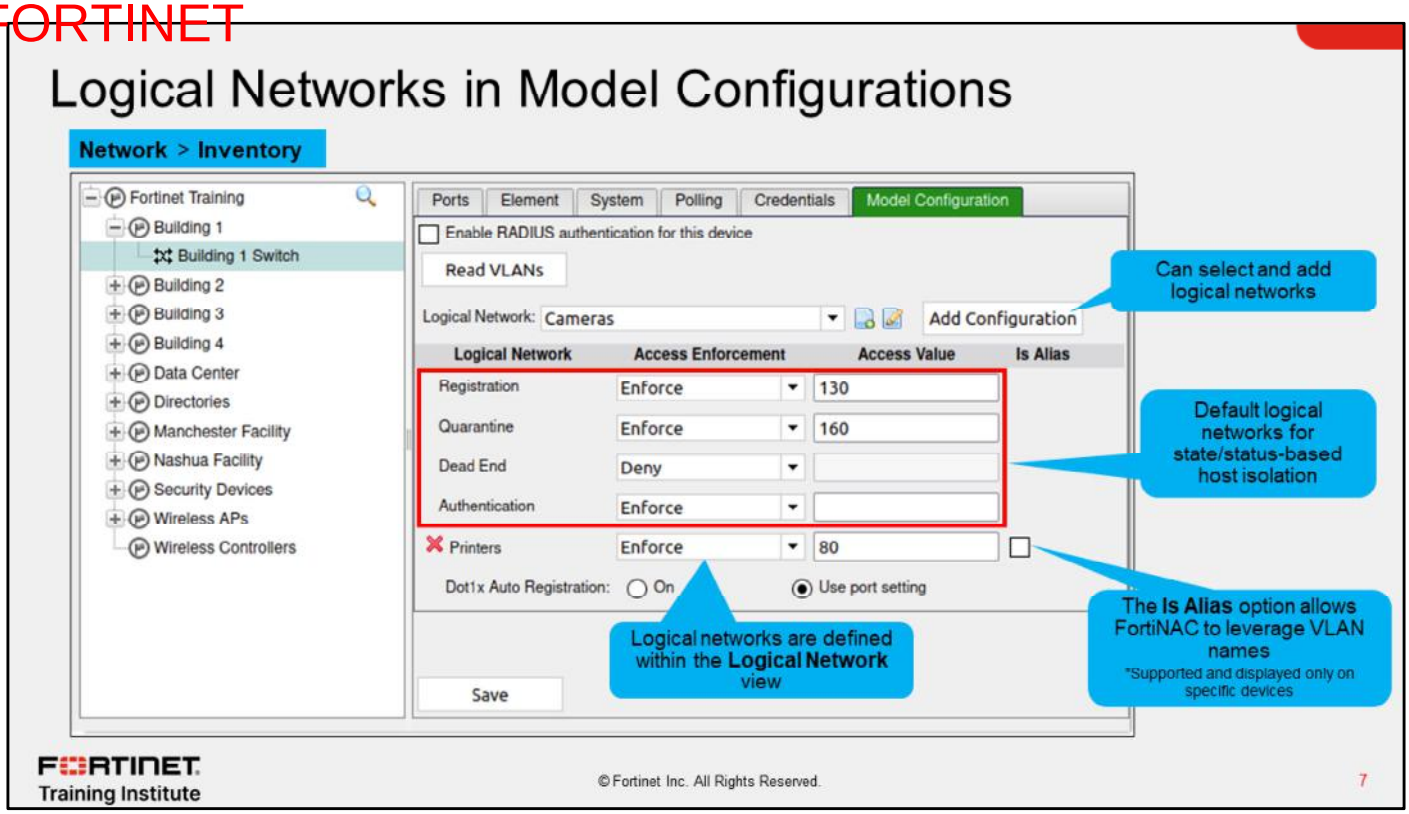
You can view existing logical networks by navigating to the **Logical Networks** view. On this view you can create, edit, or delete logical networks, as well as see where logical networks are in use.

Click **Create New** to create a new logical network and assign it a name. The name must be unique to the logical network you are creating. Optionally, you can add a description to the logical network to help clarify its purpose or use.

After you create the logical network, it appears within the model configuration of each infrastructure device that is modeled in the topology tree.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



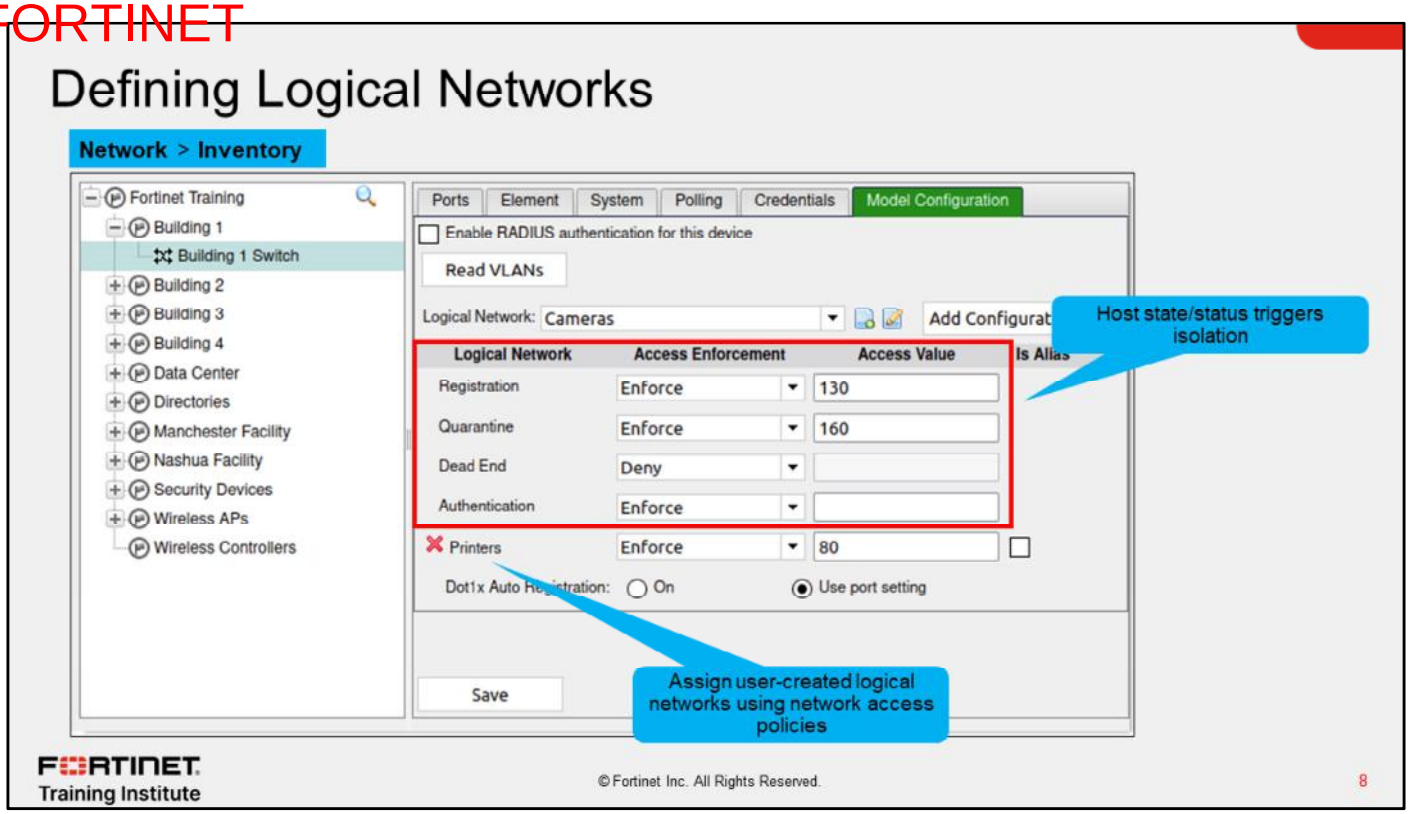
Logical networks appear in device **Model Configuration** views. Existing logical networks appear in a drop-down list, you can add them to the model configuration using the **Add Configuration** button to the right of the list. Once added, you can define a logical network value for this device or SSID. You can remove logical networks from a model configuration by clicking on the red X to the left of the logical network.

Note that four default logical networks pre-exist in each device model configuration. These logical networks—**Registration**, **Quarantine**, **Dead End**, and **Authentication**—are used for endpoint isolation, based on the endpoint state or status. You can apply all logical network configurations across any number of selected devices with a single configuration. You will learn more about this capability, as well as the use of the default logical networks, in another lesson.

Depending on the vendor and model of the infrastructure device, you may be able to identify a logical network value as **Is Alias**. Making this designation allows FortiNAC to leverage VLAN names for that logical network. For example, if the organization has more than one guest network across multiple facilities, you can provision guests on the appropriate VLAN by name, as long as the name is consistent at each facility.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can define logical networks on a device-by-device basis within each device model configuration. The assigned access values can be VLAN IDs, which is almost always the case for wired infrastructure devices, or a vendor-specific value, which is often the case when configuring wireless APs or controllers. On specific model types, user-created logical networks can contain an alias value.

In the example shown on this slide, FortiNAC will provision any device that a network access policy defines as a printer to VLAN 80, when that device connects to a port on **Switch-1**.

The decoupling of the access value from the network access policy gives you the flexibility to provision the network access desired for a specific type of endpoint, across any number of locations, within a single policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which capability do logical networks provide?

✓A. An abstraction layer separating access policy configurations from being directly associated with model configurations

B. A way to configure VLAN names across several model configurations at the same time

2. Which statement is true?

A. Logical network access values are configured in a single location and apply to all devices.

✓B. Logical network access values are configured for each device.

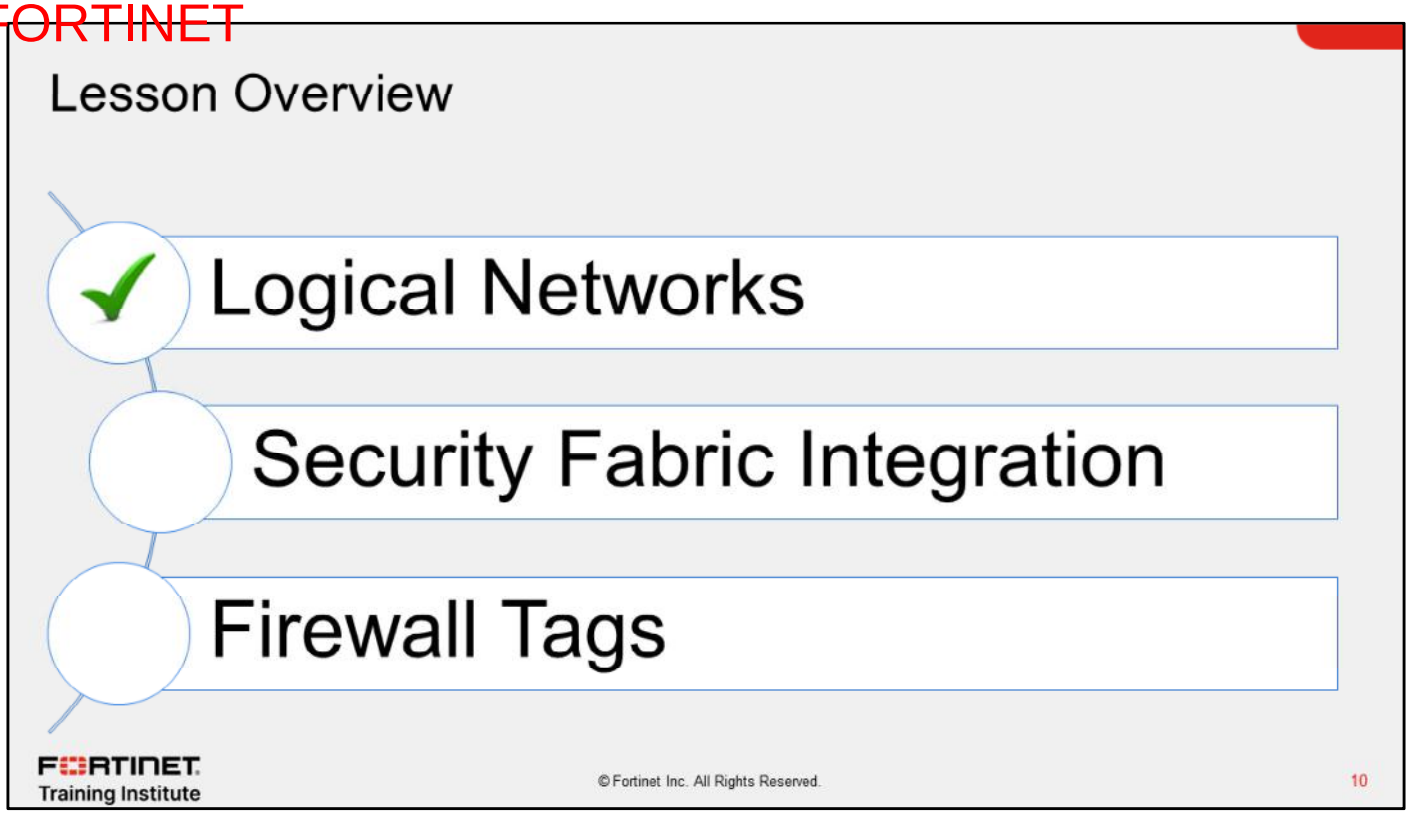
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

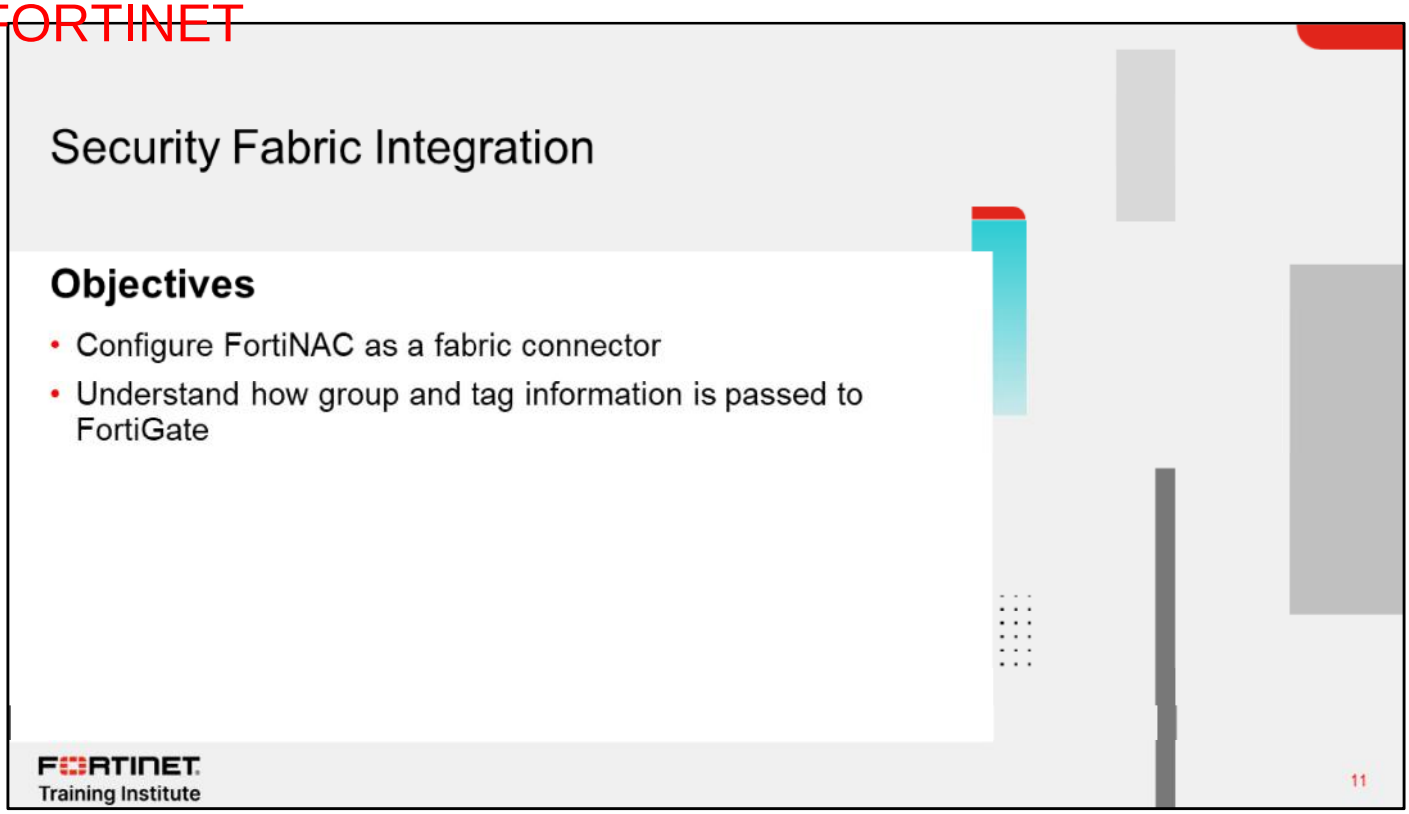


Good job! You now understand FortiNAC logical networks.

Now, you will learn about FortiNAC Security Fabric integration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

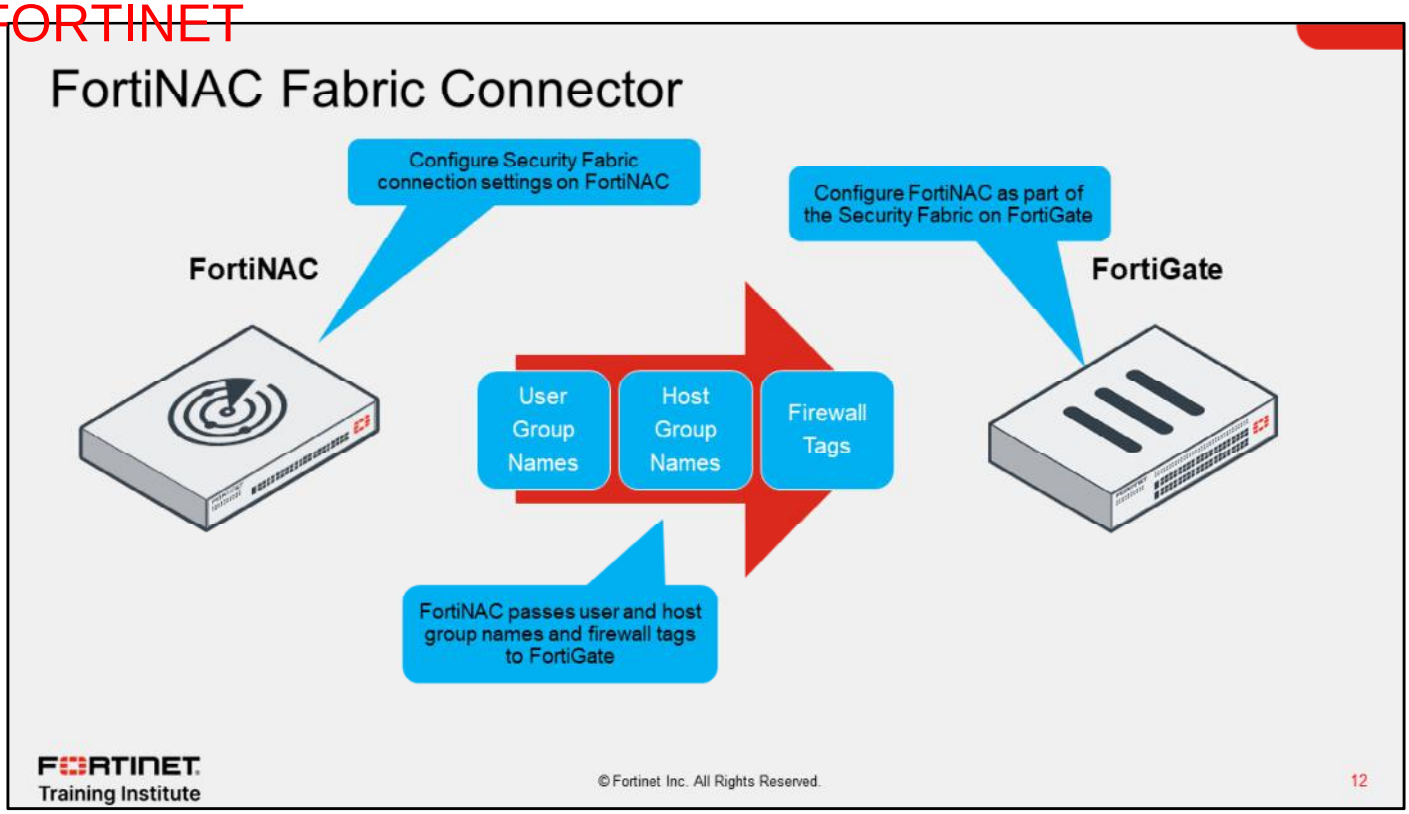


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding FortiNAC fabric integration and how locally assigned group and tag information is passed to FortiGate devices, you will be able to fully leverage FortiNAC fabric connector capabilities.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



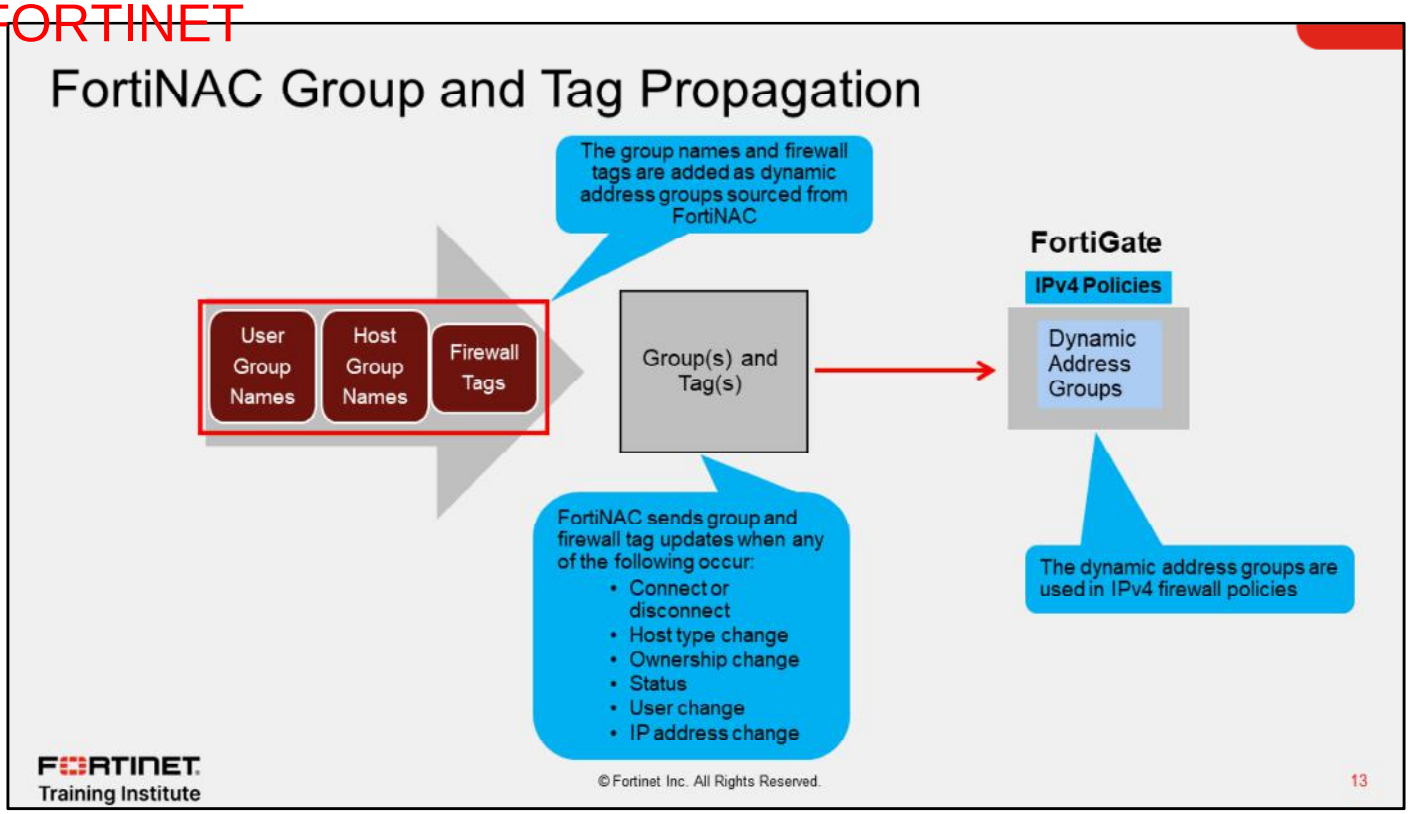
The FortiNAC fabric service connector and authorization to join the Security Fabric on FortiGate enables FortNAC to communicate directly with FortiGate, and FortiGate to communicate directly with FortiNAC.

Security Fabric integration is the key to enabling FortiNAC to automatically associate tags with devices and hosts, and pass those tags to FortiGate, so that FortiGate can enforce firewall policies using dynamic address groups, enabling intent-based segmentation.

When you configure FortiNAC as part of the Security Fabric, you can transfer FortiNAC firewall tags and group names to one or more FortiGate devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Once transferred to FortiGate, the group names and firewall tags are listed as dynamic address groups sourced from FortiNAC.

FortiNAC sends automatic updates about group membership to the FortiGate devices when any of the following occur:

- An endpoint connects or disconnects from the network.
- A host type or status changes, such as unknown or untrusted to known or trusted.
- There is an ownership change, such as BYOD, guest, staff, type of employee, such as accounting, engineering, student, and so on.
- The health status of an endpoint changes, such as compliant to non-compliant.
- A user changes, such as the owner or logged on user.
- The IP address of a host changes.

Other situations that can define which FortiGate devices are updated include the following:

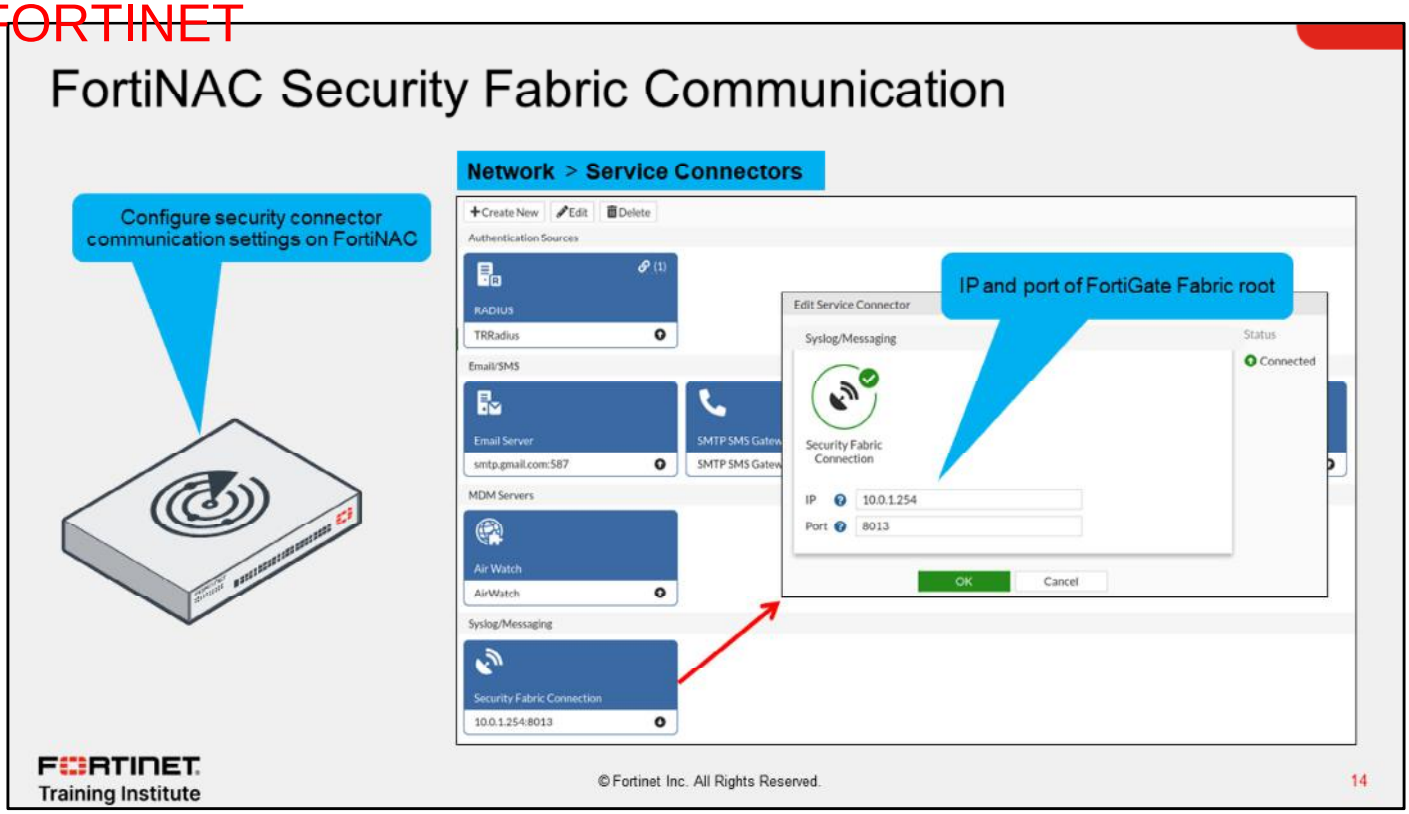
- If a device or host is directly connected to a FortiGate port, then the tag and group information is sent only to that FortiGate.

- Upon startup, FortiNAC collects all configured interface IP addresses and IP scopes defined on all modeled FortiGate devices. FortiNAC uses that list of IP addresses or network scopes to identify which FortiGate devices to update, based on an endpoint IP address.

This tight integration allows FortiNAC to manage device connections from Layer 1 to Layer 3, while FortiGate applies granular segmentation at Layer 3 to Layer 7, resulting in the ability to dynamically manage from the core to the edge.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

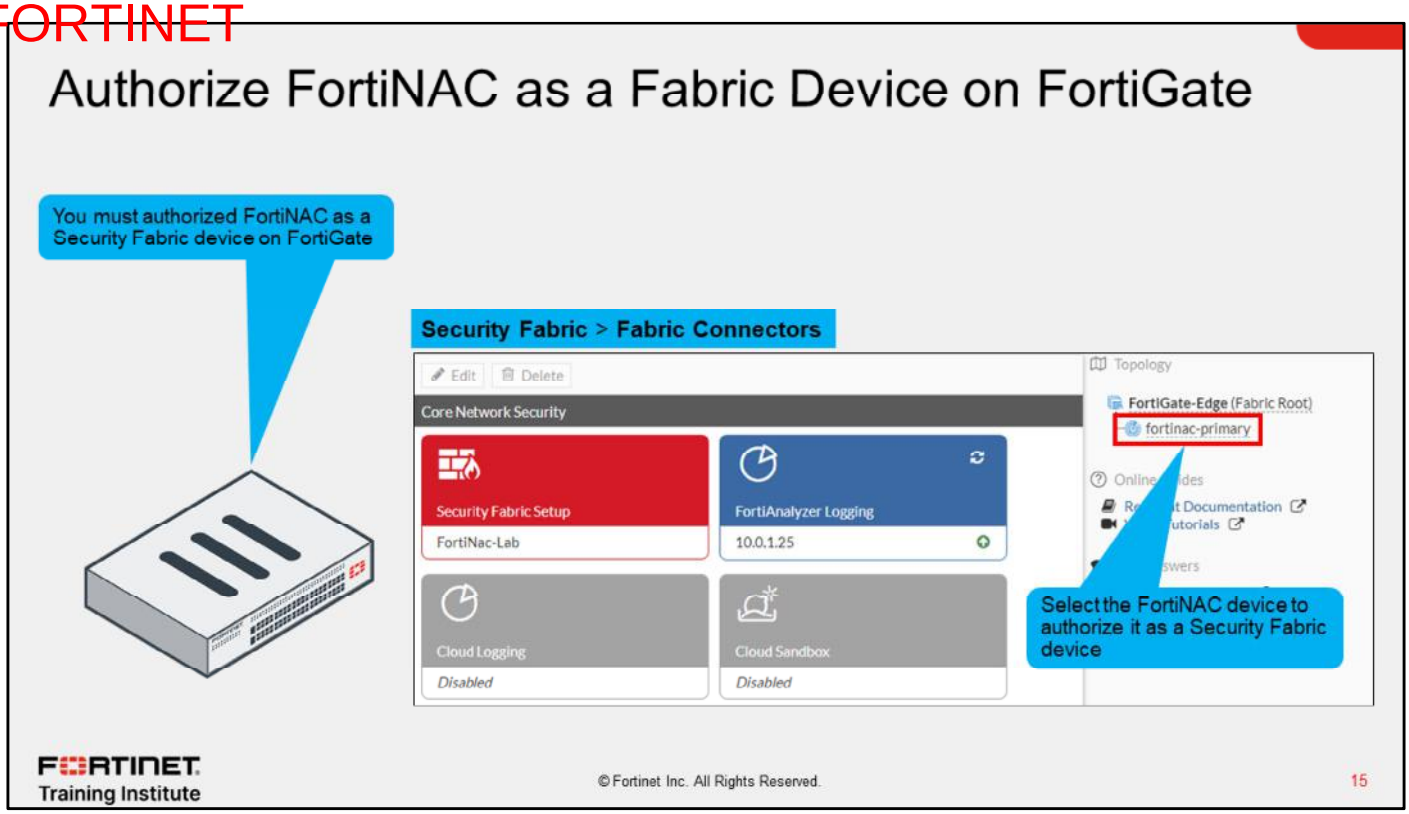


To create the Security Fabric integration, you must configure the **Security Fabric Connection** service connector communication settings on FortiNAC. You can do this by clicking **Network** > **Service Connectors** and adding or editing the service connector.

The configuration port defaults to 8013, but you can change that value.

Vouchers & Dumps are Available | WhatsApp +201224560923

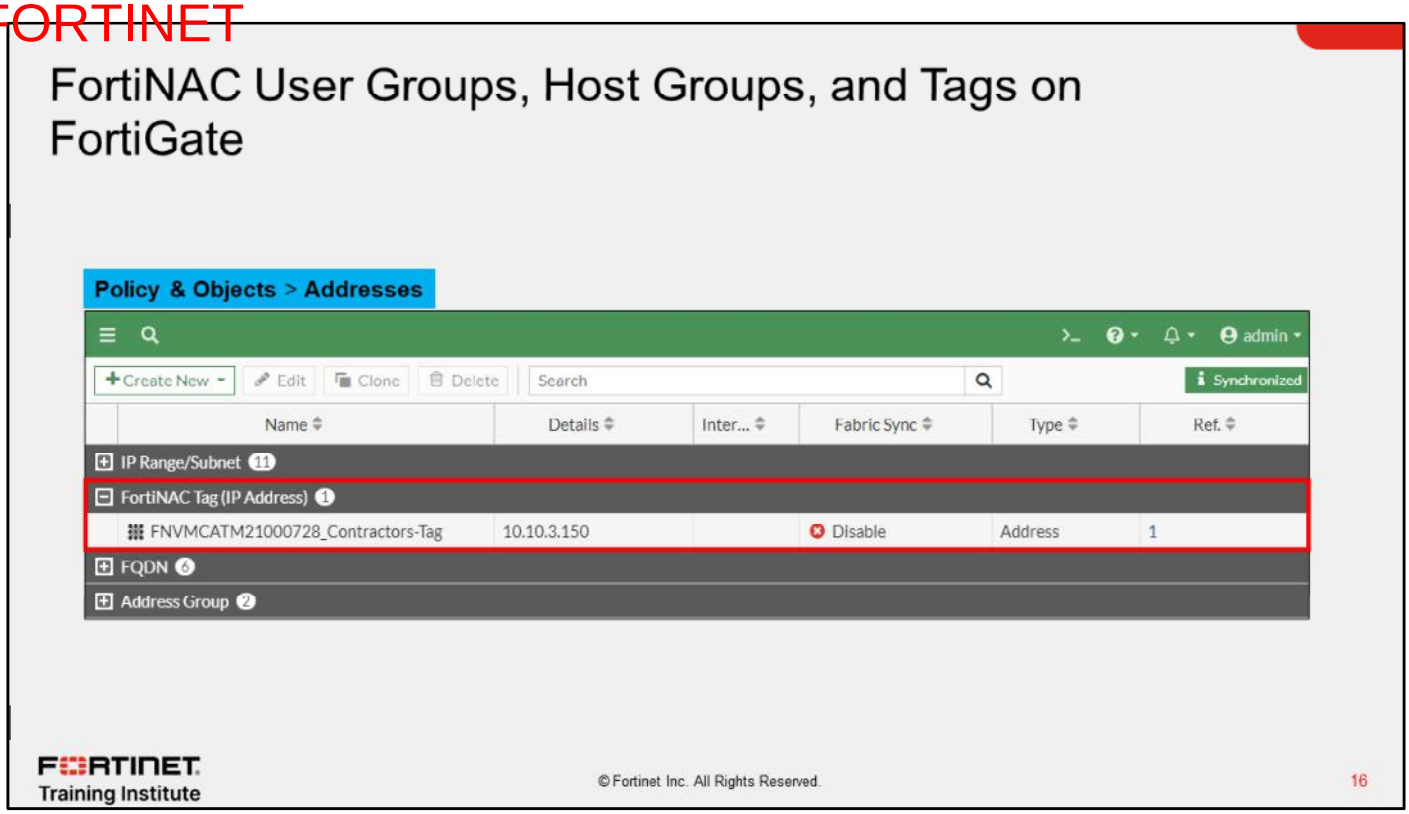
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You must authorize FortiNAC as a Security Fabric device on the FortiGate. Once authorized, FortiNAC is allowed to join the Security Fabric and pass tag and group information to FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

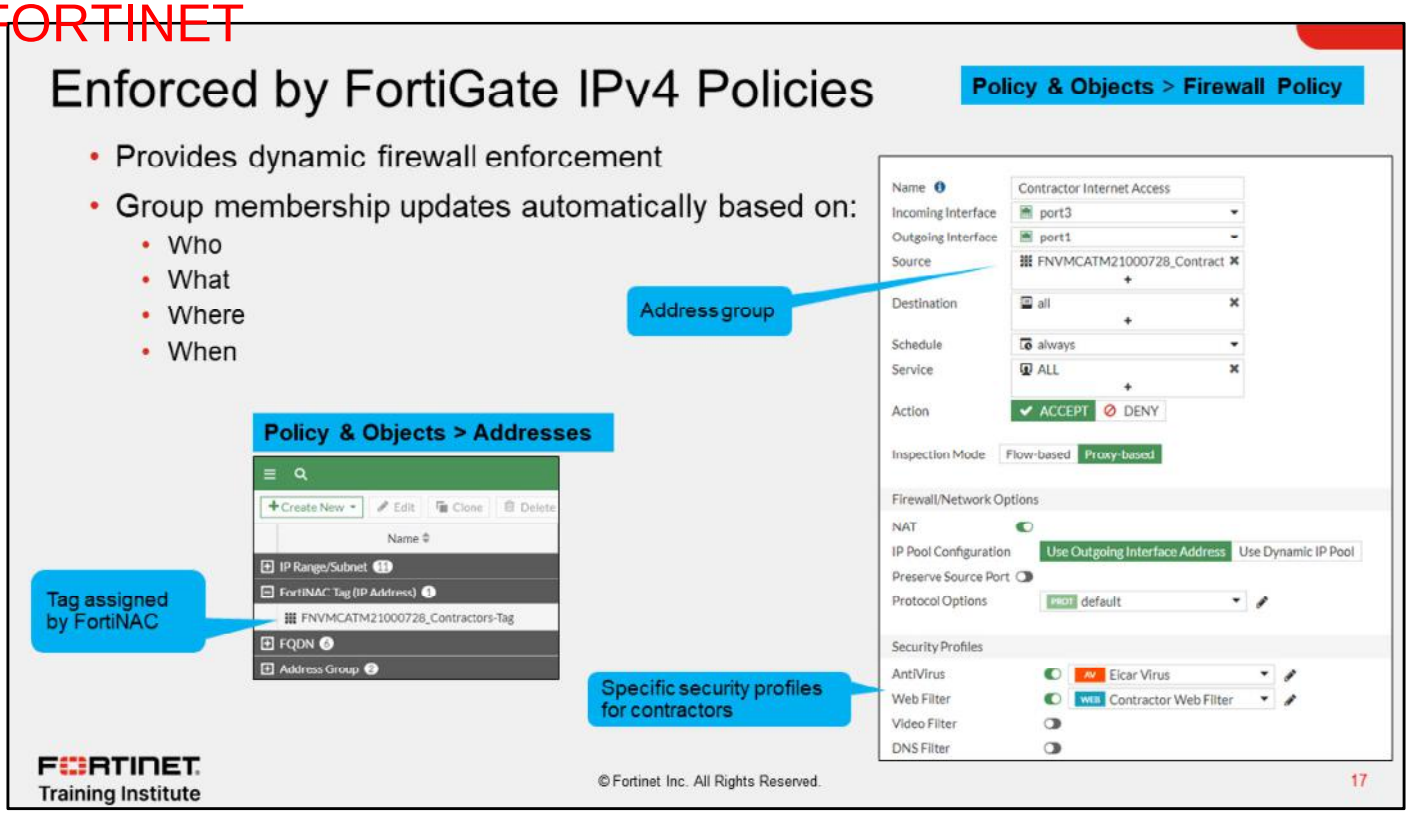
DO NOT REPRINT Brave-dumps.com
© FORTINET



When a user or host matches a FortiNAC access policy, user group names, host group names, and firewall tags associated with the corresponding logical network are brought in. These items are shown in the **Addresses** view as dynamic address groups. You must integrate FortiGate with FortiNAC in this way in order for FortiGate to receive updates from FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

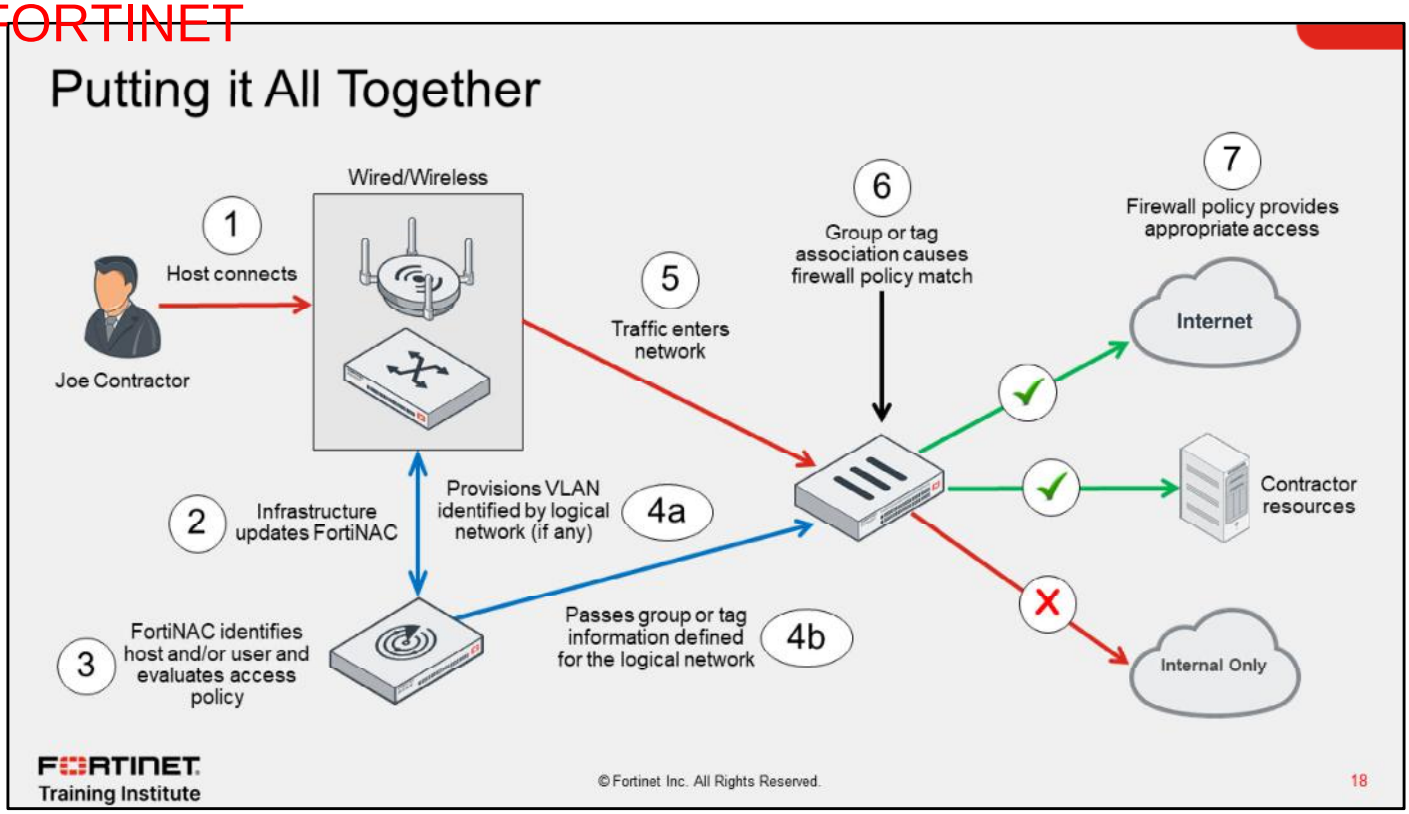


You can use the dynamic address groups in firewall policies on FortiGate. Because the groups are being dynamically updated by FortiNAC, dynamic firewall enforcement is possible. FortiGate can then manage endpoints at Layers 3 to 7. In another lesson, you will learn how FortiNAC can instantly update groups or tags based on security information passed to FortiNAC from almost any security solution.

The security policies on FortiNAC can manage hosts at Layers 1 to Layer 3. The tight integration between FortiNAC and FortiGate, as well as the FortiNAC ability to receive alert information from almost any security device, creates a dynamic solution that can quickly mitigate threats by leveraging control at Layers 1 to Layer 7.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide provides an example of the entire process. In this example, a contractor is connecting to the network and being provided access to only necessary resources. The process is as follows:

1. The contractor connects to the network using a wired or wireless connection.
2. The infrastructure device managed by FortiNAC updates FortiNAC with the host information.
3. FortiNAC identifies the host in the database and evaluates the user/host profiles associated with defined network access policies.
4. If a policy is defined:
    a) FortiNAC provisions the host to a VLAN if one is defined in the logical network of the model configuration associated with the point of connection.
    b) FortiNAC passes any user groups, host groups, or firewall tags defined in the model configuration of FortiGate devices.
5. The contractor begins passing traffic.
6. Group or tag information passed by FortiNAC associates the host with a firewall policy.
7. The firewall policy determines resource access.

Note that this process could be for any connecting endpoint, such as employees, guests, printers, card readers, cameras and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

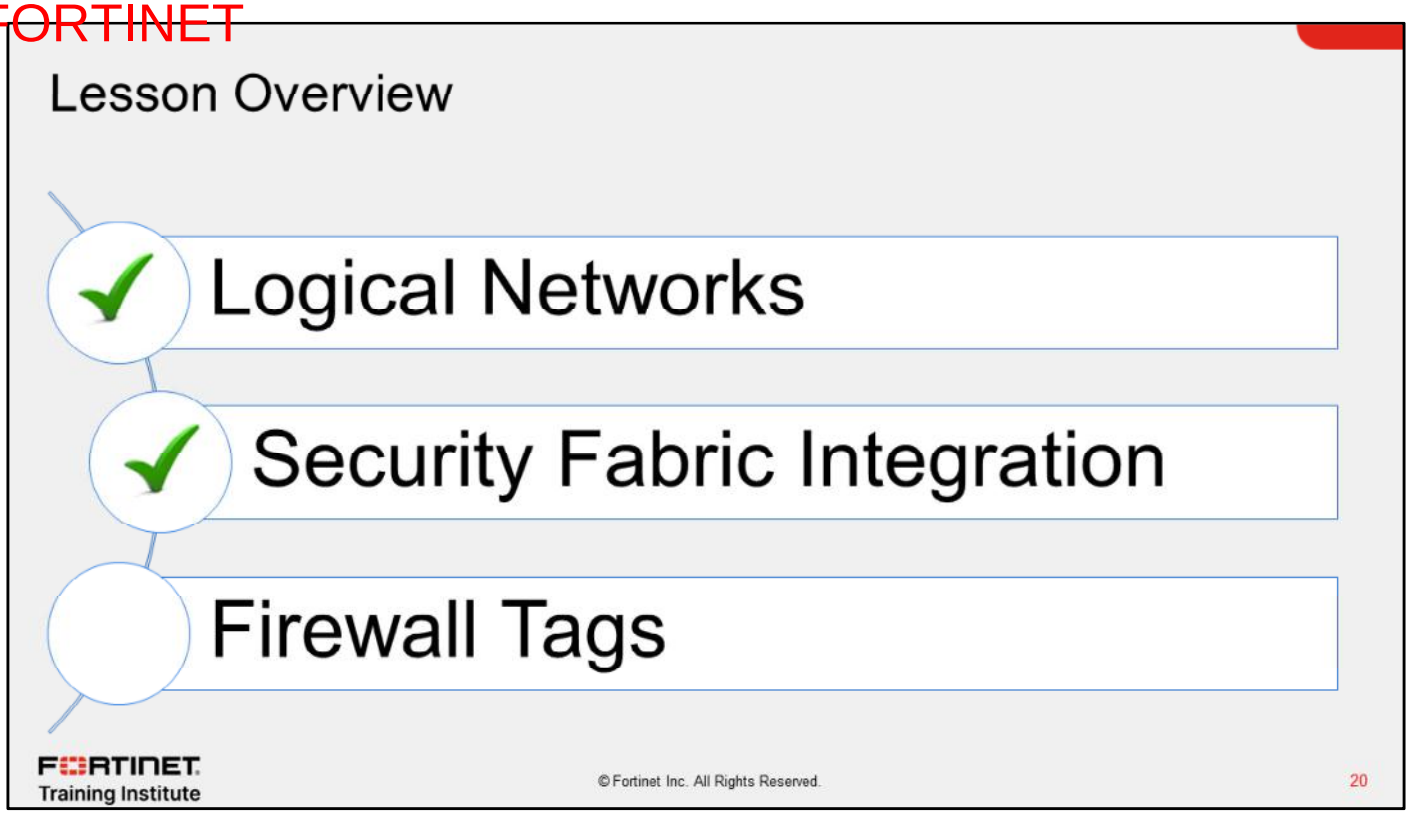
1. Does a host-type change on FortiNAC cause group and firewall tags to update on FortiGate?

✓A. Yes
B. No

FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

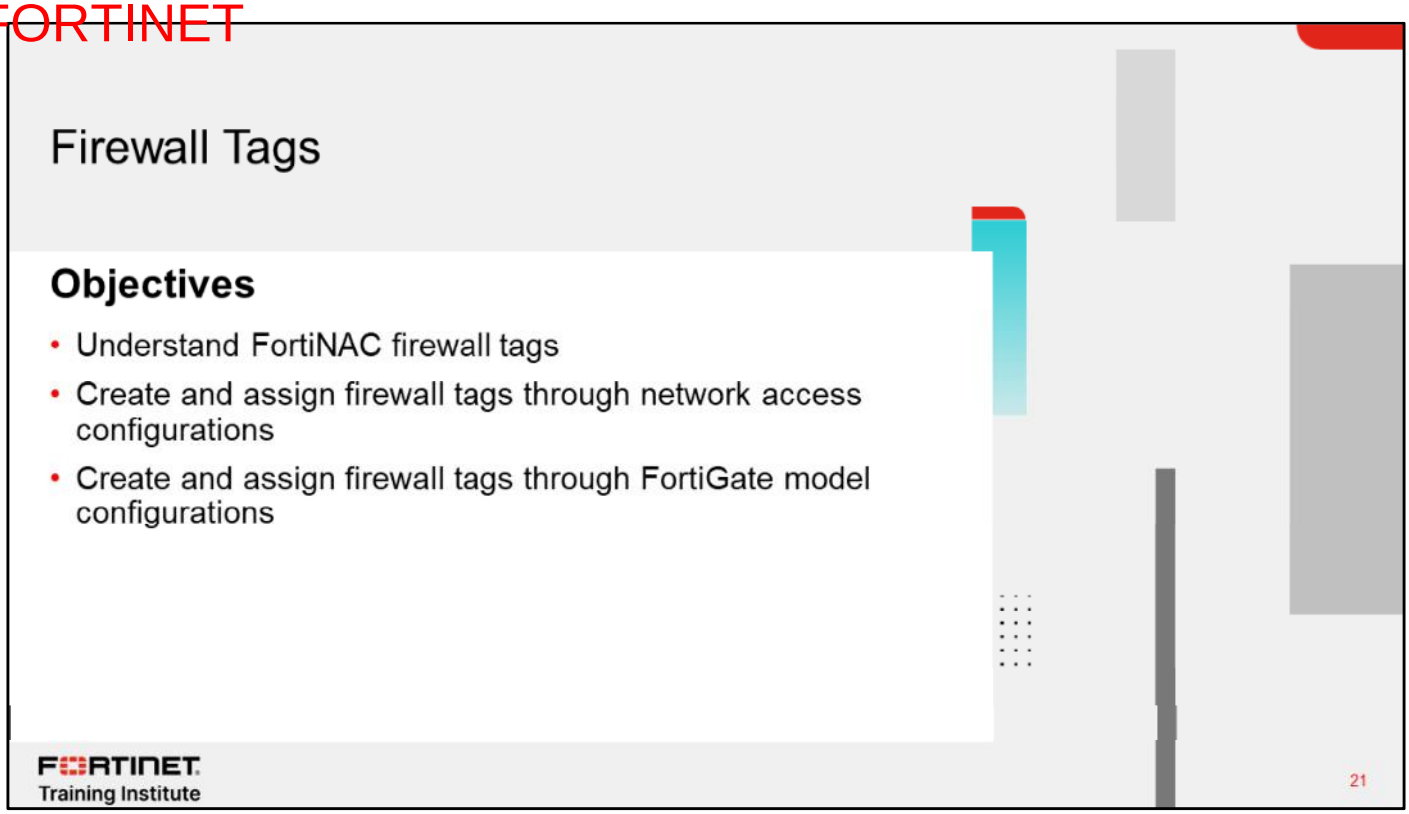


Good job! You now understand FortiNAC Security Fabric integration.

Now, you will learn about FortiNAC firewall tags.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

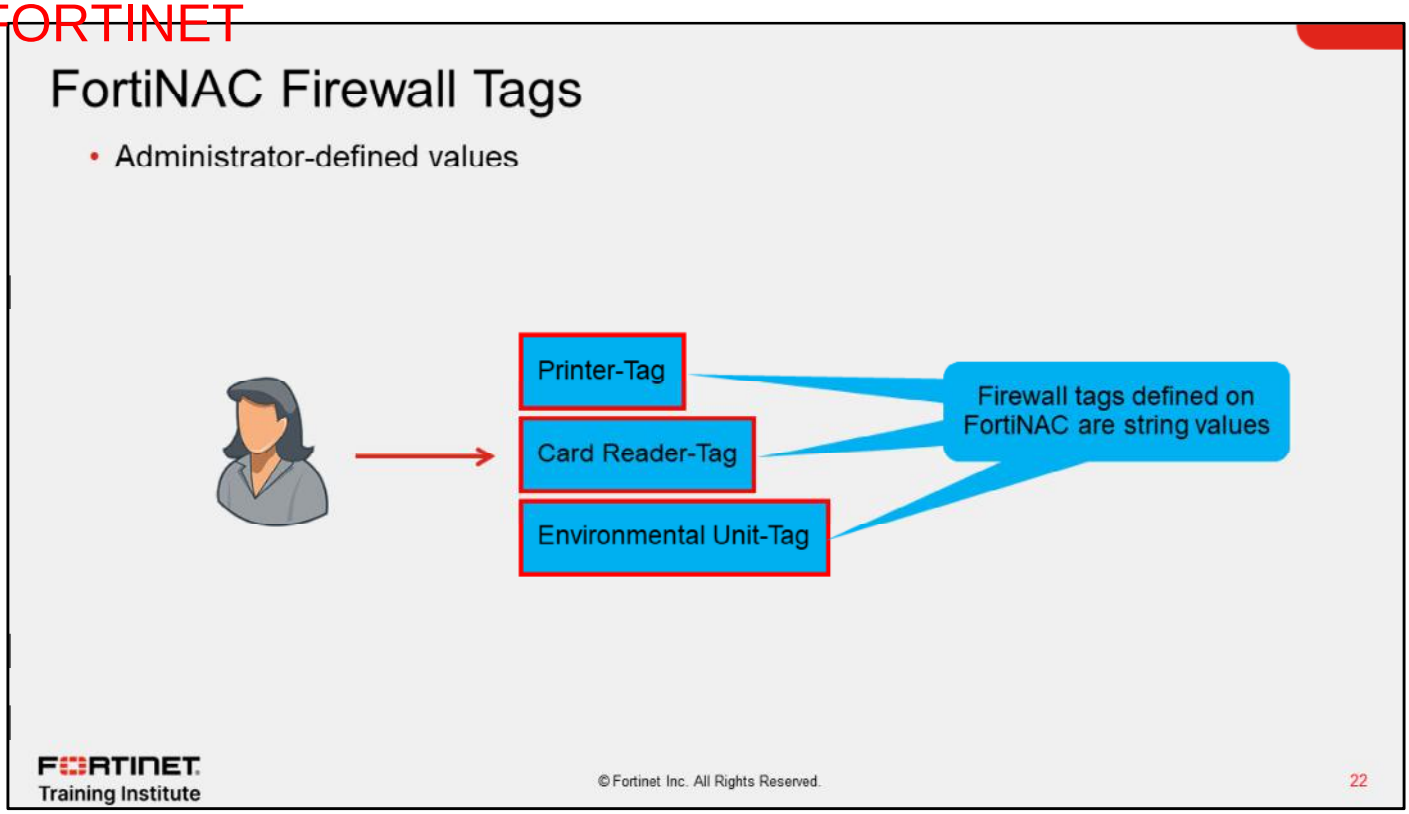


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in firewall tags, you will be able to create firewall tags and assign them within a network access configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

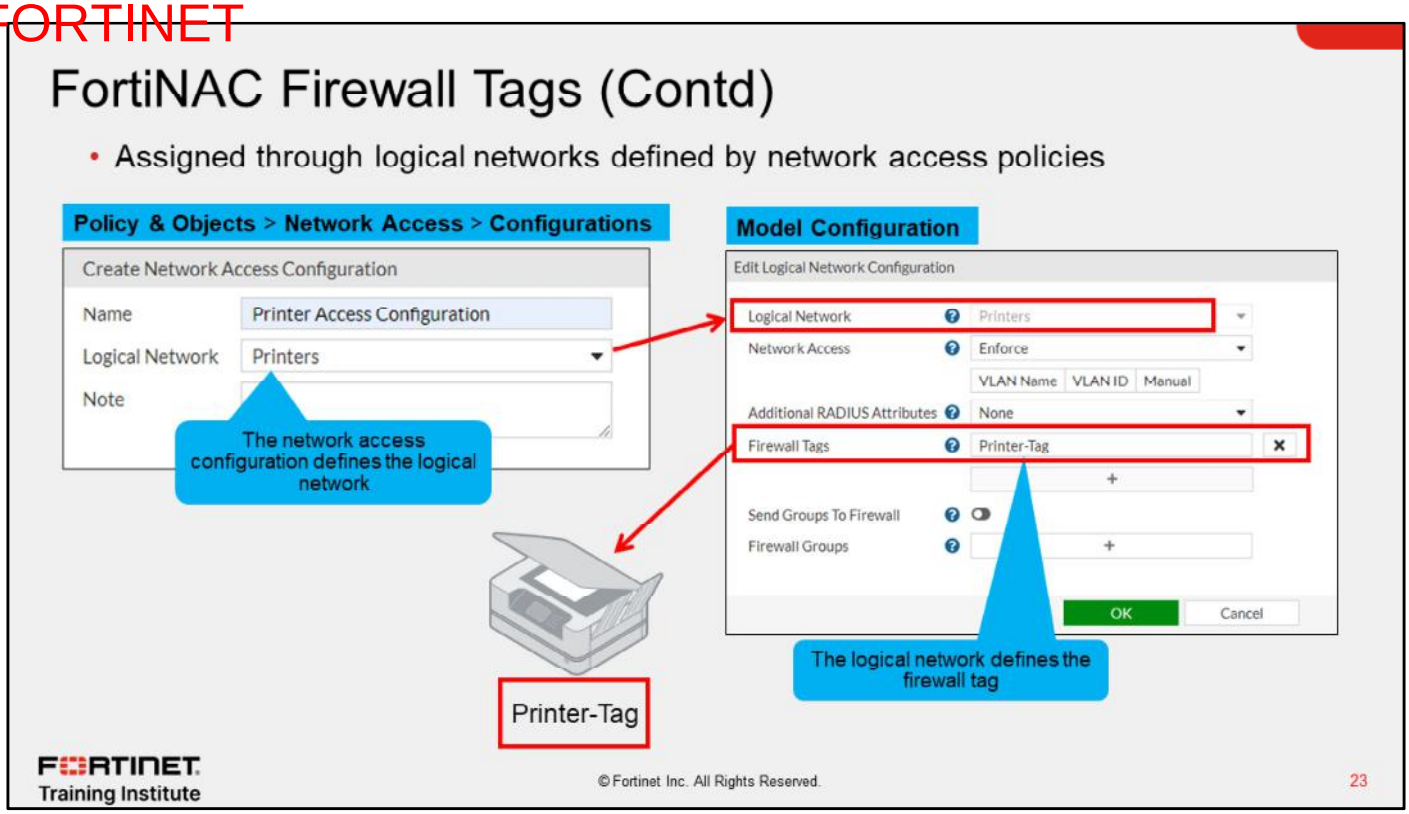


A firewall tag is a value created by an administrator that is used to identify hosts or devices. FortiNAC dynamically assigns firewall tags to hosts or devices based on a security policy or logical network. For example, you could apply a firewall tag to any device that is identified by a device profiling rule, resulting in printer tags, card reader tags, environmental unit tags, and so on. Firewall tags can also be applied as the result of a security alert received by FortiNAC from a security device, or because a host or device became a member of a specific group.

Firewall tags are passed to FortiGate for dynamic FSSO group membership updates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Network access configurations are applied when a connecting end point matches a network access policy. The network access configuration defines the logical network, and you assign firewall tags through logical networks defined on device model configurations. In the example shown on this slide, the logical network **Printers** are used to provide access for any device classified as a printer. You can then configure the **Printers** logical network to assign the **Printer-Tag** at the device model configuration.

In the example shown on this slide, a device that matches a network access policy that applies the **Printer Access Configuration** has the firewall tag associated with the **Printers** logical network passed to the FortiGate, in this case **Printer-Tag**.

Creation of network access policies will be covered in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Firewall tags are:
   A. Auto-generated policy values
   ✓ B. Administrator-created values

2. Firewall tags are used to:
   A. Define a device type
   ✓ B. Cause a dynamic IPv4 policy match

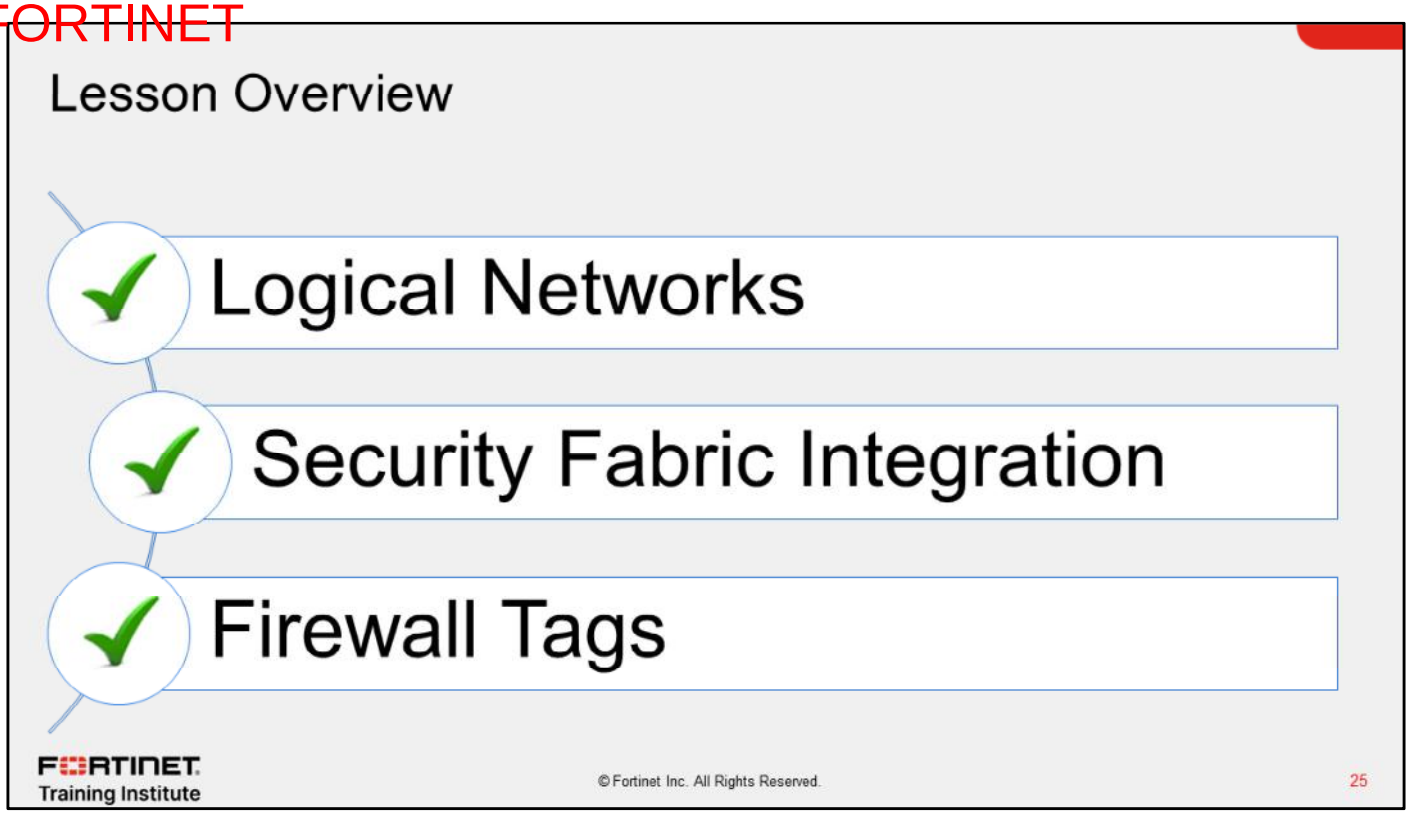
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

24

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

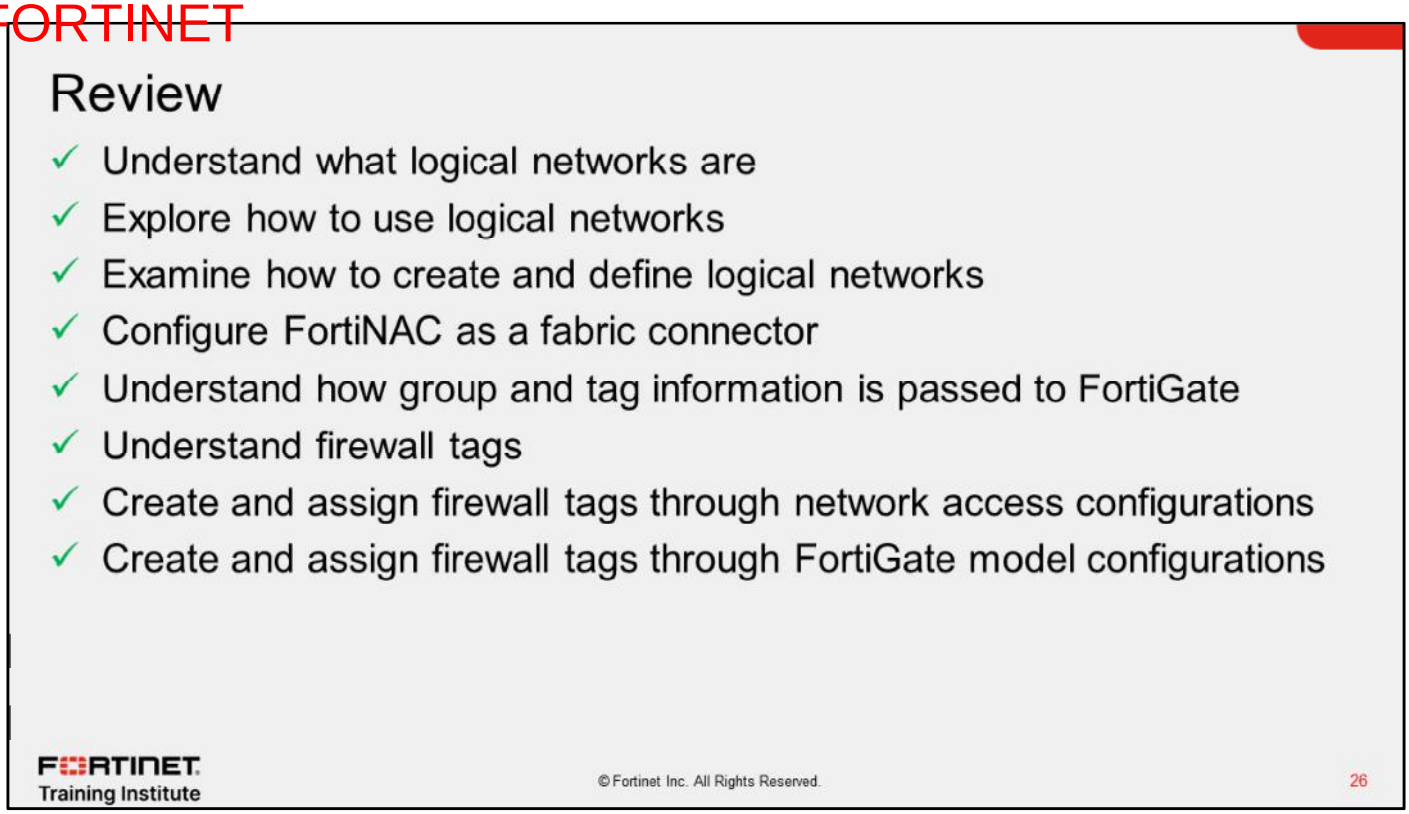


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

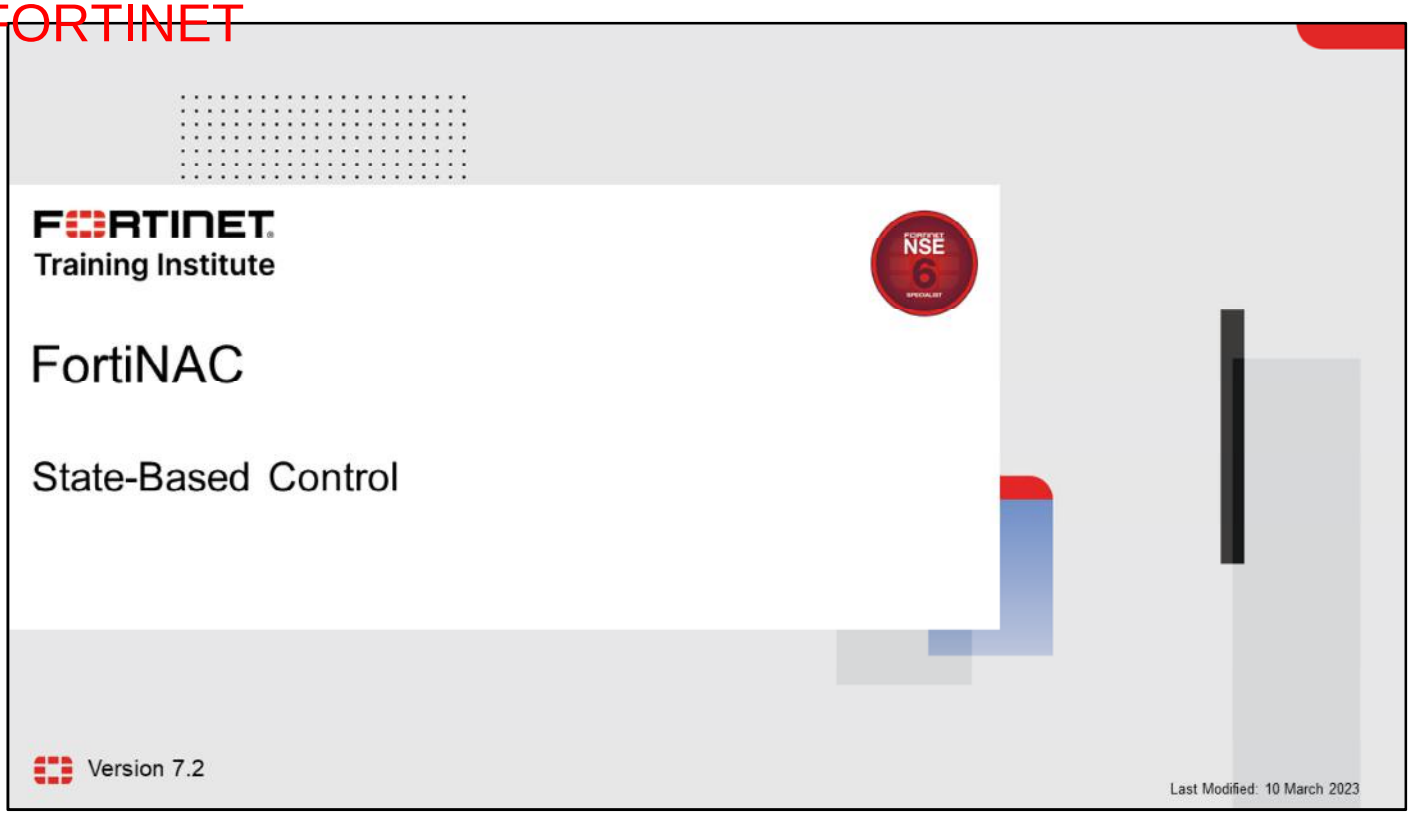


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to integrate FortiNAC into the Security Fabric for dynamic access control, and how to create and configure firewall tags.

Vouchers & Dumps are Available | WhatsApp +201224560923

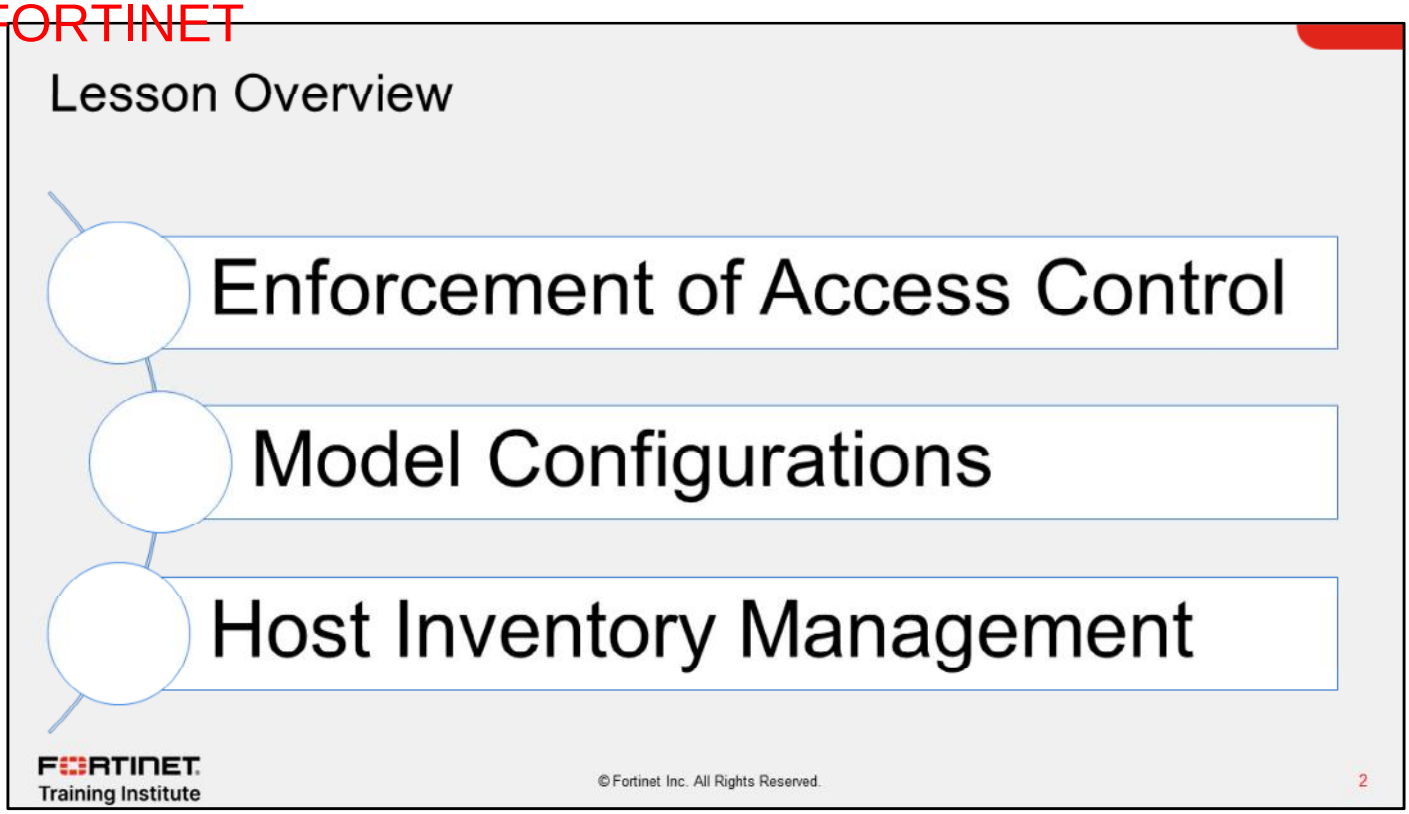
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about state-based endpoint control. This includes how FortiNAC uses its live inventory of network-connected endpoints in conjunction with its ability to manage the infrastructure at the point of connection for automated access control and isolation, as well as the different network-side configurations for deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

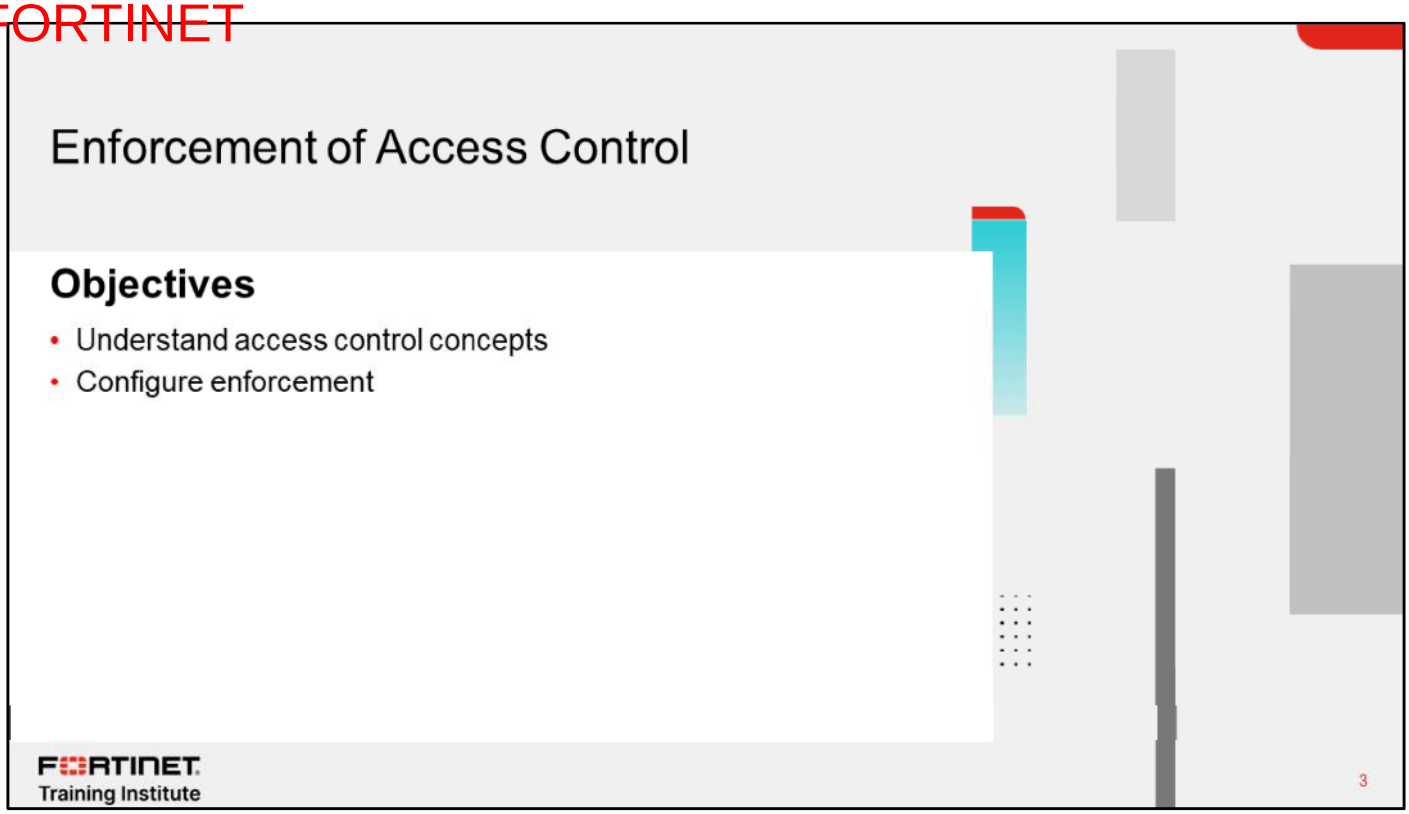
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

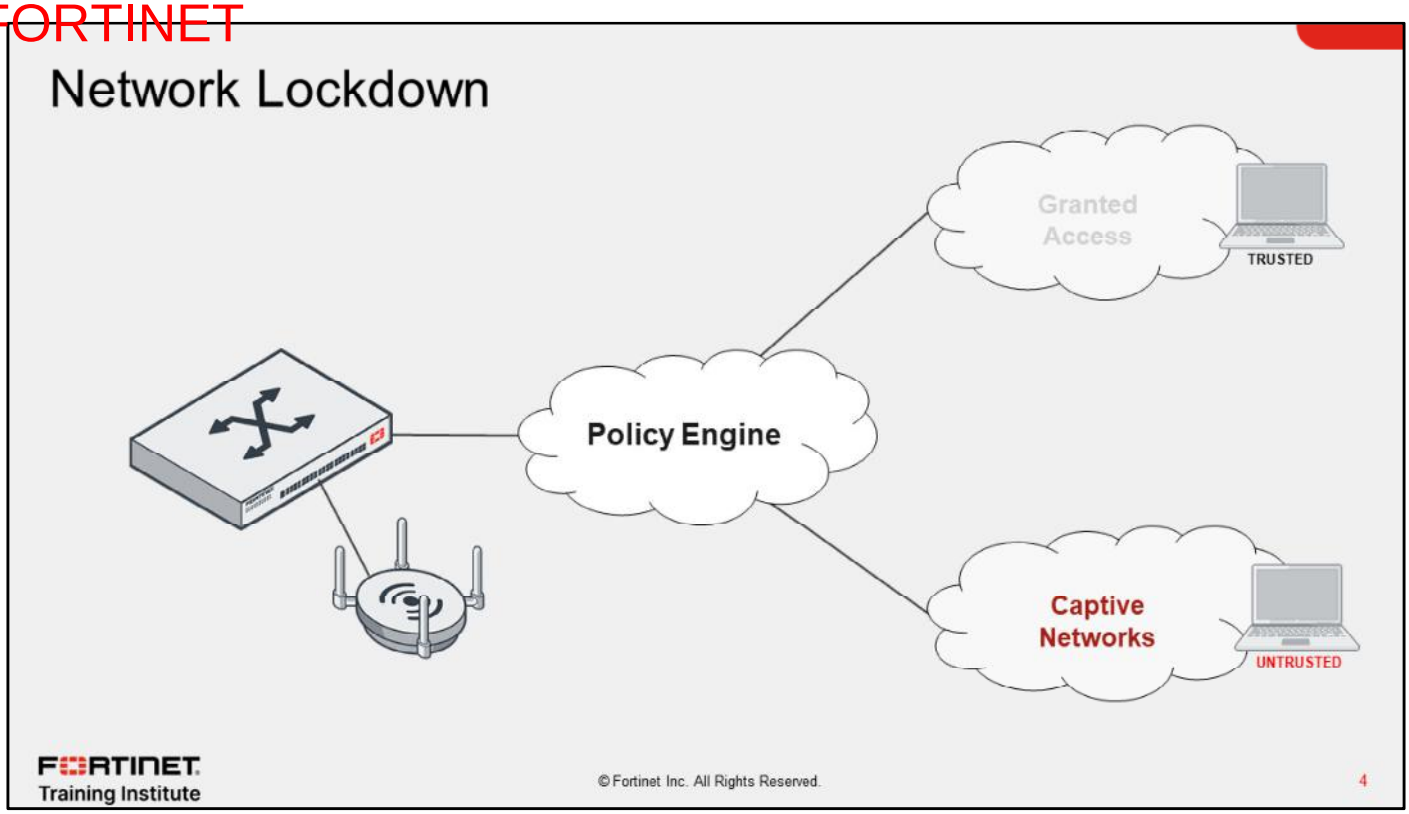


After completing this section, you should be able to achieve the objectives shown on this slide.

By understanding the concept of access control and the way in which it is enforced, you will be able to competently apply endpoint enforcement in your environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

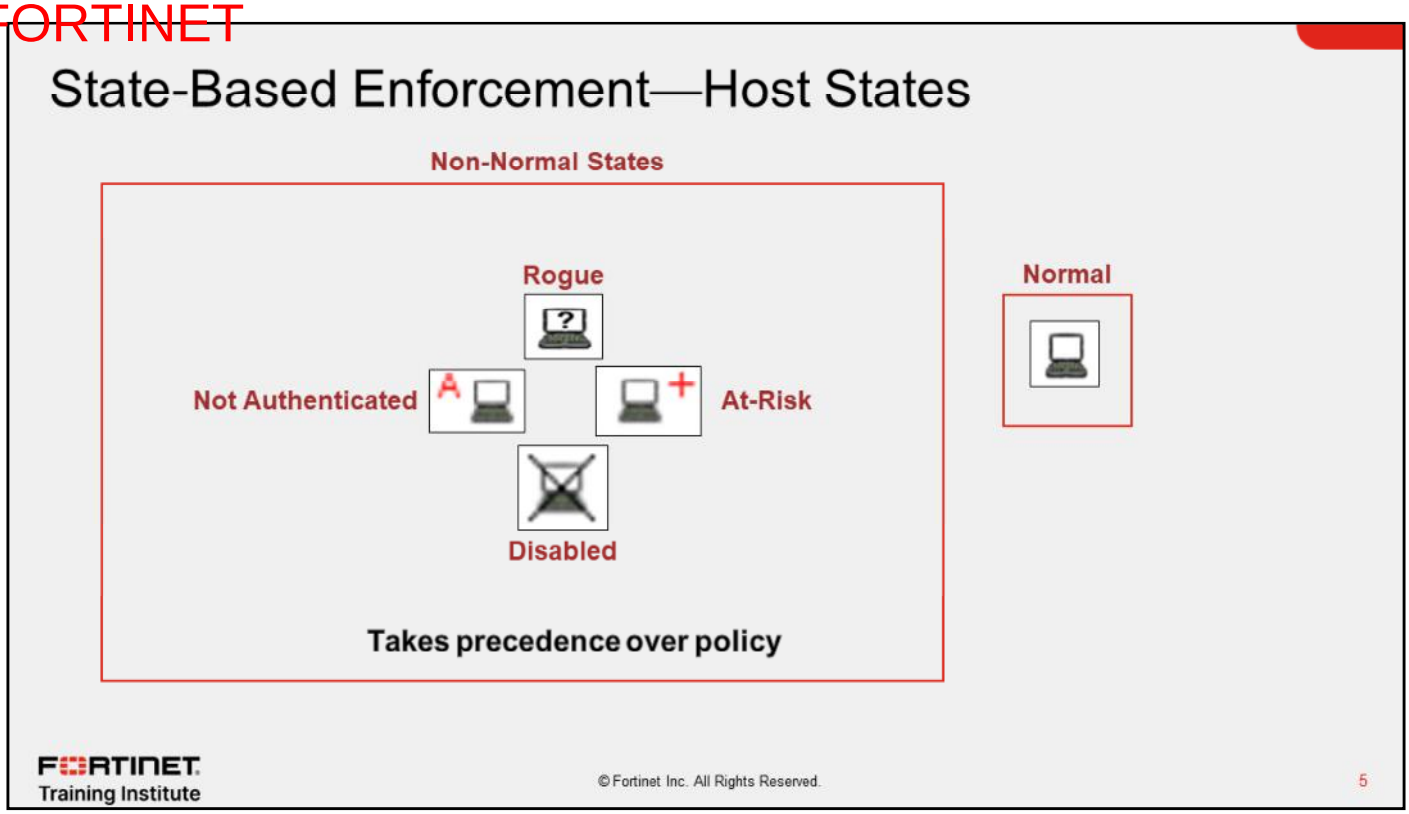


Enforcement of access control is the provisioning of network access by dynamically leveraging the network infrastructure to secure and segment endpoints appropriately. Access is provisioned based on the point of connection, and the host state in the FortiNAC database. The point of connection is a location parameter defined by a port group, in the case of wired ports, or within a controller, AP, or SSID, for wireless devices.

In its most basic form, often referred to as *friend or foe*, the FortiNAC policy engine is used to determine if a host connecting at a particular location should be allowed access to a production network, or if it should be isolated to a captive network. The state of the host determines the captive network a host is isolated to.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



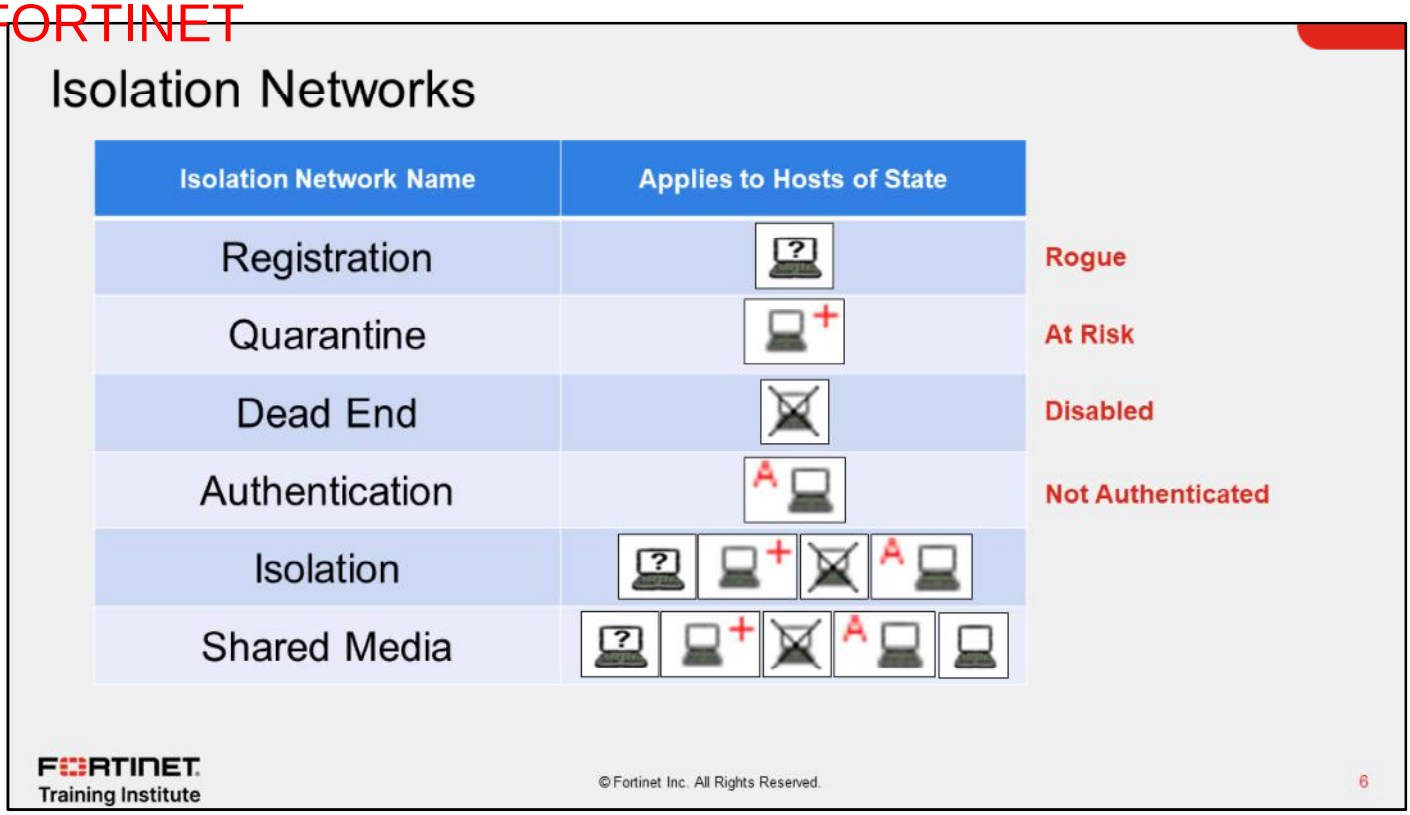
There are two situations when FortiNAC will configure network access for a host:
- Enforcement based on a host state
- Application of a network access policy

This lesson covers only enforcement based on state. As the name implies, the decision to enforce is based on the host's state in the FortiNAC database. Abnormal host state examples include: **Rogue**, **At-Risk**, **Not Authenticated**, and **Disabled**. A host state is assigned by FortiNAC and is a database attribute.
Each of these states is defined as follows:
- A state of **Rogue** is assigned if the device is not classified in the FortiNAC database. It could be anything—a printer, a card reader, an end station, and so on. Rogue devices are represented with an icon depicting a laptop with a question mark on the screen.
- A state of **At-Risk** indicates the host has failed a scan. This could be a policy compliance scan or an administrative scan. At-risk hosts are represented with an icon of a laptop with a red cross on the upper-right corner of the laptop screen.
- A state of **Disabled** indicates that the host has been administratively disabled within FortiNAC. This could be done manually by an administrative user, or as the result of an automated action. A disabled host is represented with an icon depicting a laptop with an X over it.
- A state of **Not Authenticated** indicates that no user record is currently associated as logged in to that host. User tracking with agents is one way to gather information about currently logged on users. A not authenticated host is represented with an icon depicting a laptop with a red A in a circle on the upper-left corner of the laptop screen.

Network access policies are enforced when a user or host matches a policy. State-based enforcement takes precedence over policy-based provisioning. Policies are created by the administrator and will be discussed in a separate lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Isolation networks are used to enforce access based on the state of a host. Each isolation network uses a captive portal web page to inform and assist the end user. In wired environments, these isolation networks are defined as VLAN IDs. In wireless environments, how they are defined may vary from vendor to vendor. The isolation network values used will depend on how traffic is segmented by that vendor. For example, Fortinet wireless access would be defined using a VLAN name, while Aruba would use a role value. Note that host state alone does not cause isolation. Isolation occurs only if the host point of connection is configured for enforcement for the current host state.

Registration is the process of on-boarding a host. This process will convert a host from being a rogue to being classified. The registration process, when carried out as an on-boarding exercise, takes place in the registration isolation network. The portal page is configured to provide on-boarding options.

The Quarantine isolation network is where hosts with an at-risk state are isolated. Remediation is the process of an at-risk host resolving the issues that caused it to be marked as at-risk. The portal page is configured to provide remediation steps to assist the user in clearing the at-risk state.

The Dead End isolation network is where hosts that have been designated as disabled are moved. By default there is no external access, not even to domains on the allowed domain list. The portal page is configured to inform the end user that they have been denied access to the network.

The Authentication captive network is where hosts that have no logged in user are isolated. The portal is configured to provide end-user authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Isolation Networks (Contd)

Isolation Network Name	Applies to Hosts of State	
Registration		
Quarantine		
Dead End		
Authentication		
Isolation		All except normal
Shared Media		All

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

7

The Isolation network is a special network that will handle hosts of any of the abnormal states. This means hosts of different states can all be isolated to a single network but continue to get customized captive portal pages based on their state.

The Shared Media network is another special purpose semi-captive network. Within this network, all hosts are designated as being in one of two groups: hosts that are in any state other than normal, and hosts that are in the normal state. For hosts that are in an abnormal state, this network works like the isolation network, with each host getting the appropriate captive portal for its state. Hosts that are trusted will be granted production access. This special network allows for access control to be extended to non-managed points of connection, such as unsupported or non-manageable switches or access points.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Logic to Determine Isolation

If Host State is	And System Group Membership is	Then Change VLAN to	Icon
Disabled	Physical Address Filtering (Device)	Dead End	
At-Risk	Forced Remediation (Port)	Quarantine	
Rogue	Forced Registration (Port)	Registration	
Not Authenticated	Forced Authentication (Port)	Authentication	
All	N/A	Shared Media	N/A
All Except Normal	N/A	Isolation	N/A
Normal	N/A	Policy Based or Default	

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

8

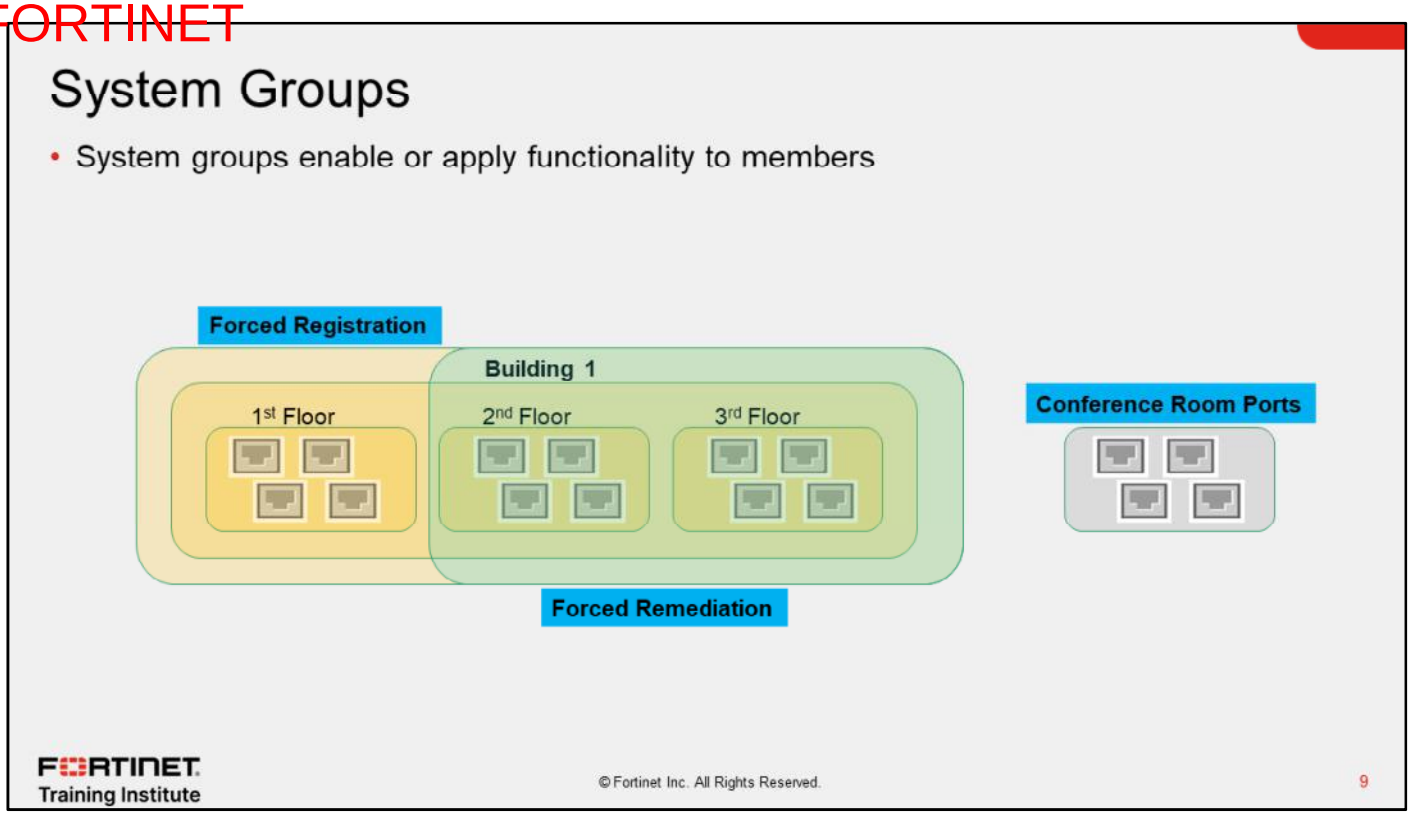
The logic used by FortiNAC when making the decision to isolate a host is summarized on this slide. When an endpoint connects to the network, FortiNAC looks it up in the database to determine its state. If the host does not exist in the database, and it does not match any enabled device profiling rules, it will be added and assigned the state of rogue. FortiNAC uses the first column as the column to key on, starting at the top and working down. For example, if a host with a state of rogue connected to the network, FortiNAC would use the third row down to determine if isolation is necessary. After the appropriate row has been identified, FortiNAC then reads to the right, applying AND logic between the first and second columns. If column one and column two, in the same row, are both true, then the host will be moved to the captive network shown in column three. On the GUI, the host will be represented with the icon in column four.

For example, if a host with the state of rogue connects to a port in the **Forced Registration** port group, FortiNAC will isolate that host by moving it into the registration captive network. The top four rows all function in the same way, with the slight exception of the first row, where the location parameter is defined by a device group, not a port group.

The bottom three rows consist of two special captive networks discussed earlier, and a row where hosts with a state of normal are provisioned.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



A determining factor for when an endpoint is isolated because of its state, is the point of connection to the network. You define this component using system groups.

The example on this slide shows five user-created groups. The first four of these groups are defining a geographic location, broken down to a desired level of granularity. There are three port groups representing the first, second, and third floors of Building 1. These groups have port models added as members, and have been nested within a fourth group called Building 1. These groups were created in this way to enforce registration and remediation on a floor-by-floor level or at the building level.

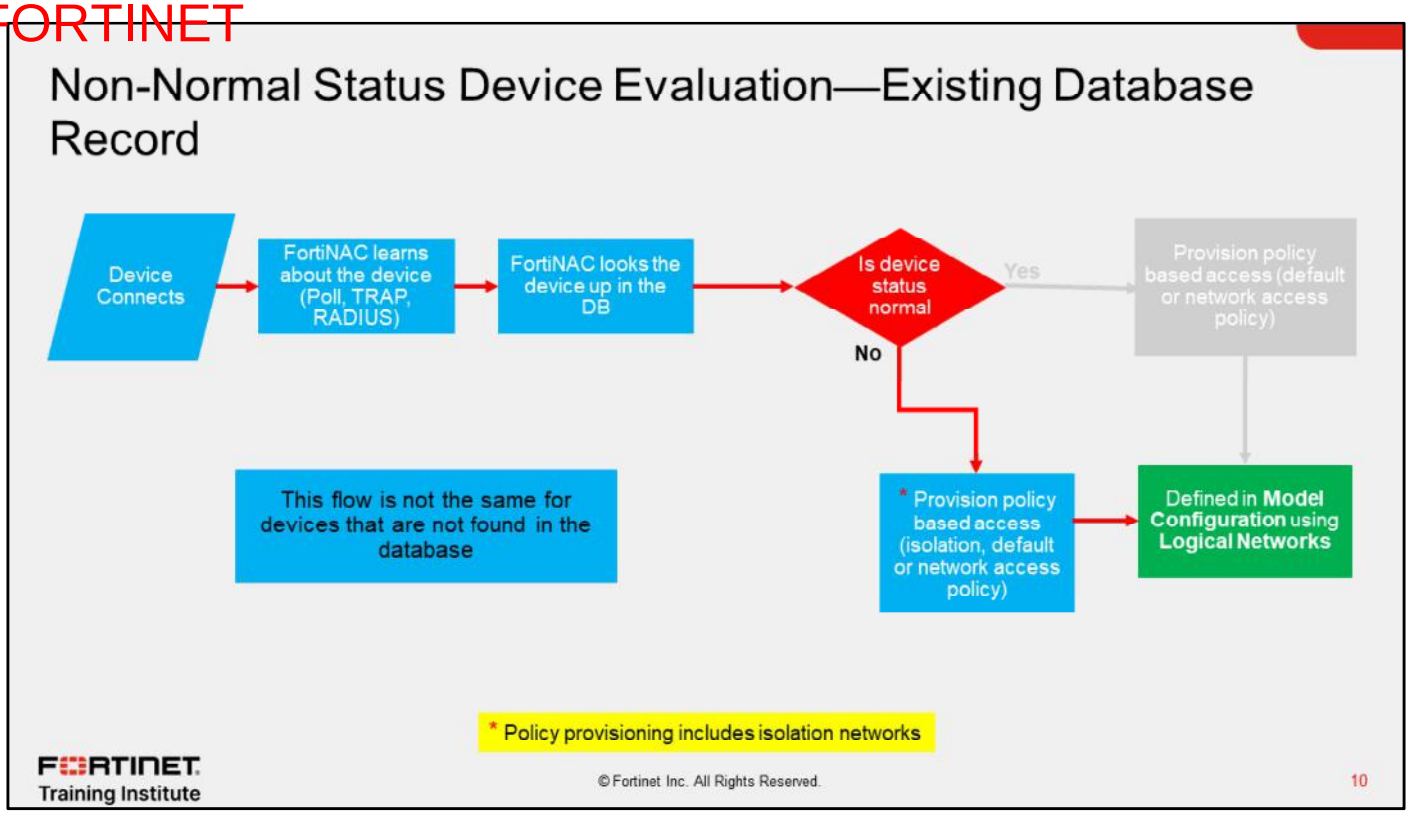
The fifth user-created group is named Conference Room Ports. This is a grouping based on functionality. These groups, organized as they are, do not enforce any type of control, they only organize the port elements. Enforcement is enabled when you add these groups to the appropriate system groups.

For example, the Building 1 group is added to the **Forced Registration** system group. Then the second and third floor ports are added to the **Forced Remediation** system group.

The result of this process is as follows:
Unknown or rogue endpoints that connect to any port in Building 1, which is any port in any of the three floor groups, will be isolated to the registration captive network. A host that has failed a policy or administrative scan, and has had its host state changed to at-risk, would be isolated to the quarantine captive network if it connected to any port in the second or third-floor port groups. Any other host state would result in the host being granted default network access. A change in the point of connection could also change the provisioned access. For example, a rogue host connecting to a conference room port it would be granted default access. An at-risk host connecting to a conference room port or a first-floor port would also be granted default access. Those examples assume that the ports within the conference room ports group are not also members of any other group. The logic that applies to these results was shown on the previous slide in the logic table.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide demonstrates the device evaluation process for hosts that exist in the database and do not have a status of normal (rogue, at-risk, disabled, non-authenticated).

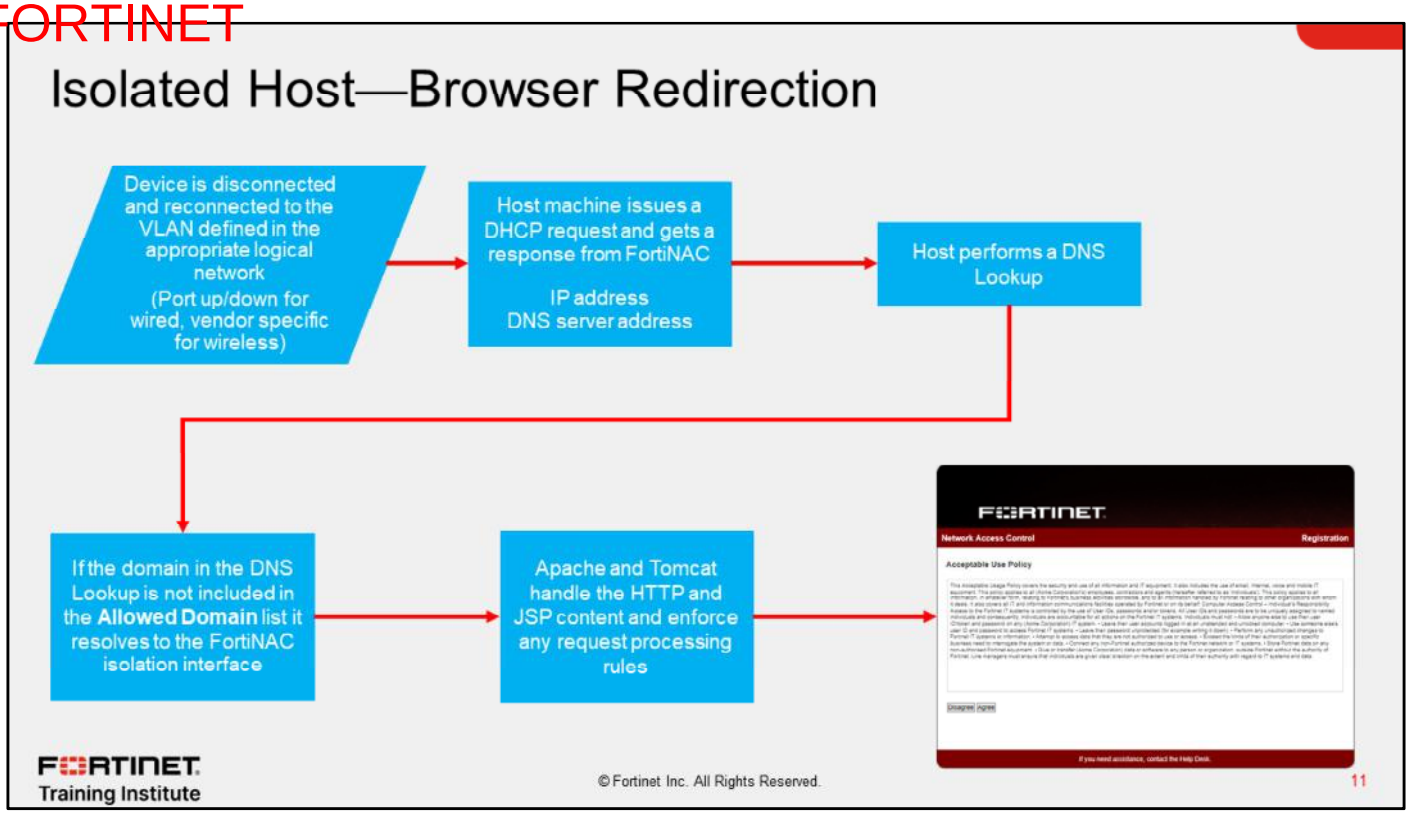
1. The device connects.
2. FortiNAC learns of the connection. This is often done using Layer 2 polling, MAC notification traps, or RADIUS. Other methods may be used, depending on the vendor of the infrastructure.
3. FortiNAC queries the database for the connected device.
4. FortiNAC determines if the point of connection is under enforcement for the current non-normal device status based on enforcement port group (**Forced Registration**, **Forced Remediation**, **Forced Authentication**, and so on). If it is, the device will be isolated to the appropriate isolation VLAN defined in the device model. If the point of connection is not under enforcement for the current device status it will be provisioned based on a matching network access policy VLAN or the default VLAN.

How the device is provisioned is based on logical networks and how they are defined for each infrastructure device. The definition for these logical networks is set in the **Model Configuration** view of the infrastructure device. Provisioning based on policy includes isolation networks. For example, the policy to isolate an at-risk host is based on the status of the device and the point of connection (the port is in the Forced Remediation group).

The evaluation process for hosts that have not been seen before (not in the database) is covered in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When hosts have been assigned to a captive network, they will be directed to a captive portal page. The page presents the user with additional information and/or capabilities, to resolve the non-normal host state. For example, a rogue host isolated to the registration captive network will be presented, by default, with a registration page that provides options for onboarding the host. The onboarding process will classify the host.

When a host is isolated on a wired port, FortiNAC will shut down the port causing the host's link to drop, the VLAN to change, and the port to be re-enabled. This will result in the host requesting a new IP address, which begins the captive portal page presentation process. This process is shown on the slide as a timeline going from left to right.

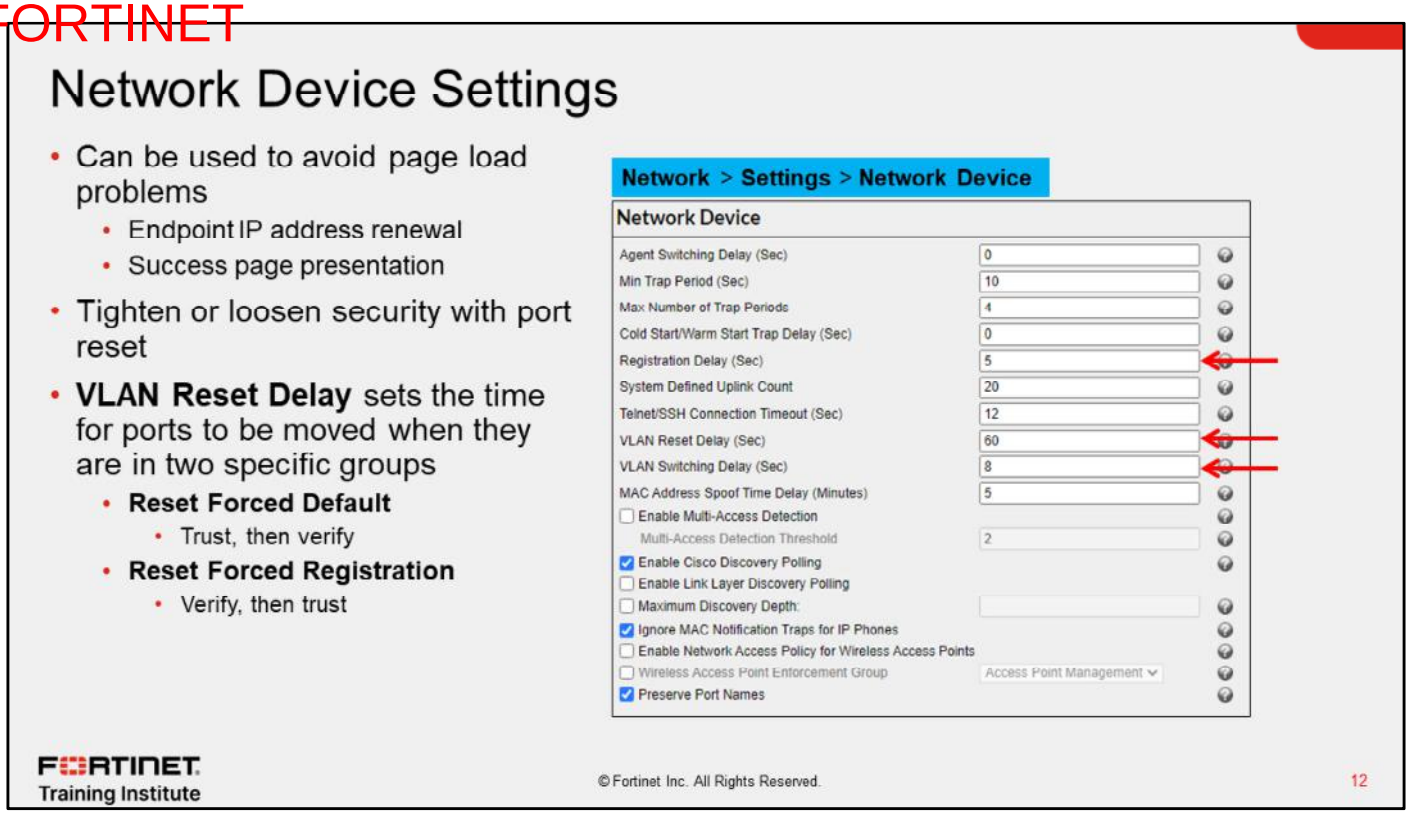
First, the host gets a new IP address appropriate for the captive network it is in, with a DNS address that is the FortiNAC captive portal interface.

When the host attempts to resolve a domain by name, FortiNAC, which has been designated as the DNS server, will respond with its own address, masquerading as the domain the host is attempting to resolve.

FortiNAC will then present the appropriate captive portal page to the isolated host.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can modify network device settings to customize the isolation process. Timers associated with the isolation of hosts can impact the end user experience, and VLAN reset timers can be used to increase or decrease the speed that ports are reset to the default or registration VLAN assigned to the port.

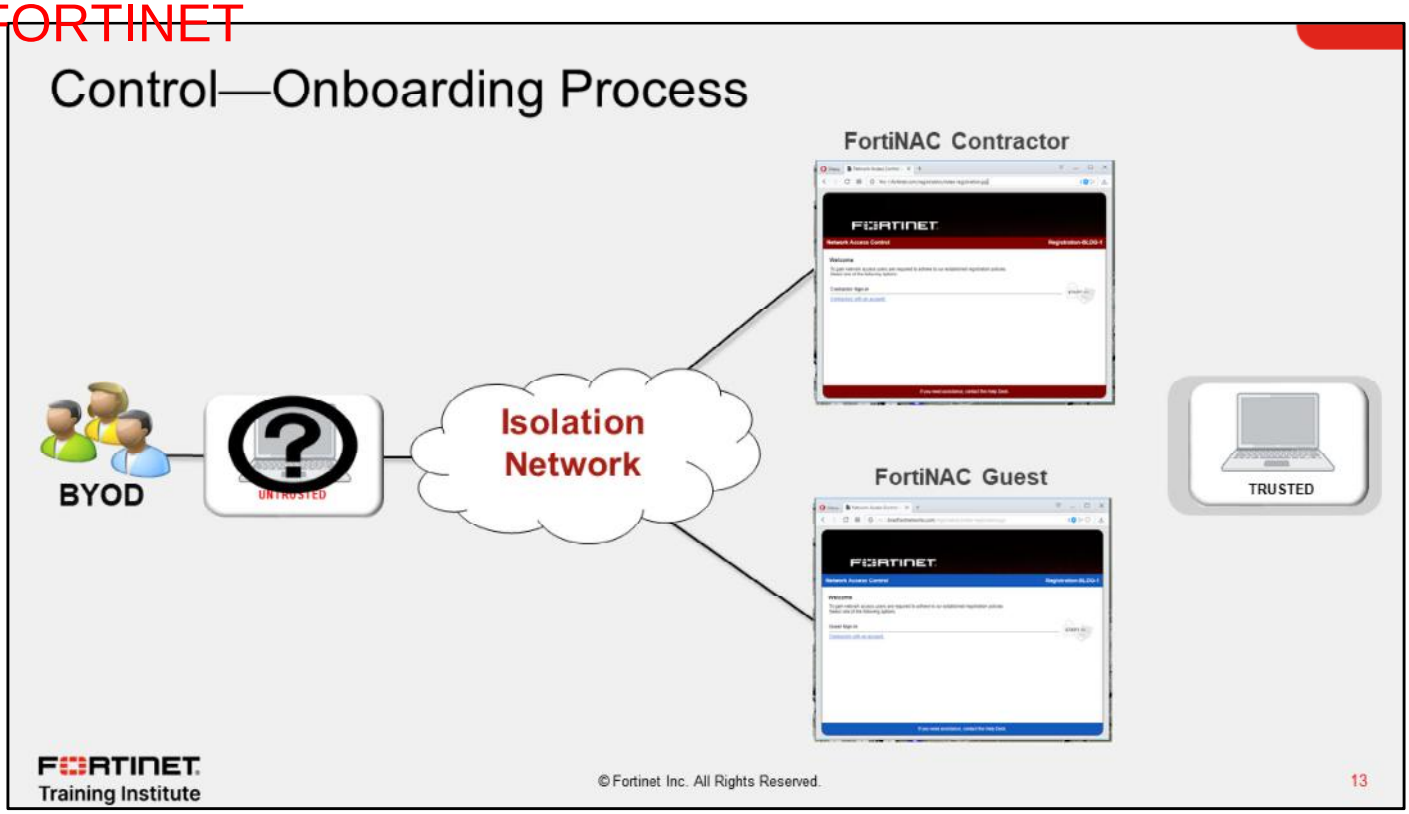
There are three settings highlighted on this slide. The **Registration Delay** setting is the number of seconds a host is held in the registration isolation VLAN after they have supplied valid credentials. The purpose of this setting is for the presentation of the registration success page. If the value is set too low, the hosts port may change before the page redirect completes, resulting in a page load error that may confuse the end user. Set too high and the registration process will take longer.

The VLAN reset feature allows you to designate ports to be moved to a defined default VLAN, or the Registration VLAN, when a host disconnects form the port. This is often used in high security environments where wired ports can not be left on an access VLAN when they are not in use. The **VLAN Reset Delay** is the number of seconds FortiNAC will wait, after a host disconnects, before moving ports in the **Reset Forced Default** or **Reset Forced Registration** port groups to the default or registration VLAN. This feature applies to ports in the **Reset Forced Default** or **Reset Forced Registration** port groups only. The access for ports in the **Reset Forced Default** group can be thought of as *trust, then verify* because a connecting host could start on a production VLAN. Ports in the Reset Forced Registration group can be thought of as *verify, then trust* because connecting hosts will start in the registration isolation VLAN.

When FortiNAC determines, based on a connected host, that a port needs to be moved from one VLAN to another (due to a network access policy or the state of the connecting host), the connected host needs to get an IP address for the new VLAN. During the VLAN change FortiNAC will keep the port down for the designated number of seconds in the **VLAN Switching Delay** field. If the delay is too short, some hosts will fail to request a new address and will not be able to communicate after the change.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can customize onboarding options for different types of isolated hosts. Allowing users to transition a rogue or non-authenticated device to a classified or authenticated device is an important capability of FortiNAC in many environments.

You can develop separate processes with unique content to support various types of user-driven onboarding procedures.

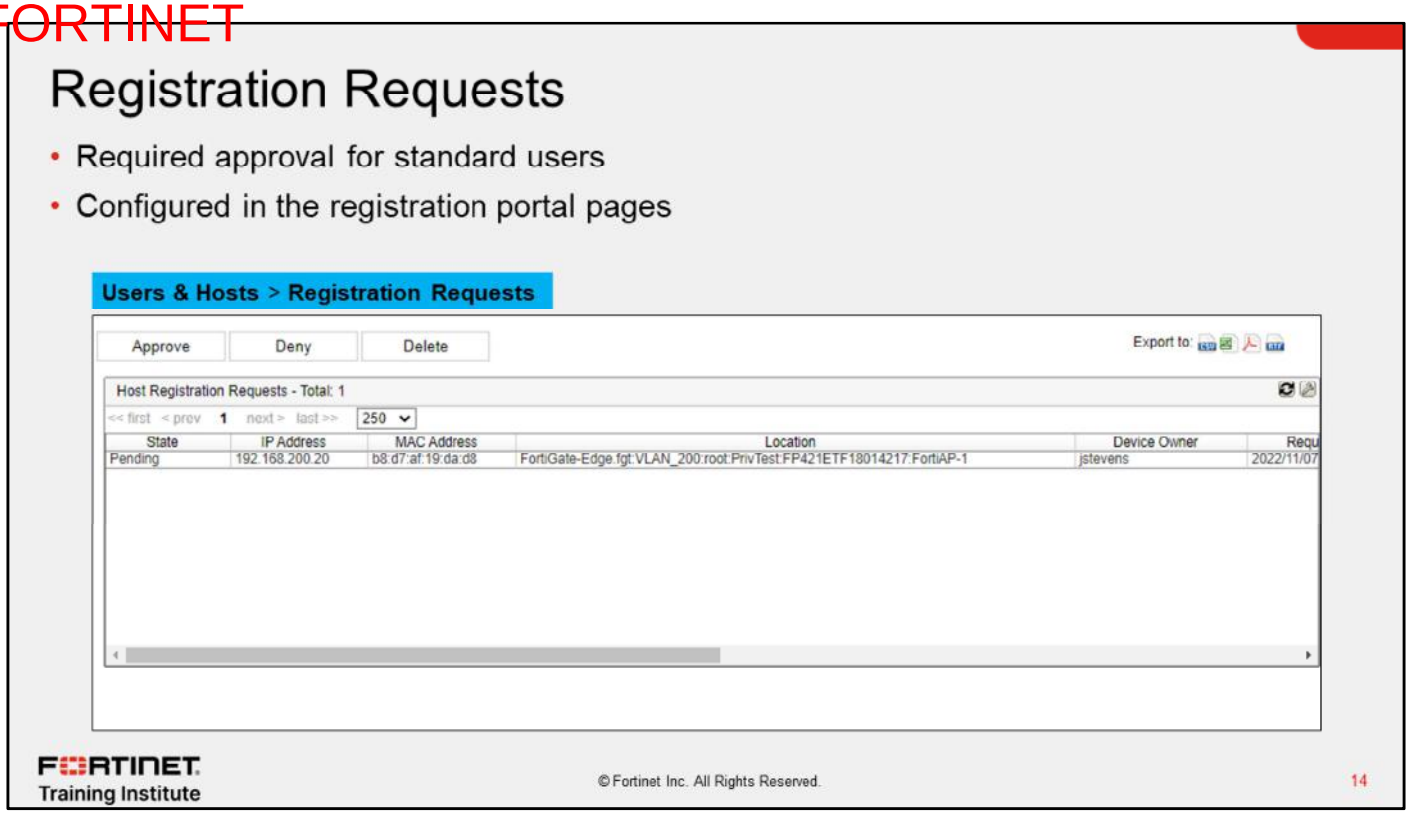
For example, a rogue connecting to an enforced point of access is isolated and presented with the appropriate onboarding portal content. The portal content that is presented can be customized based on location, time, OS, and/or user choice criteria, or a combination of any of these.

During the onboarding of a host, the state will change from rogue to normal, and an association will be made between the host and the user that onboarded it. The host will then be granted the appropriate access.

This method of onboarding is most often used for BYOD devices, typically those of guests, contractors, students, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

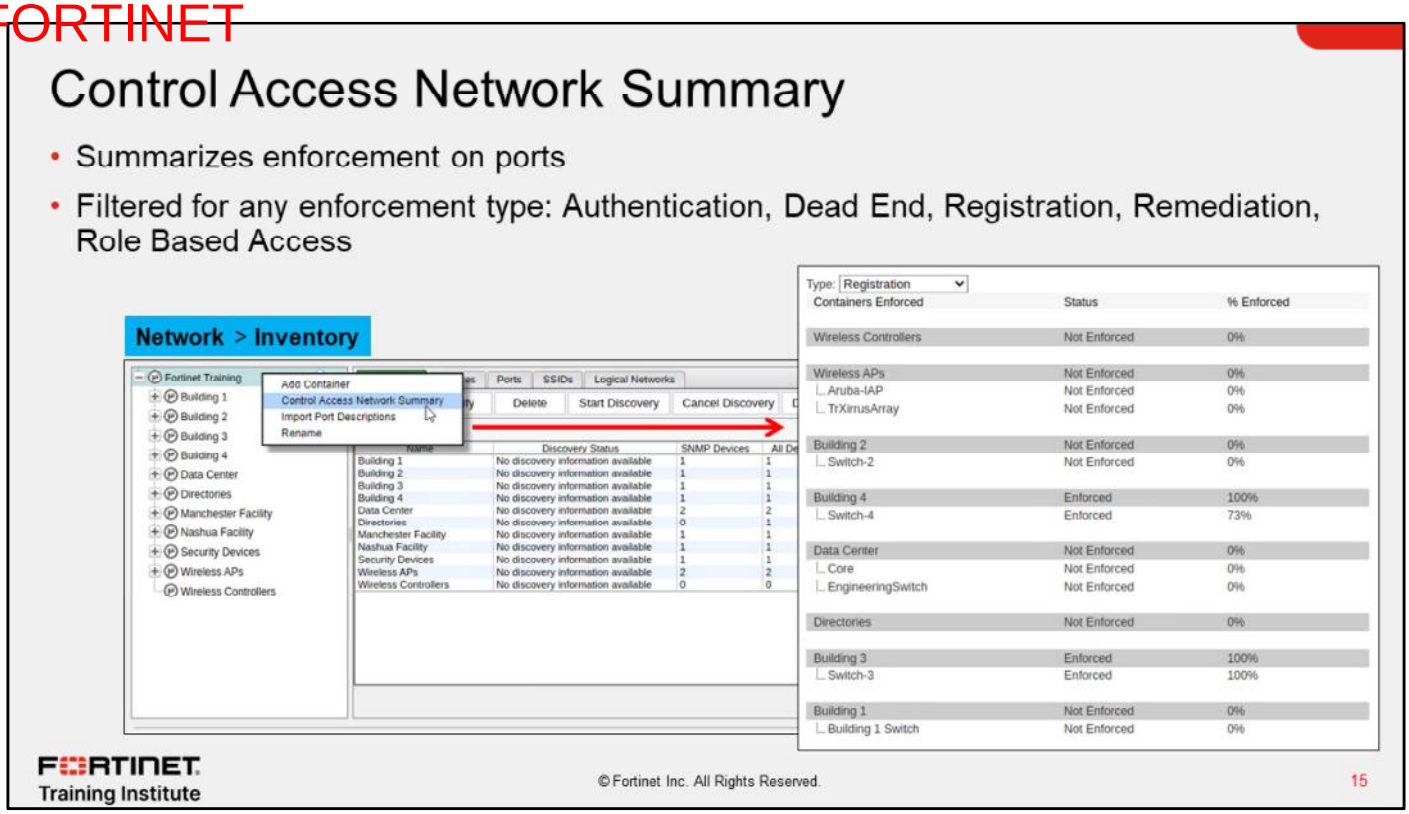
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In some environments, it may be required that employees attempting to on board personal BYOD type devices get approval prior to being granted access. You can require standard users (non-guests or contractors) to require approval similar to a self-registered guest. The requirement for approval is setting is enabled in the portal page configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



A useful administrative tool for validating appropriate enforcement is the **Control Access Network Summary** view. This view is accessible from the **Inventory** view by right-clicking the root container in the topology tree.

This view summarizes the percentage of devices within each topology container that have some level of enforcement enabled, and the percentage of ports under enforcement on a device-by-device level.

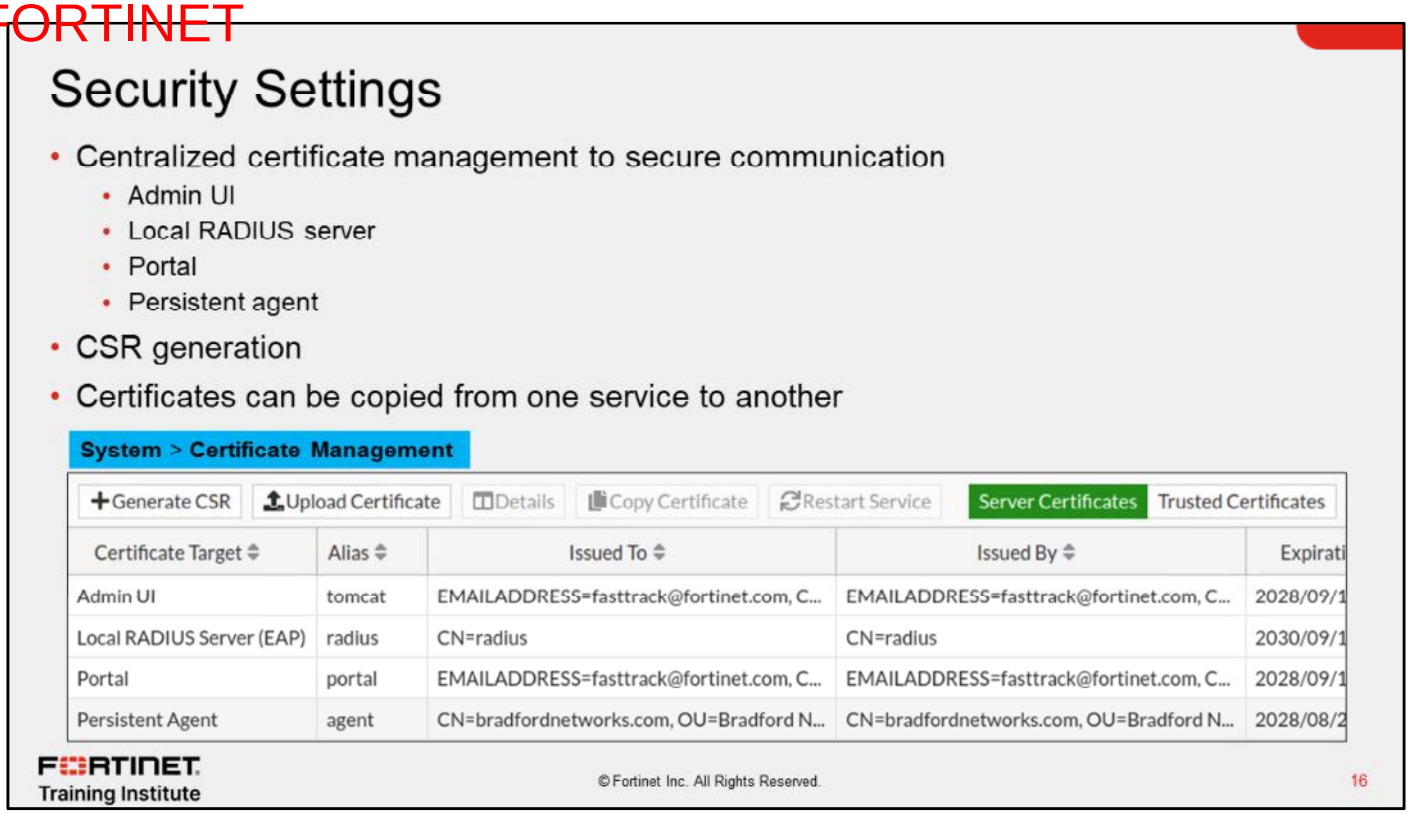
In the example shown on this slide, Building 3 has enforcement applied on 100% of the devices in that container, and on 100% of the ports on the switch. Building 4 has enforcement applied on 100% of the devices in that container, but Switch-4 within that container, has only 73% of its ports in enforcement system groups, such as **Forced Registration**.

This view is used to validate that nothing is left unintentionally unenforced. For example, a new switch could be modeled in the network inventory, and the ports accidentally left out of any enforcement group.

An administrative best practice would be to check this view frequently.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



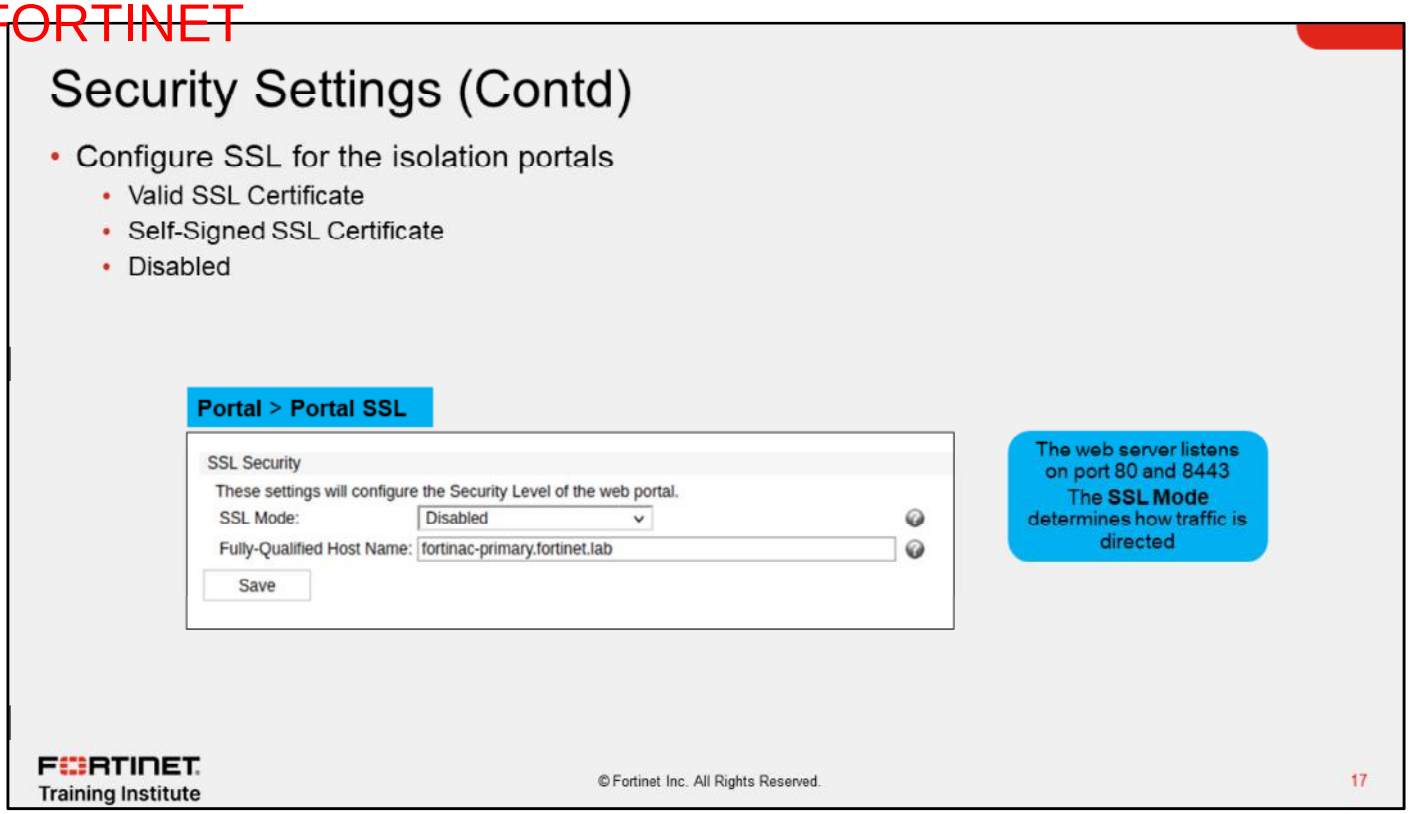
In most environments, secure communication between administrators, endpoints, and agents is a required aspect of a deployment. You configure this secure communication using certificates on the **Certificate Management** view.

The **Certificate Management** view provides the ability to manage certificates with different encoding schemes and file formats.

CSRs can be generated and certificates uploaded from this view. Once a certificate has been configured for use by one of the services, it can be easily copied for use by any other service.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Portal SSL** page is used to set the **SSL Mode** and the **Fully-Qualified Host Name** of FortiNAC. The web server listens on both port 80 and port 8443 for web traffic coming into the portal. The **SSL Mode** setting determines how the web traffic is directed when reaching the captive portal.

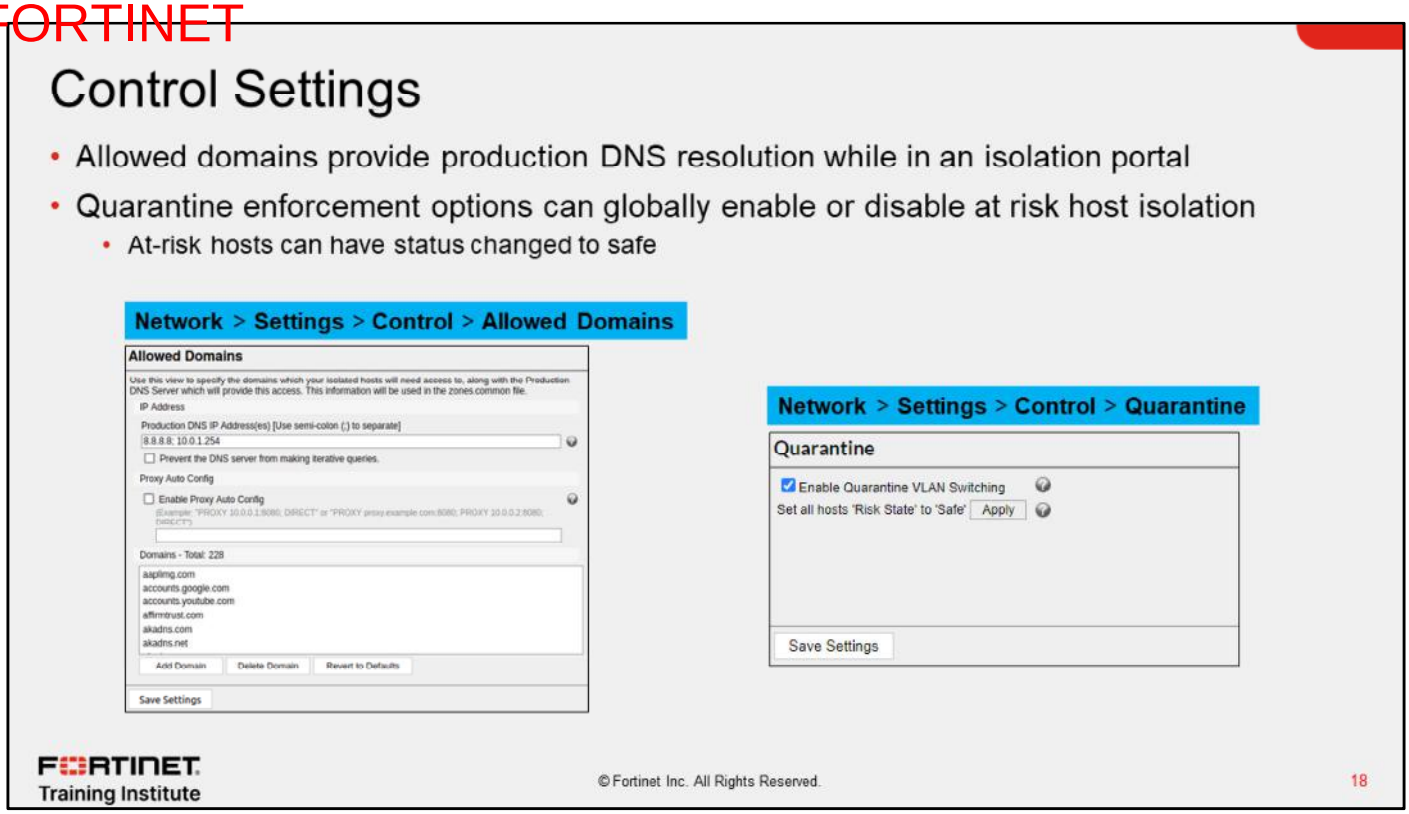
The **SSL Mode** setting options are:

- **Valid SSL Certificate**: directs web traffic from port 80 to port 8443 and presents a certificate authority-signed valid SSL certificate.
- **Self-Signed SSL Certificate**: directs traffic from port 80 to port 8443 and presents a self-signed SSL certificate.
- **Disabled**: directs all traffic to port 80 and presents a self-signed SSL certificate.

You must configure the **Fully-Qualified Host Name** field with the fully qualified hostname of FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiNAC provides Isolated hosts IP addressees and DNS configurations using DHCP. The FortiNAC isolation interface will be defined as the DNS server. Hosts are directed to isolation portals using DNS resolution. Any domain not in the allowed domain list will resolve to the FortiNAC isolation interface.

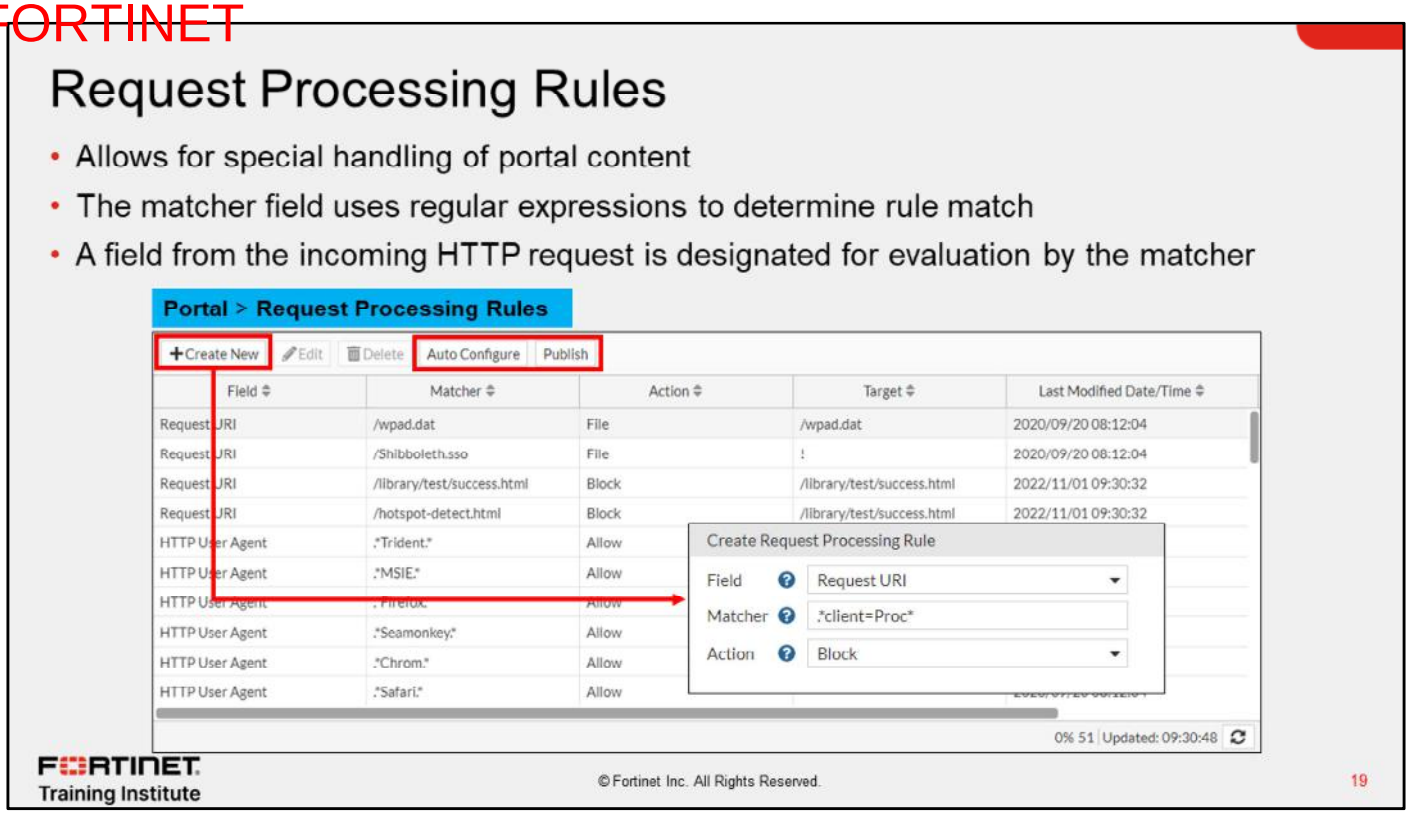
Note that, by default, the Dead End isolation network does not allow access to these domains. The **Production DNS IP Address(es)** field is where the DNS servers that will be used for DNS lookups of all allowed domains are listed, semi-colon separated if there are more than one. The **Enable Proxy Auto Config** section is for environments that use a proxy server. This populates the `wpad.dat` file with the information that allows a host to learn about the proxy server.

Any host attempting to perform a DNS lookup for one of the domains in the list, while in a captive network (other than the Dead End), will have the lookup forwarded to the DNS server(s) designated in the **Production DNS IP Address(es)** section, and the results of the query will be passed back to the host. This allows the host to resolve the IP address of the actual domain and not be redirected to the captive portal. You must configure the network infrastructure to allow access to the desired domains.

The **Quarantine** settings allow the administrator to globally enable or disable quarantine VLAN switching, or set the risk state of all hosts to safe. Setting the risk state of all hosts to safe can be useful in the event that a scan profile generates significant numbers of false negatives, which could result in hosts being unintentionally isolated.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When an HTTP request is processed by the isolation interface of FortiNAC, customization of how the traffic is processed may be necessary. In the **Request Processing Rules** view you can create and mange the rules that govern the incoming HTTP traffic. You can define the field that will be evaluated by the matcher to determine enforcement of the selected action. There are four possible actions: **Allow**, **Block**, **Forward** and **File**.

The **File** and **Forward** actions will require you to enter a URL. It should be noted, that if an action is changed from **File** or **Forward** to **Allow** or **Block**, any existing **Target** value will remain but will not be used. There are some instances of this, used as part of the auto configuration feature.

The **Auto Configuration** button is where you can enable or disable the captive network assistant (CNA) on Mac OS X and iOS devices. When disabled the rules that will cause the CNA to appear are modified, or created if they do not exist, to prevent it from launching while in an isolation network.

The **Publish** button will sort all existing rules, write them to the portal configuration and restart the portal service.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which captive network will not allow DNS lookups for allowed domains?
   A. Quarantine
   ✓ B. Dead End

2. Which host state displays a red + (plus sign) on the upper-right side of the host icon?
   A. Disabled
   ✓ B. At risk

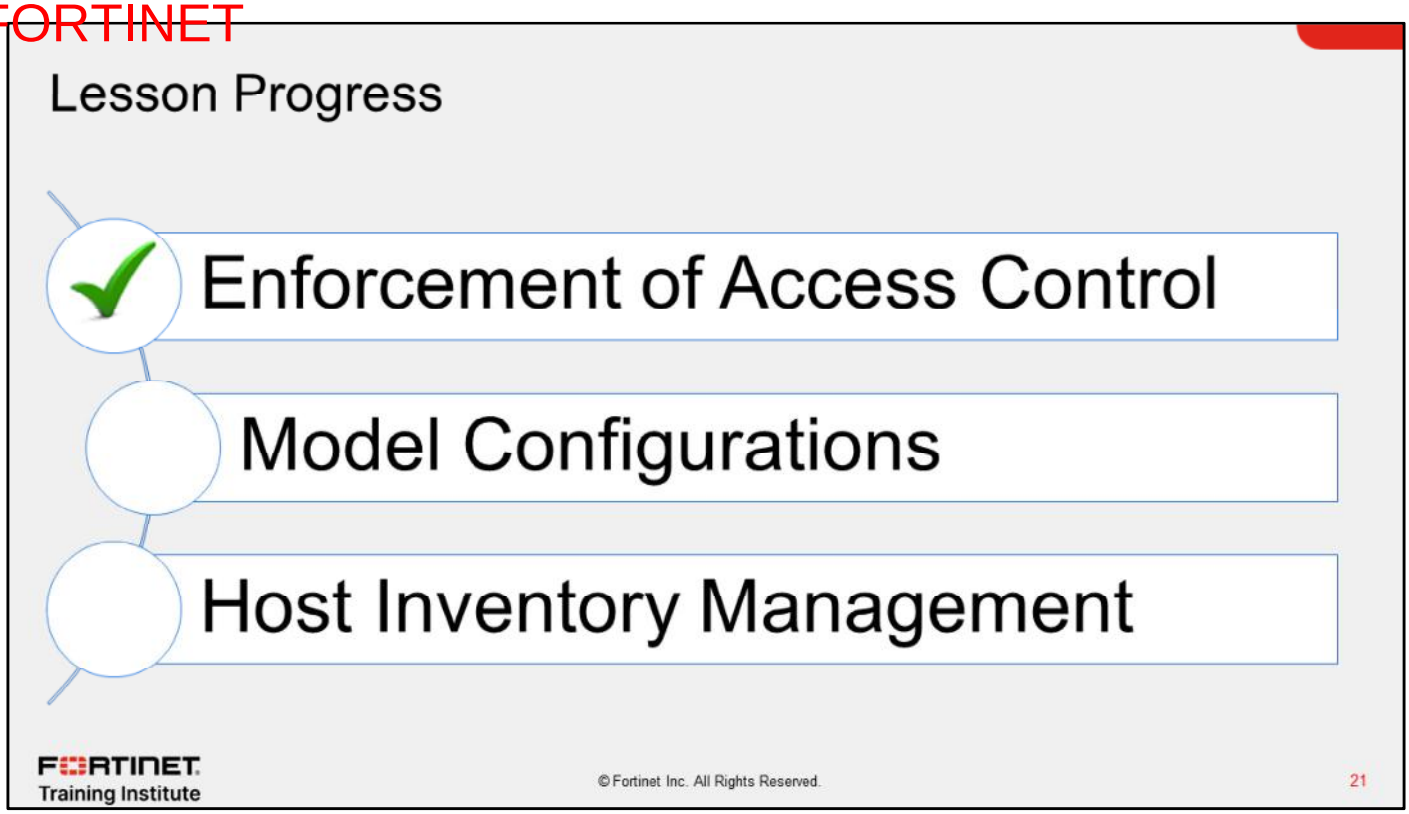
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

20

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

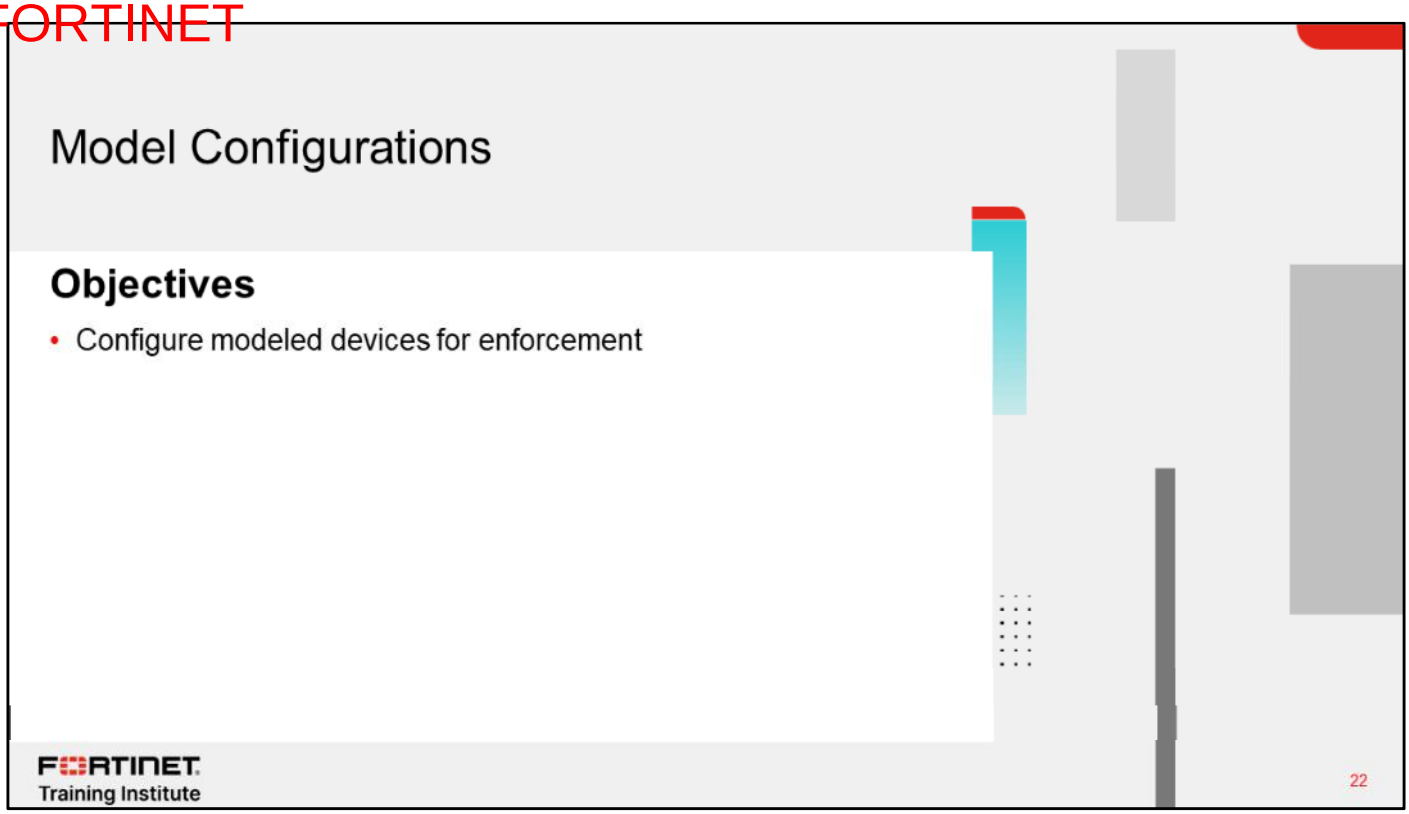


Good job! You now understand how to enforce access control.

Now, you will learn how to configure state-based isolation networks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

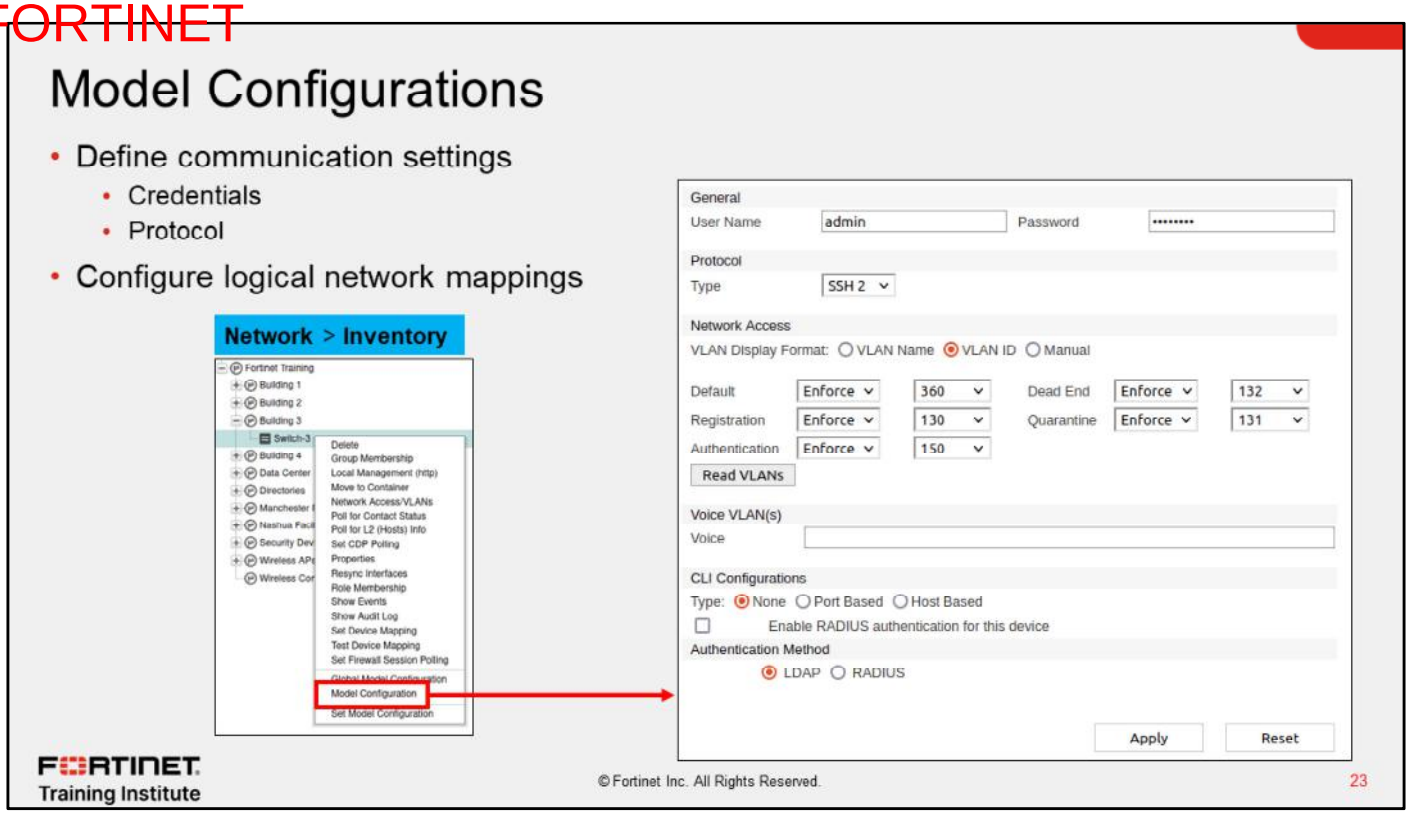


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating a competent understanding of model configurations, you will be able to appropriately deploy state-based enforcement.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To set model configurations for a device, locate the desired device in the inventory view and right-click it. The right-click menu will display a list of options, with configuration settings at the bottom. The fields available for configuration will vary, depending on the type of device.

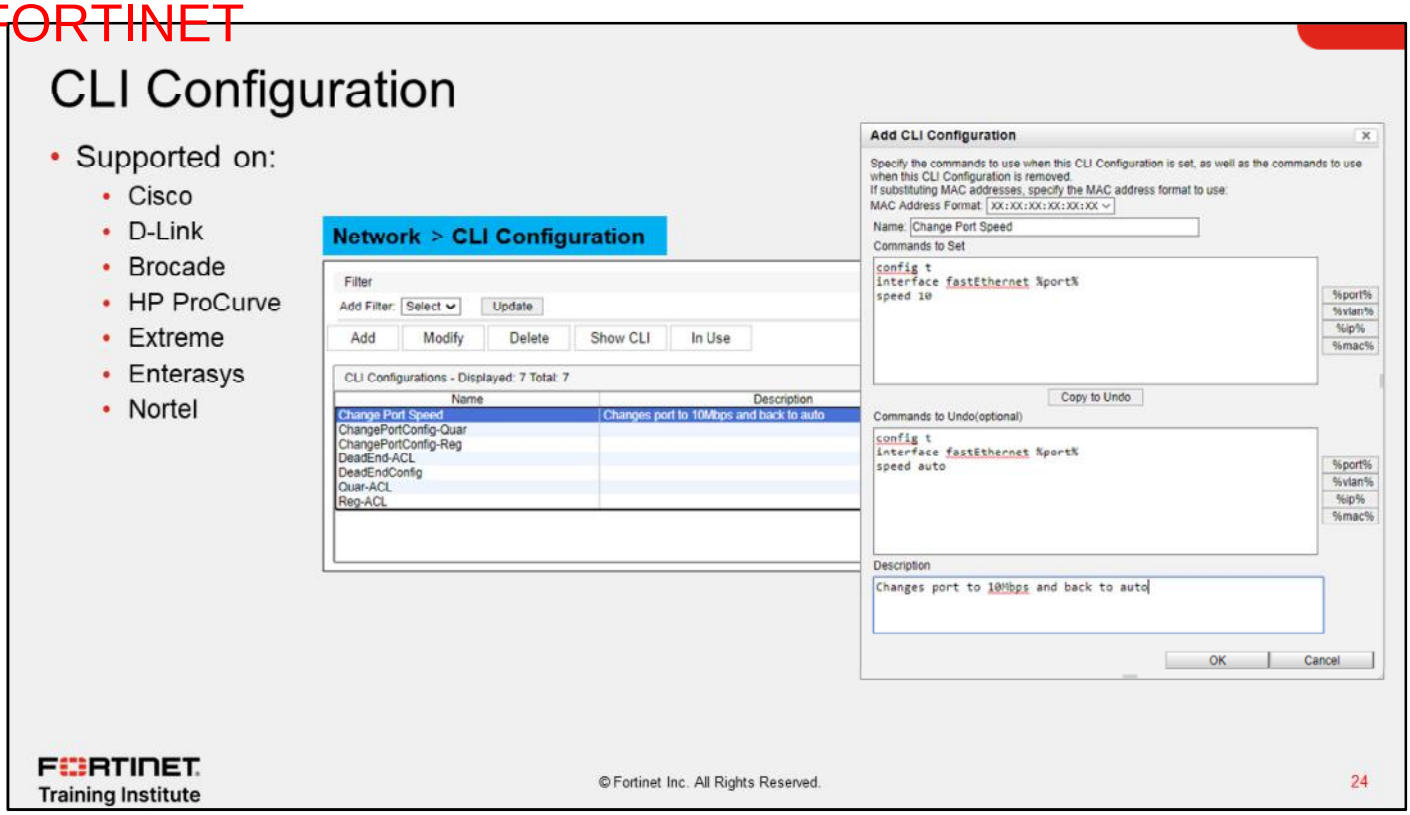
The example on this slide shows most of the possible configuration options. The first two sections, **General** and **Protocol**, define the credentials and protocol FortiNAC will use for device communication. The **Network Access** section is where the logical networks are defined for this device. The layout of this section may vary from device to device. For example, the VLAN display format options may not be available within all model configurations. If they are not, you must enter the isolation VLAN IDs manually.

The **Default** logical network is a little different, and does not define an isolation VLAN, but instead defines the default VLAN for each port on this device. Default VLANs are automatically assigned for each port to the VLAN the port was on when the device was initially modeled. Setting a value for the default VLAN here will override the initial VLAN delegations for all the ports.

It is important to keep in mind that the isolation VLANs are defined device-by-device, and default VLANs can be defined at the port or device level.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



A CLI configuration is a set of commands that are normally issued through the CLI of a device, such as a switch or router. The **CLI Configuration** window allows you to create individual sets of commands, name them, and then reuse them as needed. When a CLI configuration is applied, the commands contained within it are sent to the designated device. On the **CLI Configuration** window you can designate the MAC address format. This is important if the configuration is going to use the `%mac%` variable and inject a MAC address as part of a CLI command. You enter each command just as it would be if you were entering them directly through the CLI of the device. You can insert variables into the commands and FortiNAC will replace these variables with the appropriate values, depending on the way in which the CLI configuration is triggered.

There are three ways a CLI configuration can be triggered:
- State-based isolation of a host
- Policy-based access configuration
- The scheduler tool

The first two triggers can leverage the `%port%`, `%vlan%`, `%ip%`, and `%mac%` variable options as long as the selected variables would be known as a result of the trigger.

When using the scheduler tool to trigger a CLI configuration, no variables can be used as part of the configuration, because a specified date and time does not include any information relatable to the variable options.

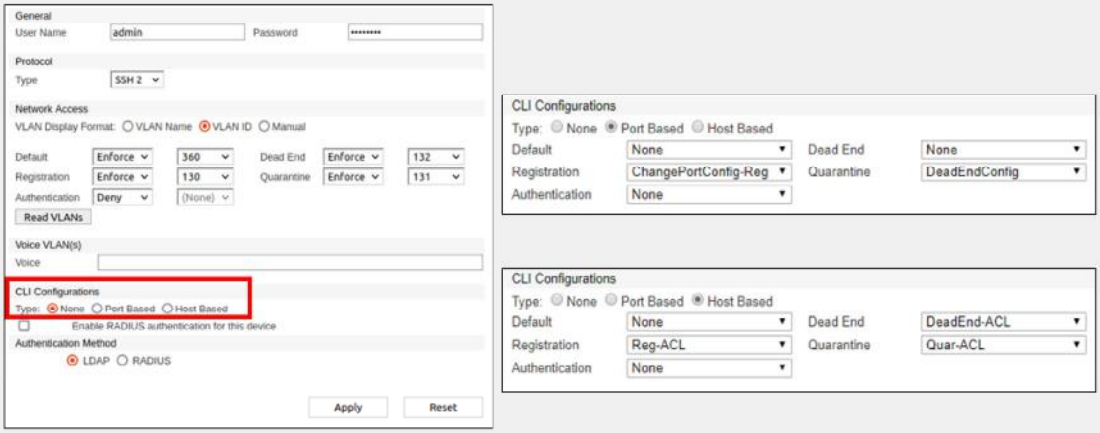
You cannot use the **Commands to Undo (optional)** field for CLI configurations triggered by a scheduled task. However, for state-based triggering, the commands in this field are carried out when the host state changes. For policy-based access configurations, these commands are carried out when the host disconnects, or when the policy no longer applies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Model Configurations–CLI Configurations

- Two CLI configuration types
  - **Port Based**–Apply the CLI during the VLAN change
  - **Host Based**–Apply the CLI and do not change the VLAN



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

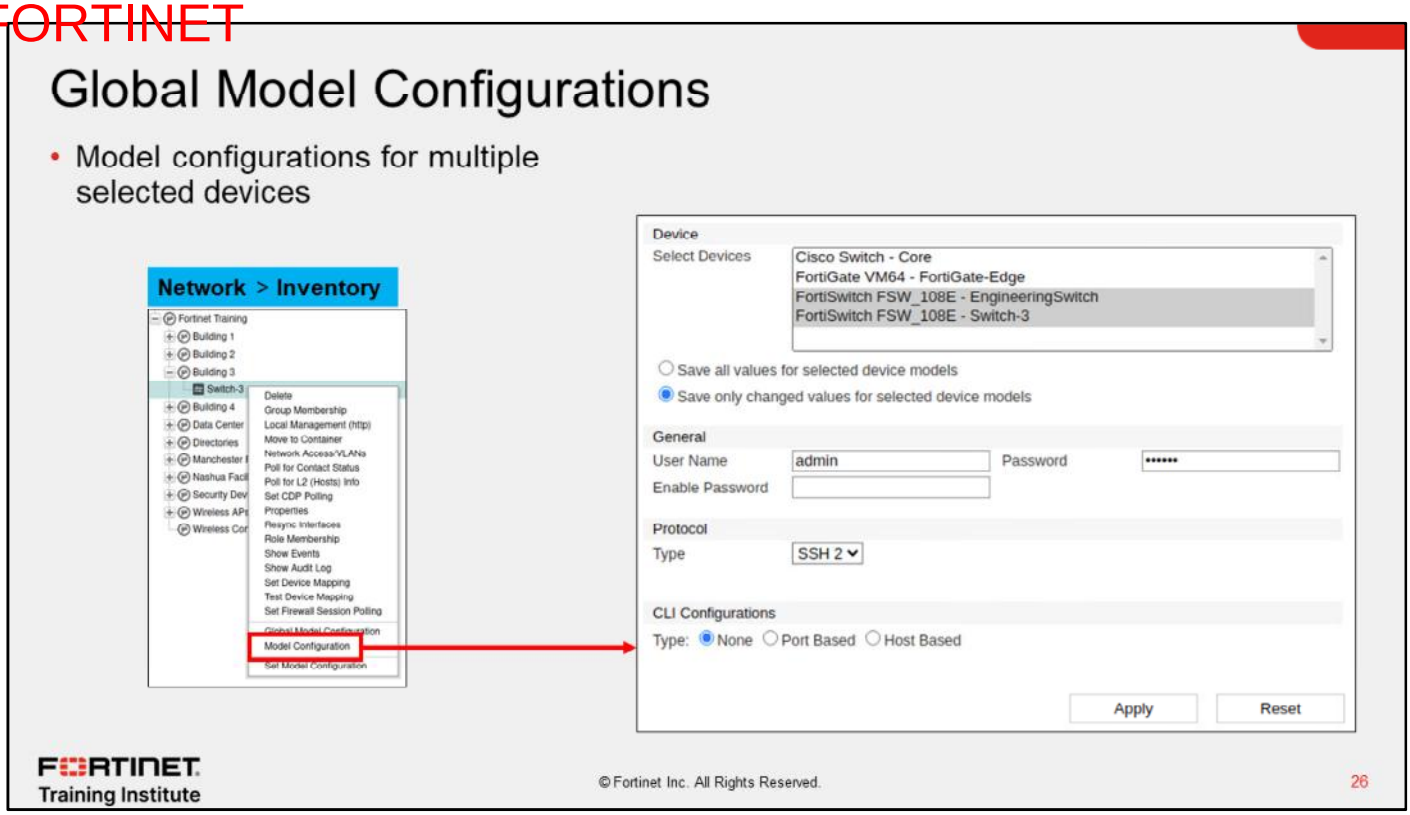
25

You can apply the FortiNAC CLI configuration capabilities during the state-based isolation of a host. The **CLI Configurations** section of the model configuration window offers three options: **None**, **Port Based**, and **Host Based**. **Port Based** CLI configurations are applied while a port is being transitioned to an isolation VLAN. The configurations will stay applied while the host is in the isolation VLAN.

The **Host Based** option in the **CLI Configurations** section will prevent FortiNAC from making the VLAN change, and instead it will only apply the CLI configuration. Host-based CLI configurations are designed to dynamically insert or remove ACL entries, enforcing isolation using ACLs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Configuring model configuration screens on a device-by-device basis in a large environment would be a time-consuming and tedious process. To assist with these large deployments there's another option in the right-click menu called **Global Model Configuration**. At the top of the **Global Model Configuration** screen, you will see all modeled devices that share the same configuration options. You can select one or more of these devices, and configure the settings at the same time. The settings will then apply to all the selected devices.

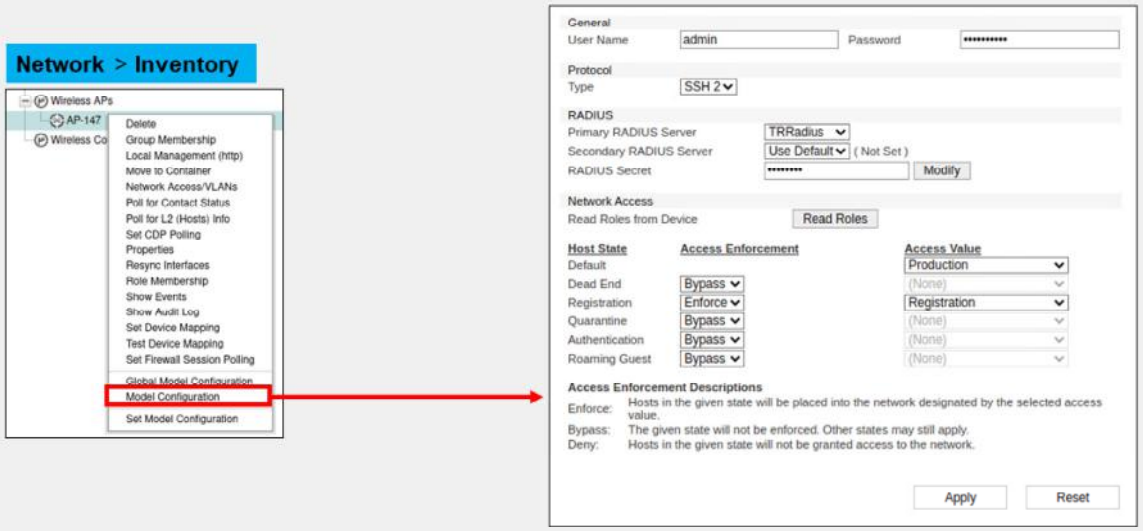
In addition, there are two radio buttons: **Save all values for selected device models** and **Save only changed values for selected device models**. These allow you to change values and have only the modified fields applied to the selected devices. This makes model configuration in large environments quick and easy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Model Configuration—Wireless

- Enforcement is set at the device model level for all SSIDs or can be set on an SSID by SSID level from the **SSIDs** tab



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

You can access model configuration screens for wireless devices in the same way as wired devices. The **Model Configuration** screen contains some of the familiar sections, such as **General** and **Protocol**, which will already be configured because that information was supplied during the initial discovery of the device.

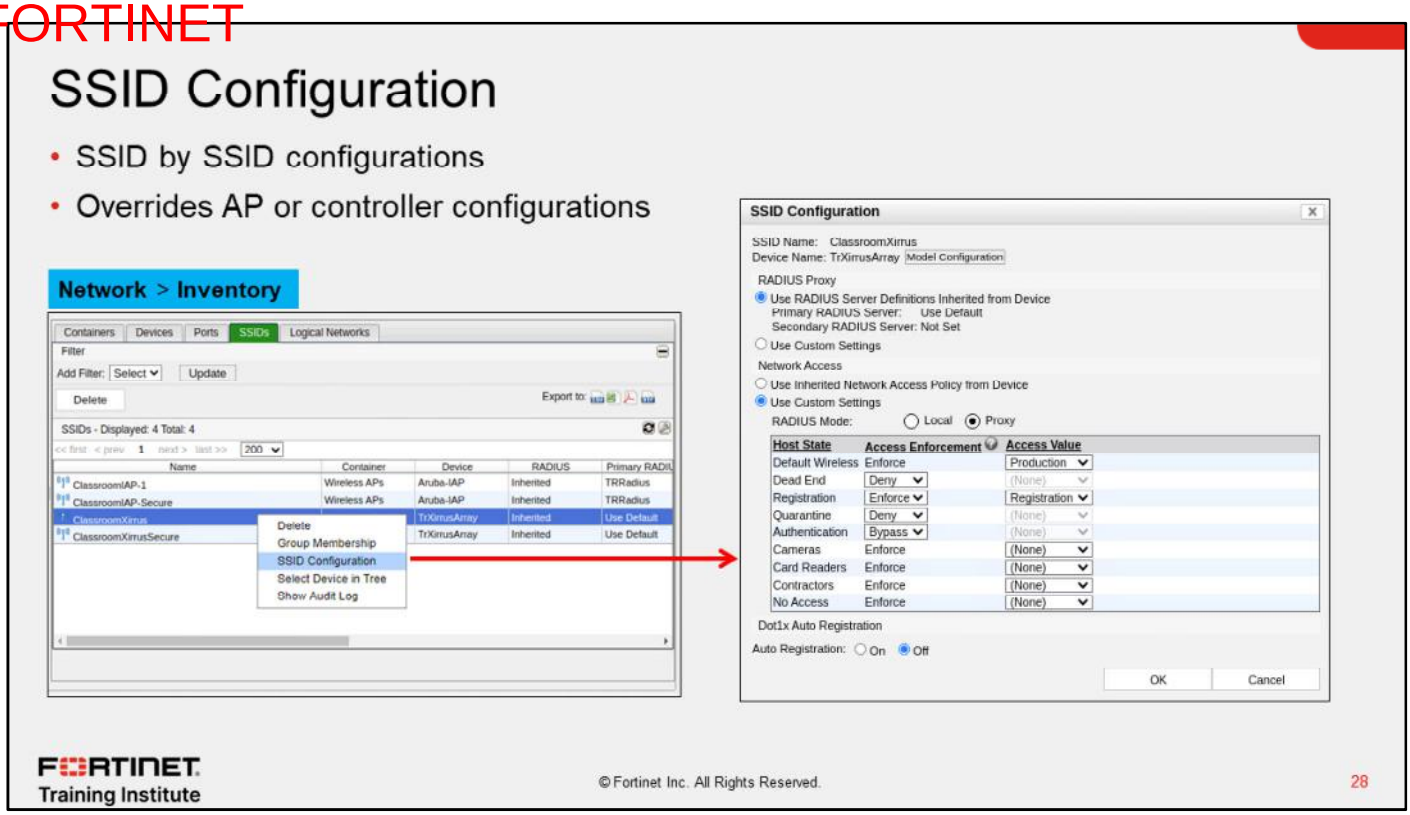
There is also a **RADIUS** section for setting primary and secondary RADIUS servers. You must configure a radius secret here as well. The RADIUS secret must be the same as the secret configured on the AP or controller and the selected RADIUS server(s).

The **Network Access** section includes a **Read Roles** button that will trigger FortiNAC to retrieve values used by the device for network segmentation. These could be VLAN IDs, roles, groups, or interface names. The value returned will depend upon the vendor of the device.

Enforcement configurations, when applied to the AP or controller model, will apply to any SSID controlled by that device that uses FortiNAC as its RADIUS server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



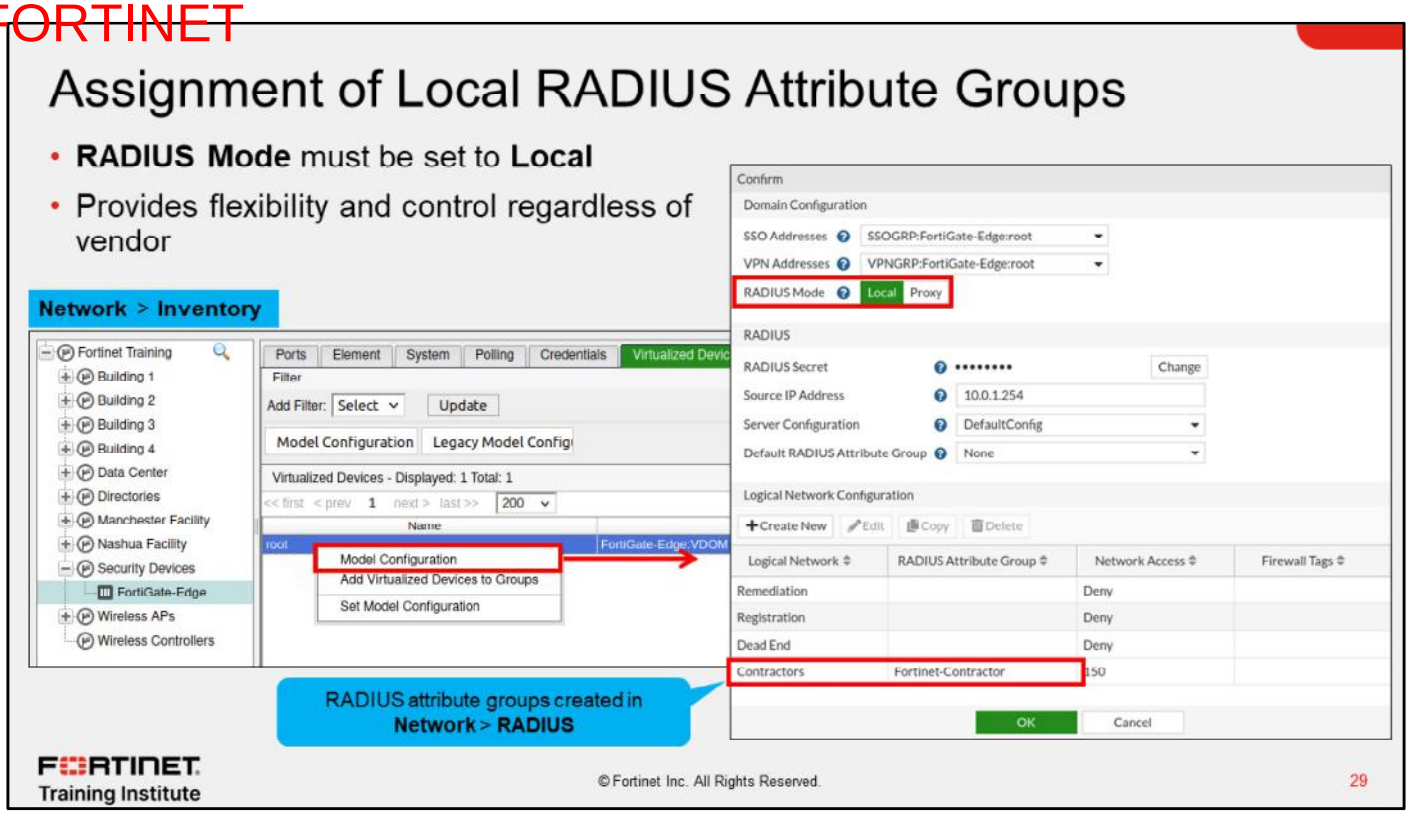
To allow for a more granular configuration, you can set RADIUS and network access configurations on individual SSIDs. On the topology view, select the **SSIDs** tab, and then right-click any SSID. Then select **SSID Configuration**.

These enforcement settings will override those configured on the AP or controller model.

As a best practice during deployment, create a test SSID and validate enforcement settings through that SSID only. Once validated, begin to configure the settings on production SSIDs.

Vouchers & Dumps are Available | WhatsApp +201224560923

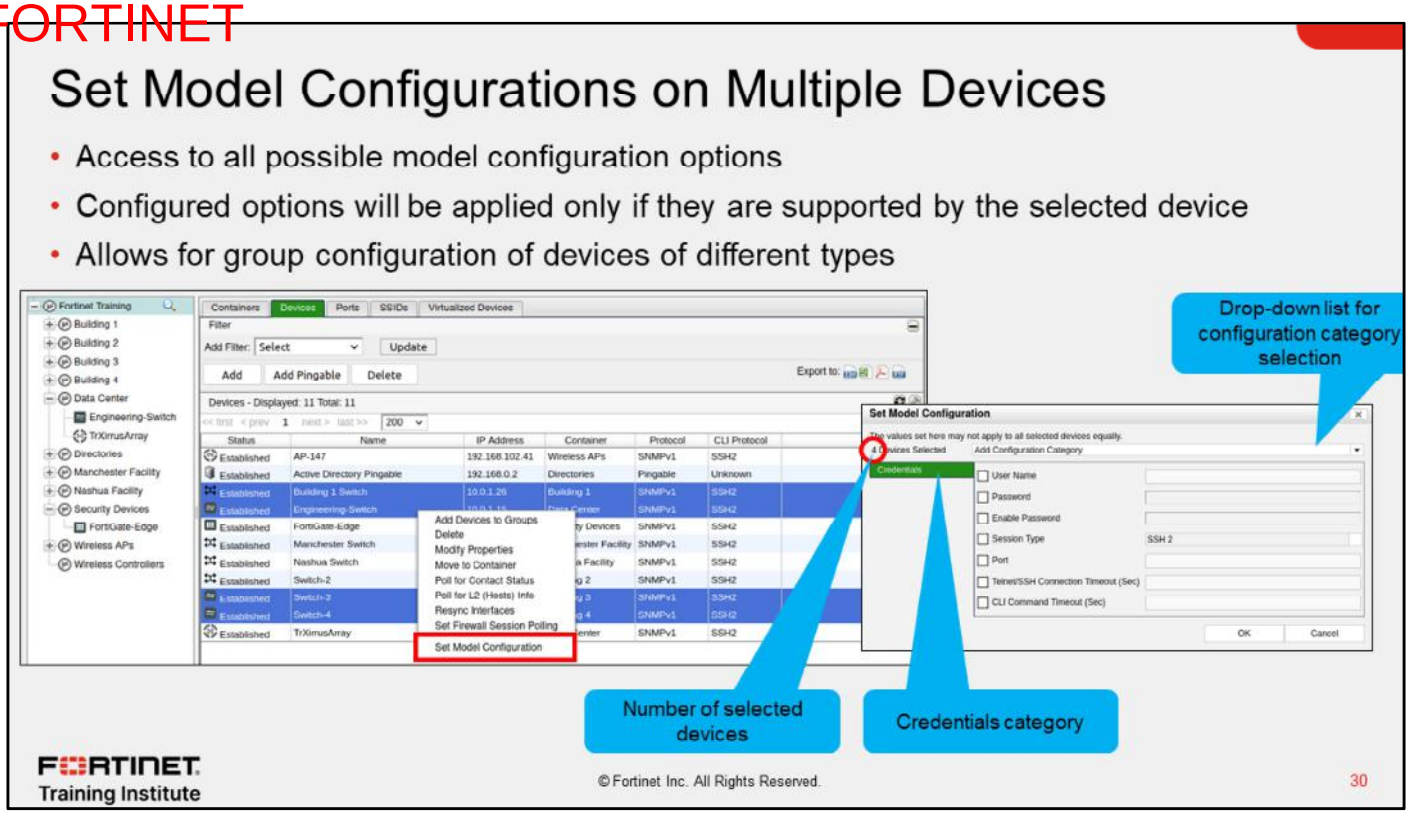
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Recall that RADIUS attribute groups contain one or more RADIUS attributes, and are defined in the **RADIUS** view. This capability can further customize access and control by enhancing the information returned to the infrastructure device, such as group membership or a security attribute. These attributes can be returned for connecting users through logical network definitions. The device or SSID must use the local RADIUS mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



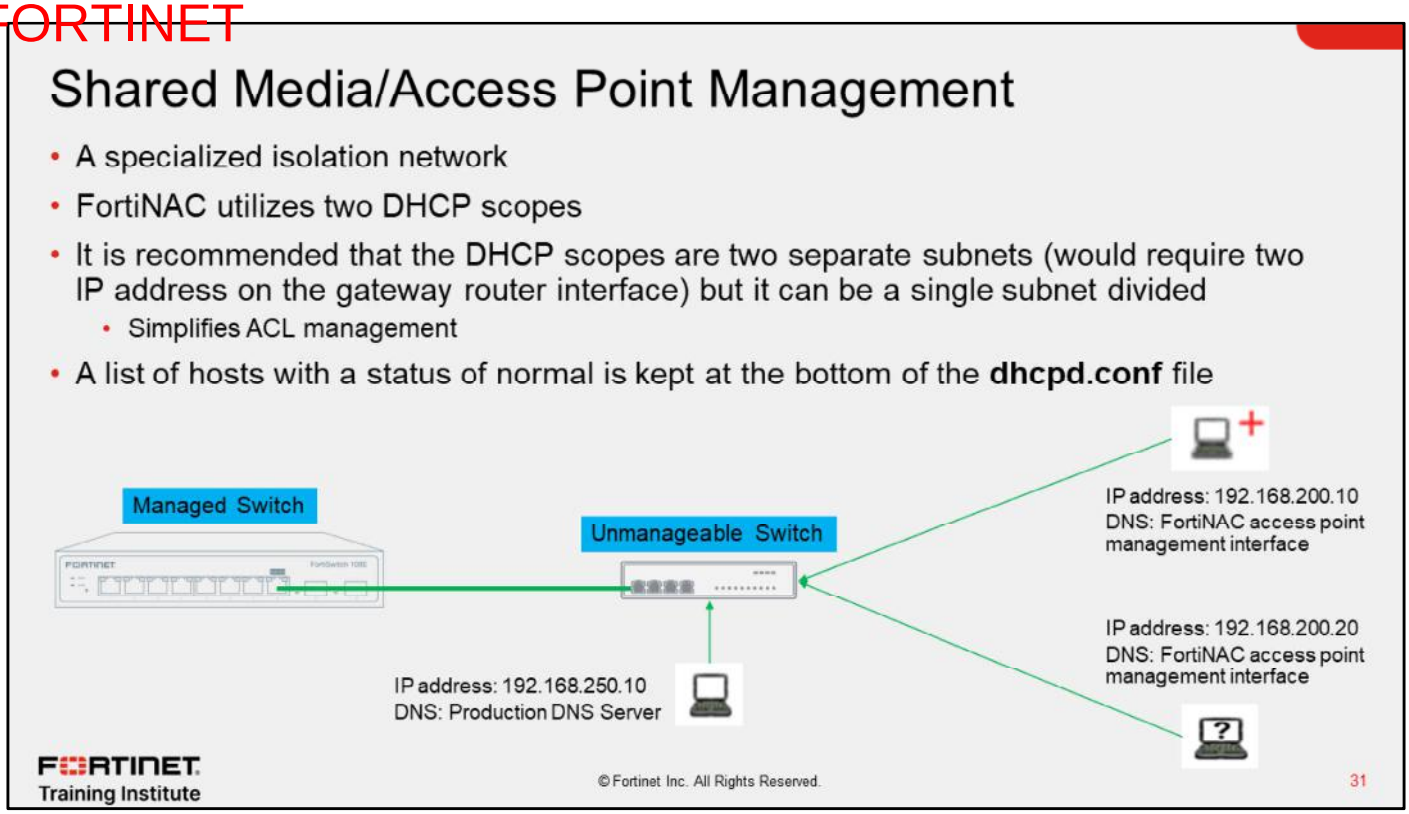
Most environments will contain a variety of infrastructure devices, often from various vendors. Device configuration can be simplified and expedited by configuring device models of different types and vendors in groups. When using the Set Model Configuration, you have access to all the possible model configuration settings.

You can set model configurations on a group of user-selected devices on the **Devices** tab in the inventory view. Right-clicking after device selection will open the **Set Model Configuration** window.

Only the settings supported by a selected device will be applied.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Shared media/access point management leverages a specialized isolation network to provide control using IP address assignment. Like the other isolation networks, the FortiNAC shared media interface must be enabled and an IP address and mask configured. However, because of the way access point management functions, there are two address pools for this isolation VLAN. The first defines the DHCP scope and DNS server for hosts that have a status of normal, and the second defines the DHCP scope for all other hosts, and will assign the FortiNAC shared media interface as the DNS server.

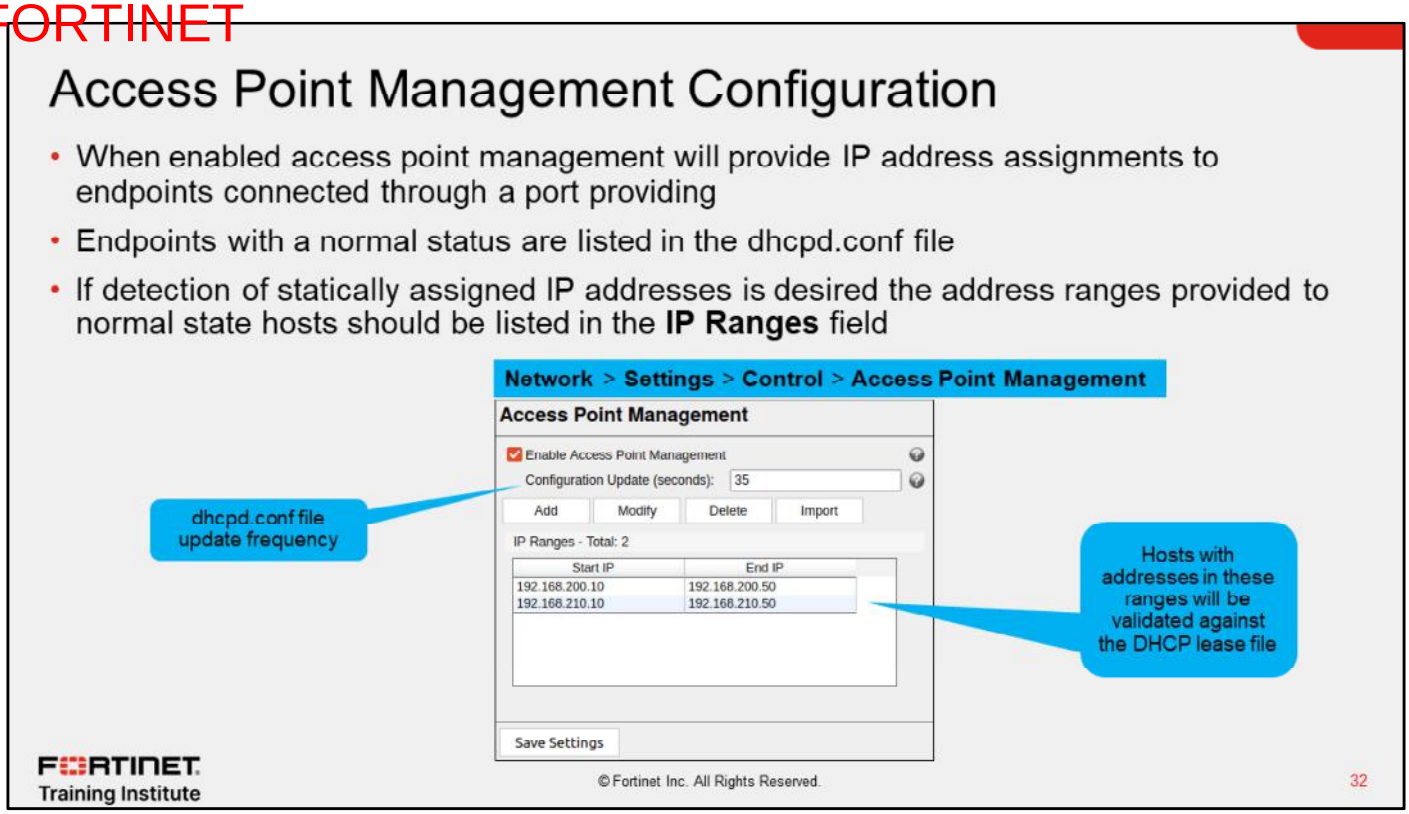
Access point management is used in environments where control over host VLAN access is not possible, for example, when hosts are connecting to the network through devices that do not support VLANs, such as non-intelligent switches or access points. With VLAN-based control, hosts of different states are on different VLANs, physically separated at Layer 2. Access point management controls hosts through IP address assignment using two address pools. One pool is for normal status hosts (called the *authenticated address pool*), and assigns an IP address and a production DNS server. The second pool is for non-normal status hosts (called the *unauthenticated address pool*), and assigns an IP address and FortiNAC as the DNS server. In this configuration, all hosts are on the same VLAN, but non-normal status hosts will get isolation pages.

When a host connects to a port that is on the access point management VLAN, and issues a DHCP request, FortiNAC consults the list of all normal state hosts, which it maintains within its configuration. If the host is found in the list, FortiNAC will assign an IP address from the authenticated address pool and assign a production DNS server. The host will now have access to allowed sites that can be resolved by that DNS server.

The second scope will be created for hosts that have a status other than normal. There is no DNS server defined for this scope. FortiNAC will automatically assign itself for DNS wildcarding and presentation of the appropriate isolation pages. It is recommended that the two scopes use different subnets.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

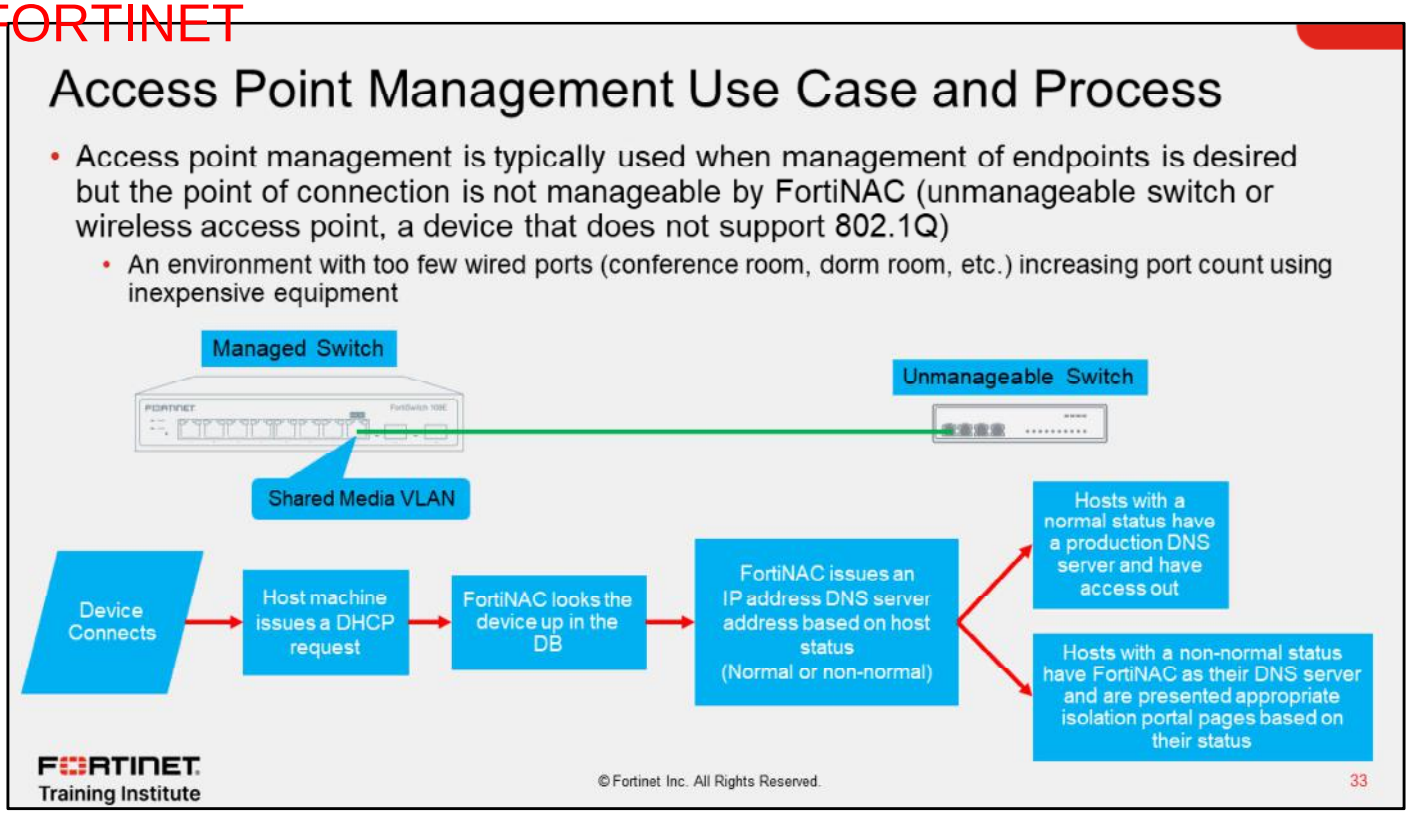


You can enable access point management to provide access control capabilities using IP address assignment.

If detection of statically assigned IP addresses is desired, for example, to detect someone attempting to configure a host with a status other than normal an address from the authenticated address pool, all addresses in the authenticated address pool or pools should be listed in the **IP Ranges** filed. Anytime FortiNAC performs an L3 poll and detects a host with an IP address that falls into one of the listed ranges, FortiNAC will validate that it assigned the IP address to that host using the DHCP lease file. If the host is not in the lease file with the appropriate address, FortiNAC will generate a **Static IP Address** event. The event can be mapped to an alarm and an action. For example, the helpdesk could be notified and control capabilities could be leveraged to block the host's access.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide highlights a couple common use cases for access point management as well as the process used to by FortiNAC to provide a solution.

A common use would be the addition of a low cost unmanaged switch to a conference room with an insufficient number of wired ports, with the desire to continue to provide access control on an endpoint by endpoint bases. The port used to connect the unmanaged switch would need to be in the access point management VLAN. Recall that the access point management VLAN is a specialized isolation VLAN managed by FortiNAC, much like the registration or quarantine isolation VLANs. FortiNAC will act as the DHCP server and, for endpoints that do not have a status of normal, a DNS server. It is recommended that the two address pools be different subnets, and the gateway route be configured to handle both subnets on the same VLAN.

The management of endpoints would work as follows:

1. An endpoint connects to the unmanaged switch or access point.
2. The endpoint requests an IP address using DHCP.
3. FortiNAC receives the DHCP request and looks up the host in the database.
4. For endpoints with a status or normal FortiNAC issues an IP address and production DNS server as defined in the authenticated address pool, if the endpoint has a status of anything other than normal it issues an IP address and DNS server as defined in the unauthenticated address pool. The DNS server issued for unauthenticated endpoints is the IP address of the access point management isolation interface on FortiNAC.
5. The endpoint with a status of normal can be provided appropriate network access provided by infrastructure configurations (such as ACLs), endpoints with a status other than normal will be redirected using DNS to the FortiNAC access point management isolation interface, there they will be presented with captive portal based on the endpoint status.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. At what level can default VLANs be defined?
   - ✓ A. Port and device
   - B. Device and container

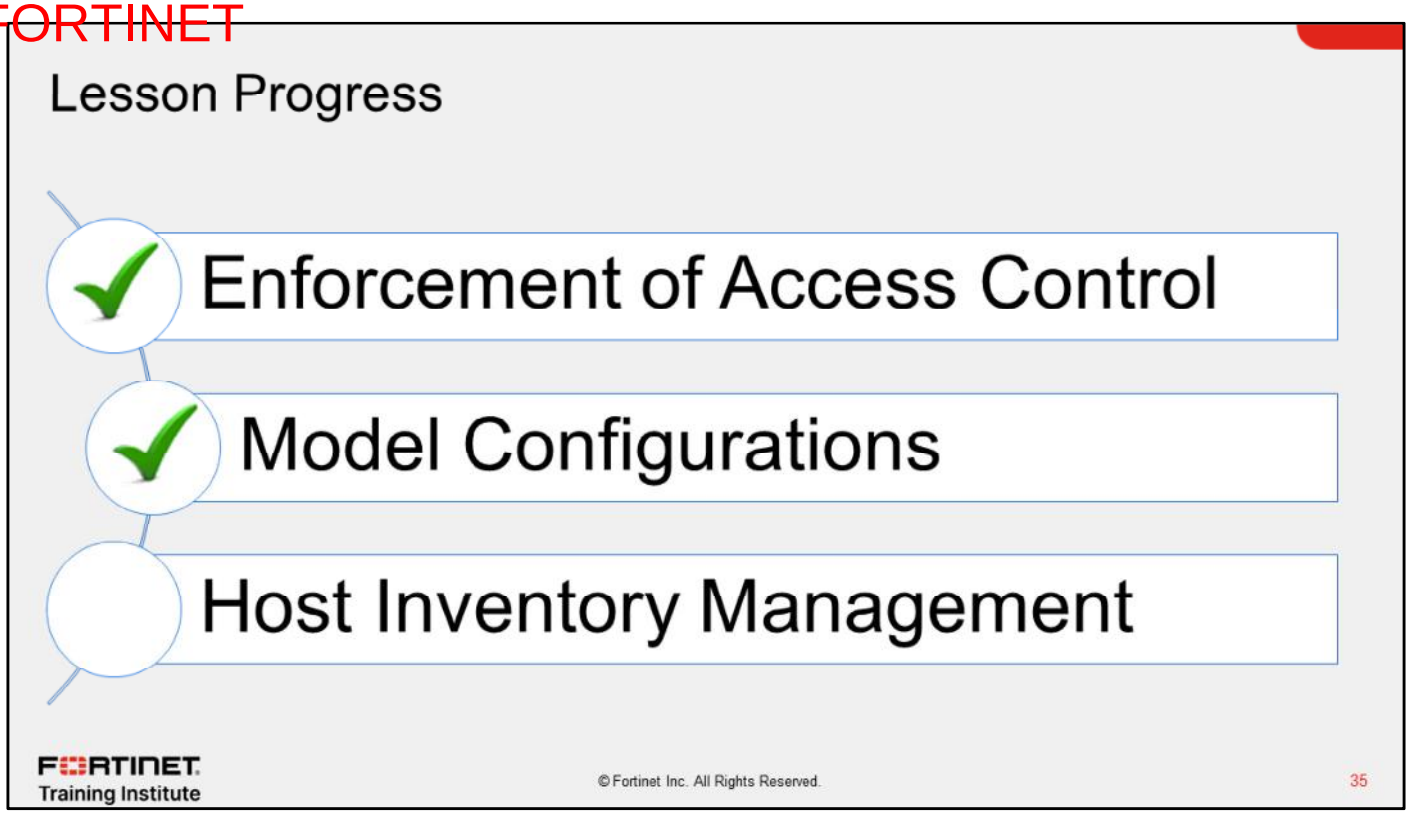
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

34

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

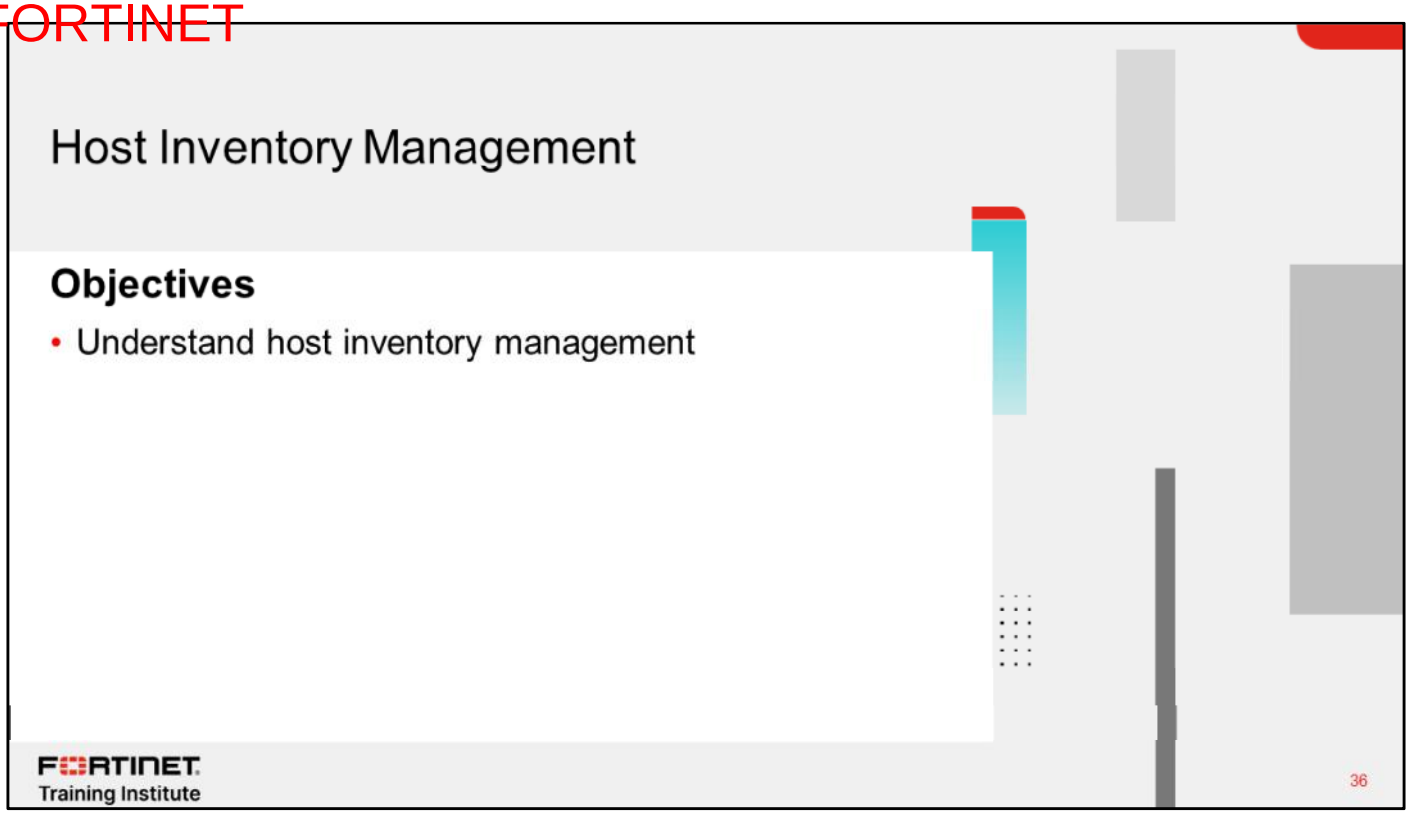


Good Job! You now understand FortiNAC model configuration settings.

Now, you will learn about FortiNAC host inventory management.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

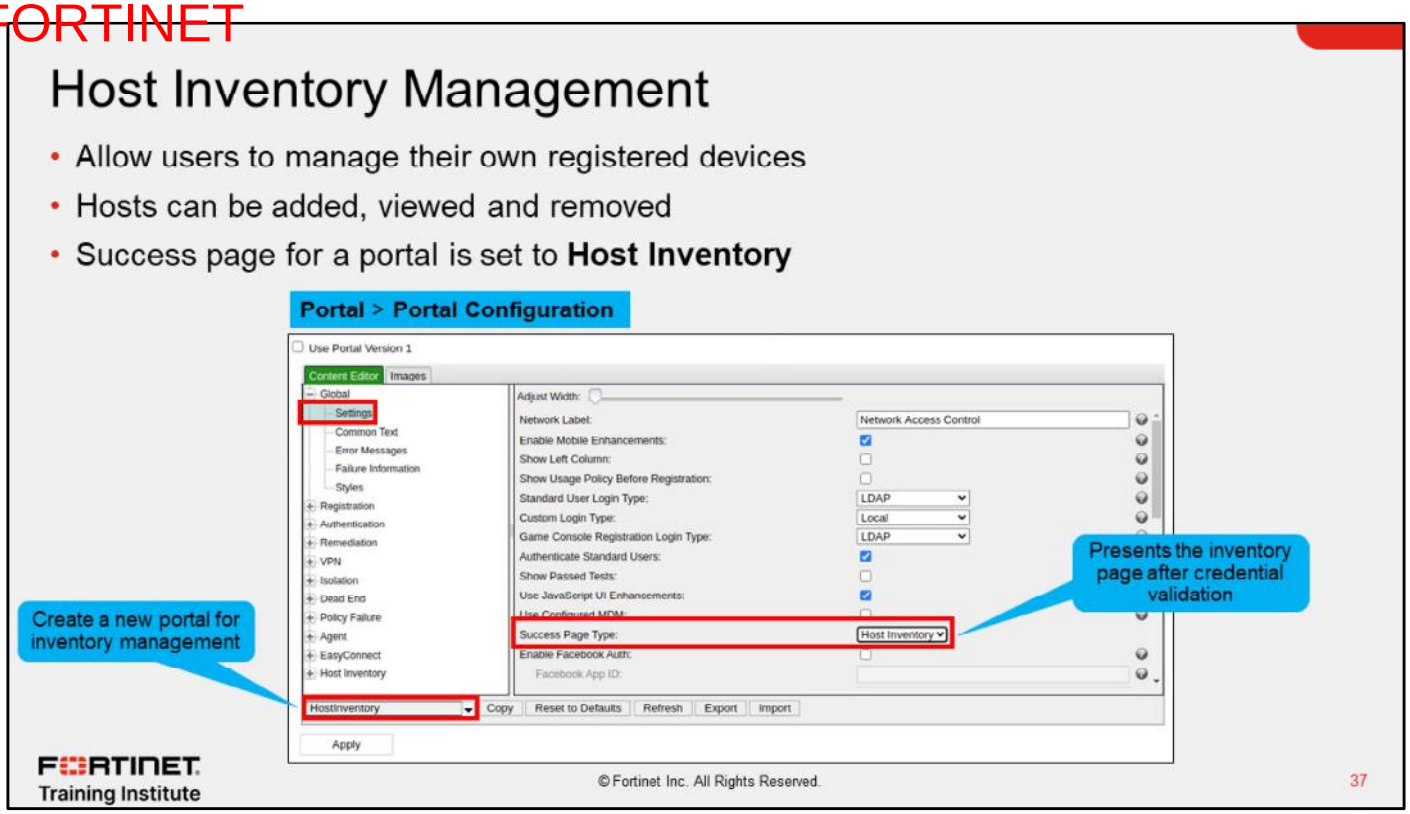


After completing this section you should be able to achieve the objective shown on this slide.

By demonstrating competence in FortiNAC host inventory management, you will be able to delegate BYOD host management end users, allowing them to manage their own devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In some environments the management of individual end user hosts can become overwhelming. An example of this would be a college or university with thousands of students, each with several devices. The host inventory management feature allows you to delegate the some basic management functions to the end users. Allowing them to add, view, and remove their registered hosts.

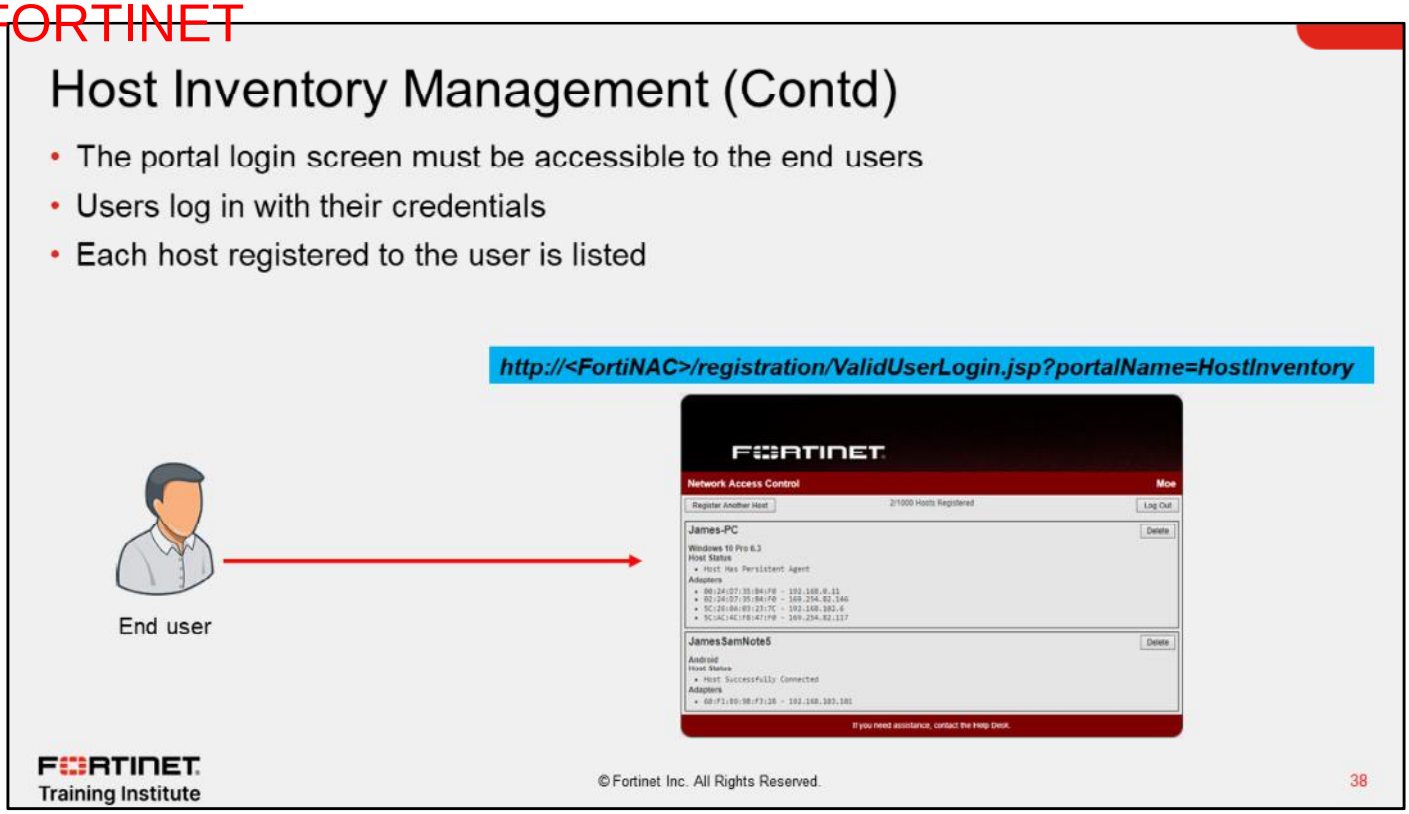
As a best practice, create a new portal specifically for host inventory management, by using the drop-down list on the lower-left portion of the view.

In this example, the new portal page is named **Host Inventory**.

Change the **Success Page Type** to **Host Inventory**. Changing the **Success Page Type** is what changes the purpose of the portal page from an on-boarding only page to an inventory management page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You must make the host inventory management page available to end users, typically through an internal web page.

The example shown on this slide shows a host inventory management screen with buttons for control. The **Register Another Host** option allows the user to register additional devices. The **Delete** button to the right of each device provides the ability to delete a device that has already been registered. This screen allows the end user of BYOD devices such as guests, contractors, or students to have complete control over their onboarded equipment.

The login screen that you must make available to end users is shown here. The URL of this screen is case-sensitive, and the portal name must match the name given on the **Portal Configuration** view, as discussed on the previous slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which configuration setting changes the portal page to an inventory management page?
   - A. **Standard User Login Type**
   - ✓ B. **Success Page Type**

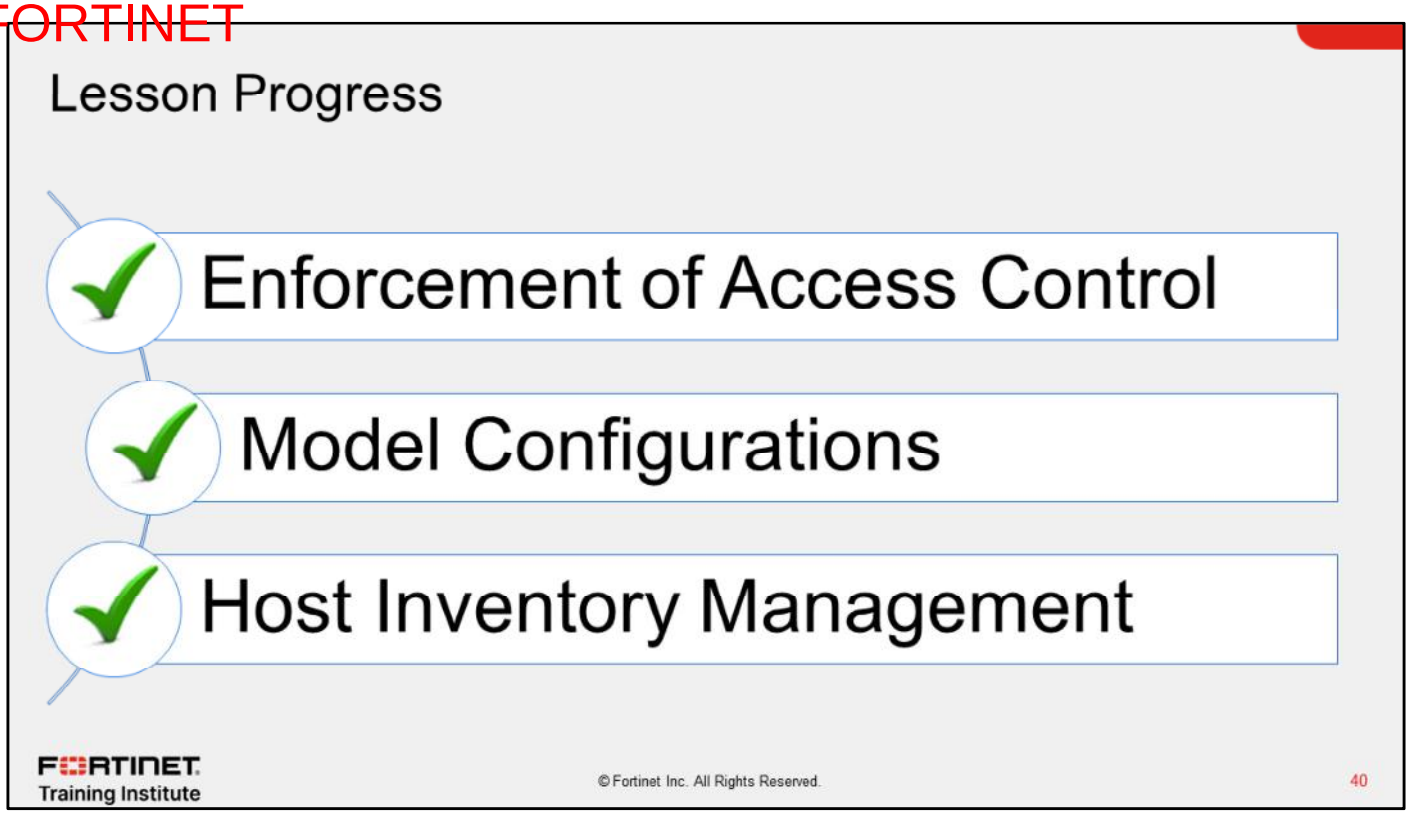
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

39

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

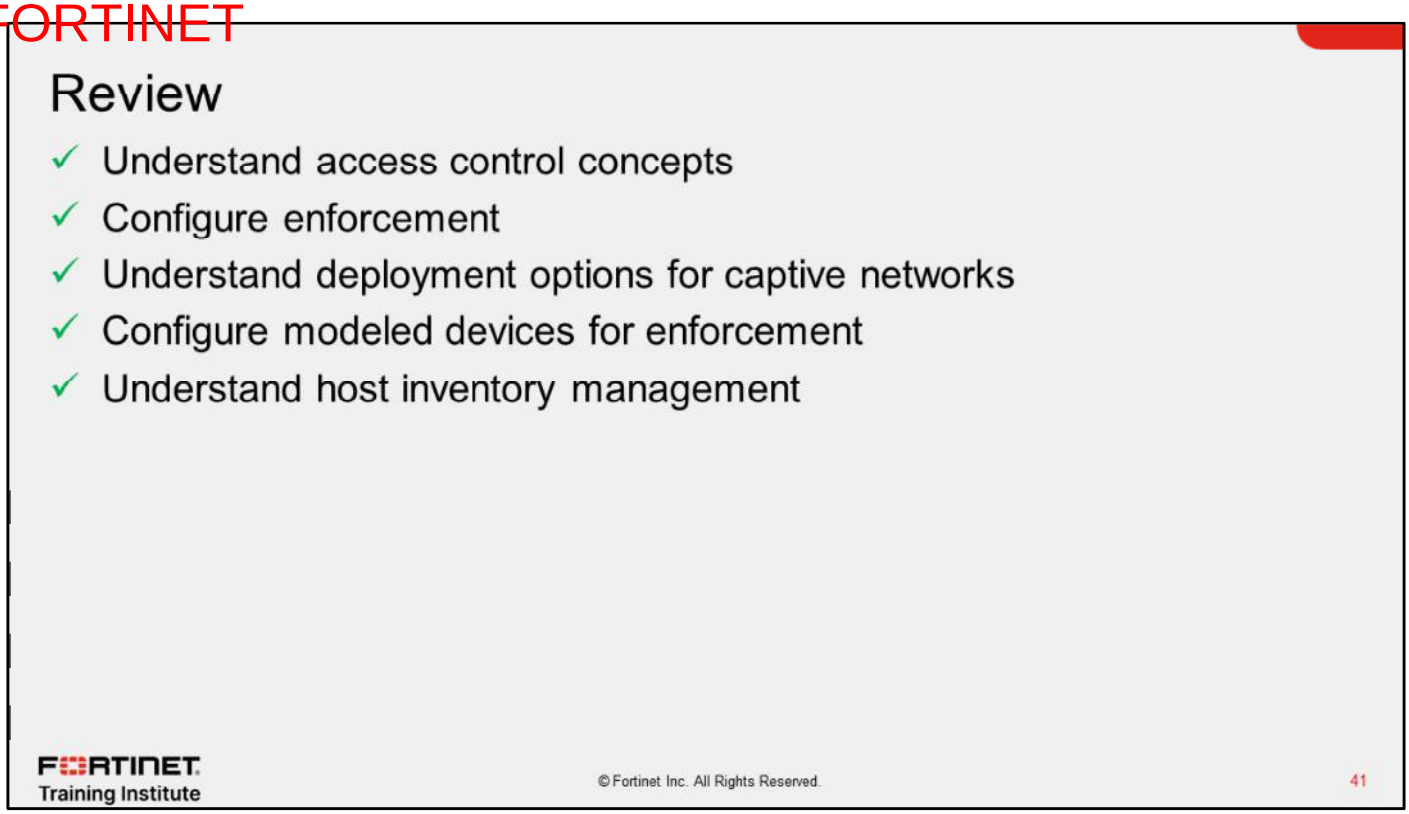


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

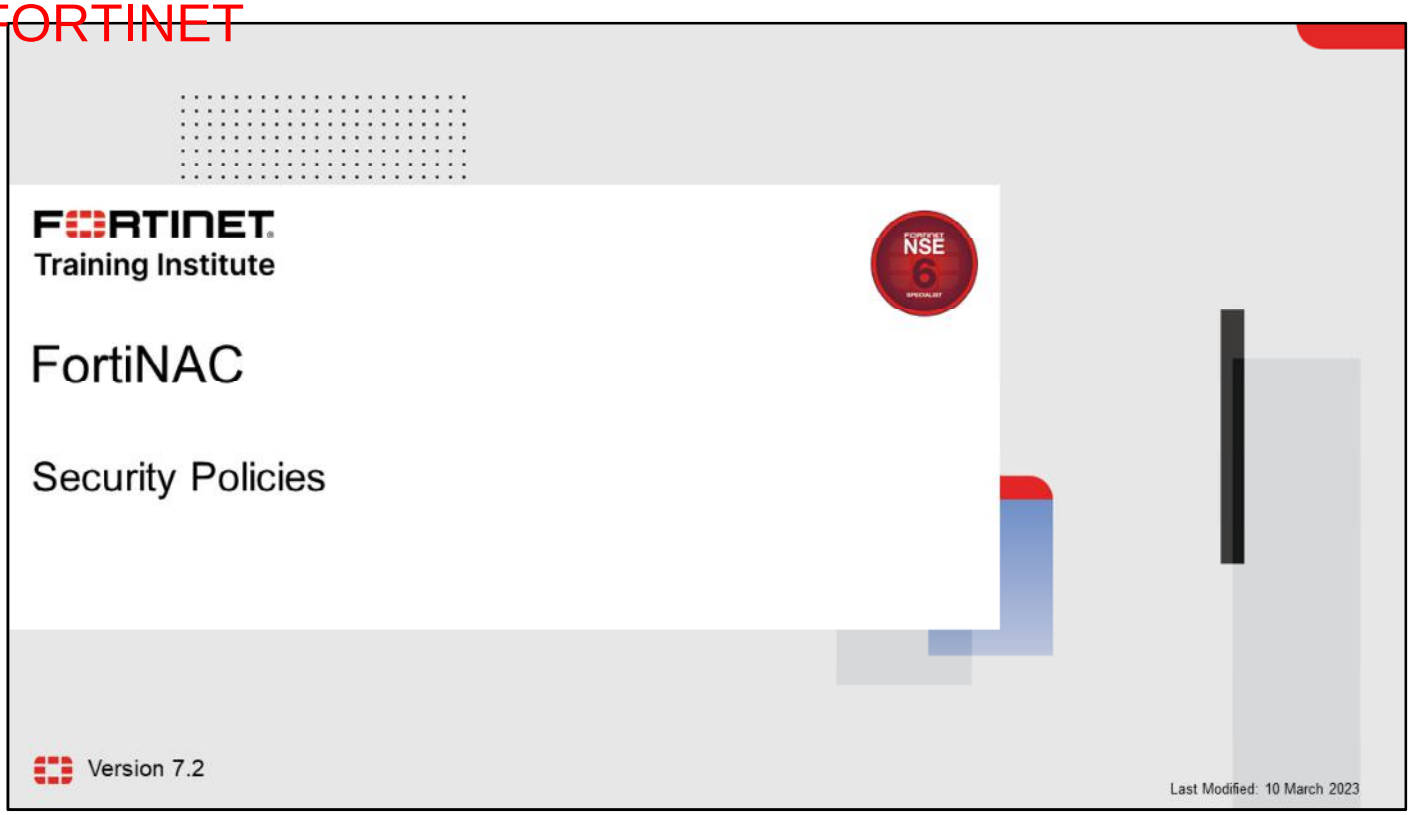


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure FortiNAC to provide dynamic access control, and how to allow end users to manage their own assets.

Vouchers & Dumps are Available | WhatsApp +201224560923

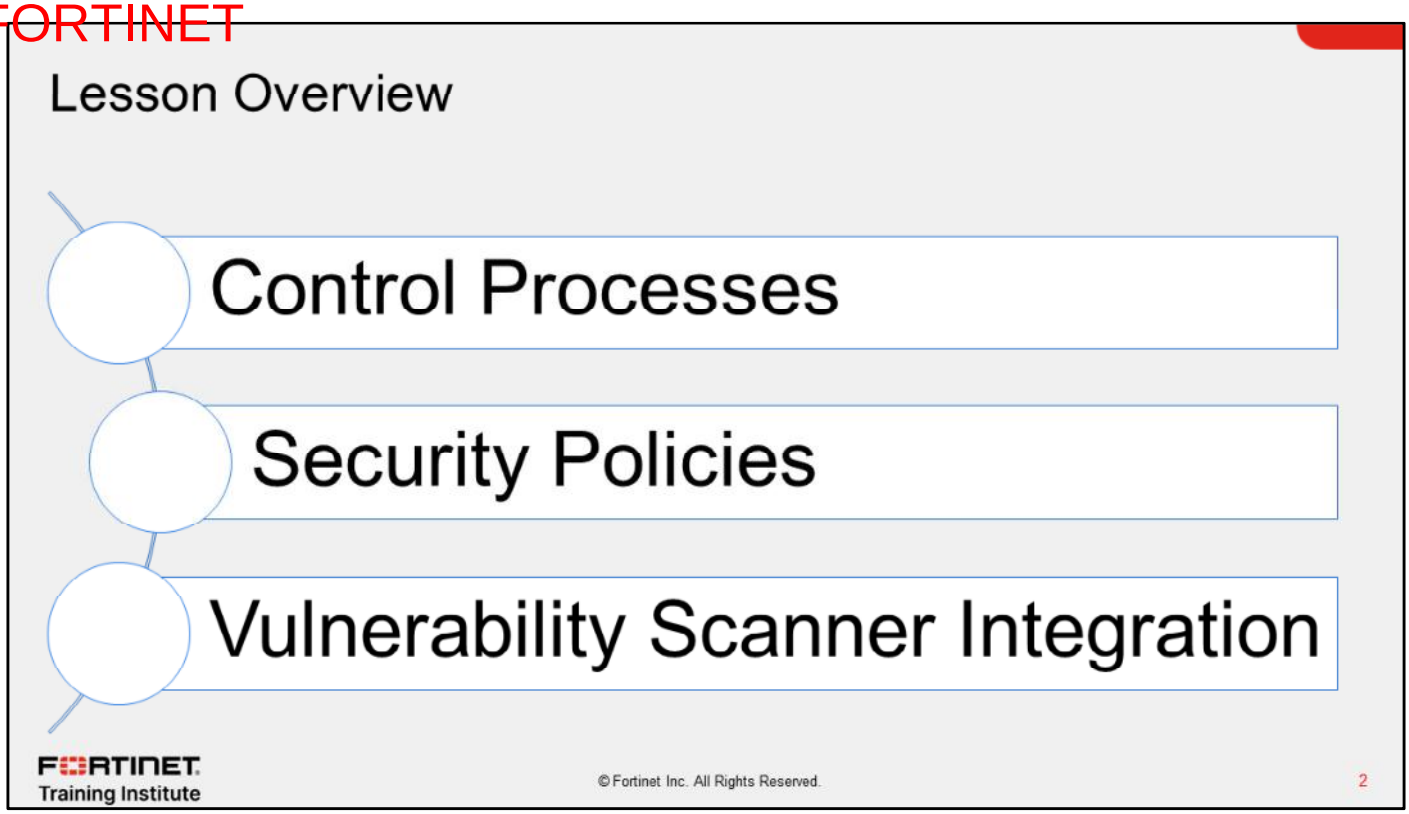
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiNAC security policies. It is through security policies that FortiNAC provides customized onboarding options, simplified security configuration for wireless access, detailed network access provisioning, endpoint compliance validation, and customizable back-end authentication services.

Vouchers & Dumps are Available | WhatsApp +201224560923

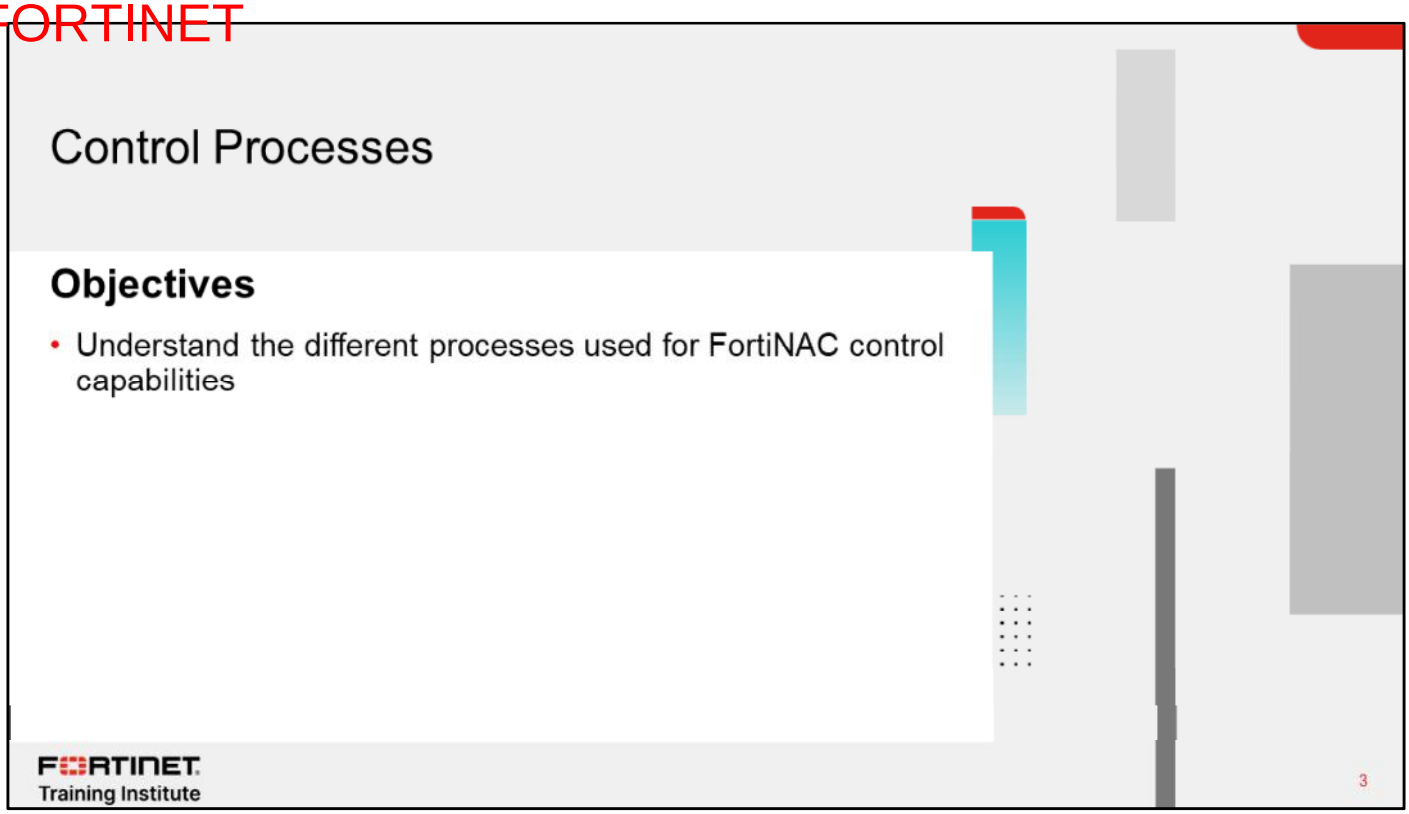
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

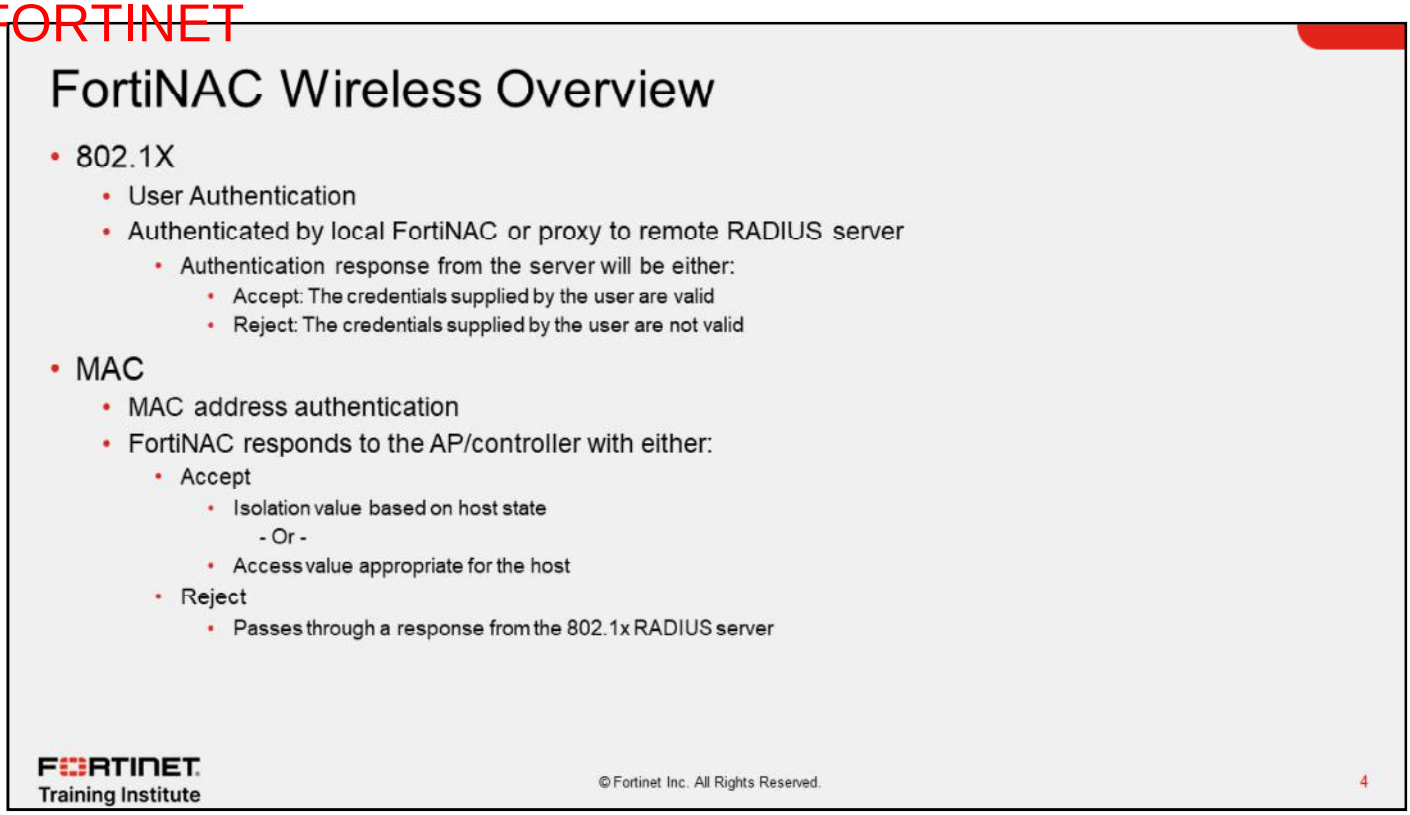


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating an understanding of the processes used by FortiNAC to control access, you will be able to effectively plan and implement FortiNAC control.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When a host attempts to access the network through a FortiNAC managed point of connection using 802.1x authentication, FortiNAC can perform the authentication or proxy the request to a remote RADIUS server.

Recall that you configure communication settings for external RADIUS servers on the **Network** menu, by clicking **Settings**, and then clicking the **Authentication** folder. The RADIUS server that will be used for validation is defined within the **Model Configuration** or the **SSID Configuration** settings discussed earlier.

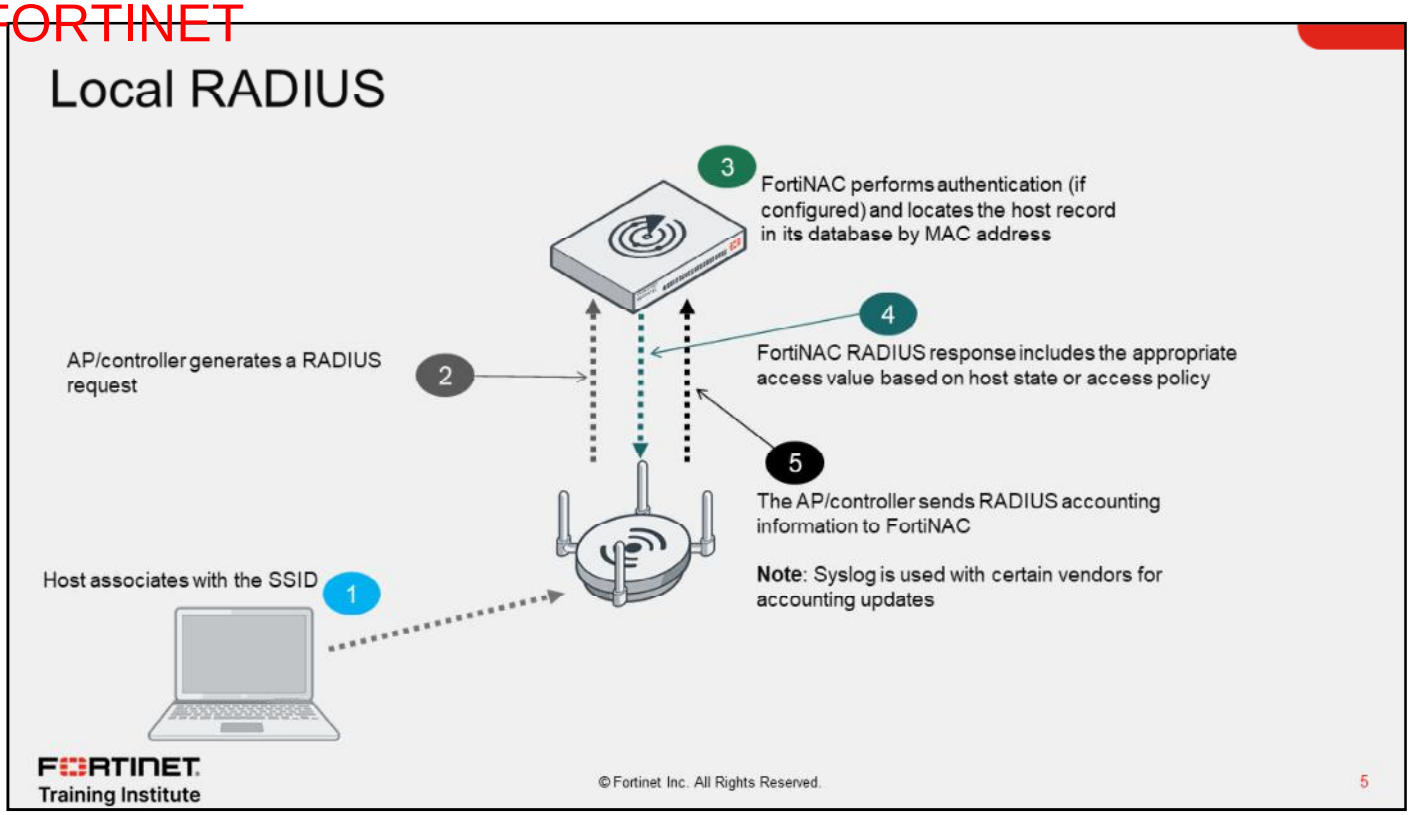
If a remote RADIUS server responds with an accept response, FortiNAC will consult its database and determine if the host needs to be provisioned based on its state or a **Network Access Policy**, or by a default VLAN or access value. It will then modify the RADIUS accept packet and return it to the requesting device.

If a remote RADIUS server responds with a reject response, FortiNAC will pass the rejection, unaltered, to the requesting device.

When configured for MAC authentication, FortiNAC validates the physical address locally and responds to the controller or AP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

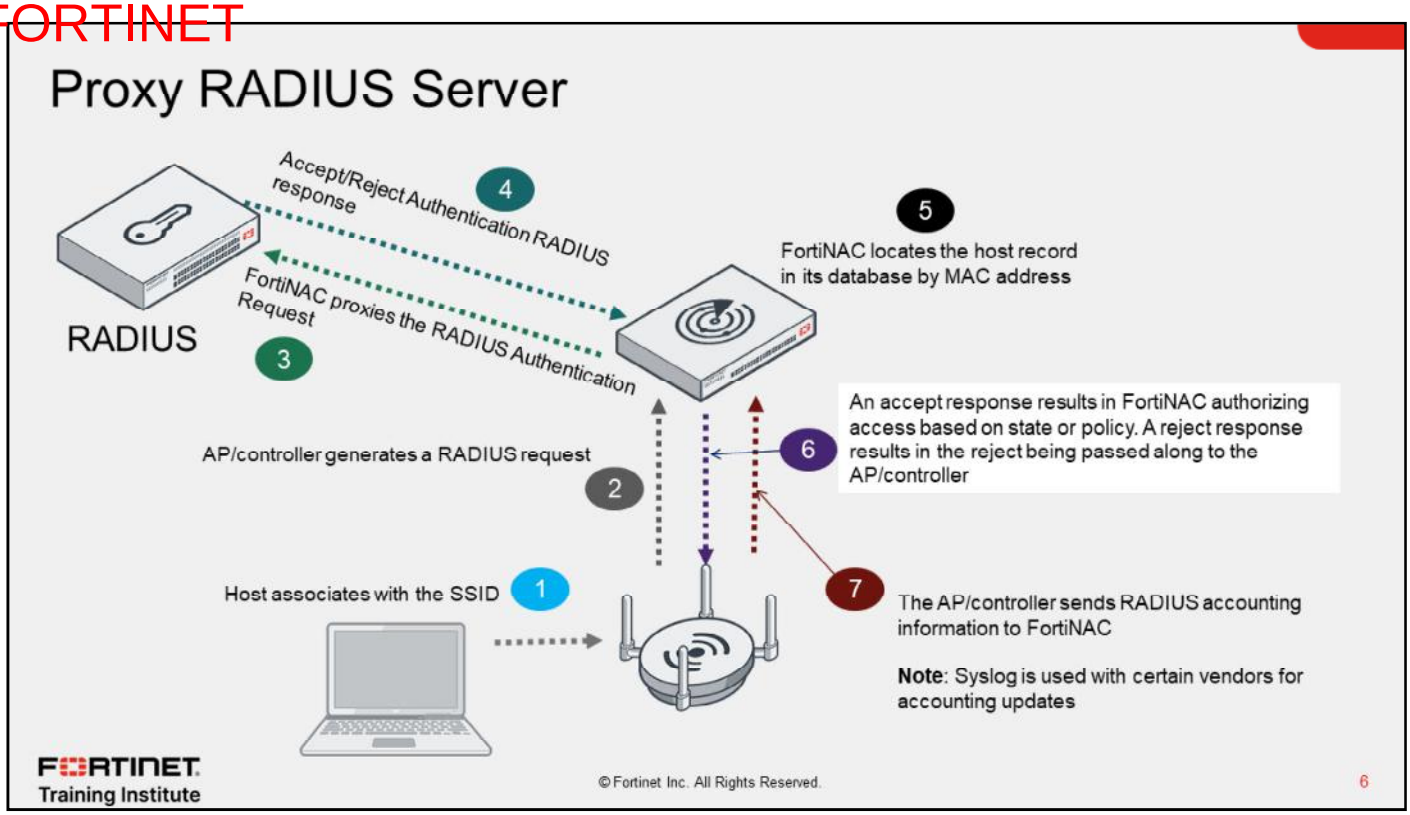


This slide shows the process of a host accessing an environment managed by FortiNAC and configured for MAC authentication or local RADIUS.

1. The host associates with the SSID.
2. The device generates a RADIUS request to FortiNAC.
3. For MAC authentication FortiNAC looks up the host in the database and determines the access that should be provisioned based on the state of the host, on a matched security policy, or a default VLAN/access value. If configured to use local RADIUS, FortiNAC performs the authentication and then looks up the host in the database and determines, based on the user, the host, or both, which access should be provisioned.
4. FortiNAC generates a RADIUS response, and forwards it to the requesting device.
5. Post connection FortiNAC keeps connection information up-to-date using RADIUS accounting or syslog information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

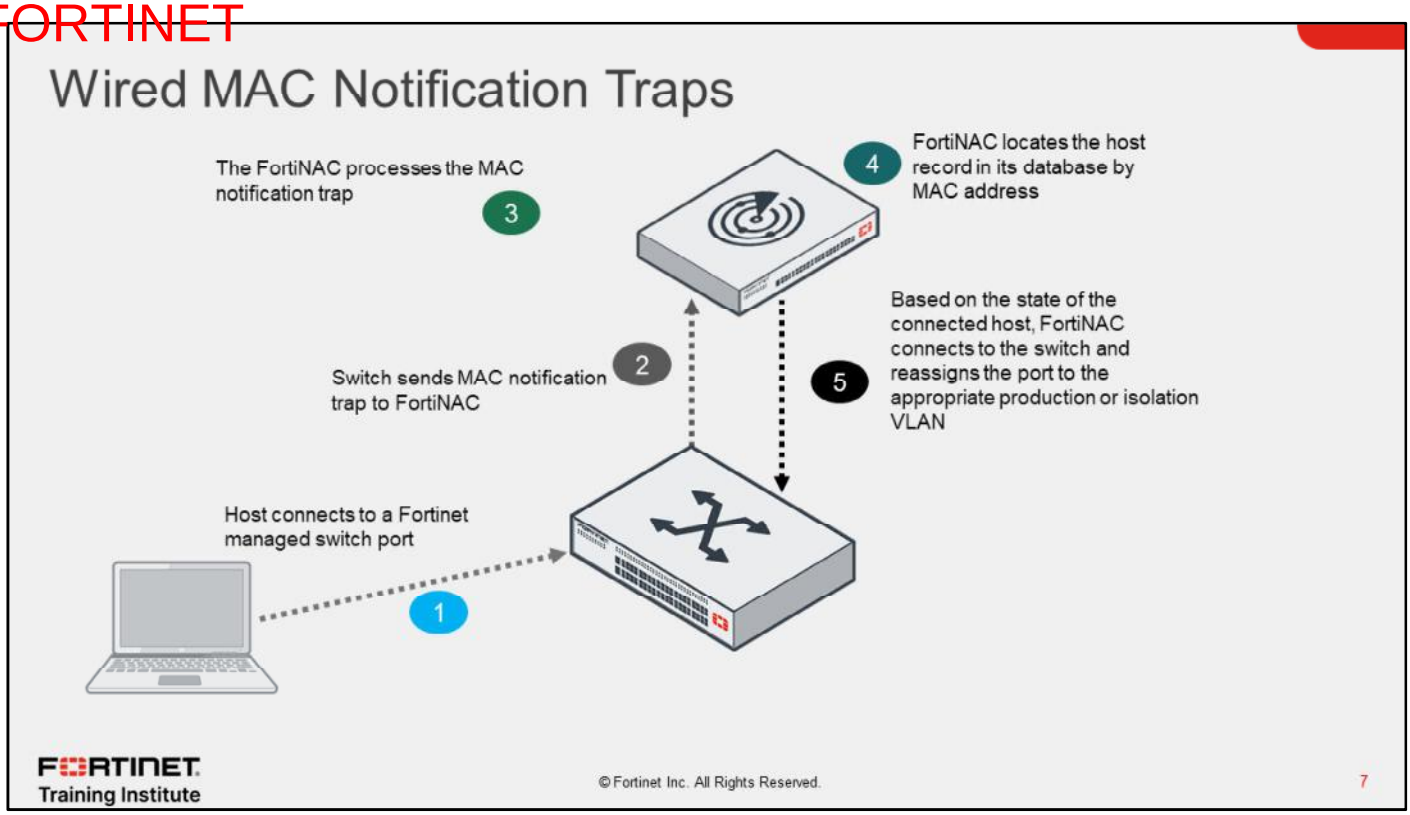


This slide shows the process of a host accessing an environment managed by FortiNAC configured to proxy to a remote RADIUS server.

1. The host associates with the SSID.
2. The device generates a RADIUS request to FortiNAC.
3. FortiNAC proxies the request to the RADIUS server defined in the device model configuration or SSID configuration set in the network inventory view.
4. The RADIUS server issues an accept or reject response. If the response is a reject, FortiNAC proxies it unchanged back to the requesting device.
5. If the response is an accept, FortiNAC looks up the user or host in the database and determines the access that should be provisioned based on the state of the user or host, on a matched security policy, or a default VLAN/access value.
6. FortiNAC modifies the RADIUS response and forwards it to the requesting device.
7. Post connection, FortiNAC keeps connection information up-to-date using RADIUS accounting or syslog information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

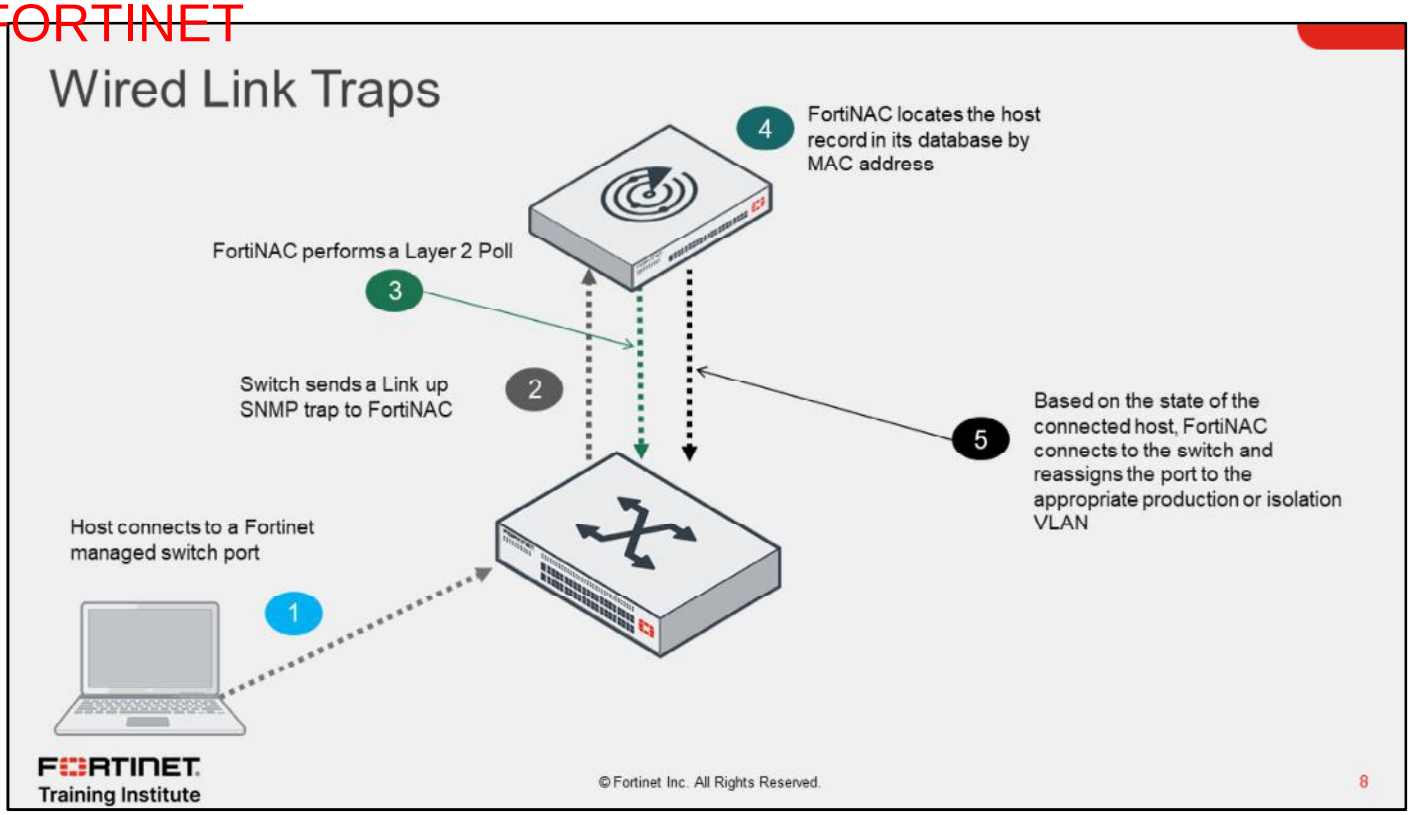


This slide shows the process of a host connecting in a wired environment configured to use MAC notification traps.

1. The host connects to, or disconnects from, a wired port.
2. The device issues a MAC notification trap to FortiNAC. This could be a MAC Added or MAC Removed trap.
3. FortiNAC processes the trap and identifies the MAC address that was added or removed, as well as the associated port.
4. If it was a MAC added trap, FortiNAC looks up the host in the database and determines the access that should be provisioned based on the state of the host, on a matched security policy, or a default VLAN/access value.
5. FortiNAC makes the appropriate configuration changes to provision the host.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows the process of a host connecting in a wired environment configured to use link traps.

1. The host connects to, or disconnects from, a wired port.
2. The device issues a link trap to FortiNAC. This could be a Link Up or Link Down trap.
3. FortiNAC performs a Layer 2 poll of the device and identifies the MAC address that was added or removed, as well as the associated port.
4. If it was a Link Up trap, FortiNAC looks up the host in the database and determines the access that should be provisioned based on the state of the host, a matched security policy, or a default VLAN/access value.
5. FortiNAC makes the appropriate configuration changes to provision the host.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When using a remote RADIUS server, which response type does FortiNAC proxy leave unchanged?
   - A. Accept
   - ✓ B. Reject
2. When gathering Layer 2 information in a wired environment, which method is more efficient?
   - A. Polling
   - ✓ B. MAC notification traps

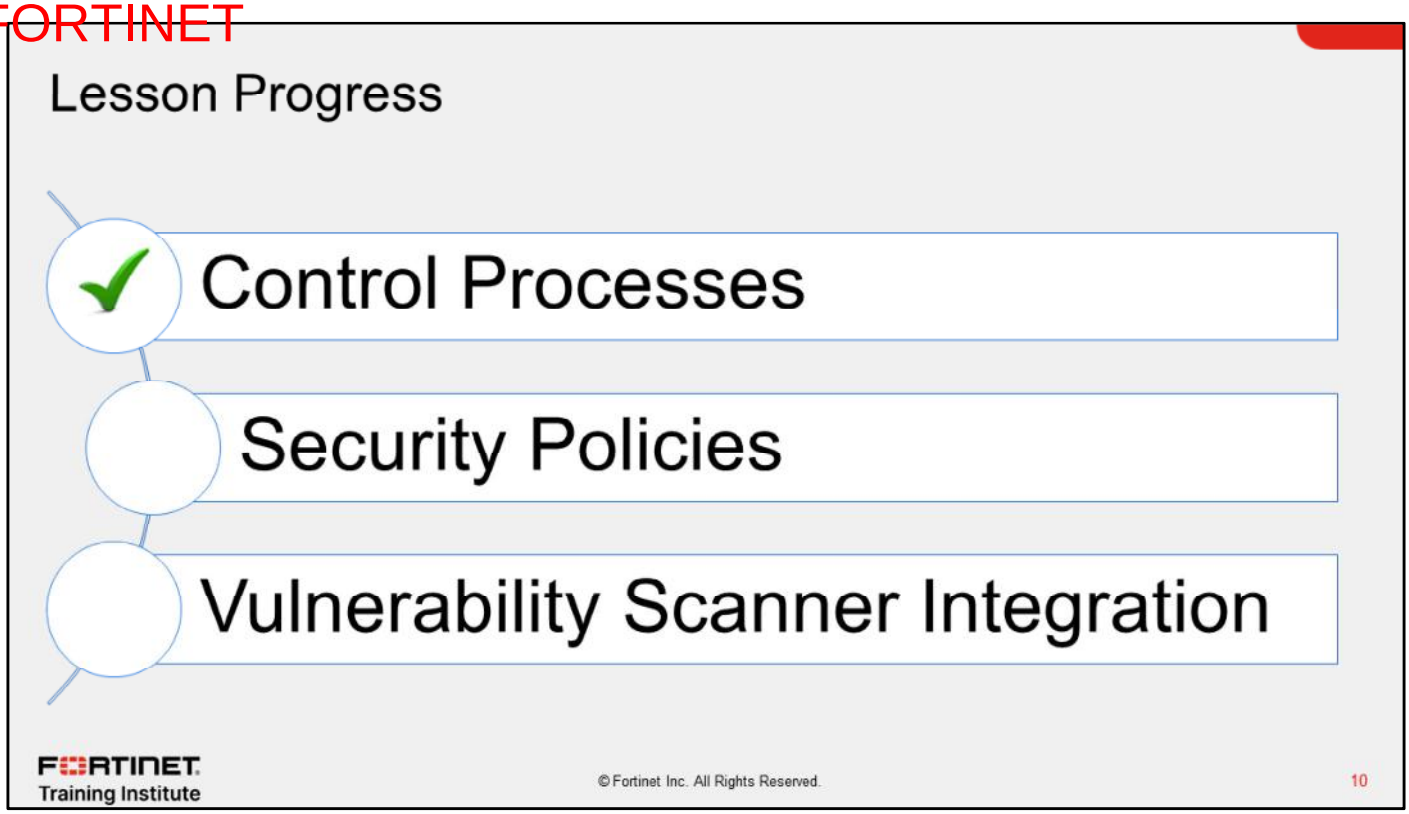
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

9

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Good job! You now understand security policies and how to configure them.

Now, you will learn about vulnerability scanner integration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

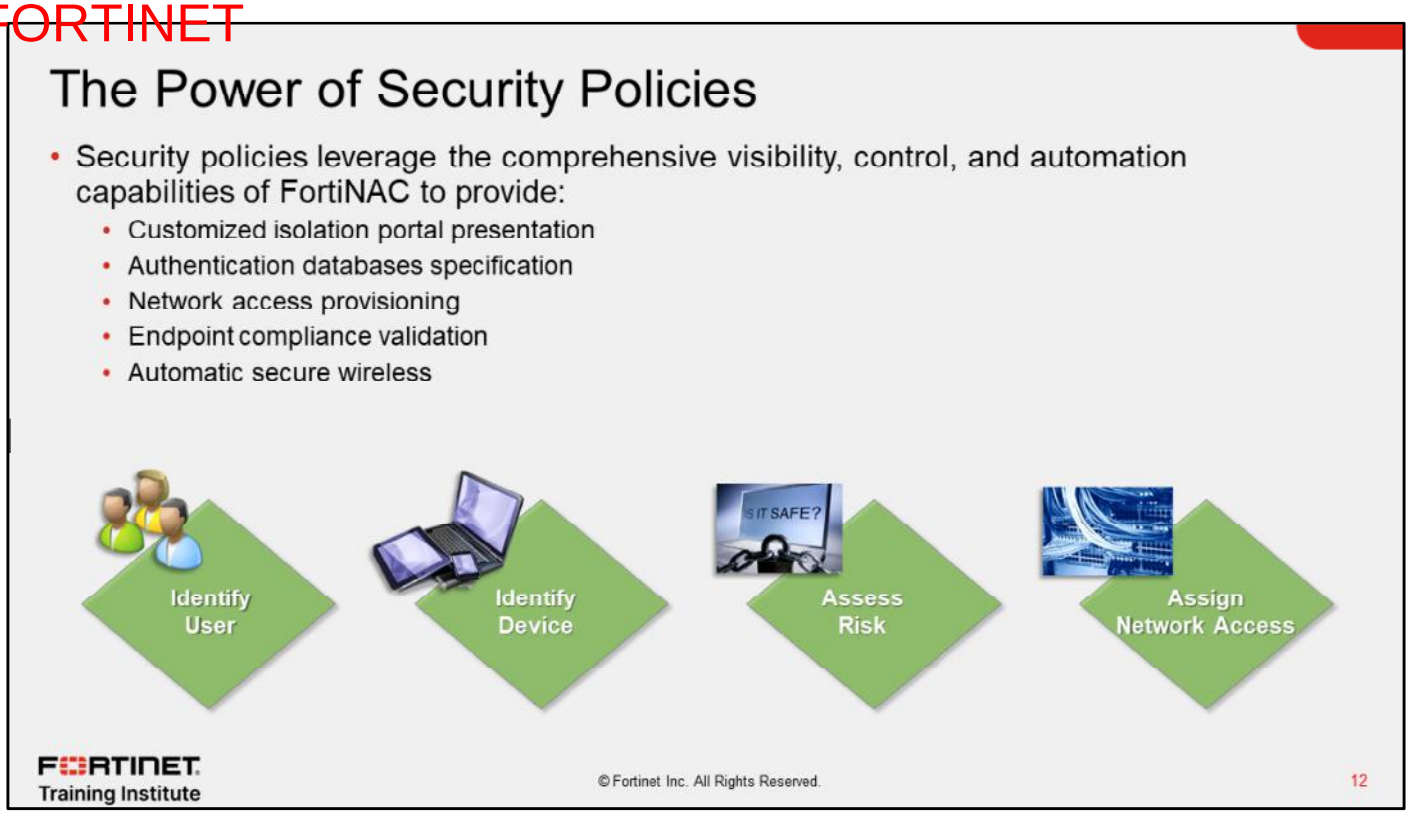


After completing this section, you should be able to achieve the objective shown on this slide.

By understanding the concepts and necessary configurations of security policies, you will be able to plan, create, and enforce security policies in your environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



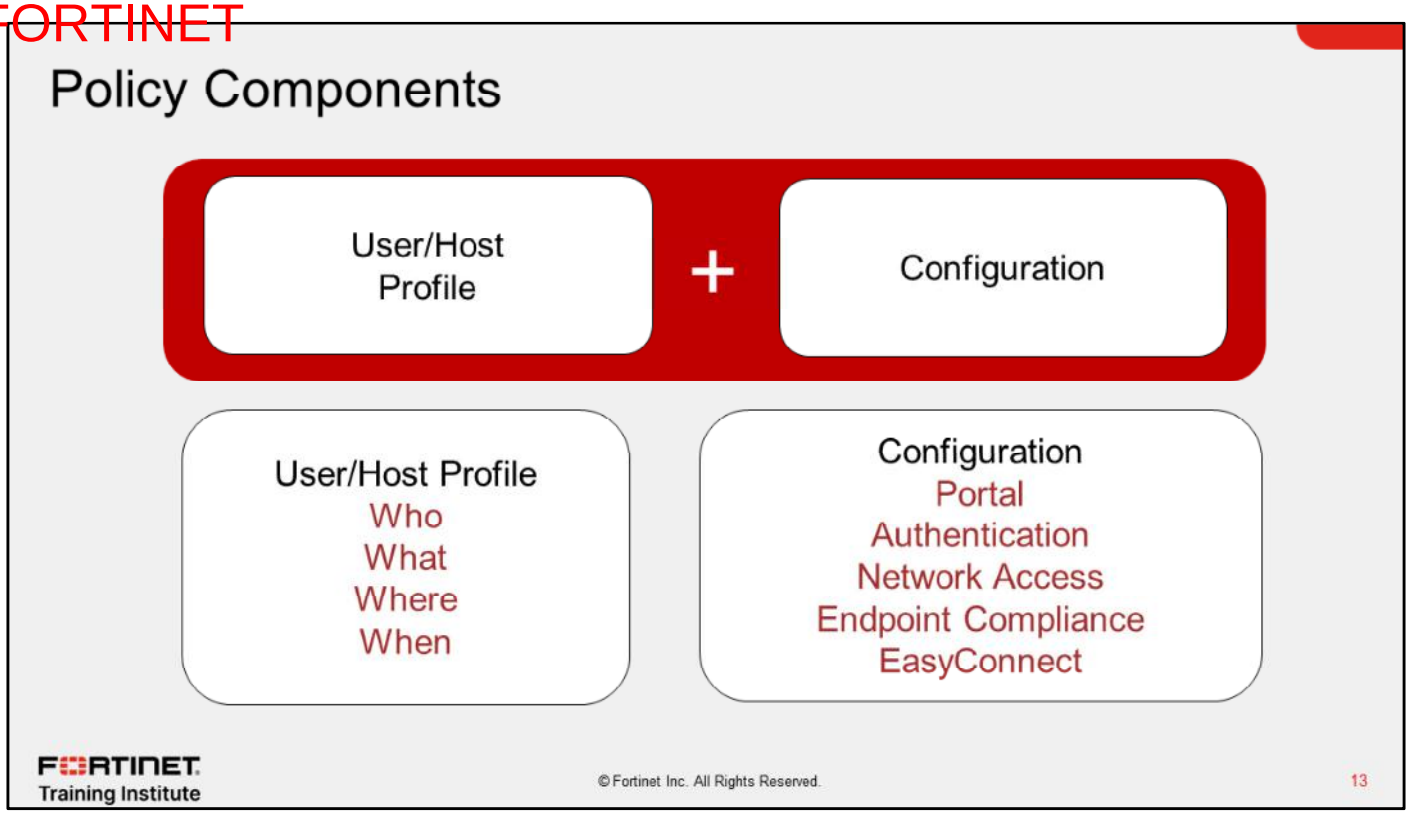
Security policies represent one of the most powerful components FortiNAC has to offer. They leverage the comprehensive visibility details gathered by FortiNAC and combine them with the control, scanning, portal, authentication, and configuration features for powerful automation and control capabilities.

Customized isolation portals can be specifically targeted to users, for example, different guest login pages by geographic location. Back-end authentication databases can be specified for user authentication. Network access can be provisioned on connection for any host, user, or device at the time of connection. Hosts can be scanned using a FortiNAC agent to validate customizable compliance criteria. Configuration of wireless security settings can be automated to simplify secure endpoint access.

The flexibility of security policies allows them to provide these powerful features to virtually any environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



A security policy is composed of two different pieces. The first is the user/host profile, which is the piece that identifies if a user or host matches a particular policy. The second piece is the configuration, which is the policy-specific settings applied if the associated user/host profile is matched.

User/host profiles are a set of FortiNAC visibility parameters—the who, what, where, and when information discussed in the *Visibility* lesson. These profiles can range from general to very specific, keying upon individual attributes, and applying AND, OR, and NOT logic.

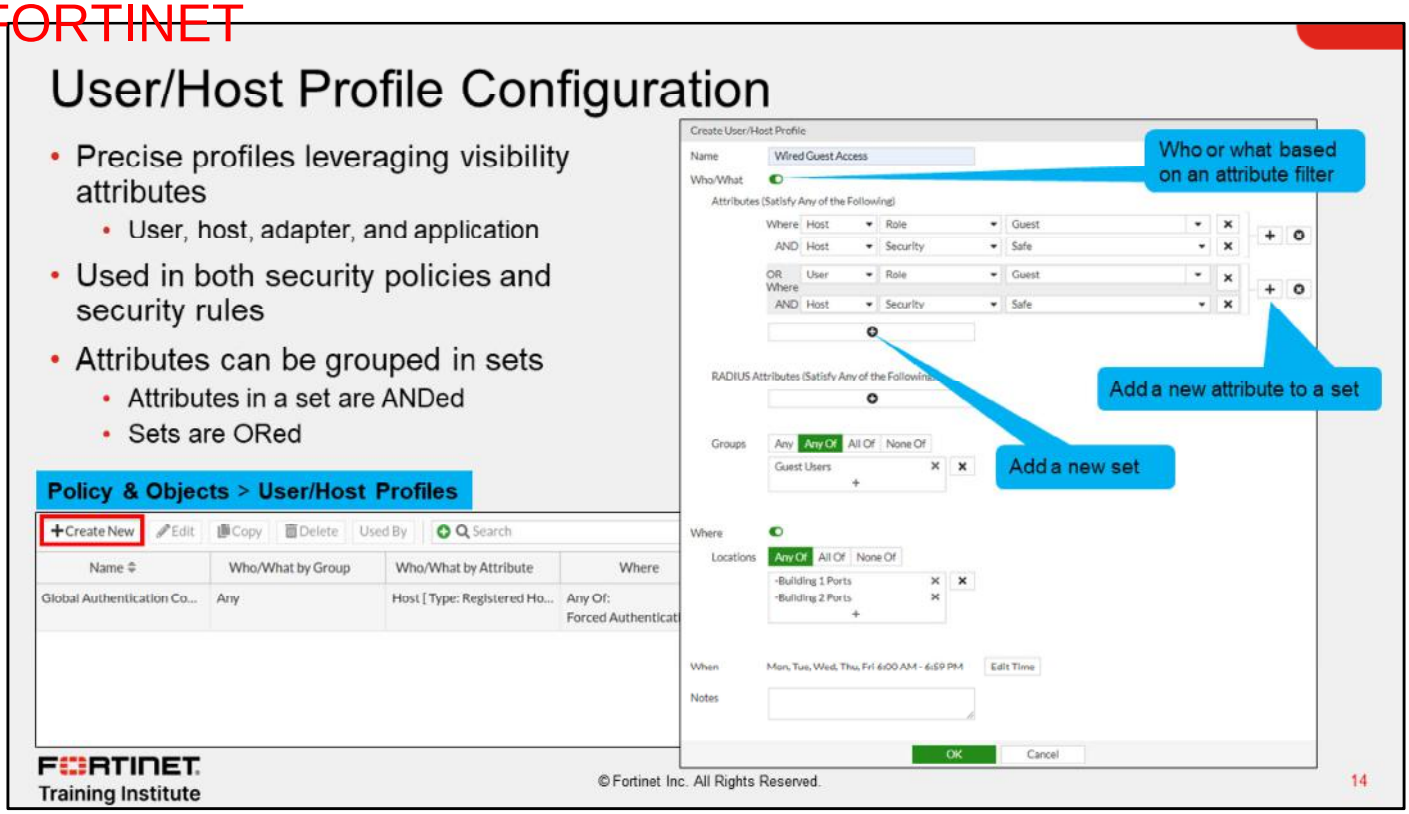
You can associate five different types configurations with a user/host profile:
- Portal
- Authentication
- Network Access
- Endpoint Compliance
- Supplicant EasyConnect

Hosts and users are continuously evaluated to identify if a user/host profile matches. Whenever FortiNAC identifies a match, the highest ranked security policy of each type, if any, will be applied.

For example, if a user matches a user/host profile that identifies guest users, and that user/host profile is associated with a network access configuration, the configuration settings will be applied, provisioning the access appropriately.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



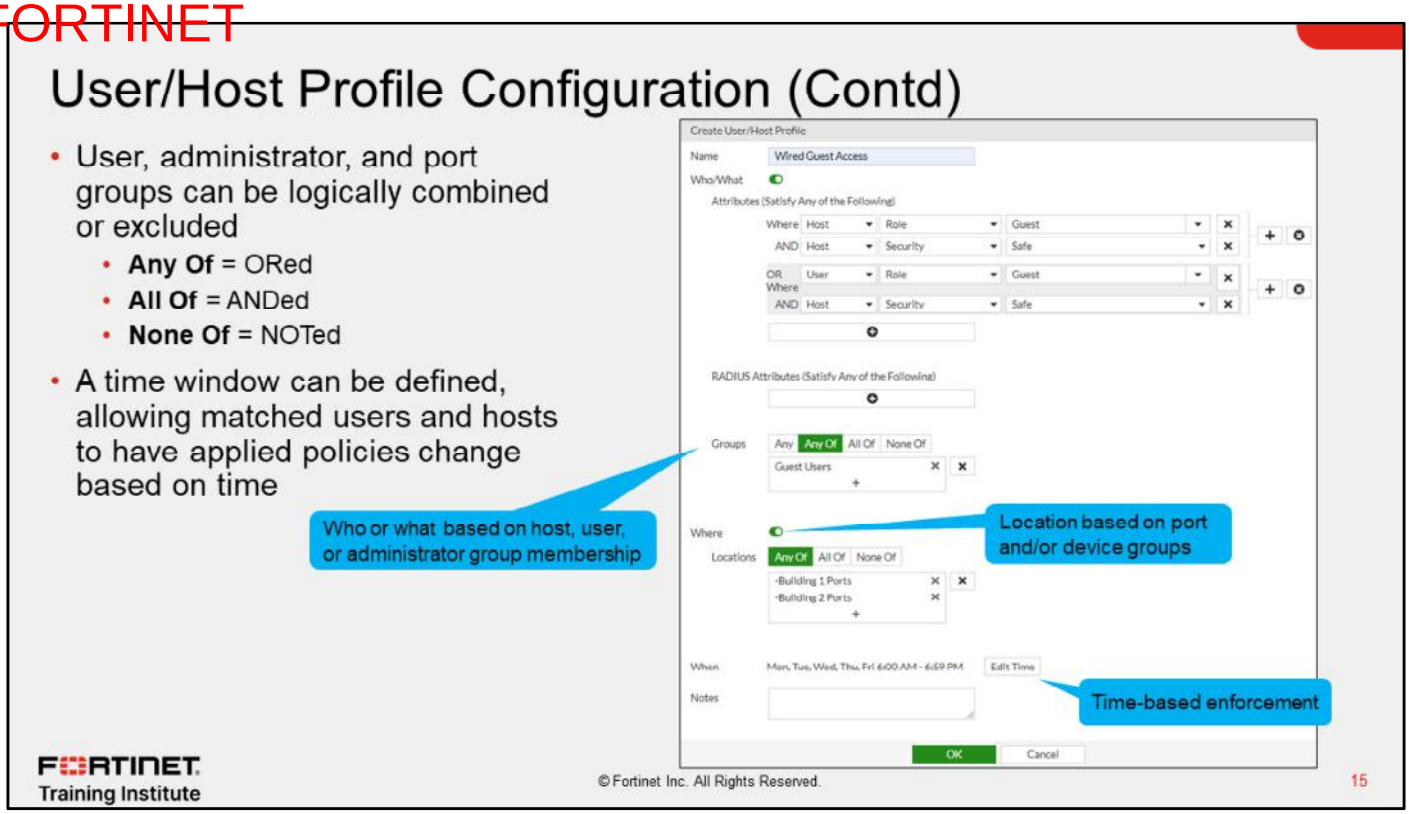
User/host profiles are used to determine the targets of all types of security policies. The detailed visibility information, organized as attributes, provides the ability to target hosts and users very specifically. In addition to targeting users and hosts for security policies, user/host profiles can be used in the definition of security incident rules. Security incident rules are covered in another lesson.

In the example shown on this slide, the name is **Wired Guest Access**. It is helpful when creating user/host profiles that will be used for network access policies, to include the type of access, such as wired or wireless, in the name of the user/host profile.

The **Attributes** component of the **Who/What** field works differently. You choose each attribute from a list of all attributes associated with the following components: **Adapter**, **Host**, **User**, and **Application**. The logic used for determining a match depends how the attributes are designated. Attribute criteria are ANDed together when they are part of the same set, as shown on this slide with the two entries, where the first set defines that the host must have a role of **Guest** and the host security state must be **Safe**. The second set defines that the user must have a role of **Guest** and the host security state must be **Safe**. Adding more than a single attribute set will result in the two sets being logically ORed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



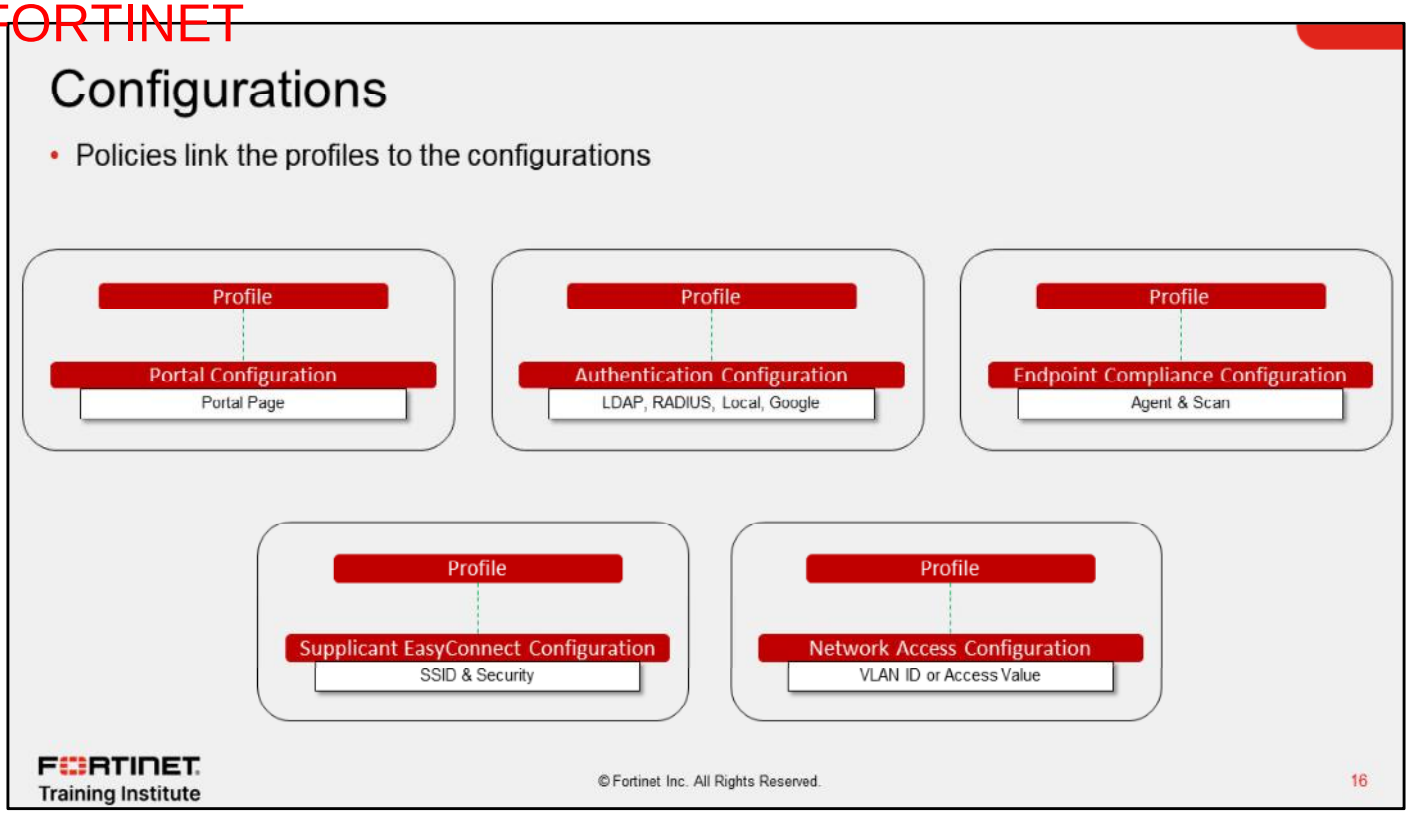
In addition to attributes, you can designate user, host, and port group memberships. It is common for host, user, and device network access to be dependant on point of connection. For example, the guest VLAN could be different from one building to the next. The same could be true for printers, security cameras, and so on. Time-based policy enforcement can be useful for dynamic policy changes. For example, guests could be moved to a dead-end VLAN after business hours.

The example shown on this slide shows the first part of a user host profile. The partial profile shown on this slide would match if:

- The connecting host has a role of guest *and* a security value of safe, *or* the user has a role of guest *and* the host has a security value of safe.
- The user is a member of the **Guest Users** group.
- The host is connecting to a port in the Building 1 Ports group *or* Building 2 Ports group.
- The current time is between 6 AM and 6 PM, Monday through Friday.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Once the FortiNAC policy engine identifies that a user or host matches a user/host profile, it will then apply any configurations associated with that profile. If a single profile is associated with more than one configuration of the same type, the highest ranked configuration is applied. Because of this, you should not assign a single user/host profile to more than a one configuration of each type.

There five different configuration types, and what they consist of is shown on this slide.

A portal configuration consists of a captive portal page that will be displayed to users with isolated hosts. This is most typically a location-based profile. For example, you could create different guest login pages for Building 1, Building 2, and Building 3. Then, depending upon a host's point of connection, a customized onboarding portal page could be displayed.

An authentication configuration defines an authentication source for authenticating or onboarding users. The available options are **LDAP**, **RADIUS**, **Google**, **Local**, and **None**.

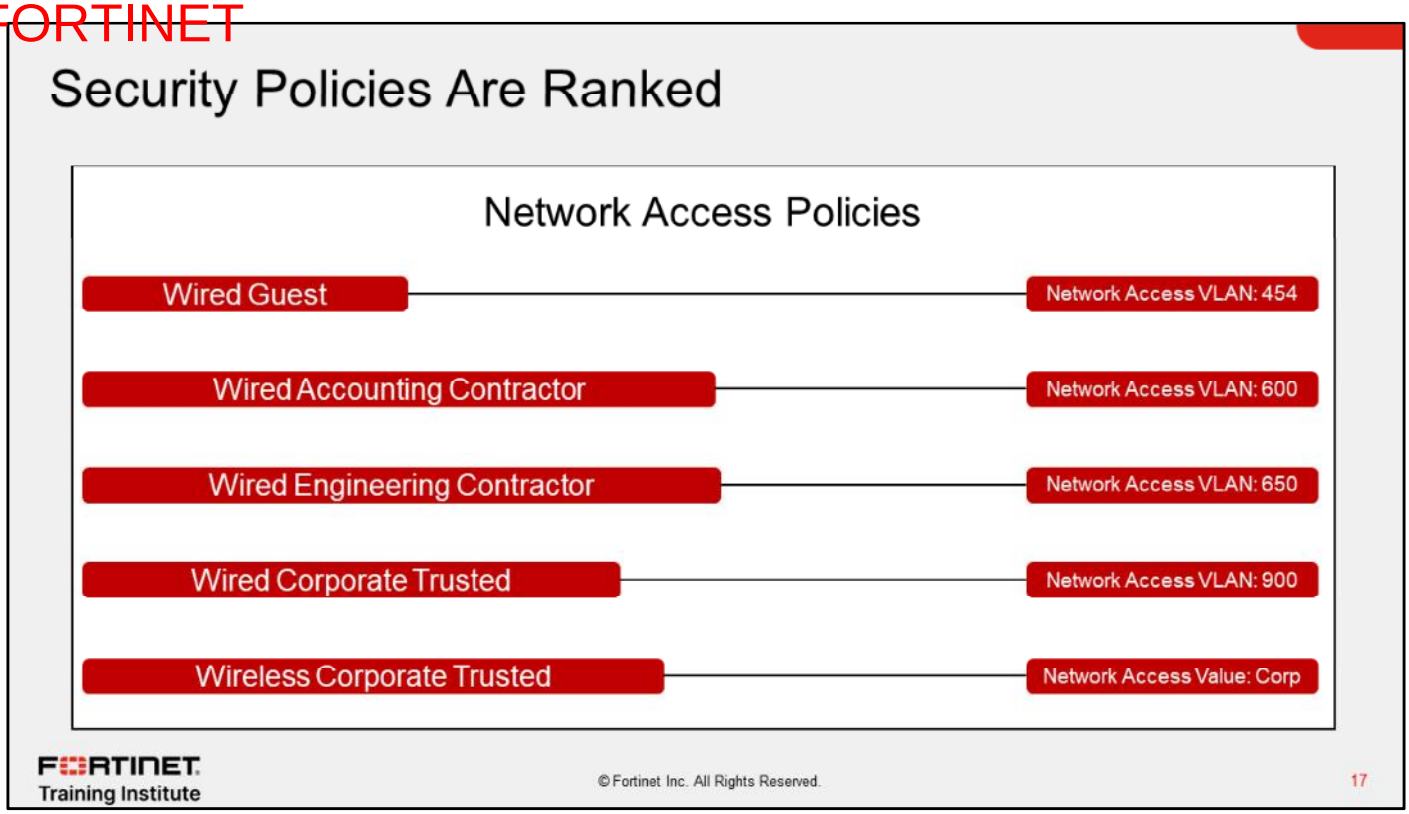
An endpoint compliance configuration defines the required compliance scan criteria and FortiNAC agent technology to be used for compliance validation.

A supplicant EasyConnect configuration results in the creation of a wireless configuration on the endpoint to access a designated wireless network. The configuration can apply the following security options:
- Open
- WEP (PSK) and WEP Enterprise
- WPA (PSK), WPA Enterprise (PEAP), WPA2 (PSK), and WPA2 Enterprise (PEAP)

A network access configuration will provision the defined VLAN, wireless access value, and/or CLI settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

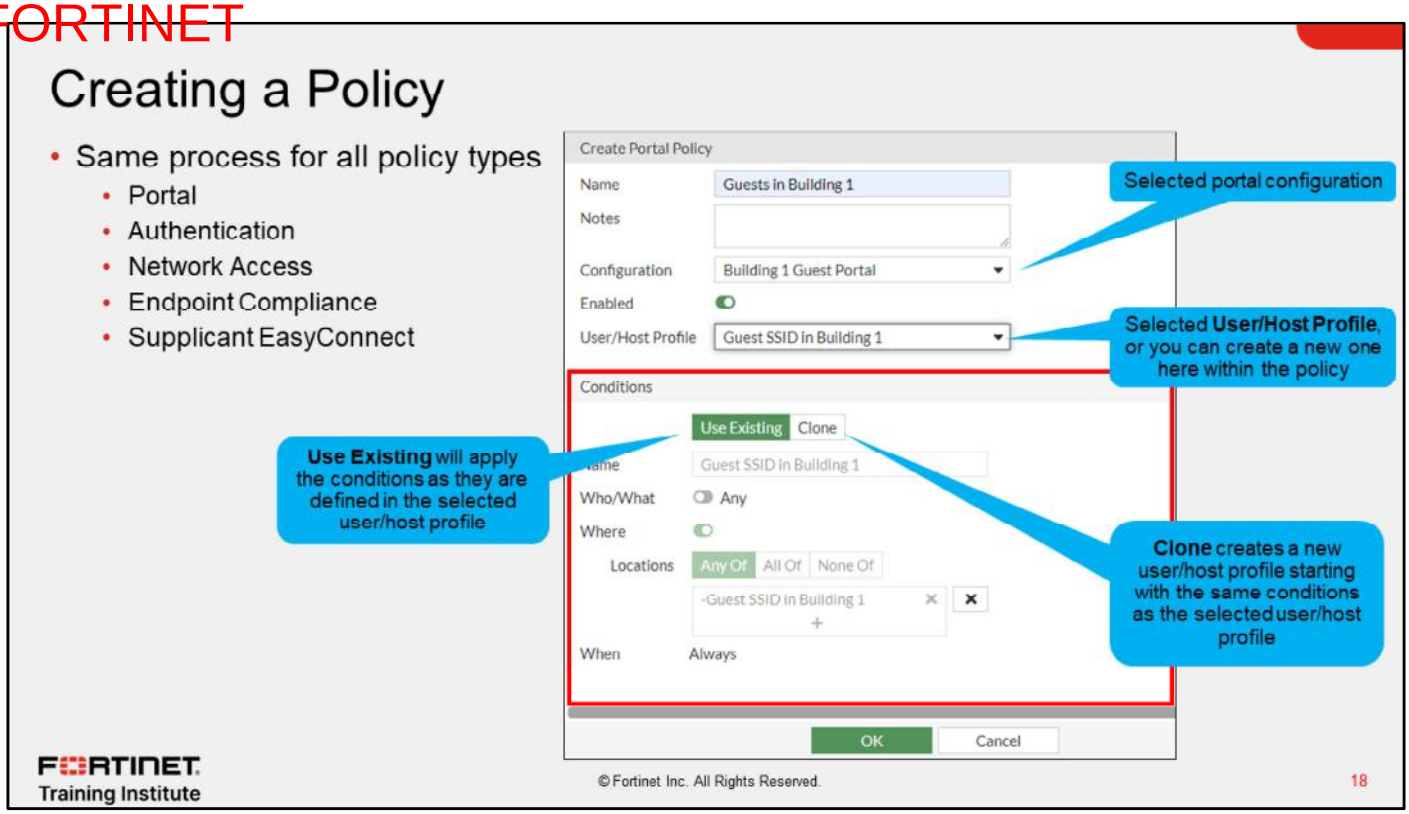


Policy configurations of each type are ranked. When a host connects to the network, that host is evaluated against each user/host profile. If FortiNAC finds a user/host profile match, it then evaluates the configurations of each policy type. In the example shown on this slide, if a user or host connected and matched the Wired Engineering Contractor and the Wired Corporate Trusted user host profile, it will be provisioned a network access VLAN of 650, because that is the higher-ranked configuration.

This example also shows why the same user/host profile would not be associated with more than one configuration of each policy type. The lower-ranked configuration would never be applied.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



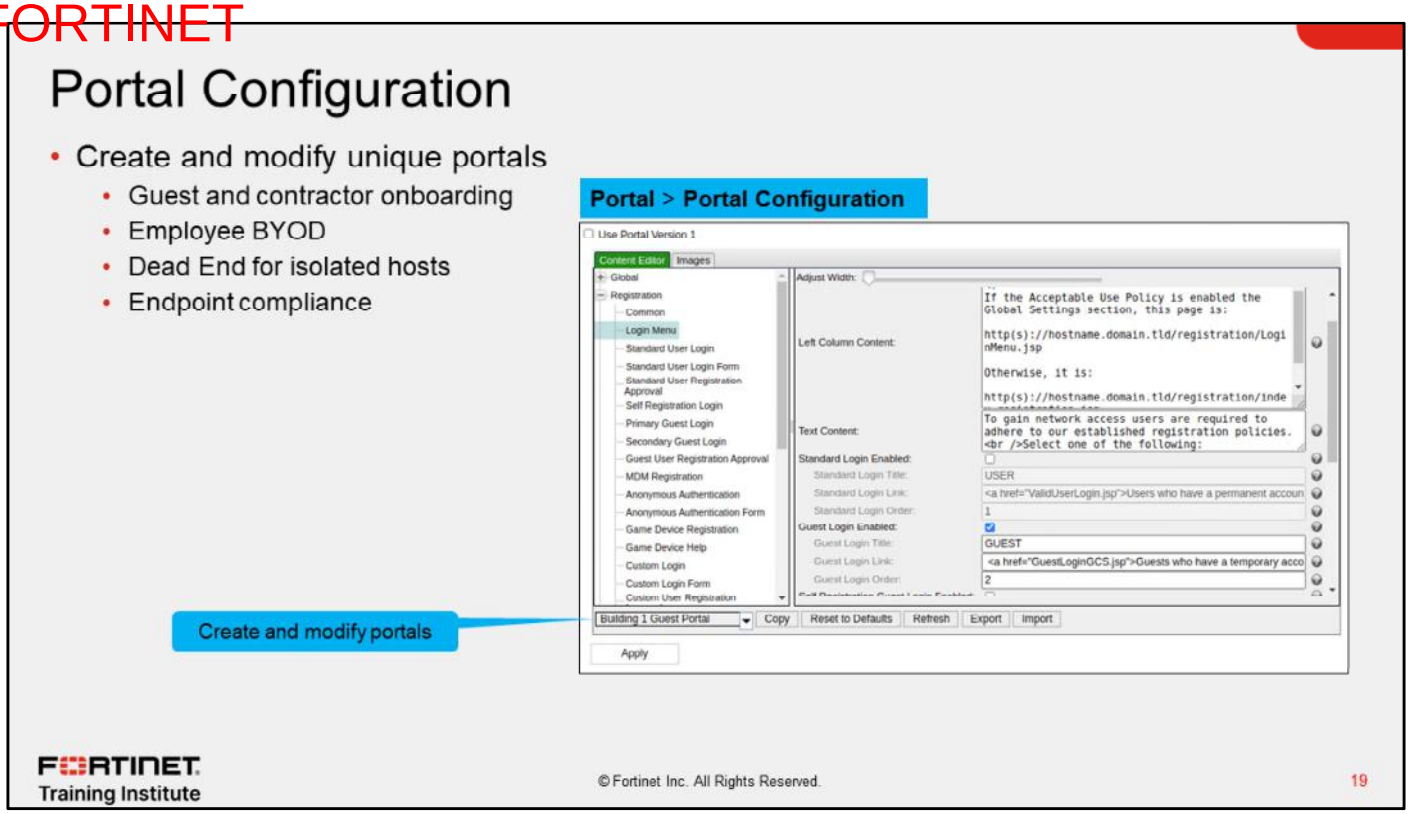
You create each type of policy in the same way, by associating a configuration of the appropriate type to a user/host profile.

In the example shown on this slide, the policy is named **Guests in Building 1**. The **Configuration** field is a drop-down list of all existing configurations for the selected policy type. In this example, it is a portal policy.

The **User/Host Profile** field is a drop-down list that contains all currently existing user/host profiles. Once associated, you can make policy specific modifications to the user/host profile in the **Conditions** section of the window.

Vouchers & Dumps are Available | WhatsApp +201224560923

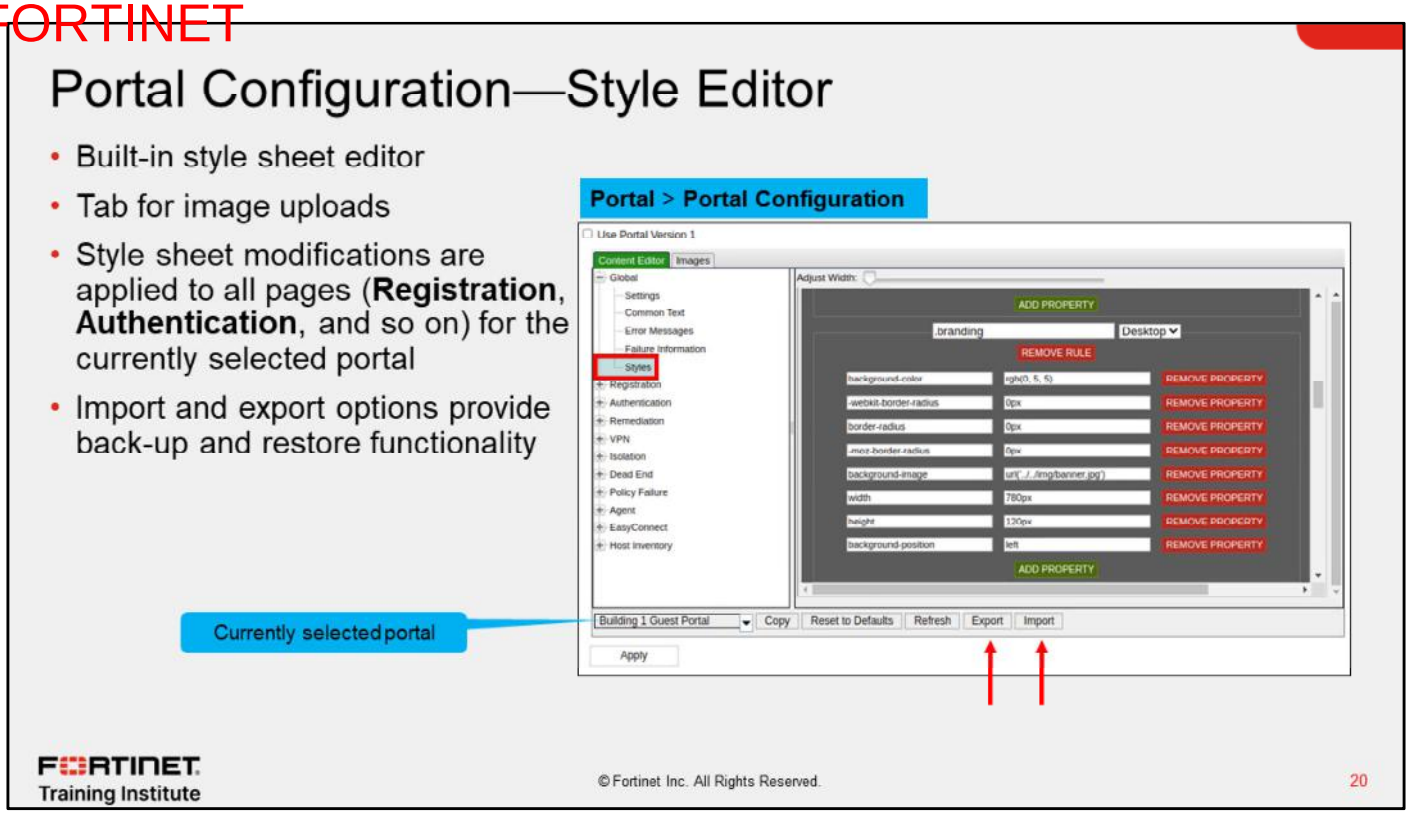
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The ability to create and customize portals allows organizations to maintain consistency from one page to the next. You can customize each of the internal pages presented by FortiNAC to comply with corporate or organizational branding and flow. When you combine a customized page configuration with a user/host profile to create a portal policy, you can take the customization a step further and target specific users or hosts. For example, guest and contractor onboarding pages could be different based on geographic location, or on the operating system of the device, or both.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



As a means to simplify the page customization process, a built-in style sheet editor provides simplified editing of all associated pages in a selected portal. All associated portal pages will reflect the style sheet changes. You use the images tab to upload images for use in page customizations.

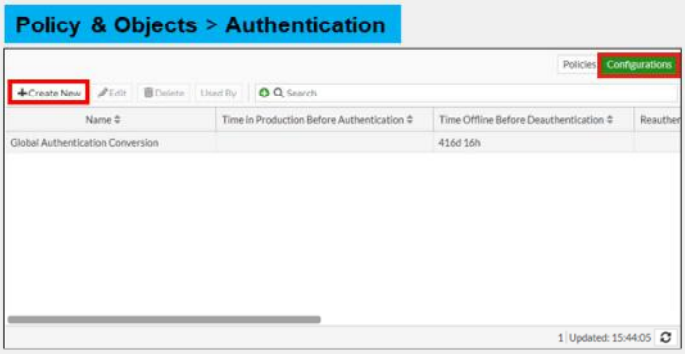
After completing page customizations, import and export options provide you a way to back up or restore your pages. Exporting pages will store all pages and images associated with the portal in a zipped folder on the local system.

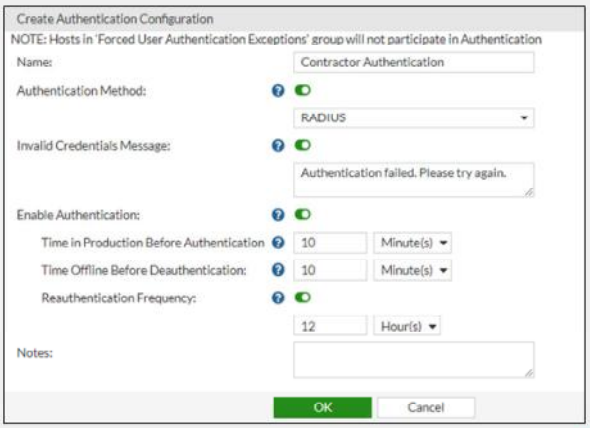
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Authentication Configuration

- Policy-based, back-end authentication server designation
  - LDAP
  - RADIUS
  - Local
  - Google





FORTINET Training Institute

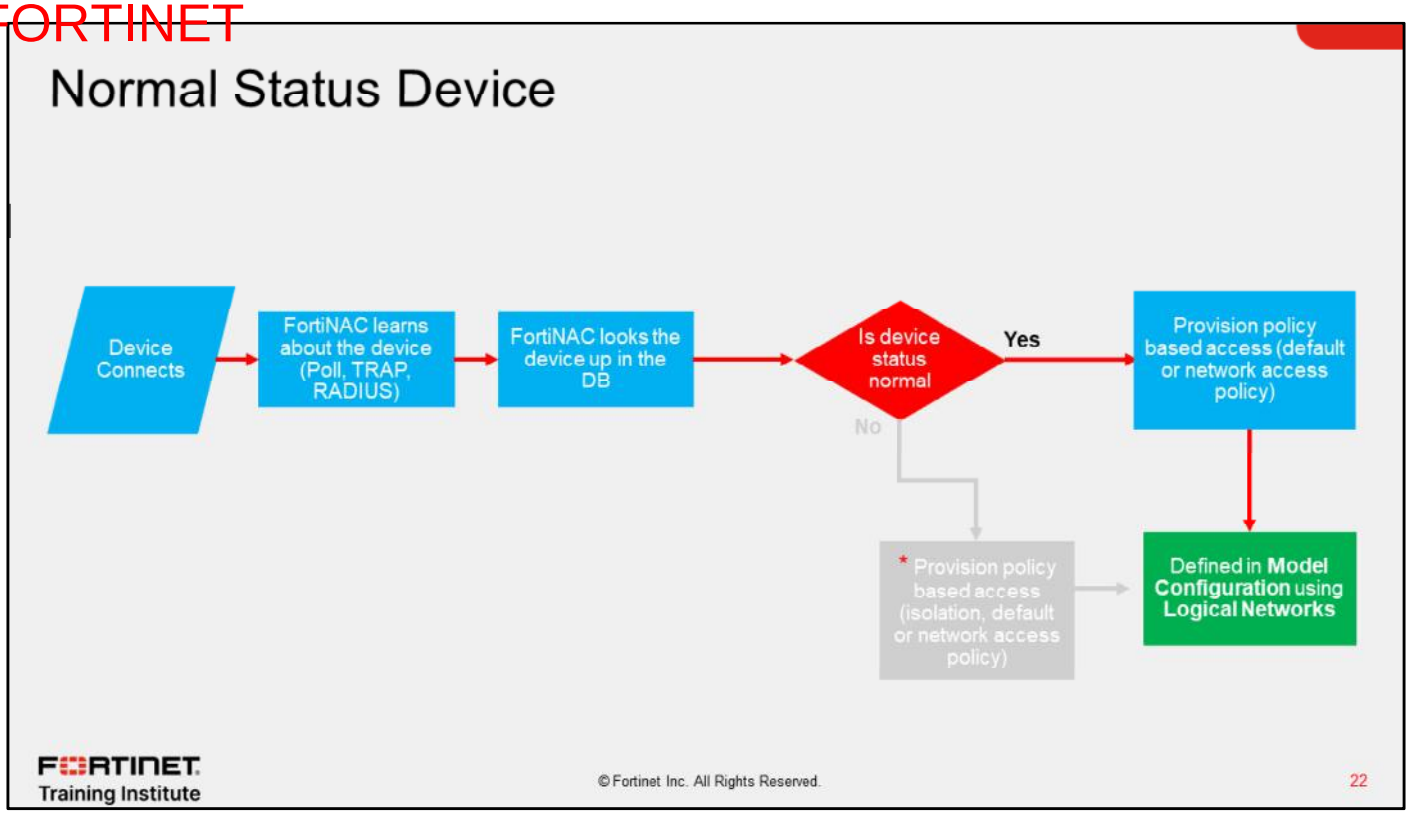
© Fortinet Inc. All Rights Reserved.

21

You may need different users to authenticate against different back-end authentication sources. For example, guests may authenticate using their Google account, while contractors use a RADIUS server, and standard users use LDAP. An authentication configuration consists of detailed settings for an authentication server that will override any default authentication servers for users and hosts that match the associated user/host profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



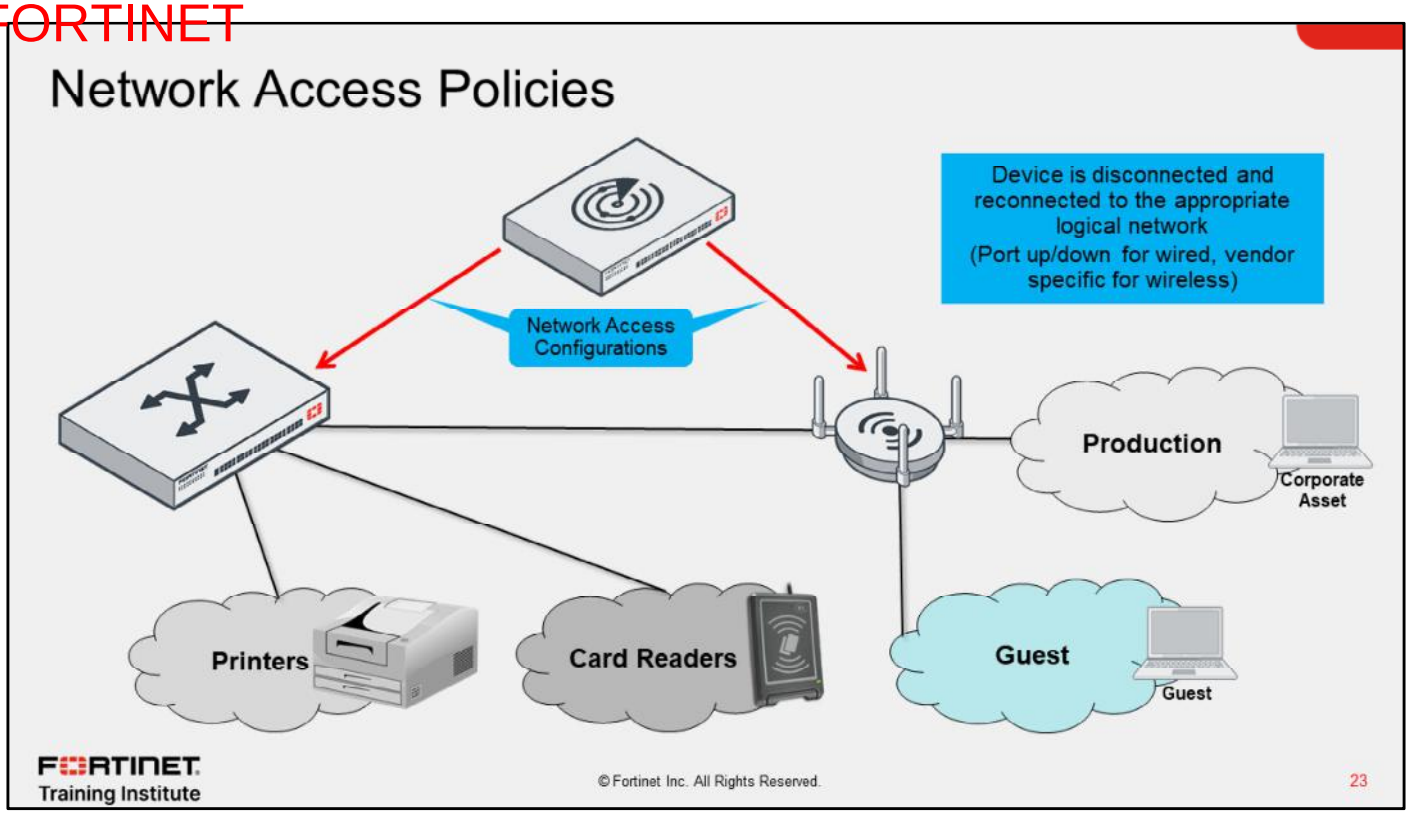
This slide demonstrates the device evaluation process for hosts that have a status of normal.

1. The device connects.
2. FortiNAC learns of the connection. This is often done using Layer 2 Polling, MAC notification traps, RADIUS. Other methods may be used depending on the vendor of the infrastructure.
3. FortiNAC queries the database for the connected device.
4. The device will be provisioned based on a matching network access policy VLAN or the default VLAN.

How the device is provisioned is based on logical networks and how they are defined for each infrastructure device. The definition for these logical networks is set in the **Model Configuration** view of the infrastructure device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

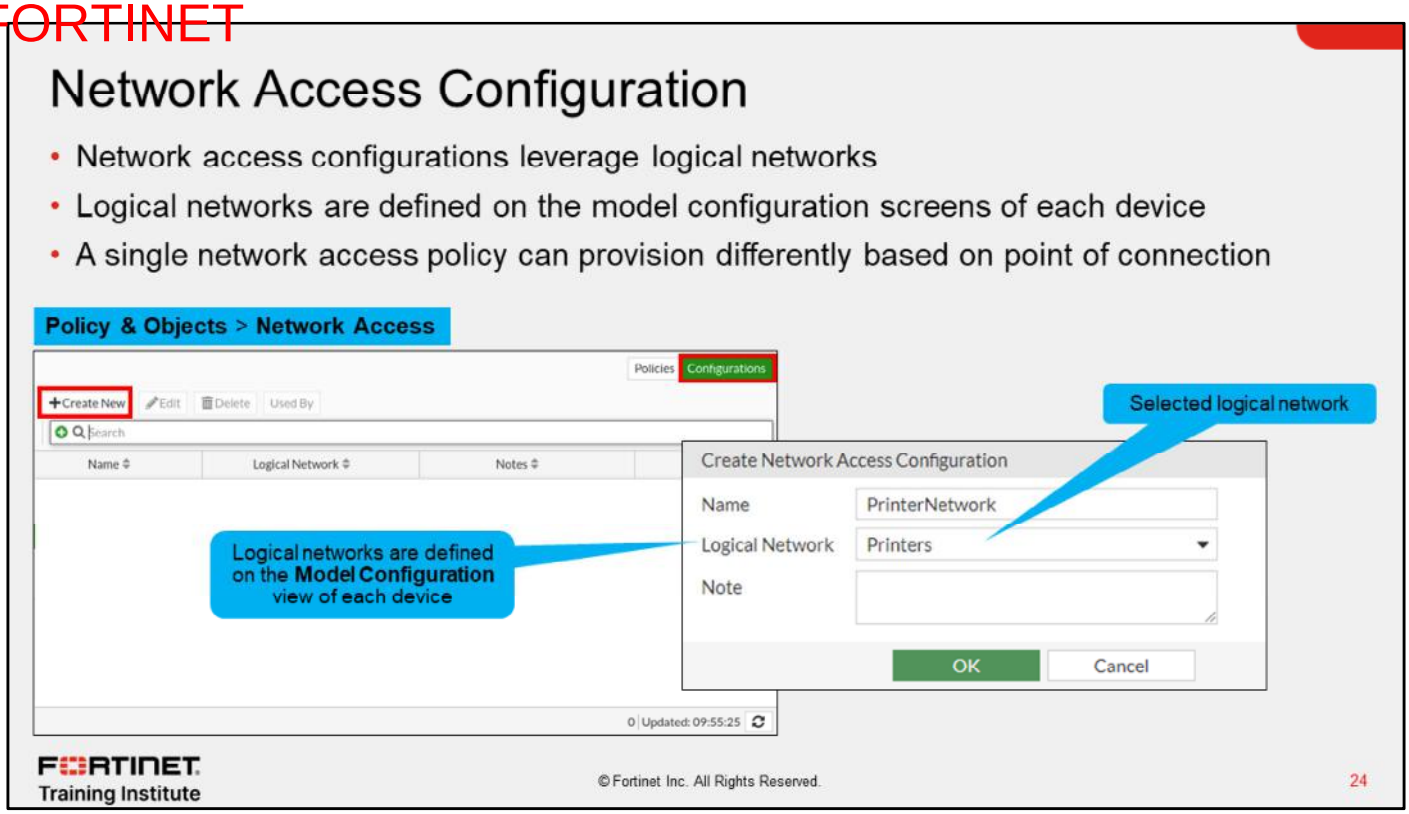


Network access policies are normally the most common type of policy. These policies are used to dynamically provision access to connecting endpoints, based on the matched user/host profiles associated with the network access configurations.

In the example shown on this slide, FortiNAC is evaluating endpoints as they connect to the network. The evaluation identifies if a connected endpoint matches a user/host profile. Printers, corporate assets, guests, and card readers are all given dynamically provisioned network access based on FortiNAC evaluation, and the associated network access configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Recall from a previous lesson that logical networks are an abstract concept that decouple a policy from a specific access value. The logical network value is defined on a device-by-device level in the **Model Configuration** of a device, the same way that an isolation network, such as **Registration**, is defined.

For example, a user could create a **`Printers`** logical network, and define, for that logical network, an access value of 100 on one set of switches, and 200 on another set of switches. Then a single network access policy could assign the logical network of `Printer` to any printer on the network.

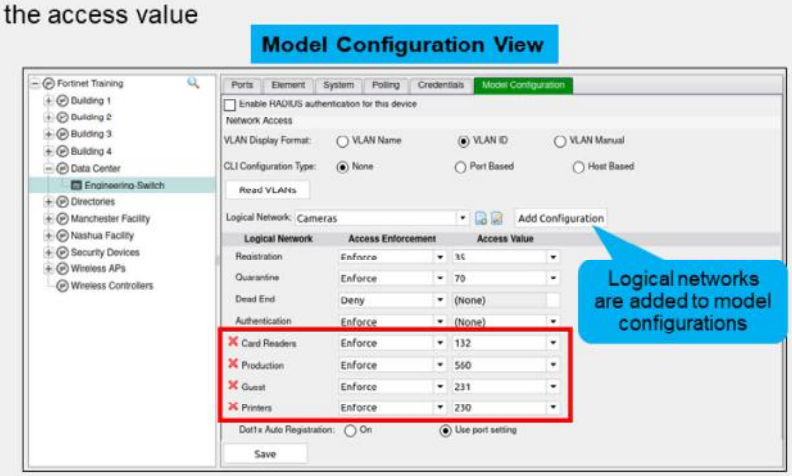
The printers would have the same network access policy applied to them, but be provisioned differently based on the point of connection. This concept can significantly reduce the number of network access policies needed, and simplify network access policy management.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Model Configuration—Policy-Based Enforcement

- Selected logical networks can be added to device model configurations
- Users and hosts that match a network access policy will be provisioned based on the logical network definition
  - **Enforce** – provision based on the access value
  - **Deny** – do not grant access



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

25

Any user-created logical networks can be added to the **Model Configuration** views, and access values can be assigned for correct host provisioning. Depending on the type of infrastructure device (such as a router or an AP), logical network settings can define firewall tags, RADIUS attribute groups, or group names to be passed back to the infrastructure device by FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiNAC Agents

- Persistent agent
  - Installed (pushed, image, manual)
- Dissolvable agent
  - Runs once (manual)
- Mobile agent
  - Installed for Android (manual)
- The passive agent is not deployed using endpoint compliance policies



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

26

Each of the three agents available for deployment to isolated hosts provides slightly different capabilities and functionality. Regardless of the agent type, however, each provides the ability to scan the endpoint for policy compliance, gather installed applications, and report host and interface details to FortiNAC.

The persistent agent is installed and stays resident on the endpoint. Note that this agent is normally deployed by either being pushed out as part of a group policy or some other software management application, or as part of an image. Deployment through a captive portal requires the end user to manually install the agent.

The dissolvable agent is a run once agent, and requires manual end-user interaction within the captive portal. Once it completes and it reports its results, it dissolves and leaves no footprint on the endpoint. This is a common choice for guests, contractors, or BYOD devices.

The mobile agent is installed manually within the captive portal during the onboarding process and is the only agent option for Android devices.

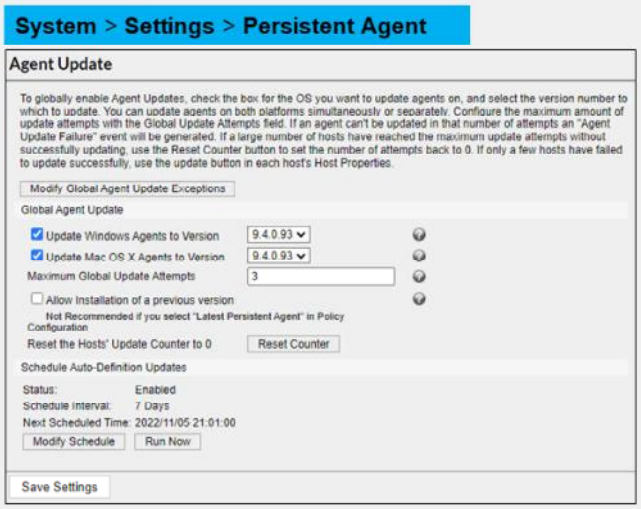
The passive agent is not included as an option in endpoint compliance configurations because it is deployed using domain login/logout scripts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Persistent Agent Settings—Agent Update

- Windows and Mac OS X persistent agents can be globally updated
- FortiNAC will attempt to perform updates if they initially fail
- Specific hosts can be excluded from the global updates
- Auto-definition updates retrieve the latest virus definitions and signature information



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

27

In most environments, leveraging the FortiNAC persistent agent, a means to globally update hosts, is a necessity. Attempting to manually update every host in an environment would be time consuming and result in hosts being missed. When an agent responds to FortiNAC, the agent version is evaluated against the update settings. Older versions will be automatically updated. This process ensures that any host on the network with a communicating agent will be evaluated.

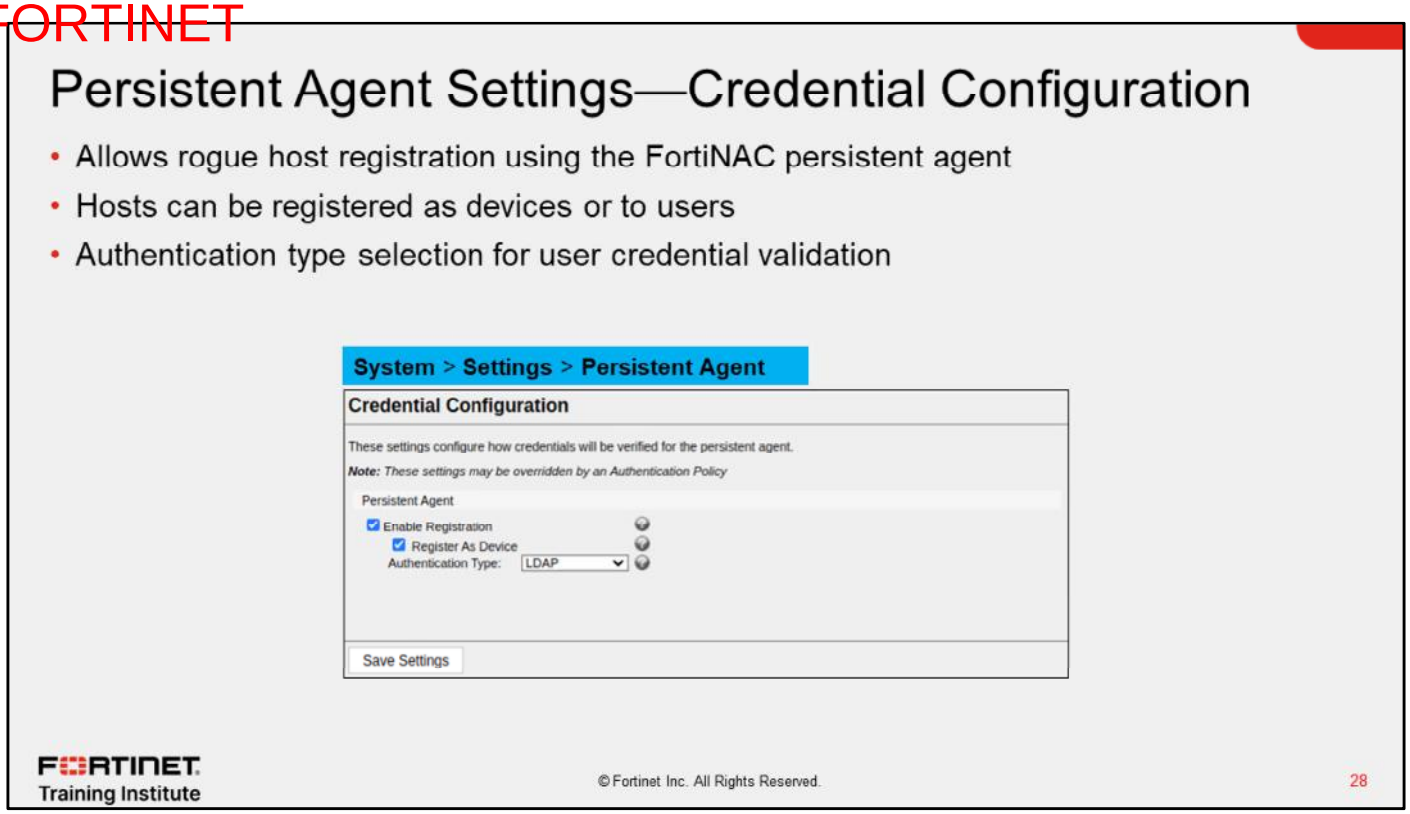
Selected hosts can be excluded from the global updates by being added to the **Global Agent Update Exceptions** host group. A button is provided at the top of this view for modification of that group's membership.

If an agent update fails, FortiNAC will continue update attempts, up to the number specified in the **Maximum Global Update Attempts** setting. If the **Maximum Global Update Attempts** specification is reached, FortiNAC will stop attempting to update that agent. An event, **Agent Update Failure**, will be generated. The reset counter option will configure FortiNAC to retry failed agent updates, up to the specified number of **Maximum Global Update Attempts**.

You can set the schedule for FortiNAC to automatically update the virus definition or signature information for the antivirus software options within endpoint compliance scans.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In some situations you may want to allow host registration through the persistent agent. This can simplify the onboarding process for hosts with pre-installed agents.

You can register any host automatically with a persistent agent that has established communication with FortiNAC. Typically, this is disabled when rogues are being registered by the **Device Profiler**.

Registering a host as a device will automatically register all rogue hosts using the hostname in the **ID** field in the host record.

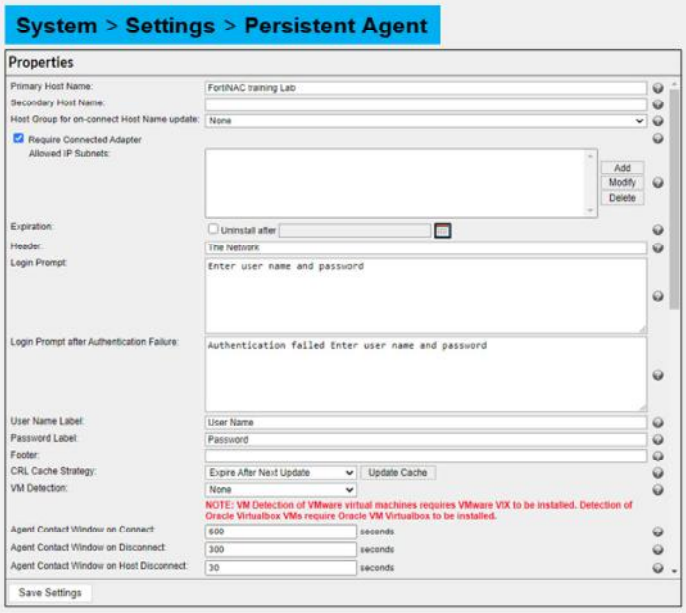
If the **Register As Device** checkbox is not selected, the **Authentication Type** defines the back-end authentication server for authentication when tracking users. Note that the authentication type selected must match the authentication method selected in the **Portal Configuration** window.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Persistent Agent Settings—Properties

- Primary and secondary FortiNAC host name settings for agent communication
- Distributed environment FortiNAC host communication settings
- Agent label and contact timer settings for FortiNAC communication
- Customization of agent notifications



FORTINET Training Institute

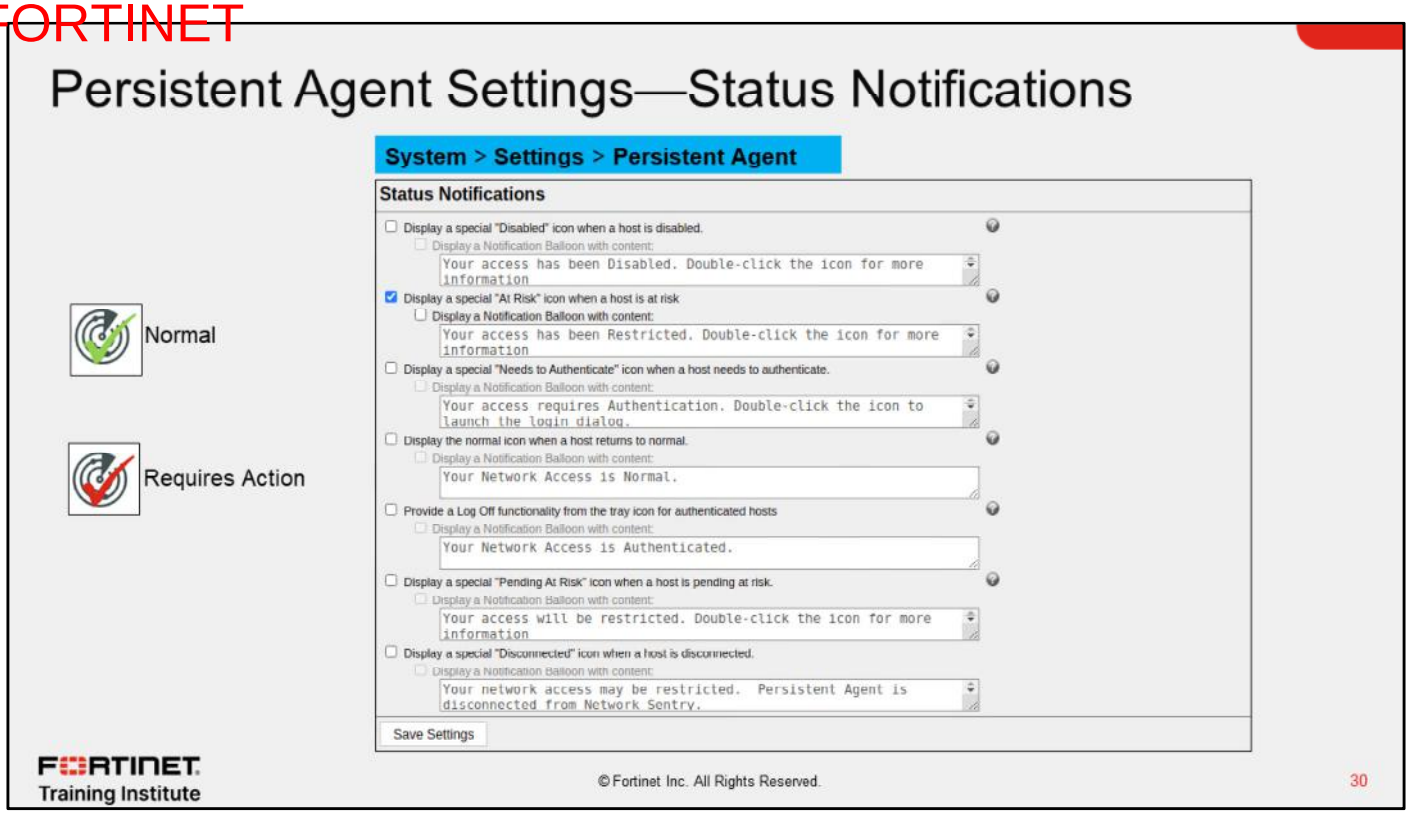
© Fortinet Inc. All Rights Reserved.

29

You have several customization options that can define persistent agents to FortiNAC communications. When you deploy persistent agents in your environment, you must have the FortiNAC FQDN configured in the properties window for successful agent communication. In high availability, you must configure the secondary host name as well. In large, distributed environments, were you have more than a single FortiNAC, the **Require Connected Adapter** and **Allowed IP Subnets** allow you to direct agent traffic to the desired FortiNAC. You can completely customize any of the notifications that can be sent to an agent.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



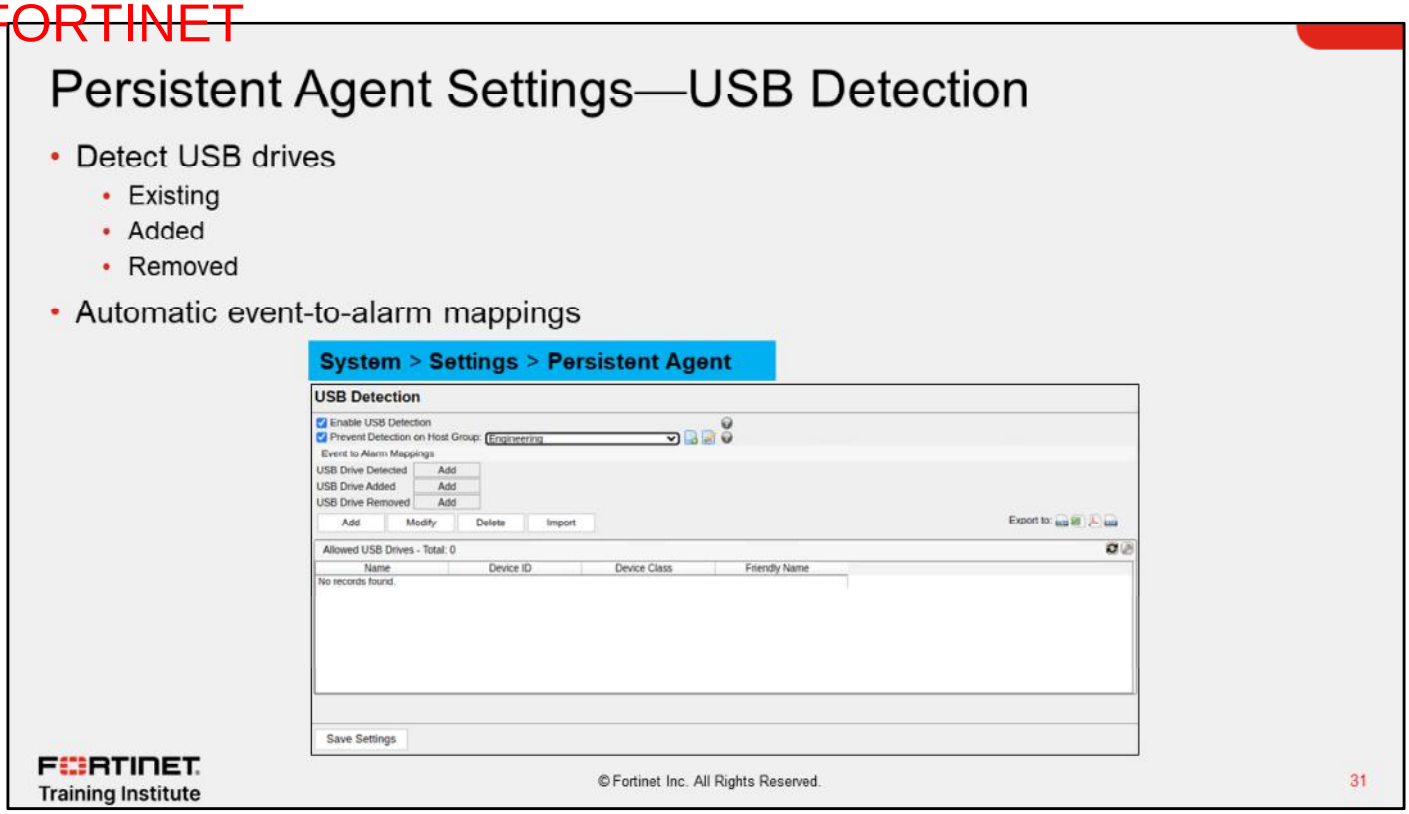
The **Status Notification** view allows you to change the icon that appears on the taskbar based on the state of the host in the FortiNAC database.

This slide shows the two possible icon states, **Normal** and **Requires Action**, that can be displayed in an endpoint's task bar.

Each host state can be selected individually so that only the desired host states change the icon. A second option within each icon display option is for a pop-up balloon notification to appear in addition to the changing of the icon. This will allow the end user to interact with balloon text and assist the user with non-normal state resolution. The text that appears in the pop-up balloons is customizable in each associated field.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Many high security environments prohibit the use of USB drives by end users to prevent possible data breaches.

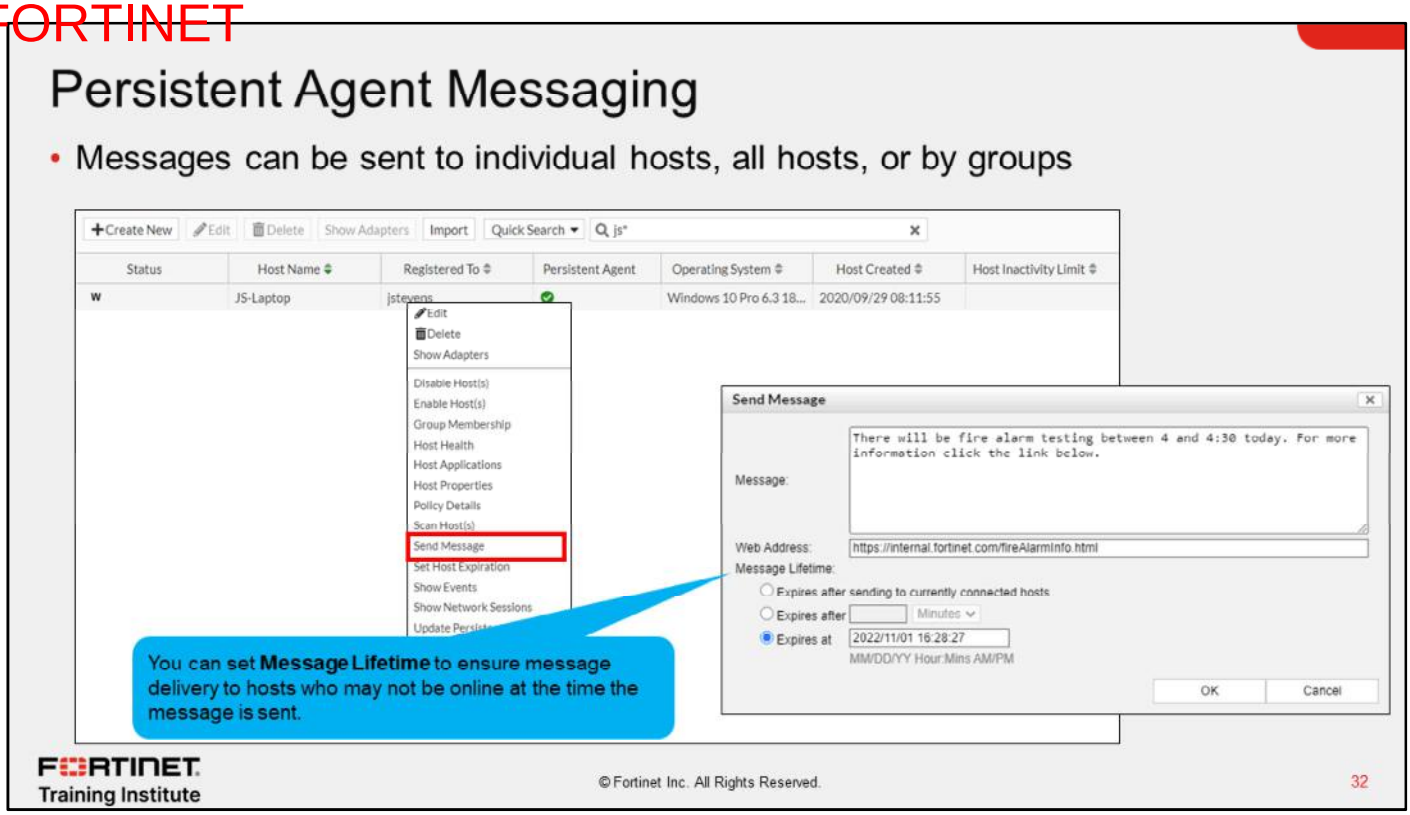
The **USB Detection** view allows you to configure FortiNAC to be notified in the event that a USB device was plugged into a host on the network. When a USB drive is detected, FortiNAC events can be mapped to alarms to specify actions based on the host where the USB drive was detected. You can also indicate which drives should be ignored by the system, regardless of the hosts they are connected to.

The **Event to Alarm Mappings** option allows you to map events to generate alarms when a USB drive is detected, added, or removed. You can then associate actions with the alarms. For example, a host detected with a prohibited USB drive could be isolated by the alarm action.

The **Allowed USB Drives** section provides a means to create a list of USB drives that will not generate events or alarms when detected, added, or removed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Another ability of the persistent agent is to display a message within the message window of an agent installed on an endpoint. Endpoint targets for the message can be an individual host, a group of hosts, or all hosts with the persistent agent installed. The messaging options are available by right-clicking an individual host, or on the **Users & Hosts** > **Send Message** view.

You can enter message content in the **Message** field, and use the optional **Web Address** field to include a URL as a link in the message.

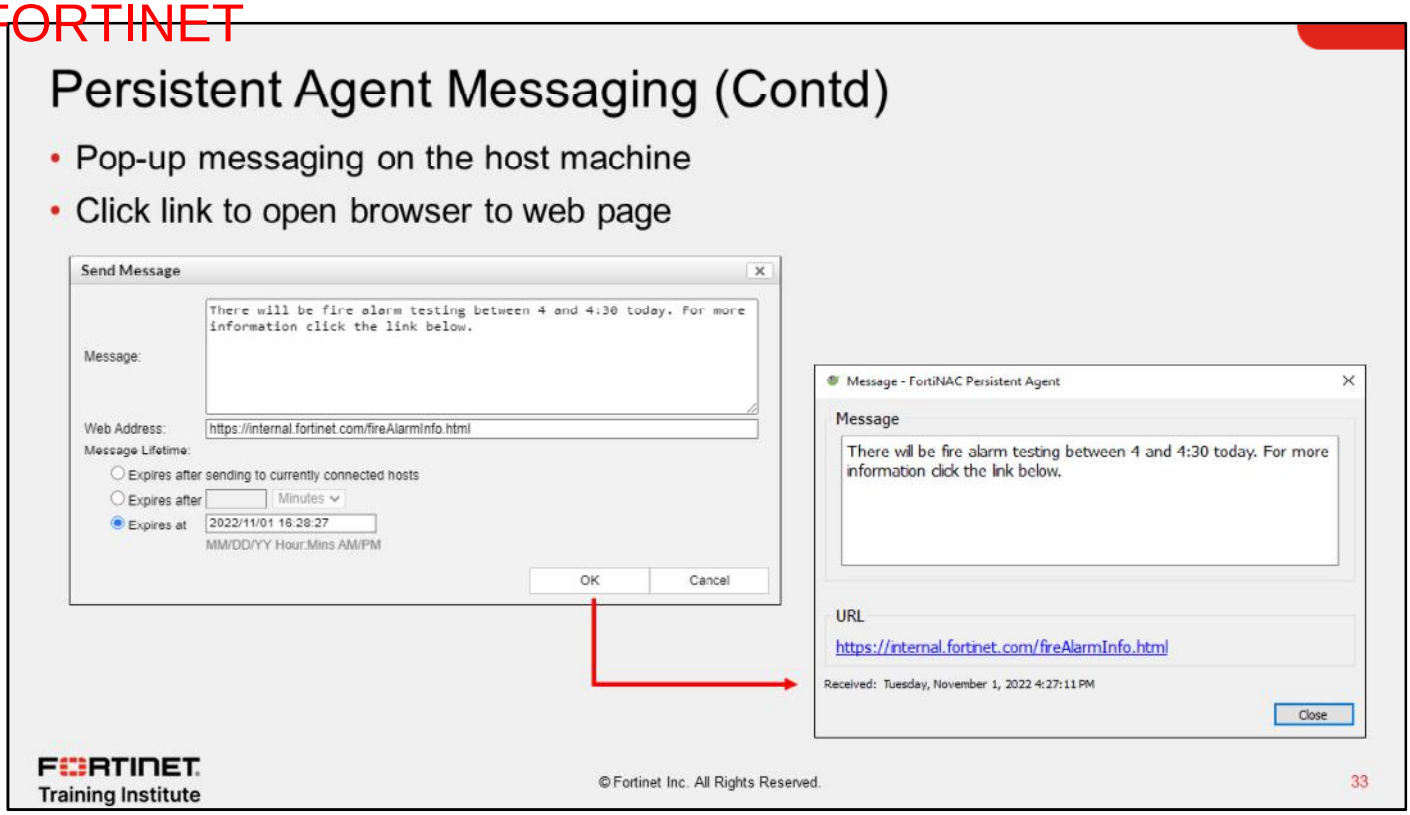
The **Message Lifetime** settings provide the following options:

- **Expires after sending to currently connected hosts**: The message will be sent only to all currently connected hosts.
- **Expires after**: The message will be sent to all currently connected hosts and all hosts that connect within the defined time period.
- **Expires at**: The message will be sent to all currently connected hosts and all hosts that connected before the designated date and time.

Note that a message will be sent only once to each host, even if the host disconnects and reconnects within a designated message time setting.

Vouchers & Dumps are Available | WhatsApp +201224560923

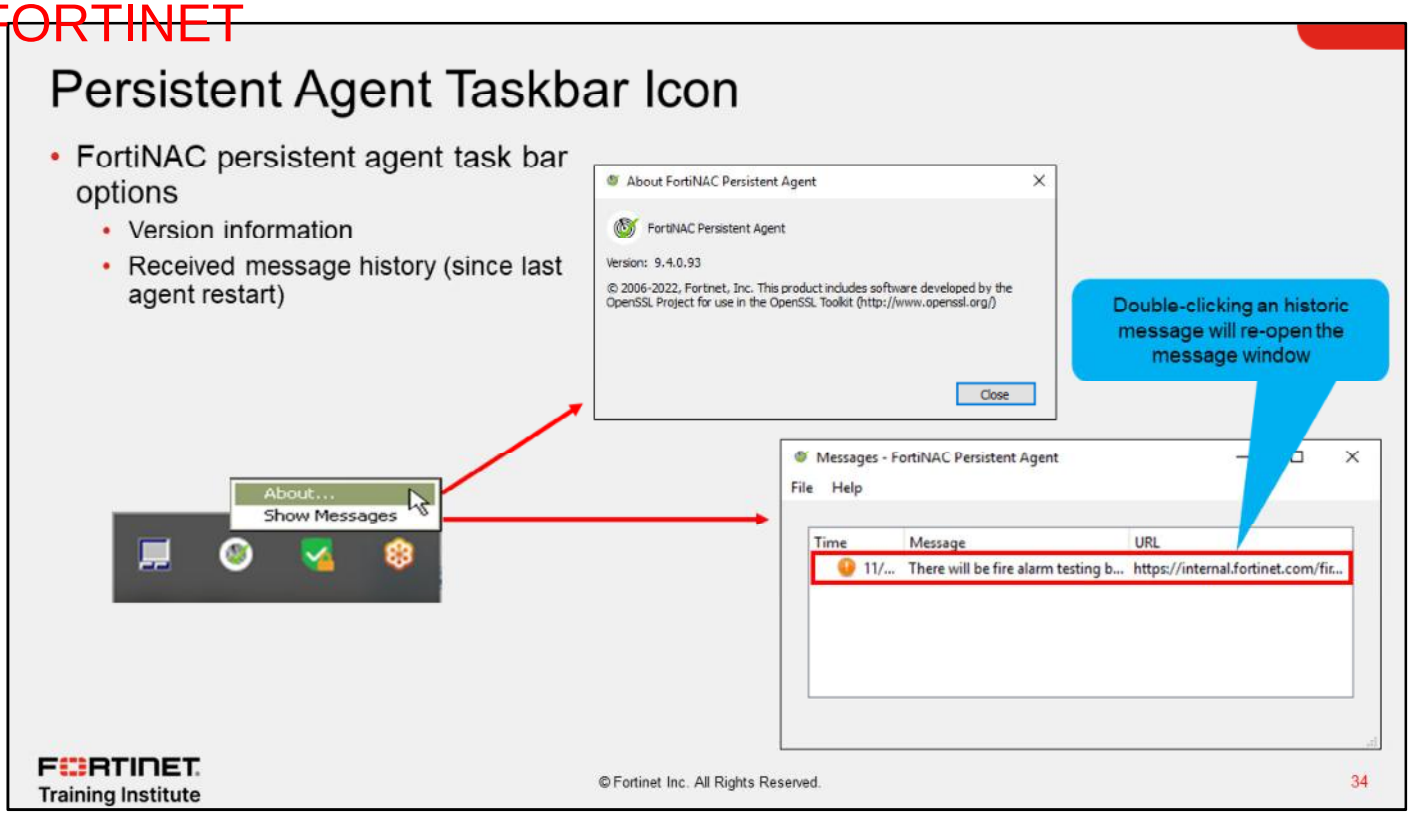
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After a message is sent, it will appear on the desktop of the targeted host or hosts. If a URL was included as part of the message, it will appear as a link that can be clicked by the end user.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can configure the FortiNAC persistent agent icon to be displayed on the taskbar of a Windows host, or hidden. When displayed, the icon is a small circle with a green check mark.

End users can right-click the icon and view detailed agent version information by selecting **About**. The **Show Messages** option will display a **Messages** window with all messages received by the agent since the last time it was restarted. You can double-click any message in the list to open the message pop-up that was received.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Mobile Agent

- Available for Android through the Android Marketplace
  - Check for rooted devices
  - Application inventory
  - Registration
- Android configuration
  - DNS must be supplied by FortiNAC (captive portal)
  - Requires an SSL certificate for portal communication



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

35

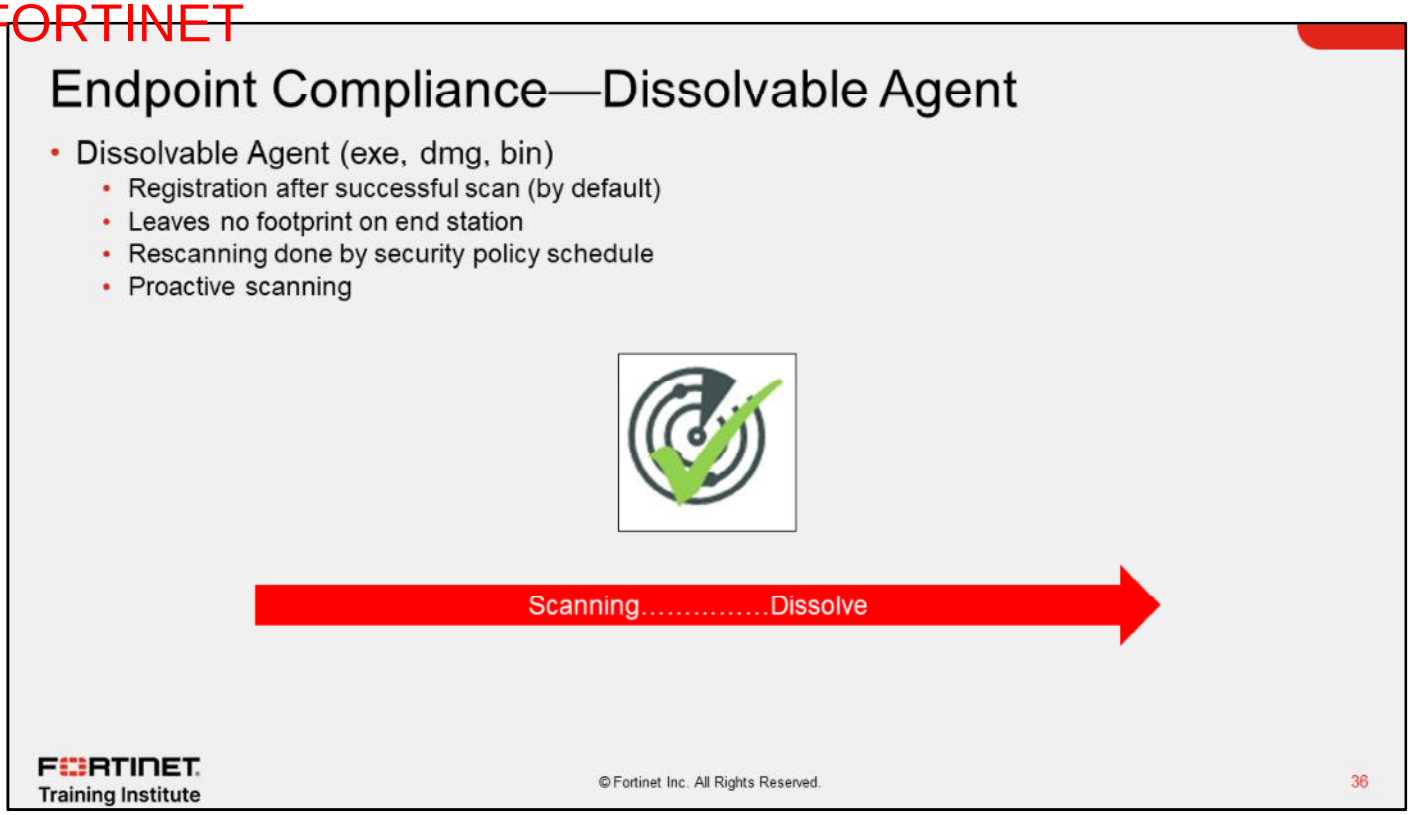
The mobile agent is for Android devices only, and provides the following functionality:

- The ability to detect if a device has been rooted
- The retrieval of an application inventory
- Device registration

You should deploy the mobile agent within the captive portal environment. Configuration settings are supplied by FortiNAC, and FortiNAC must be the DNS server during installation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The dissolvable agent is an agent that runs only once and then removes itself upon scan completion. This is used as part of the onboarding process—the default behaviour of the dissolvable agent is to register the host after a successful scan. The dissolvable agent option is a popular choice when it comes to onboarding guests, contractors, and BYOD devices.

The agent is deployed through the captive portal page in the registration network during onboarding, and through the quarantine captive portal page during scheduled rescans of previously onboarded hosts.

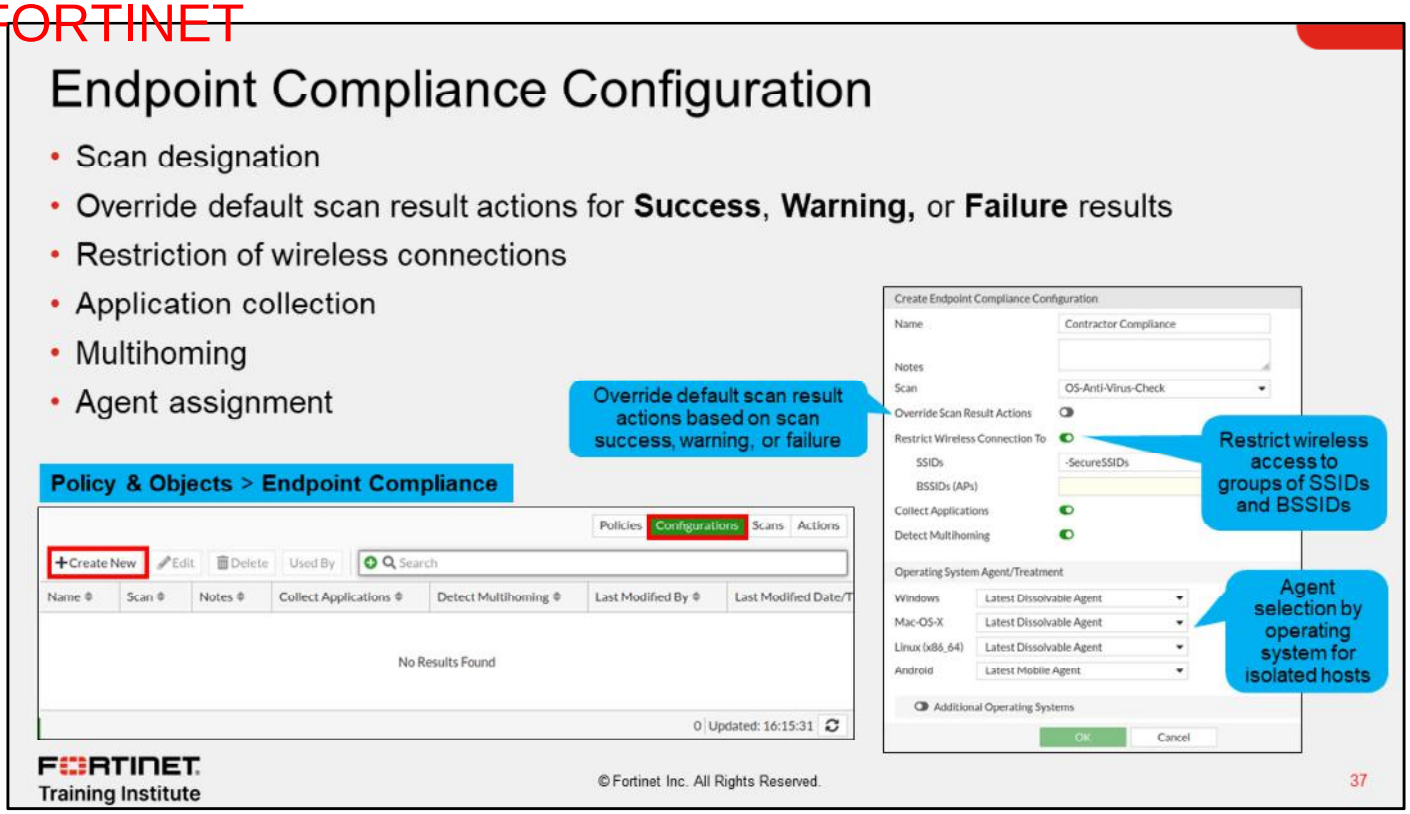
The agent runs on the endpoint, gathers the host information and scan result details, and returns them to FortiNAC.

Because the dissolvable agent does not stay resident on the endpoint, rescans are performed by changing the host state to at-risk and moving the host to the quarantine isolation network. There, the remediation page will give the user the ability to download and run the agent.

As a best practice for performing rescans with dissolvable agents, schedule them to occur during off hours, so that the isolation of the host does not happen while the host is in use. Another available option for dissolvable agent rescanning, which will be covered later in this section, is called proactive scanning.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

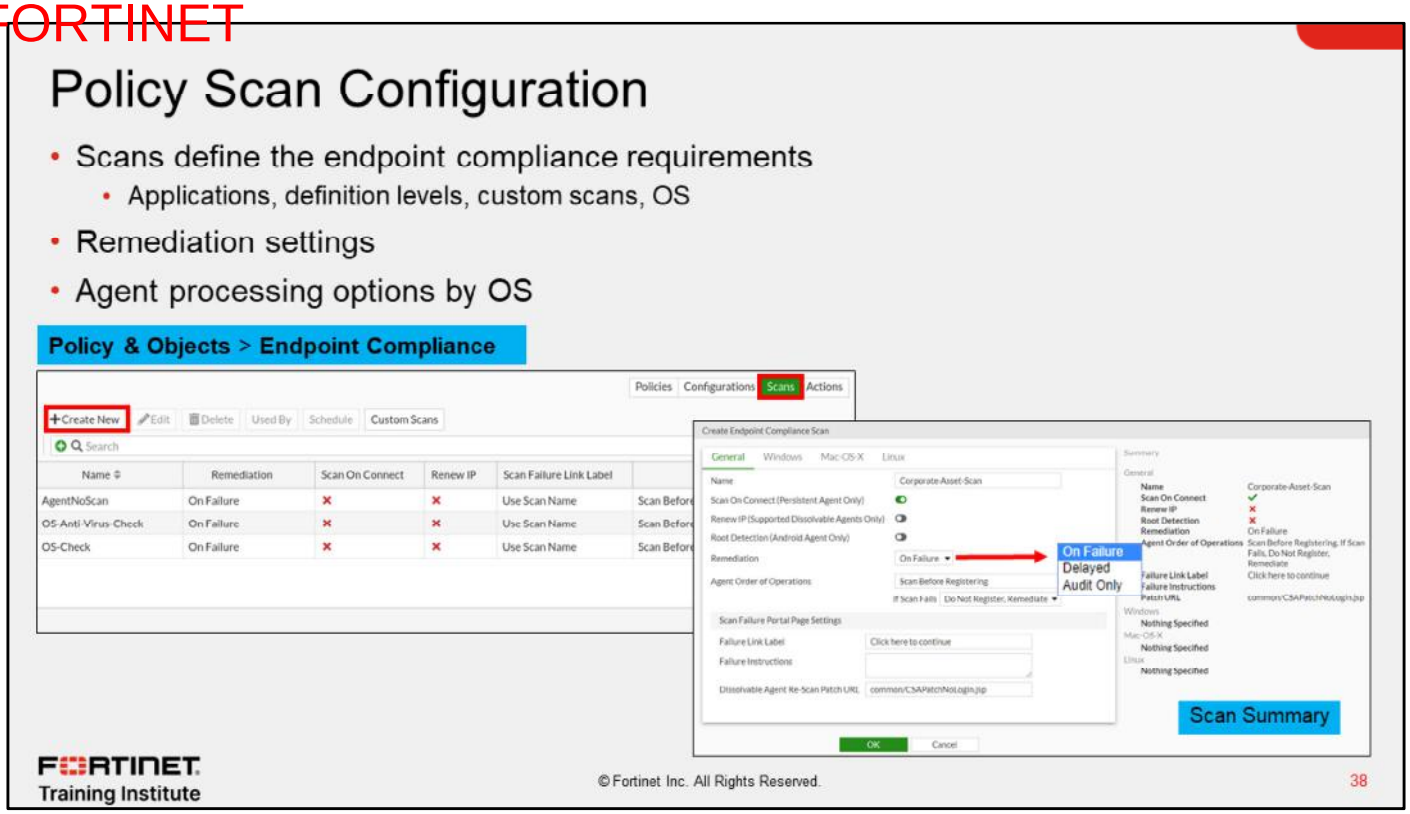


An effective way to maintain a secure environment is to validate endpoint security compliance. You can use FortiNAC agent technology to evaluate endpoints, both before and after they are granted access. When a host is targeted to be evaluated for endpoint compliance, you define the scan they must comply with and the agent they must use in the endpoint compliance configuration.

The inherent policy granularity provided by the user/host profiles allows you to specifically define the compliance requirements for different hosts or users. For example, guests may be targeted for a relatively simple compliance scan, such as having any detectable antivirus software installed. You typically won't have as much control over what is installed on a guest system, and the access provided to guest accounts will not normally include access to secure networks. Contractors and employees however may have access to secure systems and you will want to require more specific compliance requirements, such as a corporate issued antivirus, or validated domain credentials.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



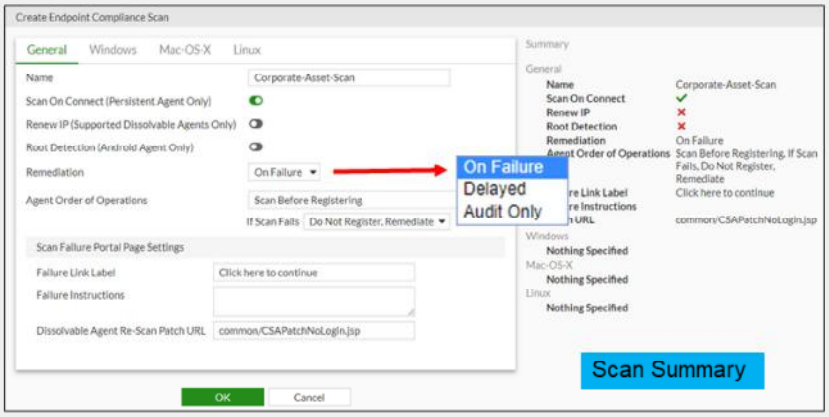
The scan component of an endpoint compliance policy is where you define the criteria necessary for scan success, how hosts should be directed upon a failure, and any agent-specific options. FortiNAC provides some preconfigured scans by default.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scan Creation

- Define agent behavior
  - Scan on Connect
  - Renew IP
  - Root Detection
- Configure when to remediate
  - On Failure
  - Delayed
  - Audit Only
- Configure portal settings for failed hosts



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

39

During scan creation you define agent specific settings. For example, you may want every corporate endpoint to validate compliance each time it connects to the network. This will help validate that an endpoint has not been compromised in the time is was not connected to the network. This can be performed only by endpoints with the persistent agent installed. In some situations, an automatic release and renew of an endpoint IP address can make a VLAN change more transparent to the end user, and root detection on Android devices can keep possibly compromised devices from being provided access.

You can also define how a host will be treated when a scan is failed. For example, a failed host can be immediately quarantined on failure, or given a defined period of time to be allowed on the network before being isolated, this could be to allow for host updates to be applied. A remediation audit will not isolate a host for scan failure, but is a means to gather host information which could be used for reports or for scan testing.

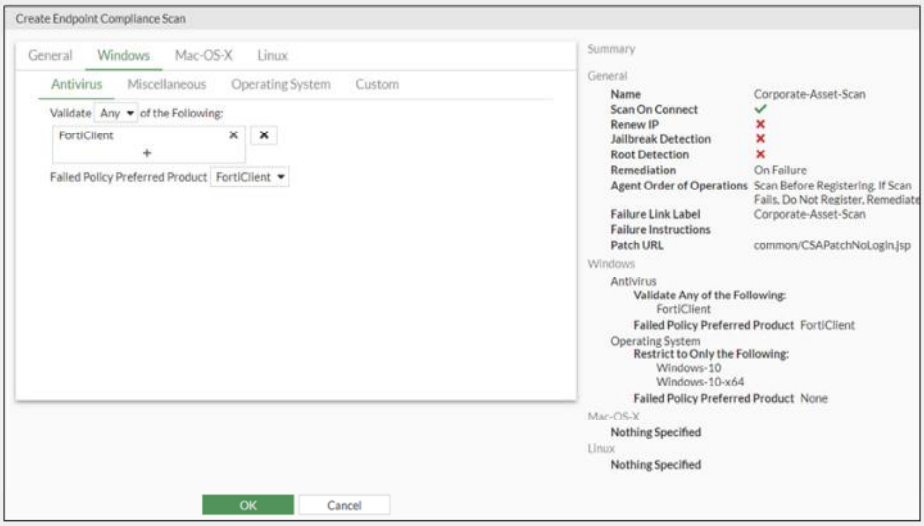
Portal page customizations can be used to improve the end user experience while in the remediation portal. In the example shown on this slide, the URL text presented will be **`Click here to continue,`** instead of a less user-friendly default hyperlink.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scan Criteria

- Scan selections for
  - Windows
  - Mac-OS-X
  - Linux
- Requirement categories by operating system
  - Antivirus (all)
  - Miscellaneous (Windows, Mac-OS-X)
  - Operating System (Windows, Mac-OS-X)
  - Custom (all)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

40

You select all of the policy requirements, category by category, for hosts based on OS. The available categories are operating system-dependant. Windows and Mac-OS-X have the following categories:

- **Antivirus**
- **Miscellaneous**
- **Operating System**
- **Custom**

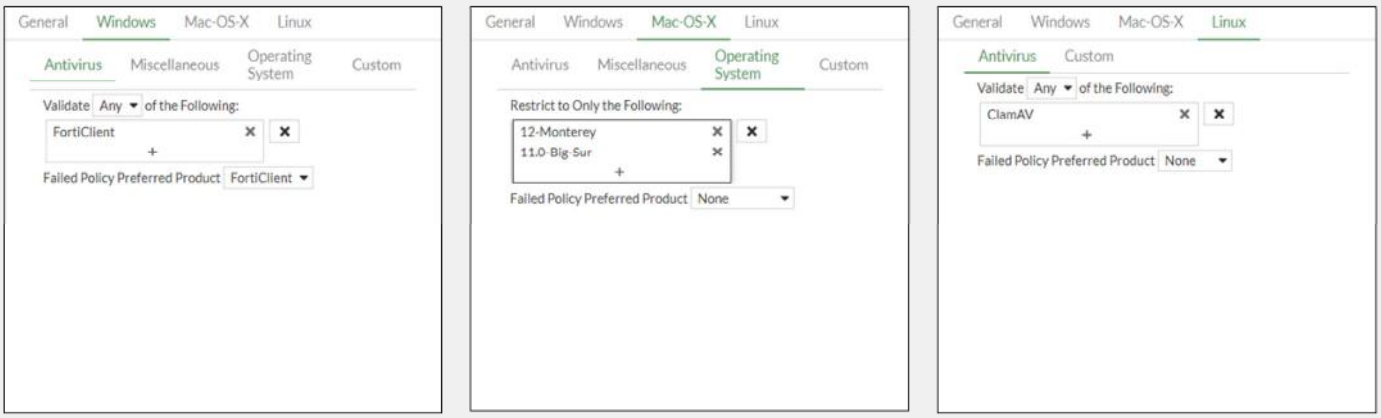
Linux operating systems have only **Antivirus** and **Custom** requirement categories.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scan Requirements for Endpoint Compliance

- Scan requirements are selected by operating system and category
- Some requirement categories have the option to require any of the selections or all of the selections



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

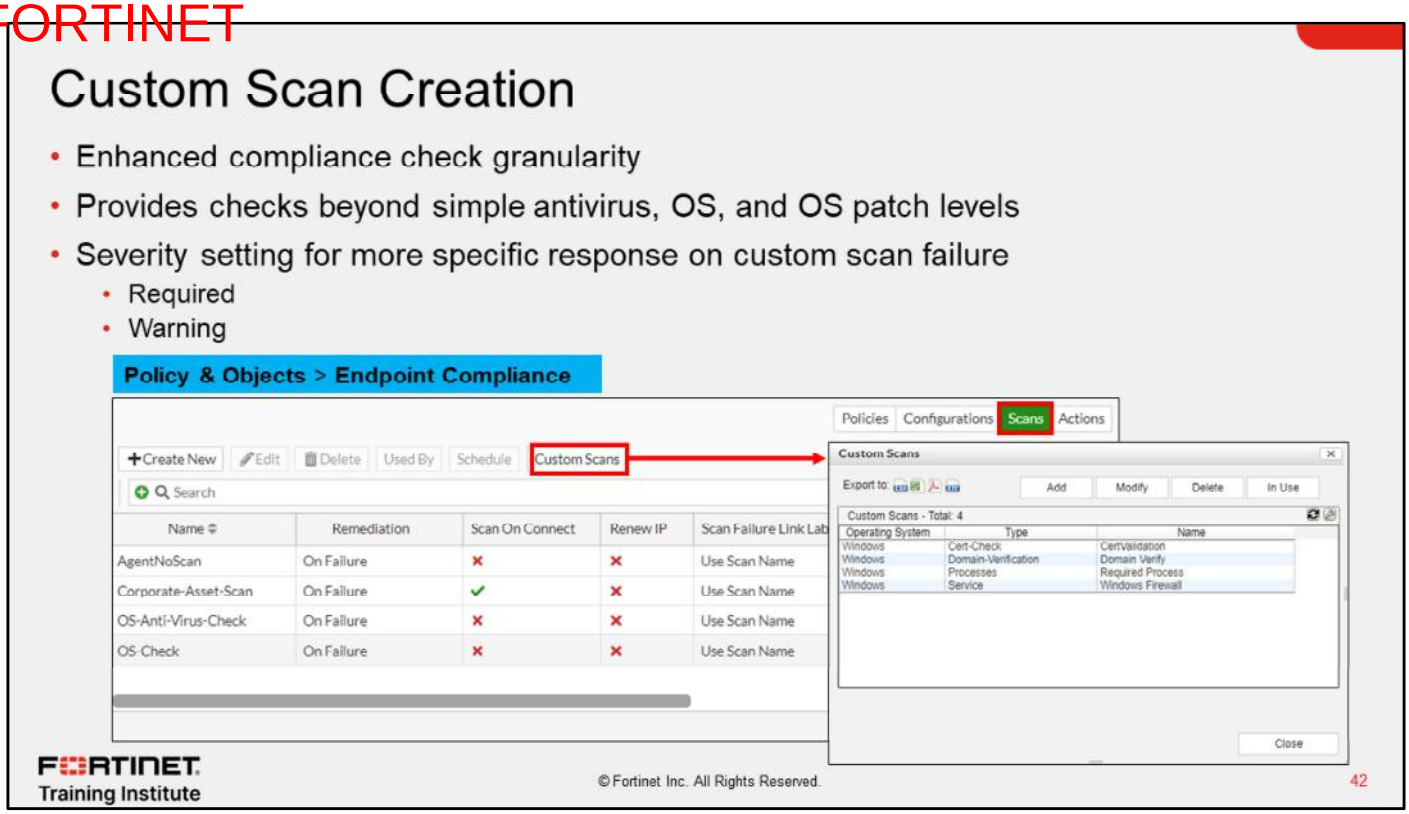
41

The **Antivirus** and **Miscellaneous** categories display all supported applications. You can apply logic to require **Any** or **All** of the applications selected from the list. Note that **Any** is the default setting, which you should use except in extremely rare situations. When you select one or more antivirus applications, the **Preferred** drop-down list will display each of the selected options. The preferred application will be the only displayed application on the remediation page if a host fails for all selected applications.

The **Operating System** category is where you create a list of all allowed operating systems. Matching any OS in the list will satisfy the requirement.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

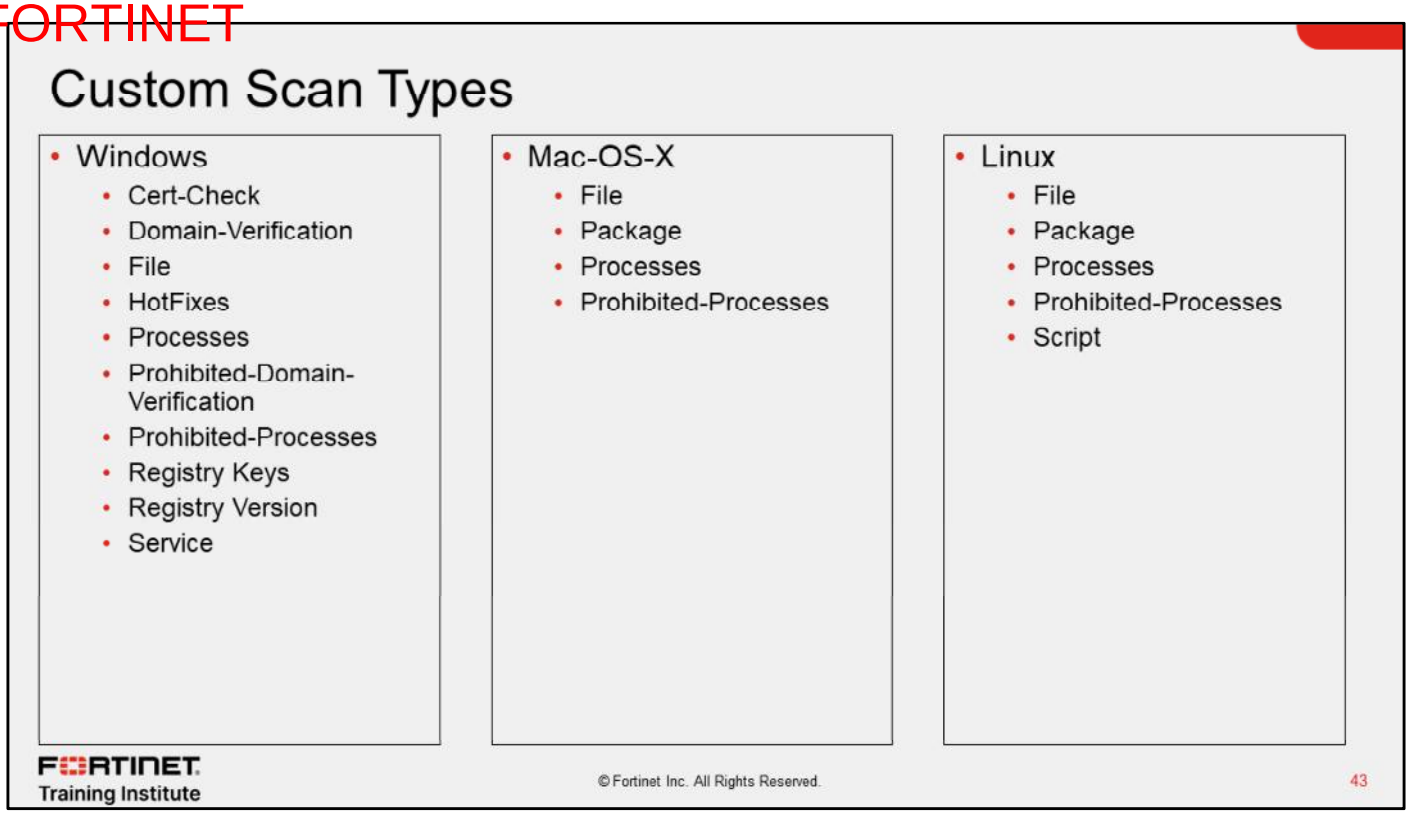


When creating policy scans for endpoint compliance validation, you can create optional custom scans. You can use custom scans within the actual policy scan configurations, allowing for specific OS-based criteria for Windows, Mac OS X, and Linux systems.

You can create custom scans using the **Custom Scans** button on the **Scans** tab on the **Endpoint Compliance** window. There are no default custom scans.

Vouchers & Dumps are Available | WhatsApp +201224560923

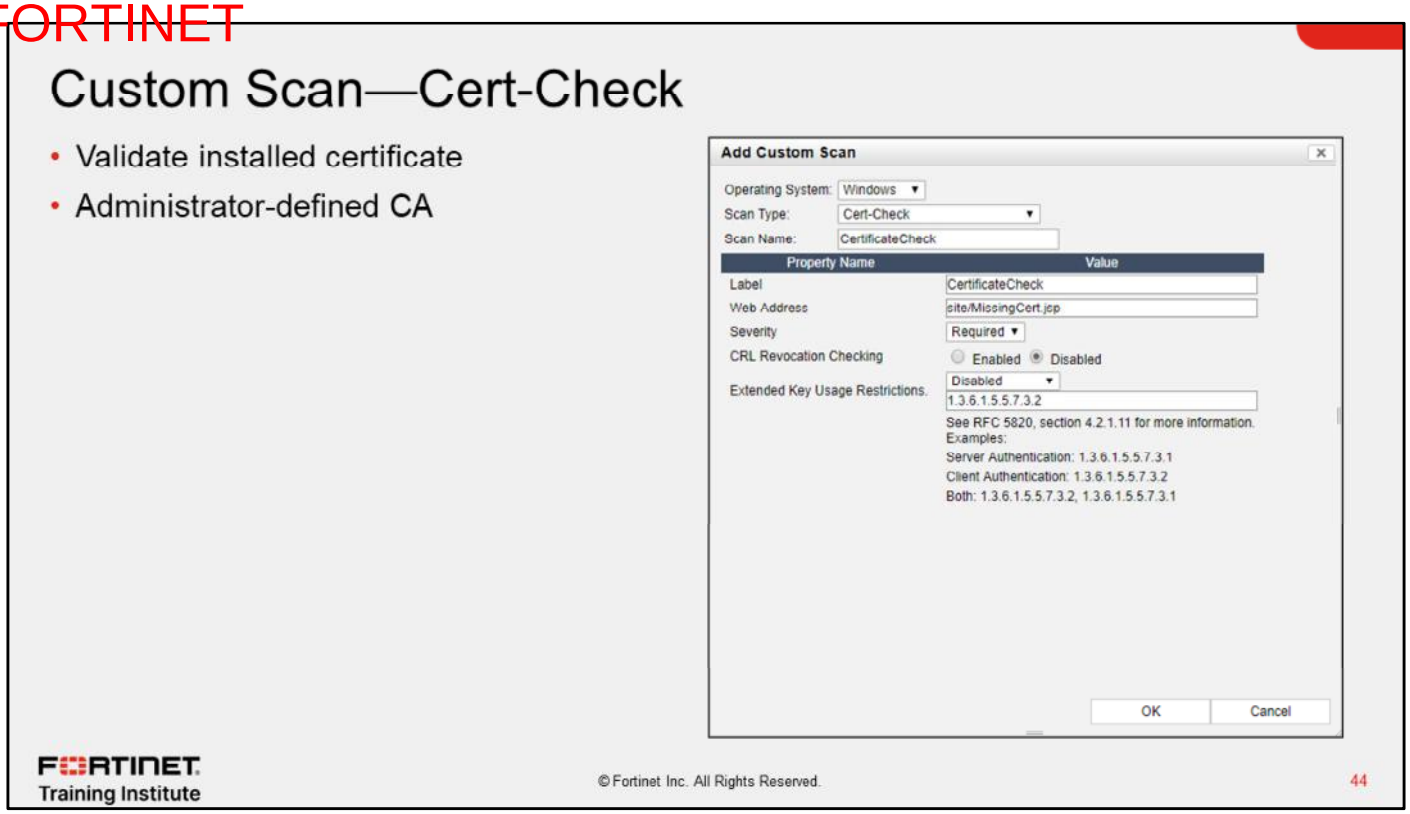
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide presents all of the different custom scan options, listed by operating system. This lesson covers some of the most common custom scans. You can find details about all custom scans in the *FortiNAC Administrator's Guide*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



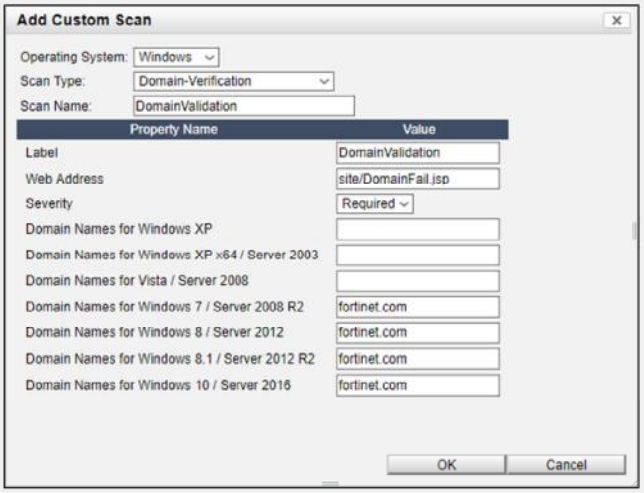
The need to validate hosts often goes beyond antivirus and OS patch validation. Custom scans provide a means for you to validate a more specific set of criteria. For example, validation that a certificate signed by a specific CA is installed in the certificate store of the host. You can leverage this to validate trusted end stations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Custom Scan—Domain-Verification

- Verify joined domain
- Add NetBIOS domain names by OS



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

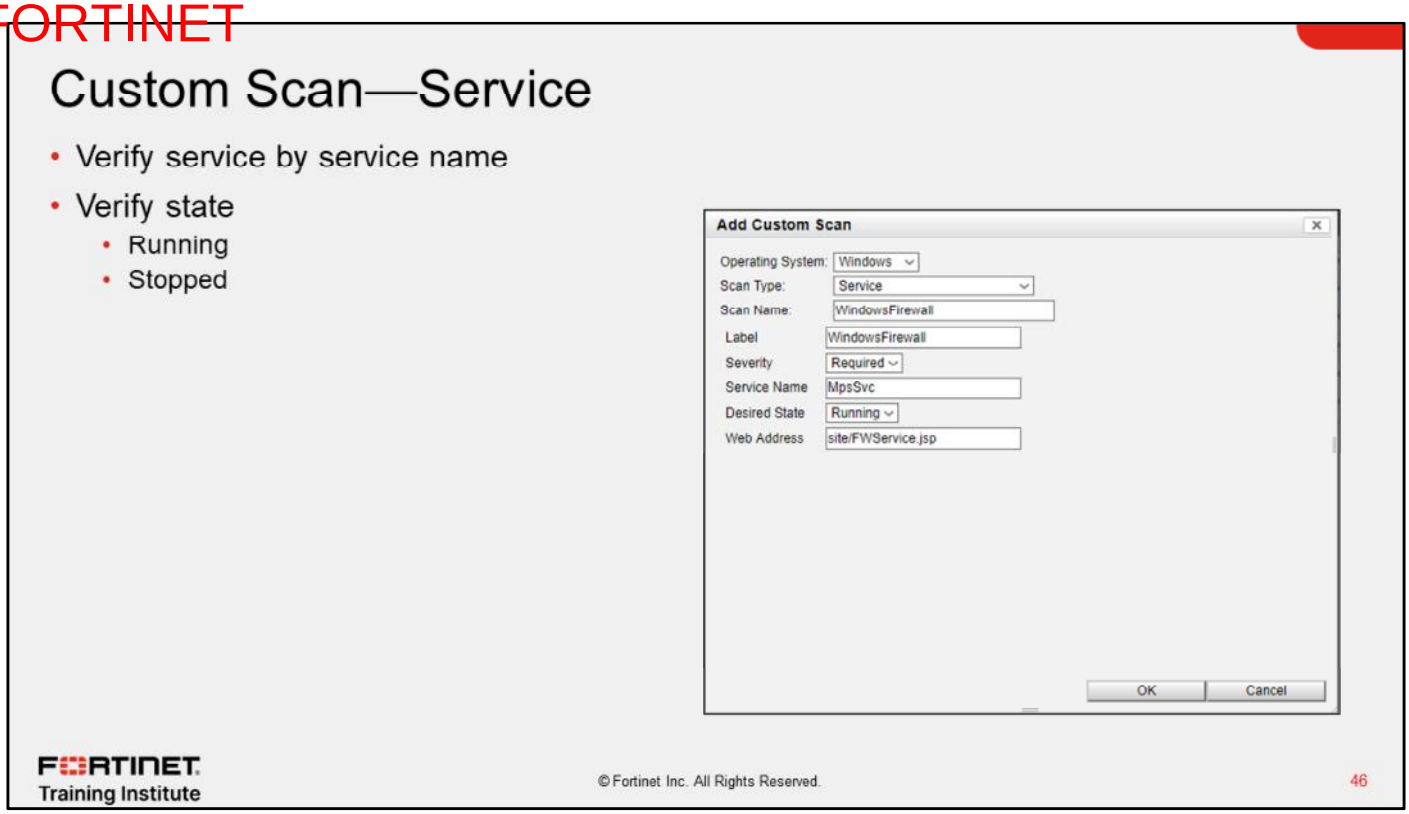
45

The **Domain-Verification** custom scan verifies that the host joined the appropriate domain when it connected to the network.

Enter a comma-separated list of the NetBIOS domain names that are required or permitted for the specific operating system(s).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



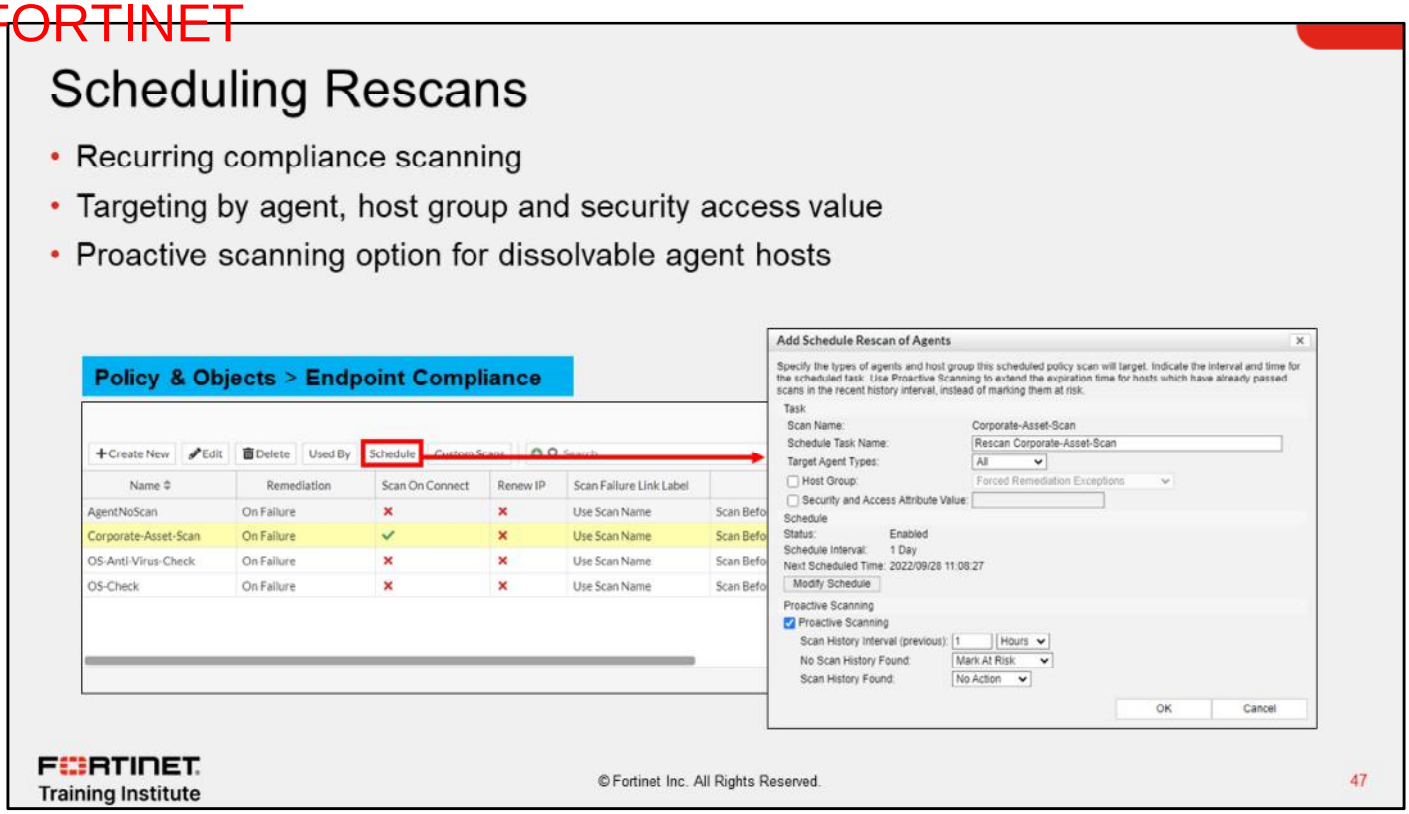
The **Service** custom scan checks for the current state of a service. You specify the service by name and the desired state of that service, either running or stopped. Hosts will fail the scan if the service is not found, or the desired state does not match.

This adds an additional layer of endpoint security, with the ability to prevent hosts access if a service, such as a Windows firewall, was disabled or has failed.

The custom scans for Mac OS X and Linux work in the same way as those for Windows, but with OS-specific options.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The evaluation of hosts for policy compliance, beyond the initial validation during onboarding, is scheduled on the **Scan** view using the **Schedule** button. Select the scan you want to schedule from the list, and then click the **Schedule** button. The scheduled tasks window for the selected scan will open.

The hosts to be rescanned can be defined by **Target Agent Type** (Dissolvable or Persistent), **Host Group**, and **Security and Access Attribute Value**.

For hosts that use the dissolvable agent, you can enable **Proactive Scanning**. This option allows hosts that scan within a user-defined period, before the scheduled date and time, to avoid being provisioned to the quarantine isolation network.

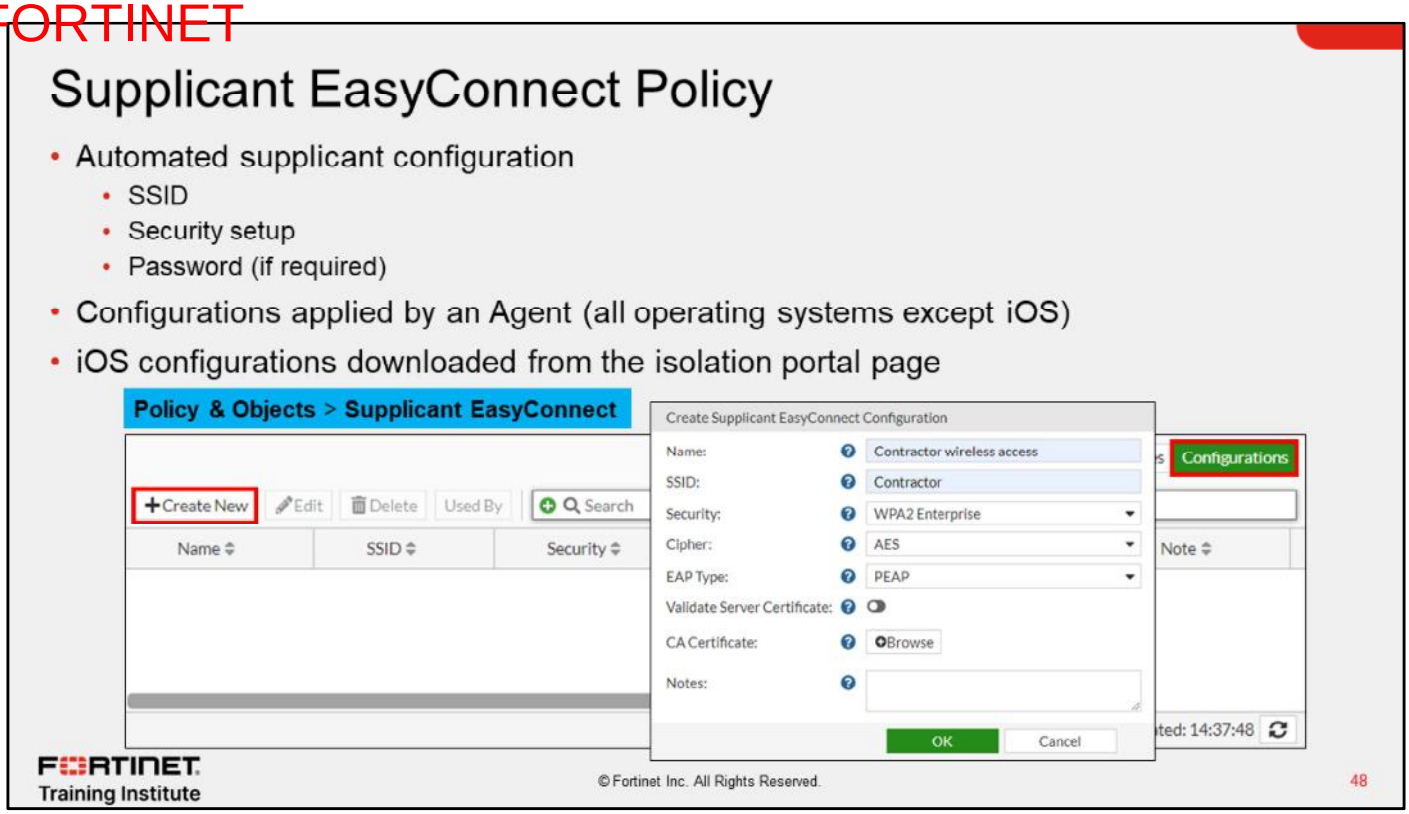
The **Proactive Scanning** settings allow you to designate a **Scan History Interval** that defines the leeway given to a host whose scheduled rescan time has arrived. For example, you could exempt a host from the scheduled rescan, if that host had successfully scanned at any point in the last two days.

If there has been no successful scan performed during the designated **Scan History Interval**, the host will be marked at risk and, if enforcement is enabled, moved to the quarantine isolation network and presented with the `common/CSAPatchNoLogin.jsp` remediation page. Another option available is to expire the host, deleting it from the database.

If a successful scan has been performed during the designated **Scan History Interval**, the host, by default, will have no action taken on it. Another option is to extend the expiration date of the host by **Hours**, **Days**, or **Weeks**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



As you learned earlier, each type of policy is created in the same way. The example on this slide shows the **Add Supplicant EasyConnect Policy** window and is almost exactly the same as the previous policy creation windows.

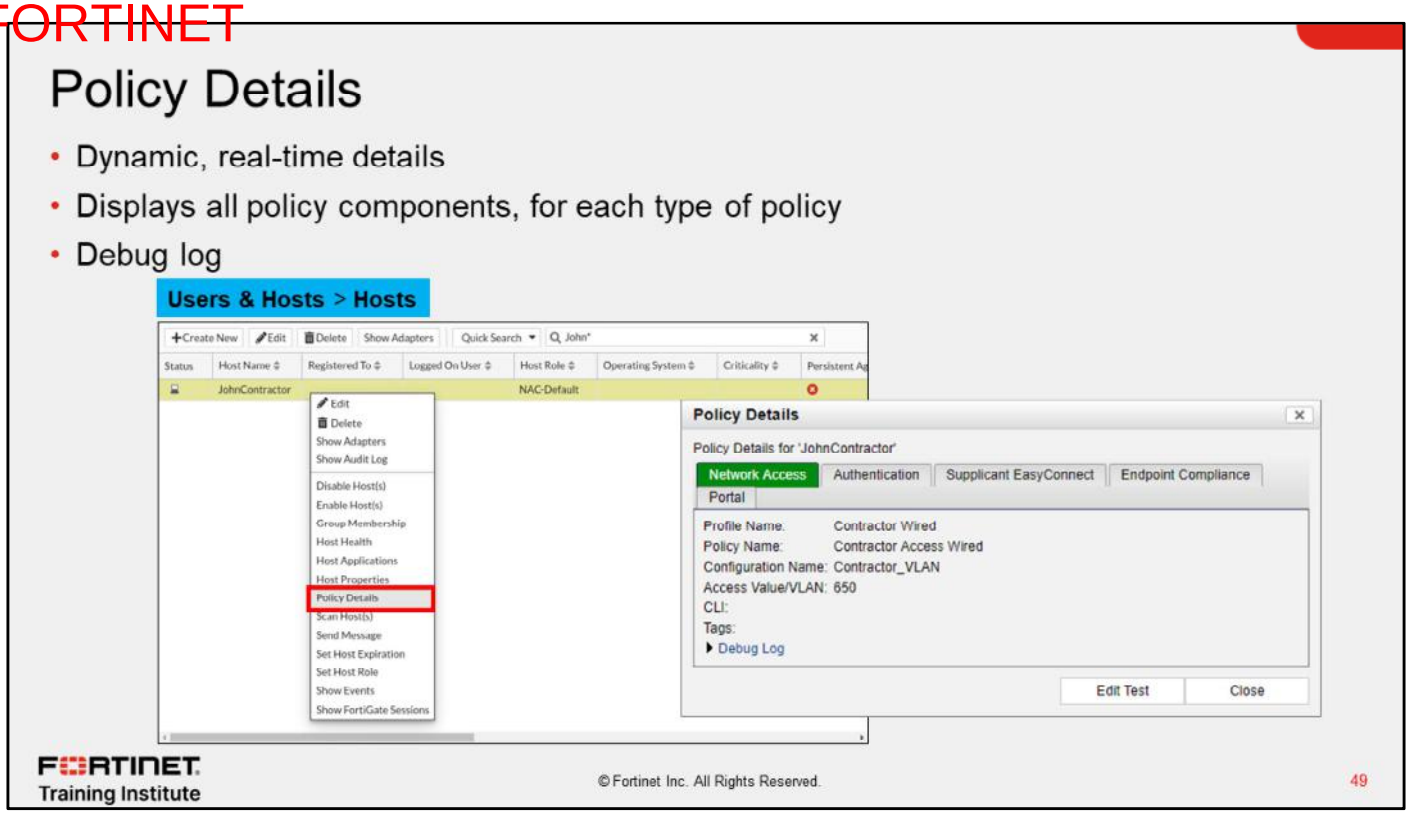
Supplicant EasyConnect policies can greatly simplify secure endpoint configuration processes for wireless networks. For example, a host onboarding through an open SSID could, after matching an EasyConnect policy, have its supplicant configured for access through a secure SSID.

For Windows and Mac OS X hosts, you must use an agent to create the configuration. Dissolvable agents must be version 3.0.2.8 or higher, and persistent agents must be version 3.1 or higher. Note that because an agent is used for these operating systems, there must be a matching endpoint compliance policy that, at a minimum, designates the agent to deploy by operating system. iOS devices do not use an agent for configuration. Instead they will be prompted to download the configuration from the captive portal.

The required security settings displayed will depend on the selected **Security** option, and will include **Password**, **Cipher**, **EAP Type**, **CA Certificate**, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Knowing which policies are being applied to a user or host at any given point in time, and why they are being applied, is essential to testing, troubleshooting, and validating any type of policy.

In the example shown on this slide, a host was located within the **Host View**, and the **Policy Details** window was accessed by right-clicking the host, and then selecting **Policy Details**.

The **Policy Details** window has a tab for each type of policy: **Network Access**, **Authentication**, **Supplicant EasyConnect**, **Endpoint Compliance**, and **Portal**. Each tab shows the **Profile Name** of the **User/Host Profile** being matched, the **Policy Name** of the policy being applied, the **Configuration Name** of the configuration attached to the policy, and any configuration settings that make up the configuration.

This information is dynamic and real time, updating as matched profiles change.

Each policy tab has a **Debug Log** branch located at the bottom of each policy detail. Expanding this branch displays detailed information about why the current policy is being applied at this moment.

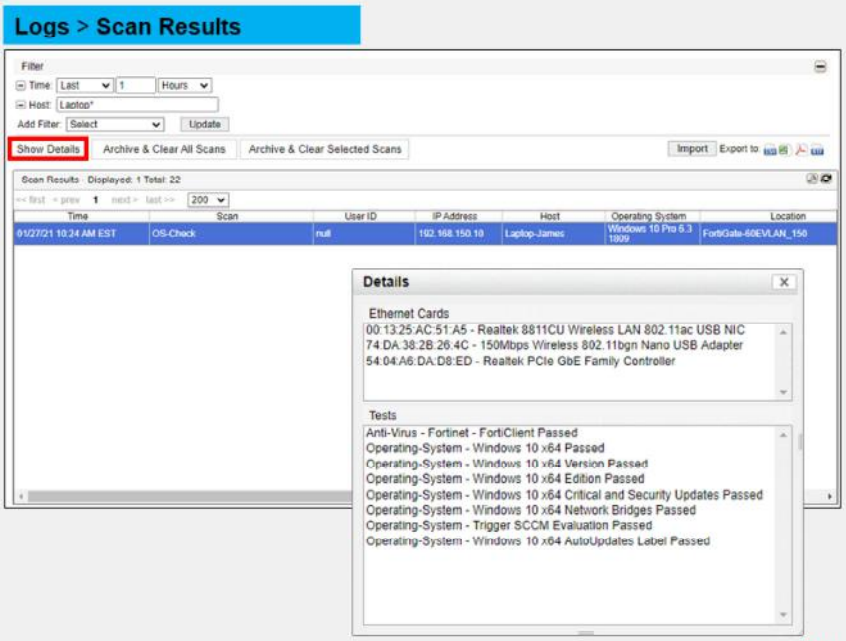
In the example shown on this slide, the details of the currently applied **Network Access** policy is displayed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Scan Results

- Global repository of scan results
- Filter tool for quick searches
- Detailed result data
- Ethernet cards detected by the scanning agent

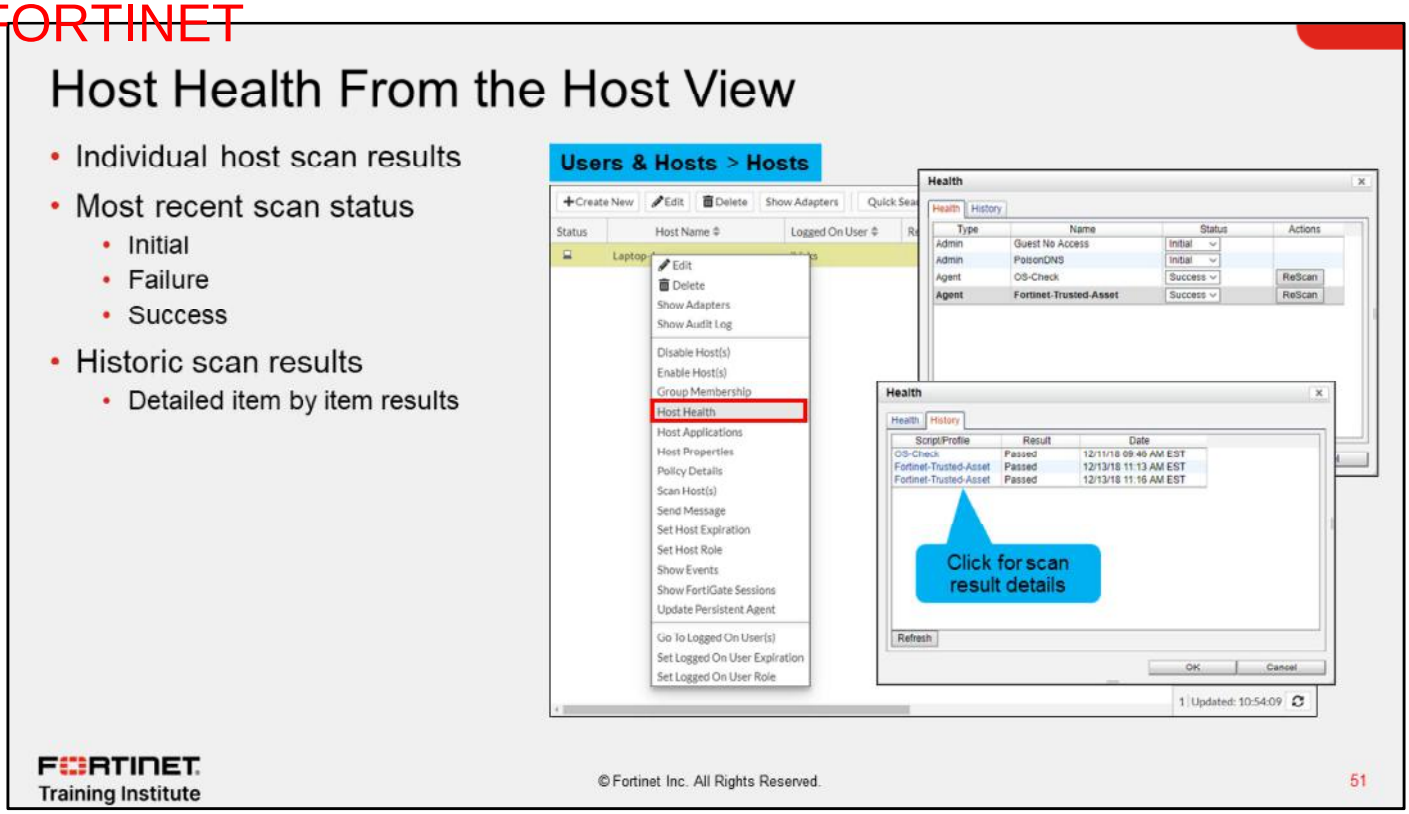


When hosts are scanned for policy compliance, detailed scan result information is obtained by FortiNAC and stored in the database. You can then retrieve and view this information from multiple views on the GUI.

Two buttons at the top of the view allow you to archive scan result information in the database and remove it from the view. This keeps a copy of the results available for import, if needed, while allowing the view to load more efficiently.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Another way to view scan results is to locate a host in the host view, then right-click the host, and then select **Host Health**.

The **Health** tab on the **Host Health** window displays the status of each endpoint compliance policy scan the host had to comply with, as well as all administrative scans. The **Status** field is assigned by FortiNAC based on the last scan result or, in the case of administrative scans, the last system or user assignment. You can manually assign this field, and the options are:

- **Initial**: The host has not been scanned. The host will not be marked *at risk*.
- **Failure**: The host has failed the scan requirements. The host state will be set to *at risk* for this scan.
- **Success**: The host has satisfied all scan requirements. The host will not be marked *at risk*.

The **History** tab displays past scan results and the date and time that the scan was performed. The **Script/Profile** column shows the scans by name. Each name is a link to the detailed scan results, as they were reported by the agent when the scan was performed. The details contain physical address information for each discovered interface, host and scan information, and a policy requirement component with pass or fail status.

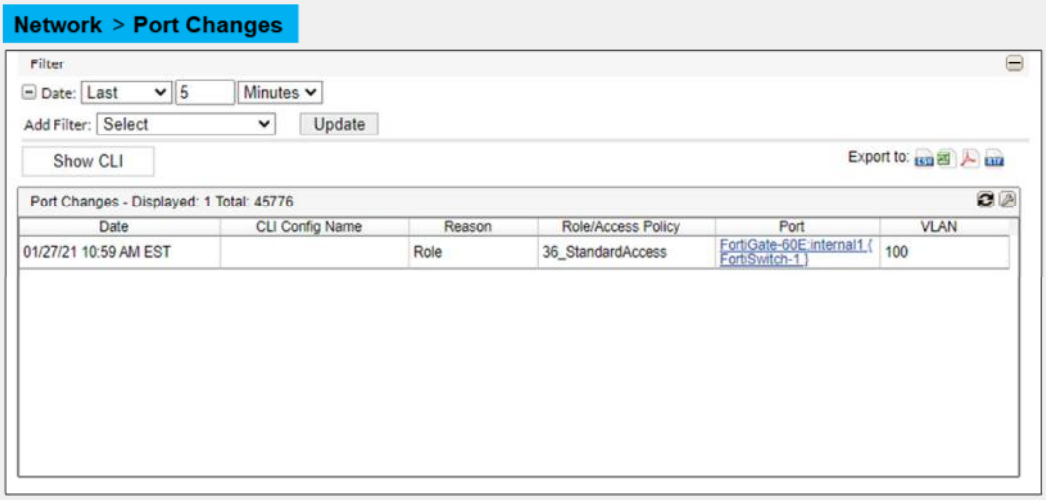
Recall that an additional way to view scan result information is through the **Health** tab within the host properties, as discussed in the *Network Visibility* lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Port Changes View

- Globally from **Network > Port Changes**
- From a port on the **Network > Inventory view**



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

52

Any time FortiNAC changes network access for an endpoint, the change is documented on the **Port Changes** view. This provides an administrator with valuable information when validating control configurations and enforcement.

A global list of port changes is available on **Network** > **Port Changes**. You can use a filter to locate specific port change events.

The view displays:

- The date and time a change was made
- Whether a CLI configuration was executed at the time of the change
- The reason the change was made
- The role or access policy that caused the change (only displayed if a role or access policy was the cause of the change)
- The port that was changed
- The VLAN the port was changed to

A **Port Changes** tab is also available from the **Network** > **Inventory** view, and the **Port Changes** option in the right-click menu of any port, shows the same information pre-filtered for the selected port

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which type of agent can you use to send messages to a host?
   - ✓ A. Persistent
   - B. Dissolvable
2. Which operating system does not use an agent to create a supplicant EasyConnect wireless configuration?
   - A. Android
   - ✓ B. iOS

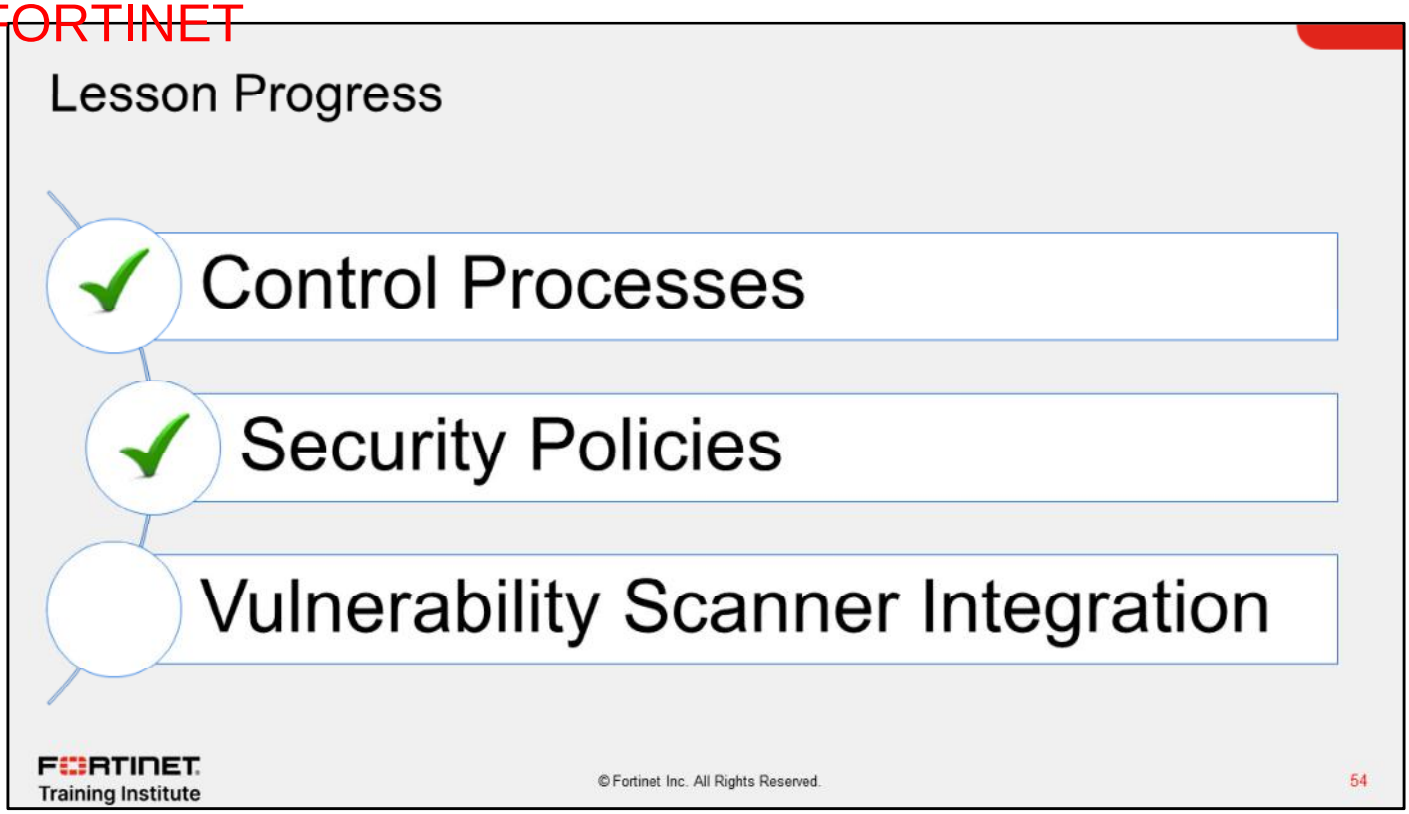
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

53

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

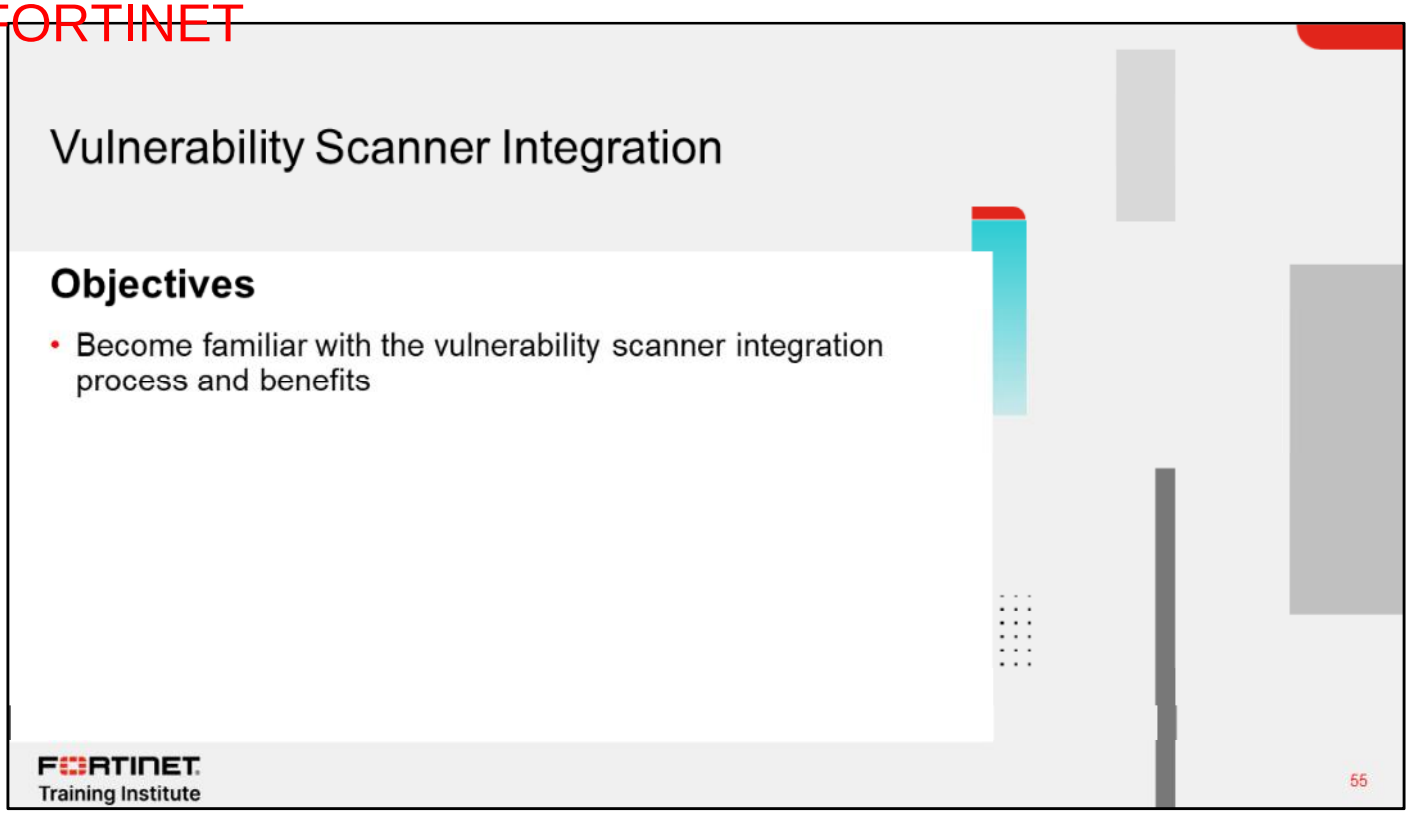


Good Job! You now understand vulnerability scanner integration.

Now, you will learn about FortiNAC control processes.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

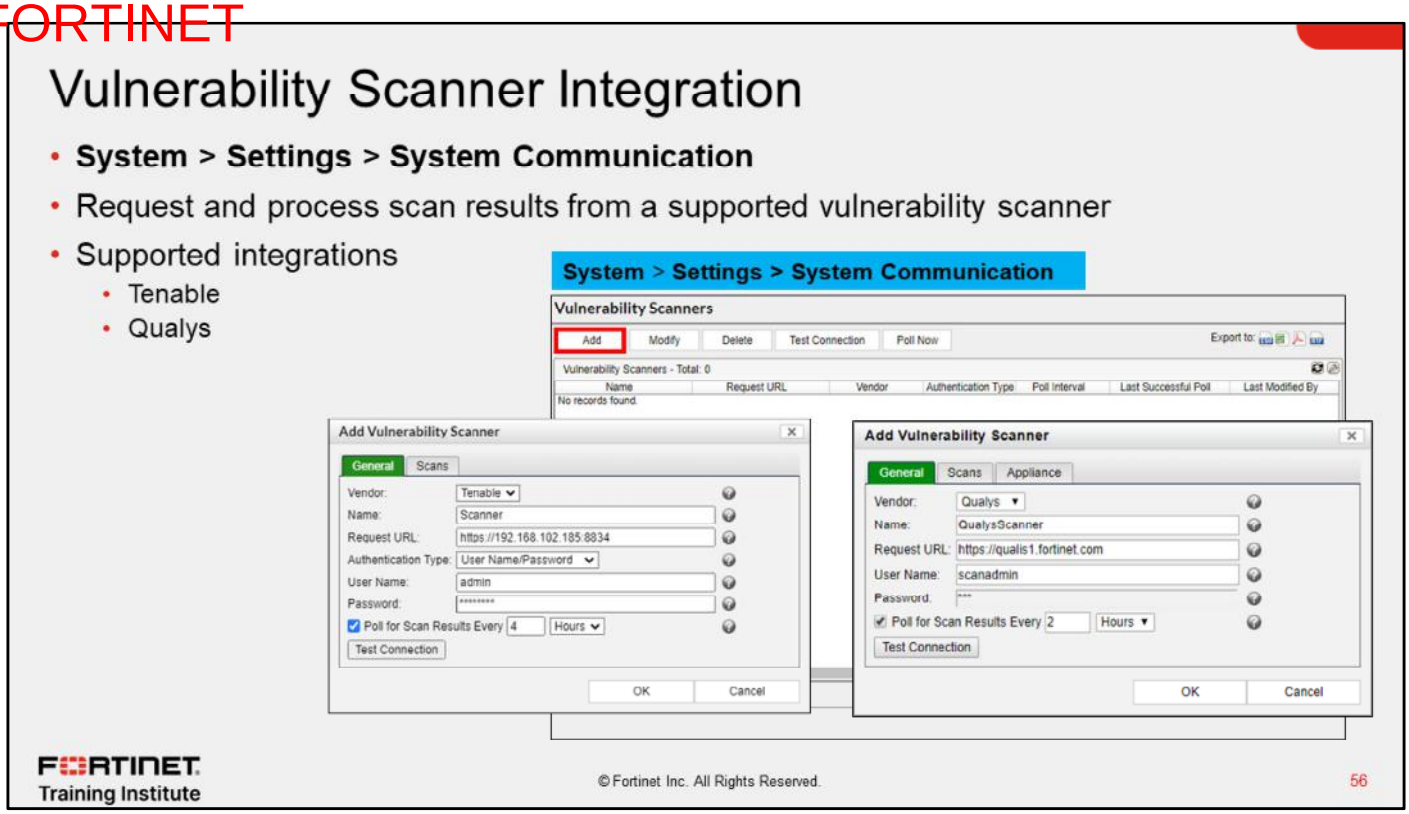


After completing this section you should be able to achieve the objective shown on this slide.

By demonstrating competence in integrating vulnerability scanners, you will be able to leverage existing Nessus and Qualys systems in your environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Integrating with vulnerability scanners enables FortiNAC to request and process scan results from the scanners.

The **Vulnerability Scanners** view displays a list of scanners that are configured, and allows you to add, modify, delete, and test a scanner connection, and configure polling for scanner results.

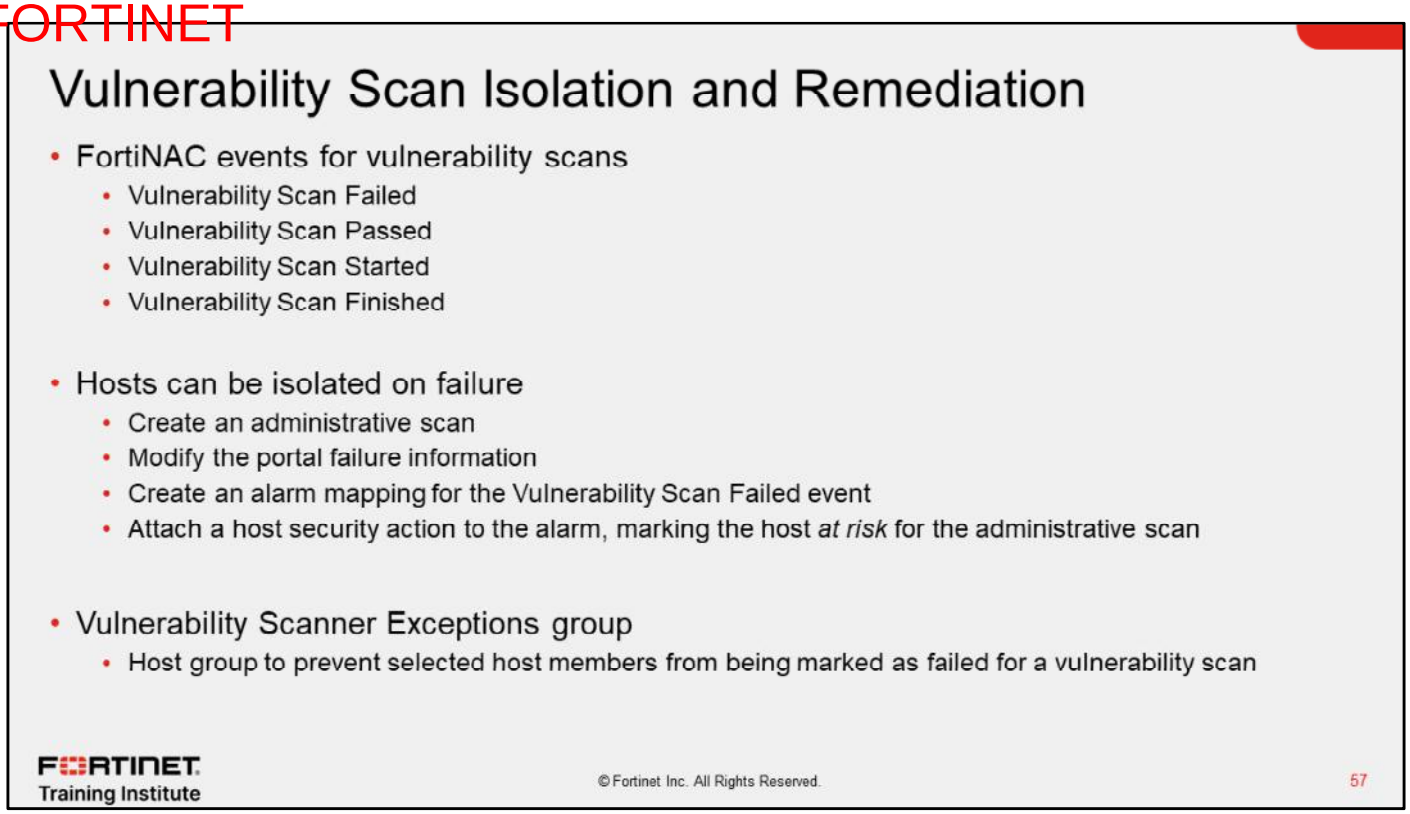
FortiNAC supports integration with Tenable (Nessus) servers and Qualys in-network scanner hosts.

Scan thresholds define a value that, when exceeded for any host, results in the host being identified as failing the scan, and triggers the creation of a **Vulnerability Scan Failed** event. If a host's results do not exceed a defined threshold, a **Vulnerability Scan Passed** event will be generated.

The **Vulnerability Scan Failed** and **Vulnerability Scan Passed** events will be used to move failed hosts in to, and out of, the quarantine isolation network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The quarantining of hosts as a result of an exceeded vulnerability scan result threshold works differently than when a host is marked at risk for failing a policy scan. Instead of the host automatically being marked *at risk* by FortiNAC, an administrative user must create an **Event to Alarm Mapping** for the **Vulnerability Scan Failed** event. Within the alarm mapping, you must designate a host security action to mark the host at risk. This process was described in an earlier lesson. Once a host is marked *at risk*, and enforcement for *at risk* hosts is being enforced, the host will be moved to the quarantine isolation network.

To customize the vulnerability scan information displayed on the **Remediation Portal** page, edit the content on the **Global** > **Failure Information** page in the **Portal Content Editor**.

The remediation portal page shows details for the vulnerability scan that failed. Users can click the scan to see details of the failed scan provided by the vulnerability scanner, and solutions to fix the vulnerability. After remediation, users click the **Rescan** button to rescan the host. To automate the process of returning an isolated host to a production network, as the result of a successful rescan, you will need to create a second **Event to Alarm Mapping** for the **Vulnerability Scan Passed** event.

Hosts that are members of the Vulnerability Scanner Exceptions host group will not generate the **Vulnerability Scan Failed** event.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which type of scan is used with a vulnerability scanner integration to isolate a non-compliant host?

✓A. Administrative

B. Custom

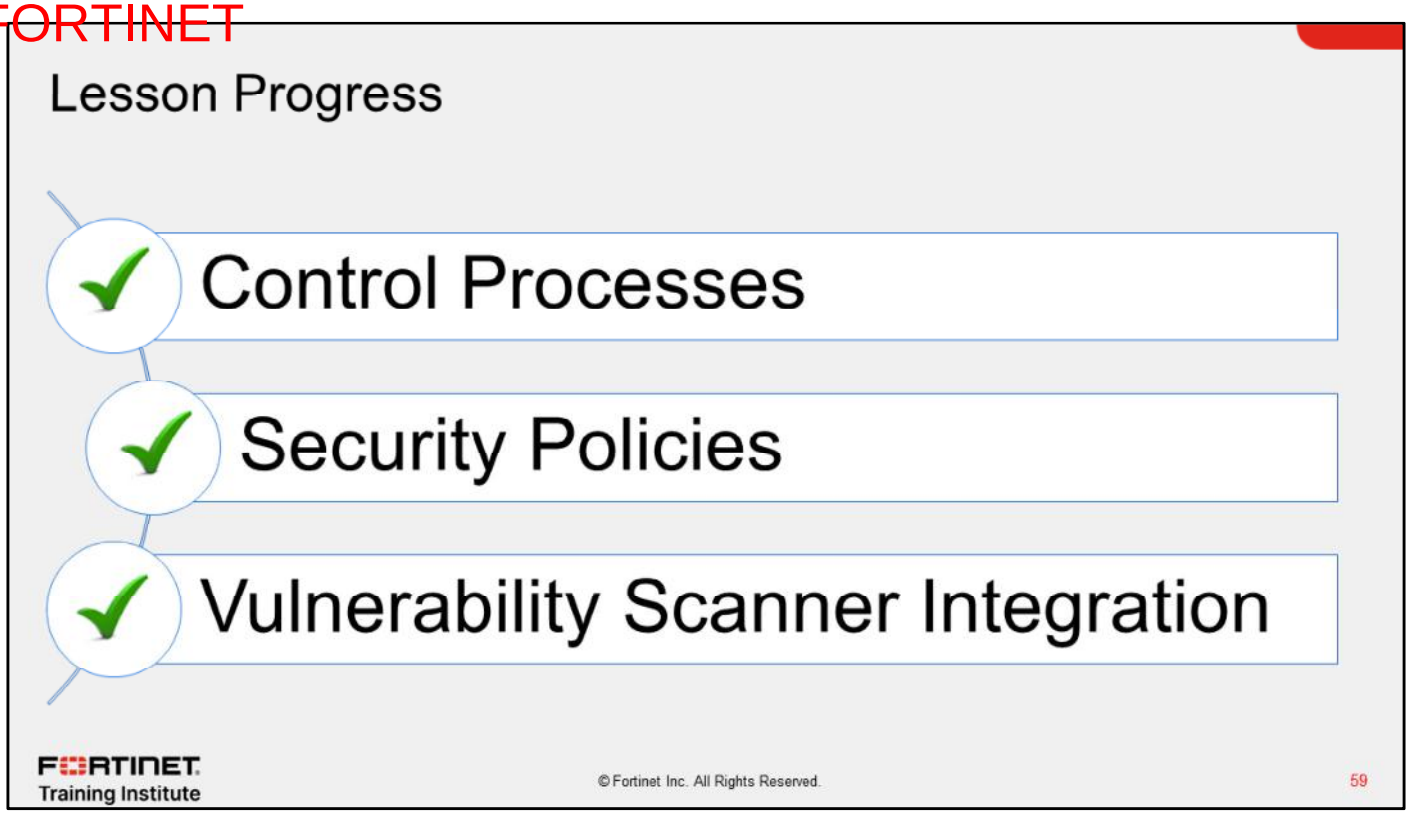
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

58

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

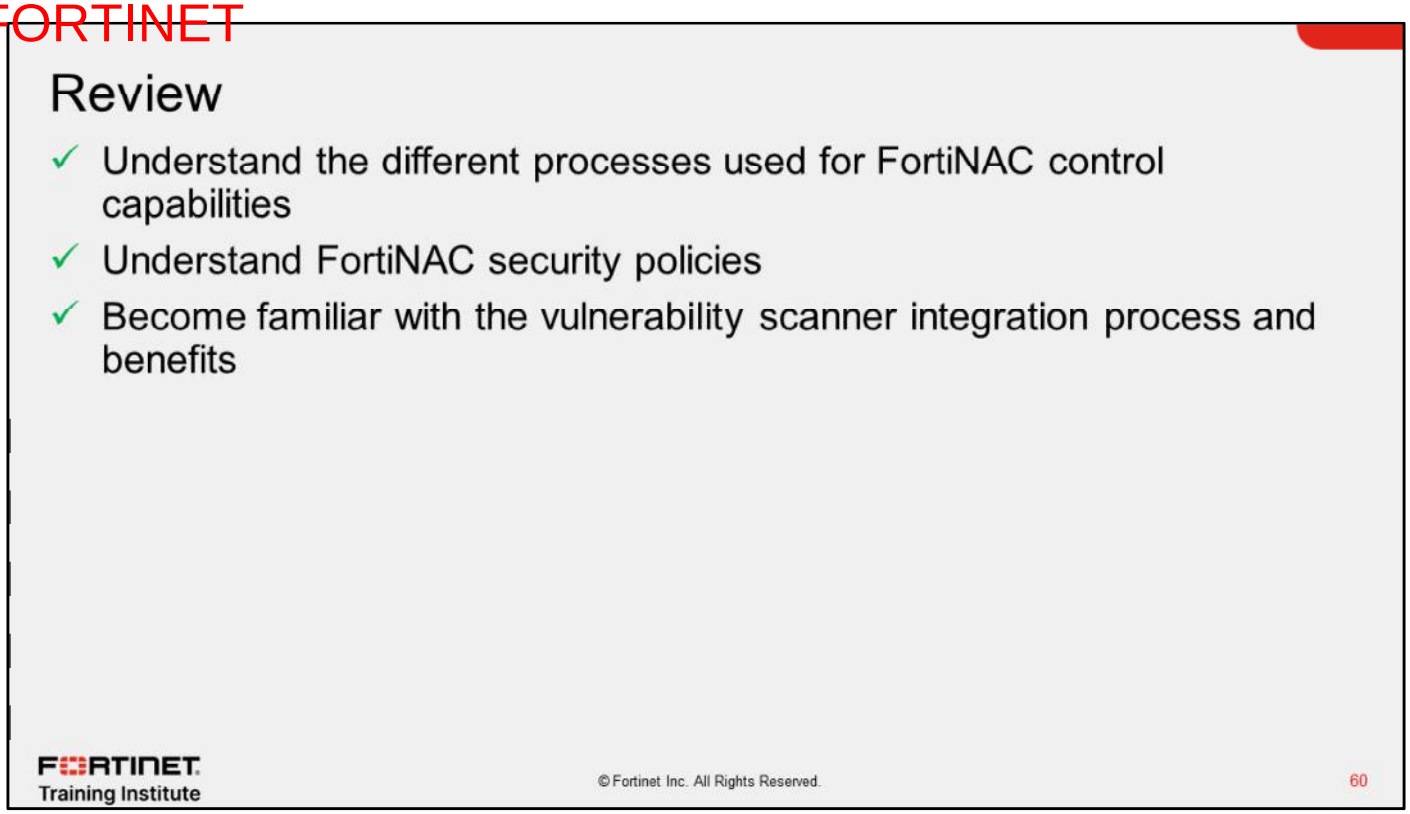


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

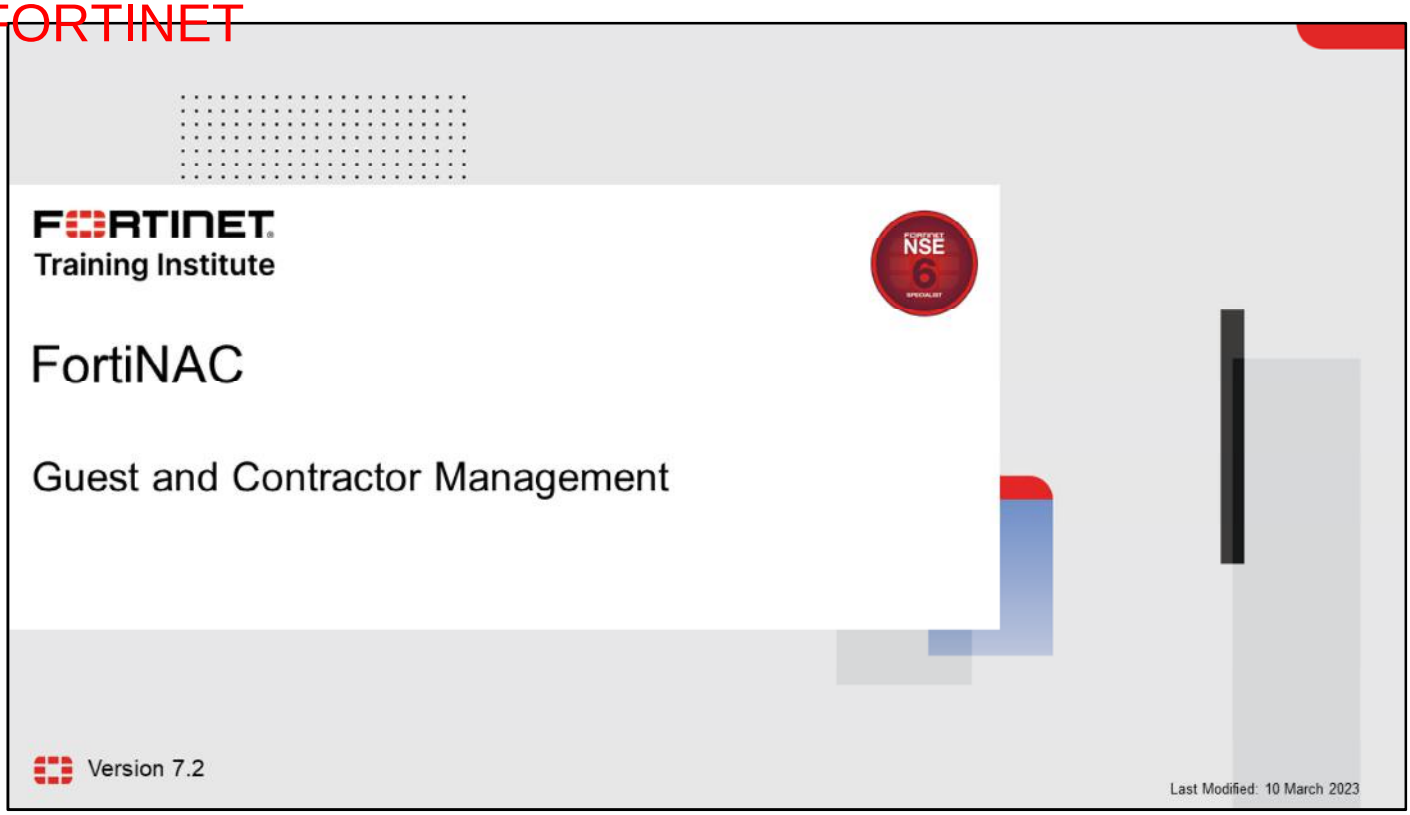


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about FortiNAC security policies. It is through security policies that FortiNAC provides customized onboarding options, simplified security configuration for wireless access, detailed network access provisioning, endpoint compliance validation, and customizable back-end authentication services.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiNAC guest and contractor management capabilities. The combination of visibility and control make FortiNAC the perfect solution for onboarding and managing BYOD devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

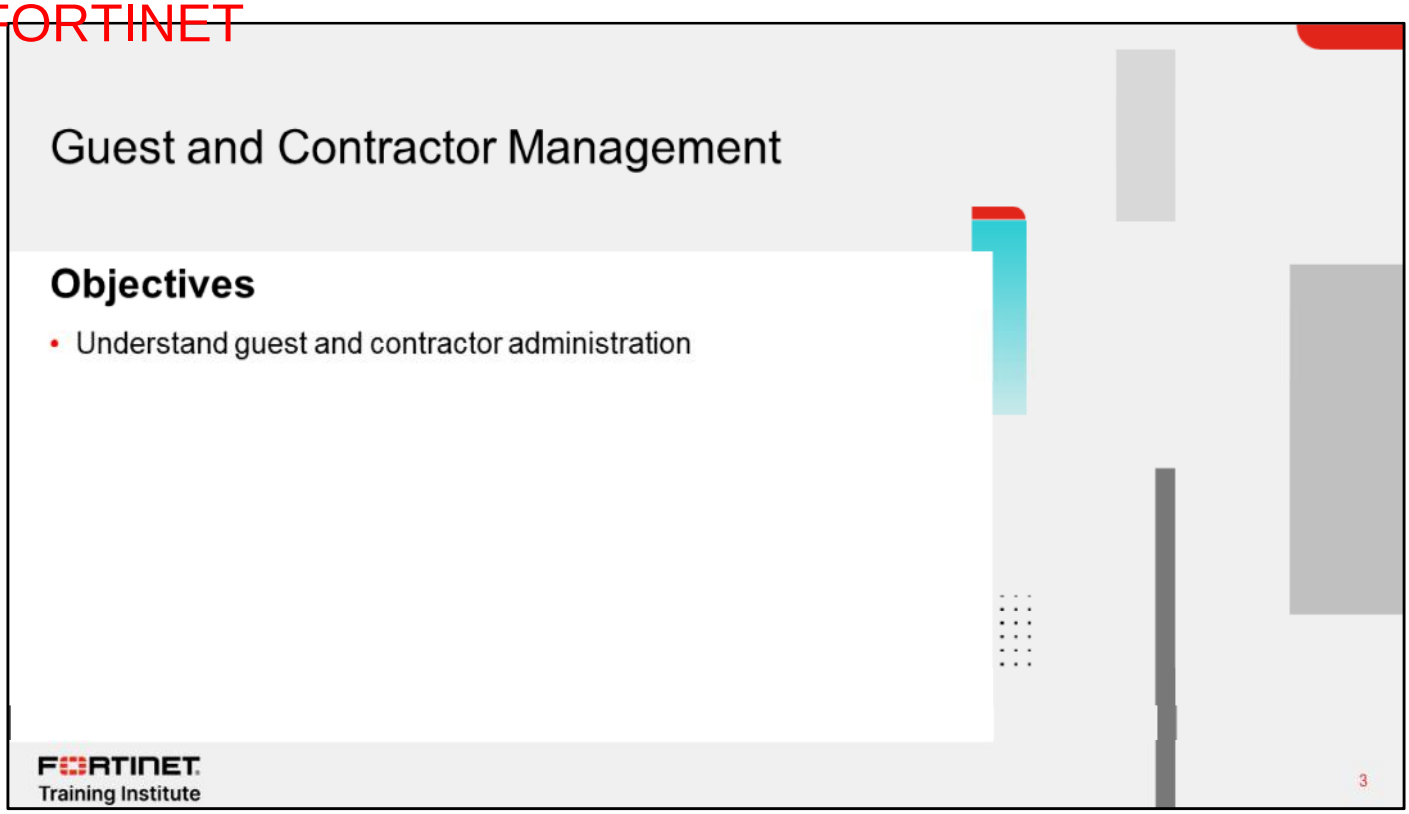
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topic shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

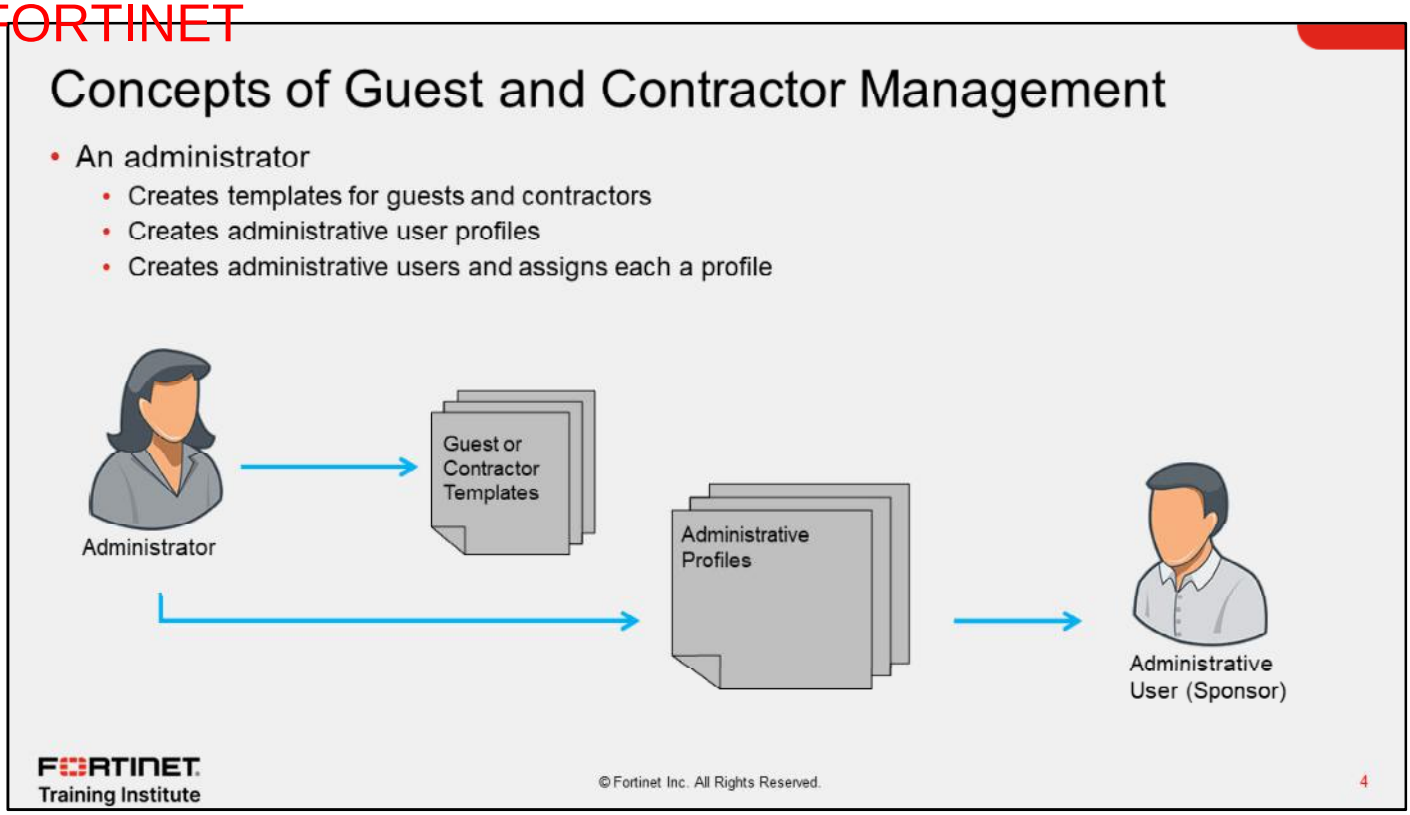


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in understanding and applying the concepts and configurations used to manage BYOD devices, you will be able to effectively use FortiNAC to securely onboard unknown devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Guest and contractor management begins with an administrative user creating a **Guest/Contractor Template**. These templates define the details of the guest or contractor accounts created from them. If you were going to have two different types of guests and four types of contractors in your environment, you would create six different templates.

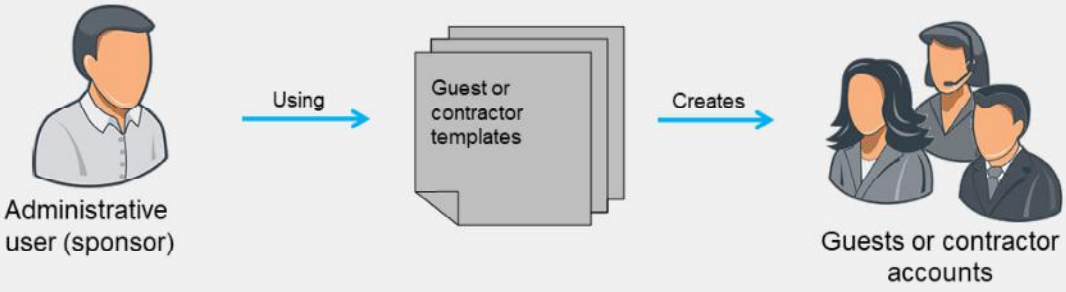
Any administrative user can be given the ability to create and manage these accounts. In this lesson, you will learn how to create an administrative profile that limits associated administrative users to having guest and contractor management capabilities only. These types of administrators are often called sponsors, and this allows for safe delegation of guest and contractor-related tasks. You can designate access to specific guest or contractor templates within the administrative profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Concepts of Guest and Contractor Management (Contd)

- An administrative user (sponsor) creates new guest or contractor accounts, restricted to the templates assigned by the administrator

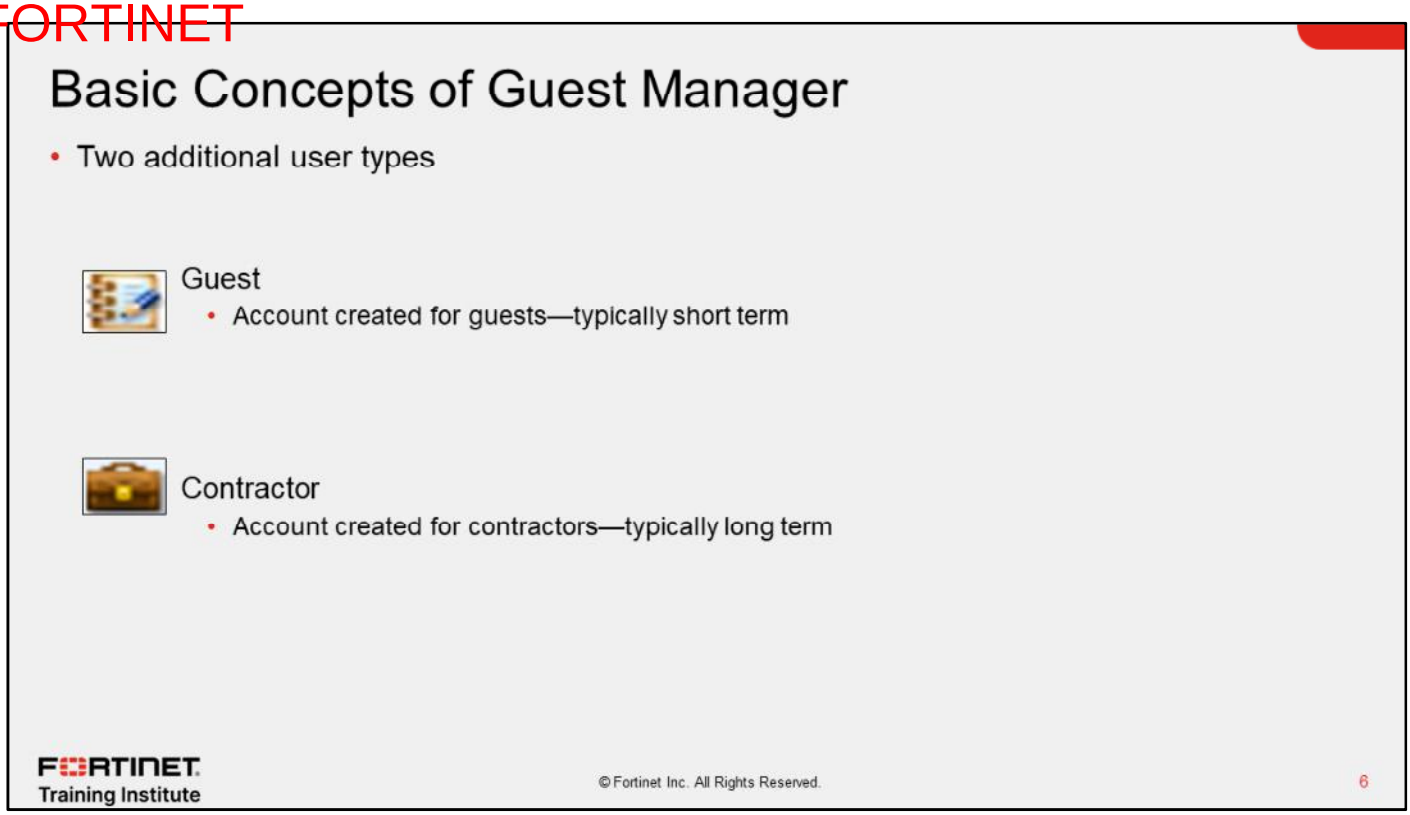


FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.
5

Sponsors can then select any guest or contractor template they have been allowed access to in the administrative profile, and create accounts. After you have created an account, you can provide the sponsor with the ability to manage the account through the administrative profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

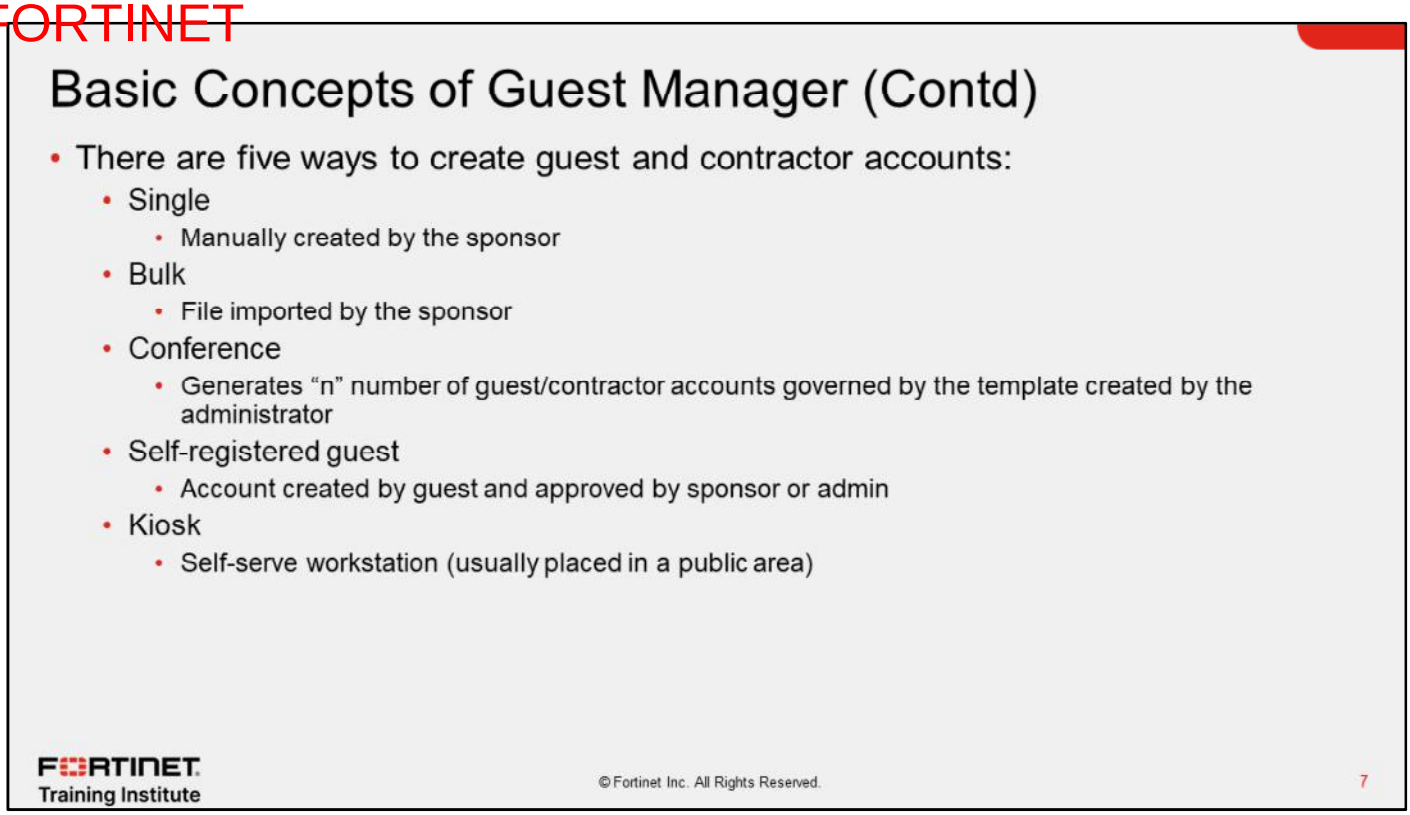


The user icons used by guest and contractor accounts differ from those used for standard network users or administrative users. Accounts created from guest/contractor templates with a **Visitor Type** set to **Guest** will have a user icon depicting a notebook and pencil. Accounts created from Guest/Contractor Templates with a **Visitor Type** set to **Contractor** will have a user icon depicting a briefcase. Other than the icon, there is no other difference between a guest or contractor account. Hosts that registered to those accounts will appear within the user branch, which is described in the *Visibility* lesson.

Guests are typically accounts with short account durations, often less than 24 hours, while contractors may have accounts that last months. Note that although the account types seen on this slide are represented by different icons, there is no difference in how they function. These icons allow quick identification of guests in the **User** view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are five different ways that guest accounts can be created in FortiNAC.

Single accounts are created by a sponsor. The sponsor fills in all fields defined by the selected **Guest/Contractor Template**.

Bulk accounts are one or more accounts either entered in a comma-separated list, one account per line, or imported from a file by a sponsor. All the accounts will share an **Account Start Date** and **Account End Date**. The account fields selected in the **Guest/Contractor Template** will define the information that needs to be entered in the comma-separated list.

Conference accounts are auto-generated by FortiNAC. The creation of the accounts is initiated by a sponsor. The sponsor sets a **Conference Type** which defines the user name and password format. The available options are **Individual User Name/Individual Passwords**, **Individual User Name/Shared Password**, **Shared User Name/Shared Password**. Conference accounts will all share the same **Conference Start Date** and **Conference End Date**.

When creating single, bulk, or conference accounts, the sponsor selects the **Guest/Contractor Template** that will be used. Recall that the sponsor will see only the templates made available to them in their administrative profile.

A self-registered guest account is an account the guest creates themselves from the registration isolation network. These accounts can be automatically approved by FortiNAC, or they can generate emails to one or more sponsors who then can approve or deny the account.

A kiosk is a dedicated workstation where guests can create their own accounts, normally located in a public area, such as a reception desk. Accounts created from the kiosk are automatically approved by FortiNAC. The kiosk workstation is enabled when a sponsor, assigned an administrative profile that has the **Enable Guest Kiosk** option selected on the **General** tab, logs in to the FortiNAC admin page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Guest/Contractor Templates

- Created by the administrator to define different types of guests or contractors

Users & Hosts > Guests & Contractors

Users | Templates

Add | Modify | Delete | Copy | Used By

Export to:

Guest/Contractor Templates - Total: 8

Name	Visitor Type	Authentication	Login Availability	Password Length	Password Exclusions	Account Duration
GuestSelfRegistration	Self Registered Guest	Local	Always	6	!@#$%^&*()_+~{}|:"<>?`-=[]\;',./	24 hours
GuestAccess	Guest	Local	Always	8	!@#$%^&*()_+~{}|:"<>?`-=[]\;',./	
GuestConference	Conference	Local	Always	8	!@#$%^&*()_+~{}|:"<>?`-=[]\;',./	
Conference	Conference	Local	Always	5	!@#$%^&*()_+~{}|:"<>?-=[]\;',./	
Accounting Contractor	Contractor	Local	Always	5	!@#$%^&*()_+~{}|:"<>?-=[]\;',./	25 hours
Engineering Contractor	Contractor	Local	Always	5	!@#$%^&*()_+~{}|:"<>?-=[]\;',./	25 hours
Standard_Guest	Guest	Local	Always	5	!@#$%^&*()_+~{}|:"<>?-=[]\;',./	12 hours
Fortinet Contractor	Contractor	Local	Always	5	!@#$%^&*()_+~{}|:"<>?-=[]\;',./	744 hours

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

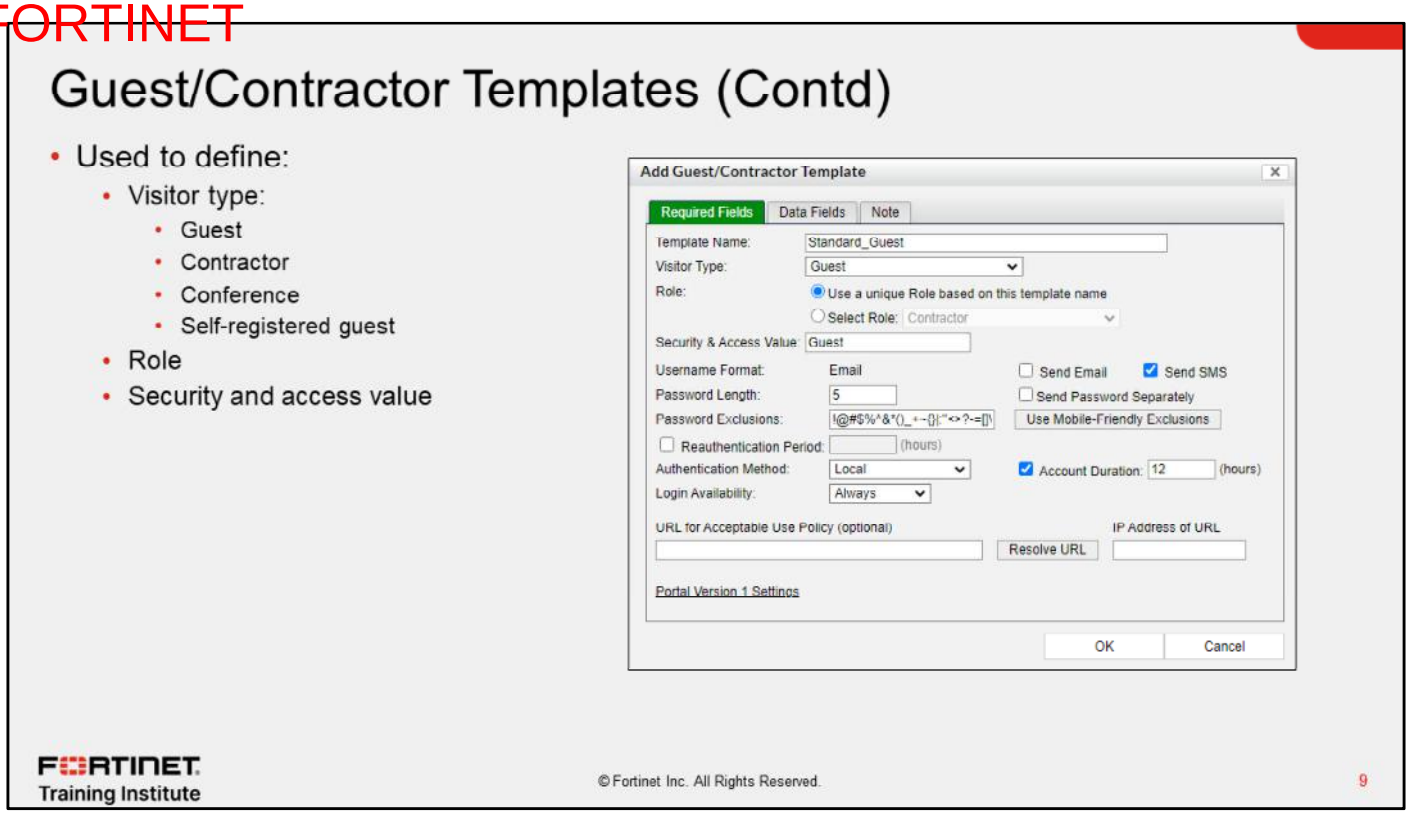
8

This slide shows the first step of guest and contractor management: the creation of a guest/contractor template. Recall that guest and contractor templates define the accounts that are created from them. These details can then be leveraged to assign security policies that could define endpoint compliance requirements, network access, and so on.

The view will display all existing templates. Clicking **Add** opens the **Add Guest/Contractor Template** window.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Each guest and contractor template has three tabs: **Required Fields**, **Data Fields**, and **Note**. The **Required Fields** tab is where template settings that define account capabilities are set. Each template must have a unique name, and this is defined in the **Template Name** field.

The **Visitor Type** sets the type of user icon that will represent any guest or contractors created from this template. The options are:

- **Guest**: This account type is used to represent short term accounts, normally lasting one day or less. The user icon used to represent a guest account is a notepad and pencil.
- **Contractor**: This account type is used to represent a temporary employee, which may last weeks or months. The icon used to represent a contractor is a briefcase.
- **Conference**: This account type is used to create a group of short or long-term accounts that all share the same account duration settings. These accounts can have unique usernames and passwords, shared usernames and passwords, or unique usernames with a shared password. The user icon used to represent conference accounts is the same person with a blue jacket used for standard network users.
- **Self-Registered Guest**: This account type is used to represent accounts created by the guest through the guest self-registration portal. The user icon used to represent a self-registered guest account depicts the same person with a blue jacket used for standard network users.

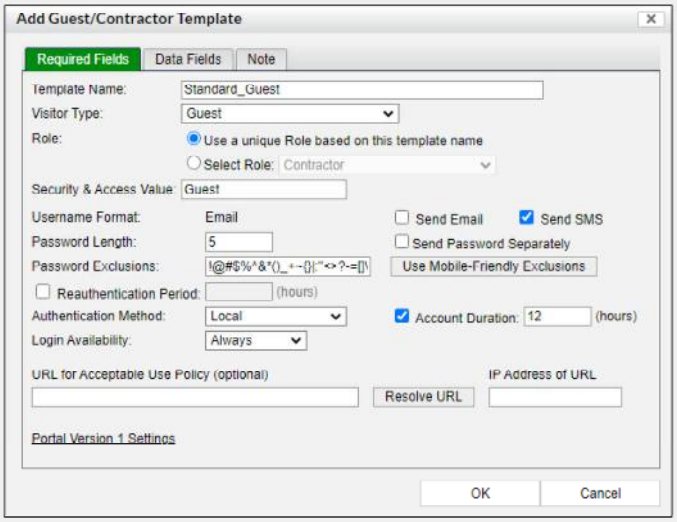
The **Role** field, by default, will populate with the **Template Name** but can be selected from a list of existing roles. Roles can be created on the **Policy & Objects** menu by selecting **Roles**. The role value of a guest and contractor template will populate the **Role** field of any account created from the template. The **Security & Access Value** field can be used to designate any value an administrator desires, to populate the **Security & Access Value** field of any account created from the template. Both the **Role** and **Security & Access Value** field values can be used to create **User/Host Profiles** for use in security policies, such as a network access policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Guest/Contractor Templates (Contd)

- Used to define:
  - Account requirements or restrictions
  - Password requirements
  - Reauthentication requirements
  - Login availability settings
  - Acceptable use policy settings



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

The **Username Format** is always **Email**, and account information can be sent to end users over email or SMS. If SMS is going to be used, the account information defined in the **Data Fields** must include **Mobile Provider** and **Mobile Number**. The **Password Length** field is where the exact length of each FortiNAC auto-generated password can be defined. The value must be between 5 and 64.

Password exclusions are characters that will not be used in the auto-creation of passwords. By default, this field is populated with all non-numeric and non-alphanumeric characters. This default list of exclusions can be repopulated by clicking **Use Mobile-Friendly Exclusions**.

If a **Reauthentication Period** is defined, the host will be isolated when the designated time expires and the user will need to re-authenticate in order to get out of isolation. Authentication method options are **Local**, **LDAP**, or **RADIUS**. **Local** is the default option and is usually the case when creating short-term accounts such as guests or self-registered guests.

Account Duration and **Login Availability** provide the administrator with a way to define when the account will be deleted from the database, or what days of the week and times of day the account will be enabled.

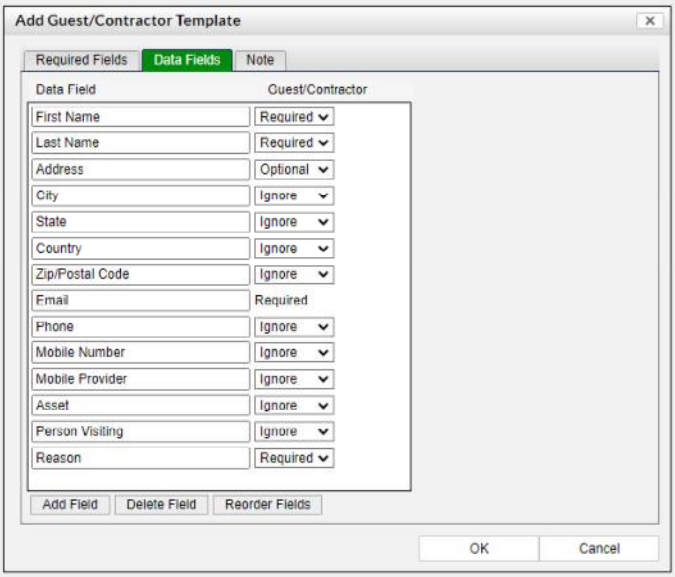
The **URL for Acceptable Use Policy** is an optional field that provides a link to an acceptable use policy page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Guest/Contractor Templates (Contd)

- Required information that will be supplied by the guest or contractor during registration



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

11

The **Data Fields** tab is where guest account fields are selected. Each pre-existing field can be set to:

Ignore: Fields set to ignore will not appear on the guest account creation page.
Required: Fields set to required will have to be filled in during account creation and an error will be generated if a required field is left blank.
Optional: Fields set to optional will appear on the account creation view but can be left blank.

Data fields can be added or deleted from the list with the exception of the **Email** field. This is a mandatory field and will act as the username. All fields can be reordered.

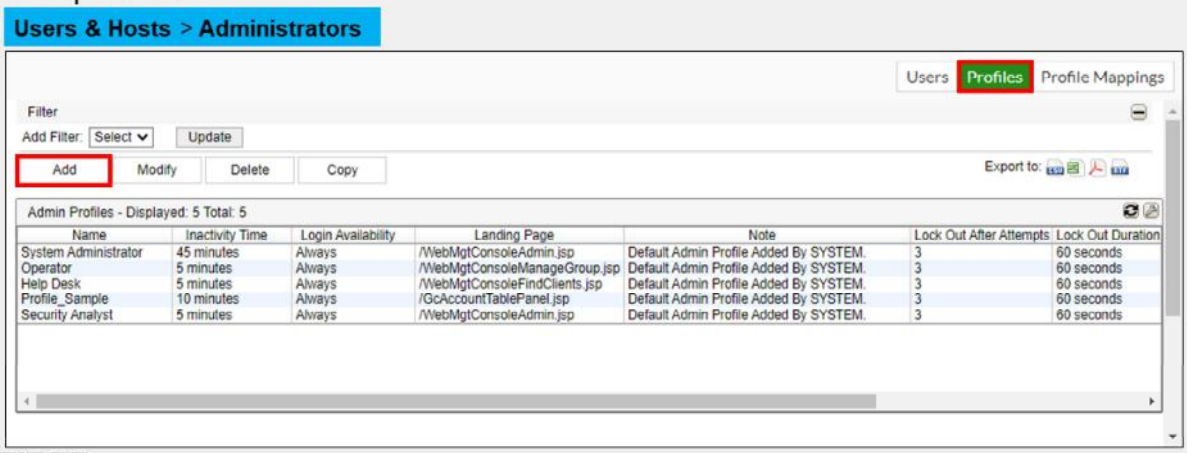
The selected fields defined within the template will make up the account creation page for the sponsor to complete, or for the guest to complete in the case of a kiosk or self-registration page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Administrative User Profiles

- Created by the administrator
- Used to define rights and restrictions of administrative users
- Administrative users with the ability to create and manage only guest accounts are often called sponsors



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

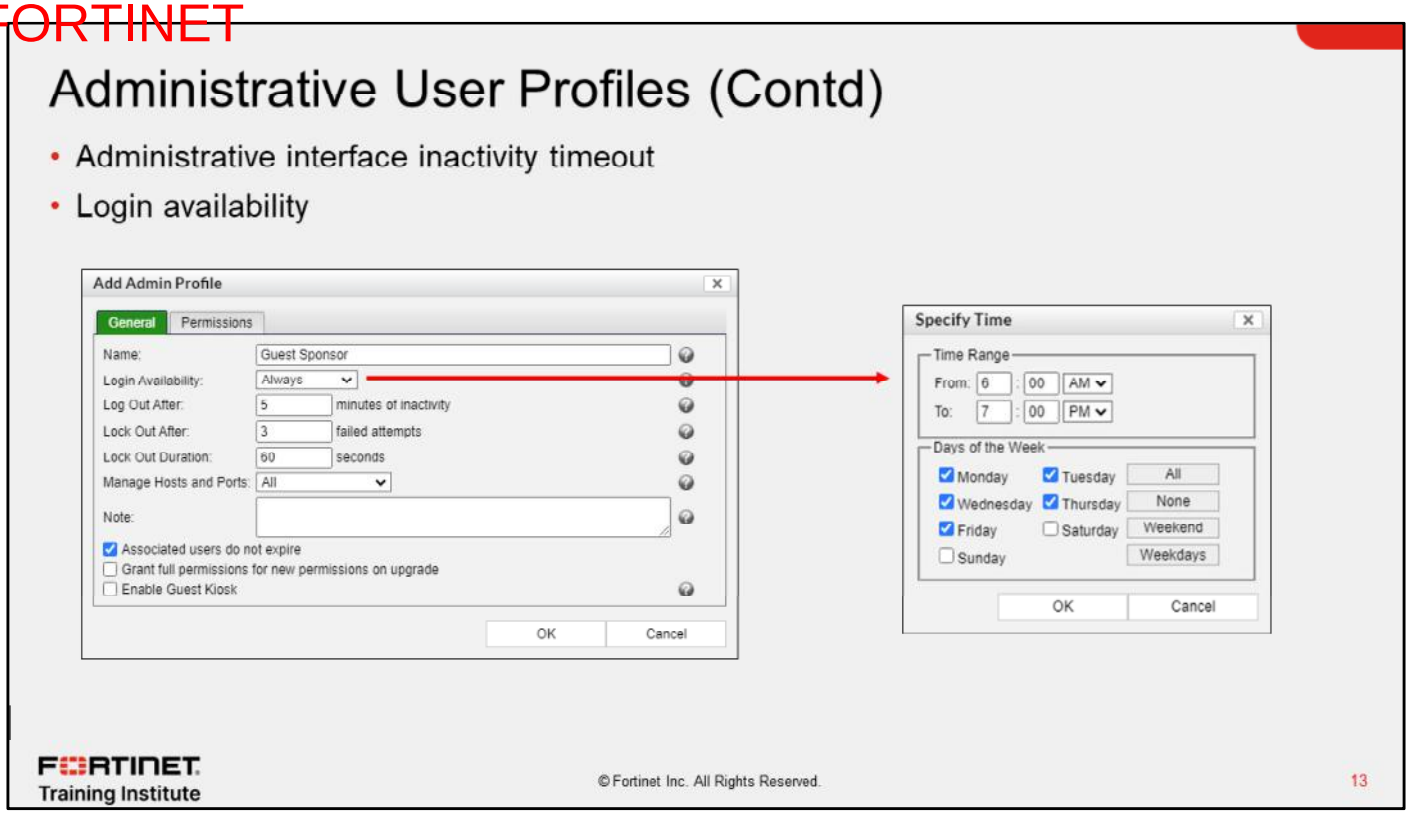
12

Administrator profiles define the capabilities of the administrative users they are assigned to. In this section, you will learn how to create an administrative user that is limited to the creation and management of guest accounts. This type of administrative user is often called a sponsor.

Administrative profiles are created on the **Users & Hosts** > **Administrators** view from the **Profiles** tab. Clicking **Add** opens the **Add Admin Profile** window.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

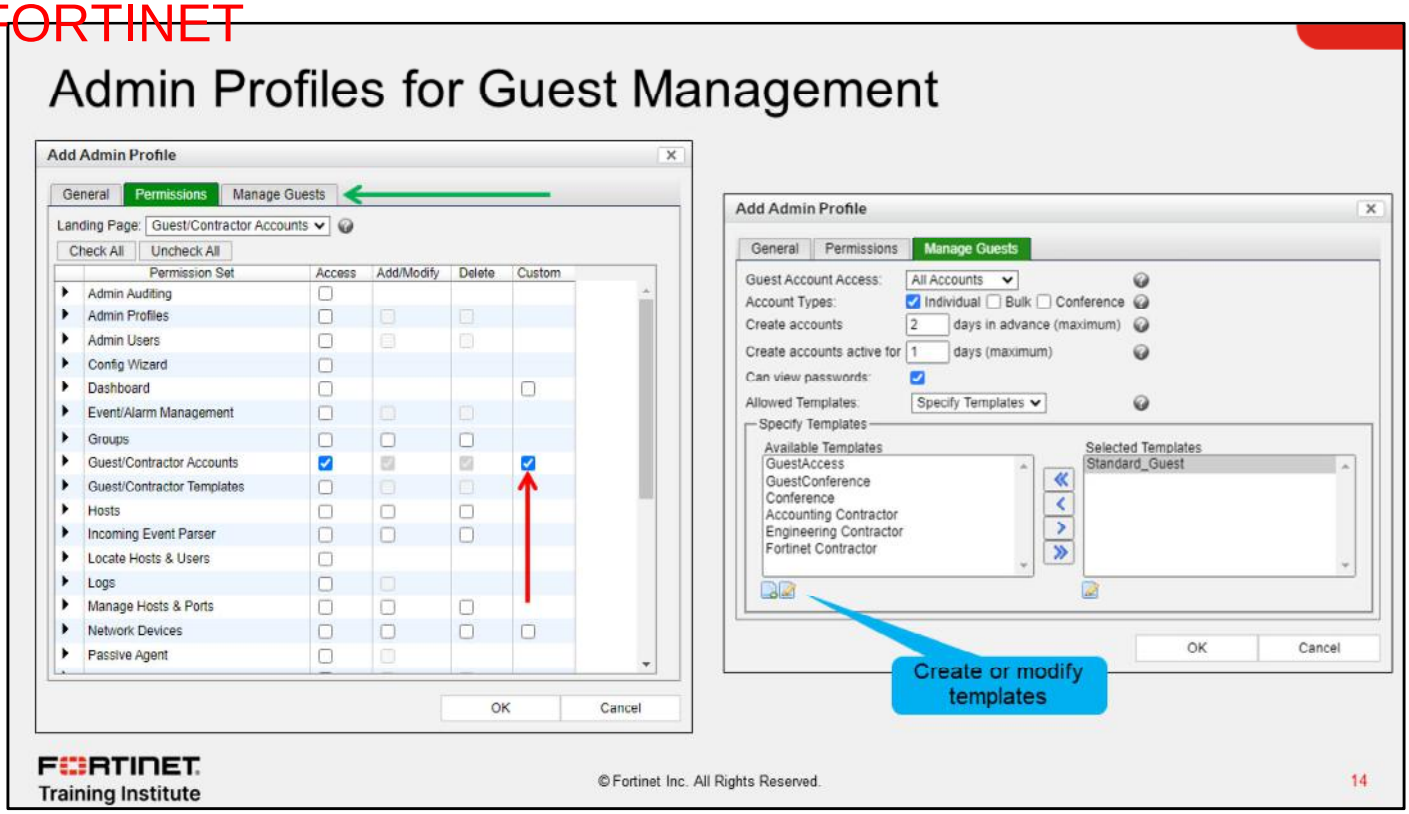


Recall from a previous lesson that each profile will have a unique name, a logout after setting for inactivity timeout, and login availability options to specifically define when administrators assigned this profile can log in to FortiNAC. The **Enable Guest Kiosk** checkbox provides a field of all available templates as well as a field for entering the welcome text that will be displayed on the kiosk screen. The **Permissions** tab will not be displayed for administrative profiles that have the **Enable Guest Kiosk** box selected.

When an administrator assigned a kiosk-enabled profile logs into the FortiNAC GUI, the page that loads will be a registration page where guests can build accounts for access.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Permissions** tab is where you can select which permission sets to define the capabilities of a sponsor. In the example shown on this slide, only the **Guest/Contractor Accounts** permission set has been selected using the **Access** checkbox. Then the **Custom** checkbox, indicated on this slide with a red arrow, can be selected to provide detailed account creation capabilities. When the **Custom** checkbox is selected, the **Manage Guests** tab will appear, which is indicated on this slide by a green arrow.

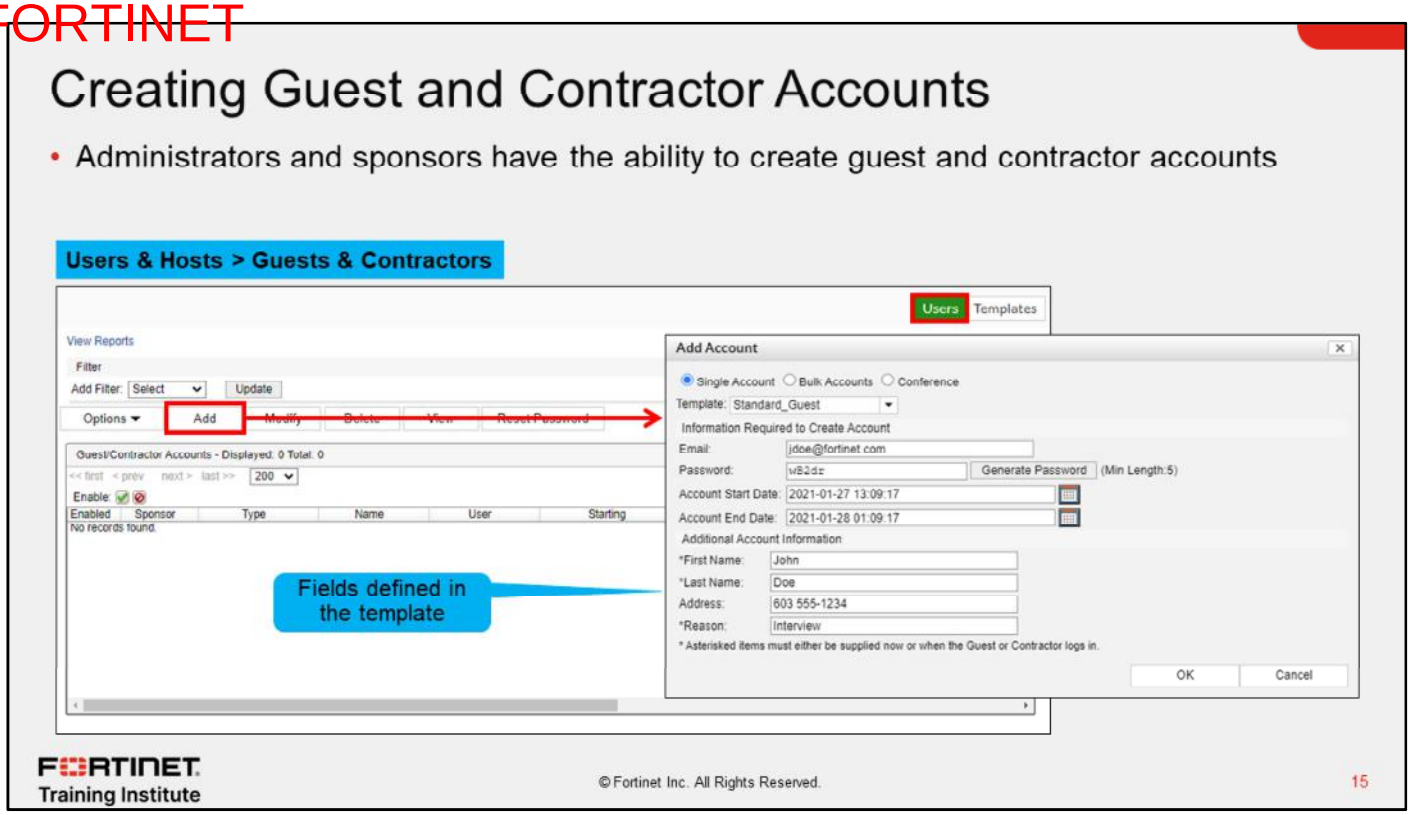
The **Manage Guests** tab contains several settings. The **Guest Account Access** field defines the guest or contractor accounts that can be managed. The options in the drop-down list are **All Accounts, No accounts**, or **Own Accounts**, with the final option meaning only accounts created by this sponsor. Management of a guest account means that the account can be enabled, disabled, or the password reset.

The types of accounts the sponsor can create are selected using the checkboxes in the **Account Types** field. Control of how far in advance a sponsor can create accounts, as well as how long those accounts will exist before expiration, can also be defined on the **Manage Guests** tab.

The **Allowed Templates** field will define if all guest/contractor templates will be available for use or if only specific templates will be made available. The **Specify Templates** section of the window will allow you to specifically select which templates will be available to the sponsor.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

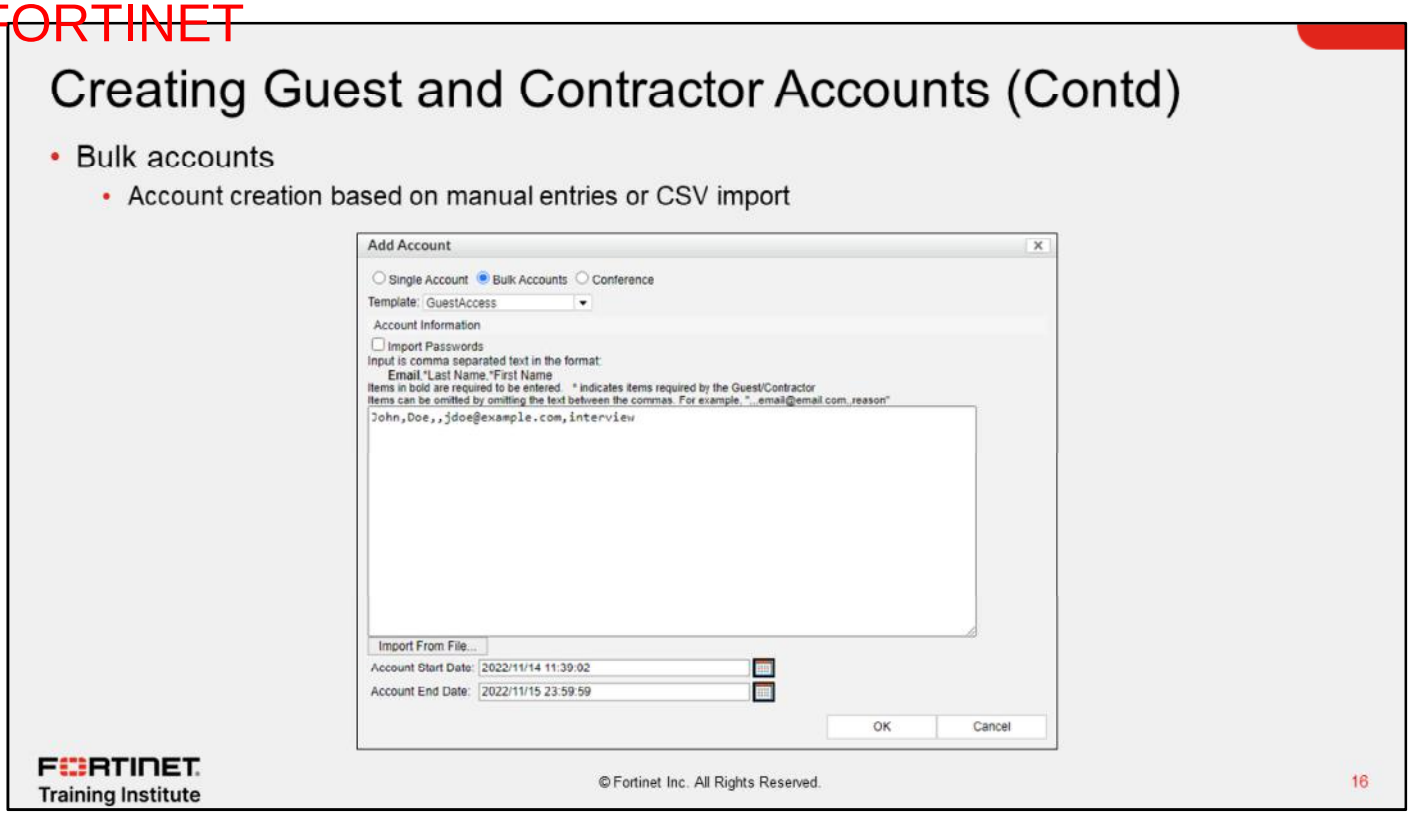


You can create guests and contractor accounts from the **Users** tab on **Users & Hosts** > **Guest/Contractor Accounts**. When adding a single, bulk, or conference account, you must select a **Template** from the field. The available templates in the drop-down list are made up of the allowed templates as defined in the **Admin Profile**.

For a single account, the remaining fields are all of the required and optional fields, in addition to the **Account Start Date** and **Account End Date** settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

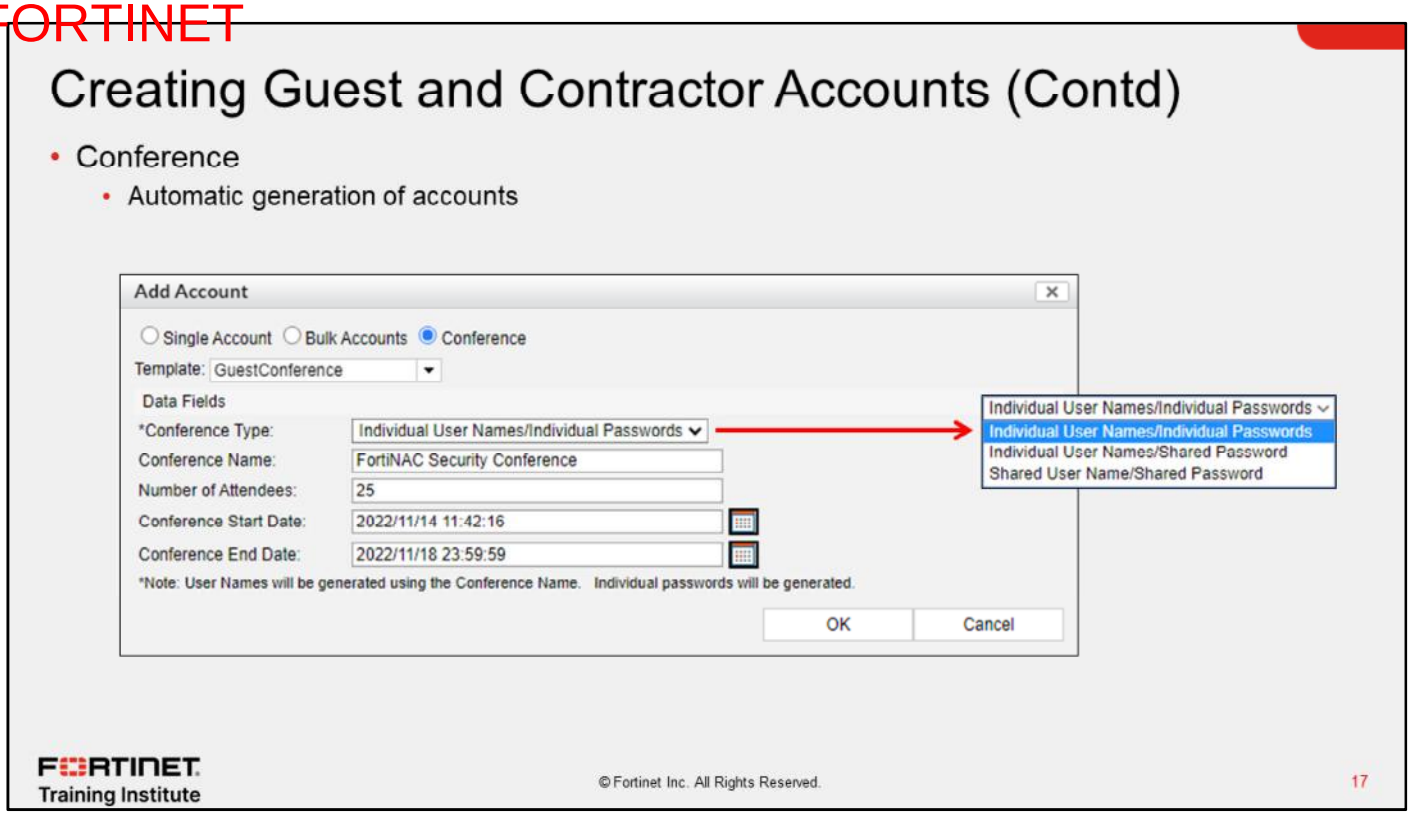
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Bulk accounts are one account per line, and information is comma separated. The selected template will define the columns and column order for manual entry or file import. Click **Import From File** to select a pre-created list of accounts. Regardless of the manner of entry, all columns must be represented, with columns being left blank identified with two commas. For example, if the data being imported was first name, last name, address, email, and reason, but street address was optional and left empty, it would look something like this: `John,Doe,,jdoe@example.com,Interview.` All bulk accounts will share the same **Account Start Date** and **Account end Date** settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



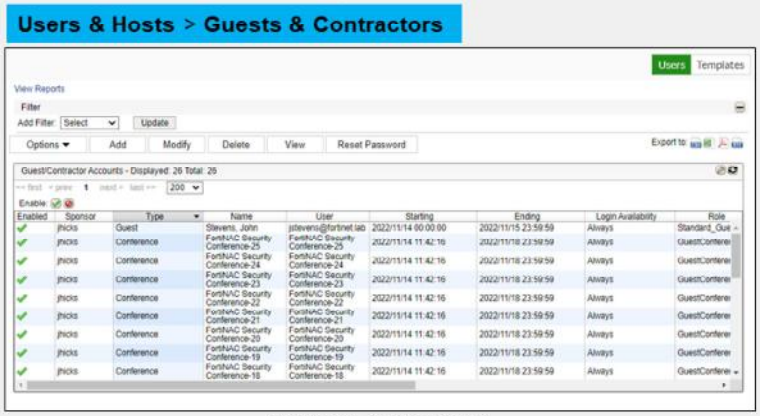
Conference accounts are initiated by a sponsor but actually auto-generated by FortiNAC. The **Conference Type** field is used to define if each auto-generated account should have unique or shared user names and passwords. The name of the conference will be used as part of the account names. The maximum number of attendees is defined within the template and any number up to that can be entered. The **Conference Start Date** and **Conference End Date** settings will be the same for all generated accounts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Managing Guest and Contractor Accounts

- Management of guest and contractor accounts allows:
  - Adding of accounts
  - Modifying, removing, and viewing of existing accounts
  - Enabling or disabling accounts
  - Resetting account passwords
  - Generation of guest and contractor account reports



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

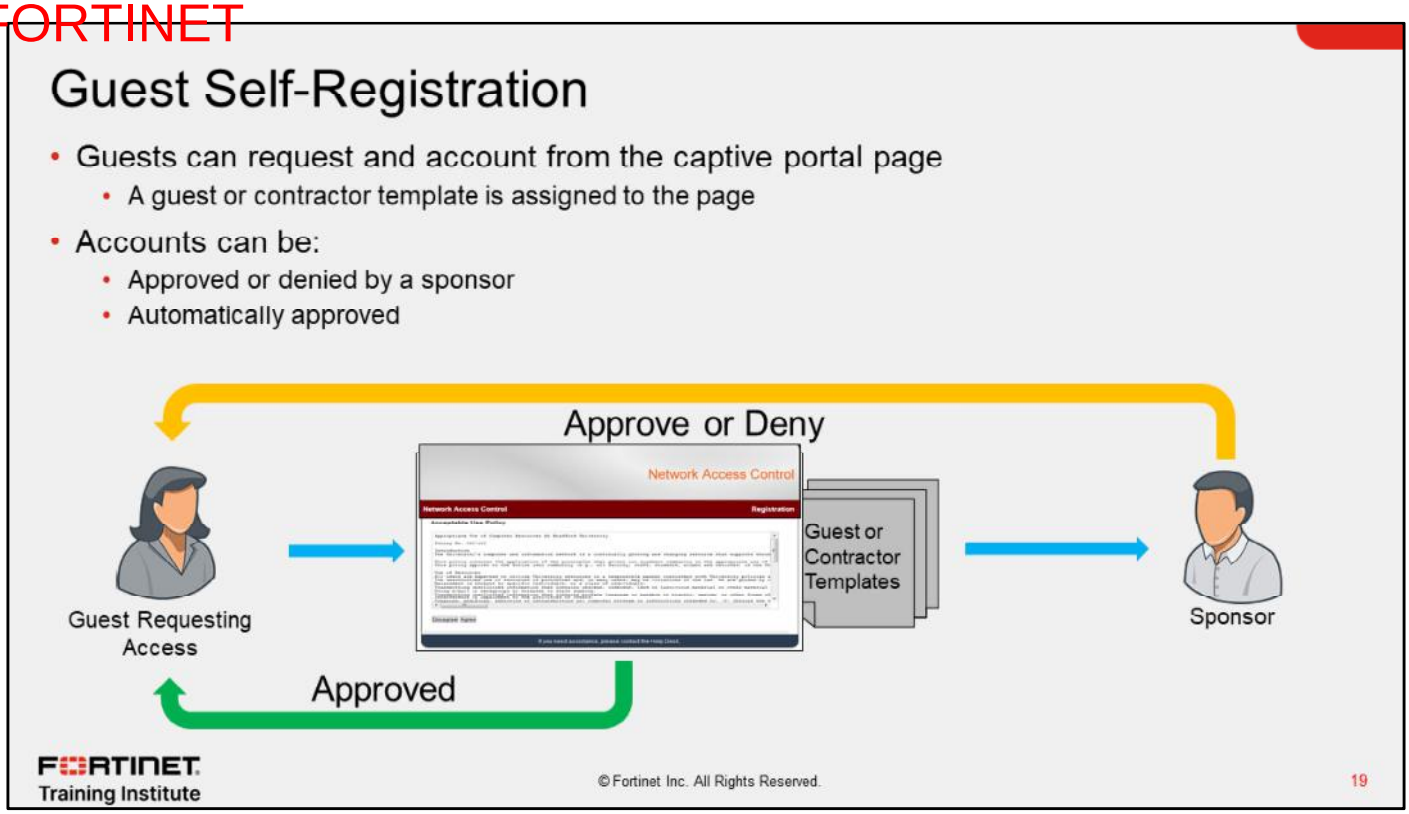
18

You can manage guest and contractor accounts on the **Users & Hosts** > **Guests & Contractors** view. Depending on the settings configured in the administrator profile, an administrator or sponsor may have the ability to manage any account, no accounts, or only accounts they created. Each account is presented with its account attributes as well as the user ID of the sponsor who created the account. This is the same view where account creation is performed.

You can modify, delete, and view selected accounts, as well as reset passwords. Viewing an account displays all the information shown on the main page in addition to the account password. On the **View Accounts** window, you can email, send by SMS, and print account information, as well as create badges.

Vouchers & Dumps are Available | WhatsApp +201224560923

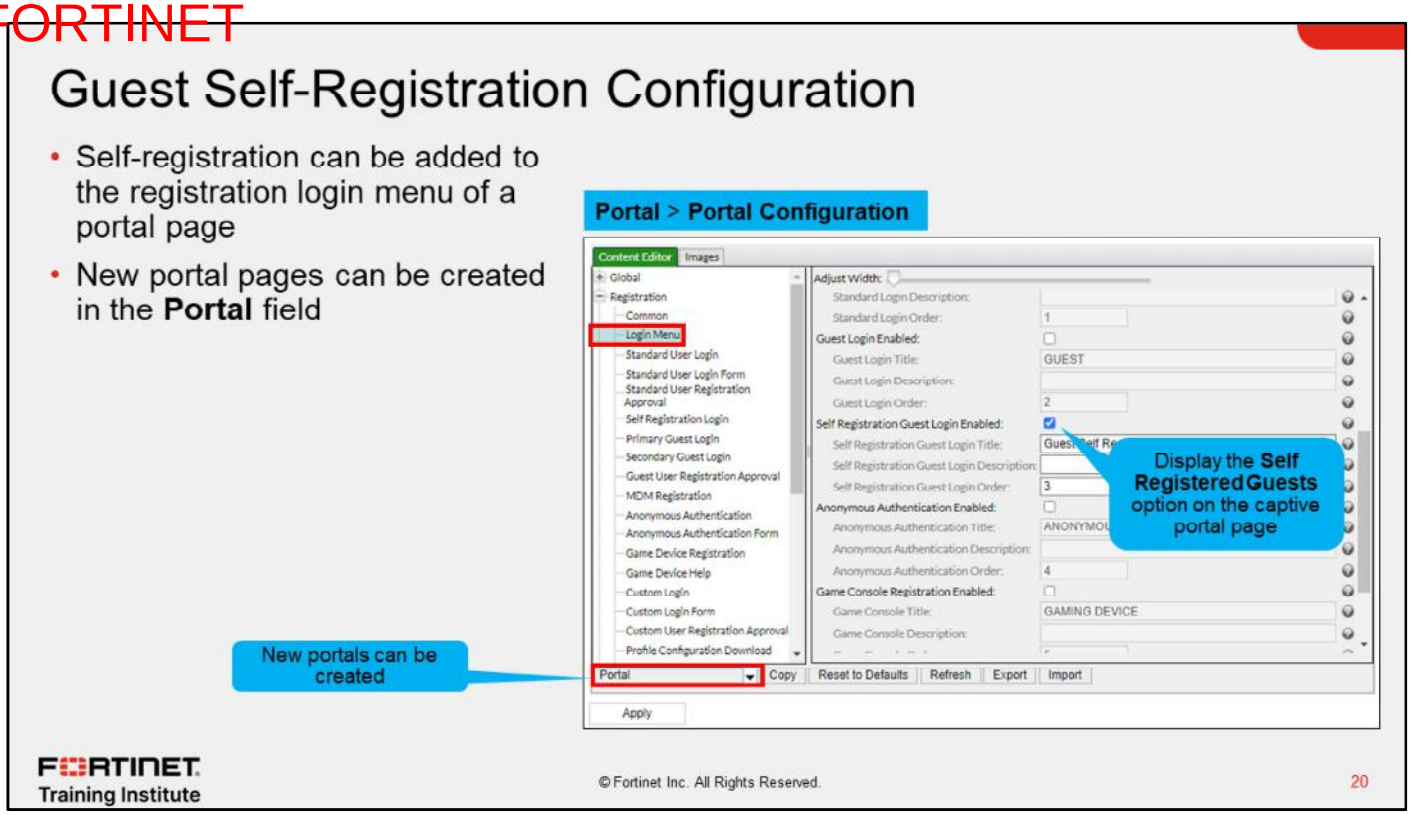
DO NOT REPRINT
© FORTINET
Brave-dumps.com



A self-registered guest account is created by the guest who wants to onboard a host. The self-registration page is presented to rogue hosts that have been isolated in the registration isolation network. The user, once presented with the isolation portal page, can fill in the required fields as defined in the **Guest/Contractor Template** associated with the page, and submit the request. You can configure FortiNAC to require approval from a sponsor, or to automatically approve the request. If sponsor approval is required, one or more sponsors can be notified of the request through an email message, and the request can be approved or denied from within the email. Sponsors can be required to enter FortiNAC credentials in order to approve or deny a request. Automatic approval results in the guest being immediately notified within the portal that their request was approved, and they will be able to onboard from the approval page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



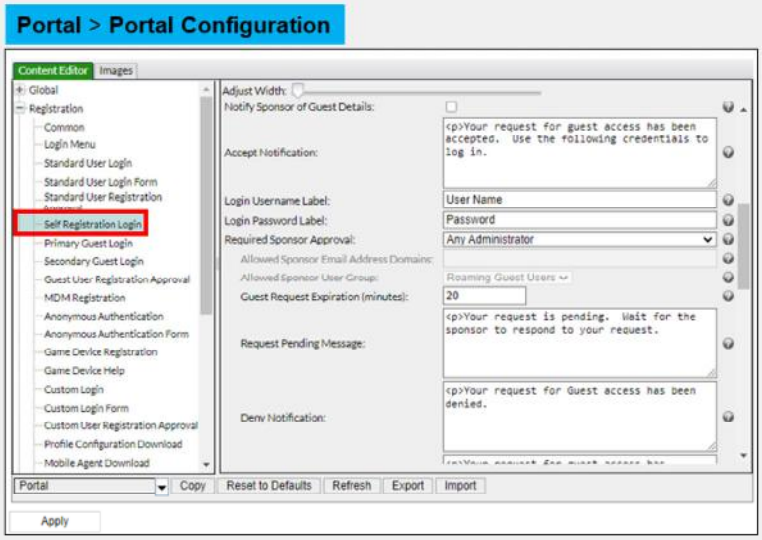
You add the option for guest self-registration by enabling the **Self Registration Guest Login Enabled** option. You can enable this option on the login menu of any portal page. In some environments, you may want to have a portal with only the self-registration option for hosts connecting to a specific SSID. For example, you may want to show any rogue host connecting to a guest SSID a page with only the self-registration request option. The example shown on this slide would create a page with only one option for guests presented with the registration isolation portal. As you learned earlier, this portal could then be presented using a **Portal Policy**. A common deployment configuration would present this portal to all rogue hosts that connect to a specific SSID, such as an open guest SSID.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Guest Self-Registration Configuration (Contd)

- Self-registration configurations are made on the **Self Registration Login** page
  - Login labels
  - Notifications and messages
  - Sponsor approval settings
  - Guest template designation
  - Acceptable use policy



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

21

When a user selects the self-registration option on the isolation portal they are directed to the **Self-Registration Login** page. You customize the page content and behavior from the **Self-Registration Login** portal configuration page. From this configuration page you can customize text and labels shown on the page, as well as notification messages. In many environments, a sponsor is needed to approve guest requests. These configurations include which users can act as a sponsor, if authentication is needed for the sponsor to approve a registration request, and how long a guest request is valid while waiting for approval.

As with any other type of guest account, guest templates are used for account creation of self-registered guest accounts.

You can add an acceptable use policy, either directly in the page or by hyperlink. When you add an acceptable use policy, users will need to agree to the policy in order to complete the request.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which setting within a guest or contractor template can be used to assign a network access policy to all accounts created from that template?
   - A. Account Duration
   - ✓ B. Security Access Value
2. In the User view, which account type is represented by a briefcase icon?
   - A. Guest
   - ✓ B. Contractor

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

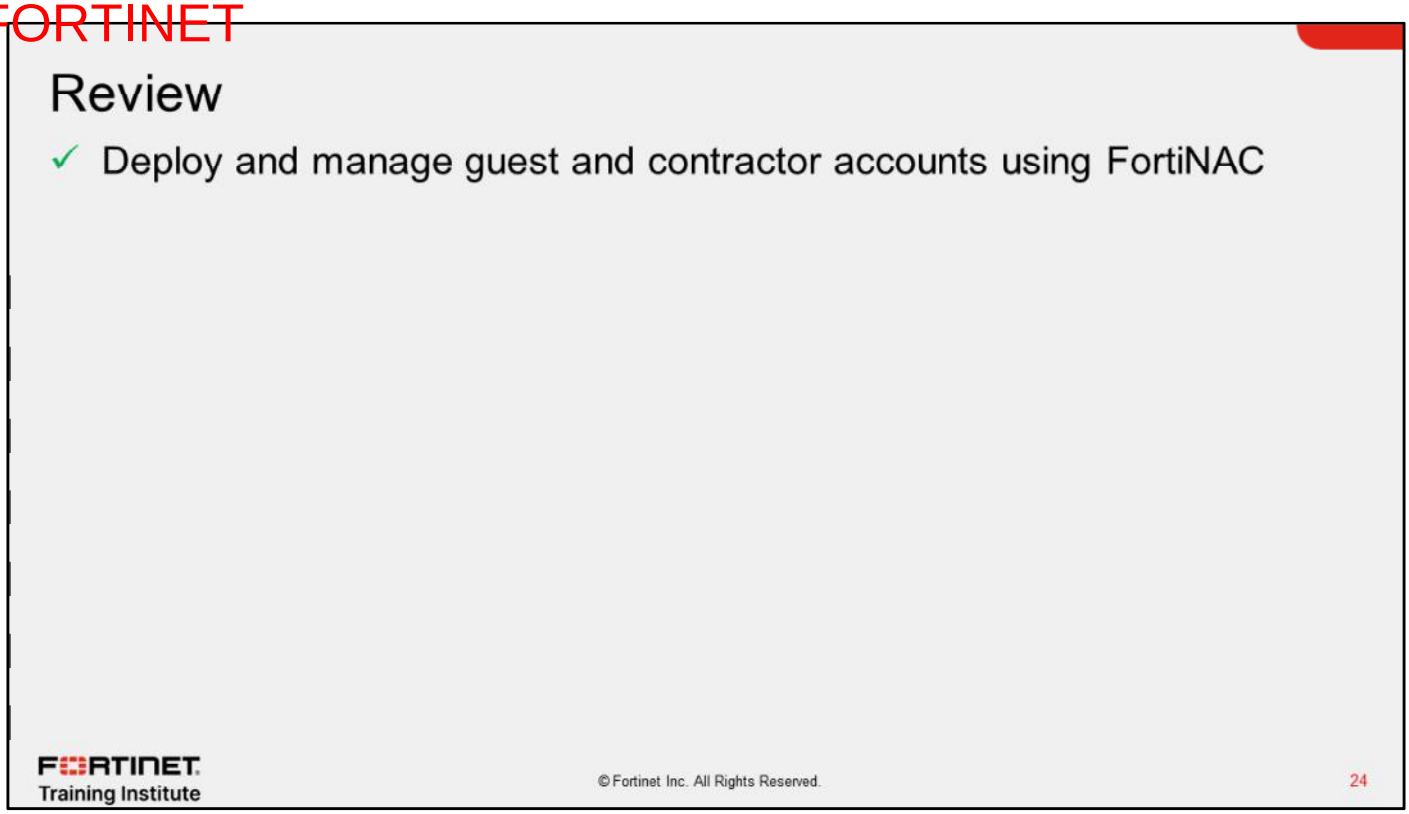


Congratulations! You have completed this lesson.

Now, you will review the objective that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

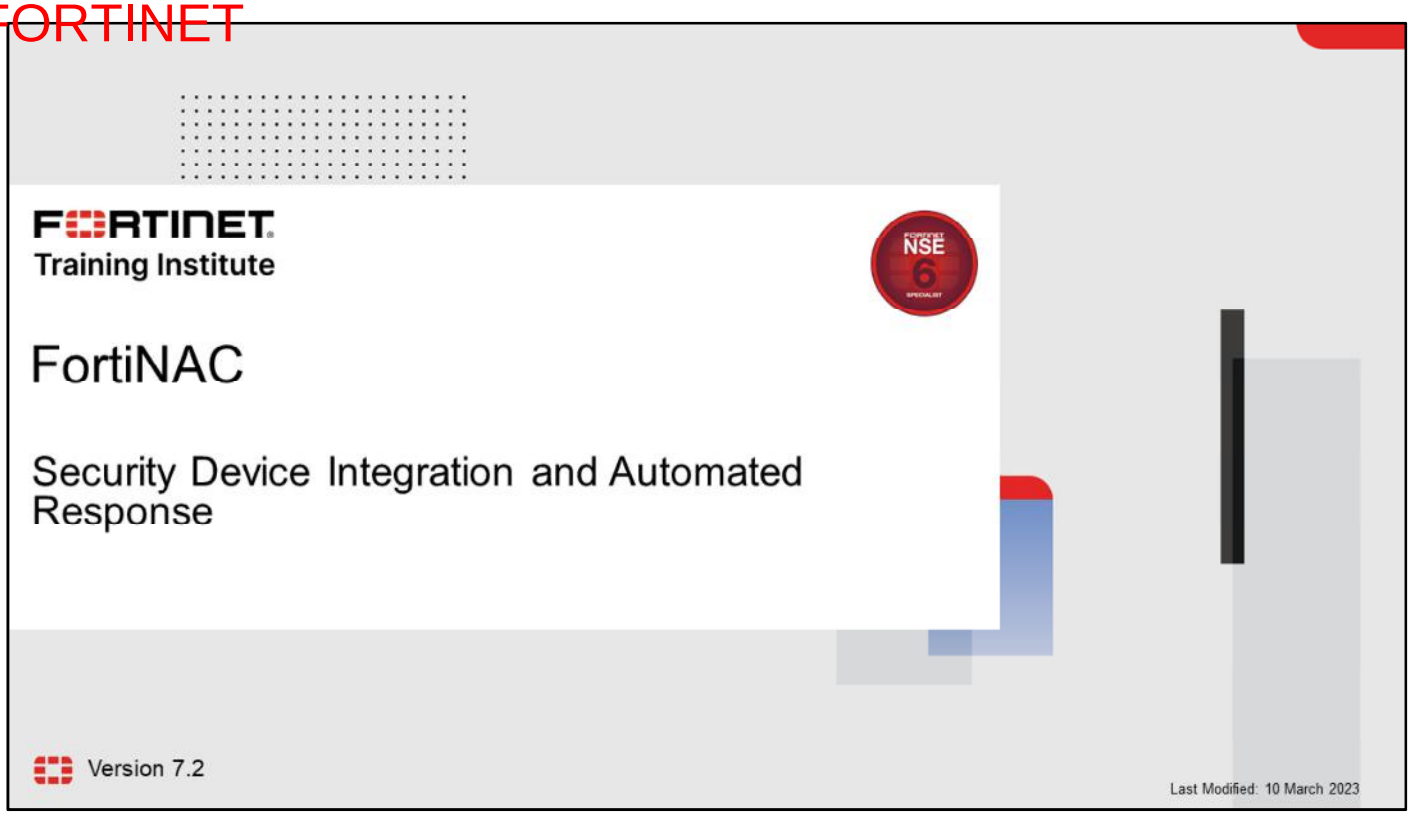


This slide shows the objective you covered in this lesson.

By mastering the objective covered in this lesson, you learned how to use FortiNAC as a tool to create and manage guest and contractor access.

Vouchers & Dumps are Available | WhatsApp +201224560923

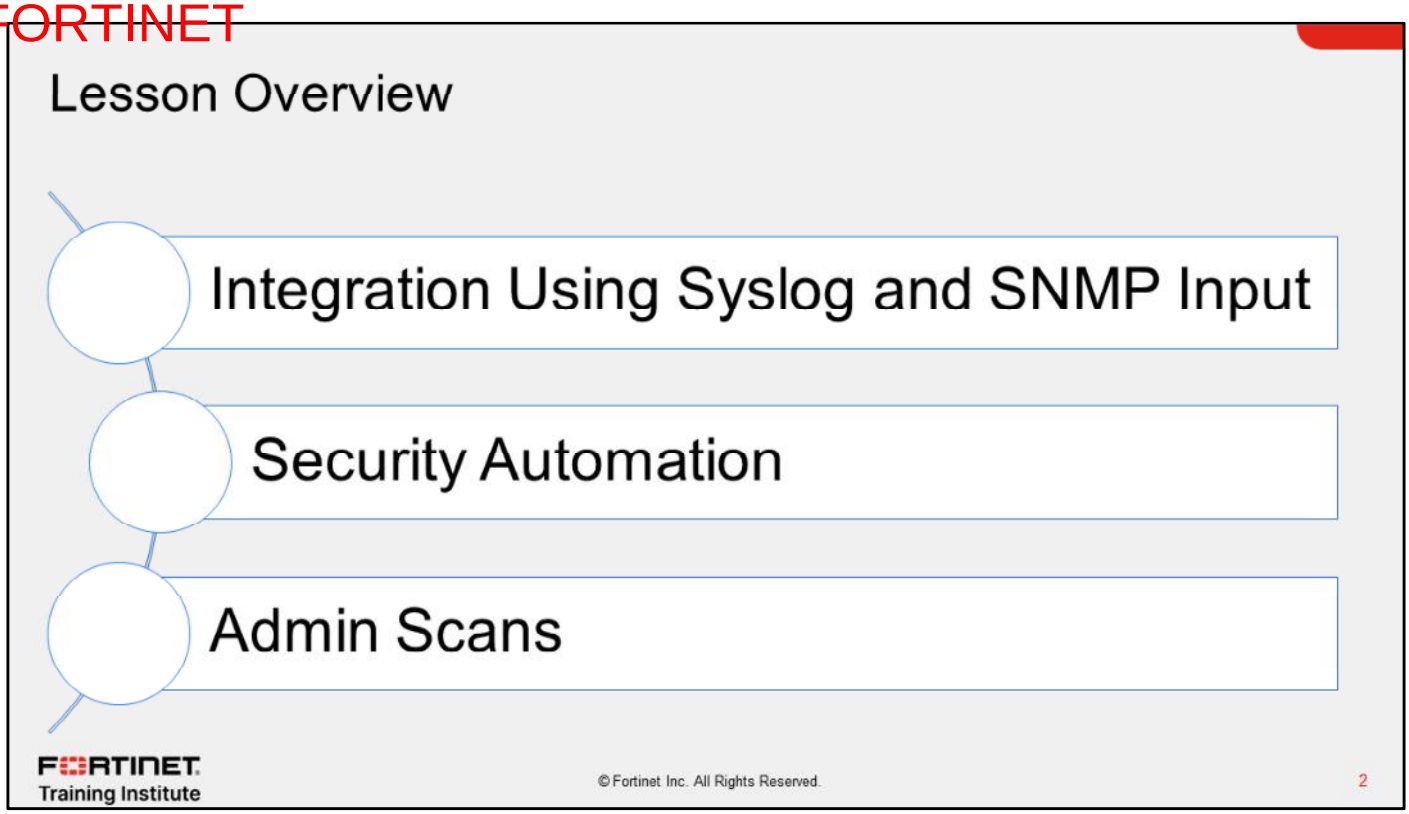
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to integrate FortiNAC with third-party devices using Syslog or SNMP traps.

Vouchers & Dumps are Available | WhatsApp +201224560923

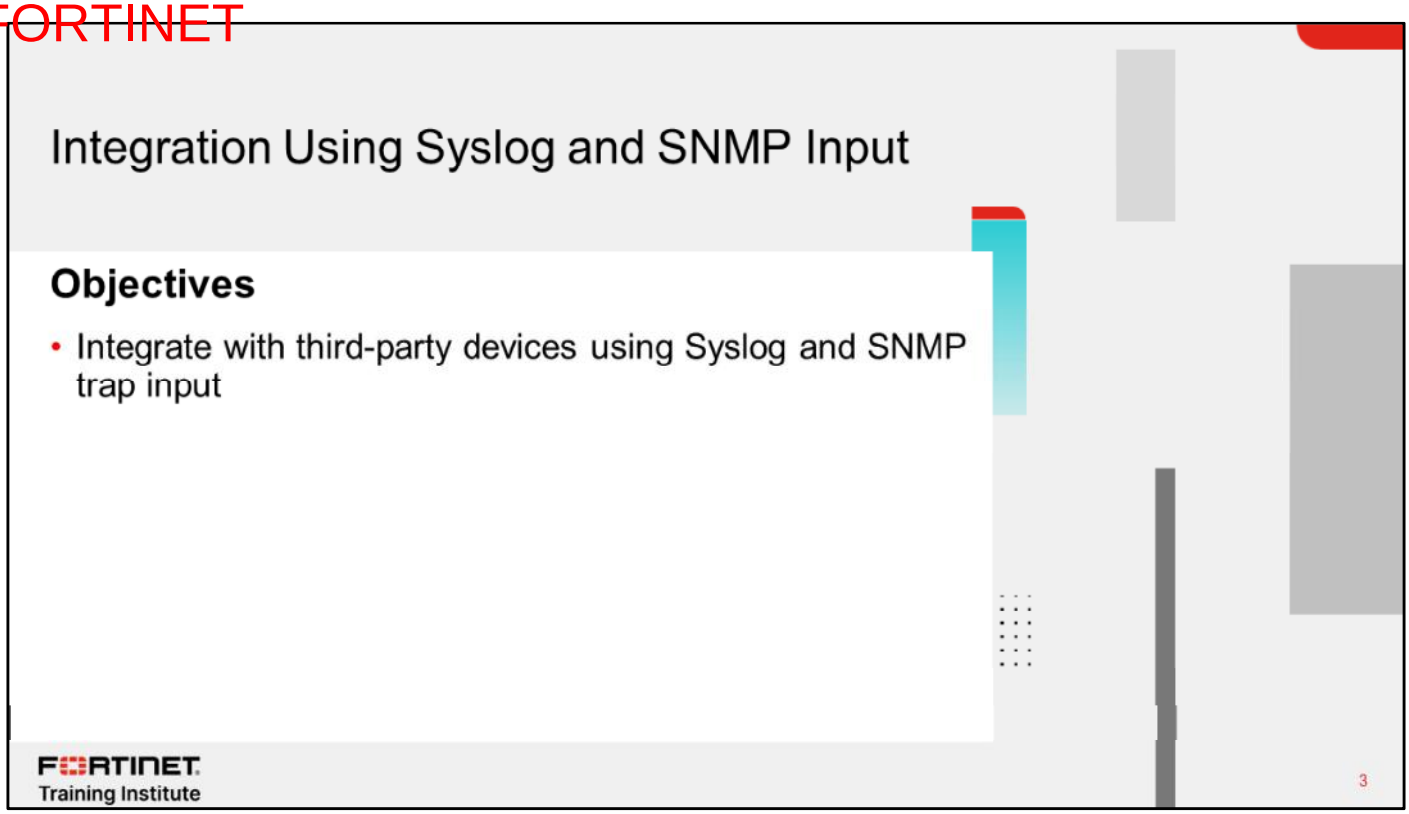
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

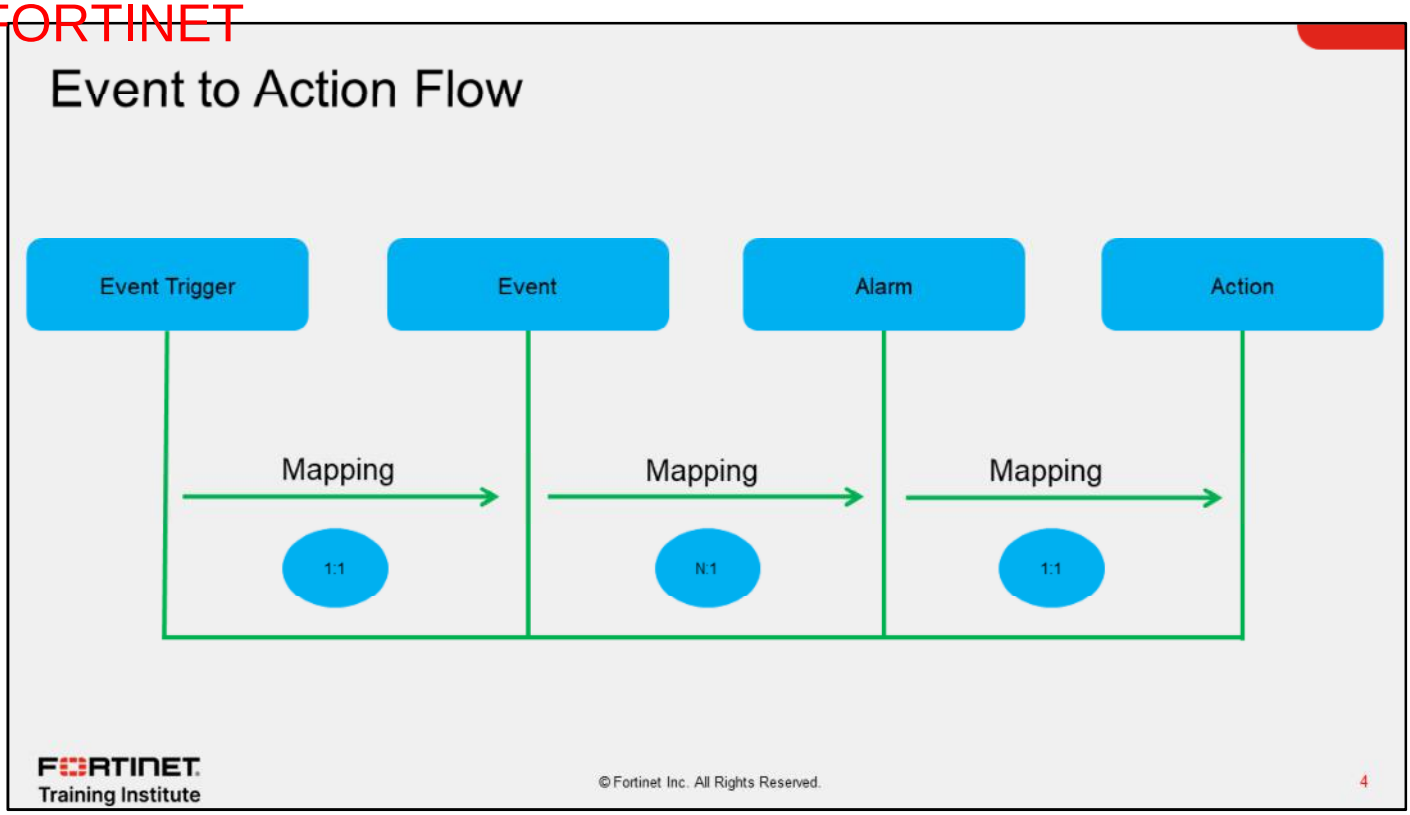


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in integration using Syslog and SNMP input, you should be able to leverage existing infrastructure devices to trigger FortiNAC notifications and responses.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In a previous lesson, you learned how an event can be mapped to an alarm, and that alarms can have actions attached to them. This slide shows the complete flow, beginning with an event trigger and ending with an action. Event triggers are a set of criteria that, when satisfied, cause an event to be generated. By default, there are approximately 430 different event triggers. This is a one-to-one association. Each time the trigger is satisfied, the event is generated. Recall that events are displayed in the **Events & Alarms** view located on the **Logs** menu.

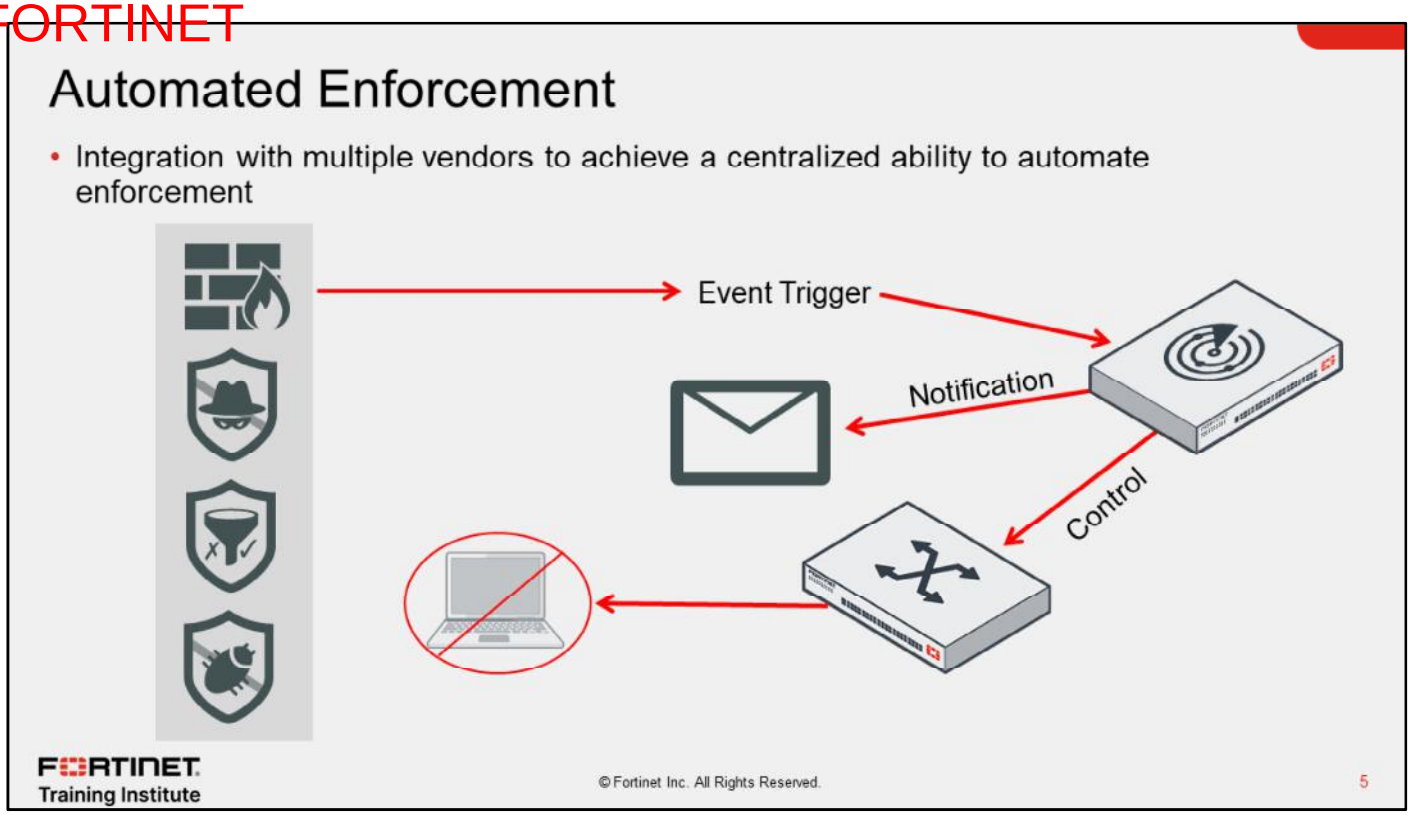
You can then map events to generate alarms. By default, there are about 55 events mapped to generate alarms. Events that generate alarms are not necessarily mapped in a one-to-one association, like event triggers are to events. You can define events to generate alarms using a **Trigger Rule** with the following options:

One Event to One Alarm: This option will generate an alarm each time the event is generated.
All Events to One Alarm: This option will generate an alarm only the first time the event is generated. No further alarms will generated until the previous alarm is cleared.
Event Frequency: This option will generate an alarm only if the event occurs a user-defined number of times within a user-defined time period configured in seconds, minutes, or hours.
Event Lifetime: This option will generate an alarm if a user-defined clear event is not triggered within a user-defined period of time, designated in seconds, minutes, or hours.

You can then map alarms to automatically trigger actions. By default, no alarms will trigger actions. These must be configured by an administrator. The available actions that can be triggered will depend on the event that triggered the alarm to be generated. For example, actions that affect hosts would be available only if the trigger event was host based and could identify the host, such as the **Host Connected** event. Alarm-to-action mappings have a one-to-one association.

Vouchers & Dumps are Available | WhatsApp +201224560923

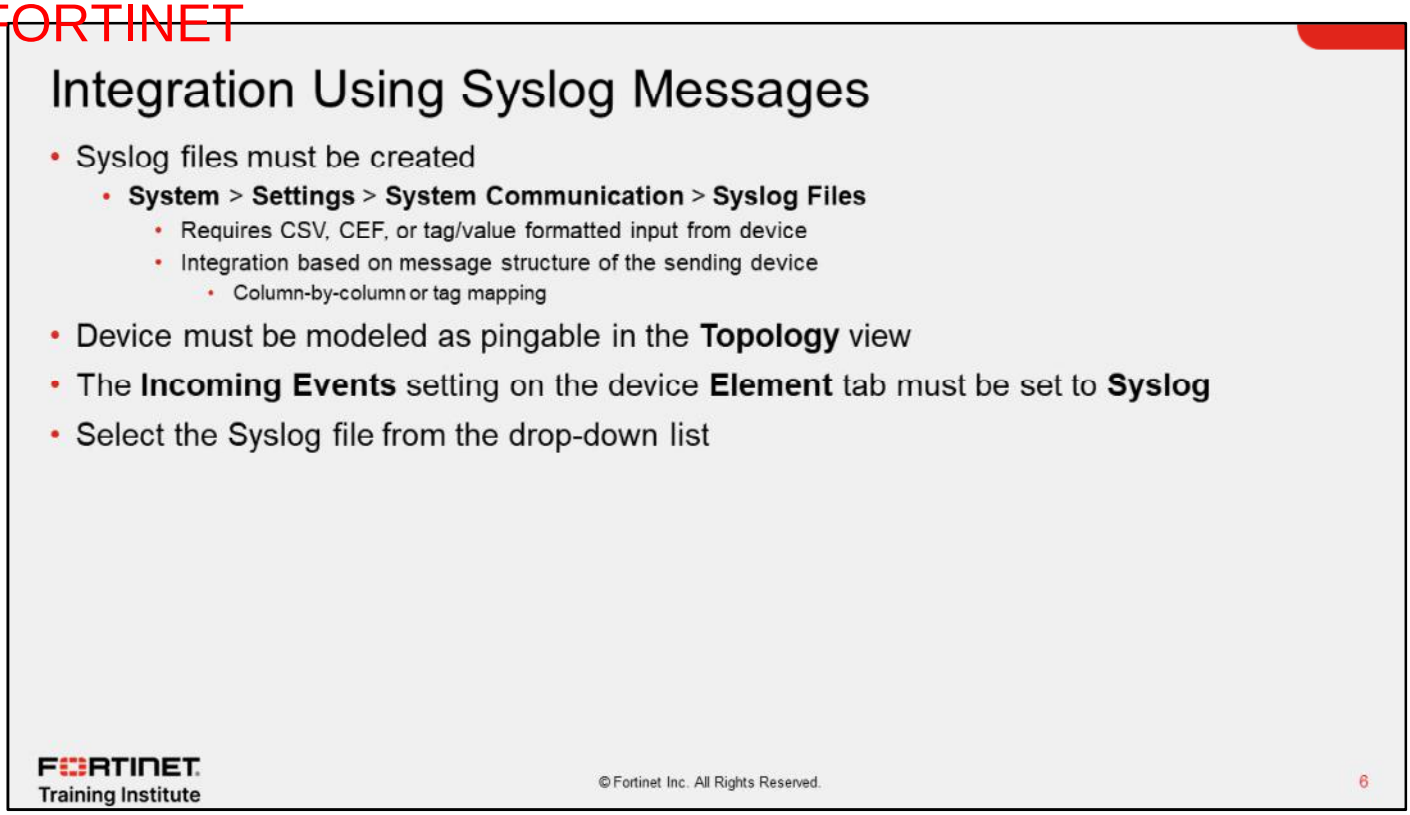
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The focus of this lesson is to learn how to create event triggers from input received from third-party devices. The input can be in the form of a Syslog message or an SNMP trap. Once the trigger has been created, the event-to-alarm-to-action flow can be configured to notify administrators or end users, as well as take host access control actions. A fundamental part of this process is the creation of a parser, so that FortiNAC can accurately identify the key components of the input it receives. A parser is then associated with the device that will be sending the input.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

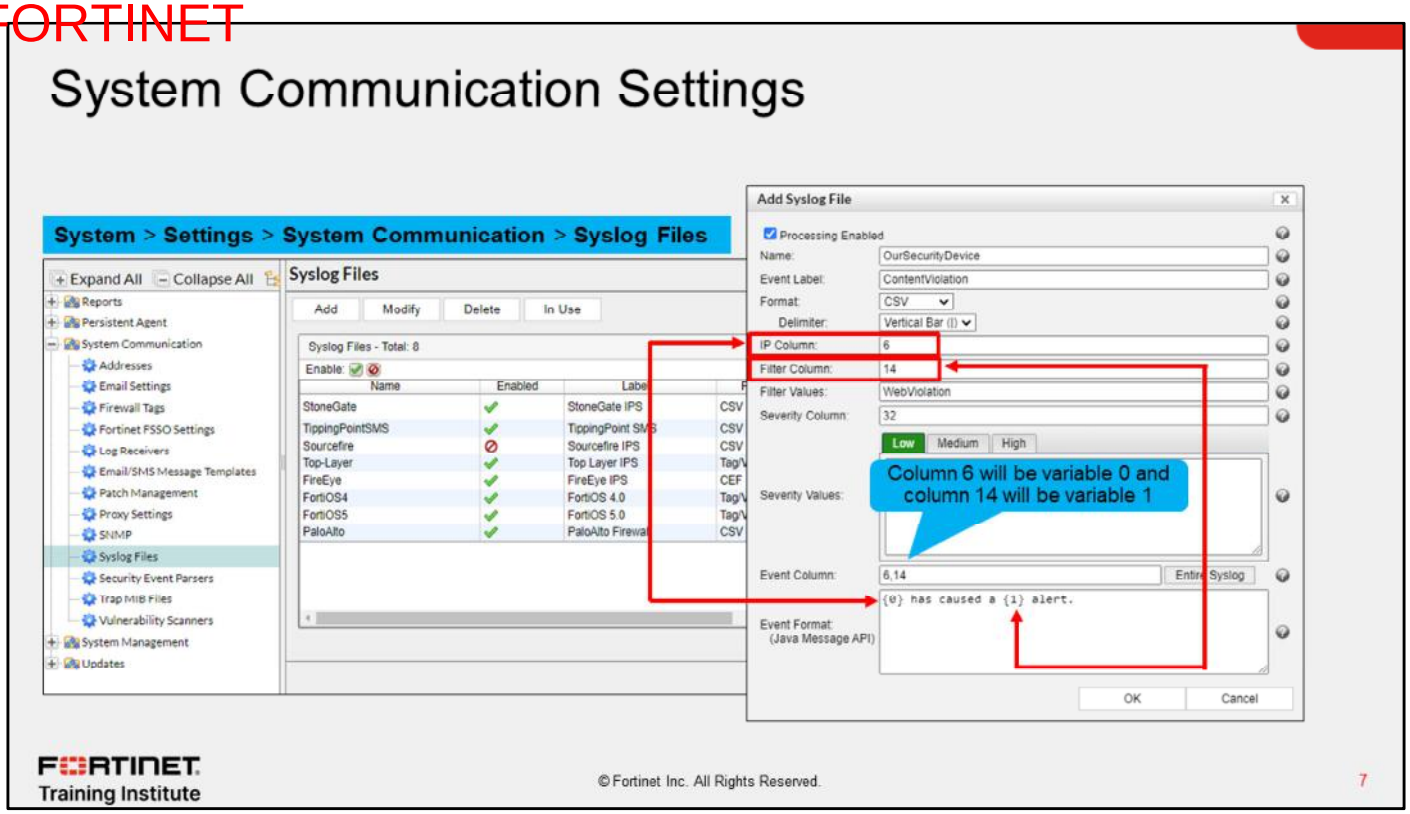


You can create **Syslog Files** for Syslog messages that are in comma separated value (CSV) format, common event format (CEF), or Tag/Value format. When using the CSV format, you can use one of three characters to designate the delimiter: a comma, space, or vertical bar. The **Syslog File** is created to parse the content of the message, column by column, or to identify the tag-to-value mapping.

Any device that will send Syslog messages to FortiNAC must be modelled in the **Topology** view. FortiNAC will not process Syslog or trap messages it receives unless the source address belongs to a topology-modelled device. As part of the modelling process, the **Incoming Events** field on the device **Element** tab must be set to Syslog so that FortiNAC understands the type of message to expect from that device. A second drop-down list will contain all Syslog files, and you should select the appropriate one for accurate Syslog parsing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To create a new syslog file, navigate to **System** > **Settings** and select **Syslog Files** from the **System Communication** branch. Click **Add** to open the **Add Syslog Files** window.

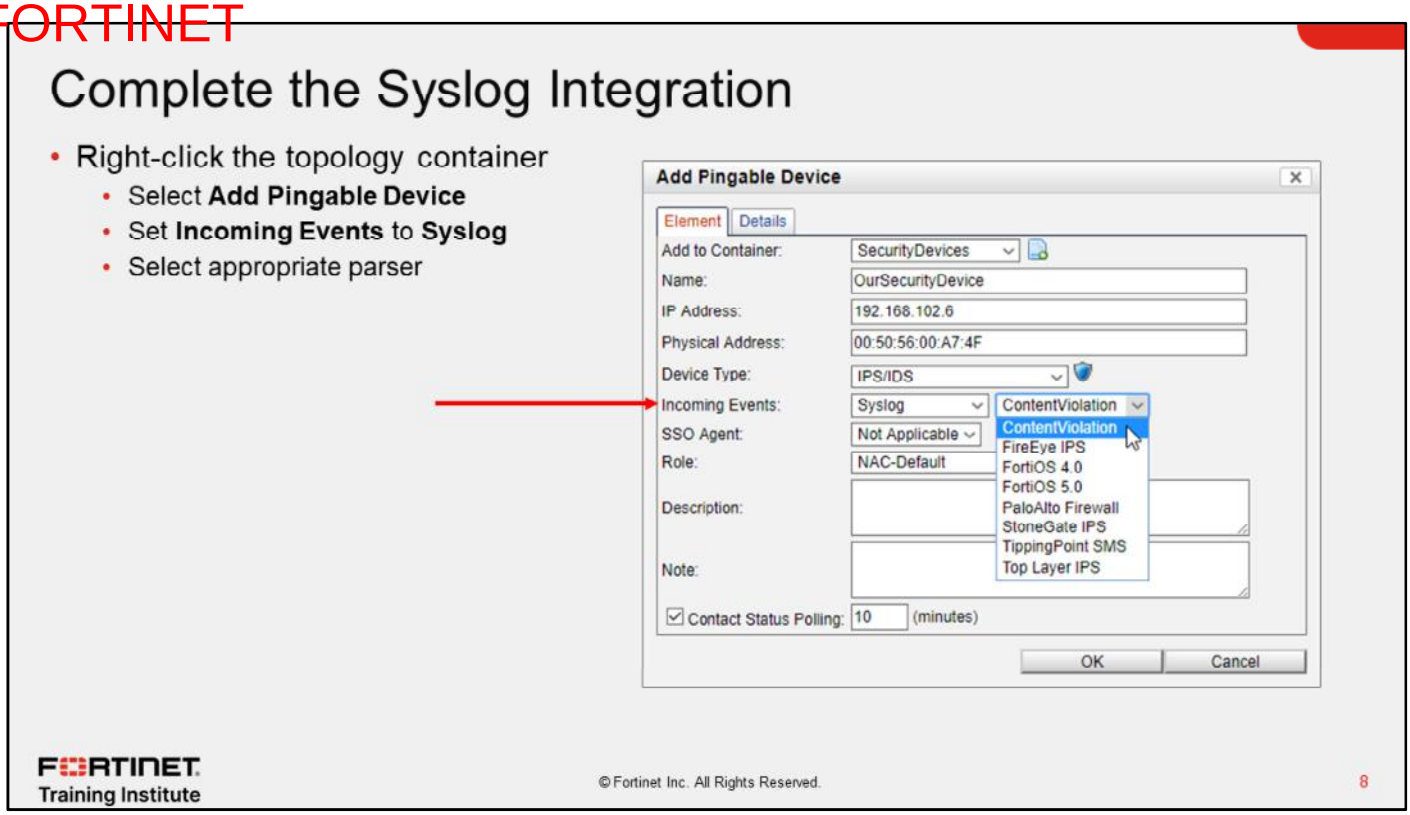
You can build a variable index **Event Column** field by indicating the fields that contain the information you want to include in the generated event. The fields that appear in the list are represented by their index location, starting with the first entry being numbered as 0 and counting up.

For example, this slide shows that the contents of column 6 will be represented by variable 0, and the contents of column 14 will be represented by variable 1.

The text entered in the **Event Format** field is the message that is displayed when the event is generated. Variables are inserted into the event text by enclosing the desired variable number in curly brackets. Events will appear in the **Logs** > **Events & Alarms** view.

Vouchers & Dumps are Available | WhatsApp +201224560923

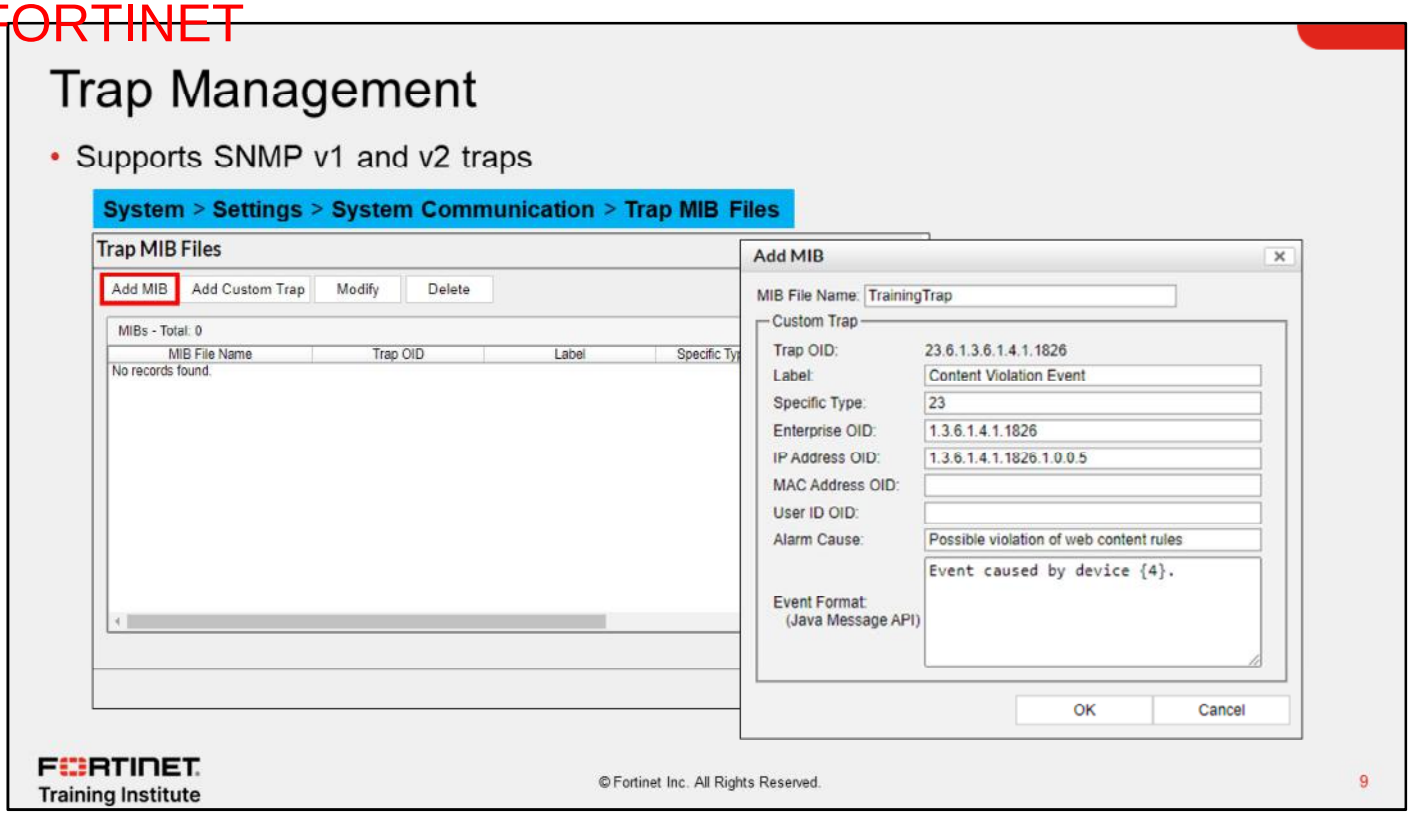
DO NOT REPRINT Brave-dumps.com
© FORTINET



When a device is modelled in the **Inventory** view as a **Pingable Device**, it will have an **Element** tab with a list of settings. For Syslog integration, the **Incoming Events** field, indicated on this slide with a red arrow, will have **Syslog** selected in the drop-down list. This defines for FortiNAC the type of message this device will send. The drop-down list on the right side will contain all of the Syslog files. Select the appropriate one for parsing Syslog messages from this device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiNAC can also process SNMP version 1 or 2 traps, and use them as event triggers. A MIB is created and will contain one or more custom traps. As a best practice, generate and capture the trap to assist in the creation of the mapping. The **Label** field is where the event name is entered. This will be the name of the new event that will be generated. This label should be alphanumeric, and not be the same as any existing event. The **Specific Type** will be a number that defines the trap as it relates to the vendor of the device. **Enterprise OID** identifies the enterprise or manufacturer of the device. For example, Fortinet has an enterprise OID of `1.3.6.1.12356`. The combination of these two values will uniquely identify the trap.

Traps will contain a varbind list. A varbind made up of an OID for an object and the data value associated with that object. FortiNAC can extract IP address, MAC address, or userid information from a trap to identify the host that caused the trap to be issued. This will allow FortiNAC to use end-user notification or host control capabilities. Only one of the fields needs to be used.

The **Alarm Cause** is for a textual description of the probable cause of the alarm. The **Event Format (Java Message API)** field is for a textual description of the event, and it can include variables pulled from varbinds within the trap. The variables are inserted by enclosing the varbind number in curly brackets. The varbind number is determined by counting down the varbind list, starting at zero. For example, the data associated with the fifth varbind down would be represented using {4}.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What is a prerequisite to FortiNAC processing a received Syslog or trap?
   - ✓ A. The device issuing the Syslog message must be modeled in the network inventory view.
   - B. The Syslog server must be visible in the host view.

2. Which Syslog formats are supported by FortiNAC?
   - A. CSV, LEEF, CEF
   - ✓ B. CSV, tag value, CEF

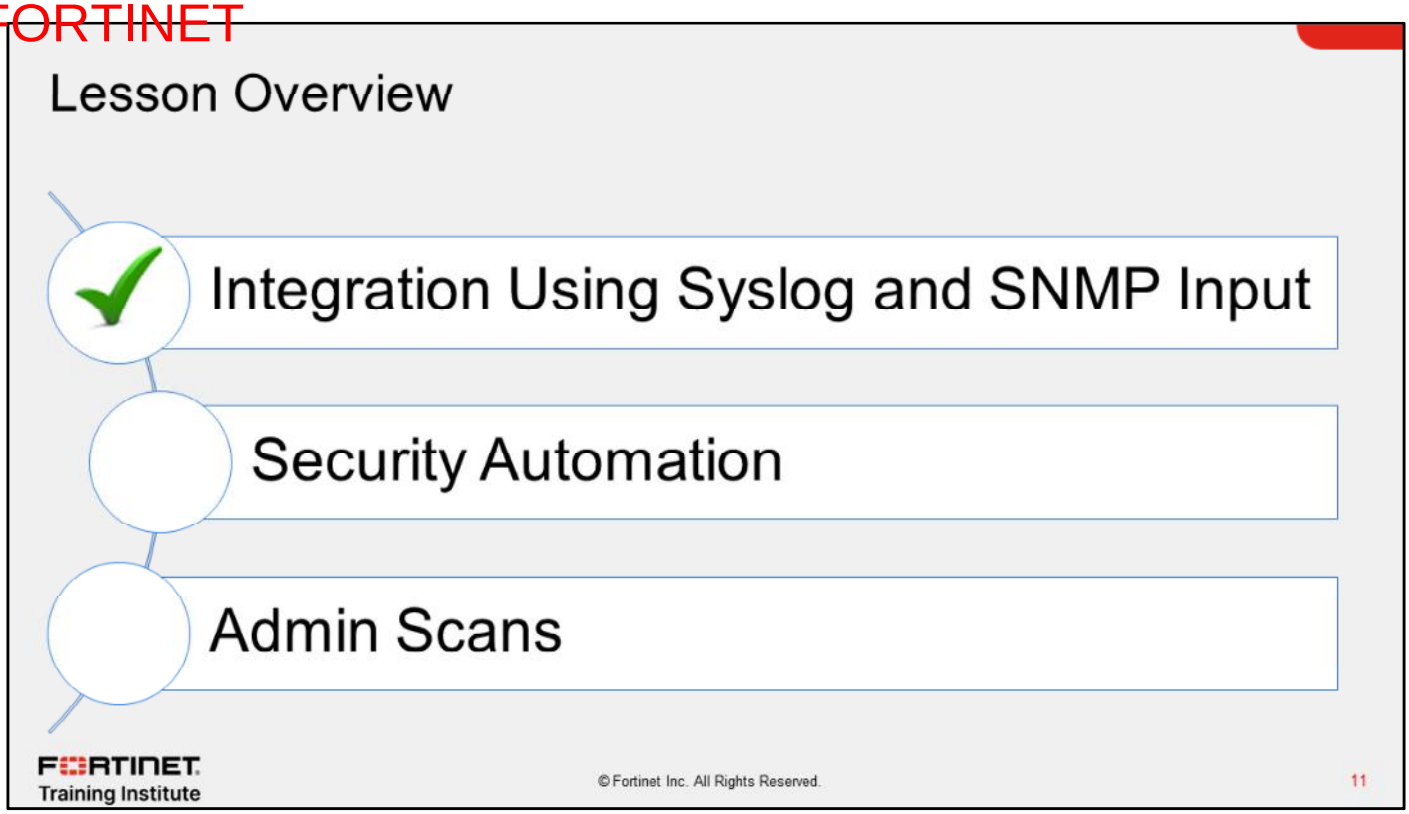
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

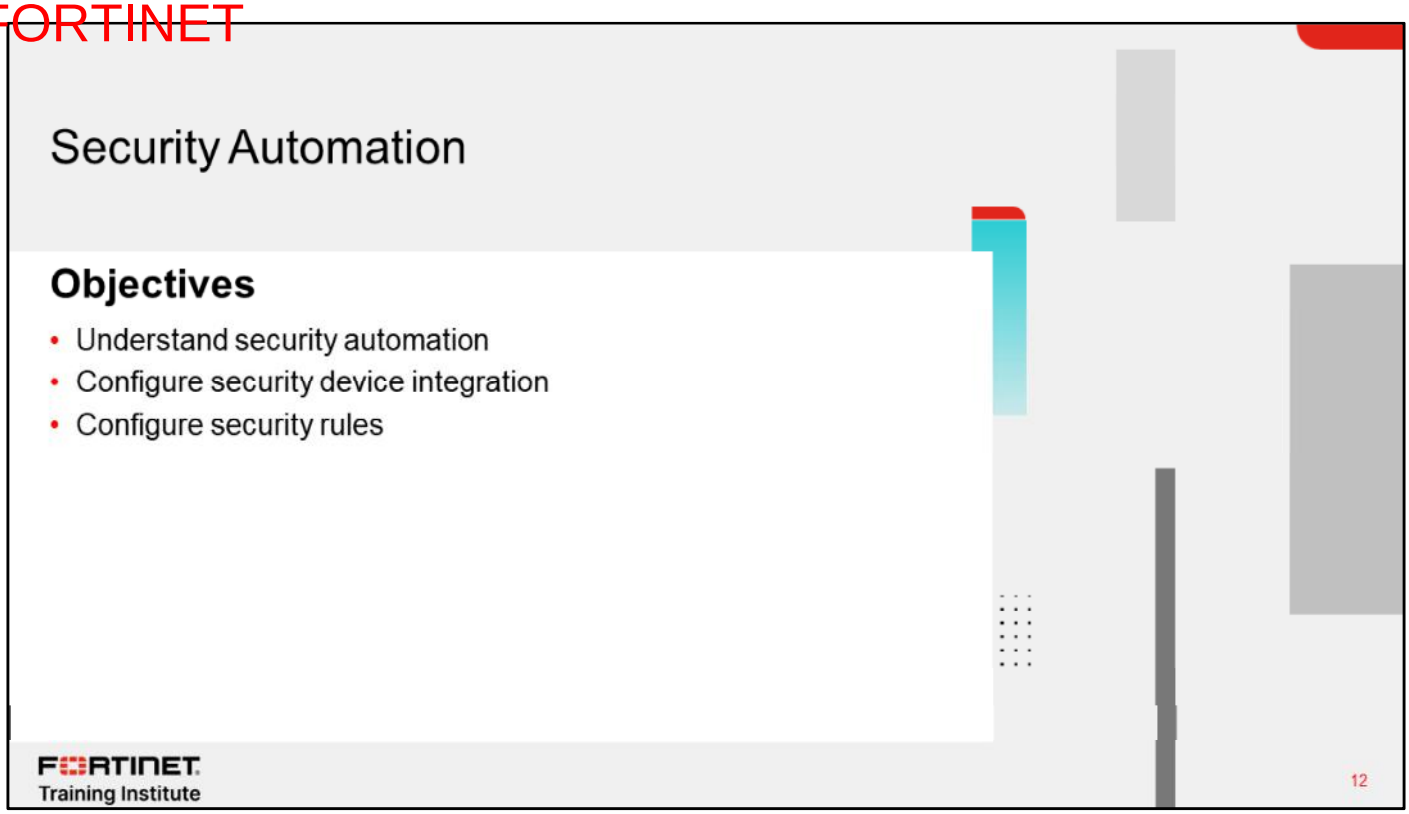


Good Job! You now understand integration using Syslog and SNMP input.

Now, you will learn about security automation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

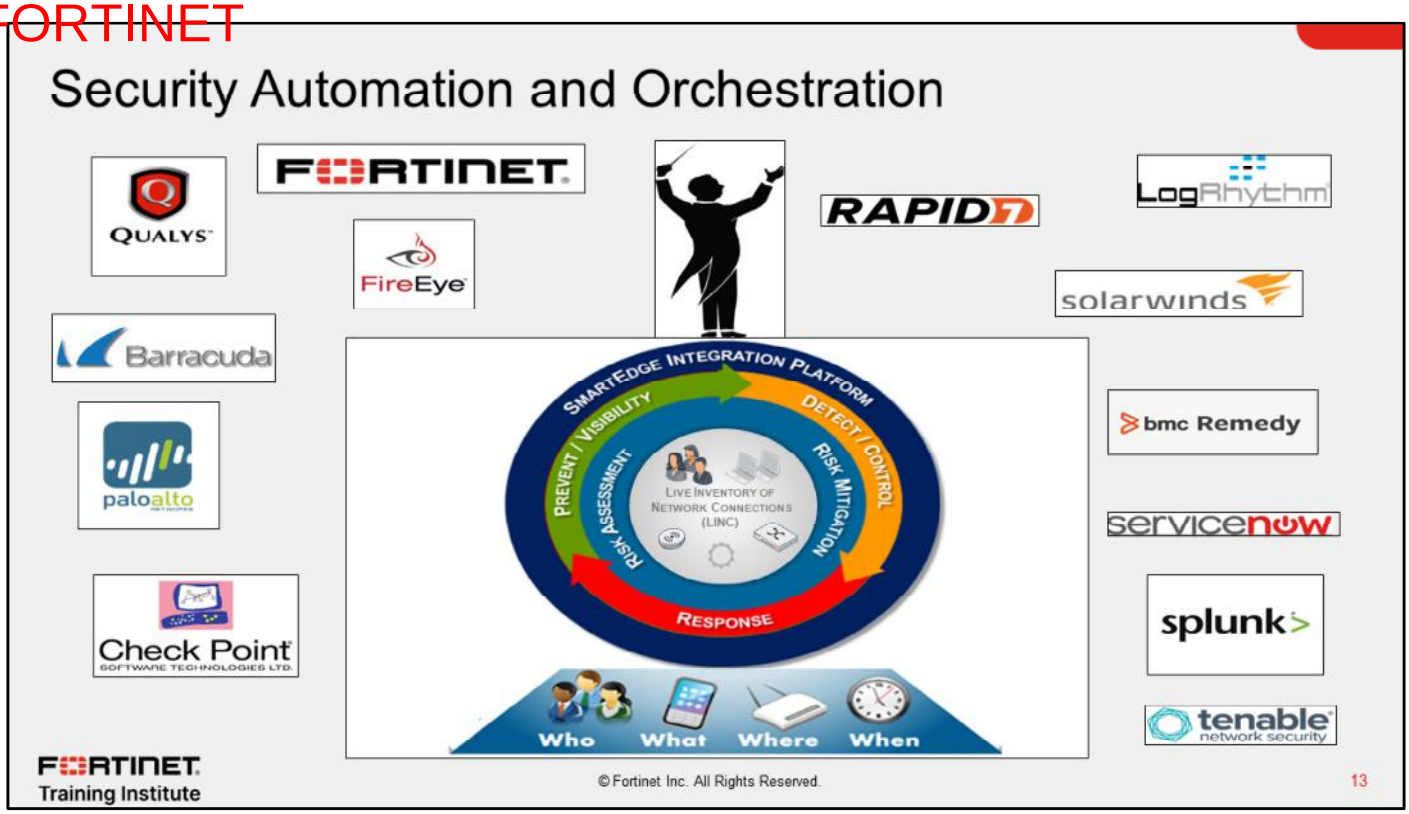


After completing this section you should be able to achieve the objectives shown on this slide.

By understanding the concepts and configurations of security automation, you should be able to leverage FortiNAC to integrate with security devices and execute workflows for dynamic threat mitigation and control in your environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

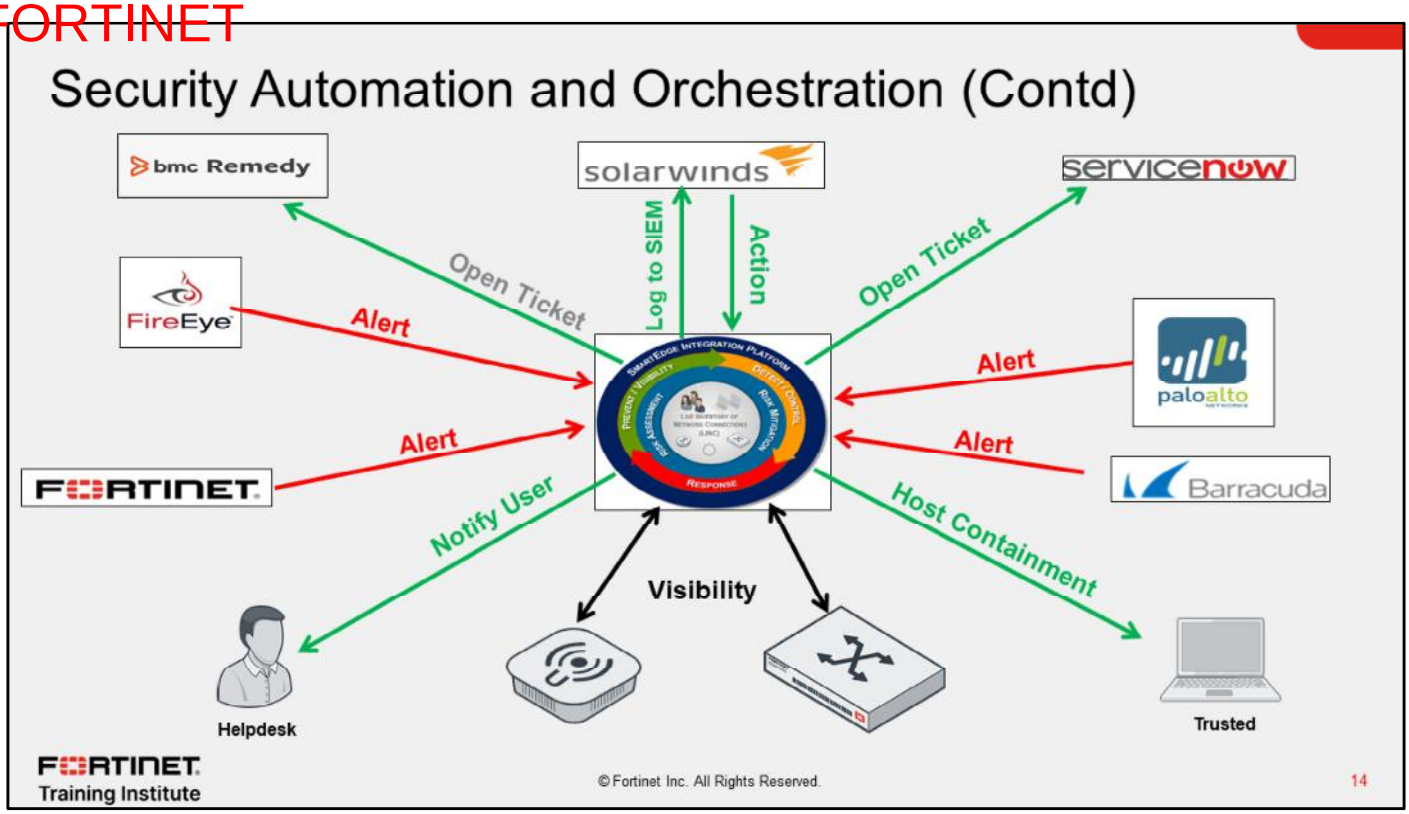


The ability to orchestrate network security processes with FortiNAC empowers an organization to automatically control network access, and respond using detailed workflows designed around received security alerts.

Visibility provides the context necessary to correlate received alerts, and control provides the ability to mitigate or notify based on administrator-defined work flows. The ability to integrate with nearly any device expands the endpoint-based visibility to include real-time knowledge of potentially threatening behavior. The integration is bi-directional, meaning FortiNAC can pass detailed information upstream as well as receive it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

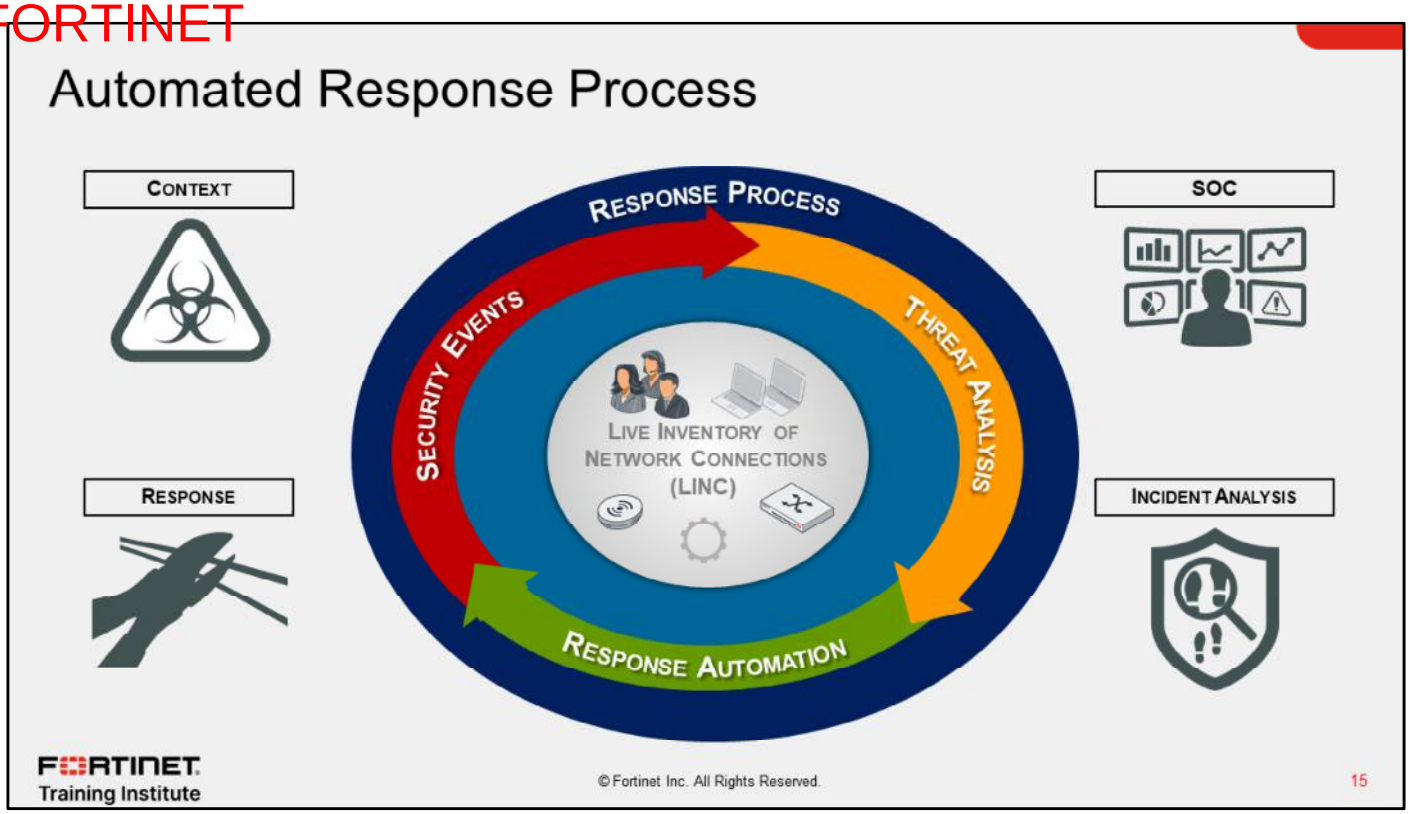


The policy-based platform, leveraging complete end-to-end visibility with the integration of these tools enables the creation of preventative network access and threat triage processes to automate NOC provisioning and SOC threat response procedures.

Security orchestration is the combining of the visibility, detection, control, and response capabilities to create automated prevention processes. The detailed workflows are created to notify, update, log, and provision based on the alerts received from external sources in conjunction with visibility details stored in the FortiNAC database.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



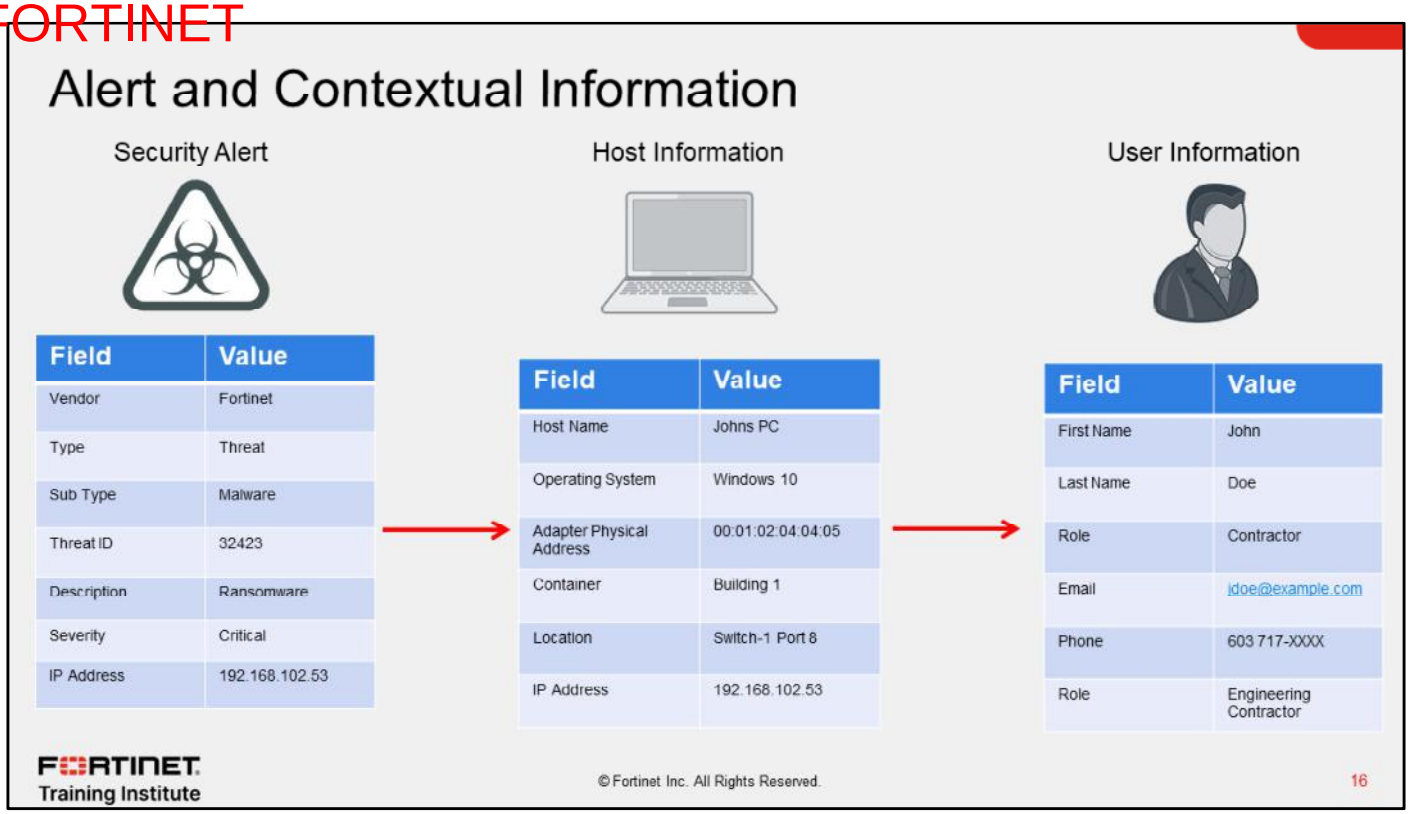
FortiNAC processes the inbound security events, correlates the contextual visibility information, performs detailed analysis of the events against defined security rules, and performs the appropriate action or response to take for that specific incident.

The development of these security rules follows a circular process. Security alerts are processed. The organization determines the desired response to the specific situation, for example, a particular security alert caused by a specific host or user. Then a security rule is created to respond the next time the situation occurs.

Then the process begins again. As more and more security rules are created, there'll be fewer and fewer alerts that need to be manually processed or evaluated.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

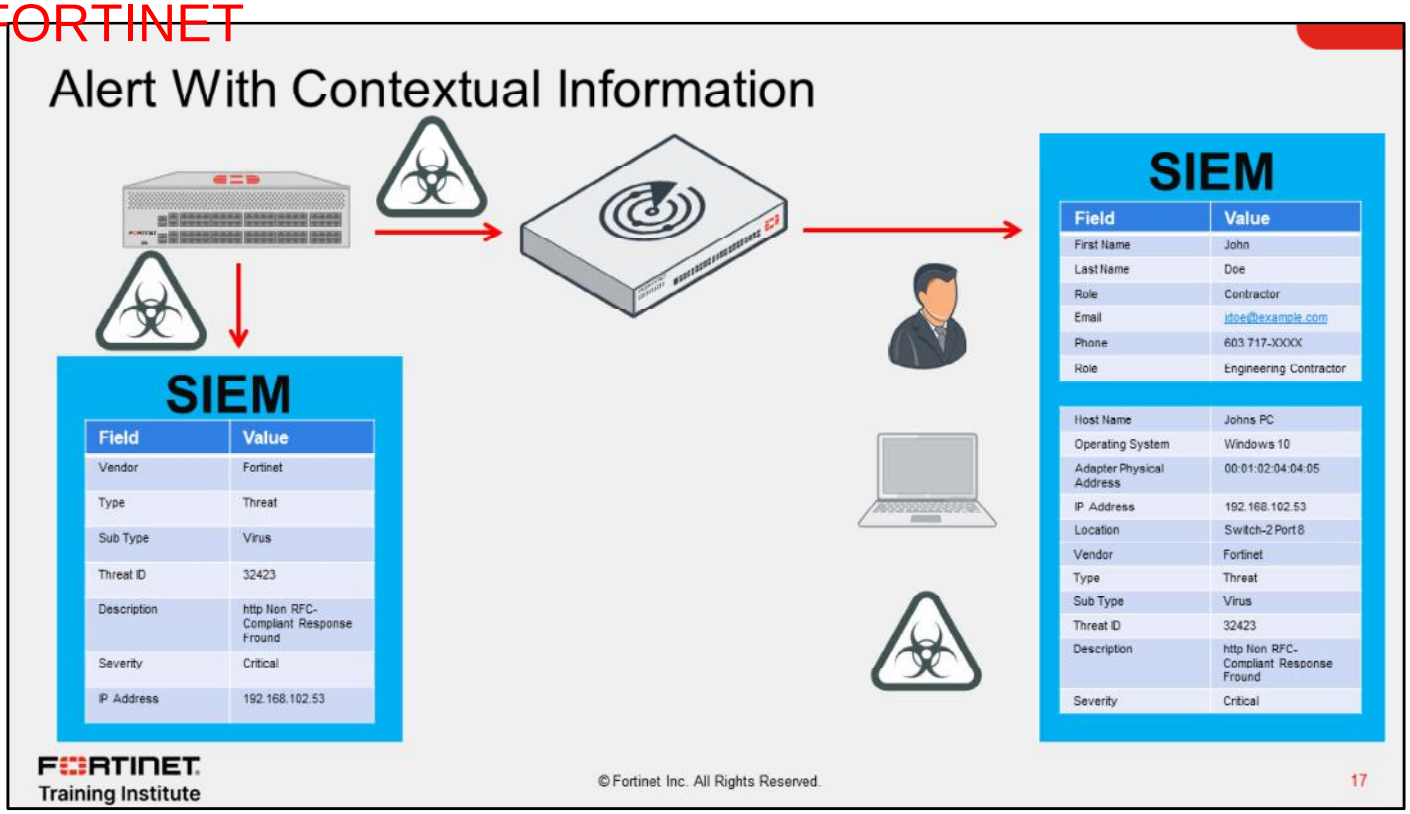


The example shown on this slide displays some of the information that may be received by FortiNAC in the form of a security alert. This information will be combined with the visibility information that exists within the FortiNAC database and will include all of the host and user attributes. For example, you would know the host by name, physical address, IP address, location, and so on, as well as the user information, such as name, email, and phone extension. This provides important information to those that are making the decisions on how to handle this particular type of alert, and helps determine what type of work flow should be designed.

The key attribute that makes the association between the security alert and the host is the IP address. The user information can be both the user that registered the device in a BYOD situation, and the currently logged on user.

Vouchers & Dumps are Available | WhatsApp +201224560923

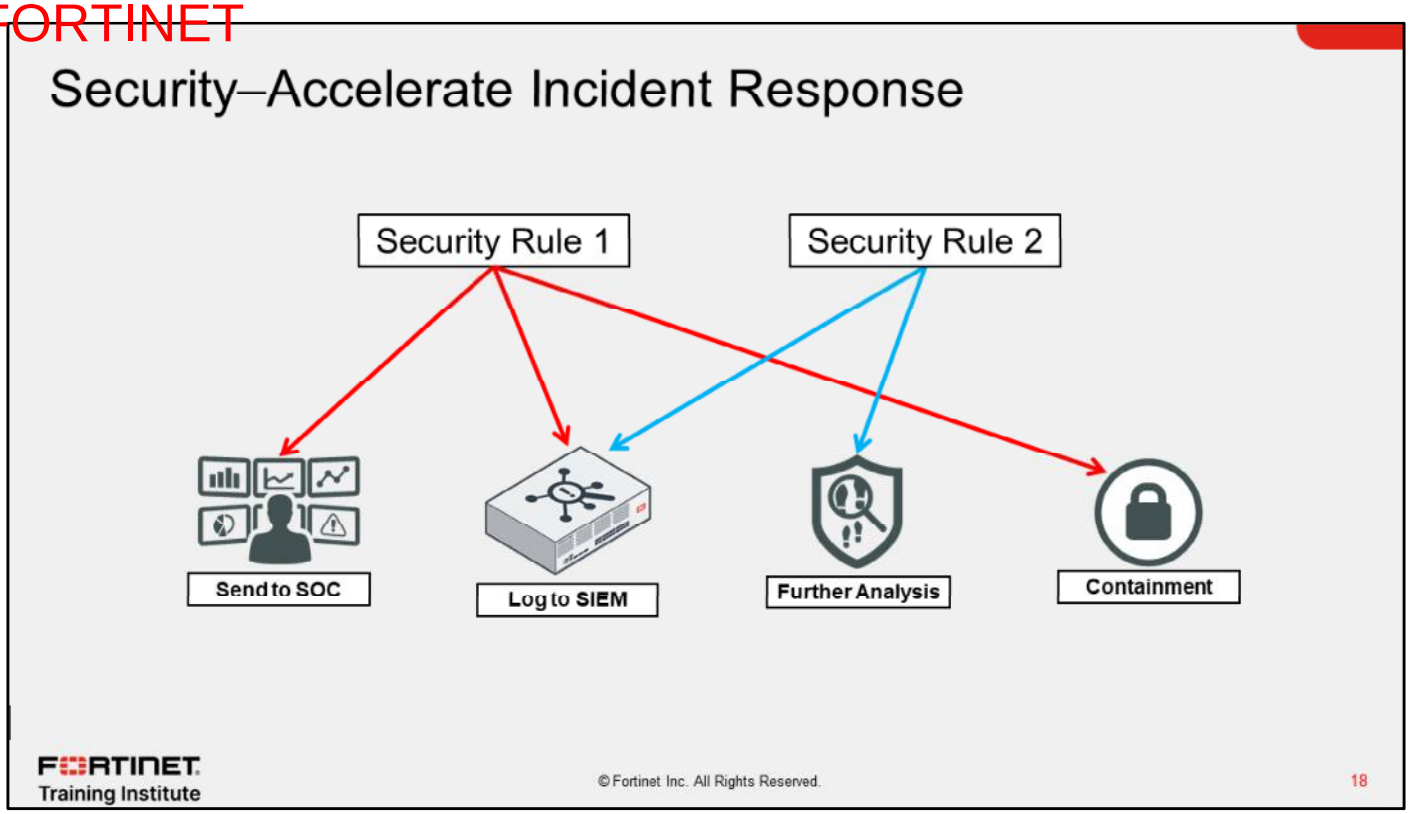
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Adding the detailed contextual information can be done by directing security alerts to FortiNAC. FortiNAC could then be configured to forward the combined information, alert, host, and user details upstream by designating a log host, as discussed in a previous lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



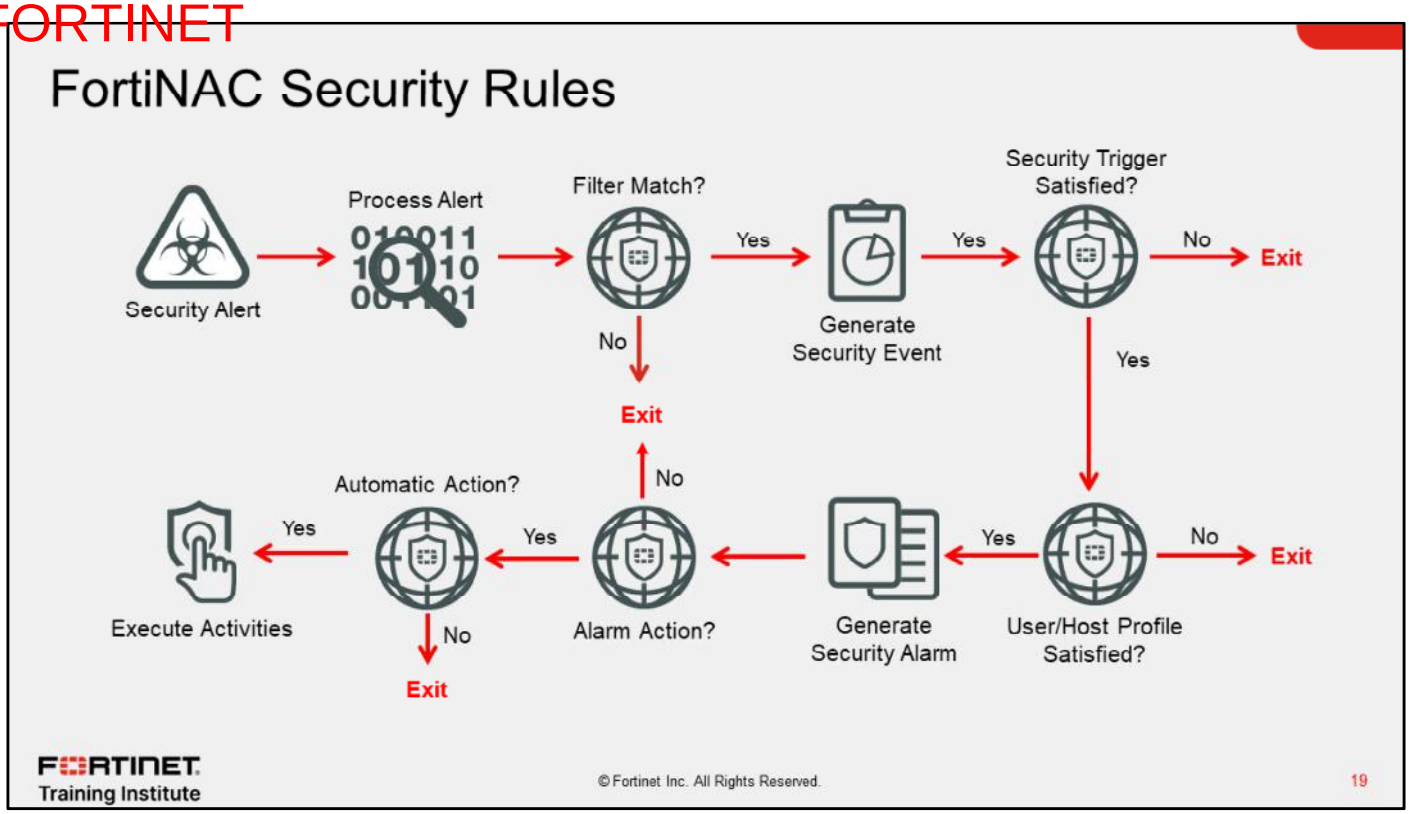
Security automation is enabled through the creation of security rules. These rules can include the actions, or work flows, desired for automated response. Each security rule can execute any number of associated tasks, allowing you to create responses with varying levels of detail. Security rules are ranked and each received security alert is evaluated against each rule in the ranked order until a match is found. If no match is found, no action is taken.

The example shown on this slide depicts two security rules, each with multiple associated actions. If a security alert is received by FortiNAC that matches security rule 1, the associated host will be moved to the quarantine isolation network, the alert, host, and user information will be logged on the SIEM and a notification with those details will be sent to the SOC. If security rule 2 is matched, the alert, host, and user information will be sent to the SIEM and passed along for further analysis.

Security alert information passed along for further analysis is normally the starting point for new rule creation. As the alerts are more fully understood, new work flows can be created to automate the responses and new rules can be created to leverage those work flows.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Understanding the terminology used, and a fairly detailed explanation of the process, goes a long way in understanding how the FortiNAC security rules work, and simplifies their development.

Starting with the top row in the example shown on this slide, and reading left to right, the process begins with the receipt of a security alert. A security alert is the Syslog message received from an integrated security device. The alert is processed by FortiNAC, which means that the message contents are parsed and each component evaluated. The contents are then compared to all existing filters.

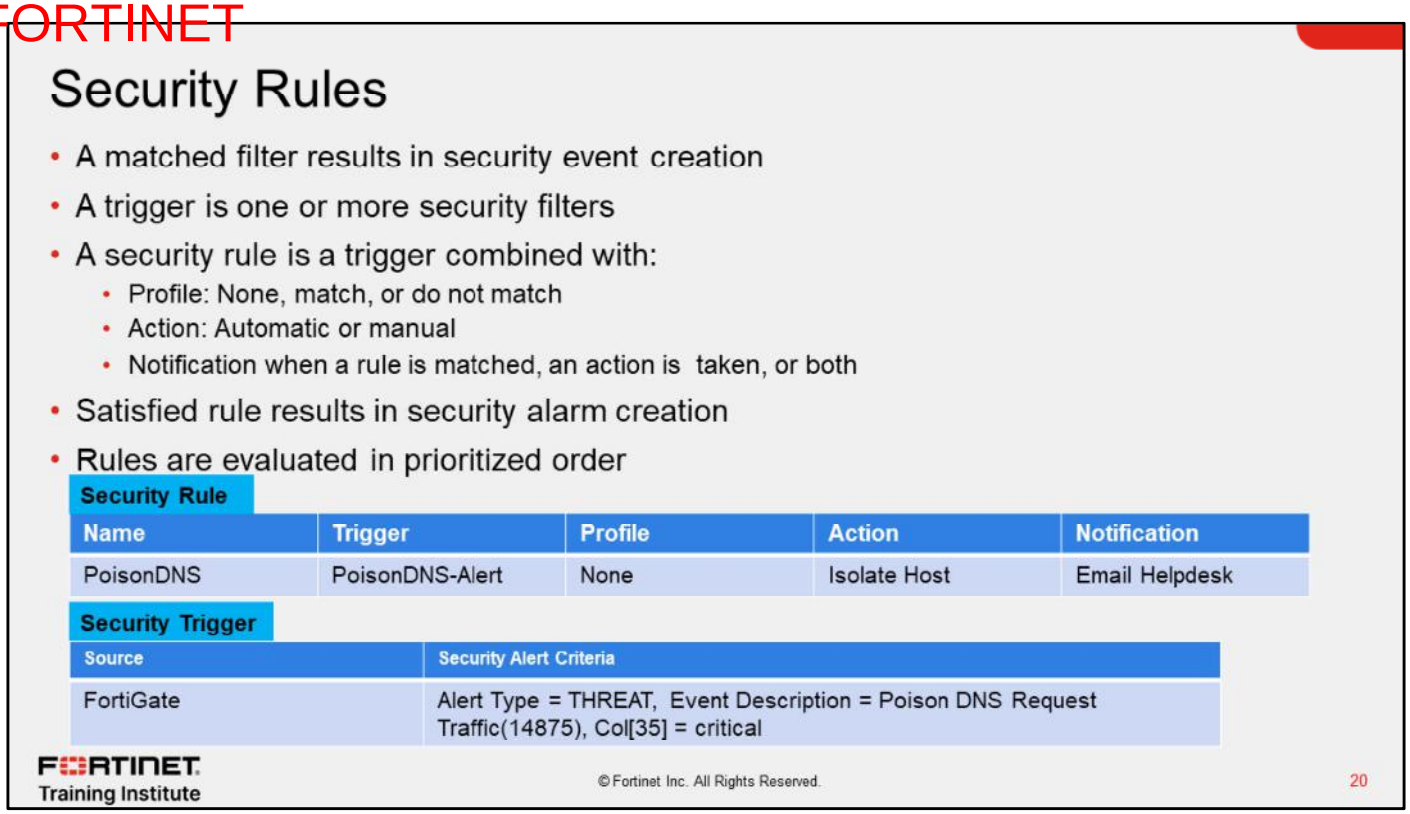
A filter is a user-created set of criteria. For example, a filter could simply look at the contents of column 35 of the parsed security alert and check to see if the value matches the defined requirement. Or, it could require the match of many columns of information. If no filter is matched, the process exits and nothing occurs. If a filter is matched, a security event is generated.

In this next step, FortiNAC evaluates all security triggers. A security trigger is made up of one or more filters. Logic can be applied if there is more than one filter making up a trigger, for example, one, all, or a subset of the filters may need to be matched within a defined period of time. If all criteria are matched for the trigger to be satisfied, FortiNAC evaluates any associated **User/Host Profiles**. These are the same profiles covered in the security policy lesson. Just as before, they are used here to leverage who, what, where, and when visibility information. The inclusion of a user/host profile allows an administrator to create different workflows for different endpoints, even if the trigger being matched is the same. If both the trigger and any associated user/host profile are satisfied, a security alarm is created.

The final step is were the workflows can be defined. If the security rule has an associated action, that action can be carried out in an automated or manual manner. Actions are one or more activities. These activities are the automated responses, and can include notification actions, network access actions, or script execution.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To summarize what was discussed on the previous slide:

A filter is a set of defined criteria evaluated against the contents of a parsed security alert. Any field contained in the security alert can be used as part of a filter. Some fields are normalized, meaning they are mapped to specific field names, such as Severity, Source Address, and so on. Other fields will be identified using column numbers or tag values. When a filter is evaluated, all designated criteria must match for a true result. When a filter evaluation returns a true result, a **Security Event** is generated.

A trigger is one or more filters. A time occurrence requirement can be configured defining a window of time setting for two or more filters. For example, the trigger could be satisfied if all or a subset of the filters are matched within 2 minutes. If all trigger criteria are satisfied, a user/host profile requirement can be added.

The logic that can be applied to the user/host profile requirement options are:
- **None**: No user/host profile requirement
- **Match**: The user or host element associated with the security event must match the profile
- **Do Not Match**: The user or host element associated with the security event must not match the profile

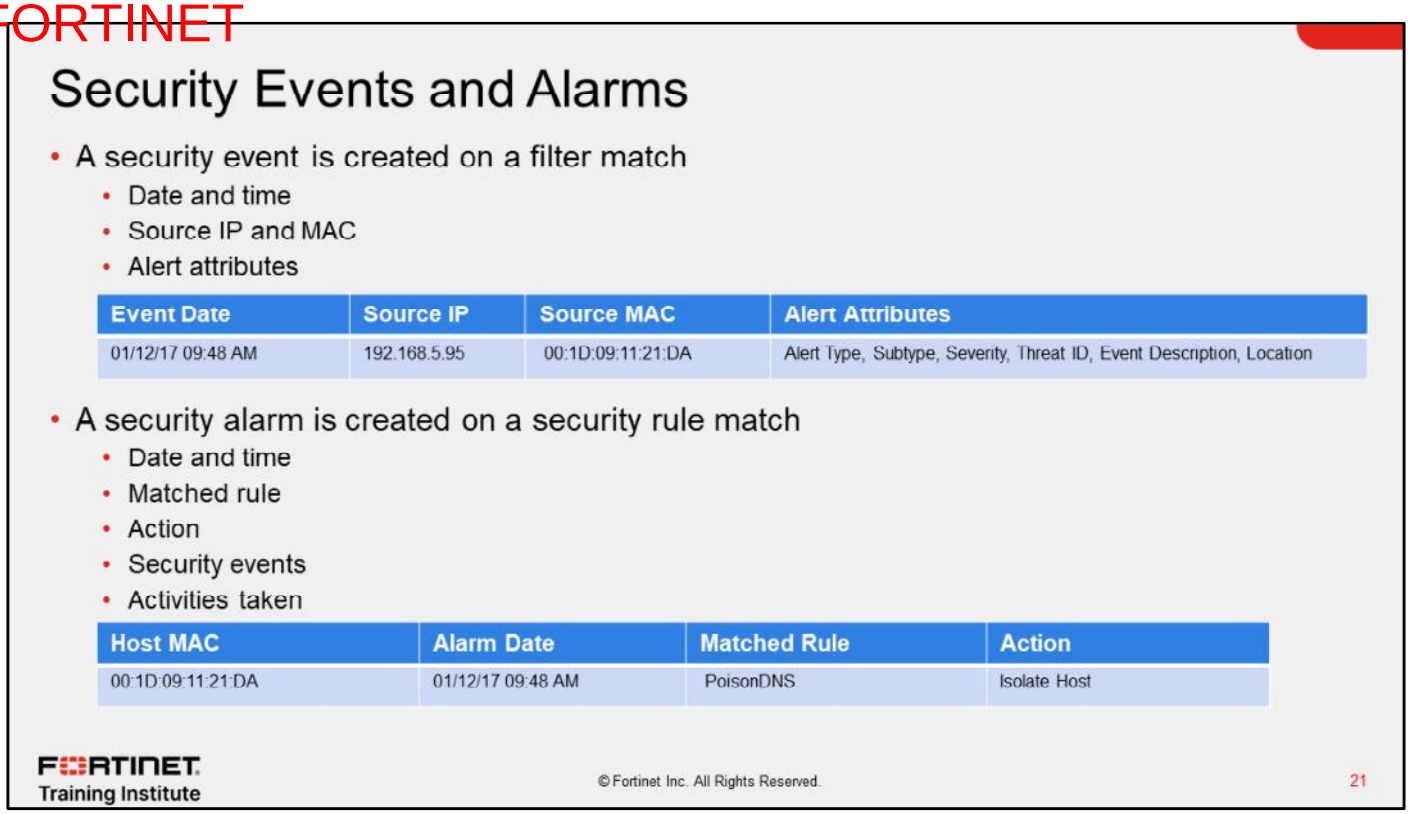
If the trigger is satisfied, and the user/host profile requirement is met, a **Security Alarm** is generated and any associated actions are executed. An action consists of one or more activities. Activities are the wide variety of tasks FortiNAC can perform. For example, an action could consist of the activities needed to mark a host at risk, change the host's role value, and/or send a message to the host.

Security rules are evaluated in order of priority.

The examples shown on the bottom of this slide highlight the components of a **Security Rule** as well as those of a **Security Filter**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Any time a filter is matched, a security event is generated. Security events will contain the following information about the host that caused the security alert to be issued:

- Date and time
- Source IP
- Source Mac
- Destination IP
- Location

The security event will also contain the Alert Type, Subtype, Severity, Threat ID, and Event Description of the security alert.

A security alarm will contain the host MAC, alarm date and time, the security rule that was matched, and any actions taken.

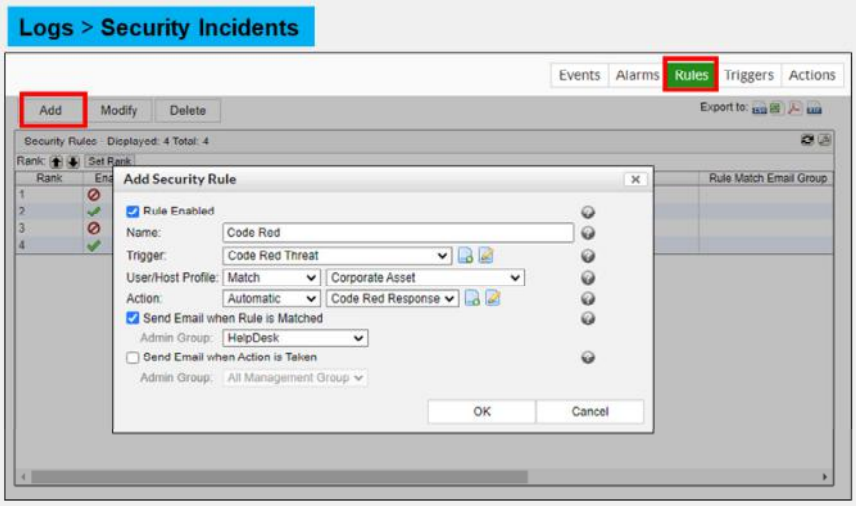
Note, that for each security alarm generated, there will be at least one associated security event. Recall that a trigger could contain more than one filter, and each matched filter would generate a security event. For example, a trigger that requires two filters to be matched, would have two security events associated with the security alarm each time the trigger was satisfied.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Creating Security Rules

- Uses triggers and user host profiles to generate security alarms
- Associated actions can be performed manually or automatically with rule match
- Email notification settings



FORTINET Training Institute

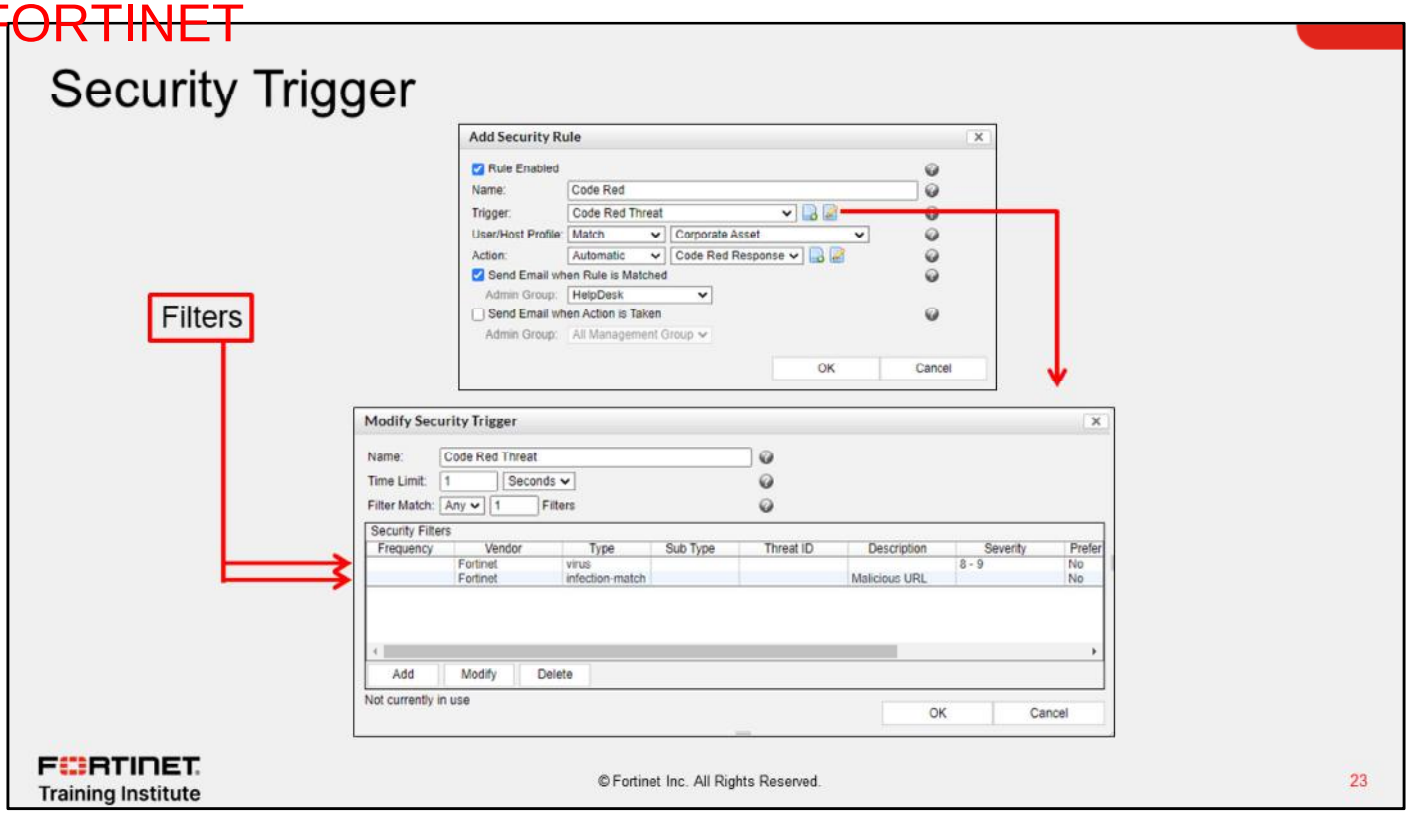
© Fortinet Inc. All Rights Reserved.

22

You create security rules in the **Security Incidents** view, on the **Rules** tab. In the upper-right corner, click **Rules**, then click **Add** to open the **Add Security Rule** window. This window allows you to enable the rule, give the rule a name, and then select or build each of the different components that make up a security rule. The icons to the right of each component allow you to create new components or edit the existing selected component. You can define notification settings to notify administrative group members each time the rule is matched, an associated action is taken, or both.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The manual configuration of a **Security Trigger** consists of entering a **Name**, defining the associated **Security Filters** requirements, any **Time Limit** requirements in **Seconds**, **Minutes**, or **Hours**, and the **Filter Match** criteria.

The **Name** must be unique among existing security triggers.

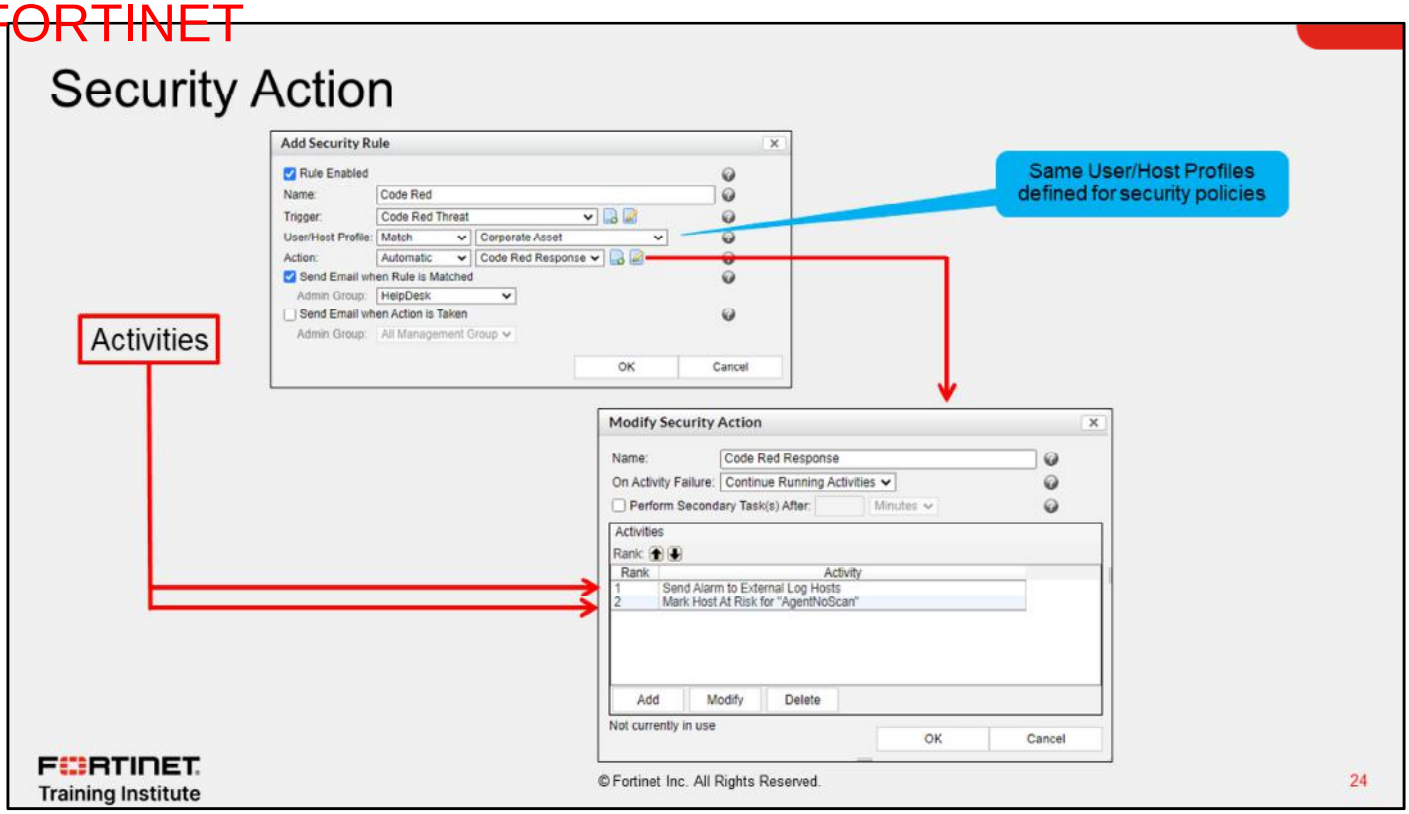
Create **Security Filters** by clicking the **Add** button. Each filter consists of the necessary values, by field, required to identify a matching security alert. You must define one or more of the fields, and all defined fields are logically ANDed together.

Use the **Time Limit** setting in conjunction with the **Filter Match** setting to define if **Any** filter match will satisfy the trigger, or if a subset of filters matched within the **Time Limit** will be required.

You can simplify trigger creation by building the filters directly from existing security events, which will be described later in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **User/Host Profile** setting is primarily used to create different responses based on the same **Trigger** being satisfied by different types of users. For example, you may want to handle an alert differently if it were caused by a guest, as opposed to if it were caused by a contractor, or employee. These **User/Host Profiles** are the same ones used by security policies, and any existing profiles will be available in the drop-down list. Icons to the right of the drop-down list allow you to add a new profile, or modify the currently selected profile. Recall from earlier in this lesson that the profile requirement can be set to **None**, **Match**, or **Do Not Match**.

The **Action** drop-down list within a security rule offers three options: **None**, **Automatic**, and **Manual**. These options define if and when the associated action is performed. A setting of **None** does not perform any action, **Automatic** performs the action as soon as the security alarm is generated, and **Manual** does not perform the action until it is initiated by an administrator.

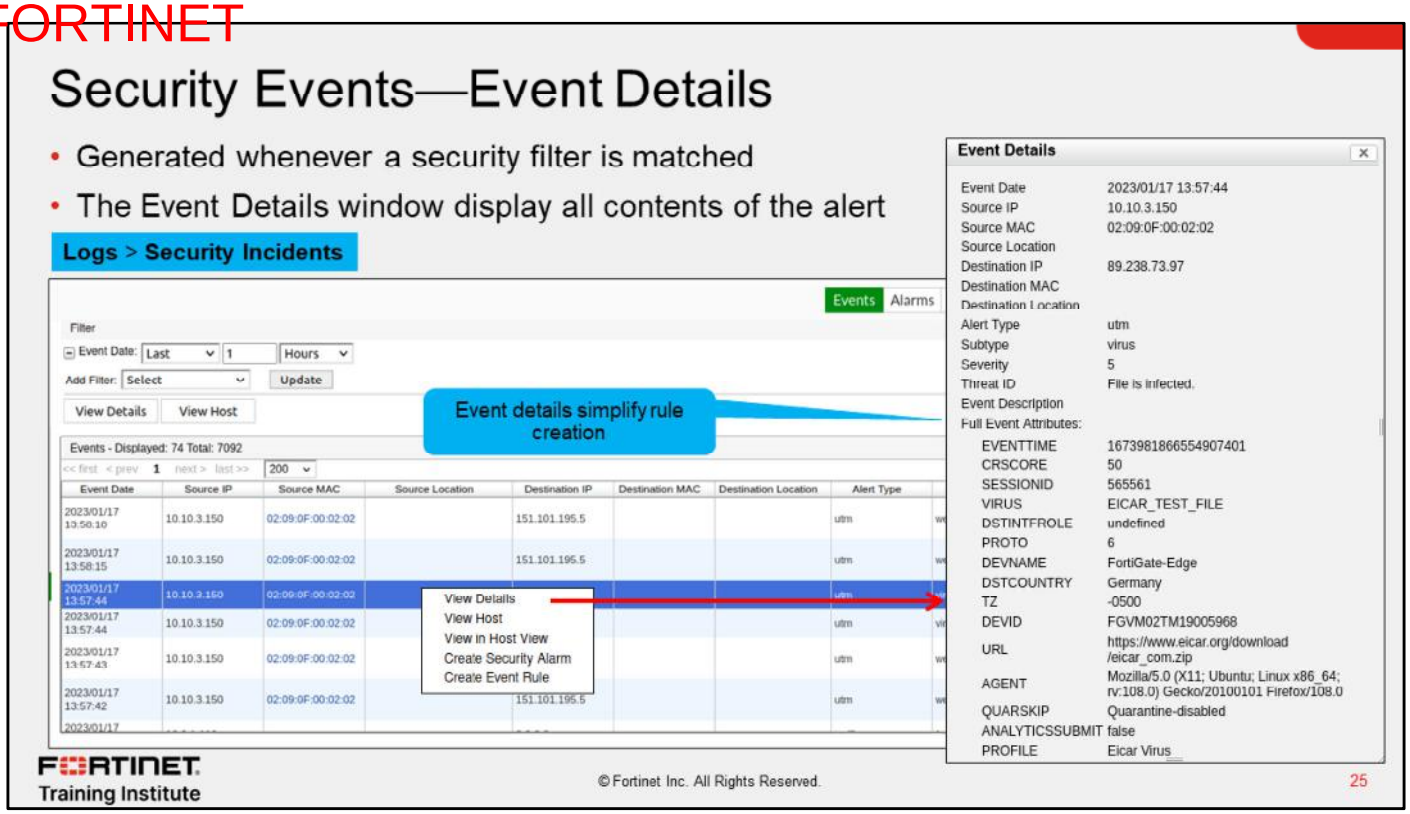
The second drop-down list contains all the existing actions, if any. To the right of the second drop-down list are two icons that provide the ability to edit the currently selected action or to create a new action.

The creation of an action begins with providing a unique **Name** and setting in the **On Activity Failure** configuration. The **On Activity Failure** setting defines how FortiNAC will proceed with the execution of **Activities** in the event an activity fails to execute successfully. Activities are organized in a ranked order and executed in that order. The options are to **Continue Running Activities**, ignoring the failed one, or to **Stop Running Activities**.

Activities are added to the list using the **Add** button. There is a long list of available options ranging from administrator or user notifications to port-based and host access control.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

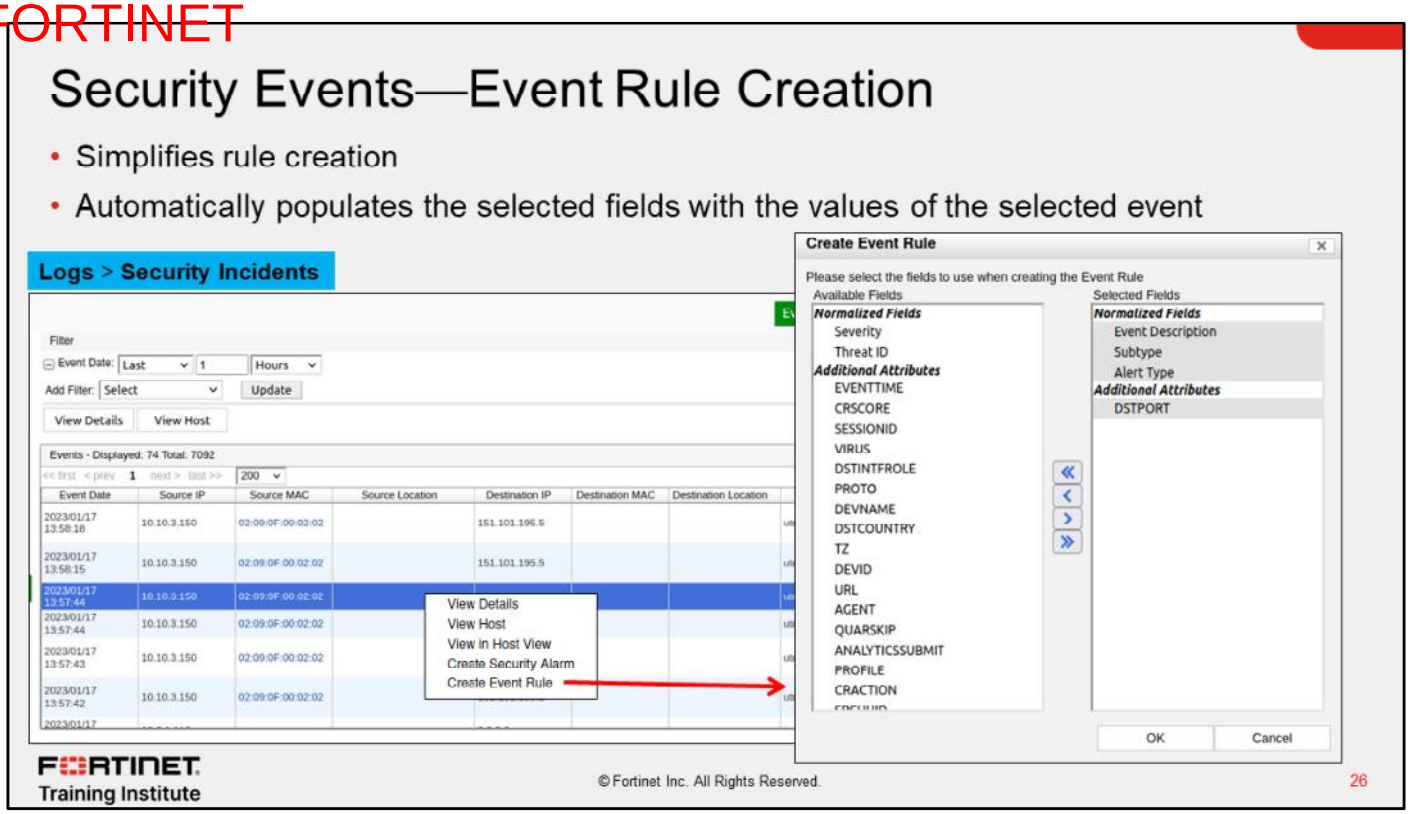


Security events are generated whenever a security filter is matched, even if the filter is used within a security trigger that is not satisfied. For example, if a security trigger requires two security filters to be matched in order to be satisfied, and only one filter is matched, the matched filter will generate a security event; however, the trigger is not satisfied.

Security events can be used to create new security filters and security triggers. Right-clicking a security event and selecting **View Details** or clicking the **View Details** button, opens the **Event Details** window. The **Event Details** window shows the complete contents of the parsed security alert. The data presented first in this view are all the normalized fields, meaning FortiNAC maps the content to the appropriate filed, such as **Source IP**, or **Event Date**. This view is helpful for determining which attributes to key on in order to create a filter that will identify this security alert, if it is received again.

Vouchers & Dumps are Available | WhatsApp +201224560923

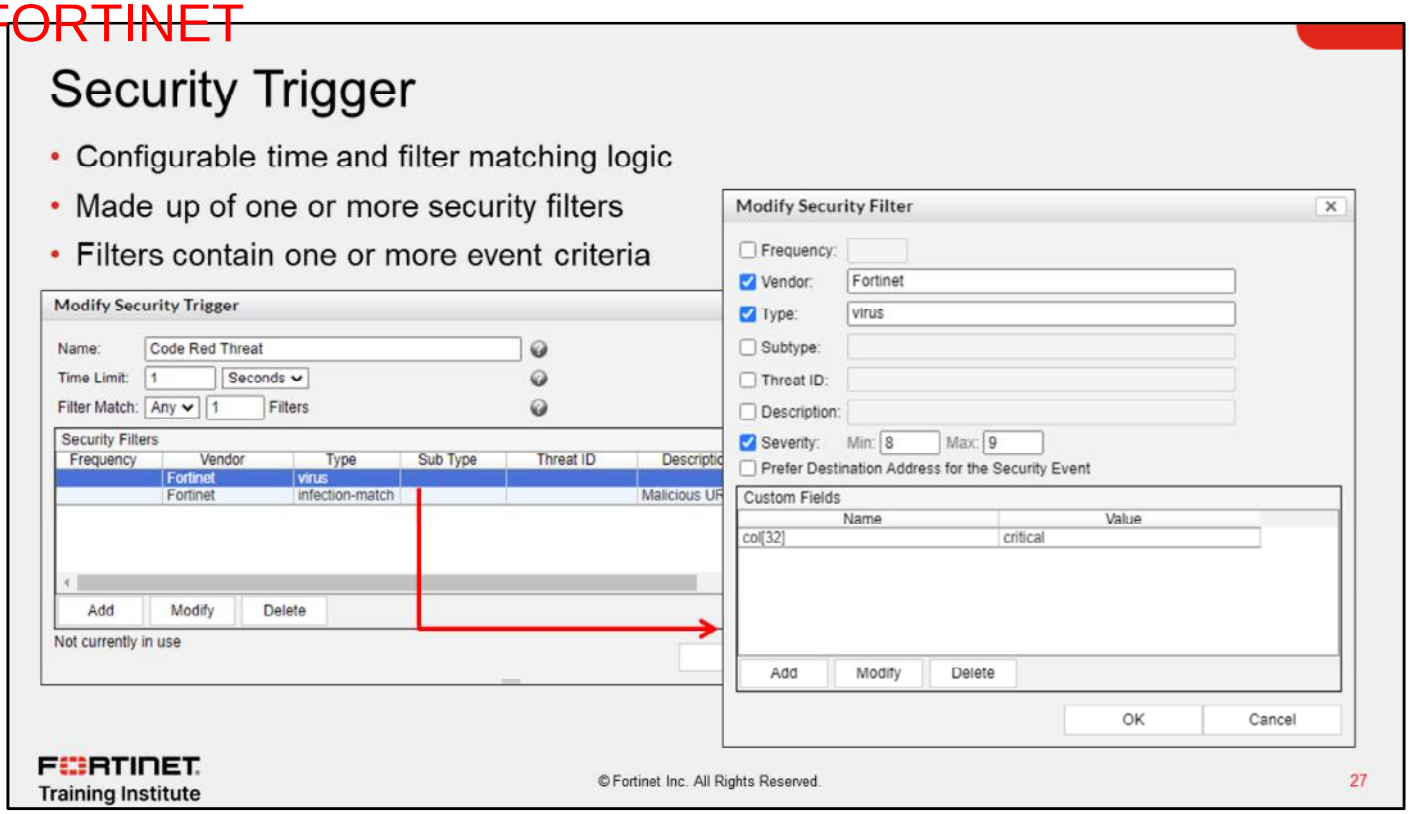
DO NOT REPRINT Brave-dumps.com
© FORTINET



You can create security filters from existing security events, which allows you to create triggers quickly. Right-clicking a security event and selecting **Create Event Rule** opens the **Create Event Rule** window. On the left side of the window, in the **Available Fields** list, the entire contents parsed from the received security alert is displayed. **Normalized Fields** are shown at the top of the list, while all other data is displayed as **Additional Attributes**. The administrator can select any fields on the left and move them to the right using the arrows that are shown between the fields. Clicking **OK** opens the **Add Security Trigger** window with a **Security Filter** automatically created from the selected fields. Any selected field associates that field with the value that currently exists in the parsed security alert. For example, if the **Severity** field in the selected event contains a value of **Critical**, the resulting security filter evaluates that field for that value.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



An administrator can view the **Security Filter** from within the **Add Security Trigger** window. The **Modify Security Filter** window shows each of the selected fields from the previous step, as well as the contents of each field. In the example shown on this slide, the normalized fields, and the values associated with them, appear in the top portion of the window with a checkbox preceding each field name. The **Custom Fields** portion of the window displays all selected fields that were not normalized by FortiNAC.

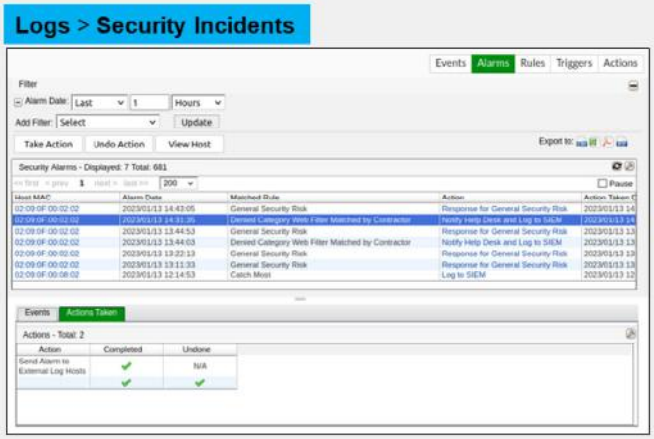
The mapping that determines which fields will be normalized is defined in the security event parser configuration window, which will be discussed in the upcoming slides. Clicking **Add** in the security trigger window allows an administrator to create security filters manually.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Security Alarms

- Generated when all trigger requirements are met
- Actions associated with the rule are executed
- Actions can be manually taken or undone
- At least one event is associated with the alarm



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

A security alarm looks like the example shown on this slide. The host MAC appears in the first column, then the alarm date, which rule was matched, if any action was taken and the time, who took the action, and so on. Then, at the bottom of the screen, you see what events were generated that go along with this alarm. Remember, an event is generated whenever a filter is matched, a trigger is satisfied, and a user host profile is matched. So, if a trigger had multiple filters in it, then there could be multiple events being matched in order to result in the trigger being satisfied and, ultimately, this alarm being displayed.

At the bottom of the window, you can select the **Actions Taken** tab to view which actions were taken. In the example on this slide, the **Disable Host** action was completed. As shown on the upper section of the window, the host that caused this alert to be sent is identified by its MAC address. That host is now marked as disabled, and may be moved to the dead end VLAN or to a quarantine VLAN. It depends on how those settings are configured on FortiNAC. The **Undone** column shows that the host has been enabled again.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Security Event Parsers

- Creation of new Syslog message mappings with customized security device integrations
- Incorporate new security devices into security rule development

System > Settings > System Communication > Security Event Parsers

Security Event Parsers

Add | Modify | Delete | Copy | In Use | Test | Export to:

Security Event Parsers - Total: 10

Enable:

Enabled	Name	Vendor	Format	CSV Delimiter	Tag Delimiter	Source IP Column	Destination IP Column
✔	StoneGate	StoneGate	CSV	,	=	5	
✔	TippingPointSMS	TippingPoint	CSV	,	=	8	10
✔	Sourcefire	Sourcefire	CSV	|	=	2	
✔	TopLayer	TopLayer	Tag/Value		=	cip	
✔	FireEye	FireEye	CEF		=	src	dst
✔	FortiOS4	Fortinet	Tag/Value		=	src	
✔	FortiOS5	Fortinet	Tag/Value		=	srcip	dstip
✔	PaloAlto	PaloAlto	CSV	,	=	8	9
✔	CheckPoint	CheckPoint	Tag/Value	;	:	src	
✔	Nozomi	Nozomi	CEF		=	SRC	DST

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

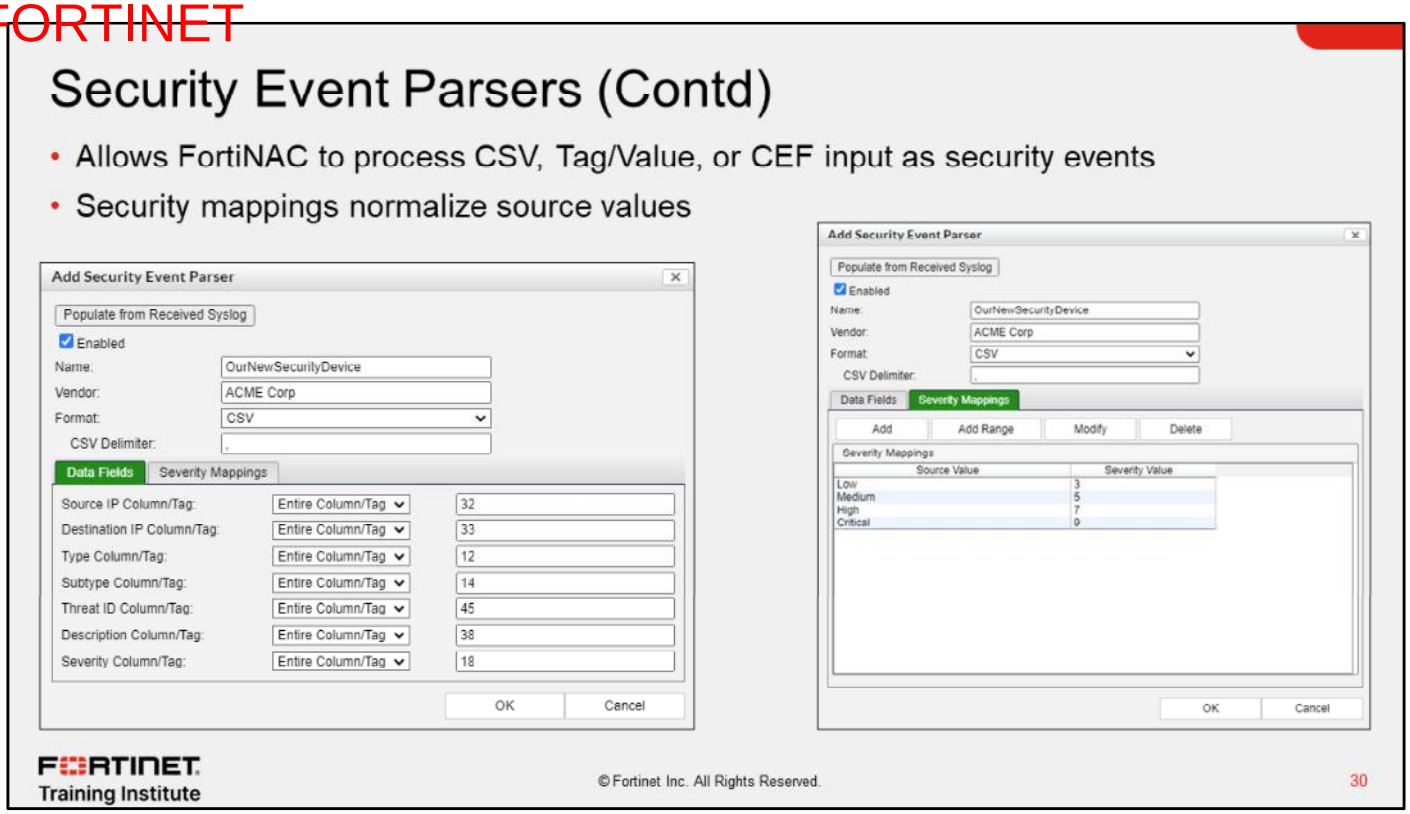
You can see all of the existing security event parsers under **System** > **Settings**. The **Security Event Parsers** settings page is located in the **System Communication** folder.

A security event parser will exist for each supported vendor, and administrators can delete or modify any of the existing parsers. Adding a new security event parser allows the administrator to support almost any device that issues Syslog messages in CSV, CEF, or Tag/Value format.

Note that you must model any security device that sends alerts to FortiNAC in the **Inventory** view, using the IP address that will be the source of the alerts. You must also set the **Incoming Events** field to **Security Events**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Creating a new, customized event parser allows FortiNAC to parse and integrate with any vendor or device that can pass syslog messages to it, as long as they are in **CSV**, **CEF**, or **Tag/Value format**. This allows FortiNAC to extend **Security Rules** and automated response and threat mitigation offerings across a diverse infrastructure, allowing it to use the individual strengths and capabilities of each device.

The example shown on this slide has the parsed syslog populating the **Source IP** field with the value contained in column 32, the **Destination IP** field with the value contained in column 33, and so on. The last normalized field in the list is **Severity**, and it is populated with the value from column 18. FortiNAC needs to be configured to map severity field values to numeric values in order to create a standardized method for evaluating severity. The **Severity Mappings** example shown on this slide assigns a severity value of 3 if column 18 contains the word Low, the value of 5 if it contains the word Medium, and so on. This capability provides integration flexibility across vendors who may not share the same terms for indicating severity.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

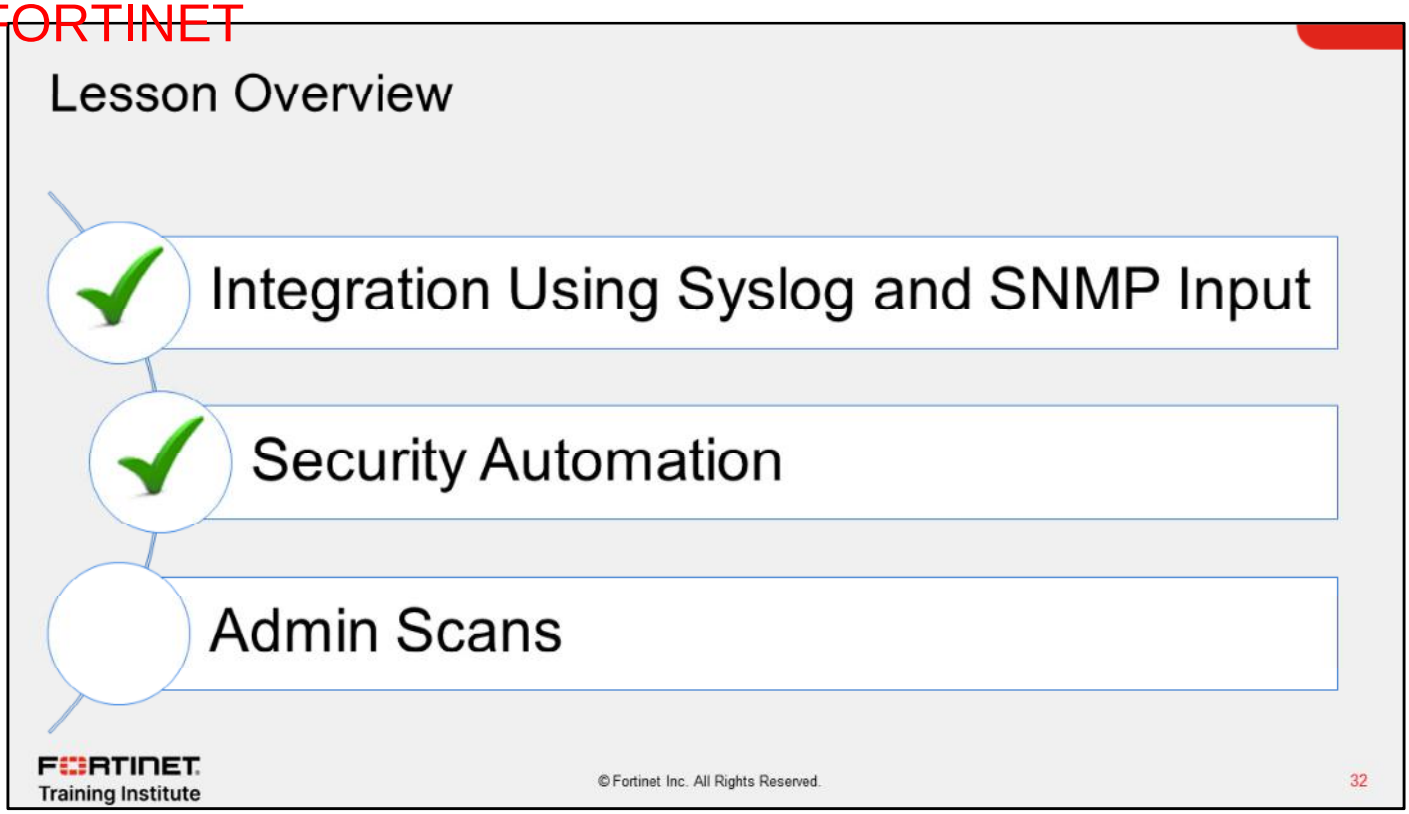
1. What is a component of a security trigger?
   A. User/Host profiles
   ✓B. Security filters

2. How can FortiNAC integrate with a security device that is not supported out-of-the-box?
   A. Through the creation of an alarm-to-action mapping
   ✓B. Through the creation of a security event parser

FORTINET Training Institute
© Fortinet Inc. All Rights Reserved.
31

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

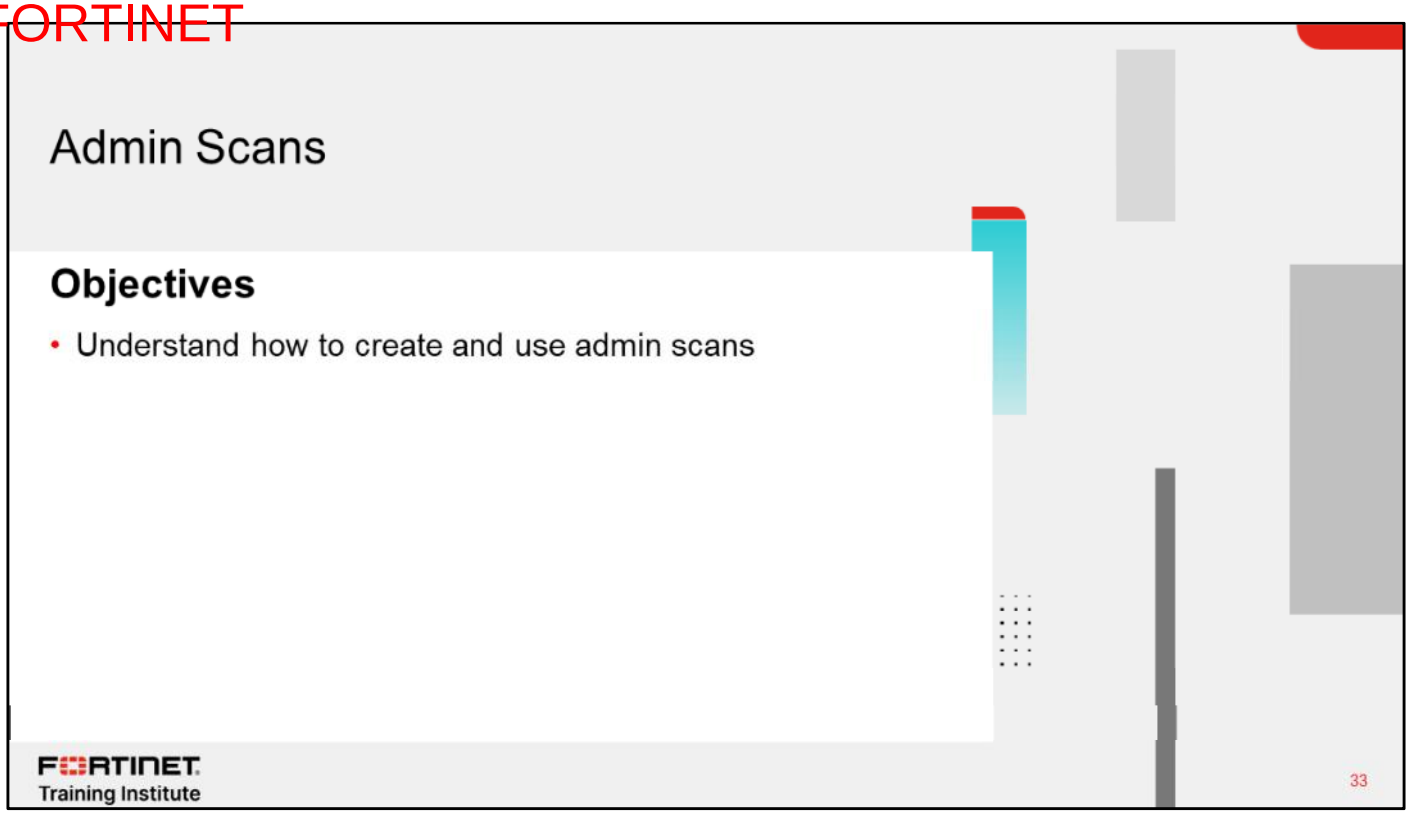


Good Job! You now understand security automation and how to configure security rules.

Now, you will learn about admin scans.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

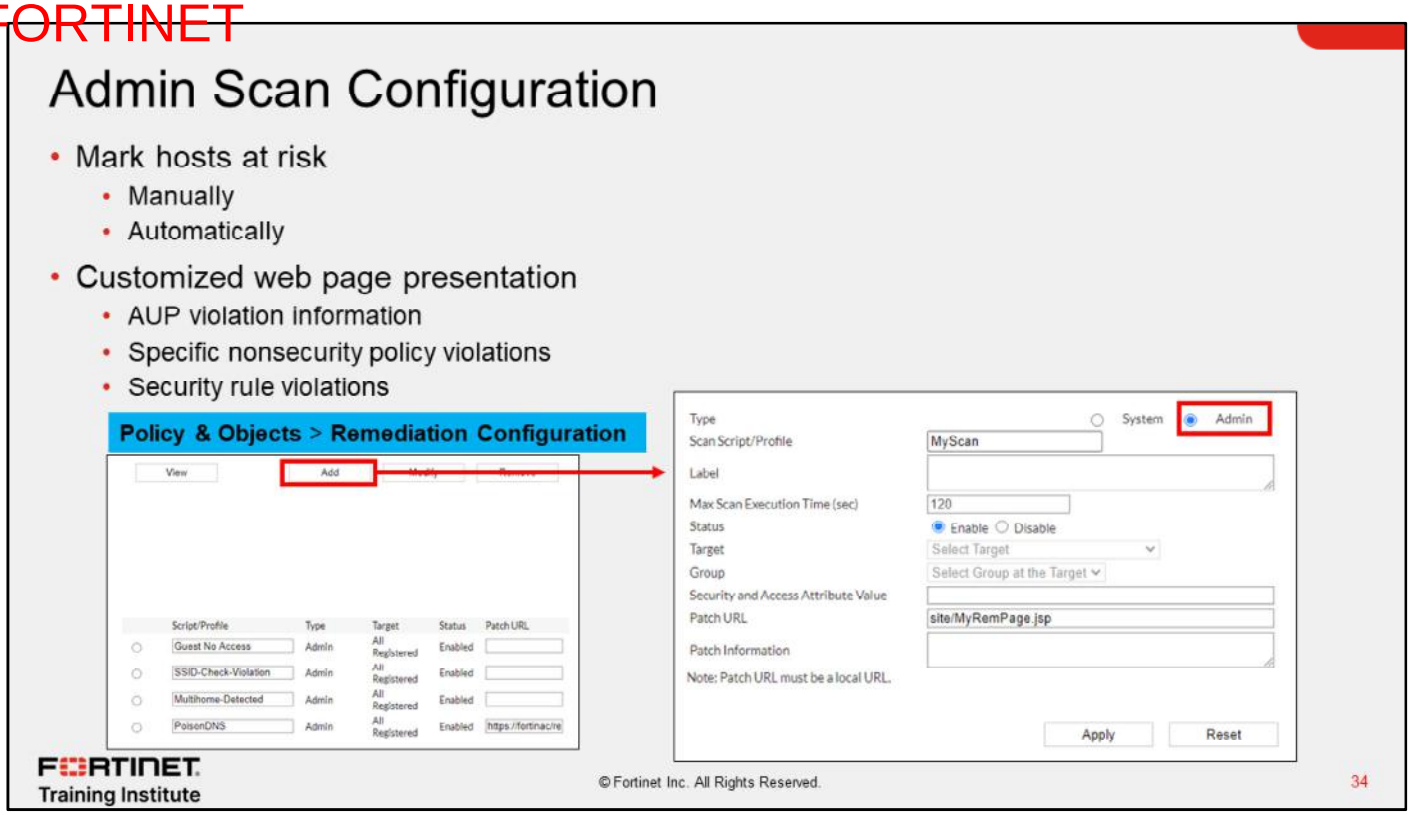


After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in the creation and use of admin scans, you will be able to assign hosts to the quarantine isolation network and present customized portal content.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Admin scans are a means to change a host's state to *at risk*. This can be performed manually, by an administrator, or as part of an automated action. The purpose of the admin scan is so that when the host is isolated to the quarantine network, FortiNAC knows what page to present to the end user. Recall that a host state is changed to *at risk* when it has failed a scan. Policy scans are preformed by FortiNAC agents, and a failed result has the necessary information contained within the policy to define which isolation portal page should be displayed.

You can create an admin scan from the **Remediation Configuration** view. All existing scans will be displayed. You can modify or remove each one by selecting the scan and clicking the appropriate button. Clicking **Add** will open the **Add Scan** window.

The admin scan creation process requires the new scan to be given a scan script/profile value to uniquely differentiate it from any other admin scans. The **Scan Script/Profile** field is the only required field. If a host has its state changed to *at risk* because of an assigned admin scan that does not have a **Patch URL** field set, the host will be isolated but the isolation page will be a default page that does not include specific information to assist the end user. The **Patch URL** field is often the only other field configured in an admin scan, and it defines the isolation page that should be presented to the end user. The isolation page should be placed in the `/bsc/Registration/registration/site` directory on the FortiNAC Application server or Control and Application server. The root portal page path is `/bsc/Registration/registration` so the configuration set in the **Patch URL** field only needs to contain the final directory in the path. The example shown on this slide would direct any host that has had its status changed to *at risk* using this admin scan, to the isolation portal page named `MyRemPage.jsp`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. What are admin scans used for?

✓A. Changing a host state/status to *at risk*

B. Scanning a host for compliance

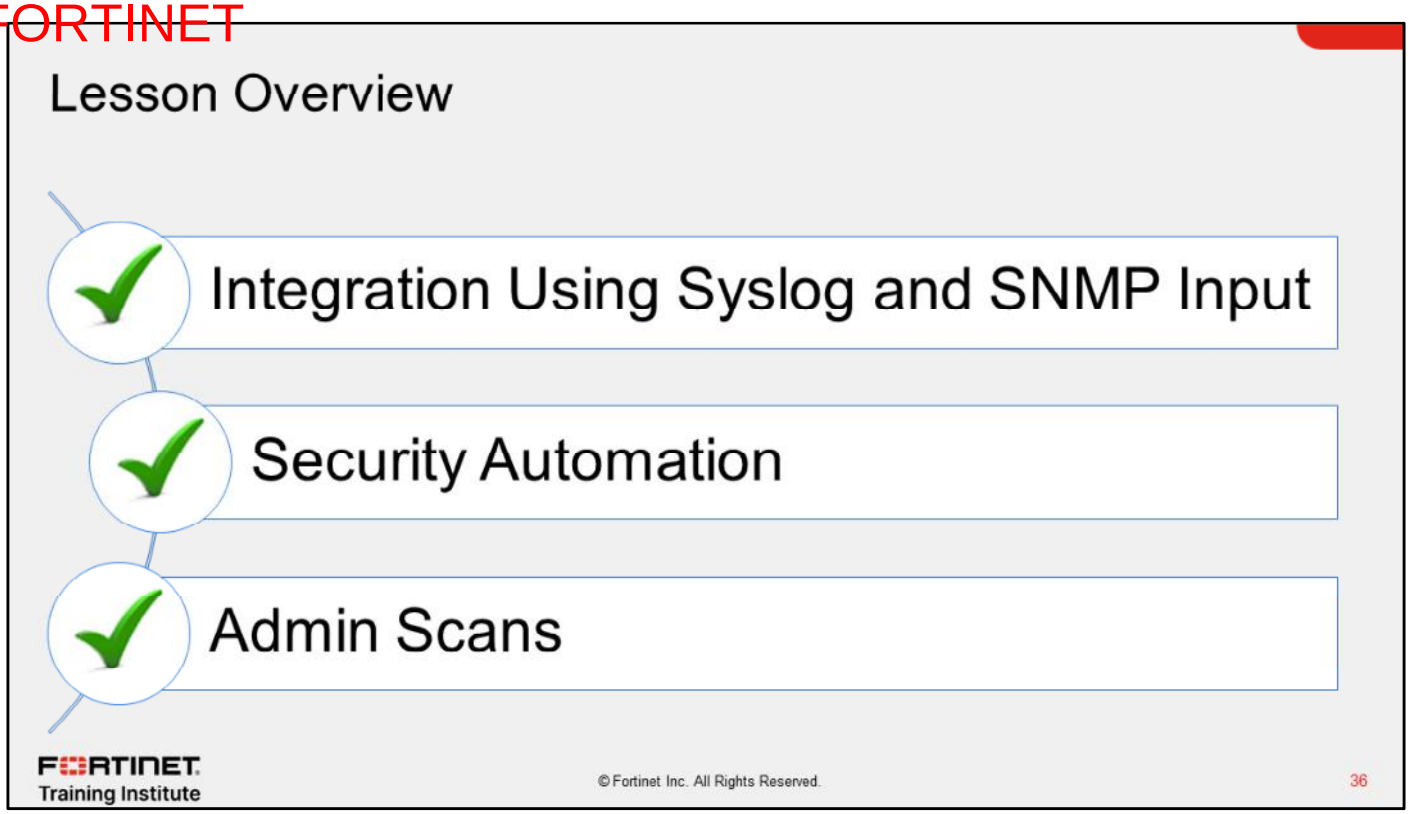
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

35

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

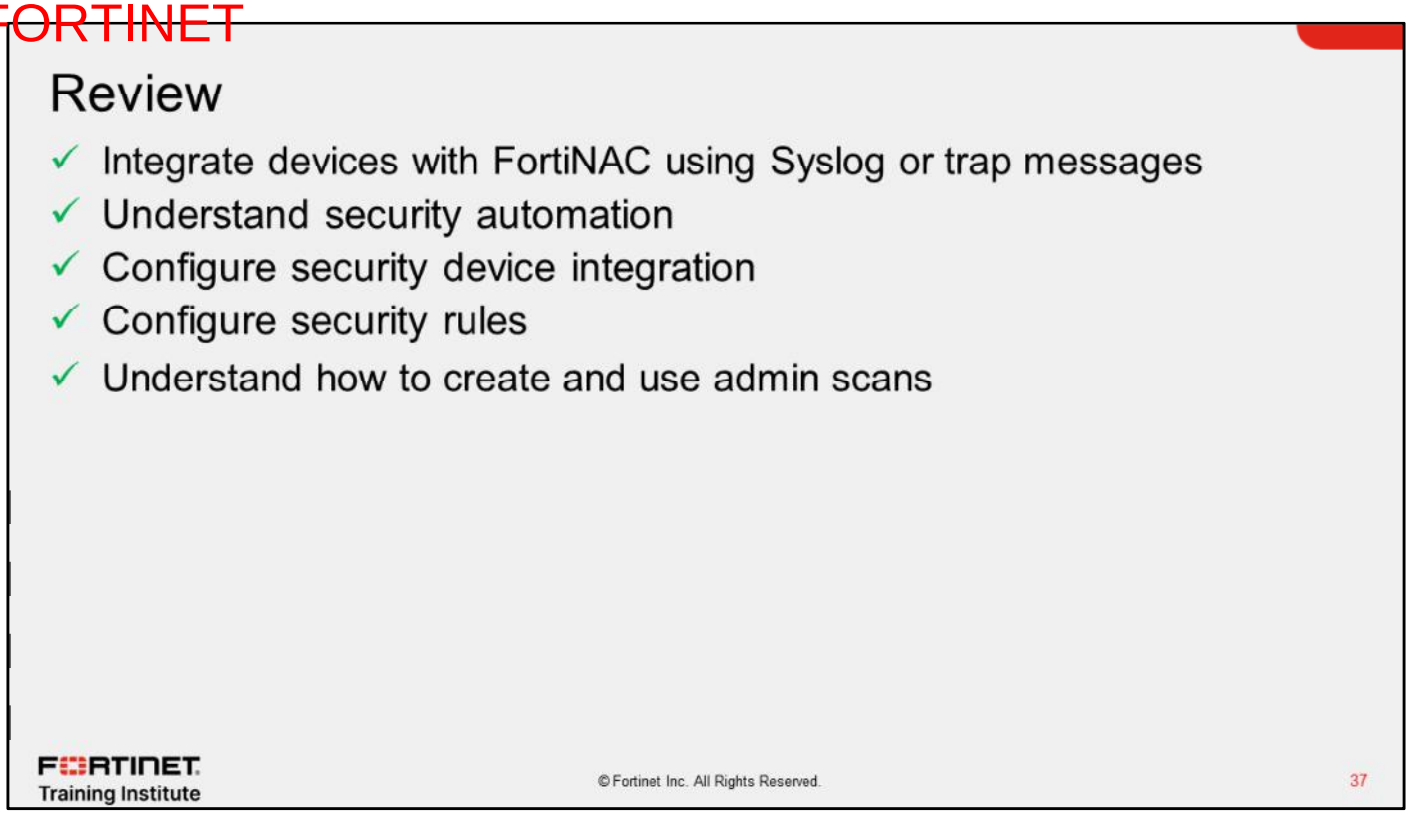


Congratulations! You have completed this lesson.

Now, you will review the objective that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

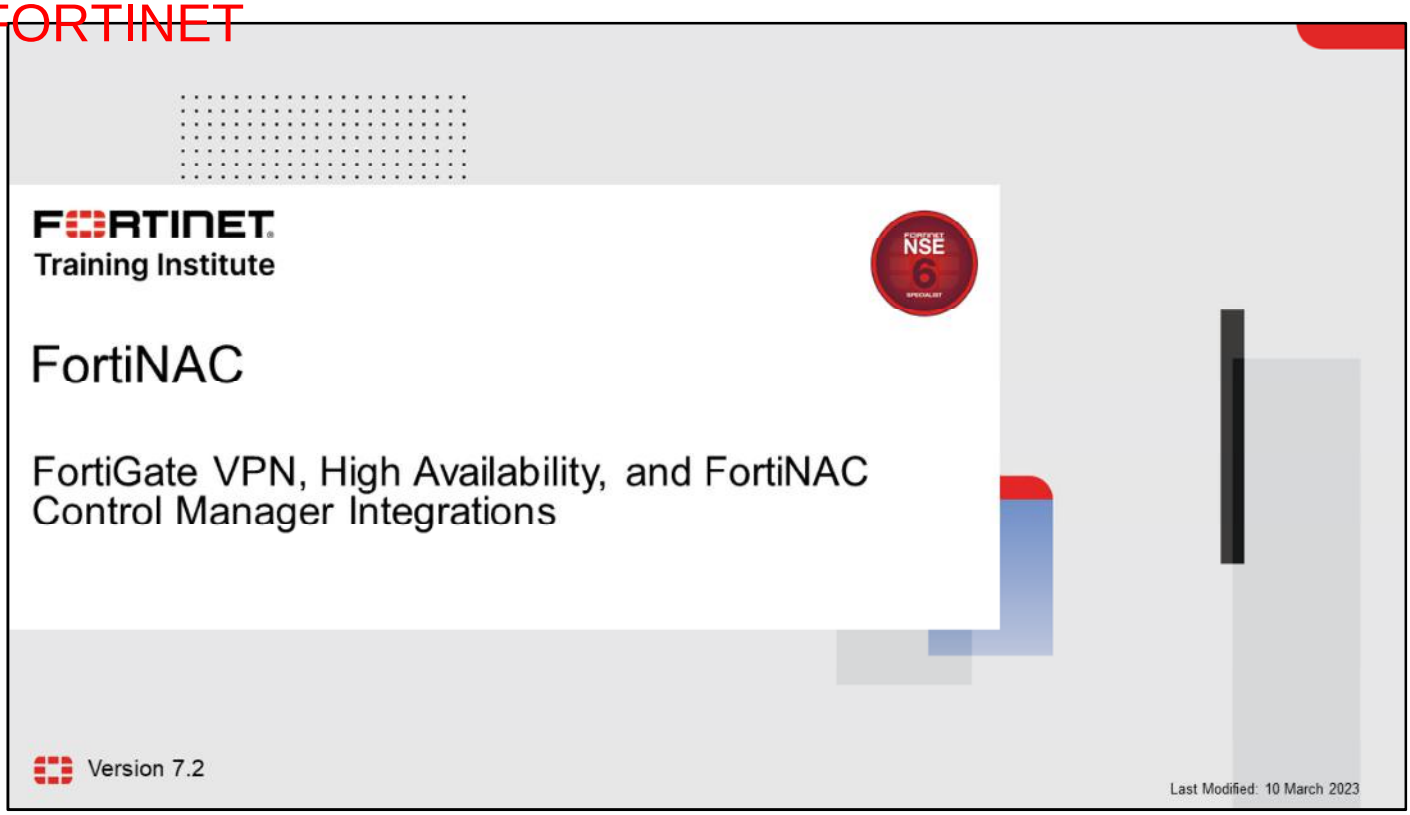


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to integrate third-party devices with FortiNAC, making it possible to be notified and trigger automated responses.

Vouchers & Dumps are Available | WhatsApp +201224560923

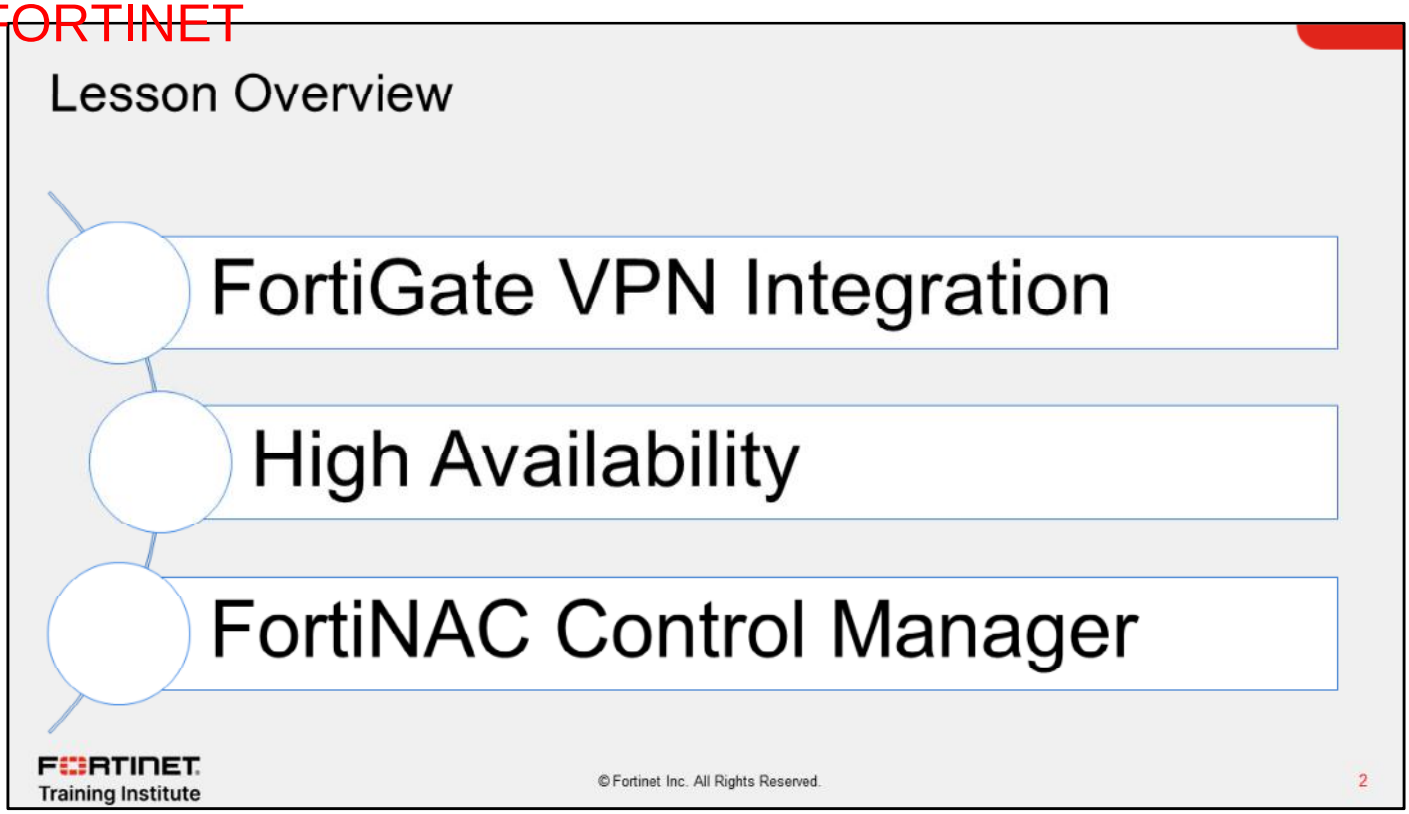
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how FortiNAC provides visibility and management to FortiGate VPN clients. You will also learn how to configure FortiNAC in a high availability deployment, as well as how FortiNAC Control Manager is integrated and used in a distributed FortiNAC deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

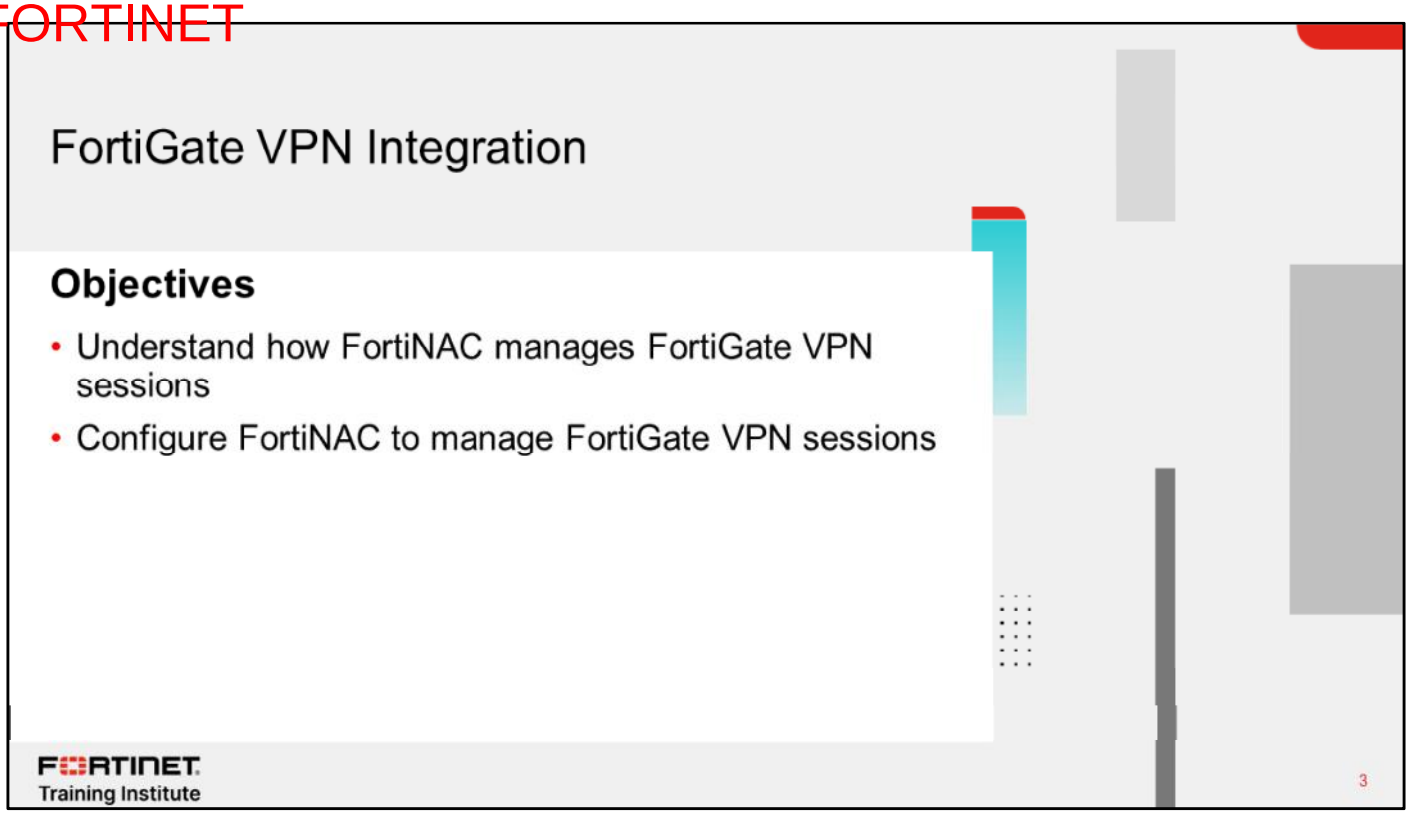
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about the topics shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

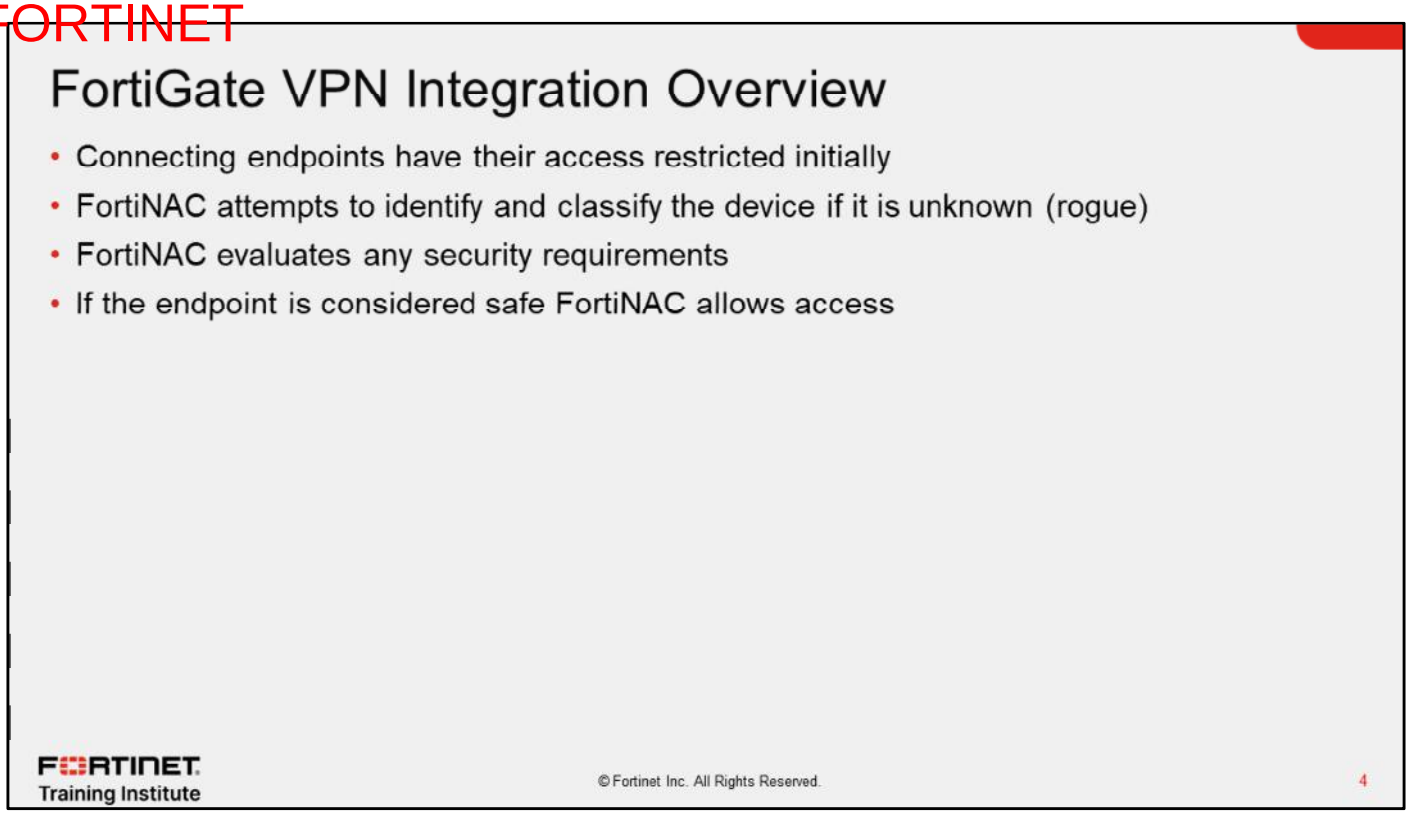


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiGate VPN integration, you will be able to understand how FortiNAC manages FortiGate VPN sessions, and how to configure the integration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



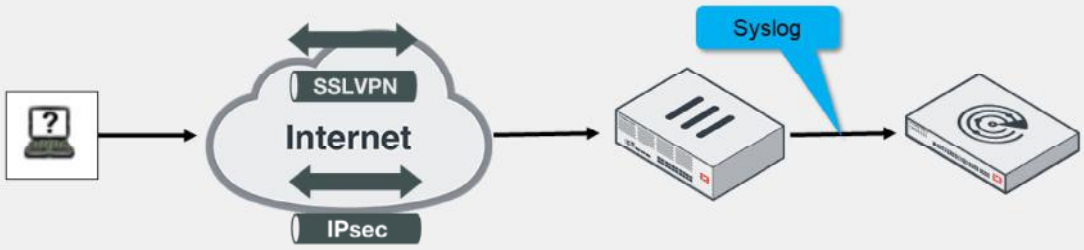
This slide outlines FortiGate and FortiNAC VPN integration process.
When a device initially connects over a VPN tunnel, the device is granted restricted access only until FortiNAC receives information about the device.
If the device is unknown (rogue), FortiNAC attempts to identify and classify the device.
Agent technology is used by FortiNAC to gather information and evaluate the device's compliance with any designated security requirements.
If the device has been classified and is considered to be safe, FortiNAC updates FortiGate and access restrictions are removed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiGate VPN Integration Overview (Contd)

- Remote user establishes a VPN connection using SSL or IPSec
  - FortiGate assigns IP address, and primary and secondary DNS servers
  - FortiGate address groups are used to define VPN IP scopes managed by FortiNAC
- Successful authentication results in FortiGate sending user, IP, and session information to FortiNAC using syslog
- Firewall policies only allow access to FortiNAC



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

5

FortiGate VPN managed with FortiNAC controls and monitors access for connecting devices using SSL or IPSec.

After the device establishes the VPN tunnel, FortiGate assigns an IP address and two DNS server addresses. The primary DNS server will be a production server, and the secondary will be the IP address of the VPN context on eth1 of FortiNAC. Following successful authentication, additional information is passed from FortiGate to ForitNAC using syslog.

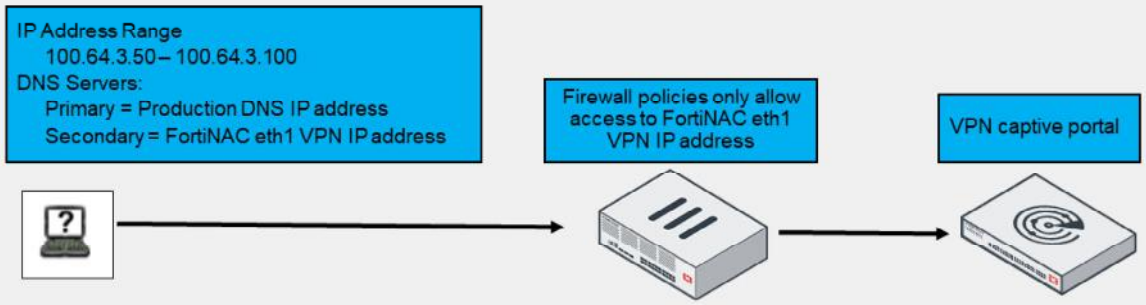
By default, network access is restricted for VPN users when they connect. Access is modified only if the user successfully authenticates through FortiNAC, runs an appropriate FortiNAC agent, and passes any required compliance checks

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

VPN Host Isolation

- While firewall policies are only allowing access to FortiNAC:
  - Host will send DNS queries to FortiNAC (firewall policies are denying access to the primary DNS)
  - All HTTP requests are directed to the VPN captive portal on FortiNAC (because of DNS response)
  - Captive portal informs user that they are isolated and must download and run a FortiNAC agent
    - Trusted hosts with a FortiNAC Persistent Agent already installed will not need to manually run an agent



FORTINET Training Institute

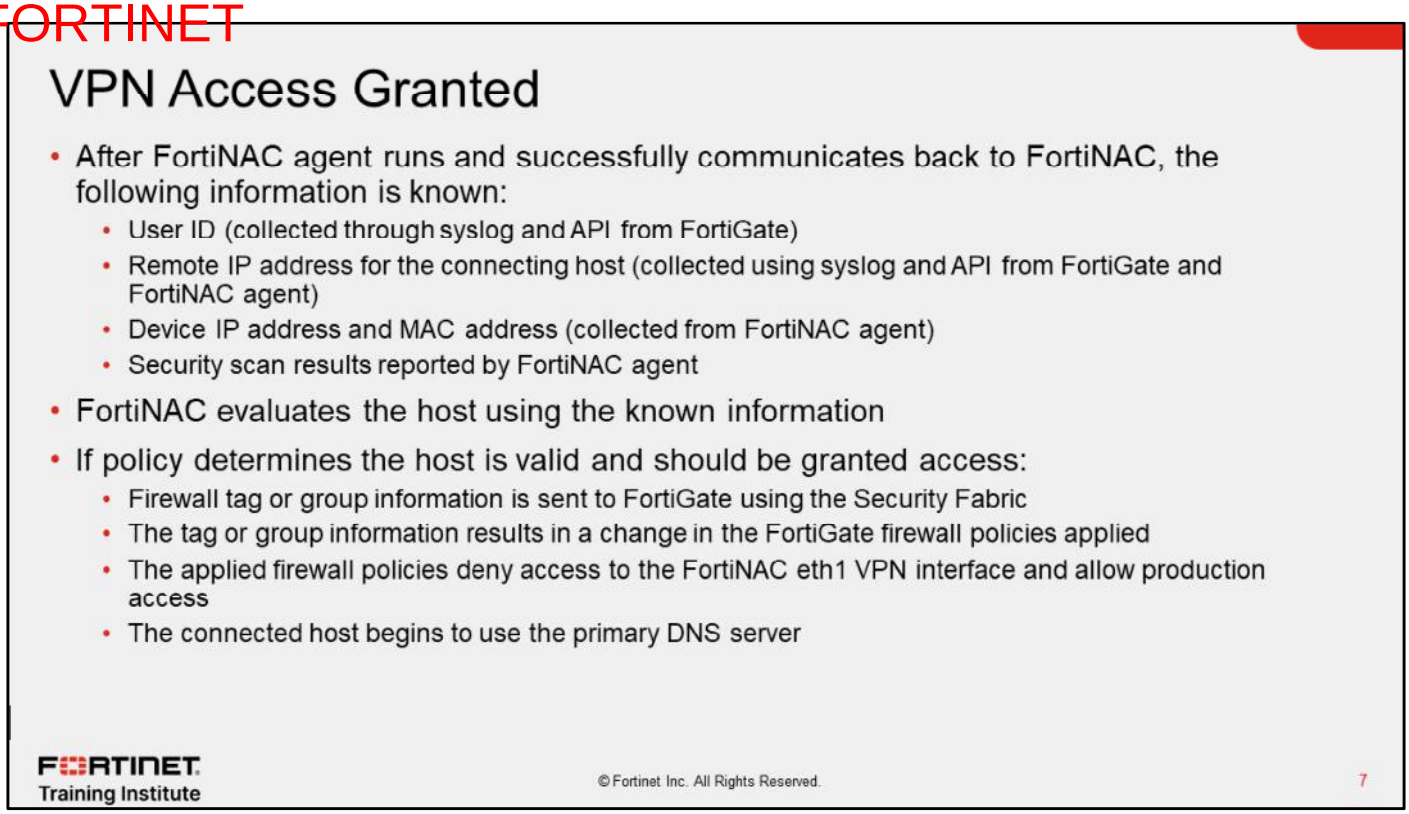
© Fortinet Inc. All Rights Reserved.

6

Host isolation is enforced by FortiGate firewall polices and DNS server assignment. Firewall policies permit the host to having access to the VPN context on the FortiNAC eth1 interface only, which the host has assigned as the secondary DNS server. When the host attempts to resolve a domain using DNS, the attempt will fail for the primary DNS server, and the host will use the secondary DNS server (FortiNAC). FortiNAC will respond to the DNS queries, and resolve them to its eth1 interface, where the VPN context portal will be presented. If the host does not have a FortiNAC persistent agent installed, the user will be forced to download and run an agent.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



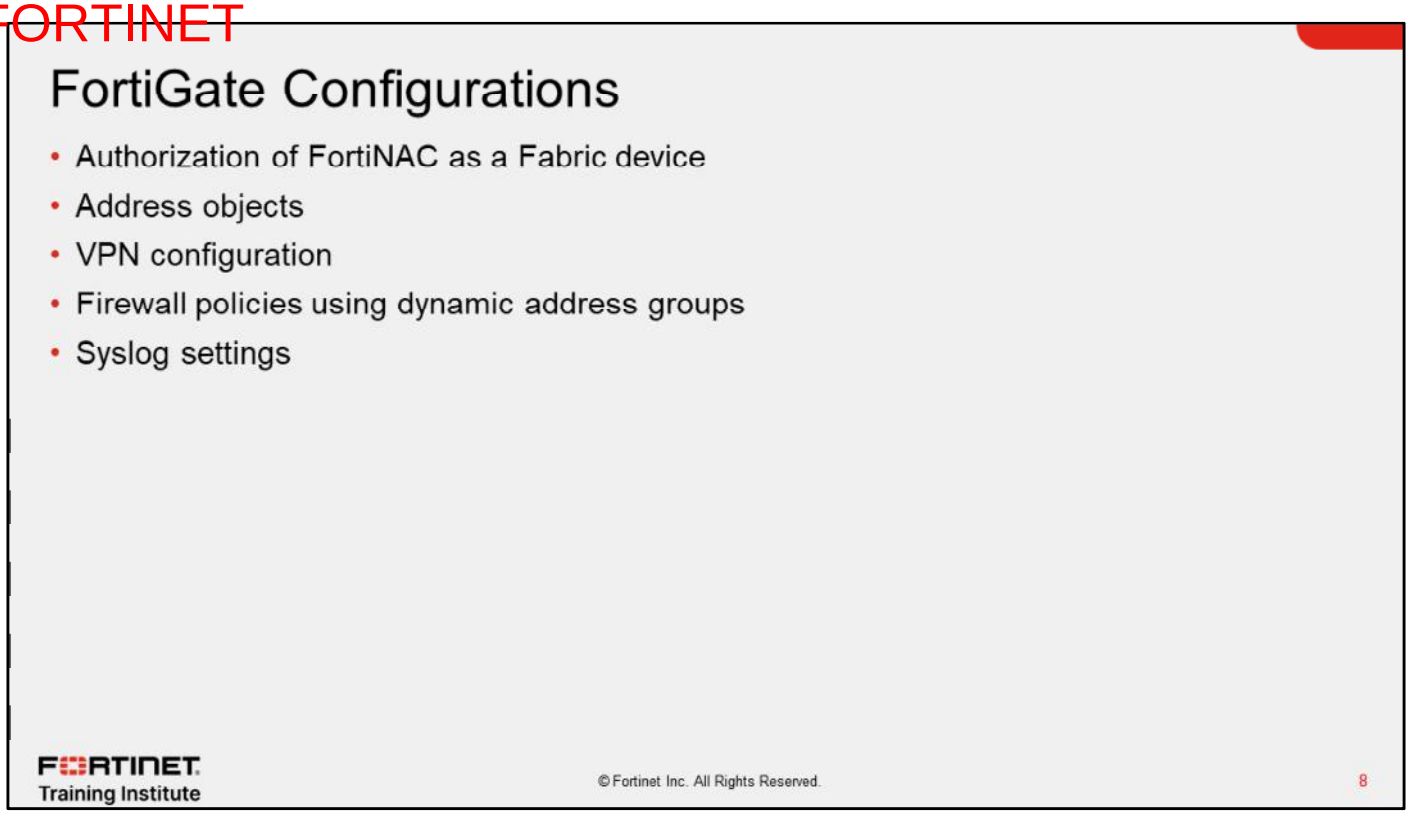
Through evaluation of the information gathered from syslog, the FortiGate API, and the FortiNAC agent (including user ID, IP address, MAC address, and scan results), FortiNAC can lift access restrictions.

To lift restrictions and grant access, FortiNAC uses the Security Fabric to send group tag information, or firewall tag information, or both, to FortiGate. Network access policies defined in FortiNAC define the group and tag information sent to FortiGate. These group and tag assignments will change the FortiGate firewall group-based policies being applied.

The enforcement of the newly applied firewall policies will deny access to the VPN context on eth1 of FortiNAC, and allow access to production-network resources. The secondary DNS server (FortiNAC eth1 VPN context) will no longer be accessible; however, the primary will, and access to all allowed resources will be available.

Vouchers & Dumps are Available | WhatsApp +201224560923

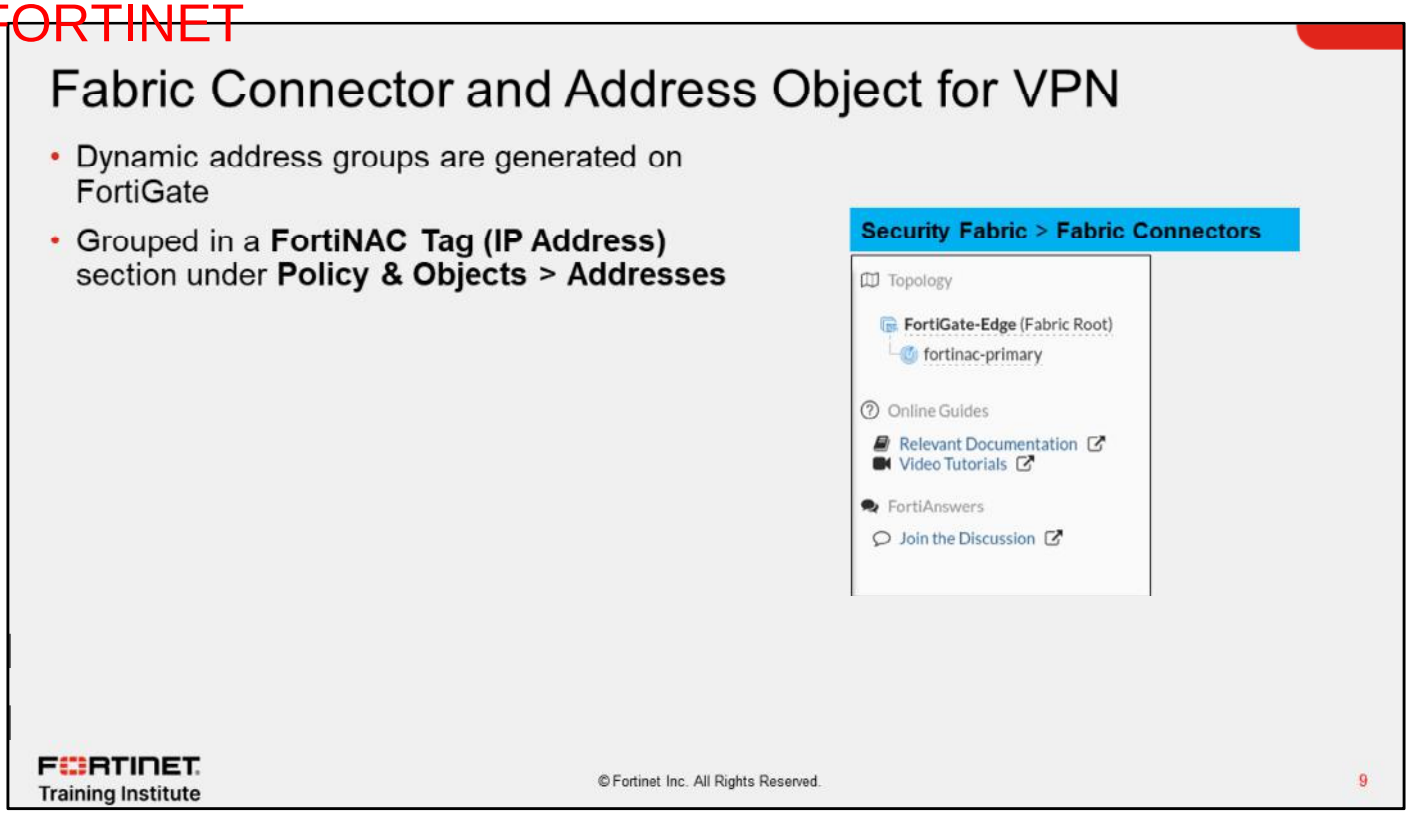
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The configurations that must be performed on FortiGate are as follows:
- FortiNAC tags fabric connector: Used to allow FortiNAC to pass tag and group information to FortiGate
- Address objects: Used in firewall policies to identify VPN hosts
- VPN configuration: Used for initial VPN tunnel creation
- Firewall policies: Used to allow or deny access to VPN hosts with dynamic address groups generated from firewall tags
- Syslog settings: Used to pass connection information to FortiNAC

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiNAC passes group membership information and firewall tags to FortiGate using the FortiNAC Tags Security Fabric connector. FortiNAC network access policies and logical networks determine the group information or tags that will be passed for each connecting host or user.

Address groups are used to identify VPN hosts, and are used in firewall policy configurations. The applied groups, tags, and addresses determine the firewall policies the connecting hosts match.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

VPN Configuration

- IPSec or SSL
  - Provide IP address assignment using DHCP (IPSec) or tunnel IP range (SSLVPN) on incoming interface
  - Assign DNS
    - Primary (production DNS server)
    - Secondary (FortiNAC VPN isolation interface)



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

10

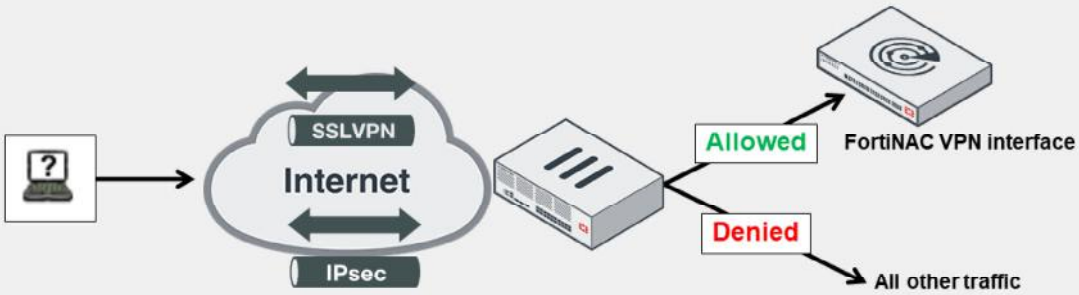
FortiGate will assign IP address and DNS server details to the connecting host during initial VPN tunnel creation. The primary DNS server will be a production server. The secondary DNS server will be the FortiNAC VPN isolation interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Firewall Policy for Unauthorized Hosts

- Create a firewall isolation policy to:
  - Allow traffic to and from the FortiNAC VPN isolation interface
  - Deny all other traffic



FORTINET Training Institute

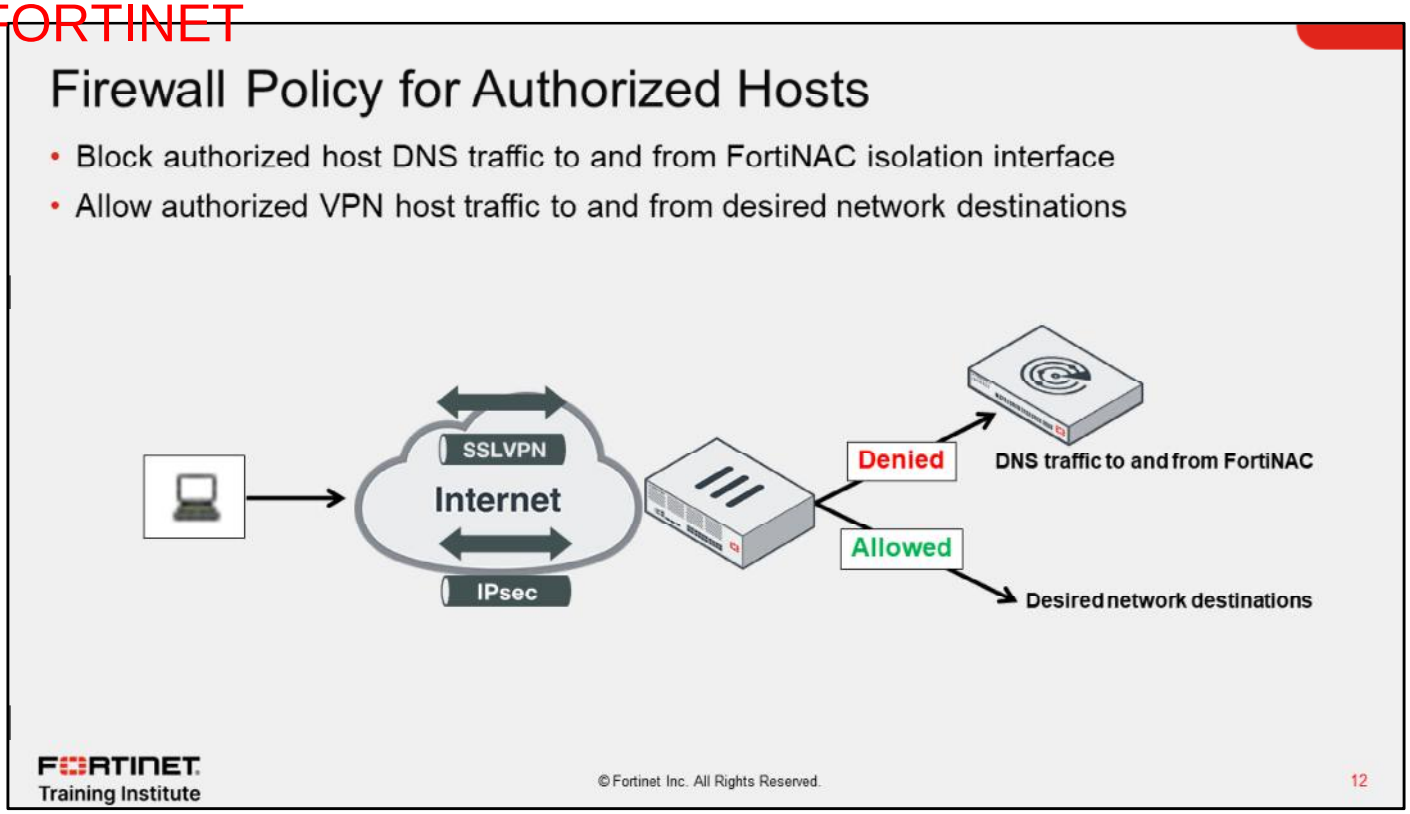
© Fortinet Inc. All Rights Reserved.

11

All VPN hosts will initially be considered unauthorized, and a firewall policy will only allow to the FortiNAC VPN interface. This policy will force the connecting host to use the secondary DNS server, defined by the FortiGate when the host initially connected. This will initiate the validation process by FortiNAC, presentation of the VPN captive portal, and FortiNAC agent communication or download.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



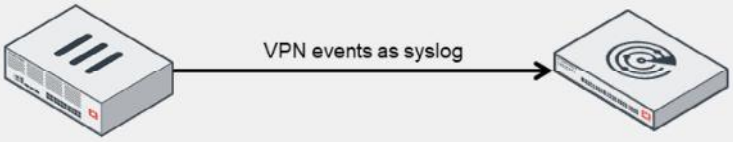
On successful completion of the validation process, the connected host will match a different FortiNAC network access policy. The FortiNAC policy will designate a logical network with associated firewall tags or groups, and FortiNAC will pass this tag or group information back to FortiGate. The tag or group information will change the firewall policy, and traffic to the FortiNAC isolation interface will be blocked, while all other traffic is allowed. The host has now been authorized by FortiNAC and appropriate production access granted.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Syslog Settings

- FortiNAC must be configured to receive FortiGate VPN events
  - Configure FortiGate to send logs to syslog
  - Add the FortiNAC primary (Eth0) IP address
  - Enable event logging on the FortiGate for VPN activity events



FORTINET Training Institute

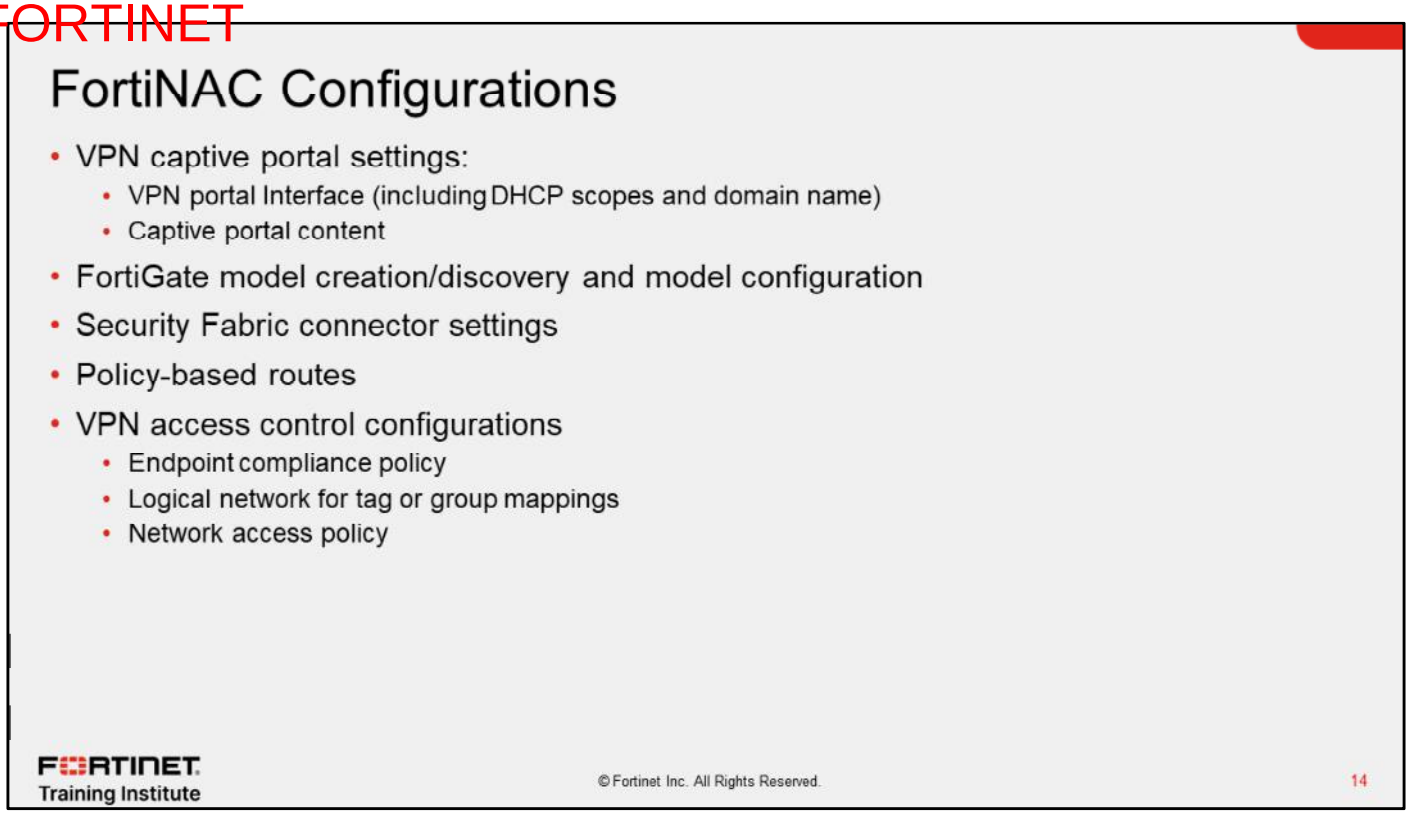
© Fortinet Inc. All Rights Reserved.

13

FortiGate informs FortiNAC of VPN host activity by using syslog messages for VPN activity events. The syslog messages should be configured to be sent to the eth0 interface of FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the FortiNAC configurations that must be made for FortiGate VPN integration.

The VPN captive portal interface must be configured using the FortiNAC configuration wizard to include the DHCP scopes and the domain name that will be used. FortiNAC will not act as the DHCP server for connecting hosts. FortiGate will perform that function, as defined in its VPN configuration. The captive portal content should be configured for page presentation to restricted users.

FortiGate must be modeled and configured in the FortiNAC network inventory.

FortiNAC must be part of the Security Fabric.

Policy-based routes must be configured on FortiNAC to ensure that traffic is forwarded out the same interface on which it was received.

VPN access control configurations must be defined. An endpoint compliance policy needs to exist to define the FortiNAC agent that should be distributed to VPN hosts, as well as any security scan requirements.

Logical networks for VPN access must be created and defined for group and tag mappings to be sent to FortiGate. Group and tag values are assigned using network access polices.

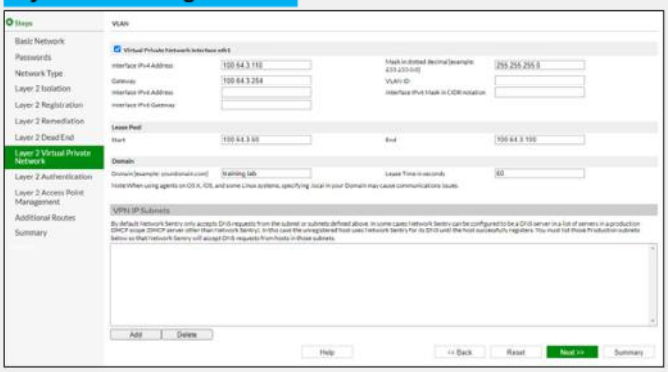
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

VPN Captive Portal Interface

- Configured in the VPN context of the configuration wizard

System > Config Wizard





FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

15

You must configure the FortiNAC eth1 VPN isolation interface using the configuration wizard.

You must assign the VPN interface an IP address, subnet mask, and for Layer 3 deployments, a default gateway.

Next, define the VPN DHCP scope, or scopes. Keep in mind that the scopes defined here must match the IP address ranges configured for the VPN on the FortiGate. Although FortiNAC will not be serving IP addresses for VPN connections, this entry updates the file `domain.zone.vpn` which handles DNS SRV queries from connecting agents.

Finally enter the domain. Note that the domain must match the domain defined in the fully-qualified host name of the FortiNAC server.

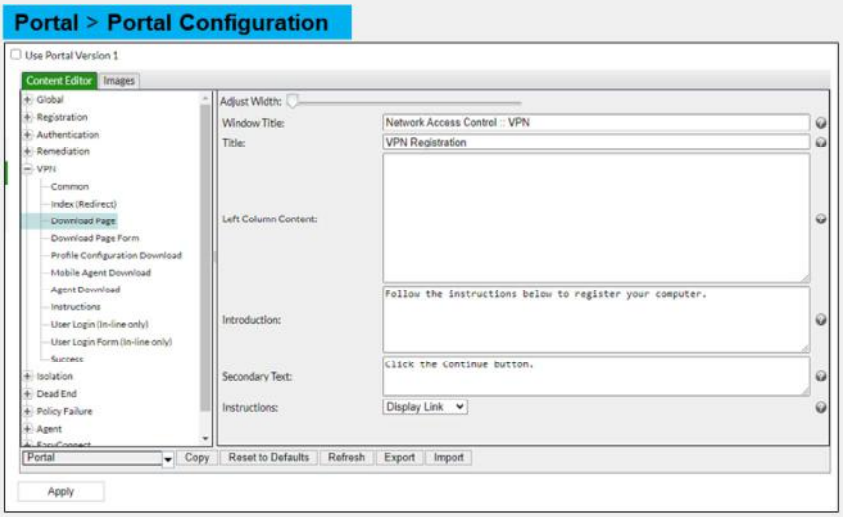
See the Configuration Wizard reference manual in the Fortinet Document Library for more detailed instructions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

VPN Portal Configuration

- VPN portal page customization
- Option to provide access to onboarding instructions



FORTINET Training Institute

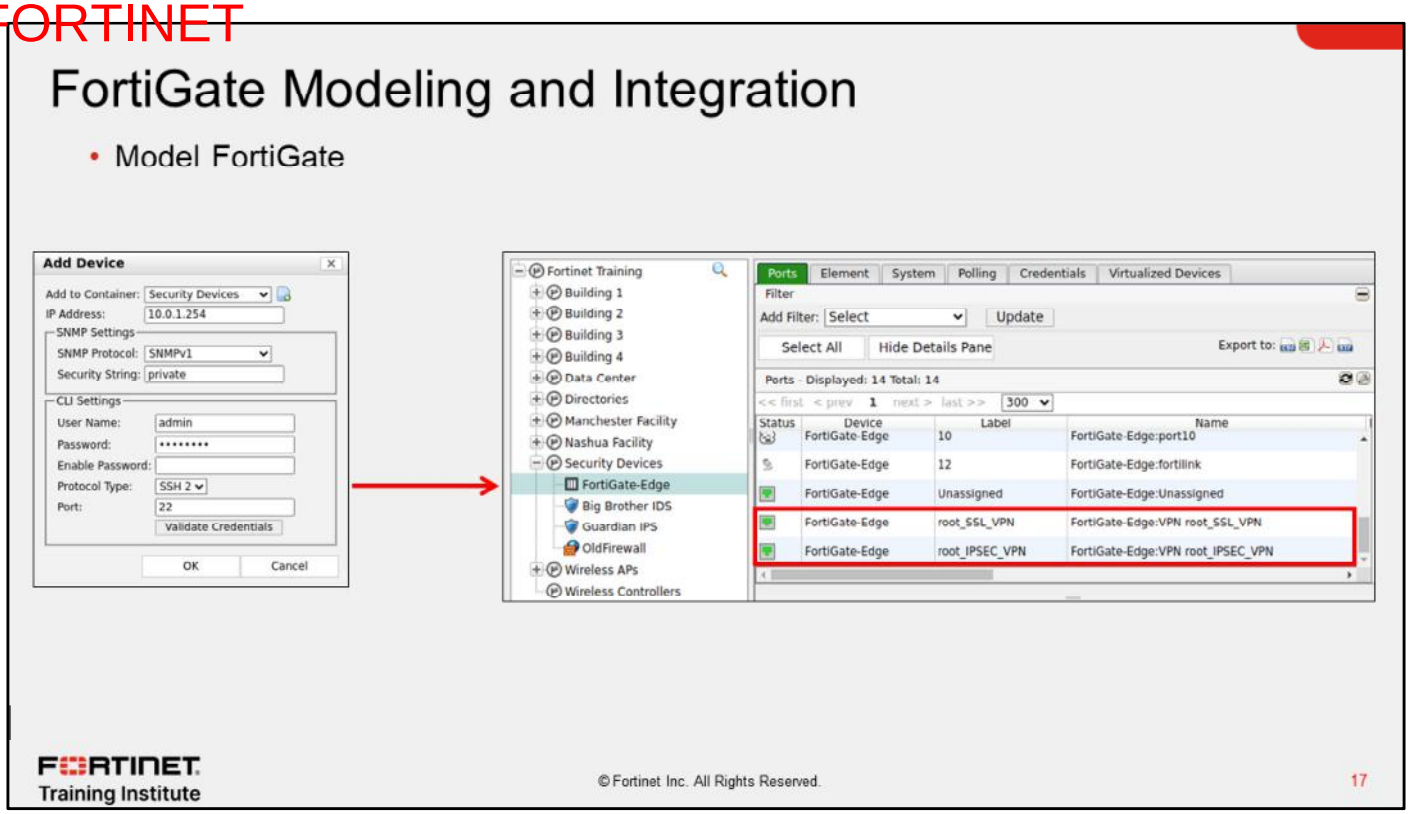
© Fortinet Inc. All Rights Reserved.

16

The VPN portal is configured from the portal configuration page. You customize wording, layout, and page design for your environment. Portal page customization is covered in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



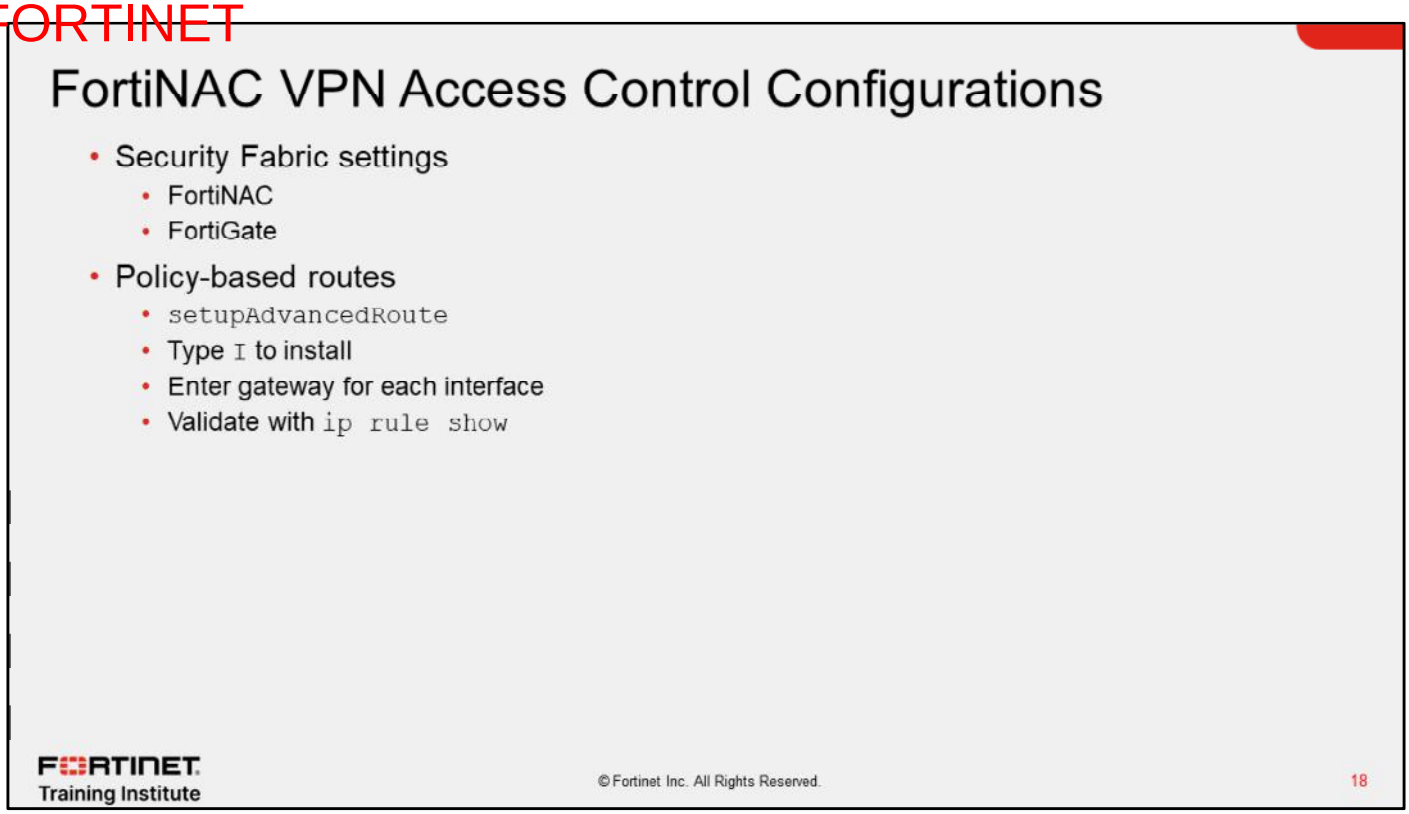
FortiGate must be modeled in the FortiNAC network inventory to manage the users connecting through VPN, and FortiNAC must be joined to the Security Fabric.

Once modeled, VPN interfaces will appear under the **Ports** tab for FortiGate. Two new interfaces are created for each VDOM configured in FortiGate, with labels beginning with the VDOM name and ending with IPSEC_VPN and SSL_VPN. If the interfaces do not appear in the list of ports, right-click the FortiGate model and select **Resync Interfaces**.

Device modeling is covered, in detail, in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



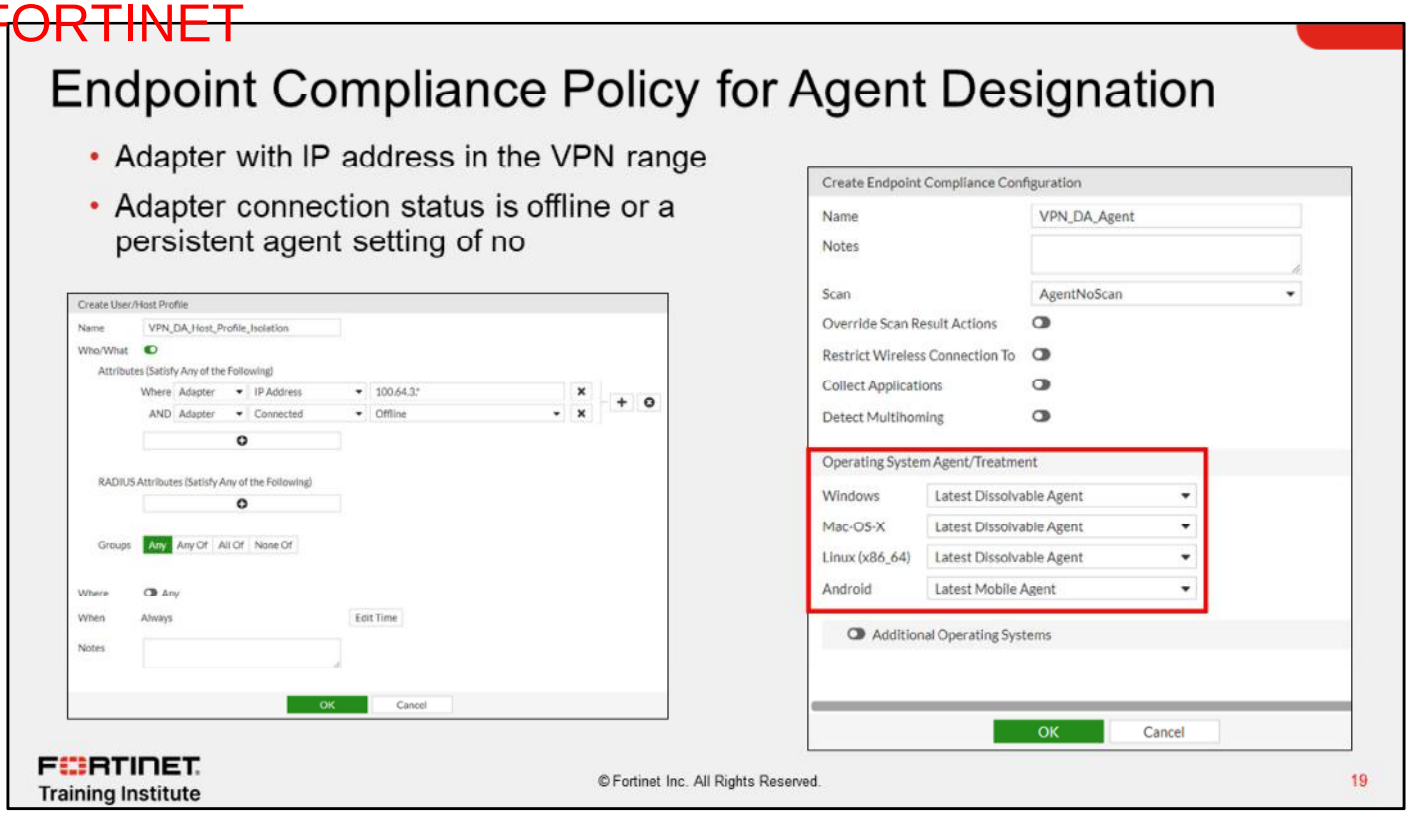
You must configure FortiNAC to be part of the Security Fabric. The Fabric connection with FortiGate was covered in a previous lesson.

Policy-based routing ensures traffic is transmitted out the same interface that received it. This allows FortiNAC agents to communicate to FortiNAC through both the management or the VPN sub-interface, depending on whether the endpoint is isolated or not.
Policy-based routing is configured on FortiNAC, from the CLI, using the command: `setupAdvancedRoute`. This must be done for both the primary server and the secondary server, in HA configurations.

1. Log in to the CLI as root of the FortiNAC server.
2. Type `setupAdvancedRoute`.
3. Type `I` to install.
4. Enter the gateway for each interface (`eth0`, `eth1`, and so on) as prompted.
5. After the script completes, verify the configuration by typing `ip rule show`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



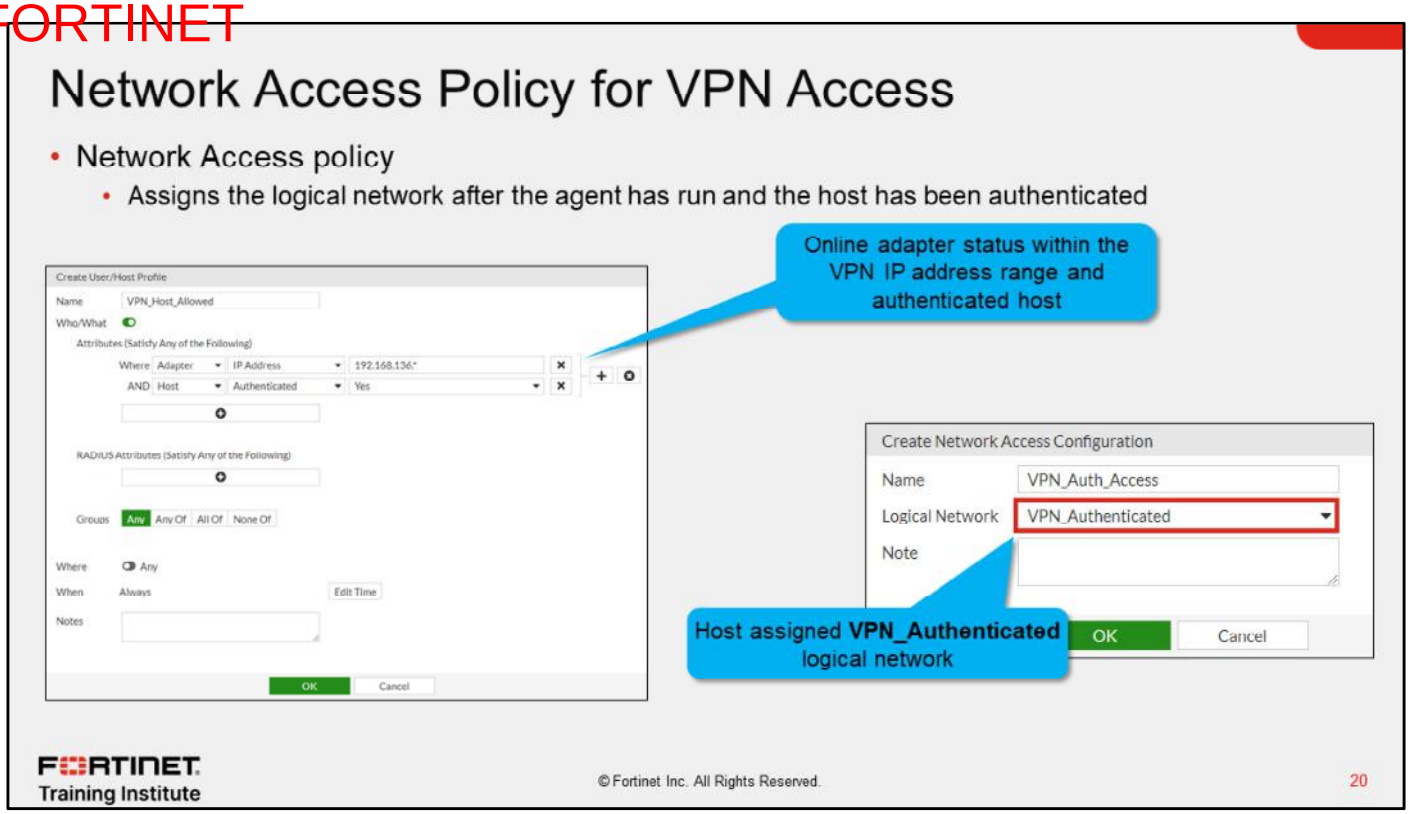
You must create FortiNAC policies with a user/host profile that identifies the IP scopes used for VPN. When using the FortiNAC dissolvable agent, the user/host profile that you create for VPN must specify either a host **Connection status** of **Offline**, or a host **PersistentAgent** setting of **No**.

As a best practice, it is recommended users are sent to the download location through DNS and URL redirection, and that split tunneling for the VPN configured on FortiGate is disabled. This ensures the user's browser is automatically redirected to the URL where they can download the dissolvable agent.

Note that it is recommended that you enable the **Restrict Roaming** persistent agent setting when connecting over a VPN managed by FortiNAC. To learn more about this setting, refer to the *Persistent Agent Settings* section in the *Persistent Agent Configuration and Deployment Reference Manual*, which you can find in the Fortinet Document Library.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



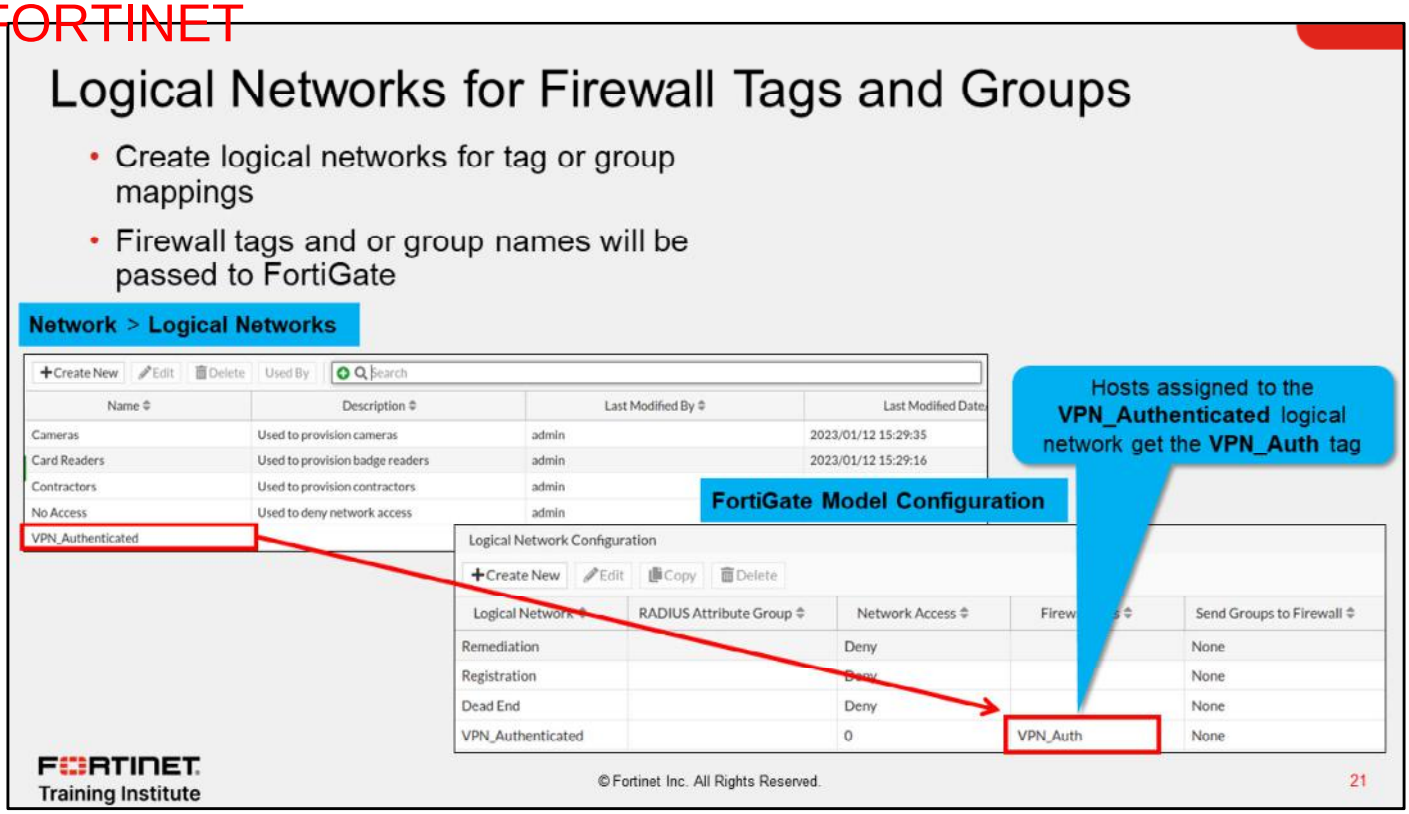
FortiNAC network access policies must exist or be created for VPN to reference a logical network. The FortiGate device model must contain mappings of the logical network to the actual tags or groups that are sent to FortiGate once the client is identified by the FortiNAC agent.

In the example shown on this slide, FortiNAC would assign the logical network VPN_Authenticated to a host that has a connected status of online and an IP address in the range being used for VPN clients.

Network access policies are covered in detail in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Logical networks are used to assign groups and firewall tags to users. These assignments are passed to FortiGate for dynamic firewall group updates. Group updates change which firewall policies are applied.

In the example shown on this slide, FortiNAC passes **VPN_Auth** as a firewall tag to FortiGate for any host that is assigned the **VPN_Authenticated** logical network.

Logical networks are covered, in detail, in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. When a host connects through VPN, which system provides an IP address?
   - ✓ A. FortiGate
   - B. FortiNAC
2. In an authorized state, what provides DNS for a connecting host?
   - A. FortiNAC DNS service
   - ✓ B. Production DNS server

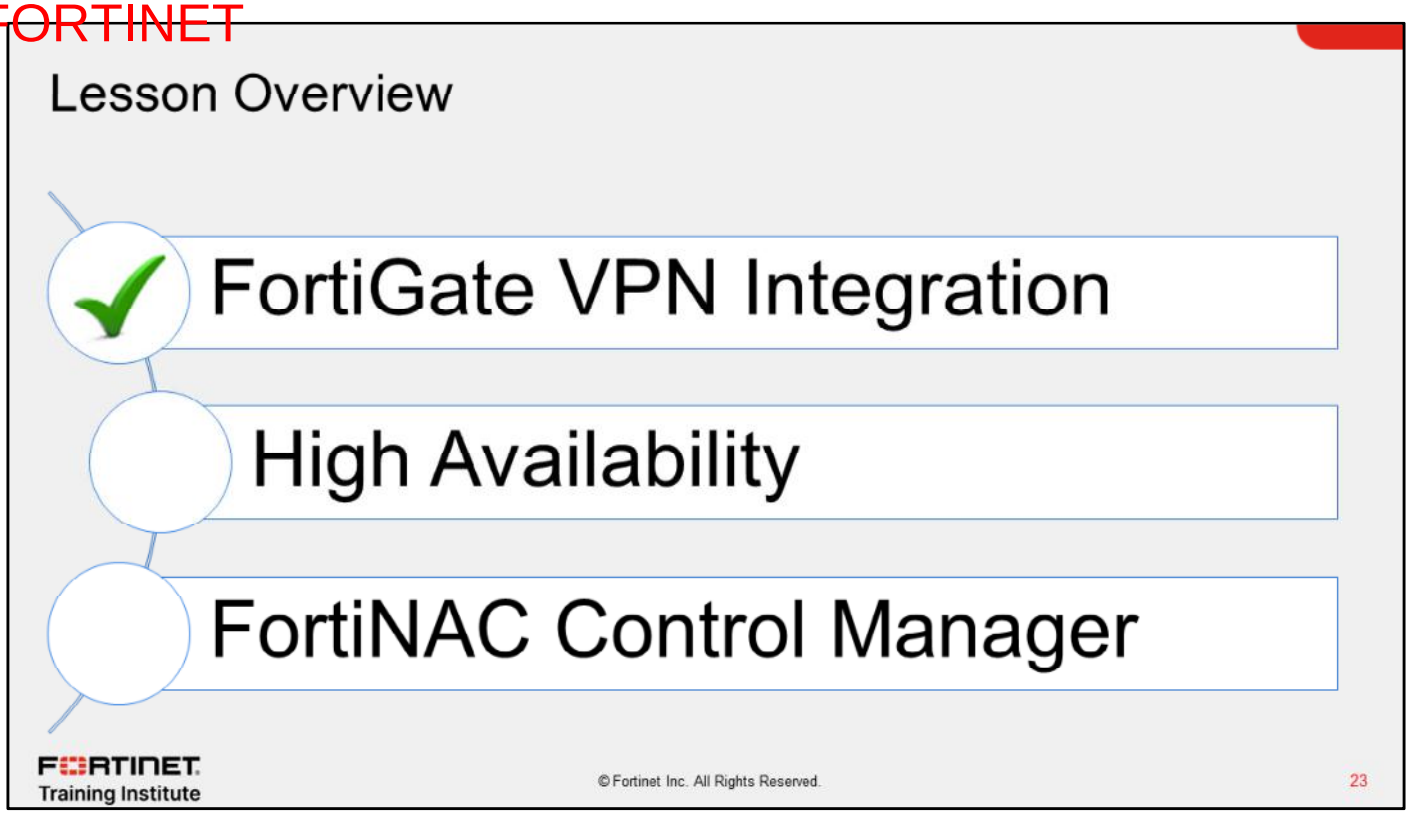
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

22

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

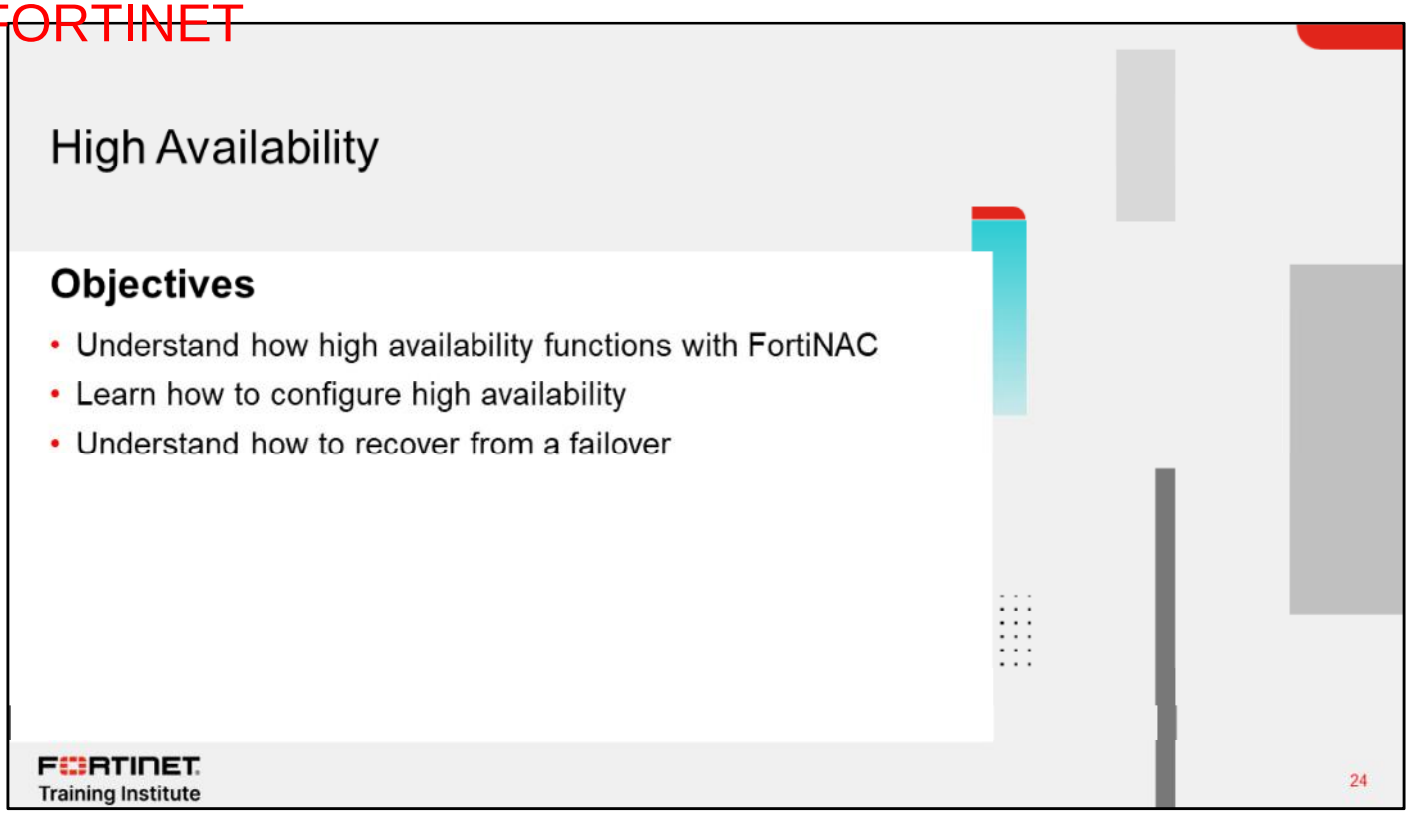


Good job! You now understand FortiGate VPN integration.

Now, you will learn about FortiNAC high availability.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

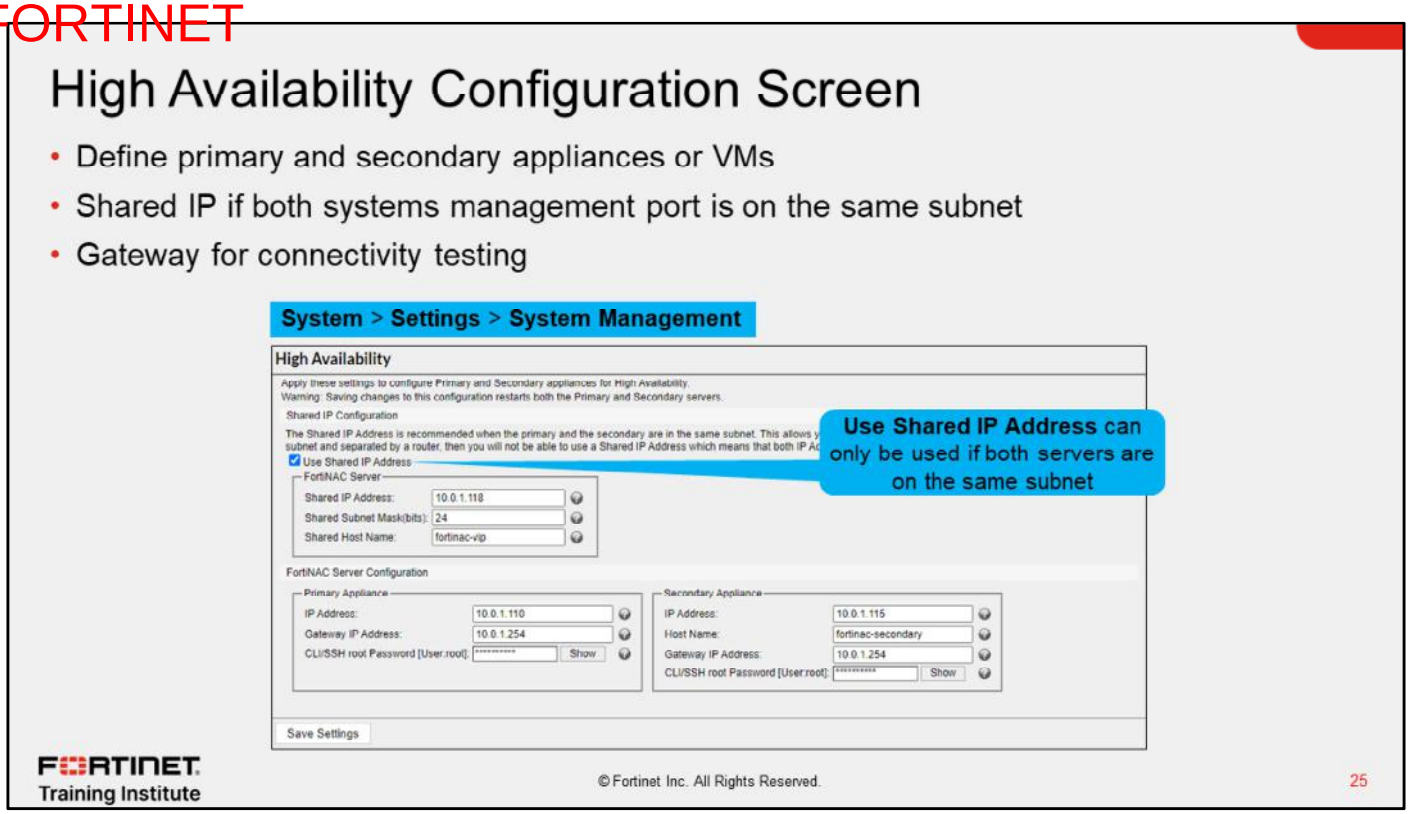


After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in how FortiNAC HA functions, how it is configured, and failover recovery procedures, you will be able to configure them in your environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **High Availability** screen is where you configure the necessary settings for HA configuration. You can use the **Use Shared IP Address** option if the eth0 interfaces of both the primary and secondary devices are on the same subnet. When you use the shared IP address option, you supply the IP address, mask, and hostname to be shared by the two devices. The **FortiNAC Server Configuration** settings are where you must define the IP address, gateway, and CLI/SSH root passwords for both the primary and secondary devices, and the host name is also required for the secondary device.

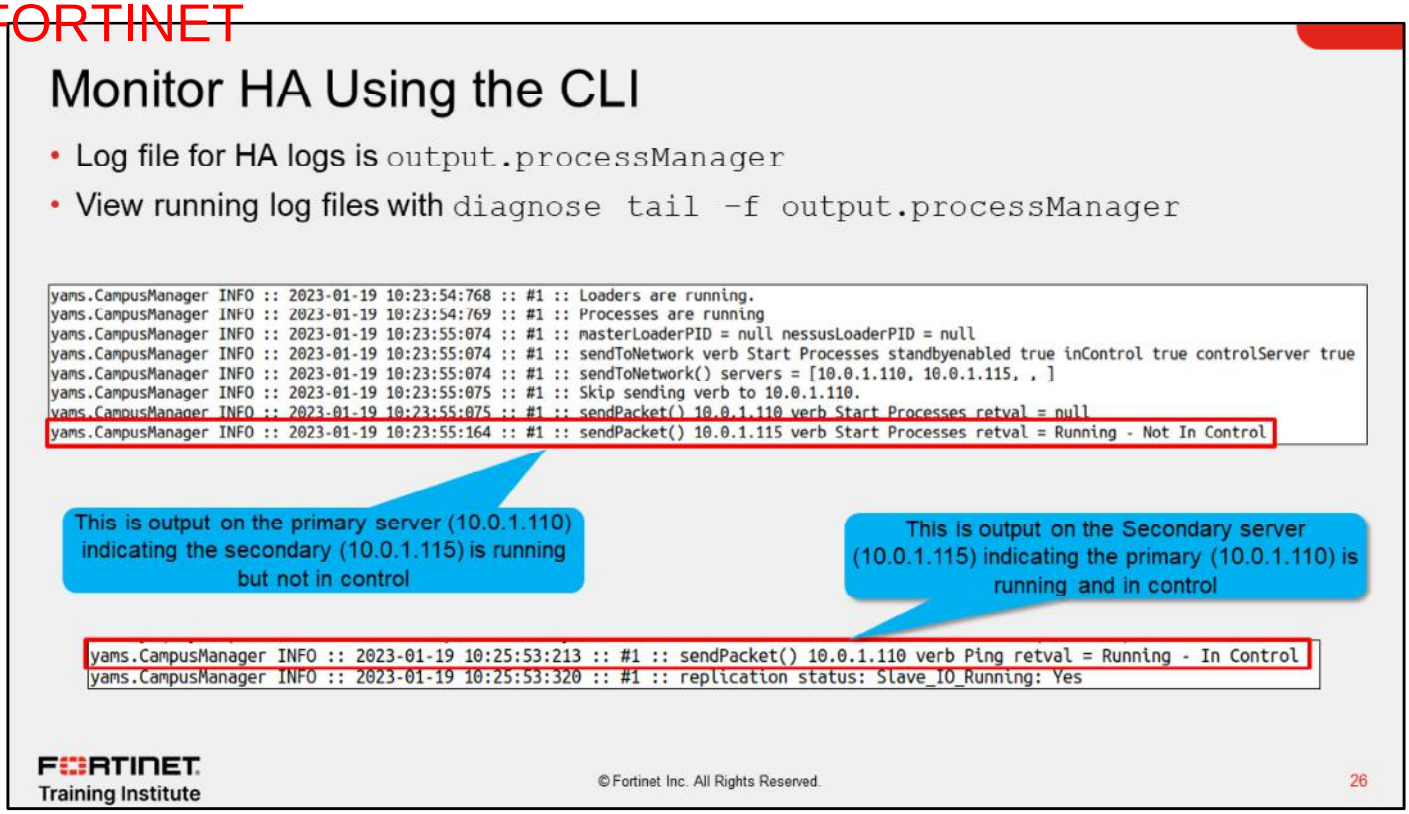
The purpose of the gateway designation is not for defining the subnet gateway to use for traffic flow, but instead is used by the devices to test network connectivity, and does not need to be on the same subnet. When the HA heartbeat fails five consecutive times, each device then attempts to ping the defined gateway. The result of the ping initiates the following behavior:

- Primary device validates network connectivity with a successful ping of the gateway: device continues to operate as the in-control device. Changes status of secondary to contact lost.
- Primary device fails network connectivity test with a failed ping of the gateway: device shuts down NAC processes and changes to a management down status.
- Secondary device validates network connectivity with a successful ping of the gateway: device starts NAC processes and status changes from *not in control* to *in control*.
- Secondary device fails network connectivity test with a failed ping of the gateway: device does not start NAC processes.

Remember, contact with the gateway is validated only after five failed HA heartbeats.

Vouchers & Dumps are Available | WhatsApp +201224560923

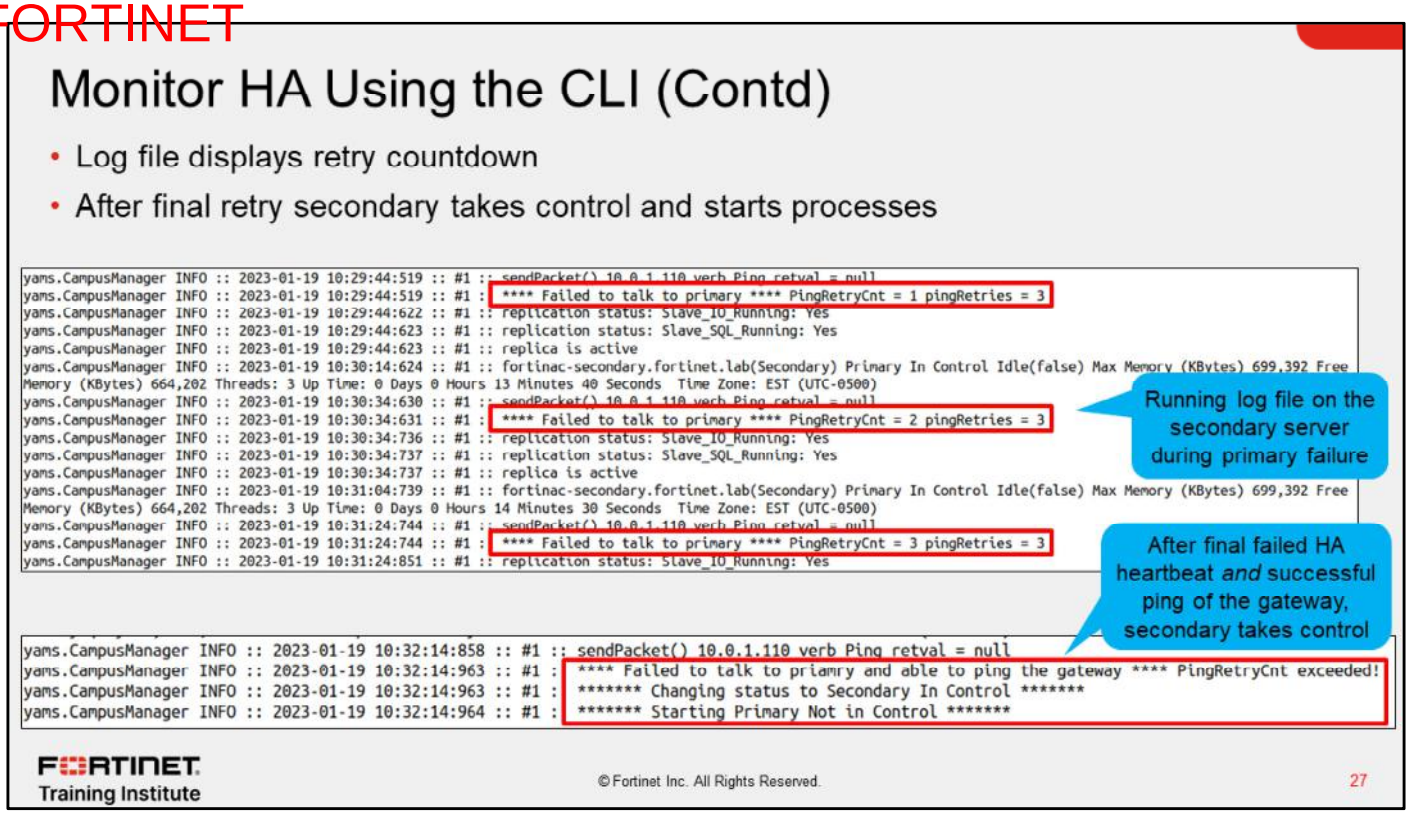
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can view information about the current state of an HA configuration within the `/bsc/logs/output.processManager` log file. You can view the log file real-time by using the `tf output.processManagr` command. The examples shown on this slide highlight output from both the primary and secondary servers when the HA configuration is running normally (primary in control).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



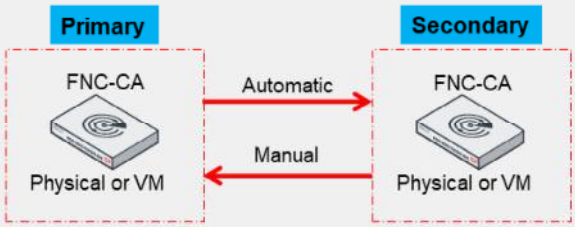
You can also monitor HA failover. In the example shown on this slide, the `output.processManager` log file on the secondary device is posting the results of the HA heartbeat. After five consecutive failed attempts, the secondary server pings the gateway to validate network connectivity. Network connectivity is validated successfully and the secondary device changes status and assumes control.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Restoring Control to Primary

- Restoring control to the primary is a manual process



System Summary — Manual

	FortiNAC-CA	
	Primary	Secondary
Host Name	fortinac-primary.fortinet.lab	fortinac-secondary.fortinet.lab
Status	Running - In Control	Running - Not In Control
Product	FortiNAC-CA	FortiNAC-CA
Version	7.2.1.6038	7.2.1.6038
Appliance	FNVMCA	FNVMCA
Serial Number	FNVMCATM21000728	FNVMCATM21000729
Certificates	Yes	Yes
OS	CentOS	CentOS
	Resume Control	

Button will be active when **Primary** is not in control

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

28

In the event of a failover, control is passed from the primary FortiNAC to the secondary FortiNAC. This generates a **System Fail Over** alarm, which is reflected in the **Summary** panel on the dashboard. The **Status** in the panel will change from **Running – In Control** to **Management Down** for the primary server, and from **Running – Not In Control** to **Running – In Control** on the secondary server.

Returning control to the primary server is a manual process. After the cause of the failover has been resolved, transfer control back to the primary server using the **Resume Control** button located in the primary server column of the **Summary** panel. The button will be active only when the secondary server is in control.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which log file contains HA status details?
   A. Output.master
   ✓ B. Output.processManager

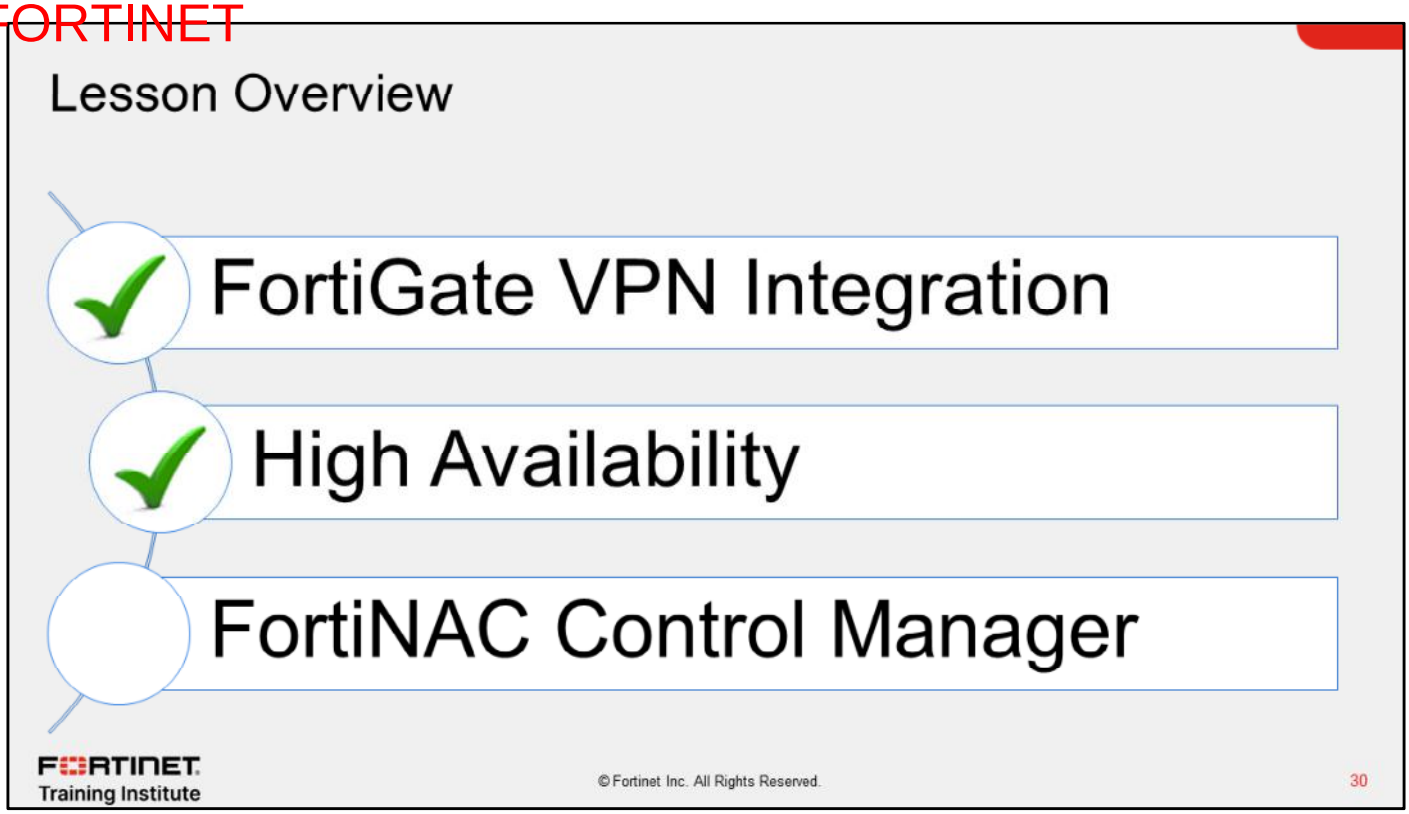
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

29

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

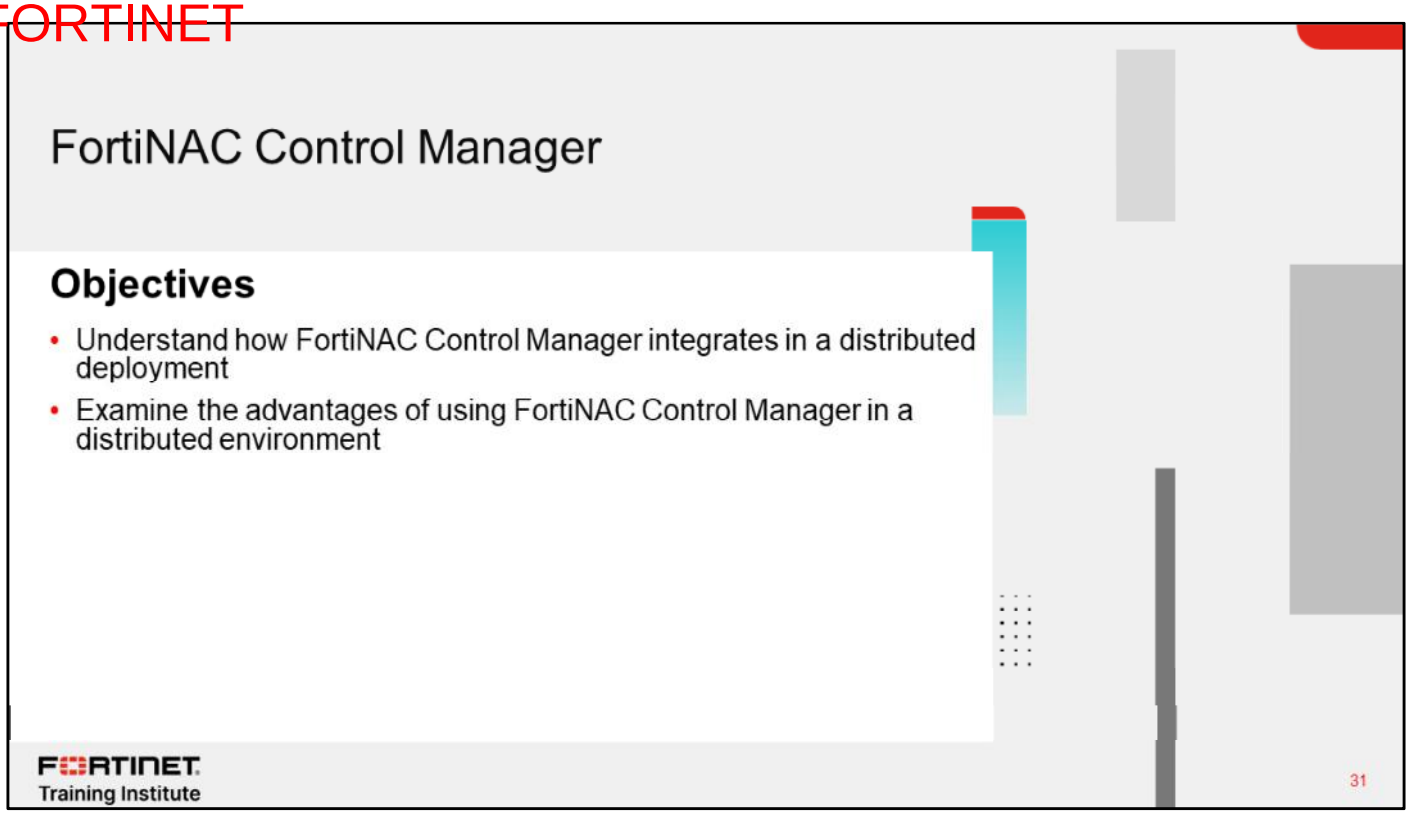


Good job! You now understand FortiGate VPN integration.

Now, you will learn about FortiNAC Control Manager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this section you should be able to achieve the objectives shown on this slide.

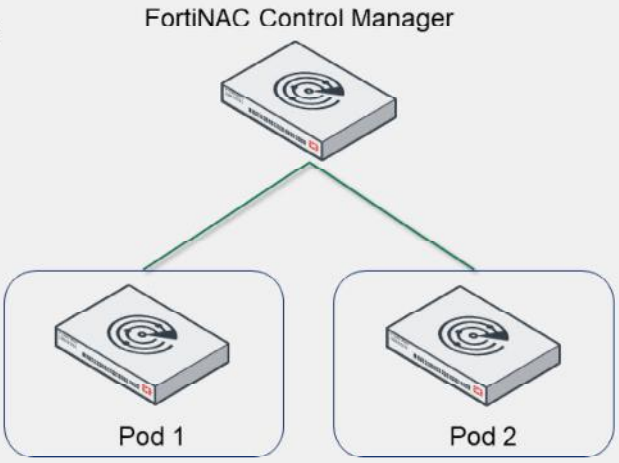
By understanding the concepts and advantages of FortiNAC Control Manager, you will be able deploy and manage FortiNAC devices in a distributed environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiNAC Control Manager Deployment

- Manages multiple FortiNAC devices in a distributed environment
- Each managed FortiNAC is added as a server in FortiNAC Control Manager
- Provides:
  - Global version control
  - Pooled licenses
  - Scalability
  - Global management
  - Global visibility



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

32

FortiNAC Control Manager provides the ability to manage multiple FortiNAC devices. FortiNAC devices are added for management individually to the FortiNAC Control Manager.

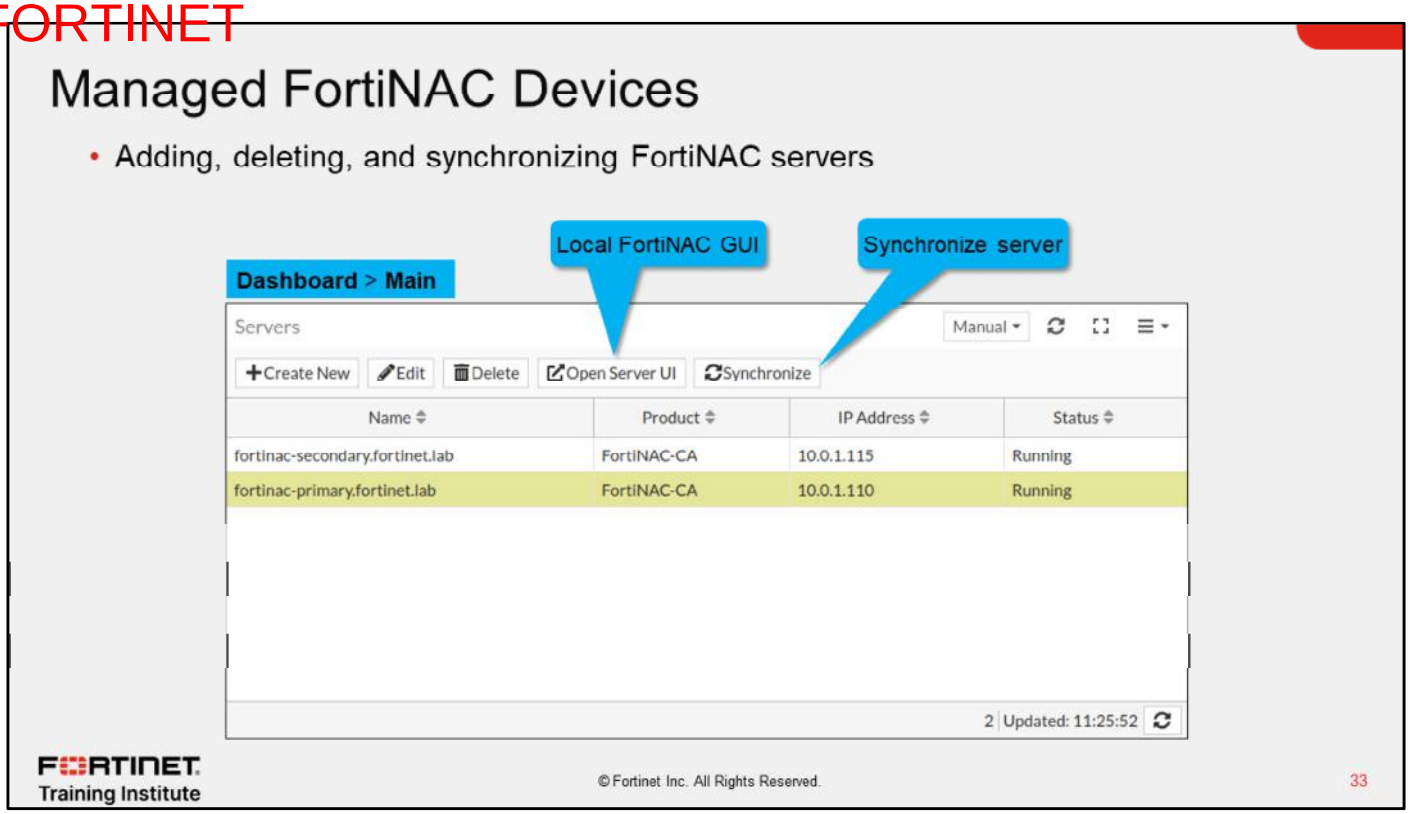
FortiNAC Control Manager can then update all managed FortiNAC devices to ensure that each device is operating with the same revision.

Licensing is pushed down from the FortiNAC Control Manager to the FortiNAC devices that it manages, dynamically distributing the concurrent license counts as needed. This architecture allows FortiNAC to scale to even the largest environments.

Global management and visibility provide a single simplified administration in large distributed deployments.

Vouchers & Dumps are Available | WhatsApp +201224560923

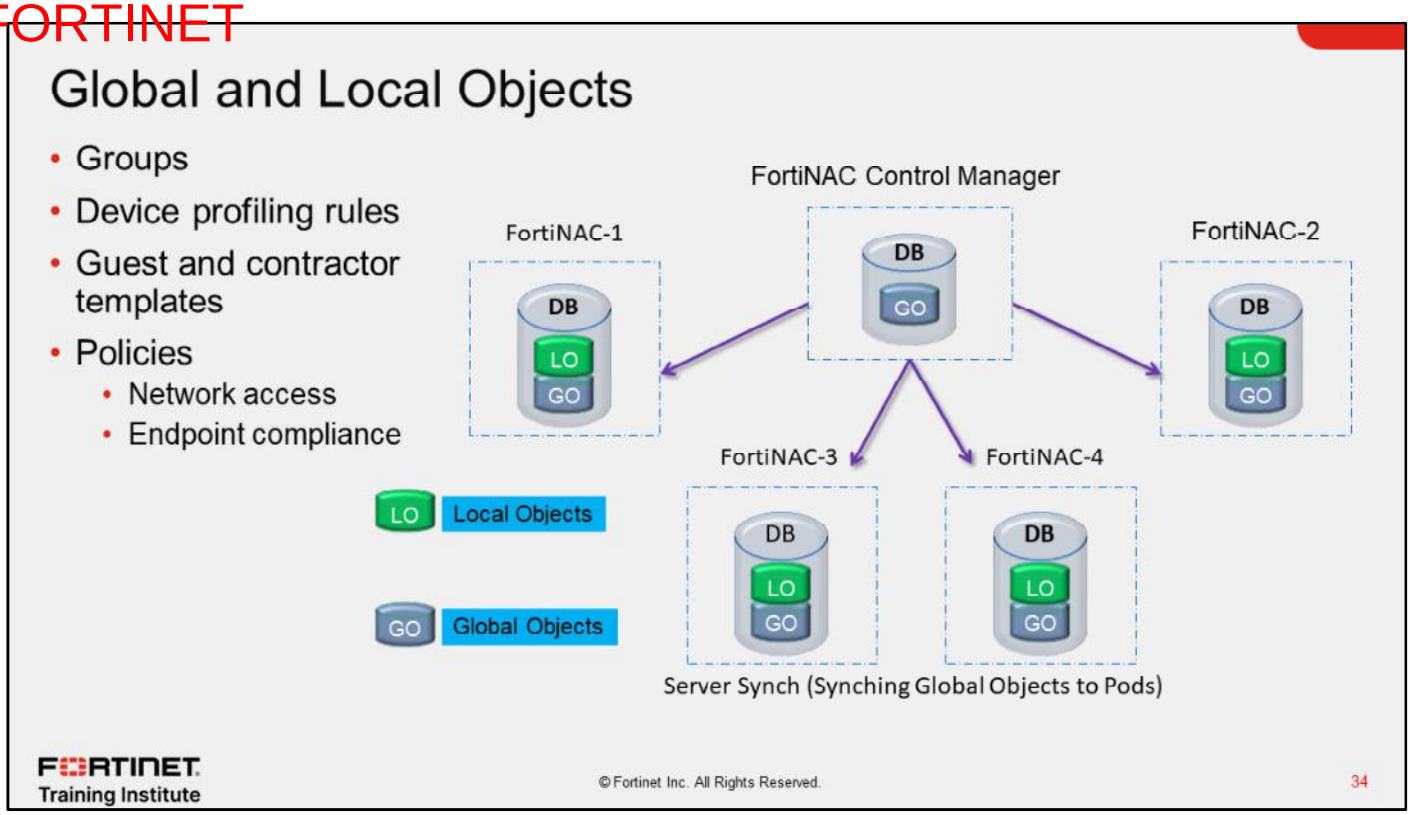
DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiNAC devices are added to a FortiNAC Control Manager in the **Server List** panel in the **Dashboard** view. FortiNAC devices configured as an HA pair, will display the status of the pair in the **Status** column. Buttons to the left of each server allow for the deletion or synchronization of the server. Buttons to the right provide quick access to the local FortiNAC GUI or properties view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



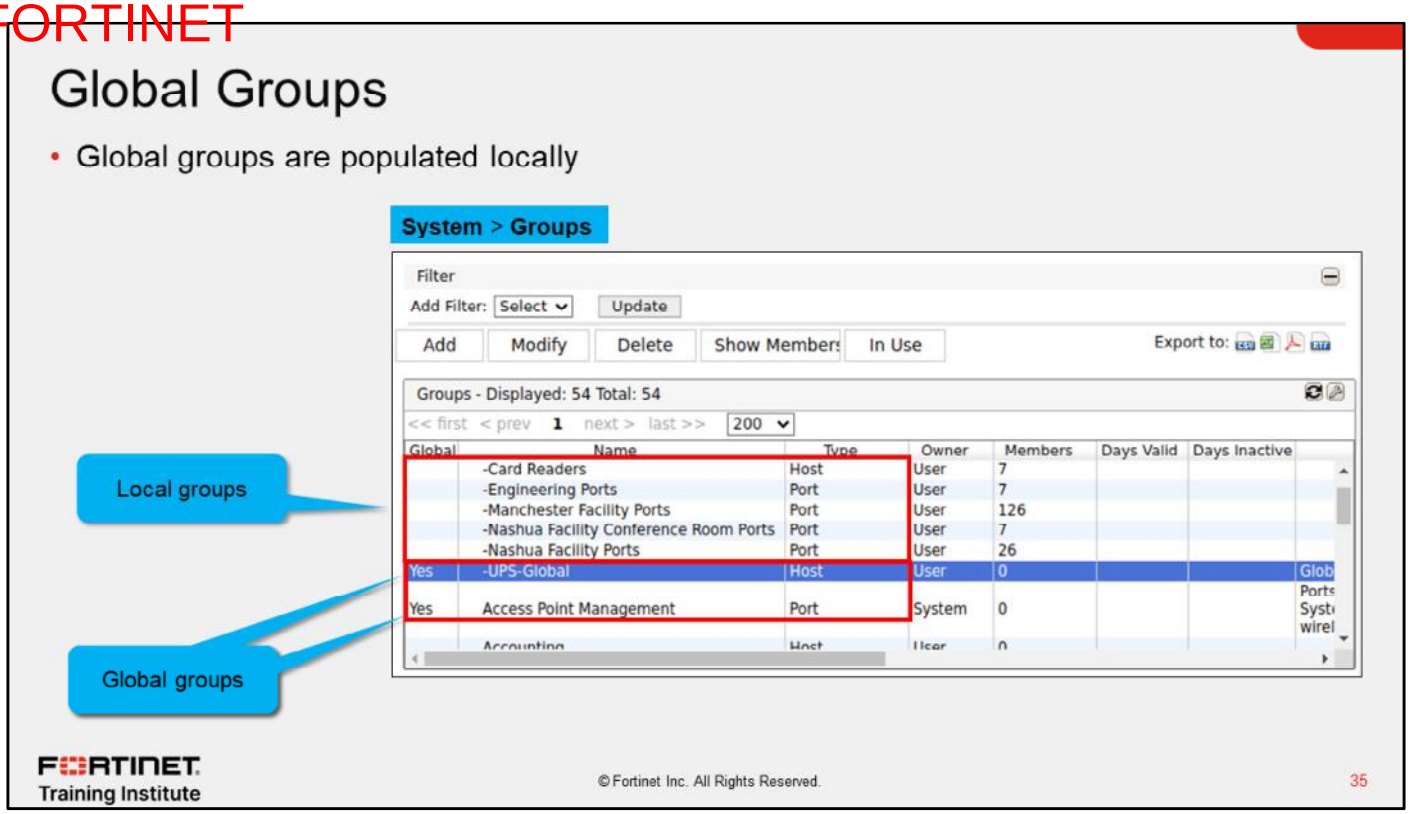
When a FortiNAC device is added to a FortiNAC Control Manager, the concept of global objects is introduced. Each managed FortiNAC synchronized with the manager inherits the global objects configured at the manager. Global objects provide the ability to perform often repetitive configurations once. In addition to the global objects, each FortiNAC device will maintain local objects. For example, each FortiNAC database will have both local groups and global groups.

Global object views display a new column, titled **Global**. A value of **Yes** in the **Global** column indicates the entry was synchronized form the manager; if the column is blank, the entry is local.

Global objects include:
- Groups
- Device profiling rules
- Guest and contractor templates
- Polices

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Groups created on FortiNAC Control Manager, once synchronized, will appear as global entries in the local FortiNAC views. Global group entries can have membership defined at the local FortiNAC level. For example, a group intended to contain all conference room ports could be created at the FortiNAC Control Manager, and then that group would be populated with ports known by each local FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Global Device Profiling Rules

- Global device profiling rules rank below local rules

Users & Hosts > Device Profiling Rules

Add | Modify | Delete | Copy | Run | Import / Export | Export to:

Device Profiling Rules - Total: 25

Rank: Set Rank | Enable: | Rogue Evaluation Queue Size:0 Detail Flush

Global	Enabled	Rank	Name	Type	Registration	Methods	Re
	✓	1	Our IP Phones	IP Phone	Automatic	Vendor OUI	
	✓	2	Card Readers	Card Reader	Automatic	Vendor OUI	
	✓	3	Cameras in Manchester	Camera	Automatic	Location, Vendor OUI	
	✓	4	Cameras in Nashua	Camera	Automatic	Location, Vendor OUI	
	✓	5	Environmental Control Units	Environmental Control	Automatic	SNMP, TCP, Vendor OUI	
	✓	6	Healthcare Device	Health Care Device	Automatic	SSH, TCP, Vendor OUI	
	⊘	7	IP Phones	IP Phone	Manual		
Yes	✓	8	Tripp Lite UPS Systems	UPS	Automatic	Vendor OUI	
Yes	⊘	9	Medical Device	Health Care Device	Automatic	Vendor OUI	
Yes	⊘	10	Android (DHCP)	Android	Automatic	DHCPv4	
Yes	⊘	11	Apple iOS (DHCP)	Apple iOS	Automatic	DHCPv4	

FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

36

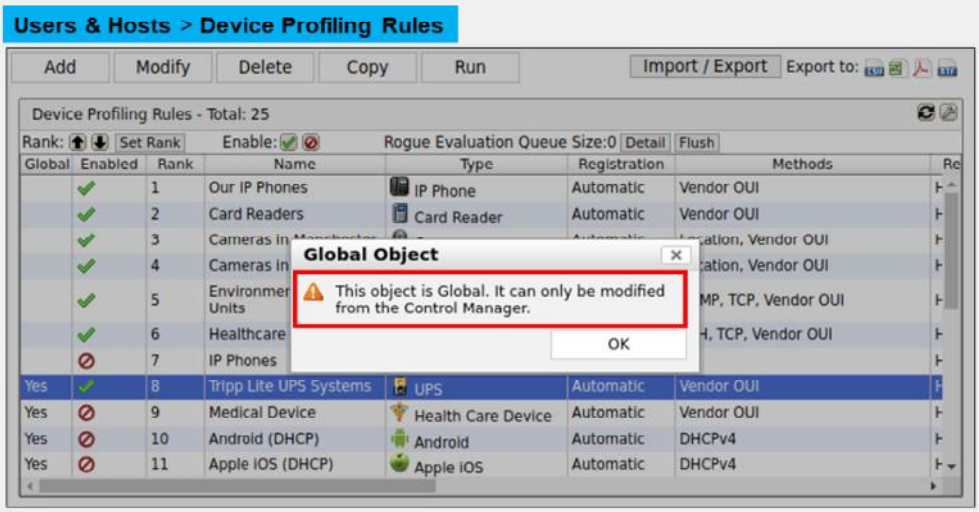
Device profiling rules created on FortiNAC Control Manager will appear, in the ranked order set at the manager, below the last ranked local rule. This is done so that local rules are evaluated before global rules. This prevents a less granular rule, created at the manager, from incorrectly classifying devices locally. In a distributed environment, the types of devices found from one location to the next could be very different. For example, a hospital administrative building may have very different devices than the hospital itself. However, there may be many universal devices across both locations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Device Profiling Rules (Contd)

- Global elements that are ranked can be re-ordered only at the manager



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

37

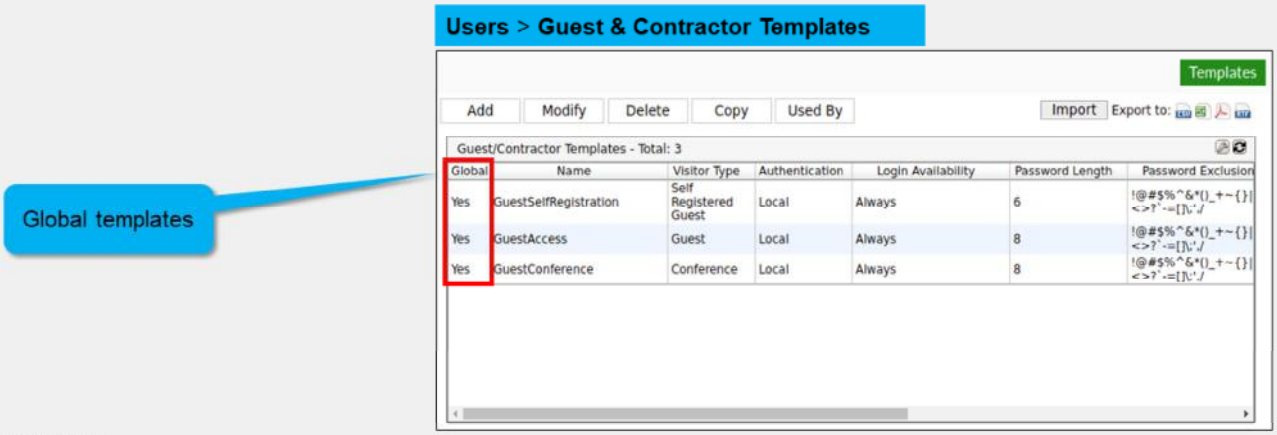
You cannot modify or change the ranking of global device profiling rules from a local FortiNAC. All global rule changes must be made at the FortiNAC Control Manager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Global Guest and Contractor Templates

- Global templates
- Created and managed on FortiNAC Manager
- Synchronized to local FortiNAC



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

38

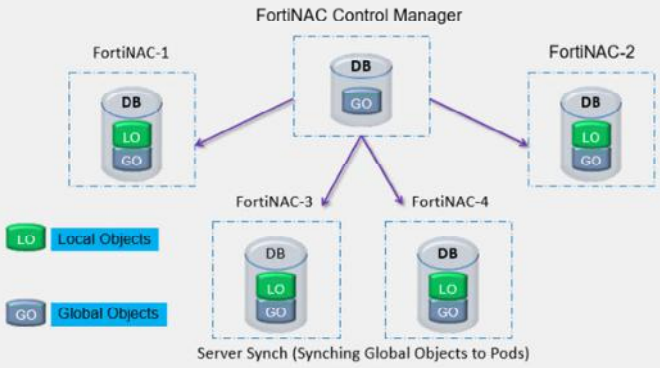
Guest and contractor templates can be centrally managed on FortiNAC Control Manager, and then used for guest and contractor account creation on each local FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Global Policies

- User/host profiles created at FortiNAC Control Manager use global groups
- Network access configurations use globally defined logical networks
- Endpoint compliance configurations use globally defined configurations and scans
- Synchronization pushes policies and policy components to the managed FortiNAC devices



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

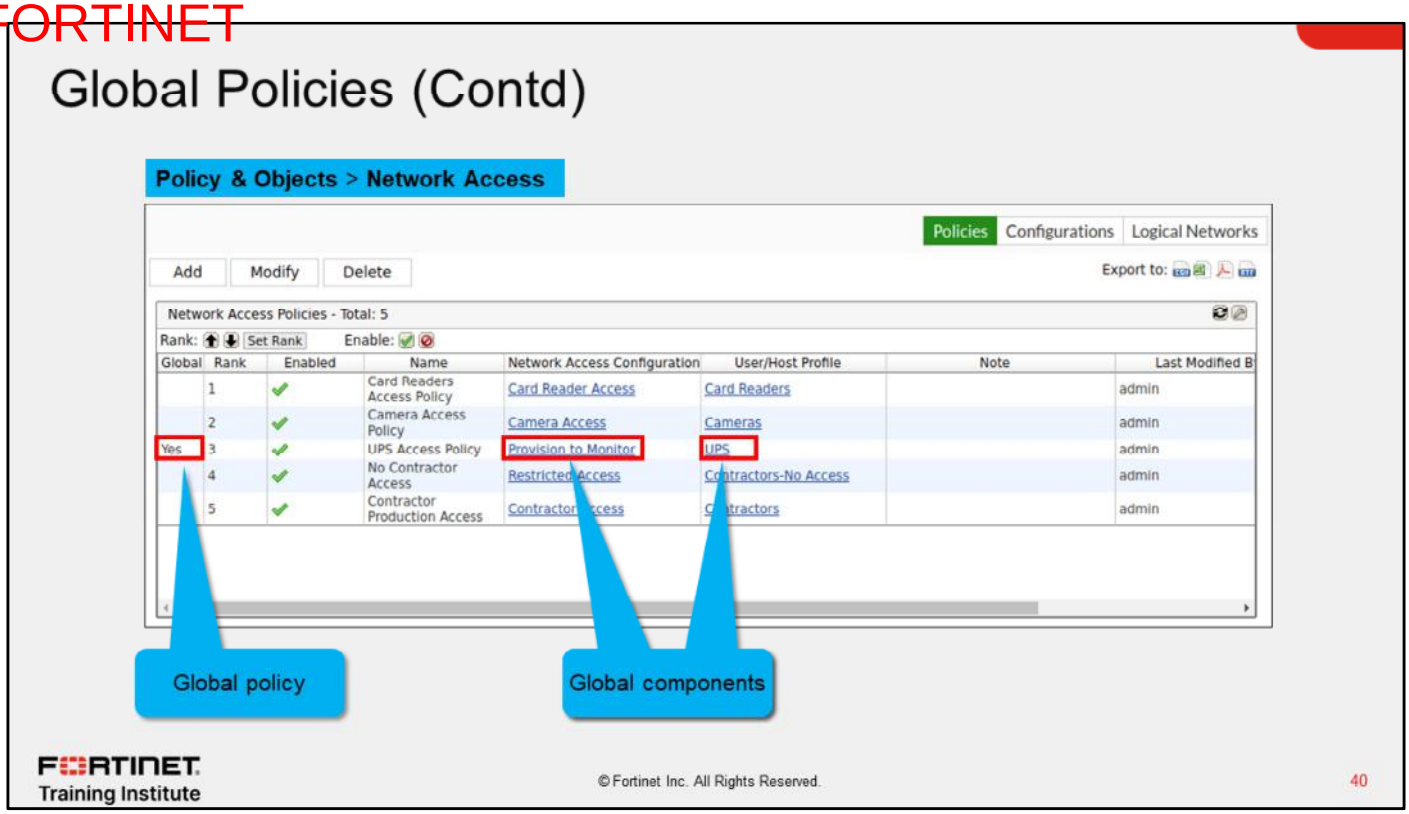
39

Policies created at the FortiNAC Control Manager use global components. User/host profiles created globally will be comprised of globally created groups. Global groups can have other global groups nested within them, but with the exception of administrator groups, these groups must be populated at the local FortiNAC device. For example, a global user/host profile could contain a global port group called Restricted Ports, but the actual designation of ports to that group would be performed at the local FortiNAC. The FortiNAC Control Manger does not have a network inventory view like a local FortiNAC device, and as a result, does not have port objects in the database.

The polices and configurations created globally will be pushed to each local FortiNAC when the devices are synchronized.

Vouchers & Dumps are Available | WhatsApp +201224560923

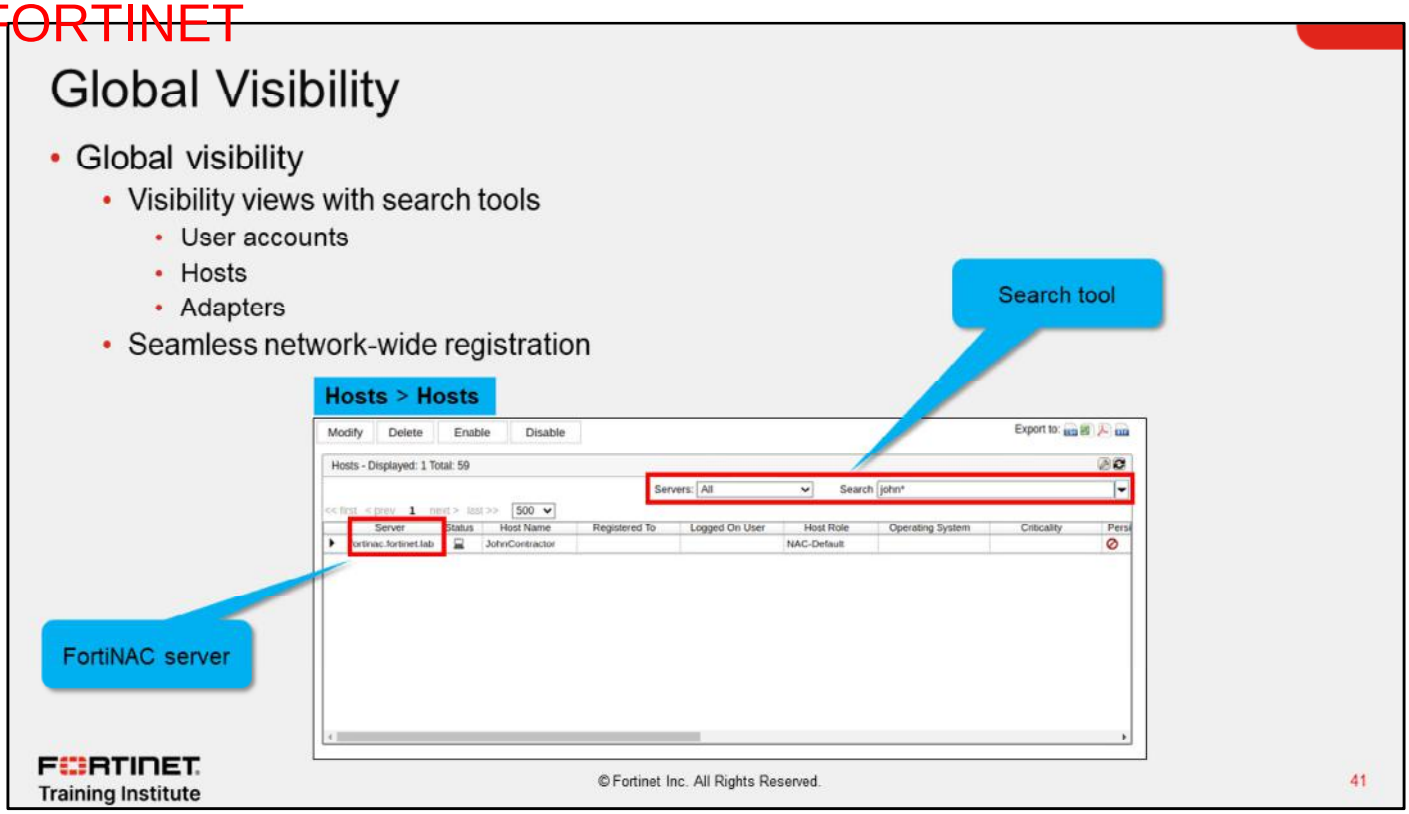
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Network access and endpoint compliance policies created at the FortiNAC Control Manager, along with policy components (configuration and user/host profiles), will appear on the local FortiNAC devices once synchronization has completed. Unlike device profiling rules, policy rankings can be set at the local FortiNAC device.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

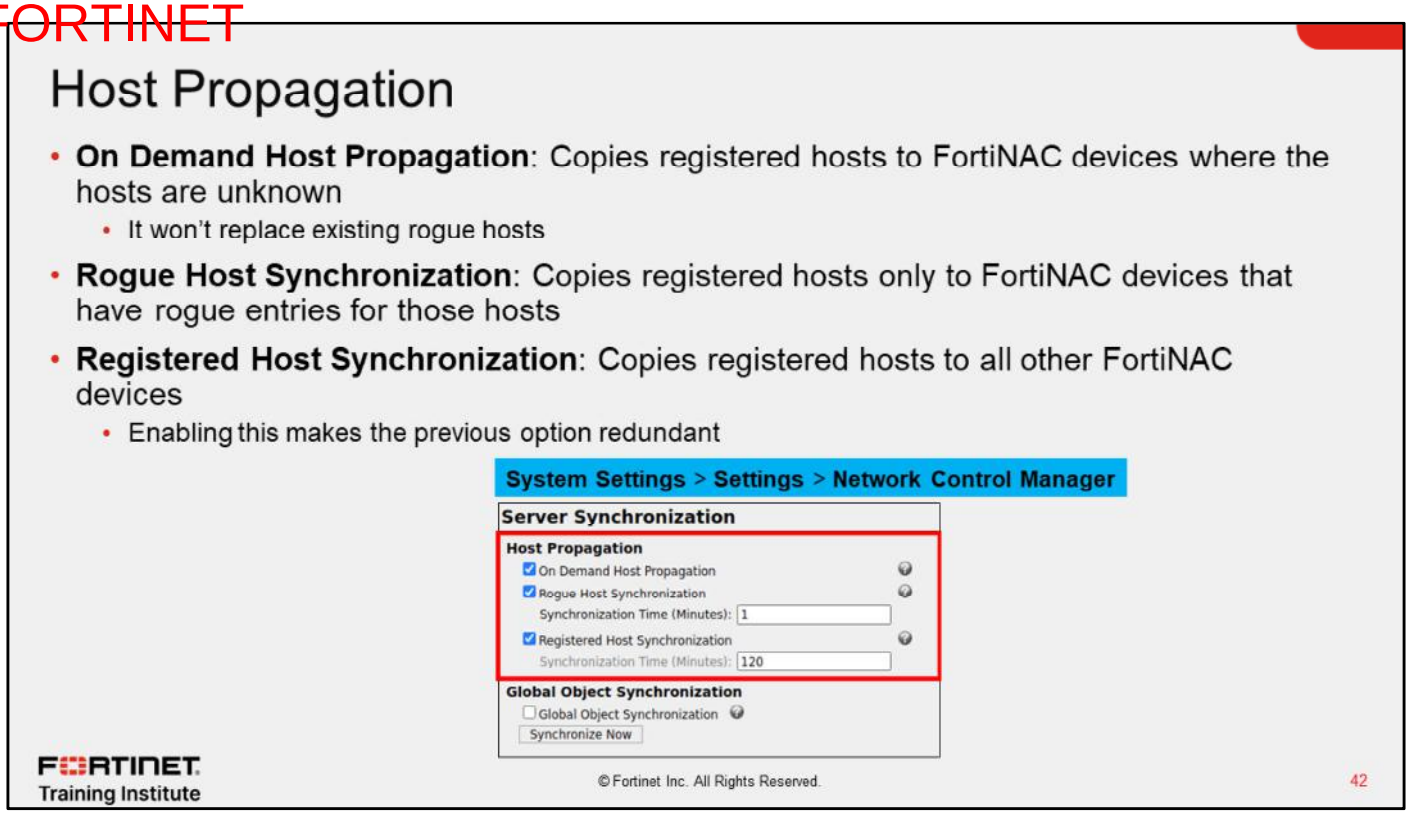


FortiNAC Control Manager brings together the user and endpoint visibility information form each FortiNAC it manages, to create a global repository of user accounts, hosts, and adapters. The integrated search tools within each view provide an efficient means to located objects quickly. User account and endpoint information received by the FortiNAC Control Manager include the local FortiNAC devices they were received from, so searches can be filtered to individual FortiNAC devices.

The global collection of users and endpoints provides seamless network-wide registration. For example, a host registered with one FortiNAC device can be updated with other FortiNAC devices, so that roaming endpoints would not need to be on-boarded or classified multiple times.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The way in which host records are propagated to, and synchronized with, other managed FortiNAC devices, is configured at the FortiNAC Control Manager. The host propagation options are:

- **On Demand Host Propagation**: This option copies registered host records that are known on any FortiNAC, to all other managed FortiNAC devices that do not contain a rogue record for those host.
- **Rogue Host Synchronization**: This option copies registered host records only to FortiNAC devices that have a rogue record for that host.
- **Register Host Synchronization**: This option copies registered host records to all FortiNAC devices.

If both synchronization options are disabled, the FortiNAC Control Manager can query all control servers when a host connects to determine the host's previous state. However, choosing one of the copy options reduces the amount of time a host waits to be connected to the network and provides a better user experience.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Host Propagation Scenario

1. A host connects to the network through FortiNAC Server A, and is added as a rogue
2. The host is directed to the registration page but does not register and disconnects
3. Later, the host connects to the network through FortiNAC Server B
4. The host completes the registration process and becomes registered on Server B
5. NAC Server C has never seen the host

The host now exists in different states on different servers



FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

43

The scenario shown on this slide outlines how a host could exist in different states across different FortiNAC devices.

A rogue connected to the network, with the point of connection managed by Server A, would appear as a rogue to that server. If the host disconnects before completion of ther egistration or classification process, the host will remain known as a rogue to Server A.

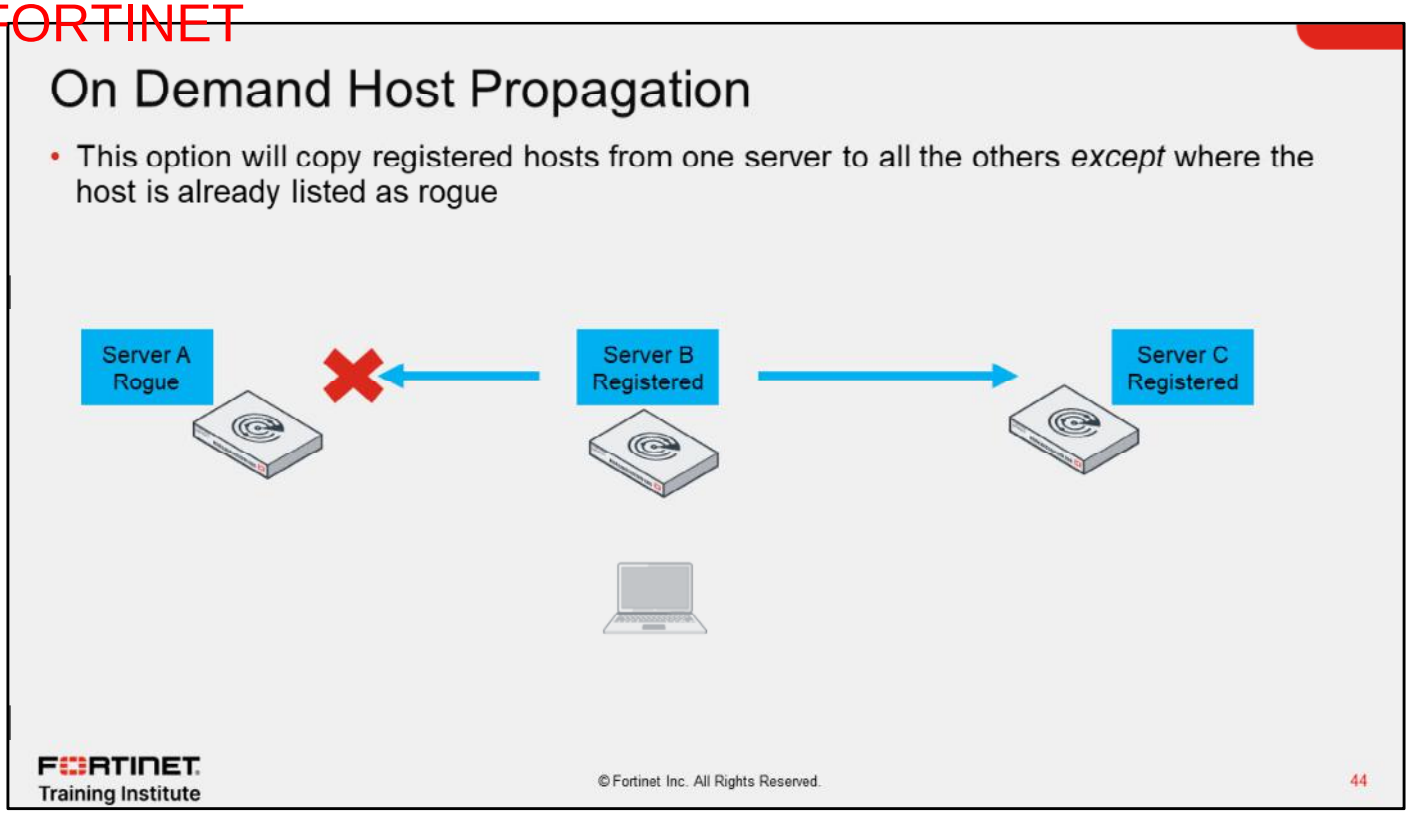
If the same host then connects through a point of connection managed by Server B and is successfully classified, the host will be know to Server B as a registered host.

The host has never connected to a point of connection managed by Server C, so the host is unknown to that server.

This host now exists in different states on two different FortiNAC devices, and remains unknown on a third. Propogation and synchronization of host records is configured to handle situations like this.

Vouchers & Dumps are Available | WhatsApp +201224560923

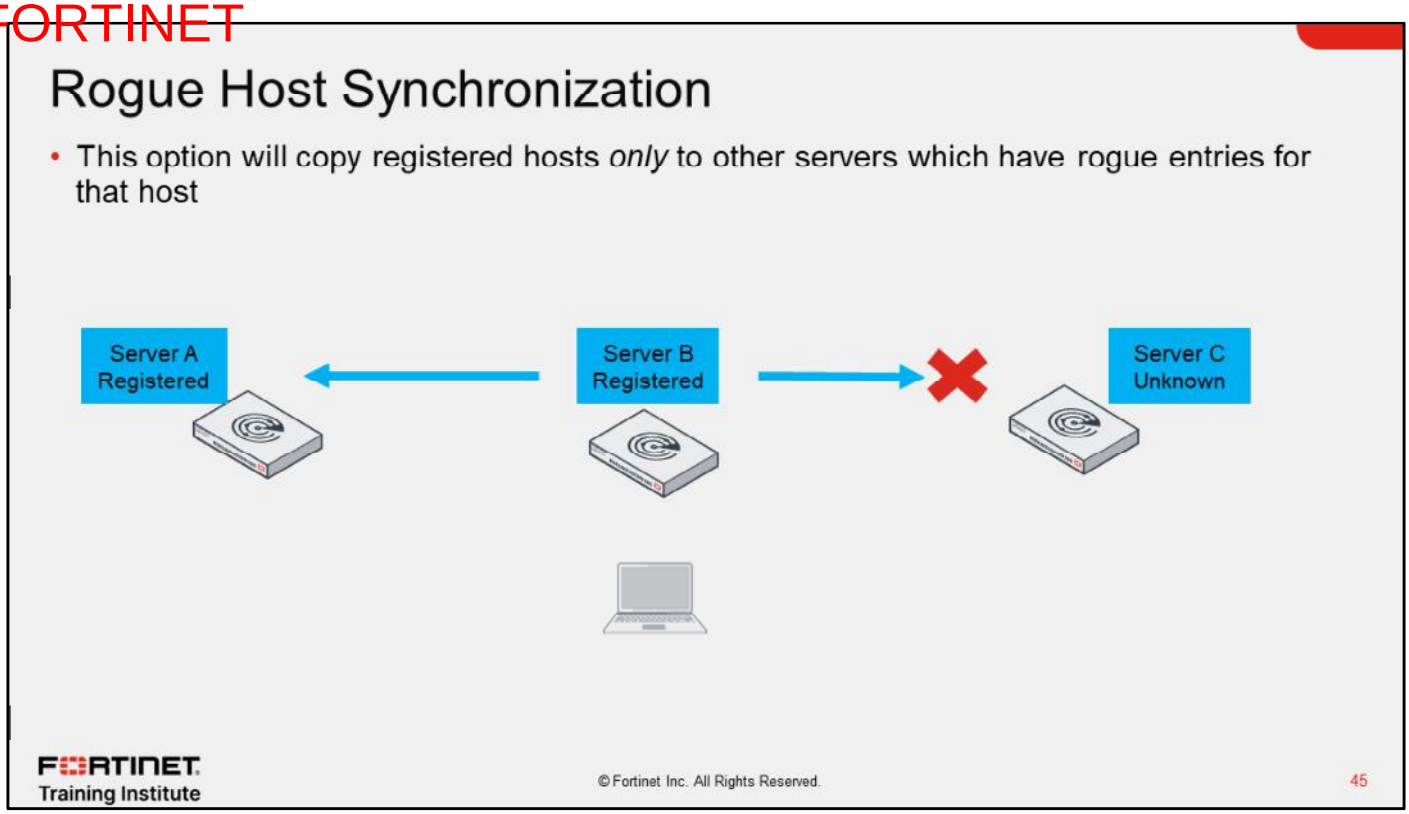
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Enabling the **On Demand Host Propagation** option copies a registered host from one managed server to all other managed servers when the host registers. However, if the host is already a rogue on a different managed server, the registered host is not copied. For example, if the host is a rogue on Server A, is registered on Server B, and is unknown on Server C, then the registered host that exists on Control Server B, is copied to Control Server C, but the existence of the rogue on Control Server A prevents it from being copied there. The user would need to re-register the host on Control Server A, if it connects there.

Vouchers & Dumps are Available | WhatsApp +201224560923

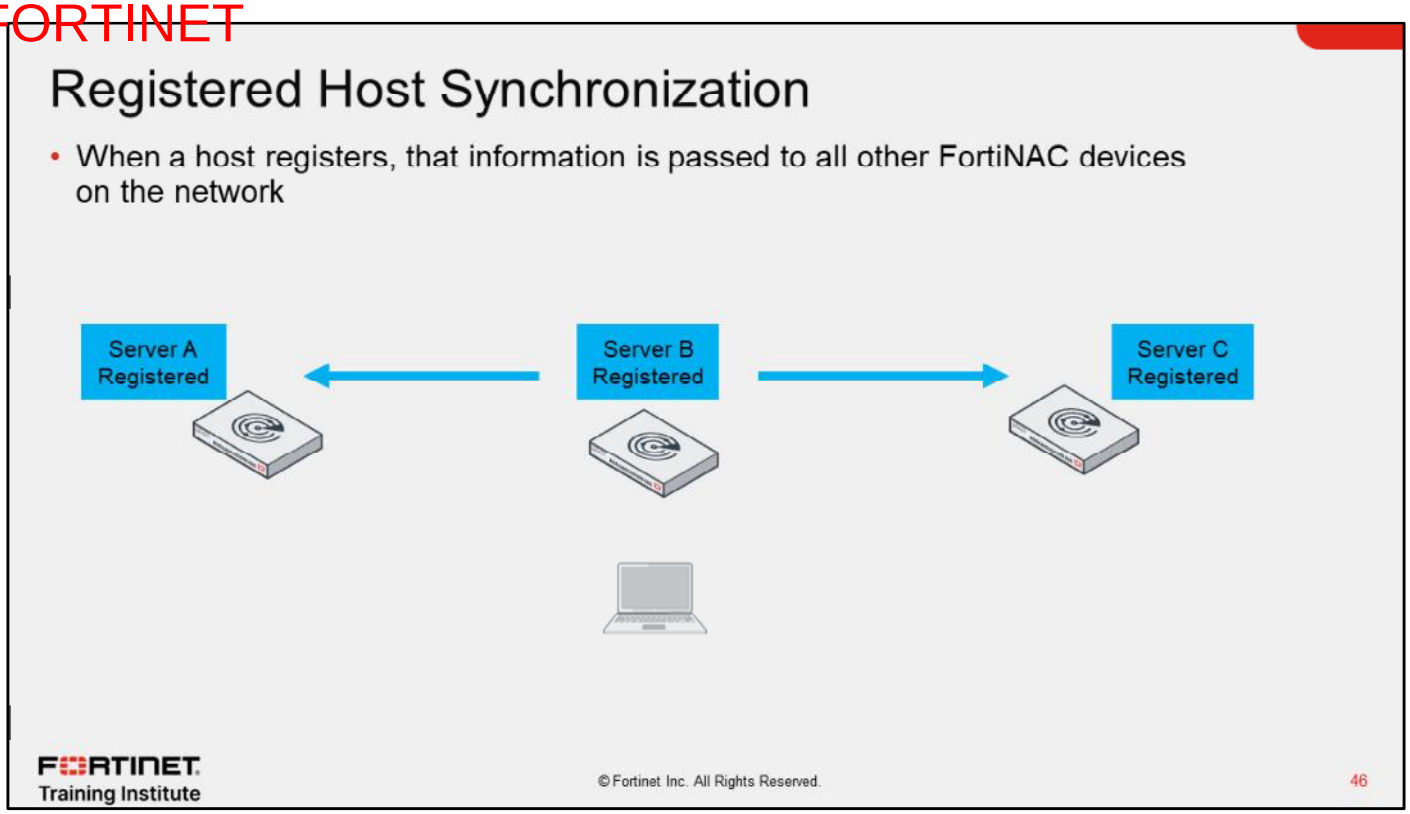
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Enabling the **Rogue Host Synchronization** option stops a rogue host from having to re-register on a second Server, if it is already registered or classified on any other Server. This option copies registered hosts only to servers that have rogue hosts, not to all servers. Choosing this option uses less bandwidth than the registered host synchronization feature. It also allows you to view which servers a host has connected to.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

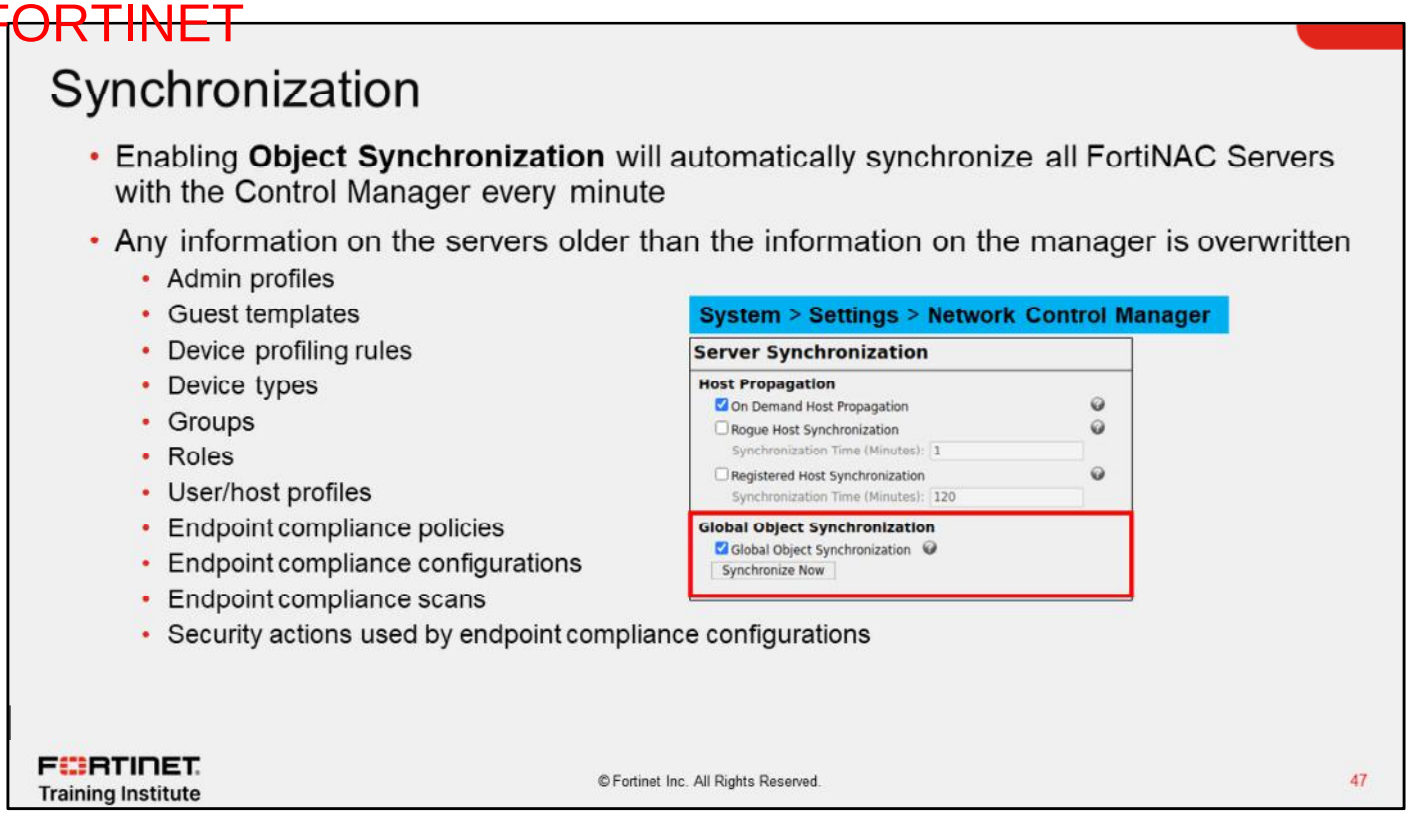


Enabling the **Registered Host Synchronization** option alleviates the need to determine whether or not an individual host is registered for each control server. When the host registers, that information is passed to all other control servers on the network. If you choose this option, you do not need to choose the previous option, since all hosts are copied to all servers.

After a host is registered on a control server, the host's enabled/disabled status will be propagated, but no other attribute or state changes are propagated. The registered host synchronization feature is used to speed up the registration process in an environment with multiple control servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Enabling **Global Object Synchronization** automatically synchronizes information between the FortiNAC Control Manager and the FortiNAC servers. The information on the FortiNAC Servers will be read-only. Automatic synchronization occurs once per minute. **Global Object Synchronization** is disabled by default. Adding a FortiNAC Control Manager to an existing deployment could cause unintended issues if the existing FortiNAC devices were not deployed with global management concepts in mind. Migrations of existing environments can be performed one FortiNAC device at a time.

Clicking the **Synchronize Now** button will manually synchronize information between the FortiNAC Control Manager and the FortiNAC Servers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Knowledge Check

1. Which configurations can have ranking adjusted at the local FortiNAC?

✓ A. Network access policies

B. Device profiling rules

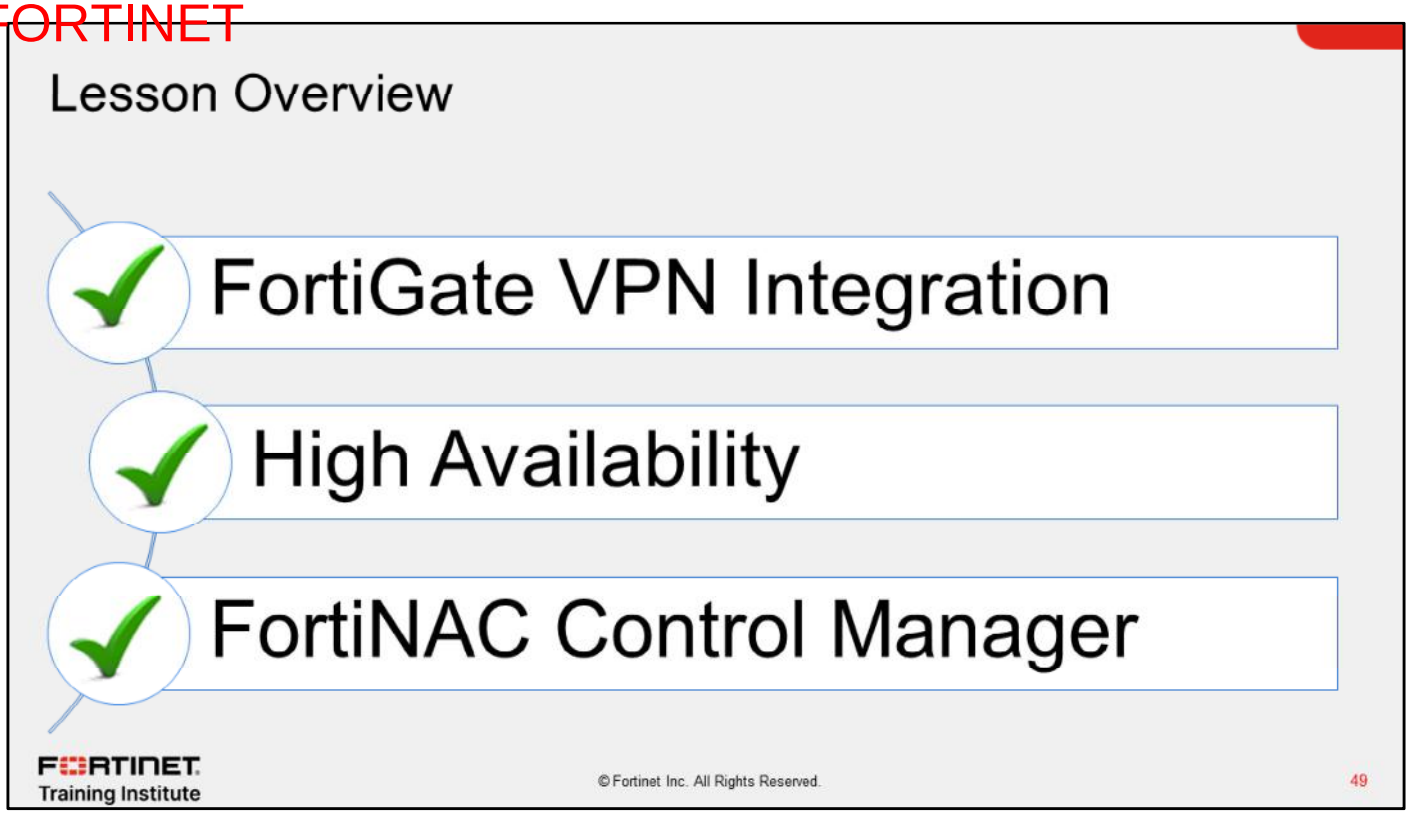
FORTINET Training Institute

© Fortinet Inc. All Rights Reserved.

48

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

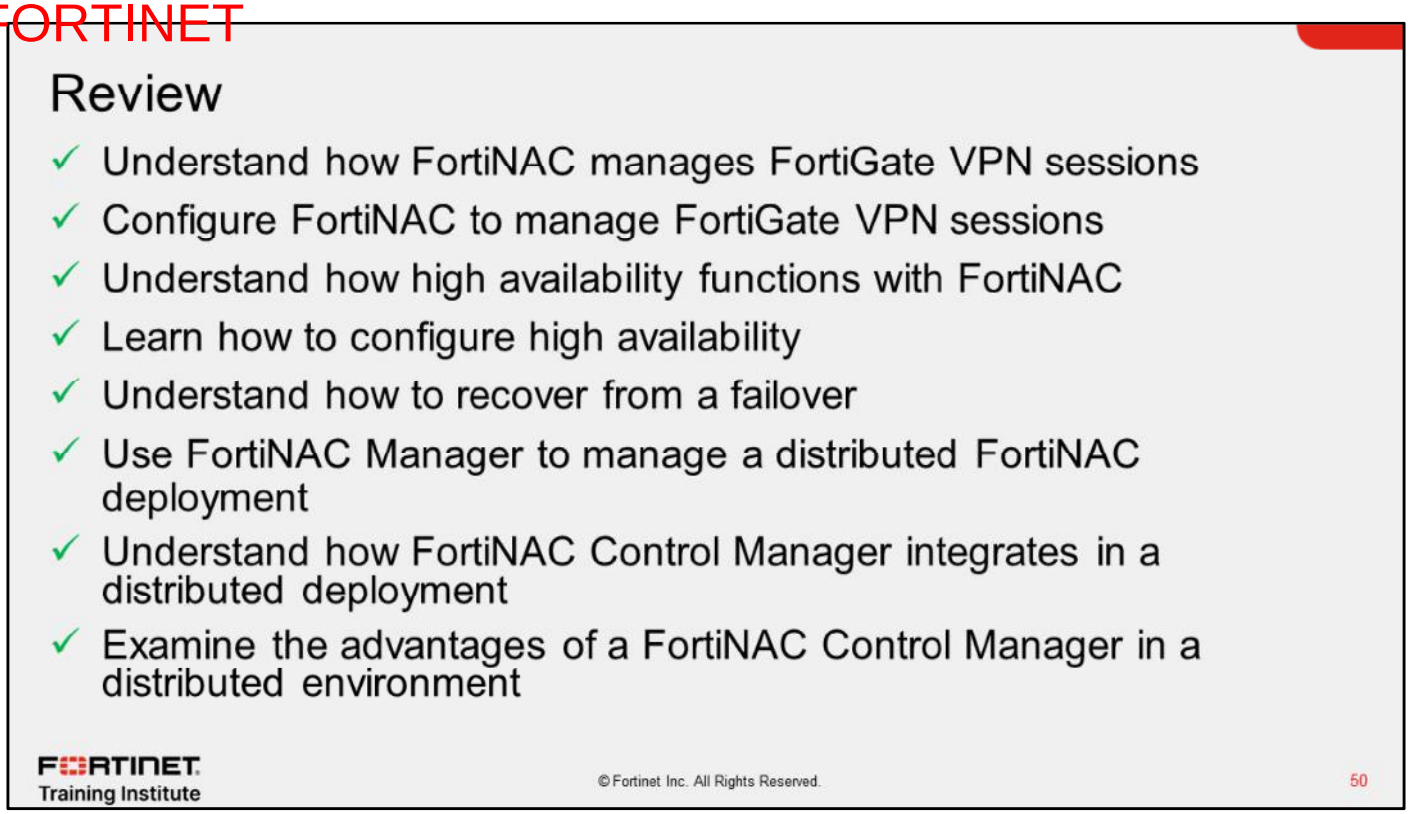


Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to manage FortiGate VPN using FortiNAC, and how FortiNAC Control Manger can be used to manage distributed environments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FORTINET

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Vouchers & Dumps are Available | WhatsApp +201224560923